



POLITECNICO DI TORINO

DEPARTMENT OF CONTROL AND COMPUTER ENGINEERING (DAUIN)

Master Degree in Computer Engineering

Master Degree Thesis

An Analysis of SOC Monitoring Systems

Author: Massimo MENNUNI

Advisor: Alessandro SAVINO

Co-Advisor(s): Nicolás MAUNERO

December, 2023

Abstract

Since 2016, ENISA (European Network and Information Security Agency) has defined the NIS (Network and Information Security) directive with the aim of ensuring high levels of security for public and private operators in critical sectors providing essential services to the European States. All EU member must take actions to ensure that these operators adopt appropriate information security measures to prevent and manage cyber security incidents, which may compromise national security. In Italy, the NIS Directive was implemented with the Legislative Decree 65/2018 that has also introduced the PNSC (Perimetro di Sicurezza Nazionale Cibernetica), which defines for the OESs (Operators of Essential Services) and DSPs (Digital Service Providers) the security measurements, incident notification procedures and cooperation policies with information security authorities. Recently (January 2023), the NIS directive has been updated better clarifying and strengthening aspects of cyber crisis management, harmonizing security requirements and reporting obligations, further improving collaboration and information sharing between member states, and, above all, increasing the areas included within the perimeter of national strategic interest.

Although the list of OESs and DSPs is not public, it is not difficult to infer that they are medium/large entities, with enterprise grade IT services. This document will adopt this general assumption and small business operators will not be considered. Due to the high rate of heterogeneity of their IT systems, large companies rely on SOC (Security Operation Center) monitoring system to correlate events generated in the infrastructure to detect anomalies and threats.

Industries standards, best practices and the regulatory framework will be analyzed in this work to provide the context where SOCs operate. Moreover, an overview of popular security architecture models, event correlation techniques and adversary analysis will be presented to better understand how SOCs work and which tools are commonly adopted to deal with the ever-evolving landscape of cyber threats. Furthermore, considering the growing adoption of cloud services, a market analysis will be provided focusing on the security features provided by major cloud providers along with an introduction of possible open-source alternatives.

The thesis addresses an in-depth examination of the sophisticated tools and techniques employed by modern SOCs to effectively identify, mitigate and respond to the ever-changing cyber threat landscape. This research is focused on SOCs capabilities that leverage advanced technologies, threat intelligence, machine learning and automation to strengthen their defenses. It will include an extensive analysis of threat detection and response solutions, starting with an evaluation of the underlying Security Investigation Languages

to ensure the detection of anomalies and threats, and it will continue by analyzing the automation and orchestration capabilities used to enhance the efficiency and flexibility of security operations.

The final outcome of this study will be a set of considerations and suggestions for security engineers and architects, providing support in decision making during the selection of tools and techniques to be adopted in a SOC. These guidelines will provide a proposal for a holistic approach to cybersecurity that will be based not only on the research activity of this thesis, but also on a personal experience in the field.

Acknowledgements

Si dice che praticare la gratitudine sia un modo per essere felici e mentre scrivo queste righe, mi rendo conto del forte senso di gratitudine che provo nei confronti di tutte le persone che hanno reso possibile questa esperienza. Ripercorrendo gli ultimi due anni mi rendo conto di essere stato fortunato e di aver vissuto un periodo intenso che ricorderò per sempre.

Tra tutti vorrei ringraziare in special modo:

i miei genitori, per il loro amore e per avermi donato la forza della determinazione Antonio, che mi ha accompagnato in questo percorso rendendolo più leggero e spensierato e Sara, che mi sopporta nella vita di tutti i giorni e mi aiuta ad esprimermi e a realizzarmi sempre

Contents

List of Tables	8
List of Figures	9
Acronyms	10
1 Introduction	27
1.1 Regulations	27
1.2 Security Architectures	28
1.2.1 Zero Trust Architecture	29
1.2.2 Cybersecurity Mesh Architecture	33
1.2.3 Tiering model	34
1.3 Security Operation Center	36
1.3.1 Security Operation Center History	37
1.3.2 Types of SOC	37
1.3.3 SOC Challenges	38
1.3.4 Security Incident Process	39
1.3.5 Cybersecurity Tools Classification	41
1.4 Threat Detection and Response	42
1.4.1 Playbook	43
1.4.2 Enrichment	44
1.4.3 Threat Intelligence	45
1.4.4 Behaviour analysis	46
1.4.5 Information Sharing	47
1.4.6 Orchestration	47
1.5 Adversary Analysis	48
1.5.1 Diamond Model	48
1.5.2 MITRE - ATT&CK framework	50
1.5.3 Pyramid of Pain	50
1.5.4 Cyber Kill Chain	51
1.5.5 Mitre ATT&CK VS Cyber Kill Chain	53
1.5.6 Malicious Actors and Malware	53
1.6 Defenses	54
1.6.1 Defender mindset	54
1.6.2 Mitre D3FEND	55

1.6.3	Mitre ATT&CK Flow Project	56
1.6.4	MITRE Engenuity ATT&CK Evaluation	58
1.6.5	Mitre - Sightings Ecosystem project	58
2	Market Analysis	59
2.1	Microsoft Azure	60
2.1.1	Operations	60
2.1.2	Applications	61
2.1.3	Storage	62
2.1.4	Encryption at rest	62
2.1.5	Networking	63
2.1.6	Compute	63
2.1.7	Identity	64
2.1.8	Other Tools	65
2.2	GCP - Google Cloud Platform	66
2.2.1	GCP Infrastructure Security	66
2.2.2	Computing Security	67
2.2.3	Network Security	68
2.2.4	Data Security	69
2.2.5	Secure Deployment	71
2.2.6	Logging and Detection	72
2.3	AWS - Amazon Web Services	74
2.3.1	Identity and Access Management	76
2.3.2	Detection & Response	77
2.3.3	Network and application protection	77
2.3.4	Data Protection	78
2.3.5	Compliance	78
2.4	Open-source	78
2.4.1	Basic Functionality	79
2.4.2	Advanced Functionality	79
2.4.3	Frameworks	80
2.4.4	Open Source Solutions	81
2.5	Cloud Service Provider comparison	81
3	Threat Detection and Response	83
3.1	Security Investigation Languages	83
3.1.1	Azure KQL	84
3.1.2	GCP YARA-L	85
3.1.3	AWS SQL	87
3.2	Event Correlation	89
3.2.1	Azure Sentinel & Defender for Cloud	89
3.2.2	GCP Chronicle & Security Command Center	91
3.2.3	AWS GuardDuty & Detective	94
3.3	Automatic Response	97
3.3.1	Sentinel - Automation rules & playbooks	97
3.3.2	Chronicle SOAR	102

3.3.3	Amazon EventBridge	103
3.4	Conclusion	103
4	Threat Hunting	105
4.1	Microsoft Sentinel	105
4.1.1	Impossible Travels	105
4.1.2	Threat Intelligence - Authentication	106
4.1.3	Threat Intelligence - File Access	107
4.1.4	Phishing Campaign	107
4.2	Microsoft Defender	107
4.2.1	Risky Users	108
4.2.2	Phishing Campaign	109
4.2.3	Advanced Investigations	109
5	Principles & Guidelines	113
5.1	Guidelines	114
5.1.1	Ecosystems	114
5.1.2	Telemetry	114
5.1.3	Automation	114
5.1.4	Security Pillars	115
5.1.5	Attack surface reduction	116
5.1.6	Continuous improvement	117
5.1.7	Multi-cloud Threat Detection and Response	117
5.1.8	Open-Source	118
6	Final Conclusions	119
6.1	Possible further studies	120
6.1.1	Migration tools - correlation rules	120
6.1.2	Test - Correlation rule	120
6.1.3	Procedure - Automatic Response	121
6.1.4	Opensource Private Cloud	121
A	Appendix	123
	Bibliography	127

List of Tables

1.1	ZTA Definitions	29
1.2	Cybersecurity Tools Classification	42
1.3	Example of correlations rules	44
2.1	Cloud Computing Market Share	60
2.2	Open-source Security Solutions	80
3.1	Security Investigation languages	84
3.2	Microsoft Sentinel Out of The Box Analytics Rules	90
3.3	Playbooks classes examples	99
A.1	Malicious Actors - Russian - state-sponsored	123
A.2	Malicious Actors - China - state-sponsored	124
A.3	Malicious Actors - North Korea - state-sponsored	124
A.4	Malicious Actors - Criminal organizations	125
A.5	Malicious Actors - Hacktivist groups	125
A.6	Most widespread malware	126

List of Figures

1.1	Security Architecture - ZTA logical components [121]	31
1.2	Security Architecture - Legacy Tier Model [83]	35
1.3	Security Architecture - Evolution of Tier Model [83]	36
1.4	Security Incident Process - Phases	40
1.5	MISP - Threat Sharing platform [115]	47
1.6	Adversaries Analysis Frameworks - Diamond Model [40]	49
1.7	Adversaries Analysis Frameworks - Pyramid of Pain [21]	51
1.8	Adversaries Analysis Frameworks - The Cyber Kill Chain [78]	52
1.9	Defenders think in lists. Attackers think in graphs	55
1.10	MITRE - D3fend Poster [92]	55
1.11	MITRE - Example of Digital Artifact Relationships [92]	56
1.12	MITRE - Example of Related Attack Techniques [92]	57
1.13	MITRE - ATT&CK Flow Builder Overview [95]	57
3.1	Microsoft - ASIM Architecture [89]	90
3.2	Microsoft Sentinel - Content Hub Solutions	91
3.3	Google Security Command Center - Landscape [57]	92
3.4	Amazon Detective - workflow [4]	96
3.5	Amazon Detective - flow [4]	96
3.6	Microsoft Sentinel - Incident investigation components	99
3.7	Microsoft Sentinel - Incidents page	100
3.8	Microsoft Defender for Cloud - Incident	101
3.9	Microsoft Sentinel - Query history	101
3.10	Microsoft Sentinel - Activity log	102
4.1	Microsoft Sentinel - KQL - Impossible Travel	105
4.2	Microsoft Sentinel - KQL - Threat Intelligence Authentication	106
4.3	Microsoft Sentinel - KQL - Threat Intelligence File Access	107
4.4	Microsoft Sentinel - KQL - Phishing Campaign	108
4.5	Microsoft Defender for Identity - Risky Users	108
4.6	Microsoft Defender 365 - Phishing Campaign	110
4.7	Microsoft Defender 365 - Phishing Actions	110
4.8	Microsoft Defender 365 - Advanced Investigations	111
4.9	Base64 Decode	111
5.1	ENISA - Top 15 Cyber Threats [36]	115
5.2	SASE - Secure Access Service Edge	116

Acronyms

ABI (Associazione Bancaria Italiana)

It is a voluntary non-profit organization that represents the interests of its member banks and financial intermediaries.

ACN (Agenzia per la Cibersicurezza Nazionale)

National cybersecurity authority for the protection of national interests in the field of cybersecurity. The Agency is responsible for safeguarding security, resilience in cyberspace and for preventing and mitigating the greatest number of cyber attacks and fostering the achievement of technological autonomy.

AD (Active Directory)

Directory service and identity management system developed by Microsoft. It is commonly used in Windows-based networks to manage and organize resources, such as computers, users and groups and to provide authentication and authorization for network access.

ADX (Azure Data eXplorer)

Fully managed data analytics service for real-time and time-series analysis on large volumes of data streams from business activities, human operations, applications, websites, Internet of Things (IoT) devices and other sources.

AntiBEC (Business Email Compromise)

Set of strategies, measures and technologies designed to protect organizations and their executives from CEO fraud or impersonation attacks.

DDOS (Distributed Denial of Service)

System which helps to prevent DDoS attacks, malicious attempts to overwhelm a target system with a flood of traffic, rendering it inaccessible to legitimate users. These attacks can disrupt online services, websites and networks, causing downtime, financial losses and damage to an organization's reputation.

Antiphishing

Measures and tools used to identify and combat phishing attacks. Phishing is a type of cyberattack in which malicious actors attempt to deceive individuals into revealing sensitive information, such as login credentials, financial data or personal information, by posing as trustworthy entities.

Antispam

Measures and tools designed to combat and mitigate unsolicited or unwanted email messages, commonly known as spam. Spam emails are often sent in bulk, typically for the purpose of advertising products or services, spreading malware or conducting phishing attacks.

API (Application Programming Interface)

Set of rules that allows two software programs to communicate with each other. It is a way for different applications to share data and functionality.

APT (Advanced Persistent Threat)

Sophisticated, sustained cyberattack in which an intruder establishes an undetected presence in a network in order to steal sensitive data over a prolonged period of time. APTs are typically carried out by state-sponsored actors or highly organized criminal groups.

ARM (Azure Resource Manager)

Provides a management layer that enables to create, update and delete resources in Azure account.

Artifact

Any tangible by-product of the software development process. Artifacts can be physical objects, such as printed documents or scripts or digital objects, such as source code, test cases and deployment scripts.

ASIM (Advanced Security Information Model)

Layer that is located between diverse security data sources and log analysis tools used to normalize security data from different sources into a common format, making it easier to analyze and query.

AWS (Amazon Web Service)

Suite of cloud computing services that runs on the same infrastructure that Amazon uses for its e-commerce website. AWS offers a broad set of global compute, storage, database, analytics, application and deployment services that help organizations move faster, lower IT costs and scale applications.

Asset Discovery

Software applications or solutions used to identify, map and catalog all devices, systems and assets within a network. These tools are essential for network and IT administrators to maintain visibility and control over their network infrastructure.

Azure

Cloud computing platform that runs on the same infrastructure that Microsoft uses for its end-user products, such as Windows and Office. Azure offers a broad set of global compute, data storage, data analytics and machine learning services that help organizations to build, deploy and scale their applications.

Backup

Process of creating and storing duplicate copies of data, files or information to protect against data loss, corruption or other forms of data damage.

Behaviour Analysis

Process of monitoring and assessing the behaviour of users, devices, applications and network traffic to detect unusual or potentially malicious activities.

BYOD (bring your own device)

Policy that allows employees to use their personal devices, such as laptops, smartphones and tablets, for work-related activities. This can include accessing email, connecting to the corporate network and using corporate apps and data.

Browser Security

Measures and best practices aimed at protecting web browsers and the users who interact with them from various security threats and vulnerabilities (e.g. crypto jacking or extension vetting).

CASB (Cloud Access Security Broker)

Security solution that sits between cloud users and cloud service providers to enforce security policies. CASBs can be used to control access to cloud resources, protect data in transit and at rest and detect and respond to threats.

CEF (Common Event Format)

Standardized format for logging security events. It was developed by a group of security vendors (Cisco, IBM, Juniper Networks e McAfee) to make it easier to collect and analyze logs from different sources. CEF is an open format and anyone can use it to generate or parse CEF logs.

CDM (Continuous Diagnostics and Mitigation)

Gathers information about the enterprise asset's current state and applies updates to configuration and software components.

CERT (Computer Emergency Response Team)

Group of IT security professionals who are responsible for providing information and technical assistance in the event of IT security incidents. CERTs may be public or private and may operate at national, regional or corporate level.

CI/CD (Continuous Integration/Continuous Development)

Set of practices that automates the software development and delivery process. CI/CD pipelines typically include the stages: Code commit, Build, Test, Deploy.

CIA (Confidentiality, Integrity or Authenticity)

These three core principles form the basis of information security and are essential for protecting sensitive data and ensuring the proper functioning of information systems.

CLI (Command Line Interface)

User interface that allows users to interact with a computer by typing commands.

CLOSINT (Closed Source Intelligence)

Collection and analysis of data gathered from closed sources to produce actionable intelligence. Closed sources can include anything from government intelligence reports to corporate databases.

CNAPP (Cloud Native Application Protection Platform)

Technology and strategy specifically designed to secure cloud-native applications. Cloud-native applications are applications that are built and deployed using cloud-native technologies and methodologies, often taking advantage of containers, microservices, serverless computing and dynamic orchestration platforms.

Conditional Access

Conditional access is a security feature that allows organizations to control who has access to what resources, based on a variety of factors, such as the user's location, device and time of day.

CSIRT (Computer Security Incident Response Team)

Team of IT security professionals that is responsible for handling IT security incidents. CSIRTs may be public or private and may operate at national, regional or corporate level.

CSMA (Cybersecurity Mesh Architecture)

Cybersecurity approach proposed by Gartner that advocates interoperability and coordination between individual security products, resulting in a more integrated security policy.

cSOC (cybersecurity SOC)

SOC focused only cybersecurity incidents.

CSPs (Cloud Service Providers)

Organizations or companies that offers cloud computing services and resources to individuals, businesses and other entities.

CSPM (Cloud Security Posture Management)

Tool that helps organizations assess and manage their security posture in the cloud. CSPM tools can be used to identify and remediate security risks in cloud environments, such as misconfigurations, vulnerabilities and compliance violations.

CVCN (Centro di Valutazione e Certificazione Nazionale)

Centre in charge of assessing the security of ICT goods, systems and services to be deployed in the context of the National Cybersecurity Perimeter.

CWPP (Cloud Workload Protection Platform)

Technology and strategy focused on securing workloads running in cloud environments. Cloud workloads refer to the individual units of applications, microservices or virtual machines that execute specific tasks within cloud infrastructure.

DAST (Dynamic Application Security Testing)

Security testing technique used to assess the security of web applications by actively examining the application in a running state. DAST tools interact with a live version of the application and test it for vulnerabilities and weaknesses.

Data Masking

Technique used to protect sensitive information by replacing, concealing or scrambling original data with fake or pseudonymous data while maintaining the data's format and structure.

DDL (Data Definition language)

Subset of SQL that is used to create, modify and delete database objects.

DLP (Data Loss Prevention)

Set of technologies and processes that help organizations to identify, classify and protect sensitive data.

DML (Data Model language)

Subset of SQL that is used to insert, update and delete data in database tables.

DMZ (Demilitarized Zone)

Physical or logical sub-network that contains and exposes an organization's external-facing services to an untrusted network such as the Internet.

DNS (Domain Name System) Security

Measures and protocols in place to protect the DNS infrastructure and DNS-related data from various threats, including DNS attacks, data exfiltration and unauthorized access.

DORA (Digital Operational Resilience Act)

European Union regulation that creates a binding, comprehensive information and communication technology (ICT) risk management framework for the EU financial sector.

DQL (Detective query Language)

SQL-like language that can be used to query data in Amazon Detective. Amazon Detective is a security investigation service that helps to investigate and respond to security incidents.

DSA (Digital Services Act)

Regulation adopted by the European Union in 2022 that sets out rules for online platforms and other digital service providers. The DSA aims to protect users from harmful content, promote competition and ensure that online platforms are accountable for their actions.

EBS (Elastic Block Store)

Block storage service that provides persistent storage for Amazon Elastic Compute Cloud (Amazon EC2) instances.

EC2 (Elastic Compute Cloud)

Re-sizable compute capacity in the cloud. It is designed to make it easy for users to launch and manage virtual servers, known as instances.

EDR (End Point Detection and Response)

Security solution that collects and analyzes data from endpoints, such as laptops, desktops and mobile devices, to detect and respond to threats.

EKS (Elastic Kubernetes Services)

Managed Kubernetes service that makes it easy to deploy, manage and scale Kubernetes applications in the AWS cloud and on-premises data centers.

Email Sandbox

Security mechanism and technology used to analyze and execute potentially malicious or suspicious email attachments and links in a safe, isolated environment.

ENISA (European Network and Information Security Agency)

European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe.

EOS (End Of Support)

Point in time at which a software vendor or hardware manufacturer ceases to provide support for a product or service.

EPP (End Point Protection)

Security solution that protects endpoints, such as laptops, desktops and mobile devices, from malware and other threats.

External Attack Surface

The total of all internet-facing assets and systems that can be exploited by attackers. It includes websites, web applications, cloud services, and any other assets that are accessible to the public internet.

FaaS (Function As A Service)

Cloud computing model in which developers can build and deploy applications without having to manage the underlying infrastructure. FaaS providers manage the infrastructure allowing to be focus on code developing.

FIDO (Fast Identity Online)

Open authentication standard that aims to replace passwords with a more secure and user-friendly authentication method. FIDO is based on public key cryptography, which is the same technology that is used to secure HTTPS connections.

Fluentd

Open-source, unified logging platform for collecting, processing and outputting logs. It is a popular tool for collecting logs from a variety of sources, such as applications, servers and network devices. Fluentd can be used to collect logs in a variety of formats, such as JSON, XML and plain text. It can also be used to filter, transform and enrich logs before they are output.

GCP (Google Cloud Platform)

Suite of cloud computing services that runs on the same infrastructure that Google uses for its end-user products, such as Google Search and YouTube. GCP offers a broad set of global compute, data storage, data analytics and machine learning services that help organizations to build, deploy and scale their applications.

GDPR (General Data Protection Regulatory)

European Union regulation governing the processing of personal data and privacy. It came into force on 25 May 2018 and applies to all entities that process personal data of natural persons in the European Union, regardless of where they are located.

GKE (Google Kubernetes Engine)

Managed, production-ready environment for deploying containerized applications. It provides a complete Kubernetes service, including load balancing, auto-scaling and monitoring. GKE is built on Google's infrastructure, so customers can be confident that their applications are running on a reliable and scalable platform.

GPO (Group Policy Objects)

Feature in Microsoft Windows operating systems that allows network administrators to implement specific configurations, security policies and settings for users and computers within an Active Directory domain.

GQL (GuardDuty Query Language)

SQL-like language that can be used to query GuardDuty findings. GuardDuty is a threat detection service that uses machine learning to identify security threats in AWS account.

HSM (Hardware Security Module)

Physical computing device that safeguards and manages secrets (most importantly digital keys), performs encryption and decryption functions for digital signatures, strong authentication and other cryptographic functions.

HUMINT (Human Intelligence)

Collection and analysis of information gathered from human sources to produce actionable intelligence. HUMINT is one of the four main intelligence disciplines, along with signals intelligence (SIGINT), imagery intelligence (IMINT) and measurement and signature intelligence (MASINT).

Hyperscaler

Cloud computing provider that operates a massive, global network of data centers and offers a wide range of computing, storage, and networking services. Hyperscalers are typically characterized by their ability to scale their infrastructure to meet the demands of large enterprises and organizations.

IaaS (Infrastructure As A Service)

Cloud computing service that provides virtualized computing resources, such as compute, storage and networking, on demand.

IaC (Infrastructure As Code)

Software development methodology that treats infrastructure as software. It uses machine-readable definition files to provision and manage infrastructure. This can include servers, networks, storage and other resources.

IANA (Internet Assigned Numbers Authority)

Key organization responsible for the management and allocation of various Internet resources, including domain names, IP addresses and protocol parameters.

IAST (Interactive Application Security Testing)

Dynamic application security testing (DAST) technique that combines dynamic analysis with real-time monitoring of an application's runtime behaviour. IAST tools are designed to identify and report security vulnerabilities and weaknesses in real time during an application's execution.

IBN (Intent Based Network)

Network architecture that automates the provisioning, configuration and management of networks based on the business intent of the network.

ICS (Industrial Control Systems)

Computer systems used to control and automate industrial processes, such as power generation, gas and water distribution or critical infrastructure management.

IDO (Indicators of Detection)

Information that indicates the presence of malware or other malicious code.

IDS (Intrusion Detection System)

Component of cybersecurity that monitors an organization's network or systems for signs of malicious activities or security incidents. IDS is designed to identify and alert administrators to potential threats, anomalies or unauthorized activities within the network.

IMINT (Imagery Intelligence)

Collection and analysis of imagery to produce actionable intelligence. Imagery can be collected from a variety of platforms, including satellites, aircraft and drones.

IOB (Index of Behaviour)

Information that indicates anomalous or suspicious behaviour.

IOC (Index Of Compromise)

Information or a detectable pattern in data that suggests an unauthorized or malicious activity has occurred within a computer system or network.

IPS (Intrusion Prevention Systems)

Network security device that monitors network traffic for malicious activity and takes action to block it. IPSs are similar to intrusion detection systems (IDSs), but they take a more proactive approach by blocking malicious traffic instead of just detecting it.

IPSEC (Internet Protocol Security)

Suite of protocols that helps ensure secure communication over an untrusted network, like the internet.

IVASS (Istituto di Vigilanza delle Assicurazioni)

Italian insurance supervisory authority. It is an independent authority responsible for supervising and regulating all insurance business in Italy.

JSON (JavaScript Object Notation)

Lightweight and text-based data format used to represent structured data in a format that is both human-readable and machine-readable expressing attributes in the key-value format.

KQL (Kusto Query Language)

Powerful query language for exploring data and discovering patterns, identifying anomalies and outliers, creating statistical modeling and more.

kubernetes

Open-source system for automating deployment, scaling and management of containerized applications. It is a portable, extensible and scalable platform that can be used to deploy applications on a variety of infrastructure, including bare metal, virtual machines and the cloud.

Log Management

Practice of collecting, storing, analyzing and managing log data generated by various devices, systems and applications within an organization's IT infrastructure.

M2M (Machine to Machine) Authentication

Process of authenticating and authorizing interactions between two or more machines or devices within a network or system.

MASINT (Measurement and Signature Intelligence)

Collection and analysis of data from unique physical characteristics or distinctive patterns of behaviour to produce actionable intelligence.

MDM (Mobile Device Management)

Software solution that helps organizations to manage and secure mobile devices, such as smartphones and tablets.

MFA (Multi Factor Authentication)

Security process in which users are granted access to a system or application only after successfully presenting two or more pieces of evidence to an authentication mechanism: “something they know“, “something they have“ or “something they are“.

MISP (Malware Information Sharing Platform& Threat Sharing)

Open-source threat intelligence platform and cybersecurity tool designed to facilitate the sharing of structured threat information among organizations and cybersecurity communities. It is specifically geared toward improving the detection and mitigation of cybersecurity threats, including malware, vulnerabilities and indicators of compromise (IoCs).

MSSP (Managed Security Service Provider)

Company that provides outsourced security monitoring and management services to businesses.

NAC (Network Access Control)

Security solution that controls who can access a network and what devices can be used on the network.

NDR (Network Detection and Response)

Cybersecurity solution that uses non-signature-based methods to detect and respond to threats on a network. NDR solutions collect and analyze network traffic data to identify suspicious activity, such as unauthorized access to sensitive data, malware infections and denial-of-service attacks.

Network Visibility

Set of technologies and practices designed to provide organizations with comprehensive insights into their network traffic, infrastructure, connected devices and performance.

NGFW (Next Generation Firewall)

Advanced type of network security solution designed to provide enhanced capabilities beyond traditional firewalls. NGFWs combine the functions of traditional firewalls with additional features like intrusion prevention, application awareness and control, deep packet inspection, identity awareness and more.

NIS (Network and Information Security)

On 16 January 2023, the Directive (EU) 2022/2555 (known as NIS2) entered into force replacing Directive (EU) 2016/1148. ENISA considers that NIS2 improves the existing cybersecurity status across EU.

NSG (Network Security Group)

Software-defined security group that acts as a basic firewall for controlling inbound and outbound network traffic to and from Azure resources, such as virtual machines, subnets or network interfaces.

OCSF (Open Cyber-Security Framework)

Open-source project led by AWS and leading partners in the cybersecurity industry to develop and promote a common vendor-agnostic schema for cybersecurity data.

OIDC (OpenID Connect)

Open-standard protocol that enables third-party applications to verify the identity of a user without having to store the user's password. OIDC is based on the OAuth 2.0 protocol, but it adds additional features, such as user profile information and single sign-on (SSO).

OPA (Open Policy Agent)

Cloud-native, open-source policy engine that helps organizations to automate decision-making and enforce policies across their infrastructure. OPA can be used to enforce policies for a variety of purposes.

OpenC2 (Open Command and Control)

Standardized language for the command and control of technologies that provide or support cyber defenses.

ORC (Optimized Row Columnar)

Columnar storage format, where data is stored in columns rather than in rows. This allows ORC to compress data more effectively and to access data more efficiently.

OSE (Operatore di Servizi Essenziali)

Organization that provides services that are essential to the maintenance of critical societal and/or economic activities.

OSINT (Open Source Intelligence)

Practice of collecting and analyzing information from publicly available sources to gather insights, intelligence or data about various subjects, such as individuals, organizations, companies or events.

OSSEM (Open Source Security Events Metadata)

Community-led project that focuses primarily on the documentation and standardization of security event logs from diverse data sources and operating systems.

OTP (One Time Passowrd)

Password that is valid for only one login session or transaction. OTPs are typically generated using a cryptographic algorithm and are sent to the user via SMS, email or a mobile app.

PA (Policy Administrator)

Component responsible for establishing and/or shutting down the communication path between a subject and a resource[121].

PaaS (Platform As A Service)

Cloud computing service that provides a platform for developing, deploying and managing applications.

PAW (Privileged Access Workstation)

Security concept and practice used in organizations to enhance security by isolating and restricting access to highly sensitive systems and data to dedicated workstations.

PE (Policy Engine)

Component is responsible for the ultimate decision to grant access to a resource for a given subject.[121].

PDP (Policy Decision Point)

System entity that evaluates applicable policy and renders an authorization decision.

Pen Test (Penetration Test)

Security assessment or testing method that involves simulating cyberattacks on a computer system, network, application or other IT infrastructure to identify vulnerabilities and weaknesses that could be exploited by malicious hackers.

PEP (Policy Enforcement Point)

System entity that performs access control, by making decision requests and enforcing authorization decisions.[129].

PIM (PIM (Privileged Identity Management))

Set of practices, technologies and policies that organizations use to manage, monitor and secure privileged accounts and identities within their IT infrastructure.

PKI (Public Key Infrastructure)

System responsible for generating and logging certificates issued by the enterprise to resources, subjects, services and applications.

PNSC (Perimetro di Sicurezza Nazionale Cibernetica)

Set of public and private Italian entities required to ensure a high level of security of the networks, information systems and IT services, because they exercise essential function or provide essential service to the state that in the case of a failure, interruption, even partial or improper use, national security may be affected.

POP (Point Of Presence)

Physical location where two or more networks or communication devices share a connection.

PSD (Fornitore di servizi digitali)

Service provider that provides one or more digital service relevant for national security (eg. cloud provider, search engine, backbone network infrastructure).

Public Cloud

Computing model where resources and services are offered to the public over the internet. This means that anyone can sign up for and use public cloud services, without having to invest in and maintain their own infrastructure.

RaaS (Ransomware As A Service)

Business model in which ransomware developers sell their malware and support services to other criminals. This allows criminals with limited technical expertise to launch ransomware attacks.

RAT (Remote Access Trojan)

Type of malware that gives an attacker complete control over a victim's computer or other device. RATs can be used to steal data, install other malware, launch attacks against other systems and even spy on victims.

RBAC (Role Base Access Control)

System that allows to control who has access to resources and what they can do with them. RBAC is a powerful tool that can help to improve the security of the environment and ensure that users only have access to the resources they need to do their jobs.

RTS (Regulatory Technical Standards)

Set of technical standards that are being developed by the European Supervisory Authorities (ESAs) to provide more detailed guidance on how to comply with the requirements of the Digital Operational Resilience Act (DORA).

SaaS (Software As A Service)

Cloud computing service model where software is delivered to users over the internet. SaaS applications are typically hosted by a third-party vendor and accessed by users through a web browser.

SASE (Secure Access Service Edge)

Cloud-based security architecture that combines network and security capabilities into a single service. SASE is designed to provide secure access to applications and data for users and devices, regardless of their location.

SAST (Static Application Security Testing)

Set of techniques and tools used to analyze the source code, binary code or byte-code of an application to identify and remediate security vulnerabilities and weaknesses.

Security in depth

Principle is a security strategy that relies on multiple layers of security controls to protect an organization's assets. The goal of this principle is to make it more difficult for attackers to penetrate an organization's defenses by requiring them to bypass multiple security controls.

SCA (Software Composition Analysis)

Security practice that involves the identification and management of third-party or open-source software components and libraries used in a software application. SCA aims to assess and mitigate security risks associated with these dependencies.

SCC (Security Command Center)

Unified security platform that helps organizations protect their Google Cloud environments.

SCCQL (Security Command Center Query Language)

SQL-like language that can be used to query security findings in Google Cloud Security Command Center (SCC). SCCQL supports a variety of functions and operators for data manipulation, including aggregations, filters and joins. This allows to perform complex queries on the security findings to find the information needed.

SIGINT (Signal Intelligence)

Collection and analysis of signals to produce actionable intelligence. Signals can include anything from radio communications to electronic emissions from weapons systems.

Software Development Kit

Set of tools and libraries that helps developers to create applications for a specific platform.

SDN (Software Defined Network)

Software-defined networking (SDN) is a network architecture that decouples the control plane from the data plane. This means that the control plane, which is responsible for making decisions about how traffic flows through the network, is separated from the data plane, which is responsible for actually forwarding traffic.

SIEM (Security information and event management)

Software solution that collects, aggregates and analyzes security data from a variety of sources, such as network devices, servers and applications. This data can be used to detect security threats, investigate incidents and improve overall security posture.

SOAR (Security Orchestration Automation and Response)

Security framework that automates and orchestrates security incident response. SOAR solutions typically integrate with a variety of security tools, such as firewalls, intrusion detection systems and security information and event management (SIEM) systems, to automate tasks.

SOC (Security Operation Center)

Team of IT security professionals constantly monitor and analyze network and security activities to detect, investigate and respond to security incidents. SOCs use a variety of technologies and techniques to collect, analyze and report security data.

SSDLC (Secure software development life-cycle)

Set of processes and activities that organizations follow to ensure that their software is developed with security.

STIX (Structured Threat Information Expression)

Language and serialization format used to exchange cyber-threat intelligence (CTI). STIX is open source and free, allowing those interested to contribute and ask questions freely.

SWG (Secure Web Gateway)

Security solution that protects users from web-based threats and enforces corporate acceptable use policies. SWGs are typically deployed between the corporate network and the internet and inspect all web traffic.

S3 (Simple Storage Service)

Object storage service that offers industry-leading scalability, data availability, security and performance.

TDE (Transparent Data Encryption)

Feature of database systems that encrypts data at rest. This means that data is encrypted when it is stored on disk and decrypted when it is accessed by applications.

TEE (Trusted Execution Environment)

Secure environment that protects applications and data from unauthorized access and modification. TEEs are typically implemented in hardware, such as a CPU or security chip and they provide a high level of isolation for applications and data.

Threat Intelligence

Crucial aspect of cybersecurity that involves gathering, analyzing, and sharing information about cyber threats. This information helps organizations understand the evolving threat landscape, identify potential attack vectors, and proactively protect their systems and data.

TI (Traces or Information)

Traces or information that can be used to detect, identify and respond to security threats.

Tiber-EU (Threat Intelligence-Based Ethical Red-Teaming)

European framework for testing and improving the cyber resilience of critical entities. The framework is developed by the European Central Bank (ECB) and is voluntary for adoption by authorities and jurisdictions.

TLS tunnels

Network connection that uses the Transport Layer Security (TLS) protocol to encrypt all data that passes through it. TLS is a cryptographic protocol that is used to secure communications over the Internet. It is used to protect data from being intercepted and read by unauthorized third parties.

Tokenization

Technique that involves replacing sensitive information with a unique identifier or token. This process is typically irreversible, meaning that it is computationally infeasible to reverse the token and obtain the original sensitive data.

TPM (Trusted Platform Module)

Hardware chip that can be used to improve the security of a computer system. TPMs can be used to generate and store cryptographic keys, perform secure boot and attest to the integrity of a system.

TTPs (Tactics, Techniques and Procedures)

Description of the behaviours, processes, actions and strategies used by a threat actor to develop threats and engage in cyberattacks.

UDM (Unified Data Model)

Combination of data from multiple sources into a single, unified view. This can be done by using a common data schema or by using a data federation layer to translate between different data schemas.

UEBA (User and Entity Behaviour Analytics)

Cybersecurity solution that uses machine learning and behavioural analytics to identify abnormal or potentially malicious user and device behaviour. UEBA can be used to detect a wide range of threats, including insider threats, data breaches and malware infections.

Users Directory Services

Database or repository that stores and manages information about users, such as their identities, authentication credentials, access permissions and other attributes.

VAPT (Vulnerability Assessment and Penetration Testing)

Comprehensive approach to security testing that combines two complementary disciplines: vulnerability assessment and penetration testing. Vulnerability assessment is the process of identifying and evaluating security vulnerabilities in a system. Penetration testing is the process of exploiting those vulnerabilities to assess the security posture of a system.

VPCs (Virtual Private Cloud)

Service that lets create a logically isolated section of the resources in a virtual network.

VPN (Virtual Private Network)

Technology that enables secure and encrypted communication over a public network, typically the internet. VPNs create a secure and private connection between the user's device and a remote server or network.

YAML (YAML Ain't Markup Language)

Human-readable data serialization language. It is often used for configuration files, but its object serialization abilities make it a viable replacement for languages like JSON.

YARA-L (Yet Another Recursive Acronym)

Language used to write rules used to detect a wide range of malware and other malicious activity in logs collected by Google Chronicle, based on YARA a rule language invented by Virus Total to detect malware into files.

WAAP (Web Application and API Protection)

Security solution that protects web applications and APIs from a variety of threats.

WAF (Web Application Firewall)

Security appliance that protects web applications from a variety of attacks, such as cross-site scripting (XSS), SQL injection and denial-of-service (DoS) attacks.

xDR (eXtended Detection and Response)

Cybersecurity framework of security solutions that combines the capabilities of endpoint detection and response (EDR), network detection and response (NDR) and other security tools to provide a more comprehensive view of threats and improve the ability to detect and respond to them.

ZTA (Zero Trust Architecture)

Security framework that assumes that no user or device is inherently trusted, even if they are inside the network perimeter. ZTA requires all users and devices to be authenticated and authorized before they are granted access to resources.

Chapter 1

Introduction

Before going deeper in the analysis of SOC monitoring systems, it could be useful to define what is a “security event” and what is a “security incident”. A security event indicates a happening that signals a potential threat to a device, data or identity. A security event is not always a symptom of a security incident, in fact for example a security event such as a failed authentication attempt might simply indicate human error and not an attempt to breach a system. On the other hand, a security incident indicates an event that has a negative impact in terms of CIA (Confidentiality, Integrity or Authenticity) with regard to a certain piece of information system.

SOC monitoring systems collect events generated by IT Security Systems. The selection of events to be sent to the event correlation systems is relevant to ensure to be able to identify and contain threats and adversaries. Although security events can be generated by any information system, the most useful for identifying an attacker are often those generated by security systems (i.e. those particular systems responsible for enforcing security policies). The selection of security measurements normally takes place after the IT-risk-assessment and in accordance with the reference security architecture and applicable regulations.

1.1 Regulations

Modern Cybersecurity Regulations are not prescriptive about what the entities target of the regulatory must do to be compliant. Instead, regulations define as a requirement the need to perform a self-risk-assessment. Legislators decided to adopt this approach because frequently there are no one-size-fits-all solutions and threats and technological solutions are constantly and rapidly evolving.

For this reason, rather than referring to the needs of a SOC, there is often a reference to the necessity of adopting organizational approaches to ensure proper management of security incidents. A non-exhaustive list of regulations that refer directly and indirectly to the need of a SOC are:

- GDPR (General Data Protection Regulatory): This regulation includes as a requirement the notification at the data subject and authority in case of Data Breach, so

implicitly it requires a continuous surveillance of the security events.

- NIS (Network and Information Security): This Directive sets as a requirement the notification to the authorities in case of security incidents that affect essential services.
- DORA (Digital Operational Resilience Act): Within other requirements, this directive sets also the necessity to be able to identify and response to security incidents.
- Tiber-EU (Threat Intelligence-Based Ethical Red-Teaming): This setting defines a framework for performing advanced security tests by contrasting red team (attackers) to blue team (defenders)
- IVASS (Istituto di Vigilanza delle Assicurazioni) Regolamentoo 38: This regulation involves the Italian insurance sector and precedes the introduction of DORA regulations, along with other requirements. It emphasizes the importance of security testing and implicitly expects the presence of a SOC.
- ABI (Associazione Bancaria Italiana) Circolare 285: Banking sector regulation, which requires the adoption of a security incident handling process.

Although there is no unambiguous and detailed definition of what a SOC is, there is a large consensus about the fact that is a team of IT security professionals whose objective is protecting an organization from cyber attacks: they achieve this goal by using specific tools to monitor abnormal activities and by intervening in case of an attack to mitigate and restore services if necessary.

The tools used by SOC's depend mainly on the security architecture adopted by the organization. Analyzing possible security architectures in detail is beyond the scope of this thesis, however, with the aim of defining a classification of the most useful and common security measures for a SOC, a quick overview of the emerging security architecture is provided.

1.2 Security Architectures

Early security architectures were focused on protecting external perimeters, because the usage of personal devices for business activities and cloud services were not so common. Before the advent of the internet, computer systems were primarily accessible only inside the company. Before the diffusion became widespread, interactions with the world outside were very limited: for this reason the main focus of security architecture was to protect corporate assets from external threats, while everything inside was trusted.

The level of confidence therefore varied according to the proximity to the outer perimeter. DMZ (Demilitarized Zone) networks served as a buffer between the internal systems on which corporate data resided and the world outside. The breach of a system in this network did not automatically result in the compromise of the system or company data. For decades, the use of a network firewall and anti-malware was considered more than enough to respond to most of the information threats. With the advent of the internet, the increasing usage of personal devices like computers, laptops, smartphones and tablets

and the progressive spread of remote working mode, the corporate perimeter has become less and less defined and has imposed a paradigm shift that has led to the definition of new security architectures able to face new cyber threats more effectively.

In the recent past the Zero Trust approach to security architectures has been posing as an improvement on classical approaches, while nowadays Cybersecurity Mesh Architecture is emerging as an improvement on the Zero Trust approach itself.

1.2.1 Zero Trust Architecture

ZTA (Zero Trust Architecture) [121] is a security paradigm that shifts the focus of defences from protecting the perimeter of the information system to protecting users, assets and resources.

This new approach was born in response to trends that have affected and transformed corporate networks including remote users, BYOD (bring your own device) and cloud-based services that are no longer located within the corporate perimeter. Unlike the traditional approach, there are no areas of the network that are considered secure, so systems always require the authentication and take in account the values of other signals in order to calculate the risk of granting or not the access to a resource or before executing any transaction. The key principles of Zero Trust are:

- **No implicit trust:** No grants are given to assets and user accounts based on their location. Users must only be authorized to access the resources they need.
- **Micro-segmentation:** Focuses on protection resources (data, services, applications, assets, workflows, network accounts, devices, etc.). Network locations are no longer considered as a separate entity to protect; instead, the focus is to protect the resources.
- **Continuous evaluation:** The model assumes that an attacker is present in the environment. Enterprise-owned environments are no more trustworthy than any non-enterprise-owned environments. Organizations must have visibility into user activities and data, in order to continuously evaluate the risk and act to minimize it.
- **End-to-end approach:** Enterprise resources and data protection must be designed considering: identity (person and non-person), credentials, access management, operations, endpoints, hosting environments and interconnecting infrastructure.

The zero-trust paradigm is based on the following definitions:

Name	Description
Subject	Entity - human or not (e.g., a service) - that needs to access to a resource
Resource	Data, devices, services, printers, computers, IoT systems to which the subject wants to have access
Access	Can take place with different levels (e.g. read, write, delete, update, etc)

Table 1.1. ZTA Definitions

Summarizing, the focus of ZTA is on authentication and authorization, minimizing areas of implicit trust through granular authorization rules. The access of a subject to an enterprise resource is granted by a PDP (Policy Decision Point) [129] and corresponding PEP (Policy Enforcement Point) [129] that ensures the subject is authentic and the request is valid, by evaluating the level of confidence about the subject identity and other security parameters like: device security posture, time and location. The parameters can be used by systems to implement dynamic risk-based access policies, which will be enforced for each resource access request. In order to reduce the implicit trust zone PDP/PEP have to be as closer as possible to the resource to be protected.

ZTA Logical Components

ZTA is described as a set of logical components that operate together in order to enforce dynamic policies based on signals produced by some of these components. In the diagram in Fig. 1.1, the control plane is in charge of making decisions based on the policies to be implemented by the data plane, transferring or giving access to data.

- **PE (Policy Engine):** Thanks to policies and external sources information, this component takes the final decision (and logs it) if the access to a resource is granted or not.
- **PA (Policy Administrator):** It generates session token to allow or shutdown communication between sources and resources thanks to the interaction with PEP (Policy Enforcement Point). Both, PE (Policy Engine) and PA (Policy Administrator) compose the PDP (Policy Decision Point).
- **PEP (Policy Enforcement Point):** It is the component where the policies are transformed in actions, allowing or blocking a specific action performed by a subject to resource. This logical component is spread in all the systems where policies enforcement is required.
- **CDM (Continuous Diagnostics and Mitigation) system:** Collects information about the state of enterprise resources, like software and configuration of a device. It can also act to update configuration and software components.
- **Industry compliance system:** This component is useful to ensure the compliance with a specific regulation, continuously checking the policy rule defined to check the compliance.
- **Threat intelligence feeds:** It provides to the PE (Policy Engine) internal and external information such as new vulnerabilities or a list of IOC (Index Of Compromise) that can impact the policy engine determining whether to allow or deny a specific action.
- **Network and system activity logs:** It aggregates asset logs, network traffic, resource access actions and other events to provide near-real-time feedback about security posture of enterprise information systems.

- **Data access policies:** Attributes, rules and policies about the access to enterprise resources. It can be statically defined by the administrator or it can be dynamically generated by a policy engine, often a mixture of both.
- **Enterprise PKI (Public Key Infrastructure):** Infrastructure responsible to handle the x.509 certificates delivered to enterprise resources, subjects and services or applications.
- **ID management system:** Infrastructure that handles user accounts and identity records. It can be integrated with PKI to ensure stronger authentication mechanisms and/or can be federated with others identity management systems.
- **SIEM (Security information and event management) system:** It collects security related information (not only logs entry) to allow future analysis and automatically generates alert in case of suspicious events.

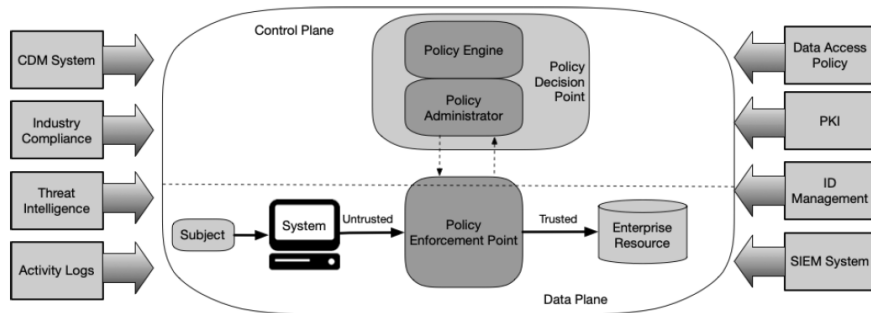


Figure 1.1. Security Architecture - ZTA logical components [121]

ZTA approaches

In the following paragraphs are presented brief descriptions of three possible ZTA approaches: *Enhanced Identity Governance*, *Micro-segmentation* and *Network Infrastructure and Software Defined*. All of them can be adopted independently or can be used together to achieve an advanced level of Zero Trust Architecture.

Enhanced Identity Governance: The Enhanced Identity Governance relies on actors identity to define and enforce the security policies. Identity and Attributes help determine whether an actor has the right or not to access a given resource. The device used, the state of the resource and environmental factors may contribute to the final calculation of the confidence level in granting or not the access to the resource. The PEP may also grant partial access or require a different level of authentication if the confidence level is not sufficient.

Micro-segmentation: With this approach, the organization aims to manage access to corporate resources through next-generation gateways and/or firewalls installed on endpoints

capable of managing configuration dynamically according to changing threats. Often the firewalls acting as PEP are managed centrally and receive a feed about network threats and user identities.

Network Infrastructure and Software Defined: This approach exploits the SDN (Software Defined Network) and IBN (Intent Based Network) concept to reconfigure the environment according with the decision of the PE. In this case the approach operates more at application level rather than at network level. For instance a resource gateway (operating as PEP) setups a secure channel for communication between client and resource only if the PE approves the request.

ZTA Limitations

There is no security architecture or solution that can completely avoid risks. Although the ZTA is associated with high security standards and is considered effective in minimizing risks, some threats must be considered. The cybersecurity industry has developed specific responses for each threat and these will be briefly described below.

Denial-of-Service or Network Disruption: ZTA does not provide any protection about Denial of Service attack. To minimize this kind of risk, organizations adopt specific Anti-DDOS solutions based on network and application traffic analysis and IP reputation in order to filter the traffic destined to a specific service by the non legitimate traffic.

Stolen Credentials/Insider Threat: Zero Trust Architecture relies on the correct identification of the subject to ensure protection to corporate assets. In case of not identified stolen credential or if the attack comes from an insider, ZTA should not be able to ensure an adequate protection. Strong Authentication is the main solution adopted to reduce the risk of stolen credential, on the other hand, Data Classification associated with data loss prevention and behaviour analysis and threat intelligence can be used to identify insiders.

Phishing & Social Engineering: ZTA does not provide any protection by social engineering attack or other kind of attacks to obtain users' credentials fraudulently. Strong Authentication, Antiphishing, Email Anti-malware, sandbox and other email protection solutions can be used to counteract phishing and social engineering.

Usage of Personal Data Storage or Devices: Data stored on cloud personal data storage services or personal devices cannot be protected by ZTA. Usage of data loss prevention tools and file encryption allows to better protect the information also outside the boundaries of the enterprise.

ZTA Complexity: ZTA security policies can be dynamically configured considering several context parameters. These parameters require a set of configurations and feeds to be delivered to the PEP. Due to the high level of complexity, it is possible to fall into miss-configuration or unwanted behaviour that are almost impossible to be verified in advance. ZTA adopts a baseline of statically defined policies to guarantee a minimum level of security even in case contextual component fails.

In addition to the classes of threats described above, it is necessary to consider that most companies adopt a hybrid-ZTA approach, i.e. an approach that mixes the principles of zero-trust architecture with those of traditional security architectures that are more focused on perimeter protection, which makes the effectiveness of the zero-trust approach inherently sub-optimal. Another major limitation of the ZTA model lies in the fact that the actual components of an IT system are rarely made by the same vendor and can rarely integrate effectively with each other. The use of standard protocols to make third-party products inter-operable is often contrasted by the vendors or allowed with limitations.

In this heterogeneous scenario, the monitoring systems of a SOC have, as their primary tasks, to collect events generated by security systems that are unable to cooperate during authentication/authorization for various reasons, but whose logs can provide important information about the security events that are occurring on the company's assets: by correlating them with each other, it is possible to identify malicious activities.

1.2.2 Cybersecurity Mesh Architecture

Another emerging cybersecurity architecture is the CSMA (Cybersecurity Mesh Architecture) proposed by Gartner [41]. This architectural approach is designed to be decentralized and distributed. It can be viewed as an extension of ZTA, because it considers user identity and context each time is required to grant access to an enterprise resource. Each enterprise resource is surrounded by a set of security features provided for the specific component (e.g., EDR (End Point Detection and Response), network firewall, IPS (Intrusion Prevention Systems), WAAP (Web Application and API Protection), TLS tunnels, and so on).

The main characteristics are:

- **Standardized interaction between tools:** CSMA provides features to make easier the interaction between different tools.
- **Reduced Vendors Footprint:** The number of cybersecurity tools adopted by the enterprise is large and rises up year by year, as many survey result reports [12]. CSMA aims to reduce the number of tools making them smaller and directly related with the resources to be protected.
- **Flexibility:** The meshed architecture allows to grow up security features according to the work load. Other types of architecture require to oversize the security features in order to be able to bear the maximum expected traffic.
- **Automation:** To allow flexibility, automation is necessary. The orchestrator takes care of deploying PODs and related security measures automatically in accordance with the desired state defined by the administrator and by using auto-scaling principles according to the workload.
- **Security in depth:** Thanks to decentralization, attackers find stronger resistance when trying to violate the organization, because they have to overcome different levels of controls.

- **AI:** CSMA takes advantage of Artificial Intelligence and Machine Learning to identify and respond to threats more quickly and reliably.
- **Centralized Management Dashboard:** All security tools, as part of a security ecosystem, can easily share information and allow cybersecurity teams to respond faster. Moreover, through the same dashboard, policies can be defined and distributed centrally.

CSMA is still in a developing phase and it is strictly related to cloud native application deployment (e.g., containerization). There is not a standard for the CSMA yet, the approach of creating an ecosystem with high interoperability from different solutions should promote the use of opensource solutions like: OPA (Open Policy Agent), OIDC (OpenID Connect), Fluentd that can work together to setup a CSMA in a kubernetes environment. However, the lack of investments in opensource solutions, can bring to success solutions proposed by leading cloud vendors that are going to create a "de facto standard" due to the strength of their customer base.

In conclusion, the CSMA was born in response to the challenge of running effectively an increasing number of stand-alone solutions.

1.2.3 Tiering model

Many companies use a centralized directory to manage the identities of their employees and collaborators. As we will see in Section 1.5 breaching the centralized directory is a common step in many attack 'paths', because it allows Attackers to impersonate any user and thus have access to any resources.

In response to this threat, the Tiering Model was proposed by Microsoft [83] this model logically separates active directory components into different tiers, with security boundaries between them, in order to reduce the risk of unauthorized changes to Active Directory objects. The split may change according to the technological and organizational context of the single organization, but it is typically done as follows:

- **Tier 0:** It contains the most critical components such as Domain Controllers and other servers that require privileged access to AD (Active Directory) (e.g. exchange, DNS, PKI). This level can only be administered through specific accounts and dedicated workstations called PAW (Privileged Access Workstation). The compromise of a Tier Zero system potentially leads to the compromise of the entire directory. To deal with the temporary unavailability of PAW and/or Tier Zero accounts, break glass accounts are often defined: these are accounts that do not require PAW to access Tier 0, but they are only to be used in an emergency and their use should be subject to the automatic generation of an alert.
- **Tier 1:** This level contains those AD objects that are critical to the organisation's activities, such as user accounts, groups and computer accounts through which business applications/services are delivered. Access to these systems is given by dedicated accounts, different from those used for normal user activities (e.g., e-mail access, network disks, and so on). The compromise of a Tier 1 system implies the potential

compromise of all systems that are part of that application/service and of all clients and users that access to the application/service.

- **Tier 2:** This tier includes objects that are less critical to the organisation’s overall security, such as end-user workstations and their accounts. Compromising this tier means compromising the individual workstation, however this is typically the first step of many attacks, this is the reason why it is crucial having a strict attention on what happens on workstations and user accounts. Administrators have to use JIT (Just-in-time) mechanisms to obtain the necessary authorisations to operate with privileged rights on these systems.

With the use of dedicated accounts for the different tiers, PAWs for Tier 0 and policy enforcement through specific GPO (Group Policy Objects), the risk of violation is significantly reduced. For example, the administrator who is victim of phishing does not have rights to access to Active Directory with his ordinary account: to perform administrative tasks, he will have to use a PAW with Tier 0 account. This strong segregation between areas, that opposes normal privileges versus administrative privileges, is the principle that underlies the operation of the Tiering Model proposed by Microsoft and shown in Fig. 1.2.

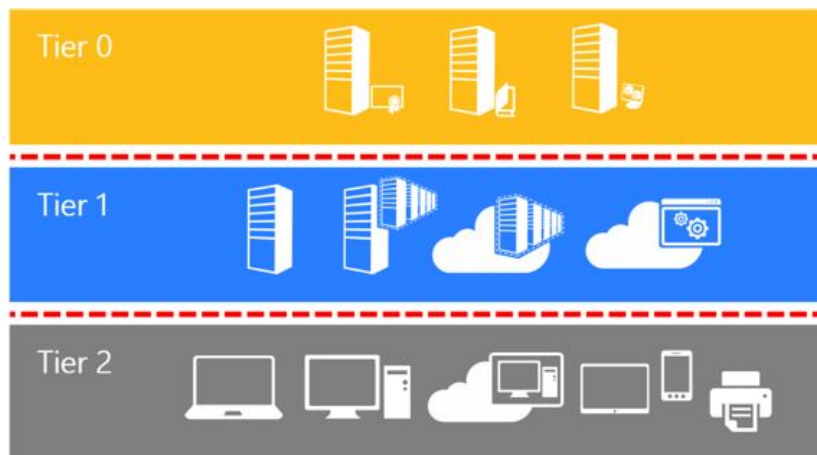


Figure 1.2. Security Architecture - Legacy Tier Model [83]

As foreseen by many advisors in the past, cloud adoption is rising year by year and nowadays only few organizations do not have at least an hybrid approach and this makes Fig. 1.2 no longer up to date, because it applies only on legacy environments (i.e. on-prem only). Public cloud infrastructures rely on control-plane and management-plane based on centralized access (e.g. Microsoft Entra ID) to identify users and provide administrative access to control plane it self. To ensure segregation between Administrators and users, it is necessary a separate privileged access path for administrators for control-plane and management-plane, while end users can only access to published applications.

The new schema, shown in Fig. 1.3 updates also the tier definitions as follows:

- **Tier 0:** It expands by including the control plane. Identity access control is used to protect the Tier 0, while network access control is used only when identity cannot be verified.
- **Tier 1:** It splits into two different areas: management plane, data/workload plane. The aim of the split is to focus the protection on the business critical systems with a limited extra effort. This approach better matches the DevOps model compared with classic infrastructure roles.
- **Tier 2:** According with customer models, it splits this tier into two areas: User Access (B2B, B2C, Public Access) and App Access (API).

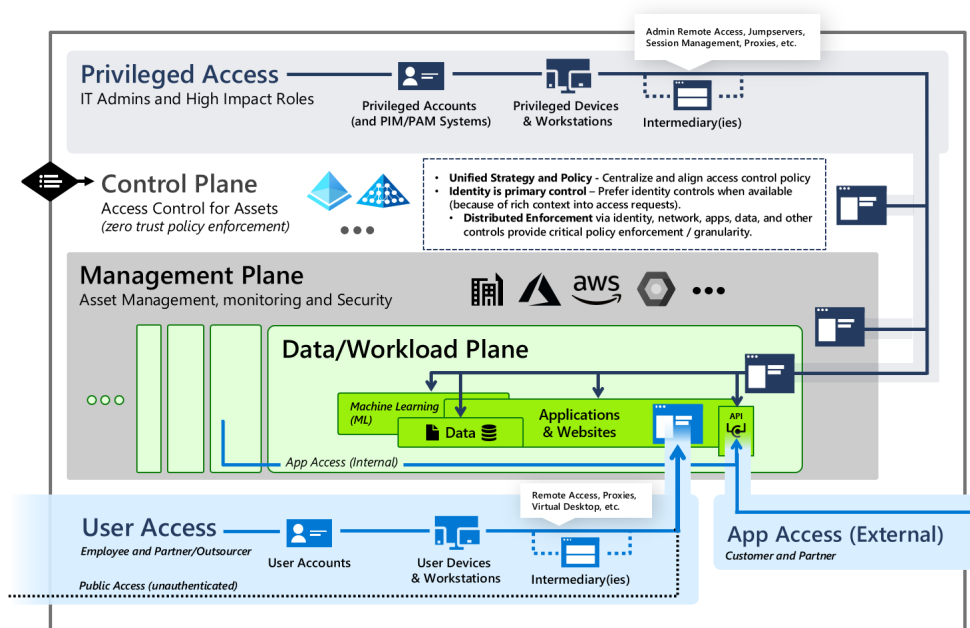


Figure 1.3. Security Architecture - Evolution of Tier Model [83]

1.3 Security Operation Center

The main objective of security architectures is to 'minimize' threats through preventive security measures. As we have seen, there are no solutions that make possible the elimination of risks, which is why, over time, organizations have equipped themselves with specialized units for managing IT security incidents that are able to identify and react to threats that cannot be, by definition, completely blocked through preventive security mechanisms.

1.3.1 Security Operation Center History

A Security Operation Center (SOC) is a unit equipped with monitoring systems to detect possible illicit activities and tools to minimize and eradicate threats once they are detected.

The SOC evolution has passed from a reactive approach to the incidents to a proactive approach with the ambition of preventing attacks. The main milestones in the evolution of SOCs are explained next.

- **(1990-2000)** In the first phase, SOCs responded reactively to security events primarily identified by network tools (firewall, IPS/IDS). The accuracy of the measurements was limited and relied mainly on updating the IDS/IPS signatures. The reaction was mainly limited to operations on network systems.
- **(2000-2010)** In the early 2000s SOCs were more advanced than their predecessors and incorporated new technologies, such as SIEM (Security information and event management) and UEBA (User and Entity Behaviour Analytics) tools. These technologies allowed SOCs to collect and analyze more data, which helped them to identify and respond to threats more effectively.
- **(2010-today)** Modern SOCs have expanded their databases to identify security events and they introduced new technologies such as machine learning and artificial intelligence, as well as threat intelligence and SOAR (Security Orchestration Automation and Response).

The expectations for SOCs' next evolution concern the use of more advanced artificial intelligence to support SOC operators in the analysis of security events as well as in the systematic reporting of all the evidence collected. It is also reasonable to expect that automation in security incident response will be supported by artificial intelligence and will involve an increasing number of attack response actions. These evolution are not only a cool way of doing things, but they will likely be necessary because even opponents will start adopting artificial intelligence to support information gathering, the development of new malware, further accelerating the execution time of an attack.

1.3.2 Types of SOC

SOC operating models change according to the organization and different terminologies are used to indicate different approaches in security incident management, like CERT, CSIRT, cSOC.

- **SOC (Security Operation Center):** The Security Operation Center is frequently more focused on security event monitoring
- **cSOC (cybersecurity SOC):** Even though the focus is still on monitoring, large organization can decide to put more emphasis on the difference between cybersecurity (related to digital data protection) and information security (extended to all the information formats, e.g. papers)

- CSIRT (Computer Security Incident Response Team): While SOC and cSOC are primarily focused on monitoring, the CSIRT's main objective is to manage incident response, investigate possible breaches and provide an immediate response with the aim of interrupting the chain of actions that compose an attack or trying to containing the impacts
- CERT (Computer Emergency Response Team): It is similar to CSIRT, but with a broader scope that often includes interaction with other corporate functions to coordinate an organic response to the security incident

As reported in NIS Investment report [35], about 37% of OSE (Operatore di Servizi Essenziali) or PSD (Fornitore di servizi digitali) do not have a dedicated SOC and rely on shared services provided by third parties. A proper incident handling requires a deep knowledge of the organizations and the context where it operates to be effective. Third Parties SOC can be considered as a first stage of the Security Incident Process, leaving to internal staff the responsibility of responding to security incidents.

1.3.3 SOC Challenges

Regardless of the organizational model adopted, the security incident management unit faces multiple challenges that make it more complex to counteract adversaries. The most relevant challenges are briefly introduced in the following sections.

Data everywhere: The amount of data generated is constantly increasing. Corporate data is often managed through systems and devices outside the organisation's control. For example, cloud services for personal data storage (e.g., Dropbox) or employees' personal devices or cloud services for sharing files for a specific purpose (e.g., slideshare, virustotal) can be source of loss of confidential corporate data and are difficult for the SOC to control.

Users everywhere: With the pandemic outbreak of 2020, many organizations adopted as a new way of working the remote mode. Employees could perform their job activities everywhere an internet connection was available. This new model brings new risks, like: connection to enterprise through internet publishing APPs and APIs that before were not necessary exposed to internet, difficulty in updating corporate devices and detecting anomalous activities while they are not connected to corporate networks.

Stratified and Heterogeneous architecture: The rate at which the IT industry introduces new technologies is much faster than the rate at which companies discontinue previous technologies. Moreover vendors rarely support their solutions for more than 10 years and enterprise companies' plan to decommission their IT systems are quite often based on business needs rather than technological obsolescence. This leads companies to accumulate a technological debt that is frequently the main cause of vulnerabilities in IT systems.

Visibility: Complex environments, fragmented management and constant changes do not make it easy to keep track of what is happening in the networks. Moreover, to get information about a system is necessary to access to several management tools that often

only provide part of them. To manage promptly a security incident, it is necessary to have information immediately available and organized in such a way to allow rapid navigation through various levels.

Increasing Attack Trends & Human Error: As reported in the Clusit Report [25], the number of attacks is increasing year by year. Ensure the adequate attention to each of them is becoming non human sustainable.

Under-staff: Cybersecurity can be considered as an emerging science and before the 2000s was mainly related to military and financial sectors. With the diffusion of internet a growing number of new threats have risen creating the need for new professionals with specific skills related to information protection. In the very last years the process of digitalization, pandemic outbreak and geopolitical changes have increased the level of risks to which organizations are exposed. Finally, the new regulations have forced even the most reluctant companies to consider cybersecurity as a necessity. This evolution has happened at a faster rate than education system was able to prepare new technicians with the required skills. The lack of cybersecurity workforce is a world wide problem as reported by ISC2 workforce study [67] and could reach a shortage of 3.4 million employees in 2025.

Supply Chain and Third Parties: Geopolitical changes have emphasised the risk related to third parties. Since few years ago the main concern about third parties was related to the fact that they could be the entrance channel for an attack, nowadays suppliers often store enterprise data and play a key role in the delivery of business services. Compromising a strategic supplier can put an important business process or the entire company fronting a severe risk.

Shadow IT: The main goal of a SOC is to identify threats and minimize the risk of impact on Confidentiality, Integrity and Availability of business data. This usually happens through the monitoring of corporate assets, however it is increasingly common for business users to subscribe to IT services (even free) without making it known to IT department. This phenomenon, called shadow IT, makes particularly difficult the identification and containment of attacks.

1.3.4 Security Incident Process

There are several international standards describing the security incident handling process, the most relevant are:

NIST Computer Security Incident Handling Guide [120]: It provides guidelines for managing incidents and determining the appropriate response.

SANS Incident Handler's Handbook [66]: It provides information about the six phases of the incident handling process.

ISO/IEC 27035:2016 [119]: It provides a structured approach to detect, report, assess, respond to incidents and apply lessons learnt.

CIS Incident Response [28]: It covers all phases of the incident response process, from preparation to detection and analysis, containment, eradication and restoration and post-incident activities.

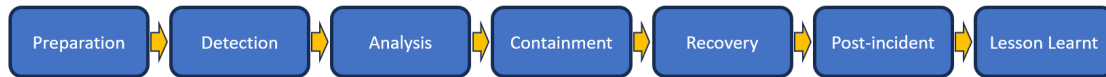


Figure 1.4. Security Incident Process - Phases

Even if with some slight differences in terminology, most of the standards agree on splitting the Security Incident Handling process into the following seven phases (see also Fig. 1.4):

- **Preparation:** It relates to process definition, assigning responsibilities, creating the necessary resources and documents.
- **Detection:** Focuses on the identification and analysis of potential security incidents. This task can be done with a variety of tools and techniques such as log monitoring, network traffic analysis and staff training.
- **Analysis:** This is the assessment phase and it focuses on evaluating the impact of the incident and determines the appropriate action to be taken. In this phase, it is necessary to gather information about the incident such as its nature, scope and potential impact.
- **Containment:** The containment phase focuses on limiting the impact of the incident. In this phase, measures like isolating affected systems or resources, must be taken to prevent the incident from spreading further.
- **Recovery:** The recovery phase focuses on restoring systems and data affected by the incident. In this phase, they must be restored to the safe state as before.
- **Post-incident:** This phase focuses on identifying the cause of the incident and gathering evidence for the investigation. In this phase, it is necessary to comprehend the incident, by studying the the activities of the attacker and the vulnerabilities exploited.
- **Lesson learned:** It focuses on learning from the incident and implementing measures to prevent its recurrence. In this phase, it is necessary to identify and fix the security gaps that contributed to the incident.

Communications and reporting are distributed in all the phases, even if since GDPR and NIS were published they are often well formalized with clear responsibilities and resources planned in advance.

1.3.5 Cybersecurity Tools Classification

ENISA provides an interactive tool [34] to link the minimum security measurements required for the OSE (Operatore di Servizi Essenziali) with the most relevant international standards: *ISO27001* [69], *NIST CFS* [102], *ISA/IEC 62443* [1]. These measurements are organized in classes that are not suitable for the purpose of this thesis, because they are not specialized in the security incident management process.

Another possible classification is provided by *NIST 800-53B* [122], that gives a set of baseline controls that must be adopted according to the system relevance and its privacy. The approach adopted in this paper does not allow to identify easily market products, because it is referred to security controls instead of security tools. CNSS Committee on National Security Systems has released its own classification with the paper *CNSSI 1253* [99], starting from NIST classification and providing explicit mapping with the relevance of the controls in terms of Confidentiality, Integrity and Availability. This classification cannot be considered suitable for the purposes of this study.

The lack of security tools classification is justified by the fact that international standards are focused on controls and do not want to implicitly sponsor a class of market solutions where there are often just a short list of suppliers world wide. More over, as reported in the “Anomaly Cybersecurity Insight Report - The state of Enterprise Cyber Resilience“, the average number of cybersecurity tools used by large enterprises overcome 130 [12] and they are increasing year by year. This can quickly make documents related to security tools obsolete if compared with those related to security controls.

In order to make the analysis of the different security solutions integrated with SIEM, SOAR and xDR easier, it is proposed a classification that groups together solutions dedicated to the protection of the same resource. In table 1.2 are reported various cybersecurity tools and their domain of application. A brief description of each tool is provided in the acronyms section.

Class Name	Description	Tools	
Identity	Solutions for digital identities protection	MFA PKI UEBA PIM	M2M Authentication Users Directory Services Conditional Access Behaviour Analysis
End Point	Solutions for End Point Protection (workstation, mobile and server)	EPP EDR SWG	MDM DNS Security Browser Security
Mail	Solutions for email protection	Antispam Antiphishing	Email Sandbox AntiBEC
Data	Solutions for structured and unstructured data protection	DLP TDE	Data Masking Tokenization
Application	Solutions for WEB Application and API Protection	WAAP WAF SAST	DAST IAST SCA
Infrastructure	Solution about cross-cutting components	Backup PKI	Log management
Network	Network level security solution protecting network access, communications, application and infrastructure	NGFW IPS IDS WAF NAC	SASE AntiDDOS VPN Network Visibility Asset Discovery
Cloud	Solutions to protect cloud workloads and to ensure compliance.	CSPM CASB CWPP	CNAPP SOAR
Intelligence	Services providing useful information to detect and counteract adversaries	Threat Intelligence	External Attack Surface

Table 1.2. Cybersecurity Tools Classification

1.4 Threat Detection and Response

To identify possible security incidents, one of the most effective ways is to analyze the traces in the logs generated by different systems. Analyzing these traces manually is not feasible, for this reason, in the early 2000s, computer industry has introduced the SIEM (Security information and event management) solution able to perform this task automatically using built-in rules or leaving the users the opportunities to define their own.

Without going into details between the different generations of SIEMs, it is important to note that these solutions have begun to introduce over the time more complex techniques to identify possible breaches, such as: predictive analysis based on artificial intelligence, expansion of the systems that can be integrated, behavioural analysis, big data analysis, log enrichment from external sources and also modules for managing the attack response.

Recently, the market has introduced a new terminology for threat detection and response solutions called xDR (eXtended Detection and Response). Although they are sold as different products, SIEMs and xDRs are very similar technologies. Compared to SIEMs, xDRs also allow information to be gathered from external sources. Configuration management systems and vulnerability assessment systems are queried to collect updated information about system configurations and vulnerabilities. Threat intelligence systems are inquired to obtain information about the evolution of threats all over the world (e.g. presence of

exploits and ongoing campaigns). Moreover, thanks to the integration with PEPs, xDR platforms are able to carry out containment actions of threats also in an automatic way, like: network isolation, password reset, taking artifacts from a device, killing a process, blocking traffic towards a certain IP/DNS direction and so on. When the response to an attack is articulated over several systems and through several phases, the contribution of a SOAR (Security Orchestration Automation and Response) is often necessary.

In addition to the tools used to identify threats affecting corporate assets, SOCs also adopt other solutions to extend the scope of monitoring beyond the boundaries of business systems. These technologies fall within the definition of threat intelligence tools and they include solutions about:

- **Deepweb/Darkweb Monitoring:** It searches within the Deepweb/Darkweb forums and chats traces of company files, information related to the company and information about apical subjects.
- **Enrich information:** It is based on reputation analysis of IP addresses, emails, domain names and other parameters that characterize internet communications.
- **Honey Pot:** It allows the early identification of the attacks by providing a fake enterprise system that can capture the attention of the attackers. This solution also allows to study the technique of the adversaries.
- **Threat forecasting:** By using artificial intelligence and machine learning, it tries to predict potential new threats.

1.4.1 Playbook

Playbooks are used by SOCs to describe the steps to follow in order to respond to a security event, they provide a guidance to security analysts and operators by standardizing their actions. Playbooks are strictly related to correlations rules that include: the fields to be correlated, the threshold values, the information to be enriched and which actions have to be taken (e.g. open an incident, define incident severity level, send a notification to SOC operators and activate automatic remediation actions).

XDR platforms combine EDR (End Point Detection and Response) and NDR (Network Detection and Response) capabilities and they are integrated with cloud APIs, in order to get visibility of the security events across the entire enterprise information system. XDR platforms also permit the definition of playbooks able to perform automatic responses against specific threats. Some examples of correlation rules are available in Table 1.3.

Correlation rules often refer to IP address, UserID, Session ID, Timestamp, application/service name, file name, object name, event type, Geo-Localization, email address and they correlate events from different logs entries.

Table 1.3. Example of correlations rules

Rule Name	Description	Action
Impossible Travel	Single user logs in from two different geographical locations within a short period of time	Generate an alert
Access to data through privileged accounts	High-privileged user account (e.g. administrator) attempts to access sensitive resources	Generate an alert
Port scanning	Series of failed connection attempts is detected on a specific range of ports from a single IP address.	Generate an alert
Malware detection	Known malware file is detected on a machine or network	Generate an alert File quarantine
Brute force	High number of failed login attempts are detected from a single IP address within a short time.	Generate an alert Block the IP address
Network behaviour analysis	Network traffic to or from a specific network or host exceeds predefined thresholds (e.g. bandwidth)	Generate an alert
User behaviour analysis	Suspicious activities are detected at specific times or days of the week, such as access during the weekend	Generate an alert
Device behaviour analysis	Device exhibits unusual behaviour compared to their historical behaviour pattern (e.g. increase in data access)	Generate an alert
Possible unauthorized data modification	Seemingly unrelated events are detected but together indicate a possible attack, such as a successful login followed by unauthorized data modification	Generate an alert
Possible data exfiltration	Large amounts of data leaving the internal network and being sent to external IP addresses	Generate an alert
Possible Phishing	Series of incoming emails contains known phishing indicators, such as suspicious URLs or malicious attachments	Generate an alert Quarantine emails
Suspicious administrator activities	High-privileged user executes obfuscated commands by changing the encoding or usage of escape characters, to make less human readable its operations	Generate an alert Disable user account
Unauthorized change detected	Unauthorized modifications to server or network device configuration files are detected	Generate an alert Recover configuration
Bad reputation communication	Network traffic from an internal host to a country known for hacking activities is unusually high or exhibits anomalous communication patterns	Generate an alert
Detection of Break Glass Account usage	Usage of Break glass account access has been detected instead of Tier Zero Account in a Tiered Active Directory	Generate an alert
Multiple EDR alerts detected	A relevant number of alert has been generated by EDR on different hosts	Generate an alert Isolate affected hosts

1.4.2 Enrichment

SIEM Platforms do not rely only on correlations between different log sources, but they also try to enrich information through different external sources, such as: System configuration, vulnerability assessment, end user information (e.g., working hours), IP address and email reputation, presence of IOC (Index Of Compromise), information collected by the asset (e.g., active process list). The following example shows how a simple log entry can be enriched to support threat detection.

Before enrichment:

Timestamp: 2023-09-15 14:30:00
 Event Type: Failed Login
 User: jdoe
 IP Address: 192.168.1.1
 Source: Web Application

After enrichment:

```
Timestamp: 2023-09-15 14:30:00
Event Type: Failed Login
User: jdoe
IP Address: 192.168.1.1
Source: Web Application Location: Turin, IT
User Role: Employee
Device: Windows 10
Department: HR
Previous Successful Login: 2023-09-14 10:15:00
```

Thanks to username, the log entry can be enriched with information about last successful login, user role and department. Moreover, thanks to IP address, it is possible getting the geo-localization and the device OS. These information are often useful to have the complete picture of a security event.

1.4.3 Threat Intelligence

One of the most effective way to enrich log information is through Threat Intelligence. It can be realized by API integration to third party threat intelligence tools or through a threat intelligence feed. In the first case, when required, the SIEM/xDR can query the threat intelligence service to get specific information, such as:

- **IOC:** They are specific data points that indicate the presence of malicious activities or threats (Suspicious IP, URLs, Domains, Hashes of files, Signatures, attacks patterns).
- **Exploit:** It reveals the presence in the Dark Web of artifacts that allow to exploit for a specific vulnerability.
- **Attack Techniques:** They give details about attack techniques used by malicious actors.
- **Attribution:** Some feeds include information about the attribution of attacks, meaning details about the actors or groups responsible for the threats.
- **Known Vulnerabilities:** They give information about known software vulnerabilities and available patches.
- **TTP:** Detailed analysis of the TTPs used by threat actors enables a better comprehension of how attacks are carried out.
- **Compromised user account detection:** It allows to get the list of user accounts exchanged in the Darkweb markets.

When threat intelligence services gather information from public available sources, we are dealing with the so called OSINT (Open Source Intelligence). Some examples of OSINT sources include: Websites (e.g. forums, blogs, news papers), Social Media and Social

Networks, Public Records (e.g. Government records, property records, IANA registry and any public accessible database), Geo-localization data (e.g. GPS coordinates, satellite images), Public Documents (e.g. academic papers, research reports, white papers), Internet Archives (e.g. historical websites archives).

Intelligence information that do not come from open source are named CLOSINT (Closed Source Intelligence) and they include the following disciplines: HUMINT (Human Intelligence) related to human sources, MASINT (Measurement and Signature Intelligence) related to physical features or patterns that allow the identification of a subject, IMINT (Imagery Intelligence) associated to collection and analysis of images and SIGINT (Signal Intelligence) associated to the study of signals (e.g. radio). All of these disciplines permit to collect information in a structured way that can be used for threat hunting or forensic analysis.

Threat Intelligence information can also be collected by Honey-pot or Canary-token. A Honey-pot acts as a trap to attract attackers and gather information about their tactics, techniques and intentions. On the other hand Canary-token is a digital or cryptographic security mechanism used to detect unauthorized access or activity within a network, system or application. It can take various forms, including URLs, email addresses, files or specific types of documents and it is placed inside the assets supposed to be more subjected to adversary attacks (e.g. home banking application). When the attackers get the asset or clone it (e.g. phishing web page), the Canary-token starts working by notifying his presence to the defender.

One of the most advanced ways through which intelligence services collect information from the adversary consists in infiltrating the adversaries networks. This type of approach is very complex and oriented only towards the largest and most active cyber-gangs. It requires in-depth knowledge of their attack techniques and a lot of time for its implementation. Cyber-gangs operate in a similar way as normal companies and, like these, they need to hire manpower. As for traditional criminal organizations, the infiltrated can access to very sensitive information, like: techniques that cyber criminals are going to use in the next attack, the chosen victims, personal information about cybercriminals and others highly confidential information. This approach is often implemented in cooperation with Europol's European Cybercrime Centre (EC3) and other National Cybersecurity agencies.

1.4.4 Behaviour analysis

Behaviour Analysis can be performed at different levels. Possible areas can be: networks, emails, users and endpoints.

This analysis aims at identifying deviations, outliers and anomalies in the activities of users, devices, services and network traffic. The techniques adopted to achieve this objective are based on machine learning, Artificial Intelligence, Heuristics and Rules-Based Analysis and Pattern Recognition. For example, an access of a user to a large number of files or outside normal working hours could be evaluated as a possible anomaly.

Behaviour Analysis is often useful to identify new types of attacks that would not be visible with the other types of investigation.

1.4.5 Information Sharing

As shown in Section 1.4.3, Threat Intelligence provides a set of useful information for decision-making: their collection and sharing, plays a very relevant role in the strategic approach against Cyber Crime. Countries, sector supervisory agencies and business associations are establishing even more programs for sharing threat intelligence information because it is becoming of paramount necessity to counteract cyber crime and cyber attacks.

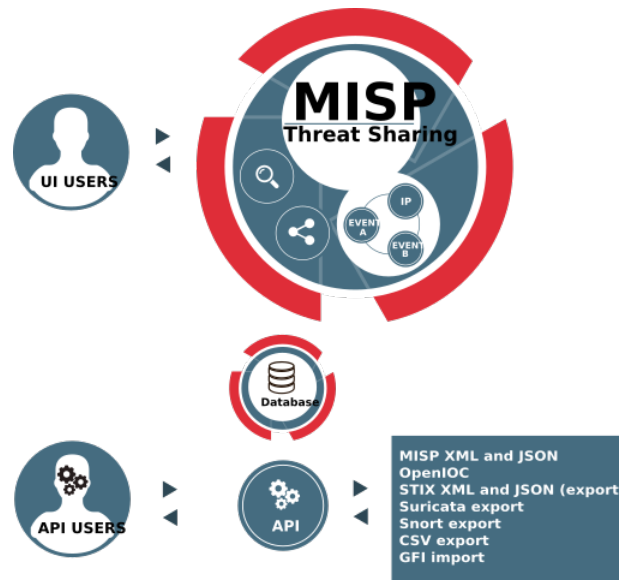


Figure 1.5. MISP - Threat Sharing platform [115]

In Fig. 1.5 is presented the logical schema of MISP (Malware Information Sharing Platform & Threat Sharing). This open source project is based on a platform that shares, stores and correlates IOCs of targeted attacks, threat intelligence, financial fraud information, vulnerability information or even counter-terrorism information. The main characteristics of the platform are: collaborative approach in sharing information, standard data format and standard protocols. The platform provides functionalities that allow to share information within a group of allies, as for instance CERTFIN [71], an association of Italian financial enterprises that shares, among other things, also threat intelligence information.

One of the side effects of sharing is that the quality of the information is highly dependent on who is publishing it. In addition, many of the indicators of compromise (e.g., ADSL dynamic IP address), have a reduced lifetime, which then leads to the necessity of using strategies of sanitising feeds or weighting them according to the type of indicator or source. These tasks often require more than one step and should be managed automatically.

1.4.6 Orchestration

Security Orchestration is a process that connects and coordinates human and security tools actions to improve the efficiency of cybersecurity operations.

SIEM/XDR platform facilitates the definition of simple automated responses for the simplest cyber threats. Whenever the response requires many phases and the cooperation with many security services, the effort for coordination becomes too much to be viable just with SIEM/XDR: in these cases it is necessary to use an appropriate platform called SOAR (Security Orchestration Automation and Response).

SOAR can operate effectively during the most complex security incidents and also during normal operation activities (for example to deal with vulnerability management) thanks to the integration with different security systems such as IDS/IPS, Firewalls, authentication systems, SIEM, WAF and so on. SOAR Playbooks are often activated by alerts generated by SIEM/XDR.

The need for orchestration is also due to the fact that attacks are almost executed automatically, leaving to analysts/operators very short time to respond to the attacks.

1.5 Adversary Analysis

Adversary analysis is a discipline used to relate authors, targets, tactics and techniques and the victims of an attack. It grants a view for better understanding security incidents and a way for identifying how to generate the greater difficulty to adversaries.

In the next sections will be presented a journey through the most interesting approaches to adversary analysis, touching: Diamond Model, Mitre Att&ck framework, Pyramid of Pain and Cyber Kill Chain.

1.5.1 Diamond Model

The Diamond Model [22] is a conceptual framework designed for supporting the comprehension of intrusion events. It was proposed by two researchers, Francesco Caltagirone and Chris Pendergast, from Recorded Future, a leading threat intelligence company.

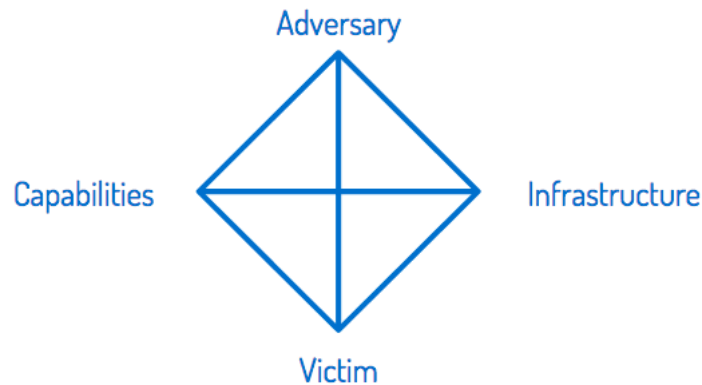


Figure 1.6. Adversaries Analysis Frameworks - Diamond Model [40]

As shown in Fig. 1.6, the model links together the 4 vertices of a diamond, where we can find: Adversary, Capabilities, Infrastructure and Victims. In the center of the diamond is located the security event in order to provide a logical schema for studying intrusion events. The idea is that there is always an adversary performing an operation to achieve a specific goal against the victim and exploiting capabilities through infrastructure. Getting into the specifics:

Adversary: Person or group that poses a threat to an organization’s information system or data. Adversaries can be motivated by a variety of factors, including financial gain, espionage or simply the desire to cause disruption. Adversaries can be internal (malicious or negligent) or external (activists, cybercriminals, state-sponsored actors). It can be described as a threat actor with various characteristics: name, nation-state affiliation, list of the references, events in which it has been involved, malware employed, countries of the victims and so on.

Victim: Target of the attack campaign. In case of nation-state sponsored adversary or a big organized group, the victim can be represented by a category like government institutions. It is to be stressed the difference between the target of the attack (e.g. a windows device) and the victim (e.g. energy companies).

Capabilities: Tools and TTPs (Tactics, Techniques and Procedures), such as malware and attack vectors, adopted by the adversary to strike the victim. Some examples are: RAT (Remote Access Trojan), mobile malware, phishing, social engineering and APT (Advanced Persistent Threat).

Infrastructure: set of IP addresses, domains, botnets and technologies in general used by the adversary to perform the attack.

The study of intrusion-events is relevant in cybersecurity and Diamond Model links together adversaries, victims, tools (infrastructure) and techniques (capabilities) adopted,

for the purpose of providing support to design more effective defenses and key information about the evolution of the attack.

1.5.2 MITRE - ATT&CK framework

Adversaries usually operate on systems of an organization for months before being detected. The main goal of the security incident analyst, is the study of how they got in, how they moved within the organization and what actions they put in place. To solve this problem, MITRE developed the ATT&CK framework: The Mitre ATT&CK observes attacks as the problem that adversaries have to solve to achieve their goals. The description of the adversaries' problem is made through TTPs:

Tactics: They are high-level attack goals organized in categories like: Reconnaissance, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement and Impact.

Techniques: They are methods for achieving tactical goals and are organized into categories such as: Phishing, Exploitation of vulnerabilities, Malware, Social engineering.

Procedures: They are step-by-step instructions for carrying out specific techniques and they are organized in categories like: Creating a phishing email, Exploiting a vulnerability, Exfiltrating data.

Mitre provides dedicated matrices according to the environment: Enterprise, Mobile and ICS (Industrial Control System). There are also sub-matrices for more specific contexts. One of the most interesting is the one related to cloud environments [91], that can be useful to counteract cloud-based-attacks. Mitre constantly updates the list of TTPs, by making them available on Mitre website [96]. TTPs are widely used by cybersecurity experts because they are found to be very effective in dealing with cybercriminals.

1.5.3 Pyramid of Pain

In 2017 David Bianco, a SANS instructor, has introduced the concept of “The Pyramid of Pain“ (shown in Fig. 1.7) [21] that is useful for understanding which actions can cause the most damages to the adversaries.

The pyramid organizes the IOC (Index Of Compromise) in six different levels, where indicators considered more valuable have been placed at the top of the pyramid, because they are the ones that can cause the greatest harm to attackers. The concept of damage means blocking the attacker's actions or the need for the attacker to change his technique. For example, the detection of an IOC related to file hash can be easily bypassed by attackers through the introduction of a minor change to the file's that result in a different file hash. On the other hand blocking a TTP results a big effort for the attacker that has to adopt another useful TTP to achieve his objective.

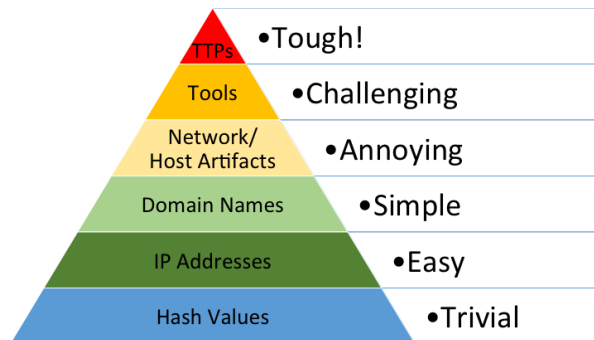


Figure 1.7. Adversaries Analysis Frameworks - Pyramid of Pain [21]

The pyramid of pain is a significant concept in countering cyber criminals, because it allows defenders to be focused on the highest value-added actions.

1.5.4 Cyber Kill Chain

The Cyber Kill Chain [78], shown in Fig. 1.8, is a key concept in intrusion detection and response that describes the different phases of an attack, from reconnaissance to exploitation. It was introduced by Lockheed Martin, a leading military and aerospace company, as part of a model related to cyber intrusion activity management.

This model illustrates the things an attacker must do to achieve his goals: it is composed of seven phases that help the analysts to enhance the comprehension of the adversary tactics, techniques and procedures. These phases are:

Reconnaissance: The attacker gathers information about the target, such as its systems, networks and users.

Weaponization: The attacker creates a malicious payload, such as a virus or malware, that can be used to exploit the target’s vulnerabilities.

Delivery: The attacker delivers the malicious payload to the target, for example through an email attachment, phishing attack, usb-pen or drive-by download.

Exploitation: The attacker exploits a vulnerability in the target’s system to gain an access.

Installation: The attacker installs malware on the target’s systems.

Command & Control (C2): The attacker establishes a command and control channel between the malware and its own systems. This allows to control the malware and issue commands.

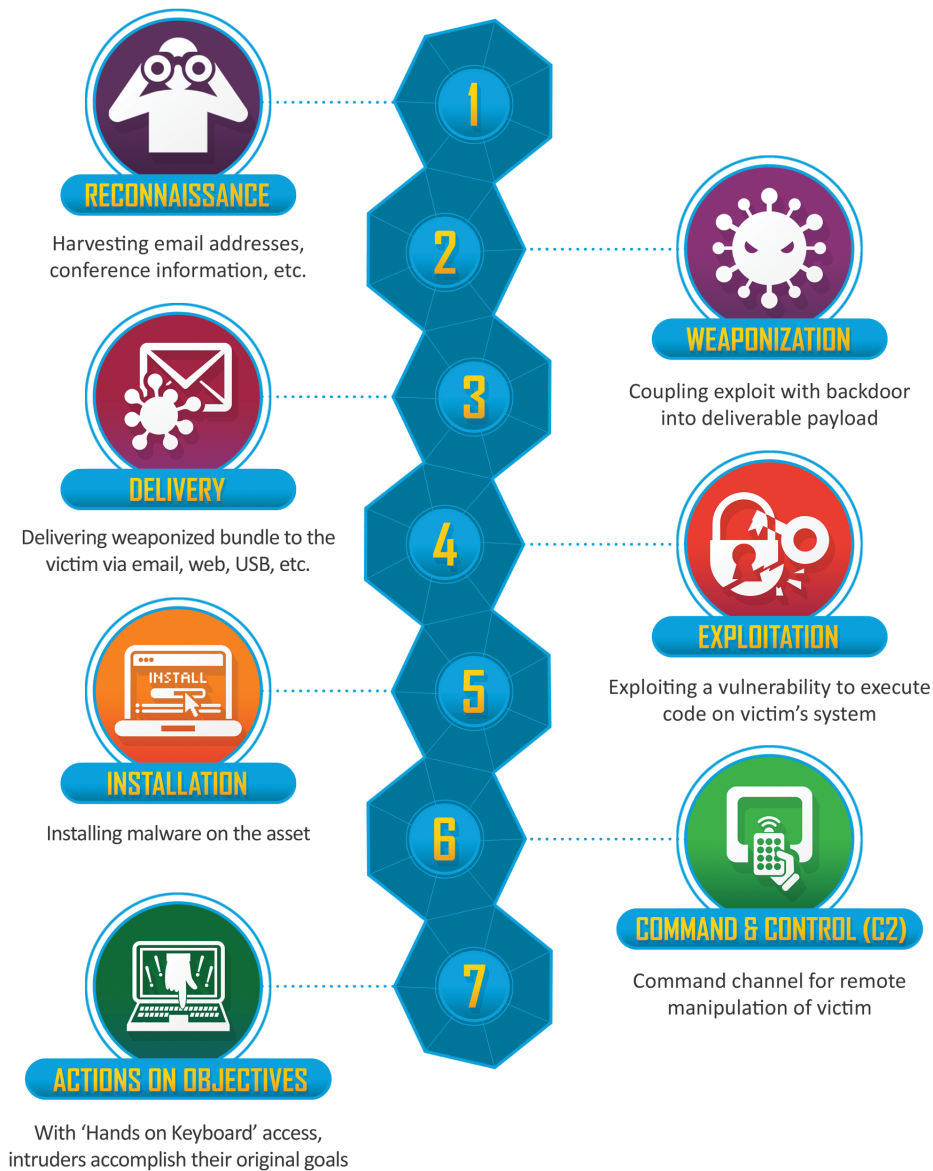


Figure 1.8. Adversaries Analysis Frameworks - The Cyber Kill Chain [78]

Actions on objectives: The attacker achieves his intention, such as stealing data, disrupting operations or launching further attacks.

The cyber kill chain is an important concept in countering cyber criminals because makes it clear that attackers have to overcome different steps before achieving their goals. The sooner these actions are identified and blocked, the less damage is going to be produced.

1.5.5 Mitre ATT&CK VS Cyber Kill Chain

To complete the sections about Mitre ATT&CK and Cyber Kill Chain, a comparison between them is provided in the following lines.

As reported in the Jorge Orchilles paper [113], The Cyber Kill Chain and the MITRE ATT&CK are complementary tools that can be used to improve cybersecurity. The Cyber Kill Chain provides a high-level view of the attack process, while the MITRE ATT&CK gives a more detailed view of the techniques and tactics used by threat actors.

Purple teams can use both tools to improve their ability to simulate realistic attacks and to identify and mitigate vulnerabilities. Red teams are responsible for simulating attacks, while Blue teams are responsible for defending against those attacks. Purple teams are composed by members of Red and Blue teams that work together to improve the overall security posture by identifying and remediating vulnerabilities and by developing and testing security controls.

Cyber Kill Chain and MITRE ATT&CK can be used to simulate more realistic attacks and to identify mitigations: the first one identifies the steps involved in a particular type of attack, the second one identifies the specific techniques and tactics that attackers might use to carry out those steps.

1.5.6 Malicious Actors and Malware

To complete the adversary analysis, an overview of the main groups of adversaries and malware classified by MITRE or other associations is provided. A first classification of adversary groups can be done on their motivations:

State-sponsored actors: There are groups or Organizations that are backed, supported or directly employed by a government or state entity to conduct cyber activities for political, economic, military or espionage purposes.

Cyber criminals: These are individuals or groups who engage in illicit activities in the cyberspace for financial gain or personal satisfaction.

Hactivists: Individuals or groups who use their technical skills to carry out cyber activities in pursuit of political, social or ideological goals.

In tables A.1, A.2, A.3, A.4 and A.5 are reported some of the most famous malicious actors identified during the last decade to provide an idea of the strength and the structure of the malicious actors that defenders have to face. What appears to be evident is that there are often collaborations between malicious actors: for example, there are actors specialized in the creation of malware that they make for others. This practice has been named “Malware As A Service“ or “Ransomware As A Service“. In table A.6 there is a short list of famous malware: a brief overview of the tools adopted by hackers can help understanding the level of sophistication achieved and predicting what may happen in the near future with a greater use of artificial intelligence and automation. The malicious

ecosystem is rapidly evolving, leading the defenders to work together against emerging threats.

1.6 Defenses

The analysis of the adversary may have designed an alarming landscape, however, the sophistication of attack techniques is a direct consequence of the constant improvement of defense systems.

In this section there will be a presentation of the most promising frameworks and tools that defenders can use to strengthen defenses. In addition, there will be some interesting analysis and initiatives that support defenders activities.

1.6.1 Defender mindset

The mindset of defenders is different from that of attackers. A famous statement by John Lambert (Microsoft Corporate Vice President, Security Fellow, Microsoft Security Research) says “Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win.“

In the paper [76], Lambert highlights how linear approach commonly adopted by defenders is not enough, because it does not consider that assets are connected to each other by security relationships and attackers breach networks by finding vulnerable systems and navigating the graph of relationships created by defenders. In the example of Fig. 1.9), Defenders surround Domain Controllers of protections (EDR, FW, PIM, Patching), while attackers try to identify breaches in one of the systems that provides a service to it. The graph is a set of security dependencies, that creates a class of equivalences of security risks. For example, the workstation used by a security administrator to administrate the Domain Controller must be protected at the same level of the Domain Controller. For this reason Microsoft proposes to adopt the Tiering Model shown in section 1.2.3. While defenders are focused on protecting one possible attack path, attackers discover multiple paths to the High Value Asset by navigating the graph. There are many security dependencies that are the paths of the graph, for example: Local admin account with common password, file server housing the LogOn Script, certification authorities and others. Along these lines, Tiering Model helps to dramatically reduce the number of the paths to Domain Controllers.

Defenders can learn a valuable lesson from how attackers perceive the system. Attackers move into the actual infrastructure, avoiding inaccurate mental models, incomplete asset inventories or outdated network diagrams. The ideal approach for defenders should be the one based on the reality of the situation.

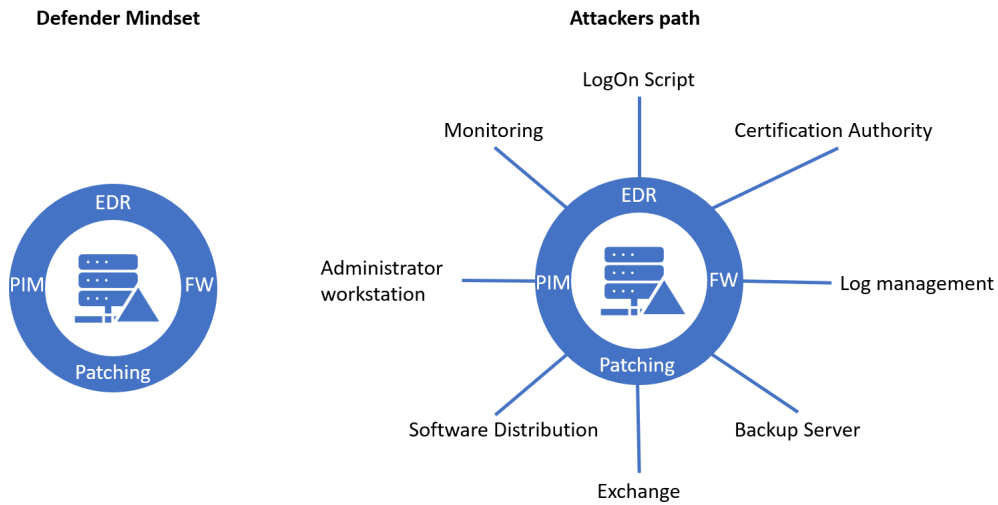


Figure 1.9. Defenders think in lists. Attackers think in graphs

1.6.2 Mitre D3FEND

According with the idea of the graph of relationship and its huge database of information about attackers, malware, techniques, tactics and procedures used by adversaries, Mitre is developing D3FEND [92], a cybersecurity knowledge graph (shown in Fig. 1.10) that provides a meaning of defensive cyber techniques and is designed to help organizations to build and implement effective cybersecurity strategies. The framework consists of three main components:

- **Knowledge:** This component provides a comprehensive overview of defensive cyber techniques, including capabilities, dependencies and relationships.
- **Tools:** This component provides a set of tools and resources to help organizations to implement the D3FEND framework.
- **Processes:** This component provides guidance and best practices for implementing the D3FEND framework.

ATT&CK Lookup		Search D3FEND's 521 Artifacts												D3FEND Lookup						
Model	-	Harden				Detect								-	Isolate	Deceive	-	Evict		
+	Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	+	Credential Eviction	File Eviction	Process Eviction			
	Application Configuration Hardening	Biometric Authentication	Message Authentication	Bootloader Authentication	Dynamic Analysis	Homoglyph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	Firmware Behavior Analysis	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation		Account Locking	File Removal	Process Suspension			
	Dead Code Elimination	Certificate-based Authentication	Message Encryption	Disk Encryption	Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Embedded Monitoring Code	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting		Authentication Cache Invalidation	Email Removal	Process Termination			
	Exception Handler Pointer	Certificate Pinning	Transfer Agent Authentication	Driver Load Integrity Checking	File Content Rules	Identifier Reputation Analysis		Certificate	Firmware	Indirect Branch Call	Credential Compromise	Hardware-based Process Isolation	DNS Denylisting		Credential Revoking					

Figure 1.10. MITRE - D3fend Poster [92]

As shown in Fig. 1.10 defences have been classified in different categories:

- **Model:** It includes information about the topology and behaviour of an information system.
- **Harden:** It includes techniques that can be used to make information systems more resilient to attacks.
- **Detect:** It includes techniques that can be used to identify and respond to malicious activity on information systems.
- **Isolate:** It includes techniques that can be used to isolate infected devices and prevent the spread of malicious activities.
- **Deceive:** It includes techniques that can be used to mislead attackers and make them difficult to carry out their attacks.
- **Evict:** It includes techniques that can be used to remove malicious actors and malware from information systems.

The largest category is “Detect“. It includes several subcategories according with the type of detection required (e.g., File Analysis, Network Traffic Analysis). For each subcategory there could be more then one defend practice. For example, within the File Analysis category, there is the countermeasure “Dynamic Analysis“ structured with information about: Definition, Synonyms (e.g. Malware Detonation), How it Works, Considerations, Implementations (e.g. Cuckoo), Digital Artifact Relationships (see Fig. 1.11), Related ATT&CK Techniques (see Fig. 1.12) and References.

While Mitre ATT&CK framework provides information about adversary tactics and techniques, Mitre D3FEND provides support developing countermeasures. It could be useful identifying which process or tool fits better against a specific threat.

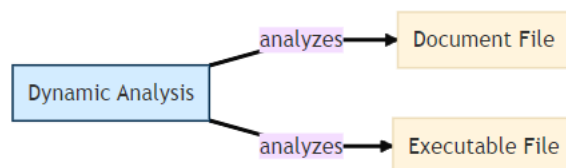


Figure 1.11. MITRE - Example of Digital Artifact Relationships [92]

1.6.3 Mitre ATT&CK Flow Project

The Attack Flow project, developed by the MITRE Center for Threat-Informed Defense, provides language and tools for describing the sequences of adversary actions that lead to successful attacks. The project has the ambition of helping defenders to understand how adversaries operate and improve their own defensive posture [94].

Collection	Defense Evasion	Discovery	Execution	Lateral Movement	Privilege Escalation	Persistence	Impact	Initial Access
Email Collection	Deobfuscate/Decode Files or Information	System Network Configuration Discovery	Command and Scripting Interpreter Execution	Internal Spearphishing	Process Injection	Hijack Execution Flow	Data Manipulation	Phishing
Local Email Collection	XSL Script Processing		User Execution		Thread Execution Hijacking	Path Interception by PATH Environment Variable	Runtime Data Manipulation	Spearphishing Attachment
	Obfuscated Files or Information		Malicious File Execution		Abuse Elevation Control Mechanism	Path Interception by Search Order Hijacking		Spearphishing Link
	Binary Padding				Bypass User Access Control			

Figure 1.12. MITRE - Example of Related Attack Techniques [92]

The Attack Flow language is based on the MITRE ATT&CK framework, which is a comprehensive knowledge base of adversary tactics and techniques: it uses ATT&CK techniques as building blocks to represent the sequences of actions that adversaries take to achieve their objectives. The Attack Flow language is supported by a set of tools that can be used to create, visualize and analyze attack flows in order to identify common attack patterns, assess the risk of specific attack flows and develop defensive strategies. To support attack flows description, Mitre offers a User Interface (see Fig. 1.13) in the Mitre web site [95]. It enables to add information about adversary actions and drawing arrows indicating the sequences of adversary techniques observed during an incident or campaign.

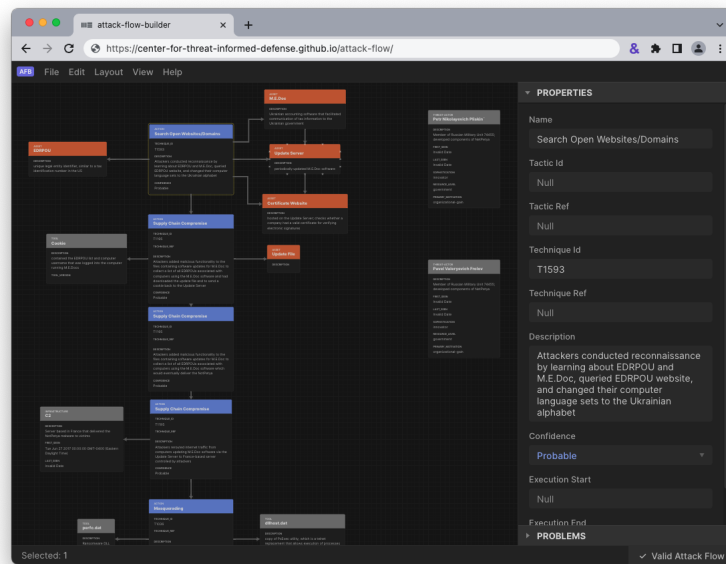


Figure 1.13. MITRE - ATT&CK Flow Builder Overview [95]

Standardizing the representation of the stages of an attack is a primary need. Defender can use Mitre ATT&CK flow both for designing security countermeasures and for incident reporting.

1.6.4 MITRE Engenuity ATT&CK Evaluation

The MITRE ATT&CK Evaluations are a series of assessments that measure the effectiveness of cybersecurity products and services against known adversary tactics and techniques.

The evaluations are conducted by MITRE Engenuity and all vendors can participate: evaluations are formalized on the MITRE ATT&CK knowledge base and they are updated regularly to reflect the latest threats and trends. Participants are presented with a series of attack scenarios that are based on the MITRE ATT&CK framework and they are then evaluated on their ability to detect and respond to attacks. The results of the evaluations are published publicly and they constitute a valuable resource for organizations that are looking to select and implement cybersecurity solutions, but, as reported by The Hacker News [100], results are not easy to be interpreted and almost all participants declare themselves as the “winners“, because during the assessment vendors have the opportunity to adjust configurations settings to match missing threats.

In conclusion, Mitre Engenuity ATT&CK Evaluations is a valuable tool that can be adopted to get independent comparisons between different threat detection and response tools against known tactics, techniques and procedures used by adversaries.

1.6.5 Mitre - Sightings Ecosystem project

Another interesting collaborative MITRE project is Sighting Ecosystem [128] which has the aim to increase the ability of cyber defenders to see threat activities across organizations, platforms, vendors and geographic boundaries, in order to prioritize defensive operations.

The unit responsible of this project CTID - Center For Threat Informed Defense, has defined a data model that helps contributors to share information: an example of sighting report is provided by a project team with the following instance: “If mimikatz was used on a victim machine to dump credentials and that was observed by an EDR tool, it would constitute a direct sighting of Credential Dumping. This might take the form of a sighting of a process accessing lsass.exe memory, for example“.

The need to share information on compromise indicators and attack techniques is something that is also gaining ground at the regulatory level, as Article 45 of the DORA Directive demonstrates: “Financial entities may exchange amongst themselves cyber threat information and intelligence, including indicators of compromise, tactics, techniques and procedures, cyber security alerts and configuration tools, to the extent that such information and intelligence sharing.“ [110].

Chapter 2

Market Analysis

Nowadays Public cloud hosts the IT services of many strategic organizations. However, one of the reasons why the adoption of cloud services has not been massive yet is because of the lack of data centers within national borders: this kind of limitation has been gradually overcome in recent years with the progressive opening of data centers in Italy by all the leading public cloud providers (Microsoft Azure [87], Google GCP [53] and Amazon AWS [6]).

It is not a hazard to predict that almost all OSEs use public cloud services for their IT services, but even those who have strategically decided to adopt an on-premise strategy, will embrace solutions that allow them to build a private cloud, i.e. a data centre with a high degree of automation, exploiting the stacks offered by public cloud providers (Azure Stack [81], Google Anthos [43], AWS Outposts [7]) or opensource stack solutions (Open Stack, Kubernetes, Ansible).

This chapter begins with an analysis of the most popular hyperscalers because they play a key role in the definition of the so called “*ecosystem*“, a set of resources that work together to protect from cyber threats. The entities inside an ecosystem can natively exchange information because they share data types and fields that have the same semantics.

As reported by CSA [26], the three main cloud security issues are in a certain way related to misconfigurations performed by customers and not by cloud platform vulnerabilities. Public Cloud providers offer a wide range of security features and services and they are responsible for the security of the underlying infrastructure, but it is ultimately responsibility of the customer to secure its applications and data running in the cloud infrastructure. For this reason, customers should take care of their security by choosing a security framework like: Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) [68], ISO 27001 [70], NIST CSF [102].

The main takeouts of the above frameworks are:

- Strong passwords and multi-factor authentication (MFA) for all accounts, because public clouds get more attention from adversary.
- Least privilege access, because it reduces the risk of unauthorized access.

- Data encryption at rest, because it ensures protection of data even if they are stolen.
- CSPM (Cloud Security Posture Management), because it identifies and remediates security risks of the cloud environment.
- xDR (eXtended Detection and Response) and SOAR (Security Orchestration Automation and Response), because their use monitors cloud environment in order to identify suspicious activities and react promptly.

The following sections will provide an overview of the cybersecurity approach of the main cloud providers, deepening the Threat Detection and Response platform and its main components: query languages and automation.

The analysis does not verify the security of cloud platform infrastructures because it assumes that the differences between main cloud providers are negligible, but it focuses on the tools made available by the various platforms to the customers.

As reported by Gartner [42], Azure, AWS and GCP cover 69% of the overall world wide market. In table 2.1 the subdivision of each CSP.

Company	Share
Amazon	40.0%
Microsoft	21.5%
Google	7.5%
Total	69.0%

Table 2.1. Cloud Computing Market Share

2.1 Microsoft Azure

Microsoft Azure offers a multitude of services IaaS, PaaS and SaaS, used by companies of all sizes and government agencies all over the world.

Cybersecurity approach of Azure is described in the document Azure Security fundamentals Overview [79], that provides a comprehensive look of Azure security by organizing it into six different areas: *Operations, Applications, Storage, Networking, Compute and Identity*.

In the following sections the features of interest for a SOC will be discussed in depth.

2.1.1 Operations

Within the *Operation* category there are a set of tools useful for security operations and the most relevant will be presented briefly.

SIEM & SOAR - Microsoft Sentinel

Microsoft Sentinel is a multi-purpose tool SIEM/SOAR and is one of the most powerful tools for SOCs that operate in an Azure environment, because it provides attack detection, threat visibility, proactive hunting and threat response features. It is strictly integrated with many of the following tools.

xDR & CSPM - Defender for Cloud

Microsoft xDR platform is named *Defender for Cloud*: despite common xDR platforms it does not rely only on agents installed on the systems (server or network equipment) but it collects also information by PaaS/SaaS services like: API Gateway, Azure Kubernetes Services, Azure SQL, APP Services, Storage, key Vault, Azure Resource manager, DNS, Azure DevOps.

This approach permits a better visibility on what happens on the enterprise assets and a more accurate response to threats. Thanks to the information collected by telemetry services deployed on corporate assets (including mobile devices, Windows and Linux boxes), Defender for Cloud acts as CSPM (Cloud Security Posture Management) and provides useful information to prevent threats like: asset vulnerabilities, presence of not monitored assets, insecure configurations, products EOS (End Of Support) and threat intelligence. Moreover it provides suggestions about what to fix first and how to fix it, in order to improve overall security in a more effective way.

Azure Resource Manager

ARM allows to deploy, update or delete all the resources through a single interface and represent a good instrument for auditing and tagging features to help the management of the resources. Thanks to template-based deployments, it helps to improve security because it includes standard security control settings that avoid configuration errors.

Log and Monitoring - Azure Monitor

Azure monitor grants the collection of the log trace of all the activities carried out on each individual Azure resource. This tool is essential for forensic analysis or during the management of an incident, because it allows to execute queries on a large amount of data without having to switch from one device to another.

2.1.2 Applications

Applications are the main channel of entry for legitimate traffic and for this reason are often the part of the attack surface most targeted by attackers. To protect application workloads, Microsoft provides a set of tools delivered in SaaS mode. If a solution is not included in Microsoft portfolio, there could be third parties available in *Azure market place* and in some cases they could be natively integrated with other cybersecurity tools.

Penetration Testing & Azure DevOps

No system or application is inviolable, that's why it is important to carry out pen tests. Microsoft does not have any built-in solution for performing VAPT (Vulnerability Assessment and Penetration Testing), but it approves security assessments on Azure infrastructures.

VAPT can only be related to Microsoft Azure resources and must not involve any other Microsoft Cloud Service: this means that is not possible to assess the security of PaaS and SaaS and customers have to trust on Microsoft Security.

Customers can perform the following assessments:

- OWASP top 10 vulnerabilities
- Fuzz testing
- Endpoints Port scanning

A relevant role in Application security is played by SAST & DAST. These solutions are employed during the whole development life-cycle, that in Microsoft environment is often performed by instruments integrated with Azure DevOps.

Microsoft Security DevOps Extension enables to manage DevOps environments through Defender for Cloud, and provides in real time visibility on Application vulnerabilities and releases to the SOC.

Web Application Firewall - Azure WAF

Azure Web Application Firewall helps protecting web applications from common web-based attacks like SQL injection, cross-site scripting attacks and session hijacking. It is pre-configured to protect through OWASP top 10 vulnerabilities: If the feature is enabled, *Azure WAF* and *Azure DDoS Protection* alerts are immediately visible in Defender for Cloud without any other configuration.

Microsoft also has a geographical WAF named *Frontdoor* which has the same features of Azure WAF, but it is delivered through edge computing: this approach helps to achieve lower latency for applications that require it.

2.1.3 Storage

Data protection in cloud resources is a complex issue because it concerns both the customer, who has to guarantee the principle of least privilege and need-to-know, and the cloud service provider who must be prevented from accessing corporate data. Microsoft guarantees this through the feature *Role-Based Access Control*: least privilege and need-to-know principles are commonly enforced by *RBAC model*. Microsoft provides an extensive set of pre-defined roles that can be assigned to end users: if special authorizations are required, a specific custom role can be defined as well.

2.1.4 Encryption at rest

Data encryption at rest is mandatory in order to be compliant with regulatory about data privacy. There are three Azure storage security features that provide encryption of data "at rest":

- Storage Service Encryption: It allows the automatic encryption of data written on Azure Storage.
- Client-side Encryption: It provides the feature of encryption at rest on workstations.
- Azure Disk Encryption: It allows the encryption of the disks used by Linux VMs and Windows VMs.

2.1.5 Networking

Network access control is a feature that limits communications between two or more peers, by allowing just the strictly required communications. On Azure environments this can be performed by several tools and features.

Network Security Groups

NSG (Network Security Group) provides stateful Layer 4 packet filtering firewall, it doesn't provide application layer inspections or authenticated access controls, but it can be used to control traffic between subnets, Virtual Network and Internet. *Azure Monitor* can collect logs about which NSG rule is applied and how many times.

Azure Firewall

Azure Firewall is a Layer 7 stateful firewall with high availability and unrestricted cloud scalability out of the box that provides threat protection by threat intelligence feeds. The premium version provides also IDS/IPS capabilities.

Internal DNS & Azure DNS

Internal DNS allows to manage the list of DNS servers used by Azure Resources. It can be protected by *Defender for DNS* that permits to gain visibility about DNS resolution and avoid Data exfiltration, malware communication, DNS Attacks and generally speaking communication with domains used for malicious activities (such as phishing). *Azure DNS* is a hosting service for DNS domains providing name resolution using Microsoft Azure infrastructure.

2.1.6 Compute

Compute categories include services related with VMs security. The list below represents just the features that could be useful during SOC's operations.

Anti-malware & Antivirus

To protect IaaS workloads, it is possible to use anti-malware software provided by many different security vendors. *Microsoft Anti-malware* is a free tool that identifies and removes malware. This feature can be also deployed using *Microsoft Defender for Cloud*.

Hardware Security Module

To perform encryption and authentication in a secure way it is necessary to handle properly the related keys. *Azure Key Vault* is a HSM (Hardware Security Module) that simplifies key management by providing features like: secret management, key management, certificate management. Using HSM makes possible to control secret distribution and to avoid the needs to store the secret inside the code of the applications. Key/Secret access is controlled by *Azure Active Directory* and Azure RBAC. Moreover centralizing key management allows to monitor access and usage of the keys by enabling *Defender for Key Vault* and to detect unusual and potentially malicious access to key vault accounts.

Virtual Machine Backup

Azure Backup, permits to be protected from data corruption due to human errors or malicious activities and protects both Windows and Linux virtual machines.

Azure Site Recovery

Azure Site Recovery helps to orchestrate replication, fail-over and recovery of workloads and apps according with the Business Continuity and Disaster Recovery Plan of the organization. When a disaster occurs, workloads will be moved from the primary site to the planned secondary site.

SQL VM TDE

This service allows to apply TDE (Transparent Data Encryption) to SQL workloads to protect information from unauthorized access. The symmetric key used for cryptographic operations is stored on Azure Key Vault. Anomalous access to the key can be detected by Defender for AKV.

VM Disk Encryption

As for TDE, this tool allows to protect the disks of Windows and Linux Virtual Machines hosted by Azure IaaS services. Symmetric keys are stored on AKV as well.

Patch Updates

Patch Updates provides support to software management process and helps finding and fixing possible issues.

2.1.7 Identity

To protect Systems, Applications and Data it is mandatory to ensure a proper identity and access management. Azure provides the features described below to support customers achieving this purpose.

Secure Identity

Secure Identity is a set of practices and technologies that manage identity and access in a secure way, by adopting at least the following characteristics:

- *Multi Factor Authentication*, always required for admins account and available for all users.
- *Password Policy Enforcement*, rules that allow to define minimum length, complexity requirements, rotations and account lockouts.
- *Conditional Access*, a configuration that allows application to require a step up authentication in case some context parameters (e.g. location, device security posture, simultaneous authentication) notify a non-appropriate level of confidence about the user.

Authentications via *Microsoft Entra ID* enable *Defender for Identity*, a cloud-based security solution that helps organizations to protect against advanced threats, compromised identities and malicious insider actions directed at their enterprise hybrid environments. It uses on-premises *Active Directory* signals to identify, detect and investigate anomalous behaviours.

Secure Apps and data

As mentioned in the section 1.3.3, Shadow IT represents one of the most relevant challenges that SOC have to deal with, because it can expose organizations to vulnerabilities and cyber attacks or compliance issues. *Cloud App Discovery* is a premium feature of *Microsoft Entra ID* that helps to identify Shadow IT and it relies on *Defender For Cloud for Endpoint* telemetry and SWG (Secure Web Gateway) logs.

2.1.8 Other Tools

The security solutions described above can also be implemented with third-party products available in *Azure Marketplace*. Thanks to the public API documentation published by Microsoft and the Software Development Kit for various programming languages, third-party solutions can easily be integrated in the Azure ecosystem.

There are also other relevant security solutions not mentioned in the Azure Security Fundamentals [79] such as:

- *Azure DDoS Protection*: Suite of Anti DDoS tools that protects against network based DDoS and application based DDoS. Alerts can be collected by Defender for Cloud.
- *Microsoft Defender for Office 365*: Cloud-based security solution that helps organizations protecting their Office 365 environment from threats such as phishing attacks, malware and ransomware.

- *Microsoft Compliance Manager*: Cloud-based solution that helps organizations to assess, manage and improve their compliance posture. Compliance Manager gives a comprehensive set of assessments that cover a wide range of industry regulations and standards, like GDPR and ISO 27001.

Microsoft solutions listed above interact with each other and they facilitate the job of the SOC analyst to control events generated by a single dashboard.

2.2 GCP - Google Cloud Platform

As described in the “Google Cloud Architecture Framework“ [51], GCP’s approach to cybersecurity is based on three pillars:

- **Integrated security**: GCP includes a number of built-in security features that protect data and applications of users. These features include: *Encryption* at rest and on transit, *Access control* to data and resources and *Incident detection and response*.
- **Managed security**: Managed security services allow customers to be focused on their business by leaving the security management to Google. It includes the following services: *Cloud Identity and Access Management (IAM)* about data and resources in GCP, *Cloud Security Command Center (SCC)* that provides a centralized view about security in GCP and *Cloud Armor* that provides protection against DDoS attacks.
- **Collaborative security**: This pillar is about collaboration with customers and security communities to improve GCP security. Google participates in open source security initiatives and shares its knowledge and expertise.

Google core security principles include defense in depth, at scale and by default: this means that GCP data and resources are protected by policies and controls through multiple layered defenses on IAM, encryption, networking, detection, logging and monitoring.

2.2.1 GCP Infrastructure Security

Google shares interesting details about its own security in the paper “Google infrastructure security design overview“ [52]. The document is organized in the following Security Domains:

- **Secure low-level infrastructure**: It explains physical aspects of cybersecurity.
- **Secure service deployment**: Google services are distributed across shared infrastructures, the same that contemplate customer services and data. According with Zero Trust principles, Google infrastructure does not assume any trust between services that are running on it.
- **Secure data storage**: Google provides security for data stored on the infrastructure through the following processes and features: Encryption at rest, Deletion of data, Secure internet communication, Google Front End service, DoS protection and User authentication.

- **Operational security:** Protection of data and services of the customers relies on the following process and features: safe software development, source code protections, safeness of employee devices and credentials, reduction of insider risk, threat monitoring and Intrusion detection.

GCP Customer security can be assured through the adoption of several security tools from different areas. In the following paragraph there will be a brief overview about each of them.

2.2.2 Computing Security

This paragraph refers directly to the official Google documentation [47], in this material is illustrated that compute resources can be protected by adopting several security features.

Shield VM

Shield VM allows to harden VM instances and prevents the loading of malicious code during the boot by monitoring the integrity of the VM image thanks to TPM (Trusted Platform Module). It can be normally used for sensitive workloads. In addition, it is possible the incorporation of third party solutions available in the Google Cloud Marketplace: many of them are natively integrated with *Security Command Center*, the dashboard that can be used for threat detection and health monitoring.

Confidential VMs & Confidential GKE

Confidential VMs and *Confidential GKE* are confidential computing features that enable to build secure VM or container where data are computed through a TEE (Trusted Execution Environment). This is a secure and isolated environment that prevents unauthorized access or modifications of the application while the data is in use.

OS Login

Os login allows the use of IAM credential instead of SSH Keys while connecting to a VM and avoids the need to handle SSH Keys. It supports two factors authentication.

Cloud NAT gateway & Private access

Cloud NAT gateway is a managed Network Address Translation (NAT) service that enables instances in a private subnet to connect to resources outside VPC networks. When it is not strictly necessary, the access from Internet should be disabled. By using *Private cluster* in GKE (Google Kubernetes Engine), nodes can assume only internal IP addresses and pods are isolated by default. Private access options for services permit to manage network access policies for pod-to-pod communication.

Node Auto-Upgrade & App Engine

GKE (Google Kubernetes Engine) cluster can be updated automatically to the last patch by activating *auto-upgrade features*, while *App Engine* allows to run only stateless and immutable container in GKE (Google Kubernetes Engine).

VPC Service Controls

It allows to control resources consumed by pods by defining quotas.

GKE Sandbox

GKE Sandbox can be used to create an extra isolation layer useful when it is necessary to run unknown or untrusted code: an additional isolation between running applications and the host operating system, can be provided by kernel application.

2.2.3 Network Security

This paragraph refers directly to the official Google documentation [56].

Moving to the cloud involves a deep change in the way network security has to be done. Boundaries are less defined in cloud environments and they require a different approach and sometimes different tools.

VPN browser-based

Access to enterprise networks via cloud-based VPNs is becoming increasingly popular. Through *BeyondCorp Enterprise*, Google allows employees to work everywhere without the need to install an agent and moves the controls on the user side also about Threat and Data Protection.

Identity-Aware Proxy (IAP)

Identity-Aware Proxy (IAP) allows to extend the Zero Trust paradigm to customer applications: it performs identity and access management basing its consideration on user and device context too.

Cloud VPN and Cloud Interconnect

Cloud VPN provides IPSEC connections, while *Cloud Interconnect* provides low latency connections. Another option is *Cross-Cloud Interconnect* that allows a dedicated connection with other supported cloud providers.

Firewall policies and rule

Firewall policies and rules can be defined in *Firewall Mash Architecture* or in *Hierarchical Firewall*. In combination with *Identity and Access Management* and *Governed Tags*, they permit to define micro-segmentation with granular control and context-based perimeter security.

Context-based perimeter security

It is an application security gateway that allows, denies, redirects or balances traffic to work nodes.

Secure Web Proxy

Secure Web Proxy allows or denies egress web traffic from worker nodes and it monitors access to untrusted sites.

Cloud IDS and Packet Mirroring

Cloud IDS inspects network traffic and it gives visibility of the traffic moving inside or outside of VPC networks. *Packet Mirroring* clones traffic of specified VM instances in VPC networks and forwards it for collection, retention and examination. This solution also allows the use of third-party tools to inspect network traffic.

Web Application Firewall

Google *Cloud Armor* provides Distributed Denial-of-Service (DDoS) and Web Application Firewall (WAF) capabilities to workloads that are exposed to Internet.

Automate infrastructure provisioning

Infrastructure can be defined through an immutable state, i.e. a state that cannot be changed after provisioning: for this reason it can be used for troubleshooting and fast rollback through the use of tools such as *Terraform*, *Jenkins* and *Cloud Build* (by Google).

Network Monitoring

Network monitoring is based on telemetry, *Cloud Logging* and *Cloud Monitoring*. It is suitable for troubleshooting or tuning network configurations and topology.

2.2.4 Data Security

This paragraph refers directly to the official Google documentation [48].

Sensitivity, Amount, life-cycle and ownership of the data are some of the parameters that must be considered to design a cloud infrastructure properly. In the following lines are exposed the tools provided by Google to protect data.

Data Classification

Thanks to *Sensitive Data Protection*, it is possible to discover and classify files stored in Cloud Storage, BigQuery and Datastore. Another way to protect custom solutions is through *streaming API*. Classification is based on info-types and matching criteria: once classified, information can be automatically masked, tokenized or transformed to protect the data in their lifecycle.

Data Governance

Data Governance is a set of processes that ensure the company's strategy regarding data management. Google provides a set of tools that help to define a framework for data

governance: *Data Catalog* helps to find and use metadata related to assets in the cloud and together with *Sensitive Data Protection* it can be used to add tags sensitive to the identified data or assets. Through *Google Identity and Access Management (IAM)* it is possible to restrict the access to the assets.

Dataproc Metastore and *Hive Metastore* are two components of Google Datalake infrastructure that handle metadatas.

Dataprep by Trifacta is a data preparation tool that can be used in data ingestion pipeline within *Cloud Data Fusion* or stand alone.

Data life-cycle management

Security controls can be applied according with data classification, risk evaluations and context of the data. Google organizes its own framework of controls in three different categories:

- **Identification:** It has the goal of understanding the identity of users, resources and applications that operate on data. It includes: *Cloud Identity* and *Certificate Authority Service*.
- **Boundary and access:** It is a set of controls on how data is accessed, by whom and under what circumstances. Data boundaries can be enforced at different levels: Network level and Identity and Access Management level.
- **Visibility:** Through *Google Cloud Logging* and *Access Transparency* evidences about how data are accessed can be collected.

Encryption

By default data are encrypted at rest: customers can decide to manage the encryption keys directly.

- **Cloud Key Management Service (*Cloud KMS*):** Keys are created by a Google service and handled by the customer. Cloud KMS allows to store the key in HMS: to ensure geographical replica of the key, the use of *Cloud HLM* is possible.
- **Customer-supplied encryption keys (*CSEK*):** Keys are created by customers and they provide them to Google when needed. Customers can also decide to provide only encrypted data to Google, in this case the data are encrypted twice (once by the customer and once by Google).
- **Cloud External Key Manager (*Cloud EKM*):** Keys are created and stored by third-parties supported by Google.

Cloud Administrator Control

Through *Access Transparency* and *Access Approval*, customers can control and approve access to their own data by Google data center operators.

Data Sovereignty

It is possible to configure access and location of the data (where they are stored) through *VPC Service Control* and *Google IAM Policy*.

Secret Management

Secret Manager allows to store data centrally, it traces access and rotates secrets. Some examples of secrets are database passwords, API keys or TLS certificates.

Data Monitoring

Cloud Audit Logs takes traces about activities of administrators. Logs can be collected by *Cloud Logging* and through *Security Command Center* it is possible the monitoring of data exfiltration: this tool scans storage systems for confidential data and detects which Cloud Storage buckets are open to the internet.

2.2.5 Secure Deployment

This Paragraph refers directly to the official Google documentation[44].

Deploy Applications in GCP is supported by a set of tools, tests, gates and stages according with the customer SSDLC (Secure software development life-cycle) process.

Automate secure releases

Automation is the key stone for a well designed SSDLC. CI/CD (Continuous Integration/-Continuous Development) pipeline helps to standardize development feedback loops and to enable fast iterations when required. Automation can be used to scan for security vulnerabilities when artifacts are created and it can provide necessary assurance before passing the gate of production environment deployment. *Cloud Build* allows integration with several software repositories like GitHub and others. With *Private pools* can be deployed a set of isolated worker nodes to perform dynamic vulnerability tests or source code analysis.

Secure application deployments

Adversaries may try to act maliciously on the CI/CD pipeline to compromise services or applications. With *Binary Authorization* it is possible to enforce the authorization process in CI/CD pipeline if target Deployment are GKE or Anthos (multi cloud container platform).

Vulnerabilities Scan

During development process, continuous scanning for vulnerabilities ensures that security issues can be addressed soon when the fix costs and the impact are lower. *Artifact Analysis* allows to perform automatic scan for containers stored in *Artifact Registry* and *Container Registry*.

Web Application vulnerability scanner

Continuous checks on OWASP TOP10 vulnerabilities allow to reduce risks. *Web Security Scanner* helps identifying security vulnerabilities in App Engine, Compute Engine and Google Kubernetes Engine web applications.

Data exfiltration

VPC Service Controls allows to mitigate the risk of unauthorized copy or transfer of data (data exfiltration) from Google-managed services. Limiting the possibility to transmit data only inside the perimeter of the services of the organization can be useful to deal with insiders. Legitimate traffic that matches access policy and passes through perimeter bridges is the only one permitted.

Encryption of containers images

Google allows to encrypt container images using *customer-managed encryption keys (CMEK)*: this lets customers to protect their own container and to make it inaccessible also by Google by just removing or destroying the key in CMEK.

2.2.6 Logging and Detection

This Paragraph refers directly to the official Google documentation [55].

Logging and detection are the most relevant set of security measurements for the purposes of this document. There will be shown the most powerful tools that SOCs can use to protect data, information and identities. Detective controls use telemetry to discovered misconfigurations, vulnerabilities and potentially malicious activities.

Monitor network performance

Network Intelligence Center is the dashboard where cloud experts can see information and get insight about network performances: through *Connectivity Test* it is possible to test firewall rules to verify if they are working properly.

Monitor and prevent data exfiltration

As described in section 2.2.4 it is possible to define a set of rules that, verifying the data tags, allows the identification of exfiltration.

Centralize monitoring

Security Command Center is the core function of Google security monitoring and it provides advanced features to identify wrong configurations, vulnerabilities and possible malicious activities. With the features available out of the box, Security Command Center is able to identify possible malicious activities from security logs generated by all the resources in GCP. It can be integrated with a third party SIEM or with log analysis tools like

Log Analytics, BigQuery, Chronicle. A set of security query or correlation rules are available in the *Community Security Analytics (CSA)*. Google provides also a guide related to Automatic Security Operations [45], that admits to transform Security Command Center in a SOAR.

The three main features of Security Command Center are:

- **Event Threat Detection:** It is a service included in Security Command Center premium level, that continuously monitors GCP workloads and recognizes threats in near real time. Event Threat Detection automatically analyzes log flows generated by GCP and Google Workspace by applying different techniques based on proprietary threat intelligence, analysis of specific parameters, machine learning and anomaly detection. Event Threat Detection findings can be exported in Pub/Sub way to others systems: system investigations can be performed through *Chronicle* that acts like a SIEM and provides pivot through related entities and events timeline. Event Threat Detection includes a set of default rules to identify some of the most common threats, moreover users can define custom detection rules based on templates written in JSON (JavaScript Object Notation).
- **Security Health Analytics (SHA):** Feature that provides an evaluation on vulnerabilities and unsafe configurations about GCP workloads. With the premium tier of this solution, vulnerabilities are detected by three different tools: Rapid Vulnerability Detection, Security Health Analytics and Web Security Scanner. Security Health Analytics provides also: a Benchmark to GCP Foundation standard, a synthetic indicator (Attack exposure scores) about the whole attack exposure, a visual representation of paths that an attacker can take and a Compliance report with international standards.
- **Sensitive Actions Service:** Feature that provides visibility about actions taken on GCP environment and that can be dangerous if taken by malicious actors. The sensible action are those that can be considered legitimate but if they are not can make relevant damages to the organization. This categories of events include, for example: changes on organization policies, admin accounts changes, relevant number of instances deletion, addition of a SSH authorized keys.

Monitor for threats

Monitoring threats in a GCP environment can be done by *Event Threat Detection*, an optional feature of *Security Command Center* that helps to identify malware, cryptomining, unauthorized access, DDOS, Brute force attacks and other threats. The main advantage of this feature is that is able to reduce the amount of data that has to be analyzed by Security Operators automatically and it correlates events and provides drill down visibility to security events when required. *Sensitive Actions Cloud Platform* helps to pay attention to potentially dangerous activities performed into GCP environment.

Chronicle allows to store and analyze security data: logs are mapped into a common model enriched by threat intelligence, IoC and other useful information and they are organized in timelines. A query language named **Yara-L** can be used for analysis purposes or to

create custom detection rules. Google also provides *curated detection*, a set of pre-defined rules that can be customized by the customer. Logs can also be collected in *BigQuery*, in this case the common model can be requested via standard SQL queries

2.3 AWS - Amazon Web Services

AWS has the ambition to be the most secure cloud solution. The building blocks of this claim are the following three pillars:

- **Security By Design:** This is the key principle for any service provided to customers.
- **Automation:** Security Operations take benefits of automation, because they reduce the risk of human errors and allow security operators to be focused on higher value-added activities.
- **End-to-end Security:** AWS, together with its partners, provides a large set of security solutions according with best practices and international standards. AWS has defined a program named *AWS Security Competency Partners* in order to make easier the identification of partners that can natively improve customer AWS environment security.

AWS Security services are organized in five categories that look like the five categories of NIST CSF[102]:

- **Identify:** Visibility and automation help to handle risks.
- **Prevent:** Identity and Access Management help to protect infrastructure and data.
- **Detect:** Visibility of security events and information help to recognize malicious activities.
- **Respond:** Automated incident response and recovery helps security operators and analysts to be focused on root cause analysis.
- **Remediate:** Event driven automation allows to quickly remediate and secure AWS environment.

Amazon provides a huge number of documents related with information security available at the URL [15]. Amazon also provides guides dedicated to AWS Security architecture, the most relevant are listed below.

- **Introduction to AWS Security [17]:** This document is a brief overview about AWS security approach and references to security products and features, security guidance documentation and compliance.
- **Defense in depth security strategy at the edge [18]:** This document shows how a layered security architecture takes advantage of the edge computing, saving response time and bandwidth and protecting resources directly at the edge. Thanks to secure content delivery (*CloudFront* provides AntiDDOS, WAF, secure API gateways and Geo-load-balancing features, while *Route 53* provide DNS protection) it is possible to

protect workloads. The document suggests to implement strong identity foundation and traceability of the events that happen at the edge, like configuration change, resource access, possible malicious activities with *GuardDuty*. Automation plays a relevant role too in edge computing, allowing to automate security operations.

- **AWS Security Reference Architecture (AWS SRA) [16]**: This Guide provides detailed suggestions to design security foundations of AWS environment. The main takeaways are about:
 - *AWS organization*: It suggest to use the “separation of duties“ principle as driver a for workloads segregation.
 - *Defense-in-depth*: It is a relevant principle for selecting security controls, because it suggests to have independent security controls to protect from the same risk, so that in case of failure of one of them the others can still guarantee protection.
 - *Ecosystem*: Security building blocks should be considered not only for their stand-alone protection features (authentication, encryption, monitoring, permission policy), but also as they fit in the whole architecture with a holistic point of view.
 - *Guardrails*: The definition of a set of shared guardrails for distributed workloads helps protecting from misuse and reduces the impact of security events. *AWS Security Hub* and *GuardDuty* play a relevant role in threat and anomalies detection. *AWS Config* and *IAM Access Analyzer* help to identify configuration changes and monitoring resource access. *AWS CloudTrail* and *Amazon Macie* allow to log service API activity and to perform data classification.
 - *Temporary authorizations*: The usage of delegated administration features when third parties support is required, provides flexibility and access limits without unnecessary permission request overhead.
 - *Monitoring*: Centralized monitoring is a fundamental feature for AWS environment and can be adopted even with workloads in different region and/or for multi-account organizations. *AWS Control Tower* includes a set of pre-built security controls for multi-account AWS environment.
 - *Infrastructure as Code*: AWS SRA code examples make possible to define Security Reference Architecture by IaC (Infrastructure As Code). With this approach infrastructure is treated as application and is subject to software development life-cycle phases like automatic testing before deployment. IaC provides consistency and repeatability and the ”code“ can be forced to be within the architectural directives through specific guardrails, for example about the usage of a specific cloud region.
- **AWS Well-Architected Framework Security Pillar [20]**: It provides guidance on how to design, deliver and maintain secure workloads on AWS. The paper includes:
 - *Security foundation*: It provides AWS context about design and shared responsibility principles, definitions, account management and separation (collection of AWS resources owned by a single organization) and secure operations on workloads.

- *Identity and Access Management*: It includes guidelines about identity management and permission management.
- *Detection*: It provides guideline about service and application logging, log analysis, automatic response to events and actionable security events (process in the form of runbook or playbook).
- *Infrastructure Protection*: It provides guidelines about how to protect networks and compute resources.
- *Data Protection*: This includes information about data classification, data protection at rest and data protection in transit.
- *Incident response*: It provides guidelines to properly design an incident response process by including: goals definition, training, preparation, simulation and iteration (automation of containment capabilities).
- *Application Security*: This section offers a set of references about Application Security Training, Test Automation, Penetration Testing, code review, software dependencies management, software deployment, SecDevOps pipeline assessment and give development teams responsibility for security.

Each paragraph includes references to further documentation that expands on the subject matter. Amazon provides over 300 security tools to protect AWS Cloud workloads. These solutions are organized in different areas as shown at the URL [14].

2.3.1 Identity and Access Management

AWS offers services and features to perform Identity Management, Access Control and Identity Governance for employees, partners and customers. The most relevant solutions are:

- **AWS IAM**: It allows to manage work-forces and customers identity. Thanks to granular information provided by AWS IAM it is possible to define rules to decide when allow or deny access to specific resources.
- **AWS SSO**: It centralizes management of identity from multiple AWS Accounts, it allows to use any identity provider and makes easier the access to multiple applications through the same user credentials.
- **AWS Directory Services**: Fully managed Microsoft Active Directory, this service allows to integrate AWS EC2 (Elastic Compute Cloud) and Amazon RDS (Relational Database Service) with Active Directory in order to support windows workloads.
- **Amazon Cognito**: Customer Identity Management tool, that helps to secure user sign-up and access control to Web and mobile applications.
- **Amazon Verified Permission**: It allows to decouple business logic from authorizations in customers applications, defining fine-grained authorizations. Permission rules can be defined in *cedar*.
- **AWS Control Tower**: It allows to control multi-accounts in AWS environment orchestrating security operations according with organization security and compliance needs.

2.3.2 Detection & Response

Amazon provides a set of services that work together with the aim to enhance security posture and simplify security operations: this setting prioritizes the management of security risks and automatically orchestrates the response to the threats.

The main goals of the following list of services are to protect workloads against security risk, centralize monitoring, provide visibility of potential risks, allow investigation, protection and response in case of incident and defend on-premises with the same approach.

- **Amazon GuardDuty:** It provides a threat detection service able to deliver detailed security findings for visibility and remediation.
- **AWS Security Hub:** This is a CSPM (Cloud Security Posture Management) service that verifies compliance of configurations with best practices, it groups issues and eventually enables auto-remediation.
- **Amazon Inspector:** This is an automated vulnerability management service that continuously looks for software vulnerabilities in AWS workloads.
- **Amazon Security Lake:** It allows to centralize security data into a purpose-built data lake. This helps to get a more complete understanding of security data: the solution adopts the Open Cybersecurity Schema Framework [39], an open standard with the aim to normalize and combine security data from a broad range of enterprise security data sources.
- **Amazon Macie:** Data discovery tool based on Machine Learning able to identify sensitive data and protect them. This solution has the capability to scale according with the growing amount of data.
- **Amazon Detective:** It is a service that simplifies security data analysis by pre-built data aggregations that help to identify the root cause of potential security issues.

2.3.3 Network and application protection

These services enforce fine-grained security policies at any network checkpoint and inspect and filter traffic to prevent unauthorized access to resources. All the services of this area are scalable, centrally managed and provide in-line protection and visibility for a large number of security risks about network traffic. The most relevant services are:

- **Amazon VPC Security Groups:** It is a service that controls the traffic allowed to reach and leave a specific resource.
- **AWS Firewall Manager:** It allows to configure and manage firewall rules centrally.
- **AWS Network Firewall:** It allows to define firewall rules the communications between VPCs (Virtual Private Cloud). Rules can be defined in AWS Firewall Manager.
- **AWS Shield:** It protects internet-facing applications by DDOS.
- **AWS WAF:** It protects Web Application from the most common attacks (e.g. OWASP TOP 10).

- **Amazon Route 53:** It allows to block DNS queries made for known malicious domains.

2.3.4 Data Protection

This set of services help to protect data introducing: controls on privacy, how data are used and encrypted and who has the access to the data. The most relevant services are:

- **AWS Identity and Access Management (IAM):** It allows to securely manage access to AWS services and resources.
- **AWS CloudTrail:** It allows to trace user and API activities.
- **Amazon Macie:** It provides Data Discovery, Classification and protection.
- **AWS CloudHSM:** It is a cloud managed service, for a single-tenant provides Hardware Security Module.
- **AWS Key Management Service (KMS):** It lets the opportunity for the customer to create and manage the cryptographic key used to encrypt data hosted by AWS services.
- **AWS Control Tower:** It helps to govern a multi-account AWS environment.

2.3.5 Compliance

The following services help the automation of compliance and audit processes:

- **AWS Config:** It allows to perform assessment and audit on resource configurations.
- **AWS CloudTrail:** It allows to Trace user and API activities.
- **AWS Audit Manager:** It performs continuous audit on AWS usage to simplify risk and compliance assessment.
- **AWS Artifact:** It provides on-demand reports about AWS and AWS partners. It is a useful service for specific compliance purposes.

2.4 Open-source

The services offered by the main CSPs (Cloud Service Providers) are almost complete overlapped. Even if the major CSPs collaborate with various opensource projects, not all commercially available services are also easily obtainable or available with the same quality as open source.

This chapter will show the main opensource projects that cover the most relevant services necessary to support the needs of modern data centers: particular attention will be paid on security solutions in order to provide reasonable coverage against the main security risks.

The next paragraphs will illustrate the essential building blocks to create a private cloud based on Open-source solutions and will try to identify functionalities not available.

2.4.1 Basic Functionality

Certain basic features are taken for granted when using cloud services, this paragraph will focus on core services expected by whom rely on the cloud for ICT service delivery.

- Manage, via a control plane, the provisioning of *Virtual Machines*, *containers* and *storage*.
- Elastically *scale computational power* as certain parameters change (e.g. number of requests received).
- Define *custom network topology* according with the organization needs.
- *Automate IT operations*.
- *Manage identity and authorizations* at different levels: control plan, data plan and user plan.
- *Log* all the activities performed at control plan and data plan levels.
- *Deploy applications* through pre-defined pipeline with automatic controls.
- Define *infrastructure as Code*.
- Allows Control Plan *API* integration.
- Automate *Cost controlling*.

Almost all the above functionalities can be achieved by mixing OpenStack and Kubernetes functionalities, for instance with Nova, Neutron and Cinder is possible to deploy virtual machines, networking and storage necessary to a Kubernetes cluster. On the other hand OpenStack Magnum [106] can also deploy containers instead of virtual machines.

2.4.2 Advanced Functionality

The effort required to properly setup an OpenStack/Kubernetes environment is not negligible, more over to complete with any essential features for a modern Private Datacenter it will be necessary to identify other Open-source solutions that can work together as an ecosystem.

In table 2.2 there are suggestions about Open-source security tools: not all of them are still supported by the opensource community while others are smokescreen to cover commercial services.

The in-depth study of an opensource ecosystem that would enable the delivery of the services needed by a modern data center, supported in addition by advanced cybersecurity services, would require a very significant effort and a careful experimental phase that is beyond the scope of this thesis.

Class Name	Open-source solution	Features
Identity & Access Management	Keycloak[74]	SSO Social Login MFA OpenID Connect, OAuth 2.0 and SAML Fine-grained authorization services
PKI	OpenSSL[105] CertBot[23][77]	x.509 certificate ACME Client
Infrastructure as Code	Terraform[127]	Infrastructure Provisioning IaC (Infrastructure As Code)
Automation	Ansible[13]	Event Driven Automation Configuration Management System Inventory
CI/CD	Jenkins[72]	Build Automation Test Automation Deploy Automation
Logging	Elastic Search & Kibana [31]	Data store Distributed search engine
SIEM	Elastic SIEM[32]	SIEM
HIDS	OSSEC [107]	Host IDS Active Response File Integrity Monitoring System Inventory
Sandbox	Cuckoo Sandbox[27]	Automated malware analysis
SOAR	Cortex XSOAR[30]	Case management Automation Threat intelligence
Threat Intelligence	MISP[115] Open Threat Exchange[3]	IoC
CSPM	OpenScap[104] Trivy[2]	Compliance Assessment
WAF/WAAP	Kong[75] NGINX[101]	API Security WAF
DNS Filtering	Clean Browsing[24]	DNS Security DNS Filtering
SecDevOps	GitHub[65] Sonar Qube[118] Owasp Zap[73] Owasp Dependency-Check[109]	SDLC SAST DAST SCA
Data protection	Fogger[64] Mydiamo[98]	Data Masking Transparent Data Encryption

Table 2.2. Open-source Security Solutions

2.4.3 Frameworks

The open-source community is very active in developing open frameworks for information exchange, examples of these are:

- **OCSF (Open Cyber-Security Framework)** [39]: It provides a vendor agnostic standard schema good to be used for common security events and includes a self-governance process for security log producers and consumers.
- **STIX (Structured Threat Information Expression)** [123]: While OCFS is focused on events representing the activities on computer system, this is a complementary framework focused on threat intelligence, campaign and actors.

- **OSSEM (Open Source Security Events Metadata)** [108]: It defines and shares a common data model in order to improve data standardization and transformation of security event logs.
- **OpenC2 (Open Command and Control)** [103]: It is a standard language for command and control technologies to support cyber defenses activities.

Simplify data ingestion and normalization helps creating a common language for threat detection and investigation, moreover it can be useful for future open-source cybersecurity solutions and for facilitating the migration from a cybersecurity solution to another.

2.4.4 Open Source Solutions

The list of tools given in table 2.2 has to intended as an overview about the large amount of open-source solutions available and their high level of specialization. These solutions are often used by manufacturers as a way to attract customers to paid services based on the same platforms, but with more advanced or unrestricted features. However, open-source solutions are optimal for costs reduction and lock-in risk reduction.

The professional use of open-source solutions often requires high skills. Enterprises may need to modify the open-source code to fix problems or to introduce new required functionalities by themselves: for these reasons, the adoption of open-source solutions is particularly suitable for big organizations or those with high growth rates, which can dedicate extremely specialized teams to open-source platforms management and eventually developments. There are examples of large companies that adopt this approach extensively (e.g. Netflix, Spotify and Pega System) and at the same time rely on cloud Service Providers for IT services. They choose to stay stuck to open-source, because it enables easy migration from one cloud service provider to another and this is an important leverage for commercial negotiations.

Leading Cloud Service Providers are also increasingly relying on open-source solutions, considering them more secure and flexible and deciding to participate in strategic open-source projects. Furthermore, it must be considered that, as reported by Synopsys [124], 96% per cent of the “commercial applications“ contain open-source. This means that open-source is a much more permeating reality than one might think.

2.5 Cloud Service Provider comparison

AWS, GCP and Azure offer a wide range of security capabilities both directly and through their partners. Although the offerings of all three providers are comprehensive, there are some differences in the approach mainly for their different backgrounds.

Microsoft’s cybersecurity strength consists in the large usage of automation and in the “natural ecosystem“ due to the worldwide extensive use of Windows in both clients and servers, as well as the most widely adopted office automation tool (Office 365).

Google's cybersecurity strength is about the adoption of the most modern cybersecurity architecture (e.g. CSMA) and usage of opensource solutions to provide cybersecurity services. Moreover Google services and products (Gmail, Chrome, Android and others) help Google to collect information about emerging threats.

Amazon leverages its long history as a Cloud Service Provider, which has enabled it to gain a leadership position and a large customer-base, to create a network of security service providers.

AWS appears to be the most "open-source friendly" CSP, with the most collaborative approach with third parties; instead Azure appears as if it wants to be the only cybersecurity provider, while GCP stays in the middle.

In conclusion there are also some small differences between cybersecurity services of CSPs (Cloud Service Providers): Microsoft does not provide VAPT tools, Google provides its own VAPT tools and AWS only supports third parties. More over, sometimes there are cybersecurity services less promoted by a CSP than others, for example Google puts great emphasis into TEE (Trusted Execution Environment), while Microsoft and AWS do not mention it within the most relevant cybersecurity features, but can provide it too.

Chapter 3

Threat Detection and Response

Threat detection and response is the main goal of a Security Operation Center: to achieve it, SOC's collect a large amount of security log events from different sources and they continuously search for traces of possible incidents by assembling pieces of information.

The alerts thus generated are investigated by security analysts, that study in detail the sequence of events to confirm or deny the existence of malicious activity. Security operators need to collect evidences from the logs or directly from the systems involved, more over they often need to perform containment activities to block in the early stages the attempted breach to the system.

These operations are performed through SIEM, XDR and SOAR platforms with threat intelligence feeds. This chapter will analyze the built-in tools provided by the main Cloud Service Providers, focusing on *Security Investigation Languages*, *event correlation* and *automatic response*.

3.1 Security Investigation Languages

Security Investigation Languages are powerful tools that allow security analysts to better understand security events by navigating within data models where they are collected.

Each cloud provider operates with a different *data model*. Data Models are complex and articulated representations of data that can be also enriched with external sources (e.g., threat intelligence). Specific query languages have been developed to make easier the investigations: they allow to aggregate, filter and correlate security events. Next sections will explore these Security Investigation Languages.

CSP	Data Model	Investigation languages	Automatic Response
Azure	OSSEM	KQL	Sentinel SOAR
GCP	UDM	SCCQL & YARA-L	Chronicle SOAR
AWS	OCSF	SQL	Event Bridge

Table 3.1. Security Investigation languages

3.1.1 Azure KQL

As reported in Microsoft website [85], the name of KQL was chosen in honour of Jacques-Yves Cousteau, a French explorer who pioneered underwater exploration: as Cousteau was known for his use of innovative technology to explore oceans, so similarly KQL was designed as a powerful and flexible data exploration language.

Kusto Query Language is similar to SQL language and organizes entities hierarchy in the same way through databases, tables and columns, so it is possible to deep dive inside security data in order to: *discover pattern, identify anomalies and outliers and produce statistics*.

Despite other cloud service providers, Microsoft has decided to use Kusto as the common Security Investigation Language for all its own data platforms (Azure Data Explorer, Azure Monitor Log Analytics, Azure Sentinel).

For the purposes of this thesis the usage in Azure Sentinel (Microsoft SIEM/SOAR platform) and Defender for Cloud (xDR/CSPM platform) will be analyzed: both tools rely on Azure Monitor Log Analytics as data platform.

KQL in Sentinel

Microsoft Sentinel works on-top of Azure Monitor service and stores data through Log Analytics workspace. Data ingestion may also take place through external sources (e.g. threat intelligence or third parties security tools), for this reason Sentinel provides *data connectors* to ingest data into predefined or custom tables. Users can define custom data connectors or use out-of-the-box connectors: data can also be generated by Sentinel itself as a consequence of the automatic analysis performed, for example by indicating an alert.

Traces or Information

Before starting talking about KQL, it is important having a look at the entities and terminologies used in Microsoft Sentinel and Defender for cloud.

Security queries often relate to TI (Traces or Information), pieces of information that can be used to detect, identify and respond to threats. There are three different types of trace information:

- IOC (Index Of Compromise): It indicates that a system has been compromised by an attack, it includes IP addresses, domains, file hashes or keywords.

- IOB (Index of Behaviour): It indicates anomalous or suspicious behaviour, like increased network traffic, the execution of unauthorized processes or access to sensitive files or directories.
- IDO (Indicators of Detection): It indicates the presence of malware or other malicious code, like malware signatures, file hashes or file names.

KQL statements

KQL provides read-only commands, extracts data and returns results. Queries are composed by statements with the following characteristics:

- They are written in plain text.
- They are separated by (semicolon) “;”.
- The Tabular Query format means that both query and results are organized in table.
- Each Tabular statement contains zero or more operators.
- Each operator starts with (pipe) “|”.
- Data flow passes sequentially through each operator (filtering, selecting, summarizing, etc).

Management commands

Management commands are requests to Kusto to process or modify data or metadata: they are not included in KQL and always start with (dot) “.” character. Management commands can also be used to show metadata not available through query results. (e.g., “.show tables”, shows the list of tables available in a schema).

3.1.2 GCP YARA-L

Unlike Microsoft Sentinel, Google Chronicle correlation rules are not written with a query language but they are written in YARA-L, a serialization Language like YAML¹. As reported in Google documentation [50], the rules are composed by different parts:

- *meta*: Meta data referring to author, description, version, creation date.
- *events*: Conditions to filter events and how to correlate them.
- *match*: Value to return.
- *outcome*: additional information extracted by detection rule.

¹YAML Ain’t Markup Language - Human-readable data serialization language often used for configuration files

- *function*: Functions to be used in rule logic.
- *condition*: Rule logic.
- *options*: Conditions to check and variables used to find the matches.

Below a Google Chronicle sample taken by Google Chronicle white paper [63]:

```
profile susp_process_with_variation_of_svchost {
  meta:
    author = "Chronicle Security"
    description = "Rule to detect variations on svchost"
    version = "0.01"
    created = "2019-12-16"
  function:
    func CheckSvchostVariations()
      if (
        re.regex(strings.lower(udm.process.command_line),
          ".*(svch0st|svh0st|svhost|svchst|svchot|svchostexe)\.exe.*") or
        re.regex(strings.lower(udm.process.path),
          ".*(svch0st|svh0st|svhost|svchst|svchot|svchostexe)\.exe.*")
      ) then
        return true
      end
      return false
    end
  condition:
    if ( CheckSvchostVariations() )
      then
        outcome.match()
      end
    }
}
```

This rule triggers when a modified version `svchosts.exe` is executed by command line or process. The regular expression identifies any similar `svchost` names, like `svch0st`, that can be hard to be identified by a human being. *Chronicle Detection Engine* uses YARA-L syntax for the rule to detect threats: the syntax is designed to be easy to read and to be understood even from non-experts.

```
rule DifferentCityLogin {
  meta:
  events:
    $udm.metadata.event_type = "USER_LOGIN"
    $udm.principal.user.userid = $user
    $udm.principal.location.city = $city
  match :
    $user over 5m
  condition:
    $udm and #city > 1
}
```

The rule above, got from Google documentation [59], does not provide any metadata and filters all the events that have as metadata event type “USER_LOGIN“, looking for users that have logged-in from two different cities in less than 5 minutes. All the fields of this rule refer to Unified Data Model, so login events are detected even if log entries are generated by different tools and services that do not share the same log format. For more details YARA-L 2.0 documentation is available [59].

3.1.3 AWS SQL

Amazon *Detective* allows to navigate the findings identified by *GuardDuty* by watching the data and showing their visualization. In some situations it may be useful to direct query security findings, for this reason, as reported in Amazon documentation [11], it is possible to export *GuardDuty* findings into external storages like *S3*, to permit the analysis through *Amazon Athena*, *Amazon CloudWatch Logs* or *Amazon EventBridge*.

Amazon Athena

Amazon Athena supports DDL² and DML³ statements. As in the example below, the query returns information about Amazon EC2 instances that might be affected by DNS exfiltration queries.

²DDL - Data Definition Language allows to create, modify and delete database objects

³DML - Data Model Language allows to insert, update and delete data in database tables

```
SELECT title, severity, type, id AS FindingID, accountid, region, createdat, updatedat,  
json_extract_scalar(service, '$.count') AS Count,  
json_extract_scalar(resource, '$.instancedetails.instanceid') AS InstanceID,  
json_extract_scalar(service, '$.action.actiontype') AS DNS_ActionType,  
json_extract_scalar(service, '$.action.dnsrequestaction.domain') AS DomainName,  
json_extract_scalar(service, '$.action.dnsrequestaction.protocol') AS protocol,  
json_extract_scalar(service, '$.action.dnsrequestaction.blocked') AS blocked  
FROM gd_logs  
WHERE type = 'Trojan:EC2/DNSDataExfiltration'  
ORDER BY severity DESC
```

Amazon CloudLogs

As reported in Amazon documentation [8], if GuardDuty findings are exported on S3 storage, they can also be analyzed by a query language that supports different functions and operations like arithmetic, comparison operations and regular expressions that make easier to identify trends or patterns.

The main commands of CloudLogs query language are:

- **Display:** Displays a specific field.
- **Fields:** Displays specific fields in query results.
- **Filter:** Filters events that match one or more conditions.
- **Pattern:** Automatically clusters data into patterns.
- **Parse:** Extracts data from a log field that can be processed in the query.
- **Sort:** Displays in ascending (asc) or descending (desc) order.
- **Stats:** Calculates aggregate statistics using values in the log fields.
- **Limit:** Defines a maximum number of log events to return.
- **Dedup:** Removes duplicates of specified fields.
- **Unmask:** Displays all the content of data protected by data protection policies.

Amazon CloudLogs supports also comparison, arithmetic, date-time, numeric, string, IP address and general functions and operations.

Amazon EventBridge

Amazon EventBridge is a general purpose integration service (not just dedicated for cybersecurity scopes) that provides a server-less event bus useful to build event-driven applications. Applications can be loosely coupled and actions can be taken when an event changes the state of an application.

The usage of EventBridge in cybersecurity can span a variety of areas, in the next few

paragraphs will be explored its use as a tool to manage the automatic response to security events. Amazon EventBridge provides also a feature to query contents of the logs with a standard SQL language, so it can be used as Athena to investigate findings.

3.2 Event Correlation

Event correlation is a critical part of Threat Detection, because it helps reducing noise and focuses on what matters, filters out false positives or irrelevant events and identifies root causes.

To support event correlation, instead of adapting data sources, SIEM are using meta-data-models like OSSEM⁴ adopted by Azure, UDM⁵ adopted by GCP or OCSF⁶ adopted by AWS, where the fields of the log source are mapped into the “standard“ data model.

This approach allows to use the same correlation rule also in case of change of the security solutions.

3.2.1 Azure Sentinel & Defender for Cloud

Sentinel correlation rules are written in KQL and they run over a security data model named ASIM (Advanced Security Information Model).

Advanced Security Information Model

ASIM allows data sources to be normalized using a common schema (see Fig. 3.1), which permits to correlate sources from cloud and on-premise services, support automatic correlation and correlate data from user-defined log sources.

ASIM adopts *OSSEM* as data model [89], so it can normalize data and enable queries between different sources. Data is not required to be modified through the use of *ASIM parsers*, so in this way source format is preserved: source codes of the built-in ASIM parsers are available on GitHub [80] and they can be used to generate custom parsers. To improve performances, parsers can also filter data at source (e.g. by defining start-time and end-time), and once normalized the data are available in pre-defined tables.

Detection out-of-the-box

Microsoft provides pre-build queries [88] to identify threats from the log sources generated by third parties like: Microsoft 365, Amazon Web Services, Microsoft Windows DNS, Azure Firewall, Windows Forwarded Events, ZScaler Internet Access, Palo Alto Networks, Fortinet FortiGate and Check Point.

⁴OSSEM - Open Source Security Events Metadata

⁵UDM - Unified Data Model

⁶OCSF - Open CyberSecurity Framework

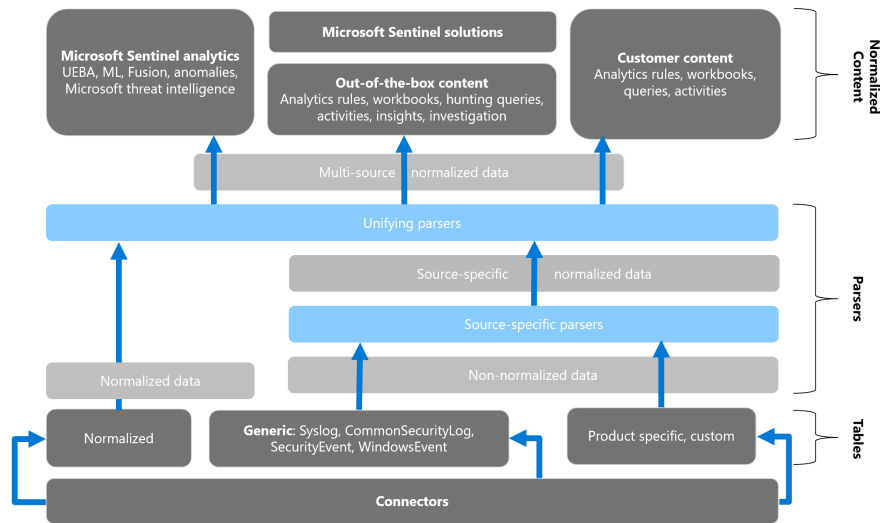


Figure 3.1. Microsoft - ASIM Architecture [89]

As reported in Microsoft documentation [82], Sentinel provides a set of analytic rules templates (see Tab. 3.2) that has been designed accordingly with known threats, common attack vectors and suspicious activity escalation chains.

Analytic Rule Type	Description
Microsoft Security	Sentinel automatically generates an incident when an alert is generated by a Microsoft security solution.
Fusion	Fusion correlation engine used Machine Learning algorithm to detect advanced multistage attacks. Fusion cannot be customized and is enabled by default.
Machine Learning (ML) behavioural analytics	This template uses Machine learning to detect anomalous behaviour, it cannot be customized and it can be activated just one time.
Threat Intelligence	It matches threat indicators provided by Microsoft Threat Intelligence in different kinds of logs. Not customizable enabled by default.
Anomaly	Thanks to Machine Learning, it can detect specific types of anomalous behaviour. Each rule has its own unique parameters and thresholds, but cannot be customized because is included in the out-of-the-box set. Users can duplicate and customize new rules.
Scheduled	Queries written by Microsoft security experts. Query logic is visible and can be modified if necessary. This rules can be scheduled after minutes, hours, or days.
NRT	Near-real-time rules are limited and are executed every minute, to provide information as soon as possible

Table 3.2. Microsoft Sentinel Out of The Box Analytics Rules

Custom Threat Detection

Creating customized analytical rules is useful for identifying potentially dangerous events and anomalies. The analytic rules generate alerts when the defined condition is reached (e.g., when a user overcomes the number of failed authentications). The generation of an

alert activates the SOC triage process, which will analyze and classify the event and if necessary, will implement the necessary containment, recovery and eradication actions.

Sentinel allows to schedule the execution of custom analytics periodically: custom queries should always refer to ASIM tables to make queries agnostic by the current and future solution. Sentinel can recognize and classify data it receives by associating predefined *entities*: the information displayed are enriched with information not directly related to the outcome of the query (i.e., user accounts, hosts, files, processes, IP addresses and URLs)

As shown in Fig. 3.2, Sentinel Content hub includes several “applications“ written by

The screenshot shows the Microsoft Sentinel Content Hub interface. At the top, there are statistics: 312 Solutions, 270 Standalone contents, 0 Installed, and 0 Updates. Below this is a search bar and a table of solutions. The table has columns for Content title, Content source, Provider, Support, Category, and Status. Several solutions are marked as 'FEATURED'.

Content title	Content source	Provider	Support	Category	Status
Amazon Web Services	Solution	Amazon Web Servi	Microsoft	Security - Cloud Security	FEATURED
Cisco Umbrella	Solution	Cisco	Microsoft	Security - Automation (SOAR), Security - Clou	FEATURED
Google Cloud Platform IAM	Solution	Google	Microsoft	Cloud Provider, Identity	FEATURED
SOC Handbook	Solution	Community	Community	Security - Others	FEATURED
VirusTotal	Solution	VirusTotal	Microsoft	Security - Automation (SOAR)	FEATURED
42Crunch Microsoft Sentinel Connector	Solution	42Crunch	Microsoft	Security - Threat Protection	
Abnormal Security Events	Solution	AbnormalSecurity	Abnormal Security	Security - Threat Protection	
AgileSec Analytics Connector	Solution	InfoSecGlobal	InfoSecGlobal	IT Operations	
AI Analyst Darktrace	Solution	Darktrace	Darktrace	Security - Threat Protection	
AIShield - AI Security Monitoring	Solution	AIShield	AIShield	Security - Threat Protection	
Akamai Security	Solution	Akamai	Microsoft	Security - Cloud Security	

Figure 3.2. Microsoft Sentinel - Content Hub Solutions

Microsoft and third parties to integrate Sentinel with other security solutions or standalone.

3.2.2 GCP Chronicle & Security Command Center

The schema in Fig. 3.3 shows how the different components of Google Threat Detection and Response are integrated with each other: *Security Command Center* is the tool used to handle Google security configuration and relies on *Chronicle* for log event correlation and on *Simplify* to perform automatic response to cyber threats. For notifications, a publisher/subscriber approach provides flexibility and scalability.

Detection logic and threat intelligence used by Security Command Center are proprietary and they are based on profiling, Machine Learning and anomaly detection. On the

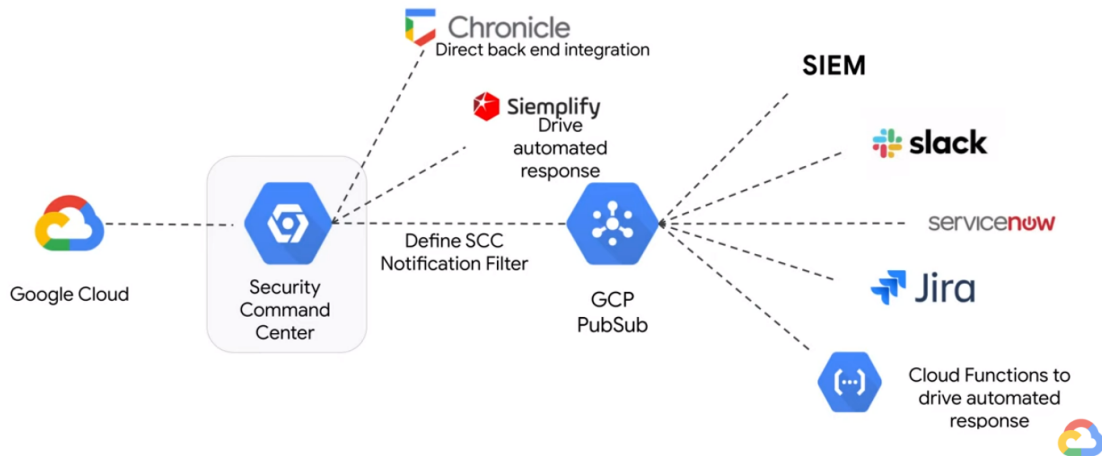


Figure 3.3. Google Security Command Center - Landscape [57]

other hand investigation can be done using Chronicle, a Google Cloud service that allows to pivot through related entities in a unified timeline.

Event Threat Detection

Event Threat Detection (the engine that identifies threats) includes a set of out-of-the-box rules to identify well known threats (e.g. Log4j RCE). Customers can define their own correlation rules to identify threats starting from templates: in case these templates do not fit the customer needs, it is possible to run unique or recurring standard SQL queries on the data exported in BigQuery, as explained in Google documentation [62].

Security findings are written in JSON in order to be easily exported and displayed in Security Command Center. Samples of findings [61] and more details about how *Event Threat Detection* identifies threats and operates with the other security solutions are available in Google Documentation [58].

Custom module for *Event Threat Detection* [49] can be defined through Google Cloud console. A custom module template can also be modified and sent to Security Command Center by Google Cloud CLI: this module only allows to modify parameters like “IP Address“, severity and custom remediation steps, but still relies on Event Threat Detection engine based on Machine learning and Threat intelligence to detect anomalies.

As reported in the Chronicle white paper [63], the correlation engine used by Security Command Center to identify threats adopts two different types of data organization:

- *UDM*: It allows rules and algorithms to operate on logs with a common data model, making reliable log correlations and so threat detection
- *Automatically-enriched data*: Log entries are enriched intelligently according with the

needs of SIEM correlation (Smart matching).

Chronicle detection engine based on machine learning and artificial intelligence supports both the analysis of specific IOCs (like file hash, URL, IP address) and TTPs (activity sequence or process execution patterns).

Chronicle also supports a language designed for threat detection named *YARA-L*. YARA is an open-source language developed by VirusTotal to detect malware inside files. In YARA-L the “L” stands for *log*, so it has to be intended as a language that allows to identify malicious activities inside the logs.

One of the main features of this language is that it permits to write queries easy to read and this is especially useful for collaborative detection between different vendors. YARA-L can be used in Chronicle for both real time detection and historical detection in an interactive way or scheduled: detections are mapped on *MITRE ATT&CK* and *Sigma open-source frameworks* [117].

Detection systems like XDR are able to collect telemetry and to identify alerts autonomously, anyway they are often not able to identify all the threats. For this reason SIEM detection rules are also useful to deeply identify threats in the case that XDR platform fails.

Security Command Center

Security Command Center collects log information by a set of built-in services and third parties extensions: all these events are monitored by *Event Threat Engine* and generate findings available in Security Command Center Findings. Findings use JSON as data format and they often include details about what was detected, attack exposure, affected resources, security marks (annotations), next steps, related links and detection services. Security Command Center allows to query findings using the dashboard or directly editing the query in the query editor, moreover it is possible to execute the query also by CLI (Command Line Interface) as shown in the example below from Google documentation [54].

```
gcloud scc findings list example-organization.com \
  --source=123456789012345678 \
  --filter="contains(connections, inIpRange(source_ip, "2001:db8::/32")) \
  AND NOT contains(connections, inIpRange(source_ip, "192.0.2.0/24"))"
```

The above command, filters the source IP address in a range and not in another.

Another option is to use *Query builder* function on Security Command Center: this will work only as if it is a *where condition* of the SQL statement. Tables selection is performed in the previous steps in Security Command Center console and these are related to findings.

```
state="ACTIVE"
AND NOT mute="MUTED"
AND containsOnly(iam_bindings,member="group:example@example.com")
```

The above query selects, within all the *findings*, the active users that are “not-muted” and that belong to the group “example”.

3.2.3 AWS GuardDuty & Detective

As reported in Amazon documentation [9], GuardDuty is a security monitoring service that collects logs called *foundational data source* and uses threat intelligence feeds and machine learning to identify malicious activities. GuardDuty produce *security findings* that can be investigated by a security analyst through Guardduty console or *Amazon EventBridge*.

Foundational data sources arise from different sources:

- **AWS CloudTrail event logs:** It traces the history of AWS API calls done through AWS Management Console, AWS Command Line Interface and AWS SDKs and APIs. This helps to identify which users are involved, from which IP addresses and at which time in order to ensure Governance, Compliance and Risk auditing.

In AWS CloudTrail, events are stored in ORC ⁷ storage format to make the read time and information retrieval faster when filters are applied. Log Insights events help to identify anomalous behaviours in CloudTrail logs, by checking volumes and error rates.

- **AWS CloudTrail management events:** Control plane events include for example the configuration of: security authorization, rules for routing data or logging set up. They are a key information to ensure proper monitoring and compliance with regulations and security best practices.
- **VPC Flow Logs:** It captures information about the IP traffic going to and from network interfaces, for example to Amazon EC2 (Elastic Compute Cloud). It can be also related to Lambda function and EKS (Elastic Kubernetes Services).
- **DNS logs:** Allows GuardDuty to access and process DNS requests and response logs. This is useful to identify anomalous activities inside the assets of an AWS account. AWS provides also a DNS protection service called “Route 53 Resolver“ that blocks DNS requests related to malicious DNS domains or IP addresses.

In addition to foundational data source, GuardDuty can ingest also log trails from other Amazon and third parties security solutions.

The main GuardDuty features that can be activated are:

- **EKS Protection:** It provides threat detection coverage, log monitoring and run-time monitoring. It helps to identify suspicious activities in EKS clusters by capturing chronological activities from users and applications. Moreover it helps to identify threats monitoring operating system-level events in EKS nodes and containers.
- **Lambda Protection:** It identifies threats when a lambda function is invoked, monitors lambda network activity logs (VPC Flow logs) including logs generated when Lambda function is invoked.

⁷ORC - Optimized Row Columnar: high-performance storage format

- **Malware Protection:** It detects potential malware by continuously scanning EBS (Elastic Block Store) volumes that are attached to the EC2 (Elastic Compute Cloud) instances and container workloads. When a potential malware is discovered a snapshot of the storage is maintained in GuardDuty as a finding.
- **RDS Protection:** It analyzes and profiles RDS login to *Aurora MySQL* and *Aurora PostgreSQL* databases in order to identify potential access threats. A learning period is required to set the baseline normal behaviour: when unusual pattern or incomplete login attempts happen, GuardDuty generates a finding.
- **S3 Protection:** It monitors AWS CloudTrail data events for Amazon S3 (Simple Storage Service) to identify potential security risks for data within an *Amazon S3 buckets*. When suspicious access to data is detected, a finding is generated.

GuardDuty findings

As reported in Amazon documentation [10], GuardDuty findings represent a potential security issue related to unexpected and potentially malicious activity. To view and manage findings it is possible to use *GuardDuty Console*, *AWS API* and *AWS CLI*. Each finding has a level of severity associated from 1.0 to 8.9. High values are associated to high security risks. The values under 1 and over 8.9 are reserved for future use. Findings are updated when GuardDuty detects more events related to the same security issue, but according with the finding type, it is also possible that the aggregation criteria requires the creation of new findings under certain circumstances.

Amazon GuardDuty findings use JSON data format and include several information according with the data source from which has been generated. The most common information included are: Account ID, count (number of repetition), creation time, finding ID, finding type, region, resource id, severity and last update. The resource indicated in a finding can play two different roles: *TARGET* or *ACTOR*. This is specified in the resource role field, while resource type specifies the type of affected resource (it can be more than one).

Amazon Detective

Amazon Detective is the best option to investigate findings. As reported in Amazon documentation [4], it helps to analyze and quickly identify the root cause of security findings or suspicious activities by creating a visualization of GuardDuty findings. Amazon Detective uses findings of GuardDuty and through machine learning, statistical analysis, summaries, graph theories, pre-built data aggregations provides access to entities in a way that helps investigation (see Fig. 3.4). Tailored visualizations are also available to rapidly investigate suspicious activities, identify patterns and resources affected in an incident.

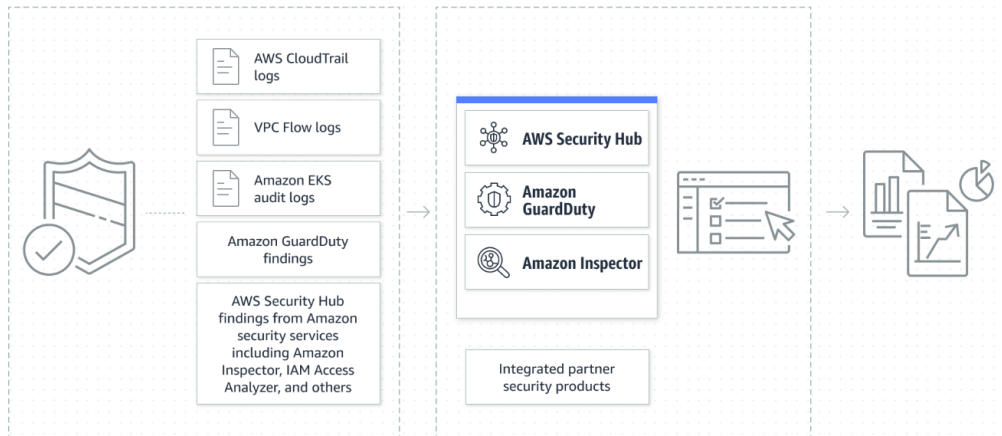


Figure 3.4. Amazon Detective - workflow [4]

Amazon Detective, allows to perform triage over security findings, investigates incidents and threat hunting. *Triage* has the goal to quickly understand if a security finding is something to be concerned for or not. Historical data *investigations* aim to understand how long threats have been ongoing and which assets have been affected. *Threat Hunting* refers to the set of activities that aim to make the threat inoperative.

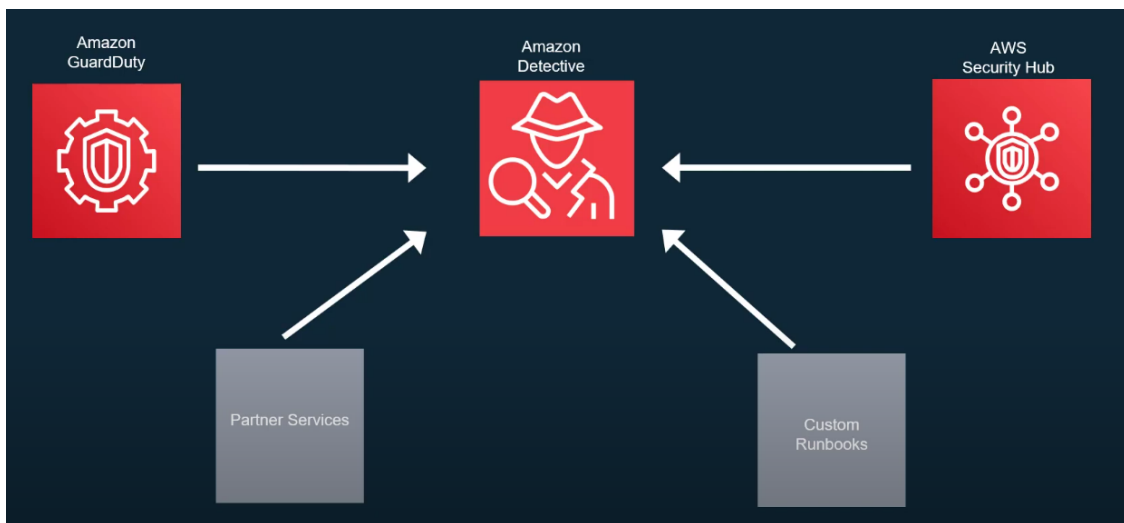


Figure 3.5. Amazon Detective - flow [4]

As shown in figure 3.5, Amazon Detective collects findings from Amazon GuardDuty, *AWS Security HUB* (Amazon Cloud Security Posture Management Service) and Security partner services, enabling deep analysis about security events in AWS environments. Amazon Detective also performs automatic investigation about ingested data, thanks to the rules designed by Amazon Security Engineers.

Security analysts can standardize and make investigation activities automatic through run-books, for example, they can block an url or IP address indicated in a finding.

3.3 Automatic Response

Automatic Response helps: to standardize SOC responses, to document phases of an incident, to reduce the workload on security teams, to improve incident response time and to reduce the impact of security incidents. The automation of security tasks is often performed by dedicated platforms known as SOAR (Security Orchestration Automation and Response).

3.3.1 Sentinel - Automation rules & playbooks

Automatic response in Sentinel can be triggered by a single event, an incident (group of one or multiple events) or an update of a previous incident. *Automation rules* allow to perform basic triage, assignment, workflow and closure of incidents, but for more complex automation a *playbook* can be invoked.

Standardization of Security Operations is one of the main concerns for a cybersecurity manager. SecOps analysts are expected to perform a list of steps or tasks during triage, investigation and remediation activities. Technicians shouldn't spend time thinking about what to do or be worried about missing some steps. Thanks to automation, it is possible to document, update procedures and standardize responses to an incident no matter who is performing it.

Sentinel provides *Automation rules* and *Playbooks* to perform automatic threat response: automation rules are predefined rules with simpler behaviours, that intend to automate responses through specific criteria. On the other hand, playbooks are more flexible and allow to define custom and complex steps to respond to security events.

Automation rules

Automatic rules should be used for static tasks that don't require interactivity. Tasks can be applied to all the rules or to a subset of the analytic ones (rules that identify a specific threat that requires specific tasks to be performed).

To define an Automation rule is necessary to define:

- **Scope:** It can be one of the following actions: Create tasks, noise suppression, change the status, tag the incident, escalate, close, call a playbook and so on.
- **Trigger:** It is the condition that activates the playbook, like: incident is created, incident is updated, alert is created. (Incident often require human action).
- **Conditions:** It selects the incident provider, the analytic rules and entities (e.g. IP address) for activating the automation. Multiple conditions can be combined with ADD or OR operator.

- **Action:** It can be one of the following actions: Assign owner, Change status, Change severity, Add tags and Run playbook. Multiple actions can be performed in a predefined sequence.

Playbooks

Playbooks should be used for advanced use cases, like conditional activities or tasks that require interaction with third-parties.

Most of the alerts that a SOC receives follow recurring patterns and can be resolved through pre-defined actions. The larger part of these activities can be automated, allowing analysts to be focused on investigation activities. Sentinel can run this tasks automatically when the analysts decide to launch one of them or when a specific condition triggers.

Through *Microsoft Sentinel Connector* it is possible to add tasks for executing automatically a list of tasks when an incident triggers. Other actions can also be defined through *Logic App Connector* (for example, send a notification email, update incident status, isolate a device or disable a user). Playbooks can be defined from scratch or can start from a playbook template. Playbook templates may arise from *Content Hub Solutions* or from Microsoft GitHub Sentinel repository [86]. Playbooks are *ARM templates* including *Azure Logic Apps* workflow and API connections, that can be used to create workflows and to automate and orchestrate tasks.

The interaction with others systems pass through the following connectors: *managed connectors* (wrapped API calls supported by Microsoft), *custom connectors* (communication with non-prebuilt connectors) and *Microsoft Sentinel connectors* (interaction with Sentinel itself). Logic App is a server-less workflow automation service that includes many actions and triggers to define almost any automation scenario. A logic APP can activate a playbook in three specific situations: the first one is when automation or analytic rule triggers, the second one is when a playbook is manually selected inside an incident or an alert and the last one is when it is called inside another playbook.

Playbooks can include an enrichment phase, they collect information from external services that regard entities involved (e.g. host DNS name can be verified in a third party threat intelligence service to collect more data). Playbooks can also comprehend organizational activities like opening a ticket in a ticketing tool, sending a message in teams to alert security analysts, changing the status of an incident.

When workflows interact with humans, we talk about *orchestration*. For example, Sentinel can send e-mails to subject matter experts giving all the details of the event and offering them the possibility to decide whether to block or not the operation and then continuing the execution of the playbook.

Reducing human activities to the minimum necessary is often the better choice in handling an incident, because it makes the response time faster and standardizes the response independently by the operators. Unfortunately it is not always possible to foreseen attack use-cases or the context is not matching with the automation rule trigger: in these cases security operators can decide to manually activate the related actions like blocking a user, blocking traffic related to malicious IP address or isolating hosts.

Automation and workflow management are the basis of Sentinel's SOAR operation. Through

the logic apps it is possible to manage the automation of actions within the services offered by Microsoft. Through API connections, the logic APPs can interact with third-party products and services. Every time a connector is installed, a new API connection is also automatically created thus enabling the interaction between Sentinel and the new services. Playbooks can be classified in classes as shown in table 3.3

Playbook Class	Examples
Notification Playbooks	Post a message in a Teams channel Send an email
Blocking Playbooks	Block IP address on Azure Firewall Block Azure AD user Reset Azure AD user password Isolate a Device using Defender for Endpoint
Incident Handling	Create an incident on Sentinel Relate alerts to an incident Create an incident on ticketing the platform

Table 3.3. Playbooks classes examples

Investigations

Once configured to collect native or third-party events, Sentinel can be used for investigations and it provides details about incidents to security operators.

A relevant parameter in incident management process is the MTTR (Mean Time To Resolve): to improve it, it is necessary the adoption of practices that enable quick, efficient and effective actions oriented to incident resolution.

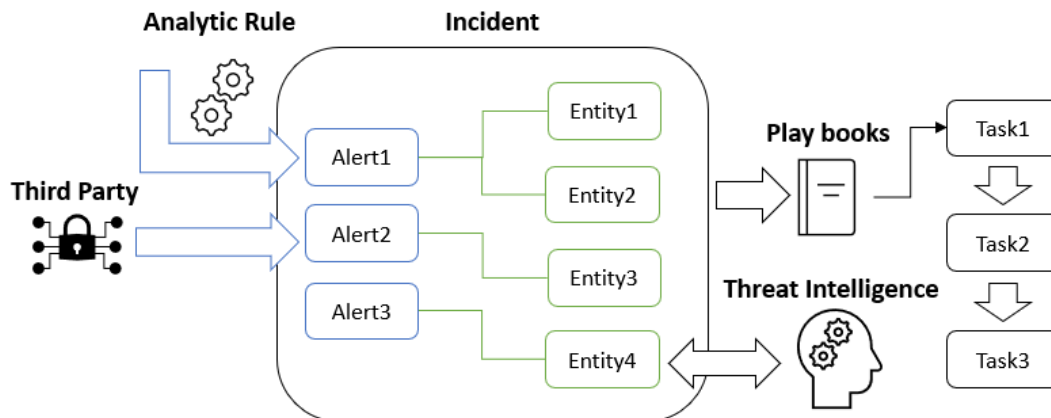


Figure 3.6. Microsoft Sentinel - Incident investigation components

As shown in figure 3.6, alerts are the most important pieces of evidence related to a specific incident, they are collected through analytic rules or received from third-party tools. Incidents are linked to entities through alerts and they can be enriched by exchanging

information with a threat intelligence platform. When required an Automation Rule or a Playbook can be activated automatically or manually.

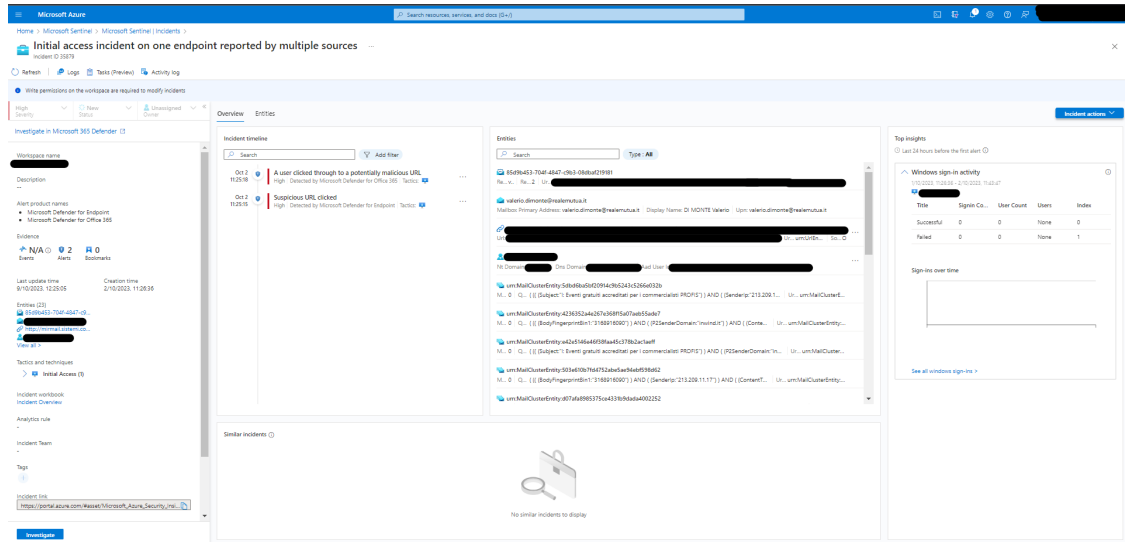


Figure 3.7. Microsoft Sentinel - Incidents page

Each analysis starts from the the incident page, which shows a list of all the incidents classified by the analytic rule that generated them. Once selected the incident to investigate (see Fig. 3.7) it is possible to take charge of the incident management, modify its status (New, Active, Close) or its severity.

The main screen of the incident shows the *number of events*, *alerts* and the *list of entities* involved, as well as a reference to the *Tactics and Techniques* of the MITRE framework. The operator has structured access to information on the *time line* of the incident and the *entities* involved. Furthermore, as shown in figure 3.8, the automatic investigation tool produces a graphical representation of the relationships between alert entities and different incidents. Each alert includes a detailed information and a *link to Microsoft documentation* providing more elements on the specific alert. In addition, there is an *insight widget* that suggests how to handle the incident correctly. If the incident was generated by a tool integrated with Sentinel, as shown in figure 3.8, it is possible to jump directly to the source of the alert for further information or to perform containment operations.

As figure 3.9 shows, the operator can also access *queries* that generated the alerts, in order to re-execute them, search for variations or modify their code for obtaining different information. Security analysts can activate bookmarks when they finds something particularly important among the examined logs.

The operator can also define new *automation rules*, execute *playbooks* in response to an incident or eventually create a *Teams channel* for handling the incident. All operations performed automatically are tracked in the *activity log*, as shown in figure 3.10: the operator can add his own comments and manually performed activities. This approach is useful both for incident reporting and for continuous improvement on the incident handling process.

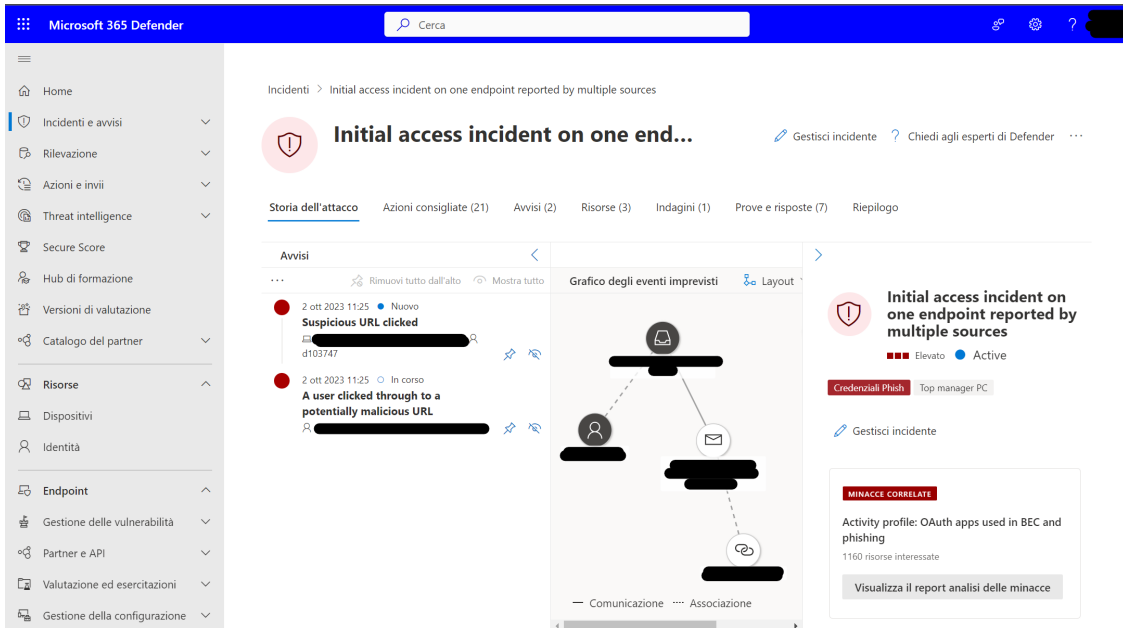


Figure 3.8. Microsoft Defender for Cloud - Incident

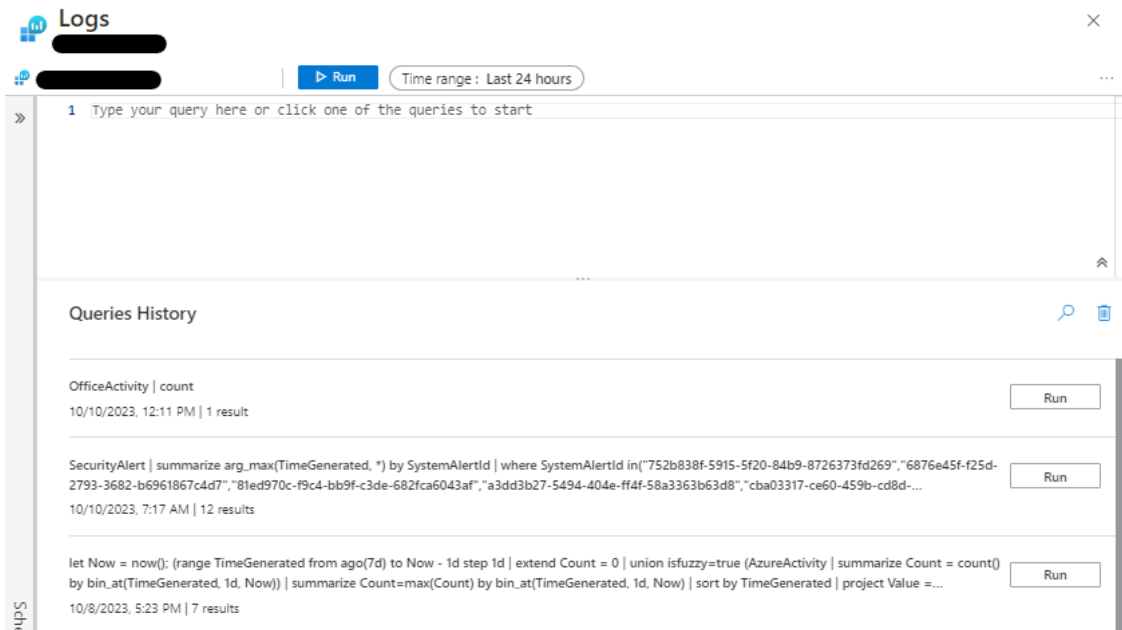


Figure 3.9. Microsoft Sentinel - Query history

Operators must add a comment and classify the incident for its closure, the options offered

are: True Positive – suspicious activity, Benign Positive – suspicious but expected, False Positive – incorrect alert logic, False Positive – incorrect data and Undetermined. The analysis of incident closures provide important information on how to improve incident management.

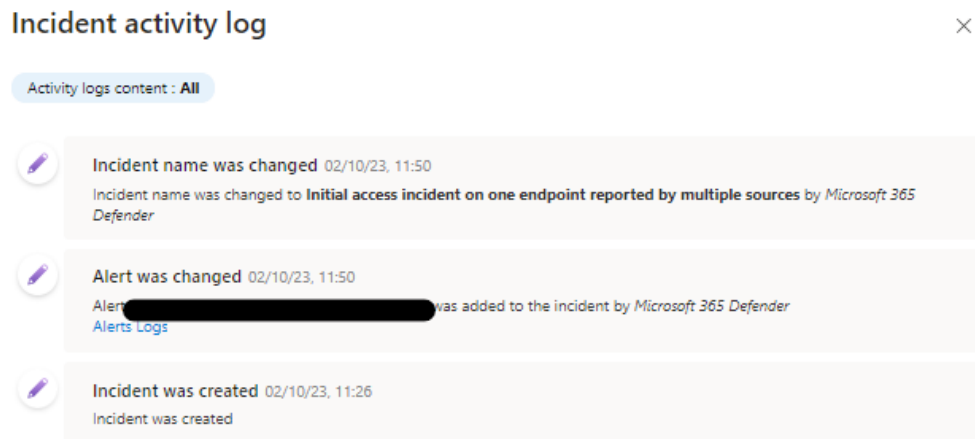


Figure 3.10. Microsoft Sentinel - Activity log

3.3.2 Chronicle SOAR

As reported in Google Documentation [46] *Siimplify* is the SOAR of Google threat detection ecosystem. Through its functionalities we can find:

- **Case manipulation:** It allows to close a case, add a comment, close alert, transform the case in incident, assign the case to an operator and add entity or attachment to a case.
- **Case metadata:** It allows to add tags, change case stage, change priority and mark as relevant.
- **Data retrieval:** It gets comments, tickets IDs or similar cases.

The whole set of built-in actions included in *Siimplify* are available in Google documentation [60]. In addition to case management features, Siimplify permits the definition of playbooks that, once triggered, execute actions up to the final resolution. Playbooks can be activated by a specific alert or for all the alerts. Actions can be Siimplify out-of-the-box services or they can be integrated services from Chronicle marketplace and they often require to enrich input or output data. *Manual actions* can be also included in playbooks, in this case the security operator has to do them and interact with the playbook by indicating to move forward. The security analyst must choose the entity on which he wants to execute the playbook. Playbook flows can include *conditional branches* that can be activated according with the result of the previous tasks. If the main branch does not match the conditions a fallback branch can be taken.

Playbooks help to be focused on investigations instead of performing repetitive activities, moreover Chronicle allows to share incident management with all the relevant departments enabling collaborations and information sharing.

3.3.3 Amazon EventBridge

Nowadays AWS does not provide its own SOAR solution [19], but relies on third parties, like CloudStrike or InsightConnect by Rapid7.

Nevertheless, EventBridge is an AWS general purpose automation tool that creates applications that will be automatically executed when a specific event occurs.

The analysis of this solution overcomes the scope of this thesis: further information are available on Amazon documentation [5]

3.4 Conclusion

Correlation and automation rules should be considered as an investment in knowledge that pays dividends over time. *KQL*, *YARA-L* and *SQL* operate hand-in-hand with their correspondent data model: *OSSEM*, *UDM* and *OCSF*. This setting limits portability to different cloud platforms.

A deep knowledge of these *Security Investigation Languages* is useful to perform advanced investigations, hunting activities and to define custom correlation rules that increase significantly detection capabilities. The operation logic under the hood of the correlation engine is almost completely hidden to customers. This mainly happens because vendors of threat detection platforms want to protect their research and development investment from other vendors. In this context, replacing one threat detection solution would result in an unpredictable loss of visibility with respect to certain events. Mitre Engenuity [97], commented in section 1.6.4 may be useful to minimize this risk.

Another relevant investment in knowledge for a SOC are playbooks, a set of automatic and manual actions performed to properly handle a security incident. Azure, GCP and AWS provide their own automation platforms that work under the hood of the SOAR platforms. Playbooks and cloud services interactions are based on proprietary connectors or APIs and they make *response rules* not portable from a cloud provider to another.

Despite the issue of no-portability, *Security Investigation Languages* and *Automatic Response* rules contribute significantly on the improval of SOC performances.

Chapter 4

Threat Hunting

This chapter includes tests executed in Microsoft Sentinel and Microsoft Defender 365 with the aim of demonstrating how ecosystems work better than tools manually integrated.

4.1 Microsoft Sentinel

This section will provide some examples of investigations to identify possible threats: they are carried out on Microsoft Sentinel through manual KQL Queries that try to replicate automatic detection rules available in Defender for Cloud suite.

4.1.1 Impossible Travels

One of the built-in correlation rules in *Defender for Identity* is related to impossible travels: a user makes authentications from two or more locations that are not compatible with a trip (e.g. authentications from Rome and New York in less than 1 hour). Customers who haven't purchased the Defender for Identity feature could use a KQL query as the following.

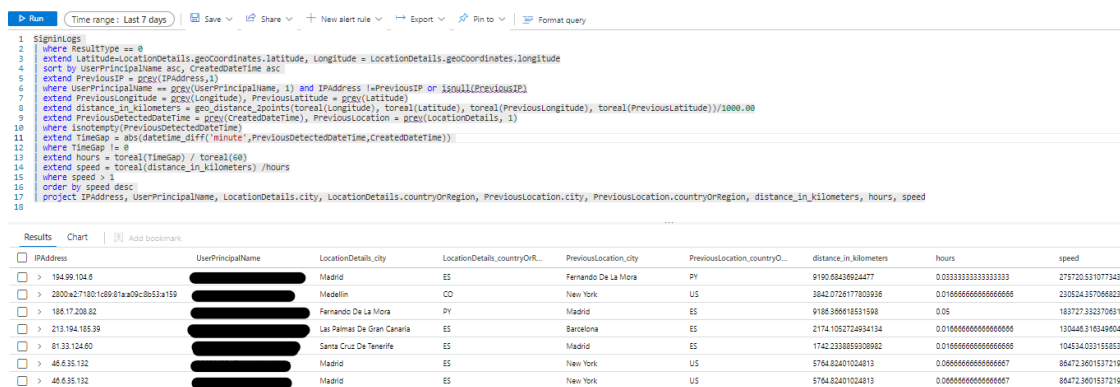


Figure 4.1. Microsoft Sentinel - KQL - Impossible Travel

The SOC operator, who wants to perform this analysis, should access the table *SignInLogs* where all the authentications are registered. This table includes information about: Authentication result, username, date and time, IP Address, latitude and longitude.

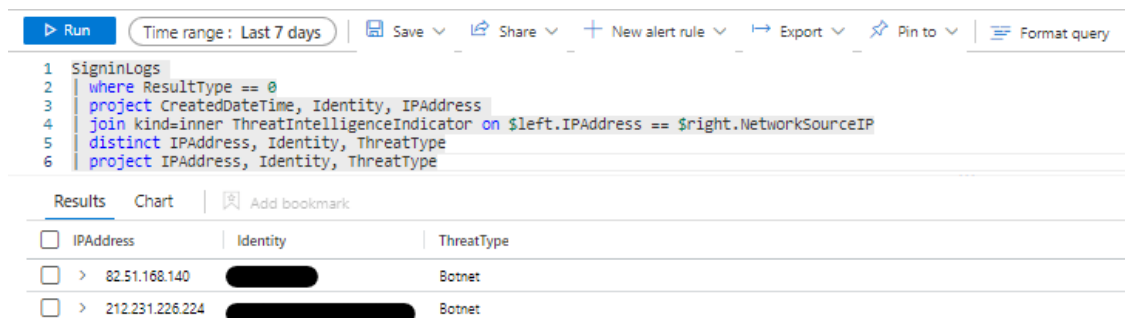
In this example (see fig. 4.1) I choose to filter for successfully authentications (`ResultType == 0`), then I define aliases for dynamic `geoCoordinates` fields (i.e. Latitude and Longitude). Sorting the results of the query by `UserPrincipal name` and `CreatedDateTime`, permits to compare the authentications row by row. If the distance between two sequential authentications for the same user is so far apart that it does not allow a travel from one location to the other, there is an “impossible travel“ that requires to be investigated.

Not all “Impossible Travels“ are malicious activities, for example the adoption of VPNs or anonymous proxy is enough to generate them, but in any case further investigations are always necessary, for instance verify if the IP address from which the authentication takes place is included in the threat intelligence feed or just a check with the users if they have activated a VPN.

4.1.2 Threat Intelligence - Authentication

Another possible area of threat investigation can be to verify IP addresses from which successful authentications have taken place and crossing these information with the threat intelligence feed.

In this case, SOC Operator has to join different tables: the one related to authentications (`SignInLogs`) and the one related to Threat Intelligence (`ThreatIntelligenceIndicator`) using the IP Address as correlation key.



The screenshot shows the Microsoft Sentinel KQL query editor interface. The query is as follows:

```

1 SigninLogs
2   where ResultType == 0
3   project CreatedDateTime, Identity, IPAddress
4   join kind=inner ThreatIntelligenceIndicator on $left.IPAddress == $right.NetworkSourceIP
5   distinct IPAddress, Identity, ThreatType
6   project IPAddress, Identity, ThreatType

```

The results table shows two entries:

IPAddress	Identity	ThreatType
> 82.51.168.140	[REDACTED]	Botnet
> 212.231.226.224	[REDACTED]	Botnet

Figure 4.2. Microsoft Sentinel - KQL - Threat Intelligence Authentication

The result of this query (see Fig. 4.2) highlights two possible authentications from IP Addresses associated to a Botnet, that may indicate that: the device of the user has been compromised and it is part of a botnet, the router behind the user’s device is under the control of a botnet or credentials have been stolen and used from a host that is part of a botnet, which is trying to access to one of the corporate assets. This type of events should be seriously considered and investigated by security operators.

4.1.3 Threat Intelligence - File Access

As shown in section 4.1.2, related to threat intelligence enrichment of authentication events, the access to the files shared in *OneDrive* or *SharePoint* can be Cross-referenced with threat intelligence feed too.

The table `OfficeActivity` (see Fig. 4.3) reports all the activities performed in Office 365 by the end users, including all the file accessed. Crossing Clients IP addresses with threat intelligence feed can help to identify suspicious connections performed by IP addresses included in the Threat Intelligence feed.

The screenshot shows a KQL query in Microsoft Sentinel. The query is:

```

1 OfficeActivity
2 | where Operation == 'FileAccessed' and isnotempty(ClientIP)
3 | join kind=inner ThreatIntelligenceIndicator on $left.ClientIP == $right.NetworkSourceIP
4 | project Start_Time, ClientIP, UserId, SourceFileName, ThreatType

```

The results table shows four rows of data:

Start_Time (UTC) ↑↓	ClientIP	UserId	SourceFileName	ThreatType
> 10/31/2023, 2:12:00.540 PM	82.51.168.140	[REDACTED]	AllItems.aspx	Botnet
> 10/31/2023, 2:12:00.540 PM	82.51.168.140	[REDACTED]	AllItems.aspx	Botnet
> 10/31/2023, 12:56:57.187 PM	82.51.168.140	[REDACTED]	AllItems.aspx	Botnet
> 10/31/2023, 12:56:57.187 PM	82.51.168.140	[REDACTED]	AllItems.aspx	Botnet

Figure 4.3. Microsoft Sentinel - KQL - Threat Intelligence File Access

As for the previous example, also the alerts arising from this KQL Query should be investigated. They can indicate a compromised endpoint or router behind it or it can be a false positive due to dynamic IP addresses allocation of the Internet Service Provider.

4.1.4 Phishing Campaign

When an incident happens it could be interesting knowing if other similar events occurred in the past. For example in case of a phishing campaign, several users may have opened a phishing link. As shown in Fig. 4.4, it is possible to get this information by querying the table `AlertEvidence` and looking for an URL that contains a specific value.

In this case the URL related to a phishing campaign was opened by two different devices.

4.2 Microsoft Defender

Performing manual investigations in Sentinel is especially useful when it collects events from non-Microsoft sources and correlates events generated by third parties and, if necessary, associates them to *automation rules* or *Playbooks*.

If the events to correlate arise only from Microsoft Security tools, it is often a better choice handle the alerts directly on *Microsoft Defender 365* console instead of Sentinel.

In the next sections there will be examples of the features provided by Microsoft Defender 365 will be described.

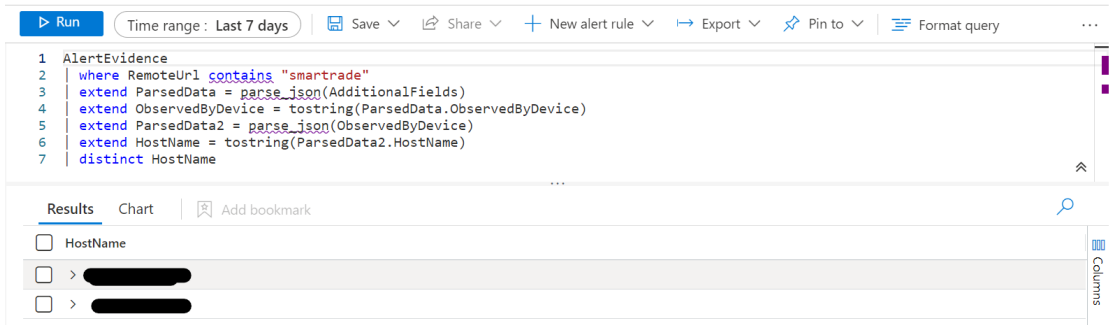


Figure 4.4. Microsoft Sentinel - KQL - Phishing Campaign

4.2.1 Risky Users

In a more advanced way compared with the one reported in section 4.1.2, Defender for Identity allows to identify *Risky Users*, by monitoring many parameters related to users authentications like: uncommon user-agent, unfamiliar location, suspicious IP Address and others.

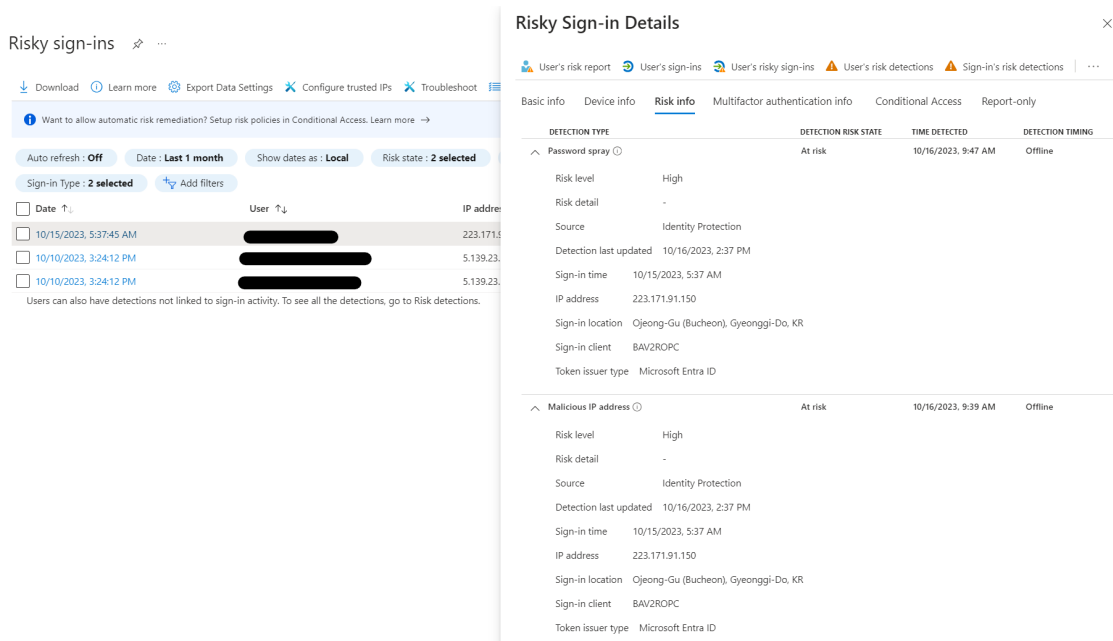


Figure 4.5. Microsoft Defender for Identity - Risky Users

As shown in Fig. 4.5 three different authentications related to a user were performed by South Korea and were associated to *Password spray* attack and *Malicious IP Address*. This information comes from an automatic feed of Microsoft Threat Intelligence and are

cross-referenced with each authentication performed in order to identify possible risky authentications and eventually perform automatic tasks as: require a step-up authentication, reset password, drop authentication token and others.

The ability of identifying authentication alerts by checking user agents, common locations or time of authentications, is possible because the authentication system is offered directly by Microsoft. Collecting the same information from third-party systems and cross-referencing them with threat intelligence information would have been much more complicated.

Ecosystem logic can be seen for example when a web application federated with Microsoft Entra ID can rely on the information collected during the authentication phase and so verify the user security posture. To gain protections from malicious IP address, applications have just to use federated authentication with Microsoft Entra ID.

4.2.2 Phishing Campaign

As shown in section 4.1.4, the identification of the number of users that have opened a phishing link is crucial to break a multi-stage-attack in the early phases.

There are also other relevant information to be considered when dealing with a phishing campaign, as for example: if it is a generic or targeted phishing campaign, the level of target exposure to vulnerabilities, if there is a malware associated to the campaign, how many recipients are involved, how many phishing messages are delivered before identification, how many users have opened the phishing link and so on.

Microsoft Defender 365 (see Fig. 4.6) provides all these information and allows the SOC operator to perform remediation activities (see Fig. 4.7) e.g., move the email into Junk mail, delete it, perform an automatic investigation and others.

The collection of information and the ability to perform automatic containment tasks is mainly due to the built-in integration between Microsoft's products; reproducing the same functionality with third-party products would require a great effort during both setup and maintenance phases.

4.2.3 Advanced Investigations

Microsoft Defender 365, as well as Sentinel, allows to perform KQL queries to investigate incidents, collect evidences and to define custom detection rules.

Threat Hunting may require to analyze in deep also events that do not have High severity. In this case what sounds strange is that a power-shell command has been encoded: this is normally done by attackers when they need to hide commands to defenders. As shown in Fig. 4.8, table **AlertEvidence** collects all the evidences of possible incidents. Any of them are related to encoded powershell commands. Through KQL it is possible to automatically decode the power-shell command in order to understand if it is something to be worried about or not.

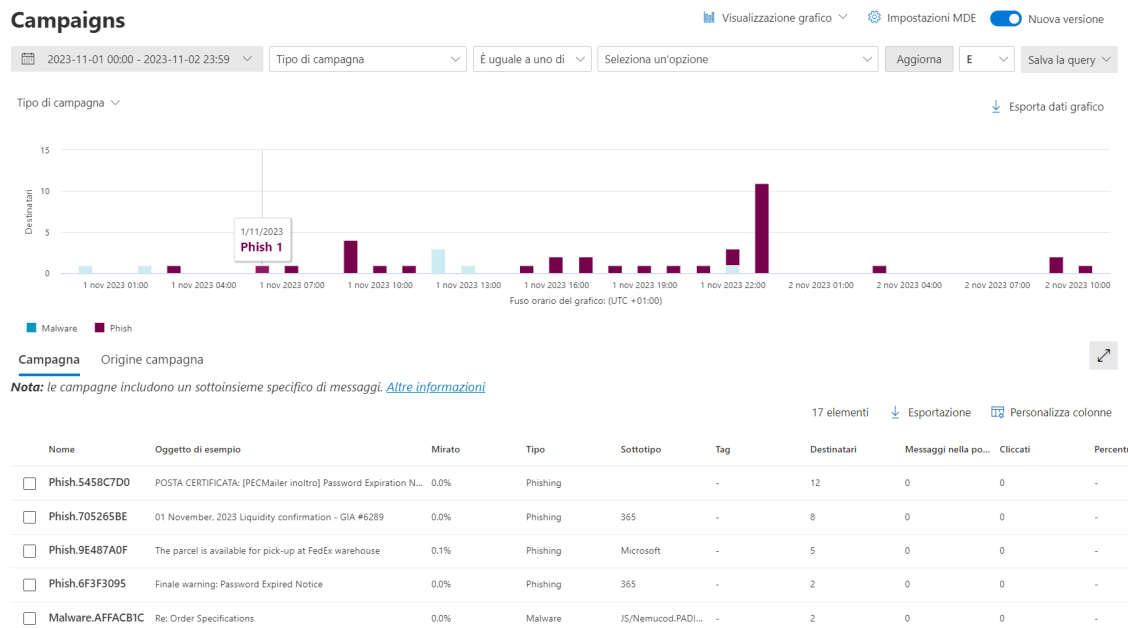


Figure 4.6. Microsoft Defender 365 - Phishing Campaign

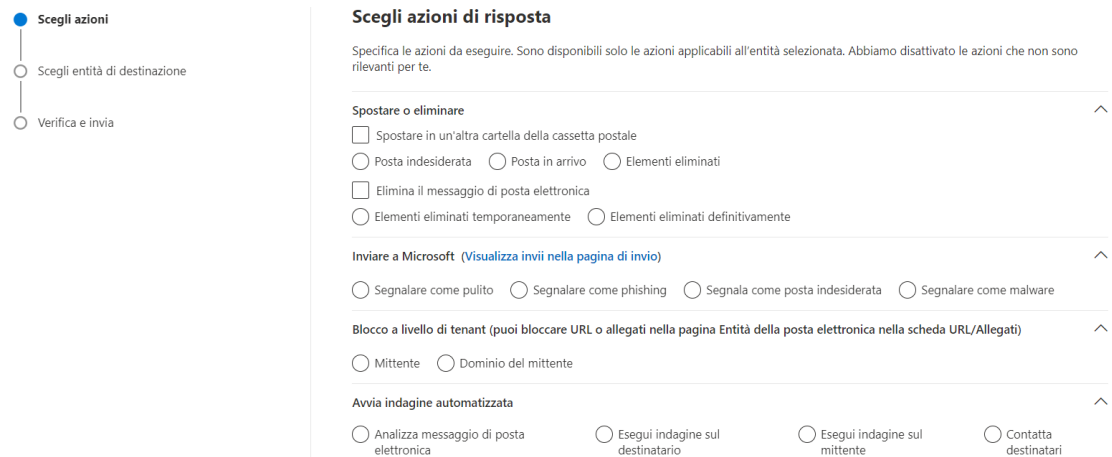


Figure 4.7. Microsoft Defender 365 - Phishing Actions

The decoded string seems to be not human readable yet, but it is just a matter of character-set: a copy and paste is enough to see the power-shell code or in alternative it can be used a Base64 converter with the original Base64 string (see Fig. 4.9¹)

¹<https://www.base64decode.org/>

The screenshot shows the Microsoft Defender 365 - Advanced Investigations interface. At the top, there's a navigation bar with 'Esegui query', 'Ultimi 30 giorni', 'Salva', 'Condividi collegamento', and 'Crea regola di rilevamento'. Below this is a 'Query' editor with a KQL script:

```

1 AlertEvidence
2 | where EntityType == 'Process' and FileName == "powershell.exe"
3 | extend ParsedData = parse_json(AdditionalFields)
4 | extend CommandLine = tostring(ParsedData.CommandLine)
5 | where CommandLine contains "encoded"
6 | extend Array = split(CommandLine, ' ')
7 | extend text = tostring(Array[6])
8 | extend decoded = base64_decode_tostring(text)
9 | extend Host = tostring(ParsedData.Host)
10 | extend Account = tostring(ParsedData.Account)
11 | extend ParsedData2 = parse_json(Account)
12 | extend Name = tostring(ParsedData2.Name)
13 | project Timestamp, Severity, Host, Name, decoded
    
```

Below the query editor, there's a 'Risultati' section with a table of results. The table has columns: Timestamp, Severity, Host, Name, and decoded. Two results are shown:

Timestamp	Severity	Host	Name	decoded
17 ott 2023 16:42:08	Medium	("\$ref":"3")	[REDACTED]	&0c0h0c0p0.0c0o0m0 0f
17 ott 2023 16:42:08	Medium	("\$ref":"3")	[REDACTED]	&0c0h0c0p0.0c0o0m0 0f

Figure 4.8. Microsoft Defender 365 - Advanced Investigations

Decode from Base64 format

Simply enter your data then push the decode button.

The screenshot shows a Base64 decoder tool interface. At the top, there's a text area containing a long Base64 encoded string. Below the text area, there's a section for settings:

- A dropdown menu set to 'AUTO-DETECT' with the label 'Source character set.'
- A checkbox labeled 'Decode each line separately (useful for when you have multiple entries).' which is unchecked.
- A radio button labeled 'Live mode OFF' with the label 'Decodes in real-time as you type or paste (supports only the UTF-8 character set).' which is selected.
- A green button labeled '< DECODE >' with the label 'Decodes your data into the area below.'

Below the settings, there's a text area showing the decoded output:

```

&chcp.com 65001 > $null
$exec_wrapper_str = $input | Out-String
$split_parts = $exec_wrapper_str.Split("@('0'0'0'0')", 2, [StringSplitOptions]::RemoveEmptyEntries)
If (-not $split_parts.Length -eq 2) { throw "invalid payload" }
Set-Variable -Name json_raw -Value $split_parts[1]
$exec_wrapper = [ScriptBlock]::Create($split_parts[0])
&$exec_wrapper
    
```

Figure 4.9. Base64 Decode

Chapter 5

Principles & Guidelines

Organizations of all sizes are struggling to respond quickly to cybersecurity threats, mainly because of the lack of personnel, interoperability between different technology solutions, multi-cloud environments, continuous growth of cyber threats, geopolitical crisis (e.g. war in Ukraine), rapid business changes not compatible with long-term investments and advanced skills required in cybersecurity.

This thesis has shown that the most relevant tools for a SOC are those that enable visibility, real-time threat detection, log collections, threat intelligence and automatic response to security events. These tools must be efficiently integrated, by exchanging information and by allowing SOC operators to move from one solution to another as if it is a single security tool. A modern SOC cannot do without xDR, SIEM and SOAR: the choice to use solutions provided directly by Cloud Service Providers is often an advantage because it permits a better correlation of events generated by the control plane and FaaS, SaaS, PaaS services. The adoptions of third-party solutions is a sub-optimal choice, because they require integration through the APIs made available by cloud providers and it is unreasonable to assume that they can offer more advanced detection capabilities in comparison to those who create the APIs and have direct control over the underlying infrastructure. In addition, leading cloud providers thanks to their huge “installation base“, can train their machine learning and AI algorithms on an enormous database of telemetry signals: this makes them in a dominant position over the rest of the market. All three major cloud service providers have a network of partners with solutions integrated into their ecosystems. Before choosing a third-party solution, it is necessary to read the documentation carefully to identify any possible integration gaps.

The on-premise components of hybrid environments often offer much lower levels of visibility and automation than the ones offered by a cloud service providers; this should suggest additional security measures to protect on-premise workloads. Anyway, in the medium term, it is advisable to consider moving to the cloud not only for the improved visibility and automation, but also because it does not require to set up infrastructures or spend time configuring log ingestions.

The next section will attempt to provide a set of guidelines aligned with these considerations.

5.1 Guidelines

In this section will be presented a guideline in each paragraph, the order represents the relevance compared to the others.

5.1.1 Ecosystems

Organizations often introduce new security solutions to respond to a specific risk ignoring how these solutions can integrate and support quick identification and management of security threats.

This approach is inefficient because the new solutions behave like an independent silos with respect to the rest of the security solutions. Choosing a new tool should always consider its integration with threat detection and response solutions, by increasing visibility and enabling holistic management of security threats.

Ecosystems consist of tools that share communication protocols, integration techniques and data models. Choosing tools inside the same ecosystem allows to simplify security operations and reduce the integration friction and maintenance costs. It is often better not to choose the best product if it is not part of the existing ecosystem.

5.1.2 Telemetry

Software distribution and patch management processes hardly achieve 100% efficiency: when analyzing risks exposure to define a remediation plan, actions to be taken should not be based on incomplete reports.

xDR platforms achieve a high degree of confidence about configuration of network connected systems by combining telemetry information coming directly from the hosts, with information extracted by network traffic captures or scans made by the hosts connected to the xDR platform. These characteristics make possible to infer even the status and configuration of hosts not controlled by the xDR platform as well.

Knowing the actual state of configuration and the vulnerability of network-connected systems is critical to effectively fight adversaries that have gained access to the network or that are trying to.

5.1.3 Automation

Targeted-Attacks are increasingly being prepared to be executed automatically without human supervision. This avoids attackers to be intercepted, because they can anonymize their accesses before the actual attack is performed and they can also realize a faster execution of the attack.

Attack automation forces defenders to use similar techniques to reduce human error and

allows more tasks to be performed than with a human-based approach. In addition reducing the effort required to respond to recurrent threats, it allows Security Operators to be focused on higher value activities like studying attackers TTPs.

SOAR platforms fully integrated with SIEMs, security systems and Cloud Service Provider APIs provide a high level of efficiency and are now an essential resource for modern SOC.

5.1.4 Security Pillars

By greatly simplifying, all security architectures and cybersecurity frameworks agree on the need to protect data, identities and infrastructures.

When an enterprise starts a new project, security architects and engineers should focus on these three pillars. During the design of security, conceptualizing how user identification is ensured, how data protection both at rest and on transit is guaranteed and how cloud and on-premise infrastructures are protected should be the main goal.



Figure 5.1. ENISA - Top 15 Cyber Threats [36]

Choosing a standard framework for threat identification, such as the *ENISA threats landscape* [36], helps in the identification of the main threats (see figure 5.1) to protect from. Threat response must be designed to be able to detect possible anomalies and to protect the data, identities and infrastructures involved.

ENISA also publishes threat landscapes dedicated to individual areas (e.g. Threat Landscape for 5G Networks [33]) that security engineers should look for when designing a new IT solution.

5.1.5 Attack surface reduction

The “remote work” explosion has led many organizations to publish back-office (non-customer-facing) applications on Internet without proper security measures in place.

A growing trend in cybersecurity is *Secure Access Service Edge* (SASE): this service reduces the attack surface increasing visibility and providing access control according with Zero Trust Architecture (ZTA). With *SASE*, business applications are accessible only to business users as shown in figure 5.2.

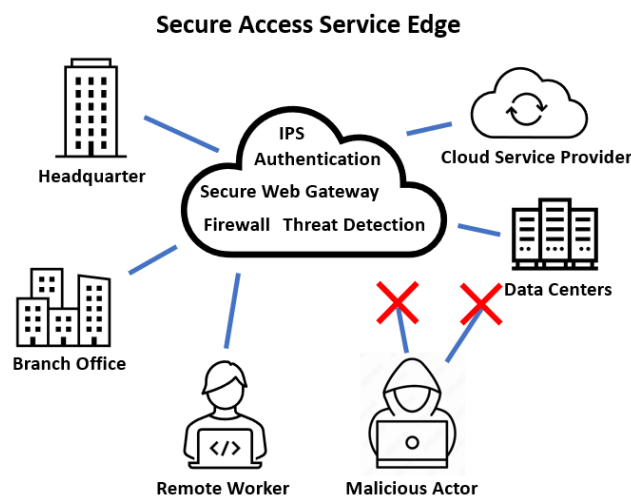


Figure 5.2. SASE - Secure Access Service Edge

Each time a user needs to access to a corporate service, first of all it is required to authenticate to SASE cloud service. It verifies identity and device security posture. After that, SASE verifies user authorization and if the user is authorized to access to the service required connection is allowed. Both service and users generate outbound connections through SASE services. No direct connections between users and service are allowed, so this reduces the attack surface of the corporate because unknown users cannot even probe the service, because it is no longer internet-facing but can be reached only through SASE. SASE applies one of the ZTA principles about not trusting anyone until not properly identified and it can be used to connect branches, data centers and cloud service providers, by centralizing authorization rules and allowing step-up authentication in case the context requires it.

SASE main concerns are about latency and service availability. The risk of unavailability can be minimized by redundancy or other solutions that ensure high level of resiliency like

Anti-DDOS or Auto-scaling. Latency depends on the location of POP¹ and cannot be eliminated.

5.1.6 Continuous improvement

The security incident process continuously refines and improves over time. Proper management helps building a knowledge base that is useful for positively evolving defense capabilities.

Lessons can be learned from each incident, even from the less relevant one is possible to understand how to “improve“ the management of security events, for example by adding new log sources to the SIEM, by creating new correlation rules or specific playbooks that make reaction automatic.

Critical analysis on how past incidents were handled is often underestimated, because everyday activities receive higher priorities. However, as suggested by Nassim Nicholas Taleb in “Antifragile” [135] in order to achieve an antifragile system, the response should not simply restore the previous situation, but has to introduce improvements.

5.1.7 Multi-cloud Threat Detection and Response

In previous chapters, I have tried to emphasize the advantages that the ecosystem logic brings over the spasmodic search for the best solution on the market, because I am convinced that assessing security from a holistic perspective is much more effective than an atomic level which looks at possible responses to each specific threat. However, there are some exceptions where full holistic approach may not be suggested, such as security management in a multi-cloud environment.

As we have observed, there is not yet a level of standardization that allows one cloud provider’s security system to be used to control the others without losing efficiency, such as when correlating data or automatically responding to an attack. In these specific cases, using stand-alone solutions for individual clouds would be inefficient both in terms of the costs ensuring the appropriate levels of expertise in each cloud context and in terms of visibility across different cloud environments.

In case a multi-cloud approach cannot be avoided, it might be more advantageous to use third-party threat detection and response platforms, that allow strong integration with the APIs of different cloud providers. This would ensure that the security operation center can gain advanced skills in managing a single platform and can also obtain a unified visibility across the different cloud environments.

¹POP - Point Of Presence, physical location where are located the devices necessary to perform network connection

5.1.8 Open-Source

Very large enterprises could decide to adopt open-source solutions to create a vendor independent threat detection and response ecosystem. Increasingly, open-source is under the hood of commercial solutions and even the three main Cloud Service Providers adopt it for their own services, mainly because they do not achieve licence agreements with third parties, but also because they have the "firepower" to be able to independently develop open-source solutions if necessary.

This approach, at first glance, might seem viable only for large U.S. software houses, but other companies have also chosen to base their core systems on opensource to ensure that as the volume of services delivered grows, costs do not also grow in the same way. Some examples of enterprises that largely adopt opensource for their core services are: Pega System, Netflix and Adobe.

The main trade-off of adopting this approach is that enterprises may have to fix software problems or lack of functionalities by themselves, for this reason only very large enterprises should consider this scenario by hiring people who have gained expertise by participating to open-source projects.

Chapter 6

Final Conclusions

With the introduction of the regulation “*Perimetro di Sicurezza Nazionale Cibernetica*“, OSEs are required to monitor and properly handle security incidents through the usage of SOCs: for this reason, systems commonly adopted by them have been analyzed. The analysis aimed to produce principles and guidelines for stakeholders of public and private organizations that have to use and configure these monitoring tools.

The landscape where OSEs operate, starts from the analysis of the regulatory and passes through security architectures, international standards and best practices. The description of how adversaries and defenders operate completes the big picture that has to be considered while selecting and configuring detection and response tools.

Enterprises of all sizes are increasingly relying on public cloud providers to deliver their IT services: for this reason, the analysis of SOC monitoring tools can't be made without evaluating the offerings of major cloud providers like AWS, Azure and GCP. In recent years, public cloud providers, also with the support of third parties, have been able to build an ecosystem of security solutions that natively exchange information reciprocally in order to ensure better performance of both preventive and reactive cybersecurity. In this scenario, Opensource solutions make an appearance, representing a good option for those enterprises that don't want to have a vendor lock-in for regulatory or for strategic decision.

Once introduced the main security features offered by public cloud providers, the thesis deals with the context where SOCs operate. Starting from this background, Threat Detection and Response tools have been analyzed in-depth, because they represent the key stone for security incident handling. Security Investigation Languages, event correlation and security orchestration tools provided by each cloud ecosystem complete the description of the main Threat Detection and Response functionalities.

Some simple threat hunting activities are shown in chapter 4 in order to highlight how ecosystems are more efficient and how they require less effort than choosing independent solutions.

The analysis is finalized with a set of suggestions for security architects and engineers

that have to choose the set of tools necessary for a SOC of an OSE (Operatore di Servizi Essenziali) or PSD (Fornitore di servizi digitali). These guidelines are based on the researches done for this thesis and on personal experiences in the field.

6.1 Possible further studies

A possible extension of the study proposed in this thesis can start from the Article 30 of the Digital Operational Resilience Act (DORA), titled “Outsourcing of critical ICT functions“: it sets out requirements for financial institutions that outsource critical ICT functions to third-party providers. Within other constraints, this article states that financial institutions “must *define* and *TEST* a migration plan to another third-party provider or bring the ICT service in-house in the event of failure of the third-party provider used”.

DORA regulations will be effective on January 17th, 2025. With the official release of the RTS (Regulatory Technical Standards), the supervisor authorities will clarify better requirements, but at the moment the article 30 appears to be one of the most critical conditions for achieving DORA compliance, because of the lack of technological solutions in the market.

In the next paragraphs will be offered some possible future investigations that can be addressed to support migrations of cybersecurity services from a cloud provider to another.

6.1.1 Migration tools - correlation rules

Correlation rules are one of the most important assets for a SOC, because they enable the identification of threats in the specific environment in which they are written. As seen in the thesis, there are different standards for defining correlation rules, for this reason moving workloads from one Cloud Provider to another involve rewriting correlation rules.

A possible further investigation can involve the analysis of migration tools, checking if the change in the underlying data model impacts the quality of the rules.

A starting point could be the analysis of the tools that allow the migration from *sigma rules* (the most widespread in the market) to KQL and vice versa. Both of them are reported into bibliography [84] [116].

6.1.2 Test - Correlation rule

Correlation rule testing plays a key role in validating the effectiveness of the migration of correlation rules. The adoption of tools that allow to simulate attacks according with MITRE ATT&CK could be a way to test the strength of correlation rules.

There are several tools available in the market (e.g. Safe Breach ¹ or Cobal Strike ²) and at least two of them are opensource (e.g. Red Canary ³ or Metasploit ⁴), on the other hand playbooks can be created to automate attacks exploiting the tools available in *Red Team Tool* repository ⁵

6.1.3 Procedure - Automatic Response

Automated response to security incidents often leverages automation provided by the cloud service provider or by the built-in SOAR platform.

Analyzing and verifying the functionality of migration procedures provided by a cloud provider (e.g. Microsoft ⁶), could be a key step in a plan to migrate from one cloud provider to another, as well as, the analysis of the challenges to face when migrating SOAR automatic response rules.

6.1.4 Opensource Private Cloud

One of the most interesting and challenging further studies that can be inspired by this thesis, could be the construction of a private cloud completely based on opensource solutions.

Starting from an Openstack and Kubernetes infrastructure, the idea could be trying to develop a control plane in order to make available the security services listed in table 1.2 as much as possible. An insight about opensource solutions is also available in table 2.2, but it must be considered that not all projects are still active and some of them have been transformed into pay-as-you-go projects.

Considering the requirements set by DORA and DSA (Digital Services Act) it is clear that Digital Sovereignty is an important goal for Italy and Europe in order to achieve national security, economic independence and development.

¹<https://www.safebreach.com/>

²<https://www.cobaltstrike.com/>

³<https://redcanary.com/>

⁴<https://www.metasploit.com/>

⁵<https://github.com/A-poc/RedTeam-Tools>

⁶<https://learn.microsoft.com/en-us/azure/sentinel/import-export-analytics-rules>

Appendix A

Appendix

Table A.1. Malicious Actors - Russian - state-sponsored

Name	Nationality	Description
APT28 (Fancy Bear)	Russia	<p>As reported by Forbes[37], Fancy Bear is a cyber espionage group that has been active since at least 2007. The group is believed to be affiliated with the Russian military intelligence agency GRU. APT28 is known for its sophisticated attacks against high-value targets, including governments, militaries, and political organizations around the world.</p> <p>The group is known for using zero-day exploits, phishing attacks, and malware to infiltrate its victims' networks installing backdoors and monitoring communications.</p>
APT29 (Cozy Bear)	Russia	<p>As reported by Sekoia[114], Cozy Bear is a cyber espionage group that has been active since at least 2008. The group is believed to be affiliated with the Russian Foreign Intelligence Service (SVR). APT29 is known for its sophisticated attacks against high-value targets, including governments, militaries, think tanks, and businesses around the world.</p> <p>They were linked to any of the most relevant attacks of the last year as Solarwind and any USA government departments</p>
Sandworm	Russia	<p>As reported by Wikipedia[138], is a state-sponsored Russian cyberwarfare unit that has been active since at least 2014. The group is believed to be affiliated with the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU), Russia's military intelligence agency. Sandworm is known for its sophisticated attacks against high-value targets, including critical infrastructure, government agencies, and military organizations.</p> <p>They are related to NotPetya ransomware attack and they are On-going performing cyberattacks against Ukraine in support of Russia's military invasion.</p>

Table A.2. Malicious Actors - China - state-sponsored

Name	Nationality	Description
APT10 (Stone Panda)	China	As reported by Forbes[38], is a Chinese state-sponsored cyberespionage group that has been active since at least 2009. The group is believed to be affiliated with the Tianjin State Security Bureau of the Ministry of State Security (MSS). APT10 is known for its sophisticated attacks against high-value targets, including government agencies, militaries, and businesses in a variety of industries.
APT41 (Winnti)	China	As reported by Picus Security[111], is a Chinese state-sponsored cyberespionage and cybercrime group that has been active since at least 2007. The group is believed to be affiliated with the Chinese Ministry of State Security (MSS). APT41 is known for its sophisticated attacks against a wide range of targets, including government agencies, militaries, businesses, and educational institutions. APT41 is a highly skilled and resourceful group that uses a variety of techniques to gain access to its targets' systems and steal data. The group is known for using zero-day exploits, phishing attacks, and malware to infiltrate its victims' networks.
APT40 (BRONZE UNION)	China	As reported by Rapid7[112], is a cyber espionage group that has been active since at least 2013. This group primarily targets defense and government organizations, but has also targeted other industries, including engineering firms, shipping and transportation, manufacturing, defense, government offices, and research universities in the United States, Western Europe, and along the South China Sea.
Lazarus Group	North Korea	As reported by Wikipedia[132] is a North Korean state-sponsored cyber threat group that has been active since at least 2009. It is one of the most sophisticated and dangerous cyber threat groups in the world, and is known for its wide range of capabilities and its willingness to target a wide range of victims, including governments, businesses, and individuals. they were related in the 2014 hack of Sony Pictures Entertainment, the 2017 WannaCry ransomware attack, and the 2019 SWIFT hack.

Table A.3. Malicious Actors - North Korea - state-sponsored

Name	Nationality	Description
Kimsuky	North Korea	also known as Velvet Chollima and Black Banshee is a North Korean state-sponsored advanced persistent threat (APT) group that has been active since at least 2013[93]. The group is known for its sophisticated cyberattacks targeting governments, businesses, and individuals in South Korea, Japan, the United States, and other countries
BlueNoroff	North Korea	also known as APT38, Stardust Chollima, BeagleBoyz, and NICKEL GLADSTONE) is a North Korean state-sponsored advanced persistent threat (APT) group that has been active since at least 2016.[90] The group is known for its sophisticated cyberattacks targeting financial institutions, cryptocurrency exchanges, and other organizations around the world.

Table A.4. Malicious Actors - Criminal organizations

Name	Nationality	Description
LockBit	Unknown	is a ransomware group that has been active since 2019.[29] It is one of the most prolific and dangerous ransomware groups in the world, and is known for its sophisticated attacks targeting organizations of all sizes. LockBit was the most active global ransomware group and RaaS provider in terms of the number of victims claimed on their data leak site
REvil	Russian	also known as Sodinokibi) was a Russia-based or Russian-speaking private ransomware-as-a-service (RaaS) operation. It was one of the most prolific and dangerous ransomware groups in the world, and was known for its sophisticated attacks targeting organizations of all sizes. REvil was known for its use of double extortion, in which the group would threaten to release stolen data in addition to encrypting the victim's files. This made REvil attacks particularly dangerous and costly for victims.[136]
Dridex	TBD	Cybercrime groups

Table A.5. Malicious Actors - Hacktivist groups

Name	Nationality	Description
Anonymous	all over the world	Anonymous is a decentralized international activist and hacktivist movement that is primarily known for its various cyberattacks against several governments[130], government institutions, and government agencies, corporations, and the Church of Scientology. Anonymous originated in 2003 on the image-board 4chan, and it has since become a global movement with members from all over the world. Anonymous is known for its use of masks and its adoption of the Guy Fawkes mask, which is based on the V for Vendetta comic books and film.
LulzSec	all over the world	LulzSec was a black hat computer hacking group that claimed responsibility for several high-profile attacks, including the compromise of user accounts from PlayStation Network in 2011. The group also claimed responsibility for taking the CIA website offline.[133] LulzSec was founded in May 2011 by a group of hackers who were part of the Anonymous hacktivist movement. The group's name is a shortened form of "Lulz Security", where "lulz" is a slang term for amusement or laughter. LulzSec's attacks were often motivated by a desire to expose security vulnerabilities and to embarrass the organizations that were targeted. The group also claimed to be motivated by a desire to entertain the public.
DDoS Crew	unknown	DDoS Crew is a group of hackers who are known for launching distributed denial-of-service (DDoS) attacks against websites and online services. DDoS attacks are designed to overwhelm a target with traffic, making it inaccessible to legitimate users. DDoS Crew has been responsible for a number of high-profile DDoS attacks, including attacks against the websites of Sony, Microsoft, and the BBC. The group has also been responsible for attacks against government websites and online services.

Table A.6. Most widespread malware

Name	type	Description
TrickBot	Modular Malware	<p>as reported by Tech Target [125] TrickBot is a modular banking Trojan that was first discovered in 2016. It is one of the most sophisticated and persistent banking Trojans in existence, and it has been used to steal millions of dollars from businesses and individuals around the world.</p> <p>In addition to stealing data, TrickBot can also be used to spread other malware, such as ransomware. TrickBot is often used as a precursor to ransomware attacks, as it can weaken the security of a victim's computer and make it easier for the ransomware to be installed.</p>
WannaCry	Ransomware	<p>WannaCry is a ransomware cryptoworm that was first discovered in May 2017. It is a self-propagating malware that exploits vulnerabilities in the Windows operating system to encrypt files on a victim's computer. Once encrypted, the files are inaccessible to the victim until a ransom is paid in Bitcoin.</p> <p>As reported by Tech Target[126] WannaCry is a very dangerous malware because it is self-propagating and can spread quickly through networks. It is also very difficult to remove once it has infected a computer.</p>
Emotet	Dropper	<p>Emotet is a type of malware that was first discovered in 2014. It is a Trojan horse that is spread through phishing emails and malicious attachments[131]. Once Emotet has infected a computer, it can steal personal information, such as passwords and credit card numbers. It can also download other malware onto the computer, such as ransomware.</p> <p>Emotet is believed to be the work of a Russian cybercrime group known as TA542. The group is known for its sophisticated attacks and its ability to evade detection.</p>
Zeus	Trojan	<p>Zeus malware is a Trojan horse that is used to steal financial information, such as passwords and credit card numbers. It is spread through phishing emails and malicious attachments. Once Zeus has infected a computer, it can log keystrokes, steal cookies, and modify web pages to trick users into revealing their personal information.</p> <p>Zeus malware is a constantly evolving threat, from which were born several variants.</p>
Ryuk	Ransomware	<p>Ryuk is a type of ransomware that was first discovered in August 2018. It is a highly sophisticated ransomware that is known for its ability to evade detection and to encrypt data quickly. Ryuk has been used in a number of high-profile attacks, including attacks against the city of Baltimore and the Travelex currency exchange company.[137]</p> <p>Ryuk is typically spread through phishing emails and malicious attachments. Once Ryuk has infected a computer, it encrypts all of the files on the computer and demands a ransom payment in exchange for the decryption key. Ryuk is known for its high ransom demands, which can range from hundreds of thousands of dollars to millions of dollars.</p>
Mirai	botnet	<p>Mirai is a malware that infects IoT devices running Linux and turns them into a botnet. Botnets of this kind are used by cybercriminals as tools to carry out such things as DDoS attacks, spam, phishing, and click fraud.[134]</p> <p>Mirai was first discovered in August 2016 and has since been used in some of the largest and most disruptive distributed denial-of-service (DDoS) attacks in history, including the attack on Dyn in October 2016 that disrupted major websites such as Twitter, Amazon, and Netflix</p>
Mimikatz	rootkit	<p>Mimikatz is an open-source tool that allows attackers to extract sensitive information, such as passwords and credentials, from a system's memory. It was developed by French programmer Benjamin Delpy and is French slang for "cute cats".</p> <p>Mimikatz can be used to exploit a variety of vulnerabilities in Windows systems, like: Pass-the-hash, kerberos tickets, Windows LSA secrets.</p>

Bibliography

- [1] ISA/IEC 62443. *The World's Only Consensus-Based Automation and Control Systems Cybersecurity Standards*. URL: <https://www.isa.org/standards-and-publications/isa-standards/isa-iec-62443-series-of-standards>.
- [2] acqua. *The all-in-one open source security scanner*. 2023. URL: <https://trivy.dev/>.
- [3] AlienVault. *Alien Vault Open Threat Exchange*. 2023. URL: <https://otx.alienvault.com/>.
- [4] Amazon. *Amazon Detective*. URL: <https://docs.aws.amazon.com/detective/latest/adminguide/what-is-detective.html>.
- [5] Amazon. *Amazon EventBridge*. URL: <https://aws.amazon.com/it/eventbridge/>.
- [6] Amazon. *AWS Italian Region Announcement*. 2023. URL: <https://aws.amazon.com/it/local/italy/milan/>.
- [7] Amazon. *AWS Outposts Family*. URL: <https://aws.amazon.com/it/outposts/>.
- [8] Amazon. *CloudWatch Logs Insights query syntax*. URL: https://docs.aws.amazon.com/AmazonCloudWatch/latest/logs/CWL_QuerySyntax.html.
- [9] Amazon. *Foundational data sources*. URL: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_data-sources.html.
- [10] Amazon. *Foundational data sources*. URL: https://docs.aws.amazon.com/guardduty/latest/ug/guardduty_findings.html.
- [11] Amazon. *Querying Amazon GuardDuty findings*. URL: <https://docs.aws.amazon.com/athena/latest/ug/querying-guardduty.html>.
- [12] Anomali. «Anomali Cybersecurity Insight Report - The state of Enterprise Cyber Resilience». In: (2022). URL: https://www.anomali.com/resources/whitepapers/anomali-cybersecurity-insights-report?utm_medium=document&utm_source=anomali&utm_campaign=harris-poll&utm_content=blog&cid=7014z000001Ivxt.
- [13] Ansible. *Event Driven Automation*. 2023. URL: <https://www.ansible.com/>.
- [14] AWS. *AWS Product Security*. 2023. URL: https://aws.amazon.com/products/security/?nc1=h_ls.
- [15] AWS. *AWS Security*. 2023. URL: <https://docs.aws.amazon.com/security/>.

- [16] AWS. *AWS Security Reference Architecture (AWS SRA)*. 2023. URL: <https://docs.aws.amazon.com/pdfs/prescriptive-guidance/latest/security-reference-architecture/security-reference-architecture.pdf#welcome>.
- [17] AWS. *Introduction to AWS Security*. 2020. URL: https://d1.awsstatic.com/whitepapers/Security/Intro_to_AWS_Security.pdf?did=wp_card&trk=wp_card.
- [18] AWS. *Security at the Edge: Core Principles*. 2023. URL: <https://d1.awsstatic.com/whitepapers/Security/security-at-the-edge.pdf>.
- [19] AWS. *Security Orchestration, Automation & Response (SOAR)*. 2023. URL: <https://aws.amazon.com/solutions/automations/security-orchestration-automation-response/>.
- [20] AWS. *Security Pillar - AWS Well-Architected Framework*. 2023. URL: <https://docs.aws.amazon.com/pdfs/wellarchitected/latest/security-pillar/wellarchitected-security-pillar.pdf#welcome>.
- [21] David Bianco. *Enterprise Detection & Response*. 2017. URL: <https://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html>.
- [22] Sergio Caltagirone, Andrew Pendergast, and Christopher Betz. «The diamond model of intrusion analysis». In: (2013). URL: <https://apps.dtic.mil/sti/pdfs/ADA586960.pdf>.
- [23] CertBot. *Cert Bot*. 2023. URL: <https://certbot.eff.org/>.
- [24] CleanBrowsing. *DNS Security Filter*. 2023. URL: <https://cleanbrowsing.org/filters/#step3>.
- [25] CLUSIT. «Rapporto Clusit 2023 sulla sicurezza ICT in Italia». In: (2023). URL: <https://www.clusit.it>.
- [26] CSA. *Cloud Security Alliance's Top Threats to Cloud Computing*. 2022. URL: <https://cloudsecurityalliance.org/press-releases/2022/06/07/cloud-security-alliance-s-top-threats-to-cloud-computing-pandemic-11-report-finds-traditional-cloud-security-issues-becoming-less-concerning/>.
- [27] cuckoo. *Automated Malware Analysis*. 2023. URL: <https://cuckoosandbox.org/>.
- [28] Cybersecurity and Infrastructure Security Agency (CISA). *Federal Government Cybersecurity Incident and Vulnerability Response Playbooks*. 2021. URL: https://www.cisa.gov/sites/default/files/publications/Federal_Government_Cybersecurity_Incident_and_Vulnerability_Response_Playbooks_508C.pdf.
- [29] Cybersecurity and Infrastructure Security Agency (CISA). *Understanding Ransomware Threat Actors: LockBit*. 2023. URL: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a>.
- [30] Demistio. *Cortex XSOAR Platform - Content Repository*. 2023. URL: <https://github.com/demisto/content>.
- [31] Elastic. *Distributed Search Engine*. 2023. URL: <https://www.elastic.co/about/free-and-open>.

- [32] Elastic. *Elastic SIEM*. 2023. URL: <https://www.elastic.co/blog/elastic-siem-free-open>.
- [33] ENISA. *ENISA Threat Landscape for 5G Networks Report*. 2023. URL: <https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-for-5g-networks>.
- [34] ENISA. *Minimum Security Measures for Operators of Essentials Services*. 2023. URL: <https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new/minimum-security-measures-for-operators-of-essentials-services>.
- [35] ENISA. *NIS Investments Report 2022*. 2022. URL: <https://www.enisa.europa.eu/publications/nis-investments-2022/@download/fullReport>.
- [36] ENISA. *Threat Landscape*. 2023. URL: <https://www.enisa.europa.eu/topics/cyber-threats/threats-and-trends>.
- [37] Forbes. *APT28 Aka Fancy Bear: A Familiar Foe By Many Names*. 2023. URL: <https://www.forbes.com/sites/emilsayegh/2023/02/28/apt28-aka-fancy-bear-a-familiar-foe-by-many-names/>.
- [38] Forbes. *Spotlight On APT10*. 2023. URL: <https://www.forbes.com/sites/emilsayegh/2023/02/21/spotlight-on-apt10/>.
- [39] Open Cybersecurity Schema Framework. *Open Cybersecurity Schema Framework*. 2023. URL: <https://github.com/ocsf>.
- [40] Recorded Future. *Understanding the Diamond Model of Intrusion Analysis*. 2023. URL: <https://www.recordedfuture.com/diamond-model-intrusion-analysis>.
- [41] Gartner. *Top Strategic Technology Trends for 2022: Cybersecurity Mesh*. 2023. URL: <https://www.gartner.com/en/doc/756665-cybersecurity-mesh>.
- [42] Gartner. *Worldwide IaaS Public Cloud Services Revenue*. 2023. URL: <https://www.gartner.com/en/newsroom/press-releases/2023-07-18-gartner-says-worldwide-iaas-public-cloud-services-revenue-grew-30-percent-in-2022-exceeding-100-billion-for-the-first-time>.
- [43] Google. *Anthos*. URL: <https://cloud.google.com/anthos>.
- [44] Google. *APP Security*. 2023. URL: <https://cloud.google.com/architecture/framework/security/app-security?hl=en>.
- [45] Google. *Automatic Security Operations*. 2023. URL: <https://cloud.google.com/solutions/security-analytics-and-operations?hl=en>.
- [46] Google. *Case Manipulation*. URL: <https://cloud.google.com/chronicle/docs/soar/reference/case-manipulation?hl=en>.
- [47] Google. *Compute Container Security*. 2023. URL: <https://cloud.google.com/architecture/framework/security/compute-container-security?hl=en>.
- [48] Google. *Data Security*. 2023. URL: <https://cloud.google.com/architecture/framework/security/data-security?hl=en>.

- [49] Google. *Event Threat Detection custom module overview*. URL: <https://cloud.google.com/security-command-center/docs/custom-modules-etc-overview?hl=it>.
- [50] Google. *Google*. URL: <https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-syntax>.
- [51] Google. *Google Cloud Architecture Framework*. 2023. URL: <https://cloud.google.com/architecture/framework/security?hl=en>.
- [52] Google. *Google infrastructure security design overview*. 2023. URL: <https://cloud.google.com/docs/security/infrastructure/design?hl=en>.
- [53] Google. *Google Italian Region Announcement*. 2023. URL: <https://cloud.google.com/blog/products/infrastructure/new-google-cloud-region-in-milan-italy-now-open>.
- [54] Google. *Listing security findings using the Security Command Center API*. URL: <https://cloud.google.com/security-command-center/docs/how-to-api-list-findings>.
- [55] Google. *Logging Detection*. 2023. URL: <https://cloud.google.com/architecture/framework/security/logging-detection?hl=en>.
- [56] Google. *Network Security*. 2023. URL: <https://cloud.google.com/architecture/framework/security/network-security?hl=en>.
- [57] Google. *Operationalizing Security Command Center Findings*. URL: <https://www.youtube.com/watch?v=hRIlFsr64Zo&list=PLIivdWyY5sqKd-Cu1HZ7v5RiYE8gVsM7P&index=11>.
- [58] Google. *Overview of Event Threat Detection*. URL: <https://cloud.google.com/security-command-center/docs/concepts-event-threat-detection-overview?hl=en>.
- [59] Google. *Overview of the YARA-L 2.0 language*. URL: <https://cloud.google.com/chronicle/docs/detection/yara-l-2-0-overview?hl=en>.
- [60] Google. *Siemplify Actions*. URL: <https://cloud.google.com/chronicle/docs/soar/reference/siemplify-action-module?hl=en>.
- [61] Google. *threat Detection Findings*. URL: https://cloud.google.com/security-command-center/docs/how-to-use-event-threat-detection?hl=it#investigate_findings.
- [62] Google. *View logs routed to BigQuery*. URL: <https://cloud.google.com/logging/docs/export/bigquery?hl=en>.
- [63] Google. *YARA-L: A New Detection Language for Modern Threats*. URL: <https://go.chronicle.security/hubfs/YARA-L%20overview%20White%20Paper.pdf>.
- [64] The Software House. *Open-source GDPR-friendly data masking tool*. 2023. URL: <https://tsh.io/blog/fogger-open-source-free-tool-gdpr-data-masking/>.
- [65] Git Hub. *The AI-powered developer platform to build, scale and deliver secure software*. 2023. URL: <https://github.com/>.

- [66] SANS Institute. *Incident Handler's Handbook*. 2012. URL: <https://www.sans.org/white-papers/33901/>.
- [67] ISC². *ISC² Cybersecurity Workforce Study 2022*. 2022. URL: <https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2-Cybersecurity-Workforce-Study-2022.pdf>.
- [68] ISO/IEC. *Cloud Security Alliance*. 2022. URL: <https://cloudsecurityalliance.org/research/cloud-controls-matrix/>.
- [69] ISO/IEC. *Information security management systems - Requirements*. 2022. URL: <https://www.iso.org/standard/27001>.
- [70] ISO/IEC. *Information security management systems - Requirements*. 2022. URL: <https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-3:en>.
- [71] CERTFIN CERT Finanziario Italiano. *CERTFIN - CERT Finanziario Italiano*. URL: <https://www.certfin.it/>.
- [72] Jenkins. *Continuous Integration Continuous Delivery*. 2023. URL: <https://www.jenkins.io/>.
- [73] Jit. *OWASP ZAP*. 2023. URL: https://www.jit.io/zap?_gl=1*3ea21k*_up*MQ..&gclid=CjwKCAjwseSoBhBXEiwA9iZtxrxsPLpifiXIWXiNl8S0_f2X5c_E3EE9iQh6VWMNagpS33f6vD1yUxoCWD8QAvD_BwE.
- [74] Key-Cloak. *Open Source Identity and Access Management*. 2023. URL: <https://www.keycloak.org/>.
- [75] Kong. *Take Control of Your Kubernetes Clusters*. 2023. URL: <https://konghq.com/solutions/build-on-kubernetes>.
- [76] John Lambert. *Defenders think in lists. Attackers think in graphs. As long as this is true, attackers win*. 2018. URL: <https://github.com/JohnLaTWC/Shared/blob/master/Defenders%20think%20in%20lists.%20Attackers%20think%20in%20graphs.%20As%20long%20as%20this%20is%20true%2C%20attackers%20win.md>.
- [77] letsencrypt. *Let's Encrypt*. 2023. URL: <https://www.letsencrypt.org/>.
- [78] Lockheed Martin. *The Cyber Kill Chain*. 2013. URL: <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html#:~:text=Developed%20by%20Lockheed%20Martin%2C%20the,order%20to%20achieve%20their%20objective>.
- [79] Microsoft. *Azure Security Fundamentals*. 2023. URL: <https://learn.microsoft.com/en-us/azure/security/fundamentals/overview>.
- [80] Microsoft. *Azure Sentinel deploy*. 2023. URL: <https://github.com/Azure/Azure-Sentinel/tree/master/ASIM>.
- [81] Microsoft. *Azure Stack Documentation*. URL: <https://learn.microsoft.com/en-us/azure-stack/>.
- [82] Microsoft. *Detect threats out-of-the-box*. 2023. URL: <https://learn.microsoft.com/en-us/azure/sentinel/detect-threats-built-in>.

- [83] Microsoft. *Enterprise access model*. 2023. URL: <https://learn.microsoft.com/en-us/security/privileged-access-workstations/privileged-access-access-model>.
- [84] Microsoft. *Importing Sigma Rules to Azure Sentinel*. URL: <https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/importing-sigma-rules-to-azure-sentinel/ba-p/657097>.
- [85] Microsoft. *Kusto Query Language in Microsoft Sentinel*. 2023. URL: <https://learn.microsoft.com/en-us/azure/sentinel/kusto-overview>.
- [86] Microsoft. *Microsoft GitHub Sentinel repository*. 2023. URL: <https://github.com/Azure/Azure-Sentinel/tree/master/Playbooks>.
- [87] Microsoft. *Microsoft Italian Region Announcement*. 2023. URL: <https://news.microsoft.com/it-it/2023/06/05/microsoft-annuncia-oggi-la-prima-cloud-region-in-italia-per-accelerare-linnovazione-e-l-opportunita-di-crescita-economica-del-paese/>.
- [88] Microsoft. *Network Threat Protection Essentials*. 2023. URL: <https://azuremarketplace.microsoft.com/it-IT/marketplace/apps/azuresentinel.azure-sentinel-solution-networkthreatdetection?tab=Overview>.
- [89] Microsoft. *Normalization and the Advanced Security Information Model (ASIM)*. 2023. URL: <https://learn.microsoft.com/it-it/azure/sentinel/normalization>.
- [90] MITRE. *APT38*. 2023. URL: <https://attack.mitre.org/groups/G0082/>.
- [91] MITRE. *Cloud Matrix*. 2023. URL: <https://attack.mitre.org/matrices/enterprise/cloud/>.
- [92] Mitre. *Defend - A knowledge graph of cybersecurity contermesures*. 2023. URL: <https://d3fend.mitre.org/>.
- [93] MITRE. *Kimsuky*. 2023. URL: <https://attack.mitre.org/groups/G0094/>.
- [94] Mitre. *Mitre att&ck flow*. 2023. URL: <https://center-for-threat-informed-defense.github.io/attack-flow/>.
- [95] Mitre. *Mitre Att&ck flow builder*. 2023. URL: <https://center-for-threat-informed-defense.github.io/attack-flow/ui/>.
- [96] MITRE. *MITRE ATT@CK Matrices*. 2013. URL: <https://attack.mitre.org/matrices/enterprise/>.
- [97] MITRE. *MITRE ENGENUITY*. 2023. URL: <https://mitre-engenuity.org/>.
- [98] MyDiamo. *The First Comprehensive DB Encryption for MySQL, MariaDB and Percona*. 2023. URL: <https://mydiamo.com/>.
- [99] CNSS Committee on National Security Systems. *CATEGORIZATION AND CONTROL SELECTION FOR NATIONAL SECURITY SYSTEMS*. 2014. URL: <https://www.cnss.gov/CNSS/issuances/Instructions.cfm>.
- [100] The Hacker News. *How to Interpret the 2023 MITRE ATT&CK Evaluation Results*. 2023. URL: <https://thehackernews.com/2023/09/how-to-interpret-2023-mitre-att.html>.

-
- [101] NGINX. *WAF - Web Application Firewall*. 2023. URL: <https://www.nginx.com/learn/waf-web-application-firewall/>.
- [102] NIST. *NIST Cyber Security Framework 2.0*. 2023. URL: <https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd>.
- [103] OpenC2. *Open Command and Control*. 2023. URL: <https://openc2.org/>.
- [104] OpenScap. *Open SCAP (Security Content Automation Protocol)*. 2023. URL: <https://www.open-scap.org/>.
- [105] OpenSSL. *OpenSSL*. 2023. URL: <https://www.openssl.org/>.
- [106] OpenStack. *OpenStack Magnum*. 2023. URL: <https://docs.openstack.org/magnum/latest/>.
- [107] OSSEC. *Host Intrusion Detection for Everyone*. 2023. URL: <https://www.ossec.net/ossec-downloads/>.
- [108] OSSEM. *Open Source Security Event Metadata*. 2023. URL: <https://github.com/OTRF/OSSEM>.
- [109] Owasp. *OWASP Dependency-Check*. 2023. URL: <https://owasp.org/www-project-dependency-check/>.
- [110] EUROPEAN PARLIAMENT and OF THE COUNCIL. *Digital Operational Resilience Act*. 2022. URL: <https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2554>.
- [111] PicusSecurity. *What Is Advanced Persistent Threat (APT)?* 2023. URL: [https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt#:~:text=APT41%20\(also%20known%20as%20Wicked,espionage%20and%20financially%20motivated%20operations..](https://www.picussecurity.com/resource/glossary/what-is-advanced-persistent-threat-apt#:~:text=APT41%20(also%20known%20as%20Wicked,espionage%20and%20financially%20motivated%20operations..)
- [112] Rapid7. *Advanced Persistent Threat Groups*. 2023. URL: <https://docs.rapid7.com/insightidr/apt-groups/#apt40>.
- [113] Jorge Orchilles SANS. *Cyber Kill Chain, MITRE ATT&CK and Purple Team*. 2022. URL: <https://www.sans.org/blog/cyber-kill-chain-mitre-attack-purple-team/>.
- [114] sekoia. *APT29 aka Nobelium, Cozy Bear*. 2020. URL: [https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/#:~:text=Nobelium%2C%20also%20known%20as%20APT29,Service%20of%20the%20Russian%20Federation\)..](https://www.sekoia.io/en/glossary/apt29-aka-nobelium-cozy-bear/#:~:text=Nobelium%2C%20also%20known%20as%20APT29,Service%20of%20the%20Russian%20Federation)..)
- [115] MISP Threat Sharing. *Open Source Threat Intelligence and Sharing Platform*. URL: <https://www.misp-project.org/>.
- [116] SIEGMA. *Automate the creation of SIEM rule consumables*. URL: <https://github.com/3CORESec/SIEGMA>.
- [117] SigmaHQ. *Sigma*. URL: <https://github.com/SigmaHQ/sigma>.
- [118] Sonar. *SonarQube Community Edition*. 2023. URL: https://www.sonarsource.com/open-source-editions/sonarqube-community-edition/?gads_campaign=SQ-Hroi-PMax&gads_ad_group=Global&gads_keyword=&gclid=CjwKCAjwseSoBhBXEiwA9iZtxiaHJOBwE.

- [119] International Organization for Standardization (ISO). *Information technology - Security techniques - Security incident management - Part 1: Overview and concepts*. 2016. URL: <https://www.iso.org/standard/60803.html>.
- [120] National Institute of Standards and Technology (NIST). *Computer Security Incident Handling Guide*. 2012. URL: <https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf>.
- [121] National Institute of Standards and Technology (NIST). *Zero trust architecture*. 2020. URL: <https://csrc.nist.gov/pubs/sp/800/207/final>.
- [122] National Institute of Standards and Technology. *Control Baselines for Information Systems and Organizations*. 2022. URL: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf>.
- [123] Stix. *Structured Threat Information Expression*. 2023. URL: <https://docs.oasis-open.org/cti/stix/v2.1/csprd01/stix-v2.1-csprd01.html>.
- [124] Synopsis. *2023 OSSRA deep dive: jQuery and open source security*. 2023. URL: <https://www.synopsys.com/blogs/software-security/deep-dive-2023-ossra-report.html#:~:text=According%20to%20the%202023%20%E2%80%9COpen,Audit%20Services%20was%20open%20source..>
- [125] Techtarget. *Trickbot malware*. 2023. URL: <https://www.techtarget.com/searchsecurity/definition/TrickBot-malware>.
- [126] TechTarget. *WannaCry malware*. 2023. URL: <https://www.techtarget.com/searchsecurity/definition/WannaCry-ransomware>.
- [127] Terraform. *Deliver infrastructure as code*. 2023. URL: <https://certbot.eff.org/>.
- [128] MITRE CTID Center for Threat Informed Defense. *Sightings Ecosystem*. 2022. URL: https://github.com/center-for-threat-informed-defense/sightings_ecosystem.
- [129] OASIS Open Moses Tim. *eXtensible Access Control Markup Language Version 2 Core Spec*. 2005. URL: <https://docs.oasis-open.org/xacml/2.0/access-control-xacml-2.0-core-spec-os.pdf>.
- [130] Wikipedia. *Anonymous (hacker group)*. 2023. URL: [https://en.wikipedia.org/wiki/Anonymous_\(hacker_group\)](https://en.wikipedia.org/wiki/Anonymous_(hacker_group)).
- [131] Wikipedia. *Emotet*. 2023. URL: <https://en.wikipedia.org/wiki/Emotet>.
- [132] Wikipedia. *Lazarus (hacker group)*. 2023. URL: https://en.wikipedia.org/wiki/Lazarus_Group.
- [133] Wikipedia. *LulzSec*. 2023. URL: <https://en.wikipedia.org/wiki/LulzSec>.
- [134] Wikipedia. *Mirai (malware)*. 2023. URL: [https://it.wikipedia.org/wiki/Mirai_\(malware\)](https://it.wikipedia.org/wiki/Mirai_(malware)).
- [135] Wikipedia. *Principio di antifragilità*. 2023. URL: https://it.wikipedia.org/wiki/Principio_di_antifragilit%C3%A0.
- [136] Wikipedia. *REvil (ransomware group)*. 2023. URL: <https://en.wikipedia.org/wiki/REvil>.

BIBLIOGRAPHY

- [137] Wikipedia. *Ryuk*. 2023. URL: [https://en.wikipedia.org/wiki/Ryuk_\(ransomware\)](https://en.wikipedia.org/wiki/Ryuk_(ransomware)).
- [138] Wikipedia. *Sandworm (hacker group)*. 2023. URL: [https://en.wikipedia.org/wiki/Sandworm_\(hacker_group\)](https://en.wikipedia.org/wiki/Sandworm_(hacker_group)).