POLITECNICO DI TORINO

Corso di Laurea in Ingegneria Informatica

Tesi di Laurea

Integrazione di Nozomi Networks e Splunk per la raccolta e l'analisi di dati provenienti da dispositivi di tipo OT e IoT

Relatori
Prof. Guido Marchetto
Ing. Alessio Sacco

Candidato
Simone Totaro

Anno accademico 2022-2023

Indice

Capitolo 1

Introduzione

1.1 Evoluzione della complessità nei sistemi informatici

Negli ultimi anni si è assistito a un significativo aumento della complessità dei sistemi informatici. Questo fenomeno è stato determinato da diversi fattori, quali l'avanzamento tecnologico e l'introduzione di nuove tecnologie, l'aumento di scala dei sistemi, composti da un numero sempre maggiore di dispositivi di vario genere, le sempre più sofisticate minacce informatiche e la presenza di dati eterogenei provenienti da diverse fonti. Vi è dunque la necessità di un approccio integrato per gestire tale complessità e garantire un adeguato livello di sicurezza nei sistemi.

Per affrontare queste problematiche diventa essenziale combinare strumenti avanzati per la raccolta e l'analisi dei dati all'interno delle infrastrutture di un'organizzazione. Nel contesto di questa tesi, ci concentriamo sull'integrazione di due soluzioni, Nozomi Networks e Splunk, per affrontare questa sfida.

Nozomi Networks è un potente strumento specializzato nella sicurezza industriale, in grado di raccogliere dati da un'ampia varietà di fonti, tra cui dispositivi OT e IoT. Splunk, d'altra parte, offre potenti funzionalità di analisi e visualizzazione dei dati, consentendo una comprensione approfondita delle informazioni di sicurezza.

1.2 Obiettivi e scopo della tesi

L'obiettivo di questo lavoro è quindi quello di integrare le piattaforme di Nozomi Networks e Splunk, sfruttando le loro rispettive capacità per la raccolta, l'analisi e la visualizzazione dei dati di sicurezza. Attraverso questa integrazione, ci proponiamo di migliorare l'efficienza nella gestione e nella sicurezza dei dati all'interno delle infrastrutture, consentendo una migliore comprensione dei dati e una più rapida identificazione di eventuali minacce o vulnerabilità.

La seguente tesi è stata svolta in collaborazione con Alten Italia SPA, società di consulenza e ingegneria che fornisce servizi di sviluppo e integrazione di soluzioni tecnologiche per diverse industrie, tra cui automotive, aerospaziale, difesa, telecomunicazioni, energia e industria farmaceutica.

Tipologia dei dati da analizzare

Con Nozomi Networks è possibile raccogliere una vasta gamma di dati relativi alla sicurezza e alle prestazioni delle reti industriali, inclusi dati su traffico di rete, vulnerabilità, attività degli utenti, allarmi di sicurezza e diagnostica di sistema. Nello specifico verrà utilizzata la piattaforma Nozomi Networks Guardian all'interno di un ambiente di laboratorio costituito da macchine virtuali VMWare per la raccolta dei dati sopracitati e dati relativi al traffico di rete in ingresso e in uscita dalle macchine virtuali, inclusi i protocolli utilizzati e la quantità di dati scambiati. Inoltre, Guardian può identificare le vulnerabilità delle macchine e generare allarmi di sicurezza in caso di attività sospette.

I dati vengono inviati a Splunk tramite una fase di integrazione delle due piattaforme e successivamente elaborati e visualizzati tramite l'app InfoSec di Splunk e un'app dedicata, chiamata "Nozomi App". Per rendere possibile la visualizzazione su InfoSec, i dati devono essere mappati conformemente ad uno standard denominato "Common Information Model" (CIM).

Risultati attesi

Con il seguente lavoro di tesi si vuole dimostrare che l'utilizzo congiunto di queste piattaforme possa garantire una gestione e una sicurezza dei dati più efficienti all'interno di un'infrastruttura, grazie ad una migliore comprensione ed analisi dei dati stessi tramite le due applicazioni di Splunk, ovvero Infosec e Nozomi App.
Queste applicazioni includono dashboard appositamente create per il monitoraggio della rete, il rilevamento di intrusioni, la segnalazione di malware, nonché per la visualizzazione degli asset, delle sessioni di rete, degli allarmi e delle vulnerabilità individuate. Tali dashboard consentono di accedere rapidamente alle informazioni chiave necessarie per comprendere lo stato della rete e per prendere decisioni informate sulla sicurezza.

Infine attraverso la piattaforma Splunk Security Essentials verrà adoperato il MITRE ATT&CK Framework, un modello di riferimento che definisce un'ampia gamma di tattiche e tecniche utilizzate dagli aggressori durante un attacco informatico. Con tale framework verranno create ricerche personalizzate in Splunk per l'identificazione di eventuali minacce, segnalate tramite la generazione di allarmi utilizzando la piattaforma Splunk Enterprise Security e visualizzate attraverso le applicazioni sopracitate.

Utilizzando tale framework in Splunk è possibile rilevare diversi tipi di attacchi, per monitorare ad esempio attività sospette di malware, come download di file dannosi, attività di movimento laterale all'interno della rete, come tentativi di passaggio da un host compromesso a un altro, oppure tentativi di "privilege escalation", ovvero sforzi per ottenere accessi privilegiati all'interno del sistema. Quando vengono rilevate attività sospette è possibile impostare diverse reazioni per gestire tali situazioni in base alle proprie esigenze, ad esempio notifiche automatiche agli amministratori di sistema, blocco degli indirizzi IP sospetti, ecc.

In questa tesi il MITRE ATT&CK Framework verrà utilizzato per rilevare tentativi di attacchi "brute force" e attività di tipo "network scanning" sui dati raccolti da Nozomi Networks. Il rilevamento di tali attività causerà la generazione di allarmi e l'invio di email automatiche agli amministratori di sistema.

Capitolo 2

Nozomi Networks: sicurezza e visibilità nei sistemi OT e IoT

2.1 Introduzione a Nozomi Networks

Nozomi Networks ha ottenuto una notevole crescita negli ultimi anni, proteggendo un grande numero di dispositivi su diverse installazioni. Mantenendosi leader di mercato nei settori Oil & Gas, Pharma, Mining e Utilities, Nozomi continua ad aumentare la propria presenza anche in nuovi mercati, in considerazione della sempre più evidente convergenza tra i sistemi OT e IoT. Tale convergenza rappresenta un processo che sta accelerando rapidamente e che coinvolge tutti i settori che si basano su reti di controllo industriale per le proprie attività. Questo comporta dunque un rischio per molte reti non protette.

Il problema che si riscontra principalmente è la mancanza di visibilità all'interno delle proprie infrastrutture, causato dalla sempre più crescente complessità delle reti industriali per via dell'aumento costante dei dispositivi collegati alla rete. Questo naturalmente determina una maggiore superficie di attacco, ovvero il numero di punti di accesso attraverso i quali un potenziale attaccante potrebbe tentare di infiltrarsi nel sistema. Questo rende più difficile proteggere efficacemente il sistema, soprattutto se non c'è una visibilità adeguata su tutta la rete. In questo contesto, Nozomi offre quindi una tecnologia molto avanzata che garantisce visibilità e sicurezza informatica in tutti i tipi di reti OT e IoT [1].

2.2 Operational Technology e l'Internet of Things

2.2.1 Sistemi OT e il Modello Purdue

I sistemi OT (Operational Technology) sono una componente vitale per il controllo e la gestione di numerosi settori che influenzano la vita quotidiana. Essi si estendono ai servizi idrici ed elettrici, ai sistemi di trasporto, alla produzione, alla logistica, ai prodotti farmaceutici, ai sistemi petroliferi e del gas, persino ai sistemi semaforici alla fine delle strade.
Ad esempio, nei servizi idrici ed elettrici i sistemi OT controllano le reti di distribuzione per fornire acqua e energia in modo efficiente. Nei sistemi di trasporto invece gestiscono il flusso del traffico, controllano i semafori e monitorano i sistemi ferroviari.

I sistemi OT sono noti con diversi nomi, come sistemi ICS (Industrial Control Systems), sistemi SCADA (Supervisory Control And Data Acquisition), sistemi DCS (Distributed Control Systems) o sistemi di telemetria, tuttavia, i componenti terminali di base rimangono gli stessi.

Il controller industriale è il dispositivo terminale principale di tutti i sistemi OT. Questi computer specializzati eseguono programmi che consentono il monitoraggio, la raccolta di dati e il controllo delle operazioni in tempo reale. Inoltre gestiscono e ottimizzano la produzione, garantendo l'efficienza e la sicurezza dei processi. Essi si basano su input provenienti dai sensori e applicano output di comando ai dispositivi di controllo, garantendo il corretto funzionamento delle macchine e dei processi. Gli input possono essere digitali, come interruttori on/off o lo stato di funzionamento di un motore, o valori analogici, come la profondità dell'acqua in un serbatoio. Allo stesso modo, le uscite possono essere digitali, come comandi per accendere o spegnere un generico trasportatore di bagagli, o analogiche, come comandi per accelerare un motore.

Il Modello Purdue

Il modello Purdue (Figura 2.1) è un modello strutturale per la sicurezza dei sistemi di controllo industriali che riguarda la segmentazione di processi fisici, sensori, controlli di supervisione, operazioni e logistica [2]. Questo modello definisce una struttura di riferimento per l'organizzazione dei sistemi di controllo industriali all'interno di un'infrastruttura di produzione, mostrando come gli elementi tipici di un'architettura ICS si interconnettono, dividendoli in sei zone che contengono sistemi IT e OT. Il modello è organizzato in livelli funzionali, ognuno dei quali ha una specifica responsabilità.

Il **livello 4/5** ospita la tipica rete IT, dove vengono svolte le principali funzioni aziendali. Include dunque le varie workstations, PC e server di vario genere.

Tra i livelli 3 e 4 vi è il **livello 3.5**, detto anche "DMZ" (Zona Demilitarizzata), per soddisfare la necessità di flussi di dati bidirezionali tra i sistemi OT e IT per via dell'aumento dell'automazione. Tale livello include sistemi di sicurezza come firewall e proxy, utilizzati nel tentativo di impedire il movimento laterale delle minacce tra IT e OT.

Il **livello 3** contiene dispositivi OT personalizzati che gestiscono i flussi di lavoro di produzione. In particolare, vi sono sistemi per la gestione delle operazioni di produzione, sistemi per la raccolta di dati in tempo reale e gli storici dei dati per l'archiviazione e l'analisi dei dati di processo.

Al **livello 2** sono presenti sistemi per la supervisione, monitoraggio e controllo dei processi fisici. Innanzitutto abbiamo le "operator" ed "engineering" workstations. Le prime, dette anche Human Machine Interfaces (HMI), forniscono agli operatori una visualizzazione grafica e tabellare di ciò che sta accadendo all'interno del processo industriale, oltre a consentire un livello di controllo. Le seconde vengono invece utilizzate per apportare modifiche al sistema di automazione.
Vi è poi il software SCADA (Supervisory Control and Data Acquisition) che supervisiona e controlla i processi fisici, localmente o da remoto, e aggrega i dati da inviare agli storici.

Il **livello 1** è costituito dai controller industriali veri e propri, che sono dispositivi in grado di inviare comandi ai dispositivi presenti al livello inferiore (livello 0). Tra i controller industriali si possono trovare i controllori logici programmabili (PLC), che monitorano gli input nei processi industriali e apportano modifiche all'output.

La zona finale, ovvero il **livello 0**, contiene sensori, attuatori e altri macchinari.

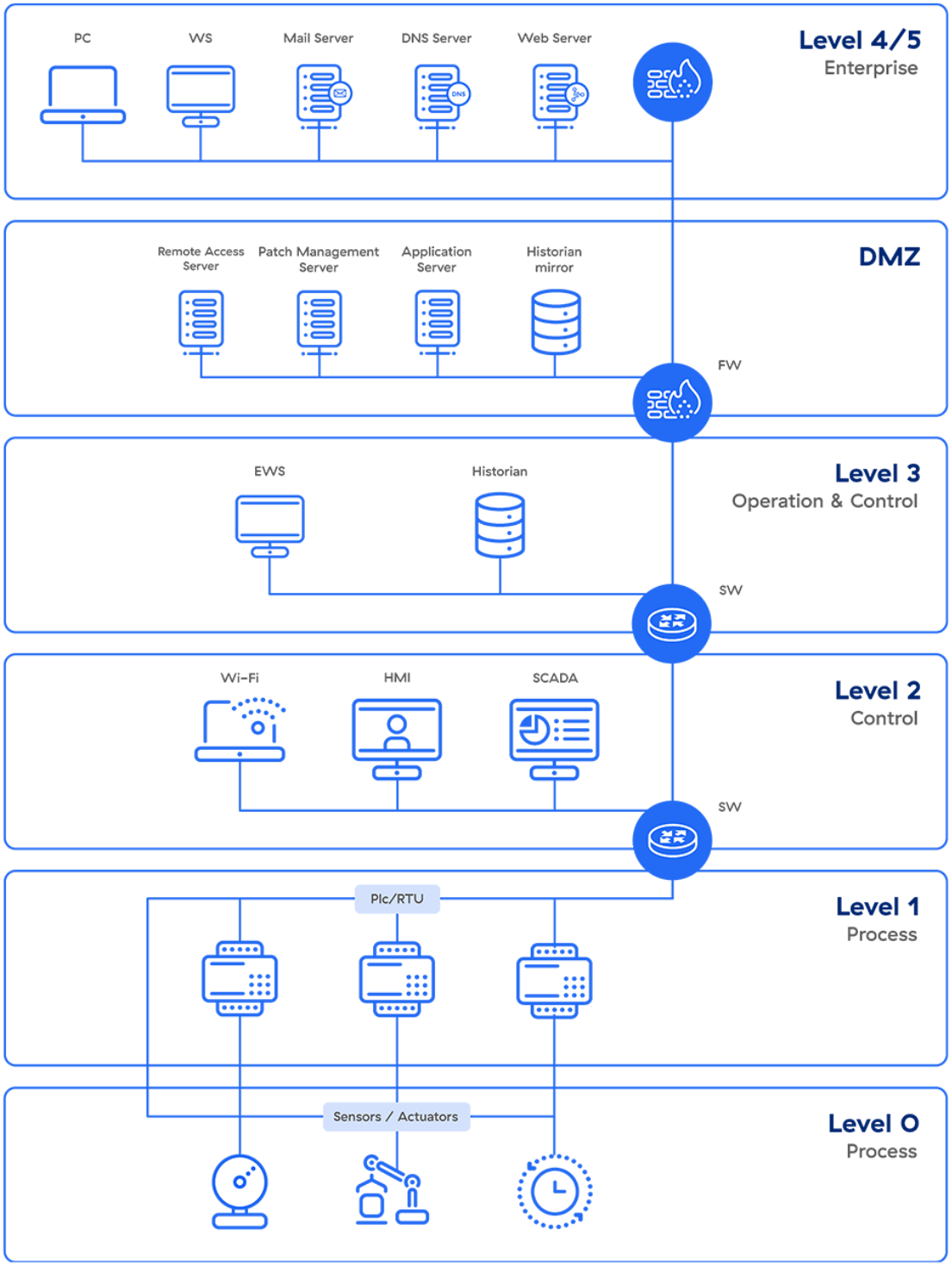


Figura 2.1. Modello Purdue [2]

2.2.2 Internet of Things e Industrial Internet of Things

Internet of Things (IoT) è un concetto tecnologico che si riferisce alla connessione di dispositivi fisici, come sensori, telecamere, veicoli e altri oggetti, alla rete Internet, consentendo a tali dispositivi di comunicare tra loro e con altri sistemi attraverso la raccolta e lo scambio di dati in tempo reale [3].

L'IoT fa riferimento principalmente a una rete costituita da dispositivi di uso quotidiano, come elettrodomestici, smartwatch, assistenti virtuali, ma viene anche impiegato per migliorare le infrastrutture attraverso l'utilizzo di sensori intelligenti per la raccolta di dati sull'ambiente circostante, sulle condizioni degli oggetti o sul comportamento degli utenti. Questi dati vengono quindi trasmessi attraverso reti di comunicazione (come Wi-Fi, Bluetooth o reti cellulari) a piattaforme o servizi di cloud computing, dove vengono elaborati, analizzati e utilizzati per prendere decisioni o attuare azioni.

Questa connessione e comunicazione tra i dispositivi abilitati all'IoT consente di creare nuove opportunità di automazione, efficienza e miglioramento delle prestazioni in diversi settori, come l'industria, la salute, l'agricoltura, il trasporto, la casa intelligente e molti altri. Le città intelligenti ("smart cities") ad esempio integrano sensori nelle infrastrutture per migliorare la manutenzione, aumentare l'efficienza e consentire operazioni remote. Questo approccio coinvolge diverse componenti, come l'illuminazione stradale, le reti idriche, le strade e i sistemi di trasporto. Un caso d'uso potrebbe essere l'installazione di timer e sensori di movimento nelle luci stradali, consentendo alle città intelligenti di programmare l'accensione in base alle condizioni di luce o alla presenza di persone.

Nell'attuale contesto è possibile parlare anche di **Industrial Internet of Things (IIoT)**, ovvero una sottocategoria specifica dell'IoT che si applica all'ambito industriale. L'IIoT coinvolge l'uso di dispositivi intelligenti e connessi nelle industrie per ottimizzare le operazioni e migliorare l'efficienza produttiva. Questa tecnologia è una componente chiave dell'Industria 4.0, che rappresenta una nuova fase della rivoluzione industriale [4].

Come per l'IoT, è possibile integrare sensori intelligenti su macchinari di produzione, sistemi energetici e infrastrutture come tubazioni e cavi. Questi sensori, grazie alla raccolta dei dati e alle funzioni avanzate che offrono, possono aiutare le attività industriali a migliorare l'efficienza, la produttività, la sicurezza del personale e molto altro.

I dispositivi IIoT sono progettati per fornire agli utenti informazioni sui loro macchinari e si integrano con le attrezzature esistenti, piuttosto che funzionare indipendentemente. Esempi di questi dispositivi includono controllori e controllori logici programmabili.

Le tecnologie IIoT supportano anche l'implementazione di programmi di manutenzione predittiva per migliorare l'efficienza operativa. Ciò implica il monitoraggio delle condizioni e delle prestazioni degli impianti per prevedere potenziali guasti. Grazie ai sensori intelligenti, gli operatori possono ottenere informazioni dettagliate sulle condizioni delle macchine e prevedere guasti in modo più tempestivo ed accurato. Possono anche ricevere notifiche di anomalie operative e potenziali problemi.

Considerazioni sulla sicurezza

Nonostante i numerosi vantaggi che l'IoT offre, esso solleva questioni di sicurezza, privacy e gestione dei dati, poiché coinvolge una vasta gamma di dispositivi e la condivisione di informazioni personali o sensibili.

A differenza dell'IoT, i dispositivi IIoT e il malfunzionamento della tecnologia possono essere più pericolosi, poiché l'IIoT è connesso in rete e potrebbe causare situazioni pericolose in caso di guasto di un macchinario pesante. Molte aziende utilizzano ancora sistemi e processi legacy, e le nuove tecnologie possono complicare l'integrazione e la sicurezza end-to-end.

L'aumento dei dispositivi intelligenti, in particolare i dispositivi dei dipendenti utilizzati per il lavoro, danno luogo a una moltitudine di vulnerabilità della sicurezza. Le organizzazioni sono responsabili dell'implementazione e della configurazione sicura di tutti i dispositivi connessi. Ma i produttori di dispositivi devono anche dimostrare di poter mantenere i dispositivi sicuri, cosa che spesso non avviene.

Problemi di sicurezza derivati dall'uso di queste tecnologie potrebbero essere le porte esposte, la mancanza di pratiche di autenticazione sufficienti o anche l'uso di applicazioni obsolete. Tutti questi piccoli problemi possono essere pericolosi per le aziende, in quanto sistemi non protetti possono provocare interruzioni operative e perdite finanziarie.

Risulta quindi fondamentale adottare misure di sicurezza adeguate per proteggere i dispositivi IoT e IIoT e garantire la privacy e la sicurezza dei dati. A questo scopo, Nozomi fornisce visibilità e sicurezza per queste categorie di sistemi.

2.3 Funzionalità e caratteristiche di Nozomi Networks

La piattaforma Nozomi Networks offre diverse funzionalità essenziali per proteggere le infrastrutture critiche e per consentire ai clienti di prendere decisioni informate riguardo i loro ambienti [5].

Asset Inventory

Una delle funzionalità principali di Nozomi Networks è l'Asset Inventory, la quale permette di identificare e catalogare tutti gli asset presenti nella rete industriale. Questa funzionalità fornisce una panoramica dettagliata di tutti i dispositivi e le loro caratteristiche, consentendo una gestione efficace e una maggiore visibilità sulla rete.
Nozomi è in grado di individuare i dispositivi terminali OT, come controller industriali, operator workstations e engineering workstations, attraverso un monitoraggio passivo del traffico di rete. Sfruttando la sua approfondita conoscenza dei protocolli industriali utilizzati per la comunicazione, Nozomi è in grado di estrarre informazioni come marca, modello, numero di serie e versione del firmware senza l'utilizzo di agenti.

Vulnerability Matching

Dopo aver completato la scoperta dell'inventario delle risorse, Nozomi confronta le informazioni sui dispositivi rilevati con un database di vulnerabilità noto come "Common Vulnerabilities and Exposures" (CVE). Questo confronto consente di identificare i dispositivi installati che presentano vulnerabilità note e valutarne la gravità. Nozomi aggrega

informazioni sulle vulnerabilità da diversi fonti affidabili, tra cui database nazionali sulle vulnerabilità, fornitori, comunità di sicurezza informatica e ricerca originale condotta presso i Nozomi Labs in Svizzera.

Process Variable Tracking

La funzionalità di Process Variable Tracking è fondamentale per il monitoraggio dei sistemi, infatti Nozomi analizza costantemente le variabili di processo scambiate dai vari dispositivi, consentendo di rilevare eventuali comportamenti anomali che potrebbero indicare un attacco informatico o un malfunzionamento del sistema.

Known Threat Detection

Nozomi offre due approcci per il rilevamento delle minacce note: il primo approccio si basa sulla logica integrata in ogni sensore Guardian, che consiste nella ricerca di comportamenti dannosi noti, come scansioni delle porte, attacchi "man in the middle" e l'uso di password predefinite. Inoltre, monitora operazioni potenzialmente pericolose, come modifiche ai programmi in esecuzione sui controllori industriali.

Il secondo approccio sfrutta l'uso delle "firme", ovvero pattern o regole specifiche che vengono utilizzate per rilevare specifici tipi di minacce o comportamenti dannosi nei pacchetti di dati che transitano all'interno della rete OT. Queste firme vengono dunque confrontate con ogni comunicazione che avviene all'interno della rete, cercando corrispondenze di malware all'interno dei file trasferiti e indicatori che riflettono la reputazione informatica dei siti esterni contattati dai dispositivi. Le firme vengono create dai laboratori Nozomi e aggiornate costantemente per garantire un rilevamento accurato delle minacce.

Unknown Threat Detection

Nozomi rileva l'uso di minacce sconosciute cercando comportamenti anomali del sistema, definendo inizialmente il funzionamento normale, ad esempio quali dispositivi esistono nel sistema, quali parlano tra loro, la frequenza delle comunicazioni o quali protocolli industriali vengono utilizzati. Successivamente, Nozomi cerca qualsiasi deviazione dal comportamento base, ad esempio un nuovo PC che si connette alla rete o un dispositivo avvia una nuova comunicazione con un altro.

Poiché il funzionamento del sistema è monitorato fino al livello delle variabili di processo (input e output discussi in precedenza), Nozomi è in grado di rilevare sottili cambiamenti nel modo in cui due dispositivi comunicano. Ad esempio: il dispositivo A, che di solito legge solamente dal dispositivo B, improvvisamente inizia a scrivere tale dispositivo B.

Operational Insights

Questa funzionalità offre analisi avanzate sui dati raccolti, fornendo informazioni sulle prestazioni dei dispositivi e sui processi in corso. Nell'interfaccia Guardian, gli asset del sistema vengono visualizzati attraverso una mappa interattiva e forniscono informazioni sia di alto che di basso livello sul sistema esistente. Possiamo ottenere informazioni utili sulle cause del malfunzionamento di un sistema analizzando i dispositivi che hanno smesso di comunicare o comunicano meno spesso, osservando livelli elevati di ritrasmissioni o throughput di dati superiori o inferiori a quelli previsti.

Smart Polling

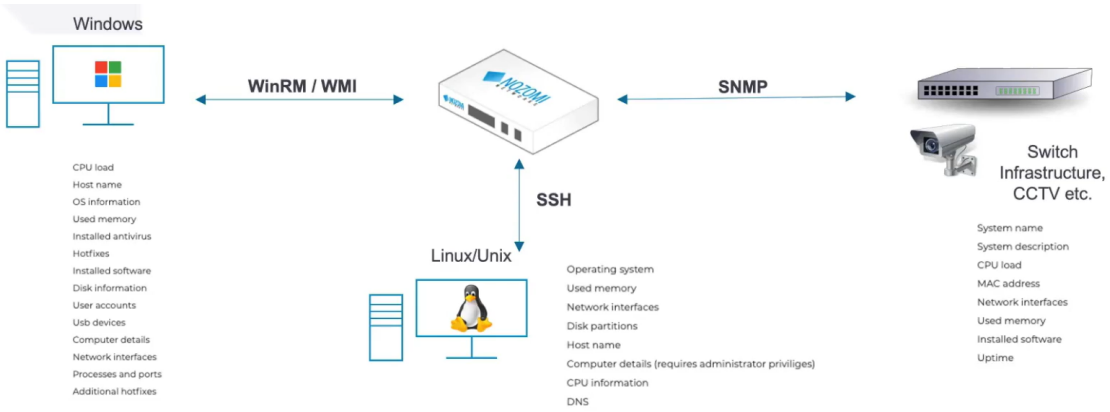


Figura 2.2. Esempi di Smart Polling [5]

Le funzionalità finora descritte si basano sull'ascolto passivo del traffico di rete tramite mirroring delle porte, senza l'utilizzo di alcun agente o query attiva. Tuttavia, Nozomi può migliorare le informazioni raccolte passivamente utilizzando query attive mirate attraverso lo "Smart Polling", ovvero una funzionalità che consiste nell'interrogare i dispositivi terminali selezionati utilizzando i loro protocolli nativi.

Un uso comune di Smart Polling è quello di migliorare le vulnerabilità segnalate associate a macchine Windows, come le operator e engineering workstations. Passivamente, Nozomi può identificare il tipo di sistema operativo e il livello del service pack, come "Windows XP Service Pack 3" e segnalare le vulnerabilità ad esso associate. Tuttavia, utilizzando lo Smart Polling, il Nozomi Guardian Sensor può interrogare specifiche macchine Windows per determinare quali patch sono state applicate e quindi quali vulnerabilità sono già state risolte, non possibile attraverso il solo monitoraggio passivo.

Strategie simili possono essere utilizzate per migliorare le informazioni raccolte da altri dispositivi, come macchine Linux, controller industriali, switch di rete, firewall, telecamere CCTV, ecc.

Architettura

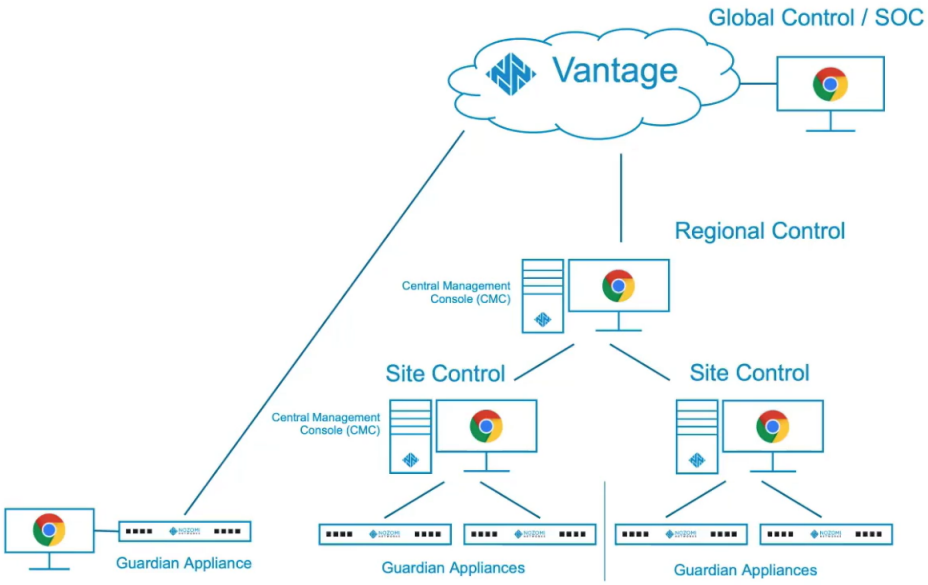


Figura 2.3. Architettura scalabile [5]

Nozomi ha sviluppato un'architettura flessibile e ampiamente scalabile per soddisfare la vasta gamma di aziende industriali, dalle piccole imprese che operano in un unico sito alle imprese multinazionali.

L'implementazione più semplice comprende un singolo Guardian Sensor senza alcuna interconnettività. Altre implementazioni utilizzano più sensori Guardian piccoli, piuttosto che un singolo sensore più grande, nel qual caso è possibile implementare una Nozomi Central Management Console (CMC) per aggregare i dati dai singoli sensori. Tutta l'elaborazione relativa all'Asset Discovery, Vulnerability Matching e Security Monitoring viene eseguita dai singoli sensori Guardian.

L'architettura di Nozomi è illimitata nel numero di livelli che può supportare, in modo che, ad esempio, più distribuzioni possano essere trasferite ad un Regional Control CMC, che a sua volta può essere trasferito a un Global Control CMC.

Inoltre, al posto della CMC al livello più alto, può essere utilizzata la piattaforma cloud Nozomi Vantage SaaS che ha il vantaggio di uno spazio di archiviazione illimitato sul computer, consentendo un'analisi back-end più sofisticata e riducendo i tempi di risposta per le funzionalità richieste dai clienti.

Integrazioni e interoperabilità

Considerando il fatto che nessuna singola soluzione fornisca tutte le funzionalità di sicurezza richieste, Nozomi è stato progettato da zero per integrarsi con le migliori applicazioni di sicurezza di terze parti. L'integrazione SIEM (Security Information and Event Management) e SOAR (Security Orchestration, Automation and Response) è supportata sia tramite interfacce standard, come JSON, sia tramite Nozomi OpenAPI utilizzata dai plug-in per Splunk e QRadar. Le integrazioni che sfruttano Nozomi OpenAPI tendono a fornire ricche informazioni sugli asset, oltre agli eventi di sicurezza.

L'integrazione CMDB (Configuration Management Database) è supportata con ServiceNow, che fornisce un modulo sia per la gestione delle risorse che per la funzionalità di "trouble ticketing".

Nozomi utilizza l'integrazione con il firewall per fornire risposte dinamiche specifiche basate sulla rilevazione di dispositivi non autorizzati da parte di Nozomi Guardian, consentendo al sistema di attivare regole specifiche, come bloccare il dispositivo non autorizzato, disabilitare una particolare connessione al dispositivo non autorizzato o terminarne una sessione.

2.4 Nozomi Networks Guardian

2.4.1 Piattaforma Guardian e Guardian Sensors

Per effettuare in modo affidabile il rilevamento e il monitoraggio delle comunicazioni di rete, Nozomi adopera il **Guardian Sensor**, ovvero un componente progettato per la raccolta dei dati e informazioni sulle reti OT e IoT in tempo reale. Questi sensori sono distribuiti all'interno della rete industriale e sono in grado di monitorare il traffico di rete, inclusi protocolli specifici, e analizzare il comportamento dei vari asset e dispositivi rilevati per identificare possibili minacce, vulnerabilità o anomalie.

Il Guardian Sensor può essere implementato sia come dispositivo fisico che come soluzione virtuale, entrambe offrendo funzionalità simili. Il dispositivo fisico del Guardian Sensor è un'apparecchiatura hardware dedicata che può essere installata all'interno del proprio ambiente, mentre la soluzione virtuale può essere implementata come una macchina virtuale o container.

In base alle proprie esigenze e alla tipologia di infrastruttura, vi è una varietà di sensori, ognuno con caratteristiche specifiche (vedi *Guardian Sensors Specification Sheet [6]*).

I dati raccolti vengono poi inviati per l'elaborazione e l'analisi alla piattaforma **Guardian**, la quale integra i dati provenienti dai sensori e li combina con altre fonti di informazioni per fornire una visibilità completa sulla rete industriale, identificare le minacce conosciute e sconosciute, monitorare le variabili di processo e le prestazioni degli asset e supportare la risposta agli incidenti di sicurezza. Il Guardian utilizza algoritmi avanzati di rilevamento delle minacce e l'intelligenza artificiale per analizzare i dati provenienti dai sensori e generare avvisi e notifiche in tempo reale. Inoltre, fornisce funzionalità di visualizzazione dettagliata della rete, dashboard interattive e report personalizzabili.

2.4.2 Funzionalità e interfaccia utente

L'interfaccia principale di Nozomi Guardian offre agli utenti una panoramica completa e intuitiva delle loro reti OT e IoT, continuamente aggiornata in tempo reale con tutti i nuovi dispositivi.

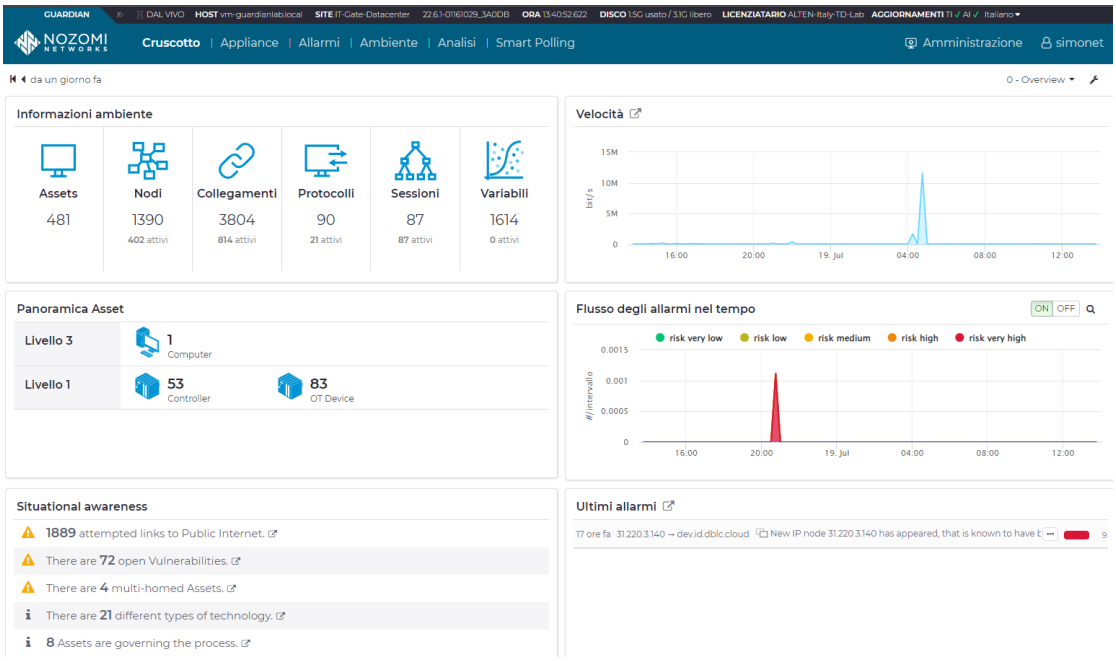


Figura 2.4. Interfaccia principale di Nozomi Guardian

La schermata "Cruscotto" presenta una dashboard con informazioni sull'ambiente, inclusi il conteggio degli asset, nodi e collegamenti nella rete, i protocolli in uso e le sessioni attive. Inoltre, offre una panoramica degli asset, un grafico che illustra la velocità di trasmissione dei dati e un pannello che mostra le ultime notifiche di allarme emesse.

Nella sezione "Situational Awareness" è possibile trovare informazioni aggiornate sul sistema, come avvisi riguardanti il numero di tentativi di accesso all'internet pubblico, o informazioni più generali, come un elenco dei sistemi operativi installati sulle macchine.

La schermata "Allarmi" offre un elenco completo degli allarmi generati, ognuno classificato con un indice di rischio, valutato su una scala da 1 a 10. Accanto sono presenti un timestamp che indica il momento in cui l'allarme è stato generato, il nome e una breve descrizione dell'allarme.

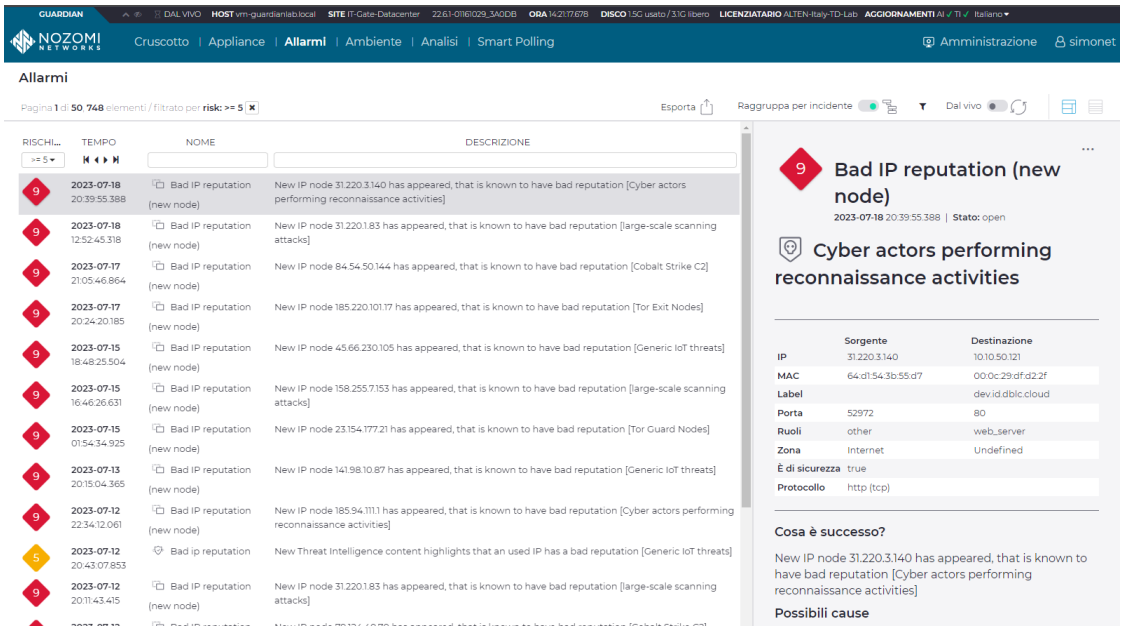


Figura 2.5. Allarmi generati su Nozomi Guardian

Cliccando su un allarme specifico viene mostrata una vista approfondita con gli indirizzi IP sorgente e destinazione coinvolti, gli indirizzi MAC e le porte associate, insieme al protocollo utilizzato durante l'evento. Inoltre, viene fornita una descrizione più dettagliata dell'accaduto, comprendente informazioni sulle cause dell'allarme e le soluzioni raccomandate per correggere il problema.

Nella Figura 2.5 è riportato un esempio di allarme di tipo "Bad IP Reputation (New Node)", che viene generato quando il sistema rileva l'ingresso di un nuovo nodo IP nella rete con una reputazione negativa. Tali indirizzi IP sono spesso inclusi in *blacklist* o database di monitoraggio delle minacce.

La descrizione dell'allarme spiega dunque che l'IP 31.220.3.140 è stato rilevato come un nuovo nodo con una cattiva reputazione, suggerendo che il nodo o i dispositivi connessi ad esso potrebbero essere stati compromessi o infettati da malware, in quanto l'IP è stato coinvolto in precedenti attività malevole. La soluzione suggerita da Nozomi consiste nel valutare attentamente l'evento e verificare la legittimità del nodo IP: se il nodo è sicuro allora è possibile utilizzarlo; altrimenti bisognerebbe avviare ulteriori controlli per verificare e risolvere eventuali problemi di sicurezza.

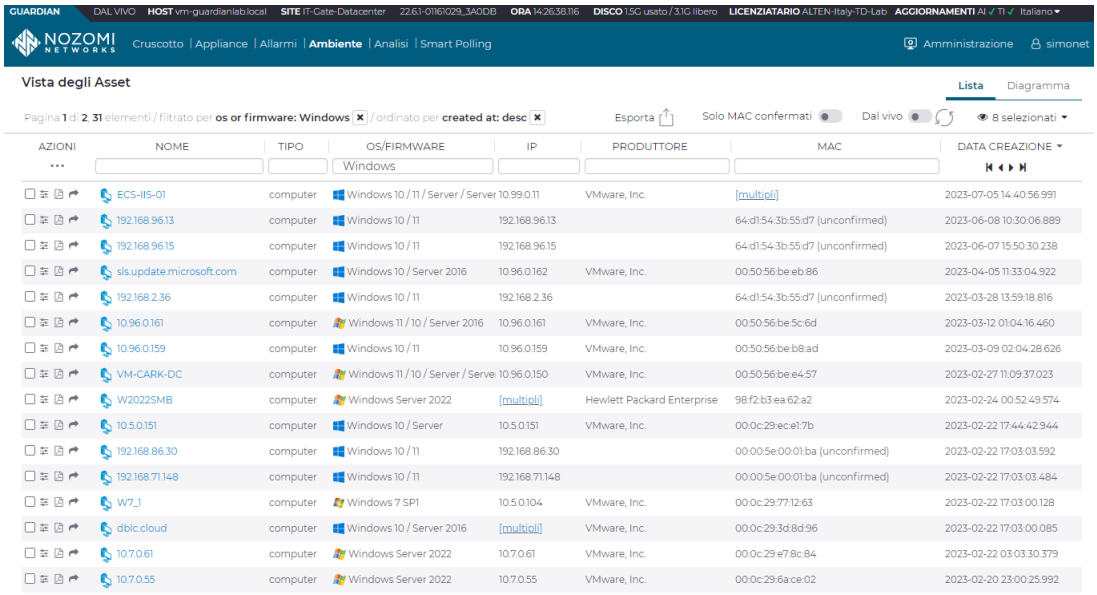


Figura 2.6. Vista degli asset con sistema operativo Windows

La schermata "Asset" offre una lista di tutti gli asset rilevati nella rete, completa di informazioni chiave di ciascuno di essi, tra cui:

- il nome
- la tipologia
- il sistema operativo installato
- l'indirizzo IP
- il produttore
- l'indirizzo MAC
- la data di creazione

Grazie alla funzionalità di filtraggio, gli utenti possono restringere la visualizzazione degli asset in base a specifici parametri. Ad esempio, come mostrato nella Figura 2.6, si è applicato un filtro per mostrare solo gli asset con il sistema operativo Windows installato. Inoltre, selezionando un asset (Figura 2.7), si apre una schermata che offre dettagli aggiuntivi, incluse le statistiche di rete che comprendono i byte ricevuti e inviati dal primo inserimento nella rete e i byte trasmessi negli ultimi 30 minuti. Vengono inoltre visualizzati il numero di collegamenti attivi, un elenco dei protocolli utilizzati nelle varie sessioni, il posizionamento del dispositivo nella rete e le sue prestazioni.

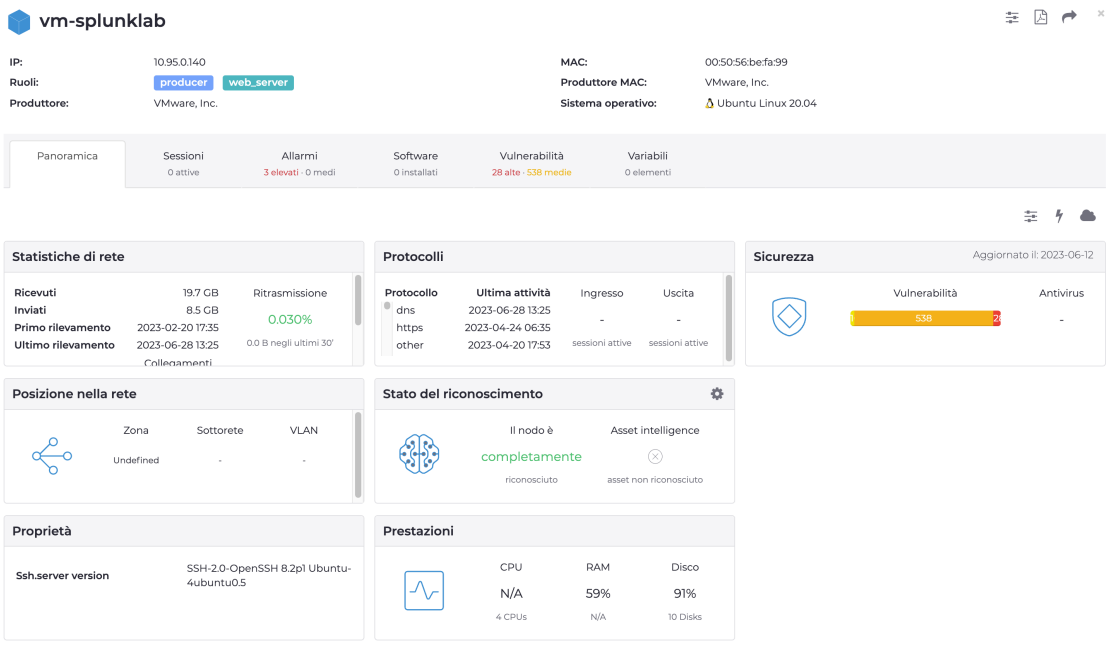


Figura 2.7. Panoramica di un asset

Una volta identificati gli asset, l'utente può anche indagare su tutte le vulnerabilità rilevate sui vari dispositivi, accedendo alla schermata Analisi → Vulnerabilità.

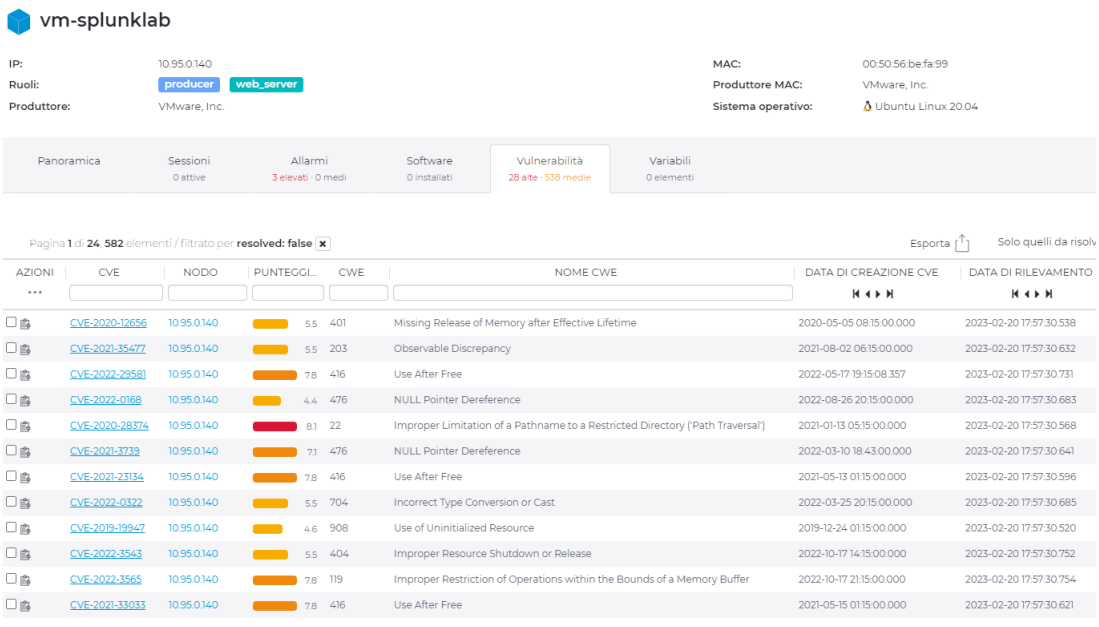


Figura 2.8. Vulnerabilità rilevate sulla macchina "vm-splunklab"

La Figura 2.8 mostra un esempio di vulnerabilità rilevate sulla macchina "vm-splunklab".

Per ognuna di esse sono riportati:

- il CVE (Common Vulnerabilities and Exposures) di riferimento
- l'indirizzo IP del nodo
- un punteggio di rischio assegnato alla vulnerabilità dal NIST
- il valore CWE (Common Weakness Enumeration)
- il nome della vulnerabilità
- le date di creazione CVE e di rilevamento

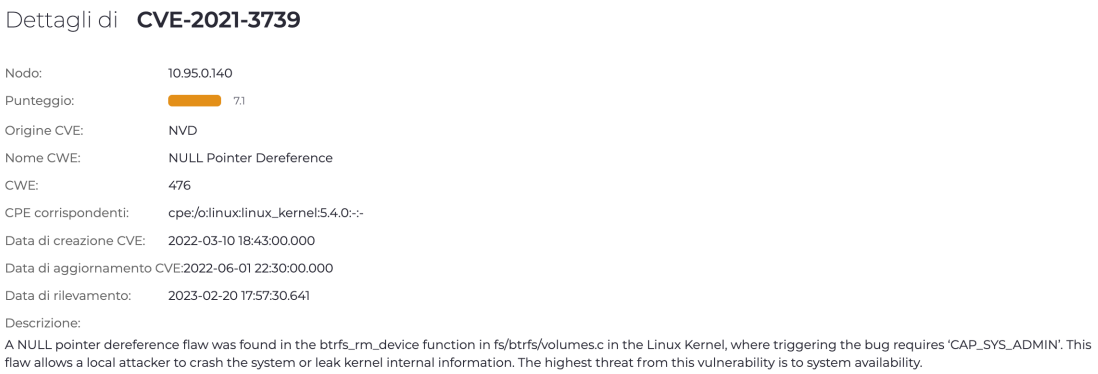


Figura 2.9. Vulnerabilità CVE-2021-3739 rilevata sulla macchina "vm-splunklab"

L'origine della CVE riportata è l'NVD (National Vulnerability Database), ovvero un database gestito dal National Institute of Standards and Technology (NIST) e fonte di informazioni sulle vulnerabilità software e sulle misure di sicurezza associate.

In questo caso, Nozomi ha rilevato la vulnerabilità CVE-2021-3739 con CWE 476, che fa riferimento alla vulnerabilità nota come "NULL Pointer Dereference" [7]. Questo tipo di vulnerabilità si verifica quando un programma tenta di accedere o dereferenziare un puntatore NULL, ovvero un puntatore che non punta a nessun indirizzo di memoria valido. Ciò potrebbe consentire ad un attaccante di causare il crash del sistema o un "leak" delle informazioni interne del kernel.

Capitolo 3

Splunk: piattaforma di analisi e ricerca avanzata dei dati

3.1 Monitoraggio e protezione delle reti industriali

L'interazione sempre più stretta tra i sistemi OT e IT, comportata dall'utilizzo di software, interfacce e protocolli standardizzati che si connettono alle reti aziendali interne, sostituendo le tradizionali tecnologie proprietarie, ha introdotto un aumento delle vulnerabilità e dei rischi legati alle minacce informatiche.

La compromissione di un sistema di controllo o delle varie risorse collegate, come PLC, "operator" workstations o server per l'archiviazione dei dati, potrebbe causare danni considerevoli alle infrastrutture e a servizi critici, sia per l'ambiente che in alcuni casi per la vita umana. In mancanza di visibilità e controllo completi del traffico in entrata e in uscita dalle reti della propria infrastruttura, vari attacchi potrebbero dunque passare inosservati [8].

Il problema principale risiede nel fatto che le reti OT sono state spesso ignorate in termini di sicurezza informatica: molte organizzazioni infatti non applicano regolarmente patch o aggiornamenti ai sistemi di controllo industriali. In molti casi, questi sistemi sono stati sviluppati anni fa e sono legati a versioni precedenti e ormai obsolete di Microsoft Windows che non sono più supportate.
L'installazione di aggiornamenti o l'applicazione di patch alle vulnerabilità spesso non vengono eseguiti in molti ambienti industriali, in quanto questi sistemi devono funzionare senza interruzioni, garantendo in ogni momento la disponibilità delle loro risorse. Se i sistemi legacy non vengono regolarmente riparati o aggiornati, è quantomeno importante monitorarli e osservarli attentamente.

Un altro problema risiede nel fatto che gli strumenti di sicurezza specificamente sviluppati per l'OT forniscono solo una prospettiva limitata sulla sicurezza complessiva. Anche se l'adozione di questi strumenti può migliorare la visibilità delle risorse e delle reti OT, non fornisce ai team le conoscenze per rilevare, indagare o mitigare le minacce sconosciute o per comprendere le implicazioni che attraversano il divario tra OT e IT. Questa mancanza di precisione nell'identificazione e la capacità di reagire prontamente alle minacce che influenzano le operazioni aziendali rappresenta uno dei principali ostacoli nell'assicurare una protezione adeguata dell'ICS.

Minacce informatiche alle reti OT

Una serie di attacchi riportati dal Center for Strategic & International Studies [9] evidenziano la necessità di proteggere le reti OT a causa della crescente convergenza con i sistemi esterni, sottolineando l'importanza della protezione e del monitoraggio di fronte alle crescenti minacce informatiche alle reti OT.

Alcuni attacchi degni di nota includono la compromissione delle reti di società energetiche, idriche ed elettriche tedesche da parte di un gruppo di hacker collegato alla Russia, hacker iraniani che prendono di mira il trasporto aereo in Arabia Saudita e hacker israeliani che distruggono un porto iraniano.
Altri attacchi si focalizzano su infrastrutture critiche, operatori del settore sanitario e aziende farmaceutiche, evidenziando un aumento del pericolo per le operazioni industriali. Questi attacchi fanno uso di toolkit di attacco contenenti malware e ransomware specifici per i sistemi di controllo industriale. Una volta eseguiti, gli script e le applicazioni costruite su tali toolkit mirano e distruggono processi digitali vitali e possono essere necessari mesi o più per riprendersi completamente dal danno.

L'importanza del monitoraggio della rete

Per affrontare le varie minacce, è dunque importante avviare un processo iniziale di monitoraggio e protezione dei dispositivi ICS tramite la rete. Sfruttando i dati generati dai vari router, switch, firewall, le organizzazioni possono effettuare un monitoraggio accurato e individuare le potenziali minacce nell'ambito dell'OT.

Mantenere un'attenzione costante sul traffico in entrata e in uscita dai sistemi OT, insieme alla supervisione regolare dell'attività della rete, è fondamentale per garantire la protezione dell'azienda, implementando soprattutto un monitoraggio accurato degli accessi, autenticazioni e altre attività rilevanti tramite l'utilizzo di uno strumento come Splunk.

Inoltre, è essenziale che i professionisti della sicurezza dell'infrastruttura abbiano la capacità di rilevare, indagare e rispondere agli attacchi ICS: sfruttando le anomalie del traffico di rete, è possibile prevedere l'azione delle minacce prima che causino danni significativi all'ambiente e all'azienda. Nel caso di una violazione, è fondamentale che un'organizzazione sia in grado di reagire tempestivamente e attuare misure correttive.

L'uso di Splunk Enterprise offre un'importante soluzione in questo scenario. Questa piattaforma infatti fornisce strumenti avanzati per il monitoraggio e l'analisi dei dati di sicurezza, consentendo di individuare rapidamente eventuali anomalie e comportamenti sospetti.

3.2 Splunk Enterprise: architettura e funzionamento

3.2.1 Introduzione a Splunk Enterprise

Splunk Enterprise rappresenta la versione completa e avanzata della piattaforma di analisi dei dati di Splunk. Questo prodotto è specificamente progettato per soddisfare le esigenze di grandi aziende e organizzazioni, offrendo funzionalità e prestazioni avanzate per gestire e analizzare una vasta gamma di dati provenienti da diverse fonti. Essenzialmente permette di raccogliere, indicizzare, analizzare e visualizzare dati provenienti da vari componenti della propria infrastruttura o azienda [10].

La piattaforma è composta da vari componenti, ad esempio il motore di ricerca svolge un ruolo fondamentale nell'elaborazione dei dati e nell'esecuzione delle ricerche, sfruttando il linguaggio di ricerca SPL (Search Processing Language), il quale permette di comporre query complesse e ottenere risultati significativi dai dati raccolti.

Splunk Enterprise offre anche strumenti per la raccolta dei dati, come il Forwarder, e servizi di gestione e configurazione, come il Deployment Server. Questi elementi consentono di gestire l'intera infrastruttura di dati in modo efficace e ottimizzare le prestazioni del sistema.

Una delle sue caratteristiche distintive è la capacità di gestione distribuita, che consente di scalare l'implementazione su larga scala e garantire l'alta disponibilità dei dati. Questa funzionalità è particolarmente utile per le grandi organizzazioni che devono gestire enormi volumi di dati provenienti da diverse fonti.

Splunk Enterprise acquisisce dati da siti Web, applicazioni, sensori, dispositivi e così via. Dopo aver definito l'origine dati, il software indicizza il flusso di dati e lo analizza in una serie di singoli eventi che è possibile visualizzare e cercare.

Per poterlo utilizzare, è necessario installarlo e configurarlo su un server o in un ambiente cloud. Successivamente sarà possibile accedere alla piattaforma attraverso Splunk Web, un'interfaccia utente utilizzabile da browser che consente di gestire la distribuzione, eseguire ricerche, creare dashboard e report, e sfruttare molte altre funzionalità. Inoltre, è possibile utilizzare la piattaforma tramite riga di comando.

Utilizzo delle App

Vi è la flessibilità di personalizzare e adattare l'ambiente in base alle esigenze specifiche della propria organizzazione sfruttando le *app*. Un'app è una raccolta di configurazioni, viste e dashboard che può essere eseguita sulla piattaforma Splunk. Possono essere installate e utilizzate più app contemporaneamente all'interno di una singola installazione di Splunk Enterprise.

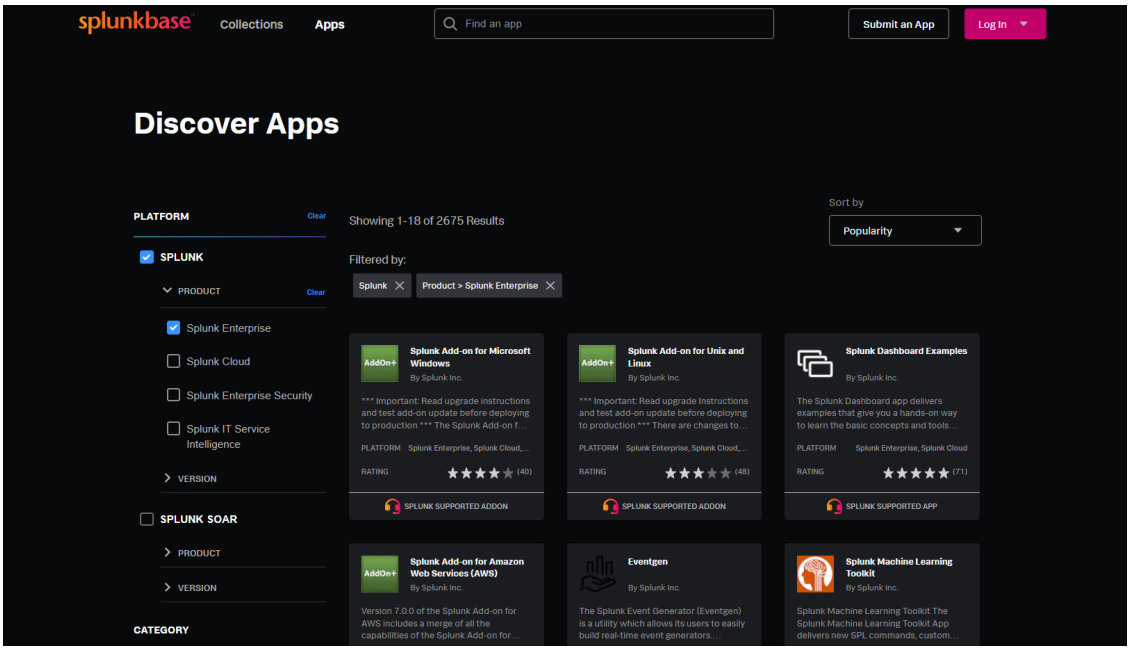


Figura 3.1. Splunkbase - Repository ufficiale per le app di Splunk

Per estendere dunque le funzionalità di Splunk, è possibile esplorare l'ampia gamma di app disponibili su Splunkbase, ovvero una repository online dedicata alle app sviluppate dalla community e dai partner di Splunk. Queste app coprono una un gran numero di casi d'uso e consentono di aggiungere funzionalità specifiche alla propria piattaforma, come il monitoraggio della sicurezza, la gestione delle prestazioni, l'analisi dei dati di vendita e molto altro. Vi è inoltre la possibilità di creare la proprie app personalizzate utilizzando il sito per sviluppatori.

3.2.2 Architettura e componenti fondamentali

Durante il processo di elaborazione dati, Splunk Enterprise svolge tre funzioni fondamentali:

1. **Raccolta dei dati:** Splunk acquisisce dati da varie fonti, come server, applicazioni, dispositivi di rete o altre sorgenti, garantendo la copertura di dati distribuiti in diverse locazioni, sia locali che remote, purché le macchine generatrici di dati siano nella stessa rete. Supporta formati di dati comuni come CSV, JSON e XML, nonché formati personalizzati.
2. **Analisi e indicizzazione dei dati:** una volta acquisiti, i dati vengono analizzati e indicizzati. Questa fase permette di strutturare i dati in modo efficiente, estraendo i campi pertinenti, come timestamp, tipi di origine e informazioni sull'host.
3. **Esecuzione di ricerche sui dati indicizzati:** gli utenti possono eseguire ricerche efficienti e accurate. Splunk infatti offre un potente motore di ricerca che consente agli utenti di trovare e analizzare i dati in modo rapido e preciso, grazie all'indicizzazione eseguita nello step precedente.

A seconda delle esigenze, Splunk Enterprise può essere distribuito in varie modalità, che vanno dalla configurazione con singola istanza fino a distribuzioni scalabili che coinvolgono centinaia o migliaia di istanze.

Implementazioni con Singola Istanza

Nelle distribuzioni di dimensioni più contenute, è possibile utilizzare una singola istanza di Splunk Enterprise per gestire tutte le fasi del processo di elaborazione dati, dall'input all'indicizzazione fino alla ricerca [11]. Questa configurazione è particolarmente adatta per scopi di test.

Implementazioni Distribuite

Nei casi in cui si ha invece la necessità di elaborare volumi di dati significativi, o in cui molti utenti devono effettuare ricerche complesse, è possibile ricorrere a una implementazione distribuita, dove le istanze di Splunk Enterprise vengono distribuite su più macchine. In una tipica implementazione distribuita, ogni istanza di Splunk esegue una specifica attività e risiede su uno dei tre livelli corrispondenti alle principali funzioni di elaborazione:

1. **Livello di input dei dati:** questo livello è responsabile per ricevere e raccogliere i dati da diverse fonti. È possibile configurare più istanze di Splunk Enterprise su questo livello per la raccolta distribuita dei dati provenienti da sorgenti eterogenee.

2. **Livello dell'indicizzatore:** in questo livello, le istanze di Splunk Enterprise indicizzano i dati raccolti, consentendo ricerche e analisi efficienti. Anche in questo caso, è possibile avere più istanze distribuite per gestire grandi volumi di dati.

3. **Livello di gestione della ricerca:** questo livello si occupa della gestione delle ricerche effettuate dagli utenti. Una singola istanza di Splunk Enterprise può risiedere su questo livello, consentendo una gestione centralizzata delle ricerche.

Componenti principali

Le istanze specializzate in particolari attività e che si trovano su determinati livelli sono note come "componenti". È possibile, ad esempio, creare una distribuzione con molte istanze che risiedono sul livello di input dei dati, altre che risiedono sul livello dell'indicizzatore e una sola istanza sul livello di gestione della ricerca.

I componenti principali dell'architettura Splunk sono il *forwarder*, l'*indexer* e il *search head*. La seguente tabella elenca tali componenti di elaborazione insieme ai livelli che occupano, fornendo inoltre una breve descrizione delle funzioni svolte da ciascuno di essi.

Componente	**Livello**	**Descrizione**
Forwarder	Input dati	Consuma i dati e li inoltra in avanti, di solito a un indicizzatore. Richiedono solitamente risorse minime.
Indexer	Indicizzatore	Indicizza i dati in entrata che di solito riceve da un gruppo di forwarder. L'indicizzatore trasforma i dati in eventi e memorizza gli eventi in un indice. L'indicizzatore cerca anche i dati indicizzati in risposta alle richieste di ricerca da una search head. È possibile distribuire più indicizzatori in cluster di indicizzatori.
Search head	Gestione ricerca	Interagisce con gli utenti, indirizza le richieste di ricerca a un insieme di indicizzatori e restituisce i risultati raggruppati all'utente. È possibile distribuire più search head in cluster di search head.

Tabella 3.1. Descrizione componenti principali [12]

Il forwarder è un agente che raccoglie i log e li invia all'indicizzatore. Splunk ne ha due tipi:

- **Universal Forwarder:** inoltra i dati grezzi senza alcun trattamento preventivo. Questo è più veloce e richiede meno risorse sull'host, ma si traduce in enormi quantità di dati inviati all'indicizzatore.

- **Heavy Forwarder:** esegue l'analisi e l'indicizzazione all'origine, sulla macchina host e invia solo gli eventi analizzati all'indicizzatore.

L'indexer trasforma i dati in eventi (a meno che non siano stati ricevuti pre-elaborati da un Heavy Forwarder), li archivia su disco e li aggiunge a un indice, consentendo la ricerca. L'indexer crea i seguenti file, separandoli in directory denominate *bucket*:

- Dati grezzi (raw) compressi
- Indici che puntano a dati raw (file .TSIDX)
- File di metadati

L'indexer esegue l'elaborazione di eventi generici sui dati di log, ad esempio applicando un timestamp e inserendo un'origine, e può anche eseguire azioni di trasformazione definite dall'utente per estrarre informazioni specifiche o applicare regole speciali, ad esempio il filtraggio di eventi indesiderati.

La search head si interfaccia con i vari indexer per ottenere l'accesso ai dati richiesti. Essa fornisce l'interfaccia utente che gli utenti possono utilizzare per interagire con la piattaforma, consentendo loro di cercare e interrogare i dati d'interesse.

Il **deployment server** è infine un componente che viene utilizzato per la distribuzione di configurazioni, app e aggiornamenti a gruppi di istanze di Splunk Enterprise. Funzionalmente, il deployment server è essenzialmente un'istanza standard di Splunk Enterprise, ma è stato configurato appositamente per distribuire gli aggiornamenti a diversi componenti, come forwarder, indexer non clusterizzati e search head [13].
A seconda delle dimensioni e del numero di istanze alle quali distribuisce gli aggiornamenti, potrebbe essere necessario dedicare l'istanza del deployment server esclusivamente alla gestione degli aggiornamenti.

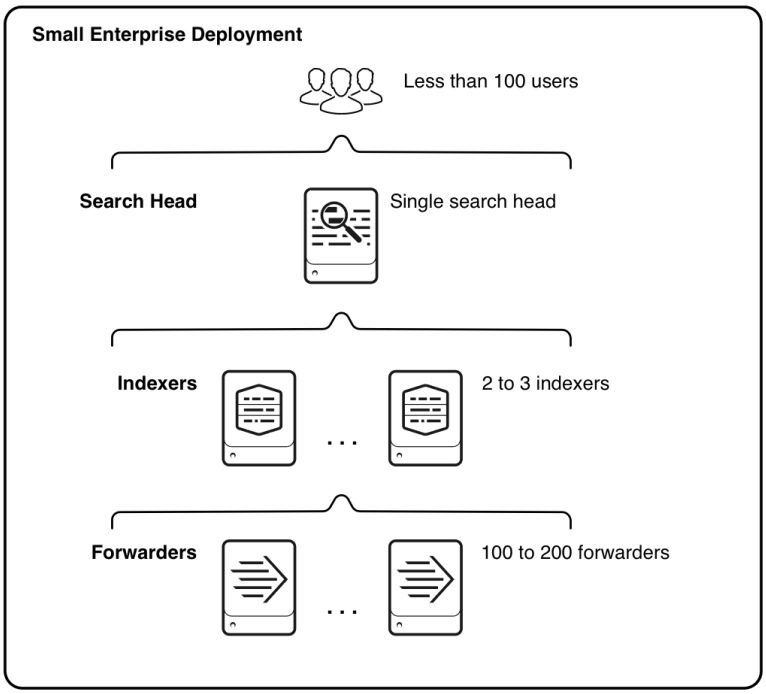


Figura 3.2. Esempio di un deployment distribuito [12]

Il diagramma in Figura 3.2 illustra il tipo di distribuzione che potrebbe supportare le esigenze di una piccola impresa, costituito da una singola search head, un numero minimo di indexer (2-3), ed infine 100-200 forwader per gestire la raccolta dei dati.

Architettura completa di Splunk

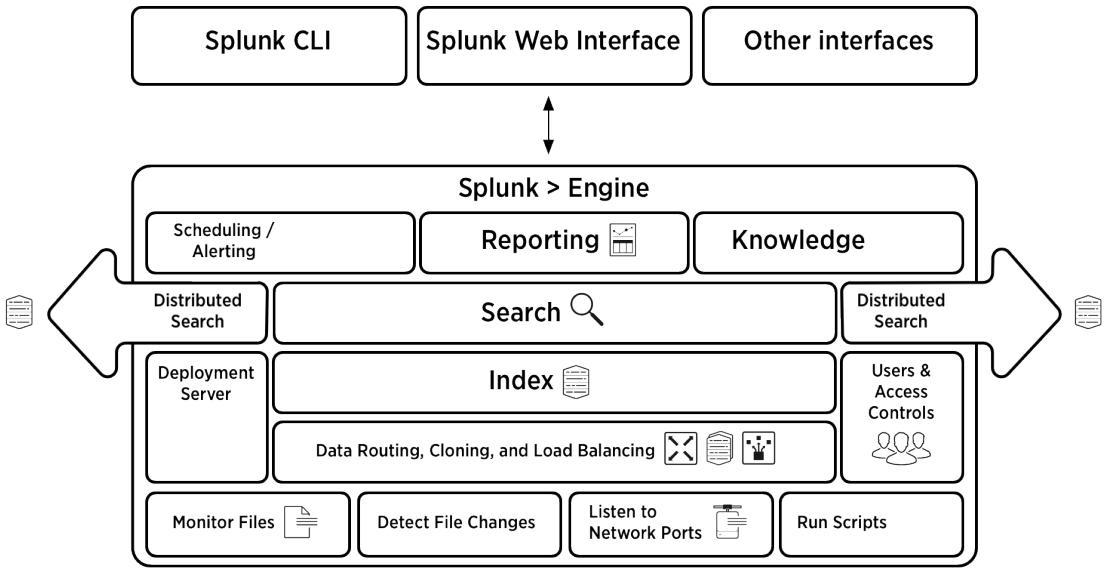


Figura 3.3. Architettura completa di Splunk [14]

In Figura 3.3 è riportato un esempio completo dell'intera architettura di Splunk, mostrando come i vari componenti comunicano tra di loro per gestire il flusso di dati, partendo dalla raccolta, per finire all'esecuzione di ricerche sugli eventi tramite l'interfaccia utente.

Il meccanismo è dunque il seguente [15]:

1. Il forwarder raccoglie i log monitorando i file, rilevando le modifiche ai file, mettendosi in ascolto sulle porte o eseguendo script per raccogliere i dati dei log.
2. Il meccanismo di indicizzazione, composto da uno o più indexer, elabora i dati oppure può ricevere i dati pre-elaborati dai forwarder.
    - Il deployment server si occupa della distribuzione di aggiornamenti e configurazioni ai vari indexer e search head.
    - I controlli di accesso e degli utenti vengono applicati a livello di indexer: ogni indexer può essere utilizzato per un archivio dati diverso, che può avere autorizzazioni utente diverse.
3. La search head viene utilizzata per fornire agli utenti funzionalità di ricerca, interfacciandosi con i vari indexer.
4. Tramite le funzionalità di Scheduling/Alerting, Reporting e Knowledge gli utenti possono utilizzare le ricerche per generare avvisi e report.
5. Infine, attraverso le varie interfacce (CLI, Web, ecc.) è possibile accedere ai dati indicizzati, visualizzandoli in vari modi.

3.2.3 Accedere all'interfaccia utente tramite Splunk Web

Per accedere a Splunk Enterprise si utilizza Splunk Web, ovvero l'interfaccia utente vera e propria che permette agli utenti di interagire con i dati e le funzionalità di Splunk tramite il browser web.

Inizialmente bisogna eseguire l'installazione di Splunk Enterprise su un server o un ambiente cloud. Questa fase include la preparazione del server, l'installazione del software e la configurazione delle impostazioni necessarie. Per istruzioni approfondite sull'installazione di Splunk in base al proprio sistema operativo, si consiglia di fare riferimento alla guida fornita nella documentazione ufficiale di Splunk [16].

Successivamente, per accedere alla piattaforma, è sufficiente aprire il proprio browser web e e digitare l'indirizzo IP o il nome host del server in cui è installato Splunk Enterprise, seguito dalla porta di default per Splunk Web, che di solito è 8000. Ad esempio, "http://indirizzoipserver:8000/" o "http://nomehost:8000/".

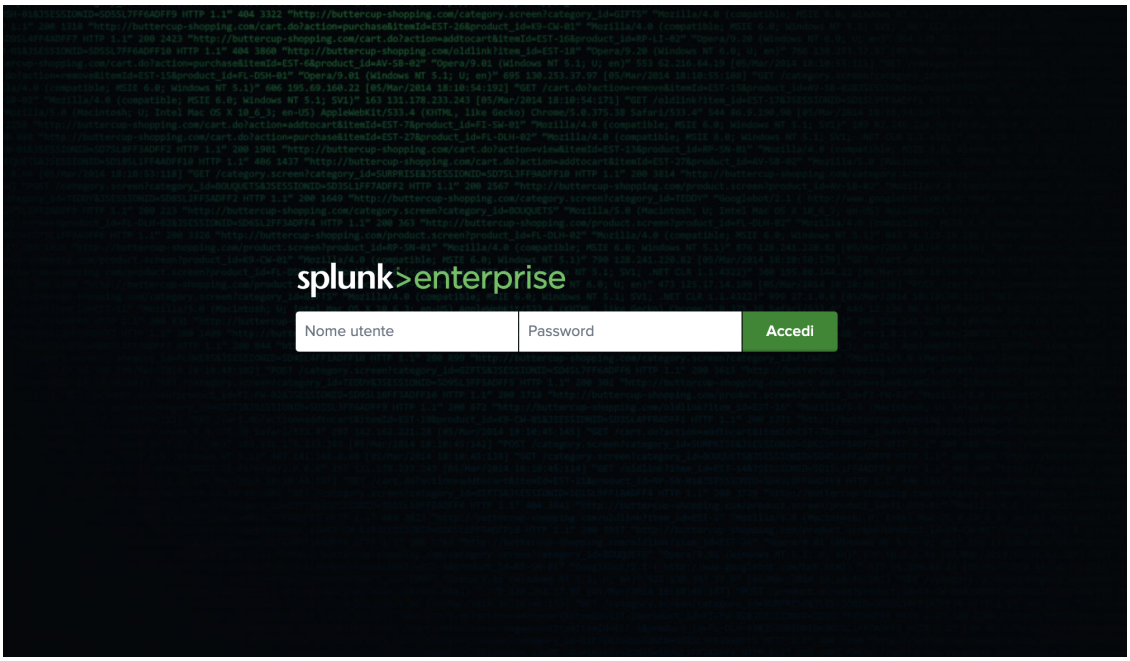


Figura 3.4. Pagina di accesso di Splunk Enterprise

A questo punto si verrà reindirizzati alla pagina di accesso di Splunk Web, come mostrato in Figura 3.4, dove sarà necessario inserire le credenziali di accesso della propria utenza.

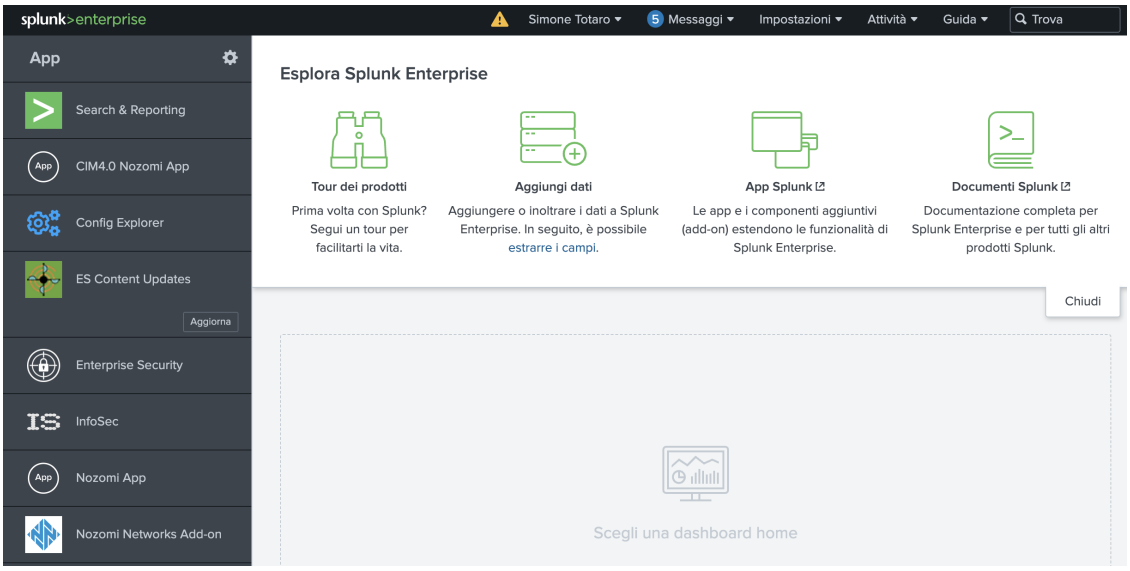


Figura 3.5. Homepage di Splunk Enterprise

Una volta inseriti il proprio nome utente e password si verrà autenticati e reindirizzati alla homepage di Splunk (Figura 3.5). Nella parte sinistra dell'interfaccia è possibile trovare l'elenco di tutte le app installate nella piattaforma, mentre dalla barra di stato è possibile accedere alle impostazioni di sistema, dove gli utenti con privilegi di amministratore possono definire ruoli e autorizzazioni per gli utenti, monitorare le prestazioni del sistema e gestire le connessioni ai dati in ingresso.

Tra le app più rilevanti troviamo "Search & Reporting" (Figura 3.6), ovvero l'applicazione principale che consente di effettuare ricerche per interrogare e analizzare i dati ricevuti da Splunk, creare dashboard personalizzate, generare report, e altro.

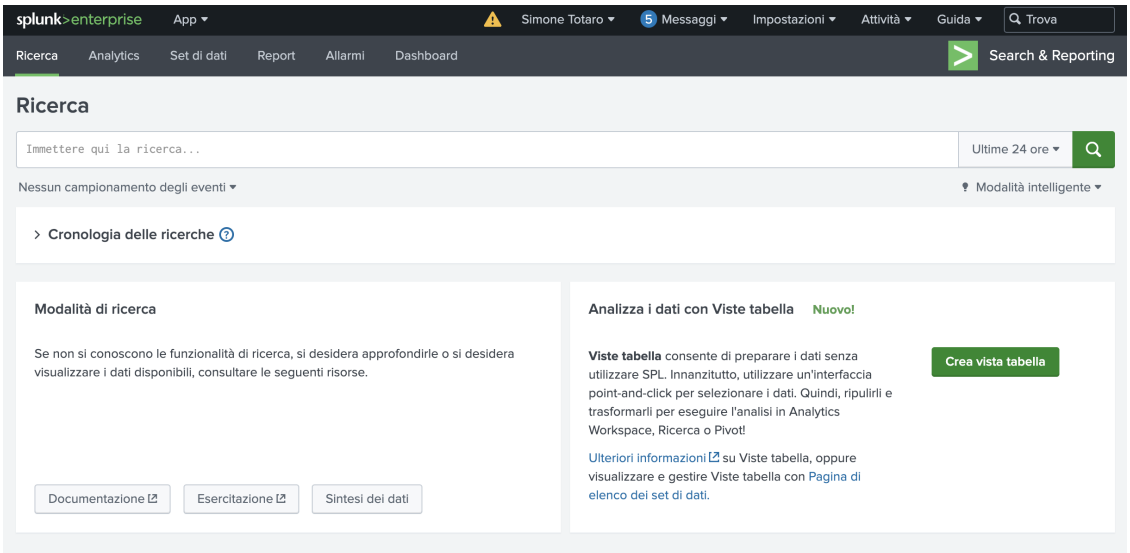


Figura 3.6. Applicazione di Search & Reporting

Le query di ricerca vengono effettuate utilizzando il linguaggio di ricerca SPL di Splunk, che consente di filtrare e manipolare i dati in modo efficiente.

3.3 Splunk Search Processing Language (SPL)

Il linguaggio di ricerca SPL (Search Processing Language) rappresenta il motore che alimenta l'analisi dei dati in Splunk, permettendo di interrogare, filtrare, aggregare e visualizzare i dati raccolti, utilizzando una sintassi piuttosto semplice ed intuitiva.
Il linguaggio si basa su comandi e funzioni che consentono di eseguire operazioni specifiche sui dati, ad esempio operazioni di filtraggio, aggregazione, trasformazione, calcoli statistici e altro ancora.

Inserendo una query nella barra di ricerca, utilizzando l'app Search & Reporting menzionata precedentemente, è possibile trovare eventi che contengono valori provenienti da più fonti di dati, consentendo di analizzare ed eseguire statistiche su di essi. I risultati delle ricerche SPL possono quindi essere visualizzati in varie forme, come tabelle, grafici, dashboard e report.

3.3.1 Knowledge Objects: componenti principali del linguaggio

Il linguaggio si basa principalmente sull'uso dei cosiddetti "**Knowledge Objects**" (oggetti di conoscenza) che rappresentano elementi chiave per organizzare e dare un significato e un contesto ai dati raccolti. Questi oggetti possono essere una o un insieme di ricerche, campi e report definiti dall'utente che arricchiscono i dati e li strutturano, consentendo agli utenti di ottenere un'analisi più approfondita e significativa dai dati raccolti [17].

Ecco una breve descrizione dei Knowledge Objects più importanti:

- **Fields**: Sono coppie chiave-valore che contengono valori estratti dagli eventi e permettono di suddividere i dati in elementi specifici, come indirizzi IP o nomi utente. I campi possono essere estratti automaticamente o manualmente dai dati in entrata (**extracted fields**), oppure possono essere definiti dall'utente (**calculated fields**) attraverso operazioni matematiche o manipolazioni su campi esistenti.
- **Index**: Struttura in cui vengono raggruppati gli eventi in base a criteri specifici, come la fonte o il tipo di dati. Ciò semplifica la ricerca e l'analisi dei dati, in quanto ci si può concentrare su un particolare subset di eventi invece di dover attraversare l'intero insieme di dati.
- **Sourcetypes**: Etichette assegnate a ciascun evento per indicare la sua natura o il suo formato. Rappresentano infatti il tipo di dati o il modello da cui proviene l'evento, ad esempio, un evento proveniente da un sensore avrà un sourcetype diverso da un evento di log di un'applicazione.
- **Event Types**: Sono categorie personalizzate che consentono di raggruppare e identificare eventi che condividono caratteristiche o proprietà simili. Possono essere creati dall'utente in base a determinati criteri, ad esempio è possibile definire un event type "Errore di sistema" che include eventi con messaggi di errore dai log di sistema.
- **Tags**: Etichette che possono essere applicate a eventi e campi per categorizzarli e raggrupparli. Possono essere creati manualmente o definiti attraverso estrazioni in tempo di ricerca. Supponendo ad esempio di avere eventi provenienti da diversi server, si può assegnare un tag "Server Web" a tutti gli eventi provenienti dai server web e un tag "Server Database" a quelli provenienti dai server database, in modo da filtrare solo gli eventi d'interesse.

- **Alerts**: Gli utenti possono definire allerte basate su condizioni specifiche. Quando i dati soddisfano tali condizioni, Splunk può inviare notifiche per segnalare eventi importanti o situazioni critiche, oppure lanciare l'esecuzione di uno script.
- **Reports**: Sono ricerche salvate che vengono programmate per essere eseguite a intervalli specifici per generare rappresentazioni visive o sintesi dei dati, spesso sotto forma di tabelle o grafici.
- **Lookup**: Tabelle di dati utilizzate per aggiungere un contesto agli eventi o per mappare i campi a valori diversi. Solitamente vengono create da file CSV o da database e possono essere utilizzate nelle ricerche e nelle visualizzazioni.
- **Dashboards and Panels**: I pannelli consentono agli utenti di comporre dashboard personalizzate, aggregando report, grafici, mappe e altri elementi in un'unica visualizzazione per mostrare i dati in tempo reale.
- **App**: Discusse in precedenza, sono pacchetti preconfigurati che includono dashboards, ricerche, report e altre risorse, semplificando l'analisi dei dati ai vari utenti. Un'app potrebbe essere progettata ad esempio per monitorare l'utilizzo di un sito web, mostrando report sulle pagine più visitate, il tempo di permanenza medio degli utenti, ecc.

Field Extraction

Quando i dati, provenienti da fonti diverse, sono inviati a Splunk, vengono assegnati ad uno specifico indice (index). I dati entrano dunque nell'indicizzatore e, dopo essere stati analizzati, e riconosciuti ad esempio come "log di Apache", vengono etichettati con un sourcetype, il quale viene utilizzato per suddividere i dati in singoli eventi. Gli eventi vengono quindi memorizzati nell'indice Splunk, dove possono essere successivamente ricercati tramite una query SPL.

Alcuni campi vengono estratti ad "index time", mentre altri vengono estratti a "search time": **Index time** è l'intervallo di tempo che intercorre da quando Splunk riceve i nuovi dati a quando i dati vengono scritti in un indice, mentre **Search time** è il periodo di tempo da quando viene avviata una ricerca a quando essa termina [18].

Durante l'index time, i dati vengono suddivisi in segmenti ed eventi. Dunque, quando Splunk inserisce i dati nell'indice, viene estratto automaticamente un certo numero di campi, inclusi i campi di metadati, come *host*, *source* e *sourcetype*, e campi interni come *_time* e *_raw*, che contengono il timestamp degli eventi e i dati originali grezzi (raw) di un evento.

Durante il search time vengono automaticamente estratti campi aggiuntivi dai dati raw (ad esempio, product_name, categoryId, action, ecc.) in base al sourcetype assegnato e alle coppie chiave-valore (ad esempio action=purchase) trovate nei dati. Questi campi sono persistenti e verranno estratti ogni volta che viene eseguita una ricerca contenente gli stessi termini di ricerca, a meno che non vengano omessi con il comando *fields*.

3.3.2 Comandi e operatori fondamentali

I comandi SPL sono le istruzioni che definiscono cosa fare con i dati e possono includere operazioni di ricerca, aggregazione, filtraggio, e altro ancora. Ecco alcuni esempi dei comandi più utilizzati:

- **index**: Specifica l'indice da cui recuperare i dati.
- **sourcetype**: Filtra i dati in base al sourcetype.
- **eval**: Permette di creare campi personalizzati basati su calcoli, operazioni matematiche o manipolazione di dati esistenti. Ad esempio, è possibile definire un nuovo campo "TotalAmount" scrivendo: *eval TotalAmount = Quantity * Price*.
- **stats**: Esegue aggregazioni statistiche sui dati, come la somma, la media o il conteggio. Ad esempio, *stats count by host* effettua un conteggio degli eventi per ciascun host.
- **chart \timechart**: Creano grafici interattivi, come grafici a barre o a linee, basati su dati aggregati, per visualizzare le informazioni o le tendenze temporali. Ad esempio, *chart sum(Sales) by Product* somma le vendite per ciascun prodotto e crea un grafico a barre in cui l'asse x ha i nomi dei prodotti e l'asse y le vendite corrispondenti.
- **table**: Crea una tabella specificando quali campi visualizzare, ad esempio: *table _time, src_ip, dest_ip*.
- **where**: Filtra gli eventi in base a condizioni specifiche. Ad esempio, *where user="alice"* restituirà solo gli eventi correlati all'utente "alice".
- **sort**: Ordina i risultati in base a uno o più campi. Ad esempio, *sort _time* ordina i risultati in base al tempo in ordine crescente.
- **rex**: Permette di estrarre informazioni da campi testuali complessi attraverso l'uso di espressioni regolari. Per estrarre ad esempio gli indirizzi IP da un campo "src_ip", è possibile utilizzare il comando rex per definire un nuovo campo "IP" in questo modo: *rex field=src_ip "(?<IP>\d+\.\d+\.\d+\.\d+)"*.

Ecco invece alcuni operatori fondamentali:

- =: Operatore di assegnazione.
- ==: Operatore di uguaglianza.
- **!=**: Operatore di disuguaglianza.
- < e >: Operatori di confronto.
- |: Operatore "pipe" per concatenare diverse operazioni di ricerca in una singola query.
- **AND**, **OR**, **NOT**,: Operatori logici per combinare condizioni.
- **IS NULL** e **IS NOT NULL**: Operatori per verificare la presenza di valori nulli.

3.3.3 Esecuzione di una ricerca SPL

Una ricerca inizia solitamente specificando l'indice d'interesse, seguito da ulteriori comandi che definiscono le operazioni da eseguire sui dati. Se vogliamo eseguire una ricerca sull'indice "nozomi", basterà inserire nella barra di ricerca *index=nozomi*, altrimenti per eseguire una ricerca su tutti gli indici a disposizione è sufficiente inserire un asterisco, scrivendo *index=**.
Apriamo dunque l'applicazione "Search & Reporting" e creiamo una query semplice, facendo riferimento ai dati forniti da Nozomi per questo esempio (il capitolo successivo tratterà la ricezione dei dati di Nozomi su Splunk):

```
index=nozomi sourcetype="nozomi:session"
```

Con questa query stiamo effettuando una ricerca sull'indice "nozomi" e sul sourcetype chiamato "nozomi:session", escludendo tutti gli eventi relativi ad altri indici e sourcetype. Specifichiamo il time range d'interesse (di default sulle ultime 24 ore) ed eseguiamo la ricerca.

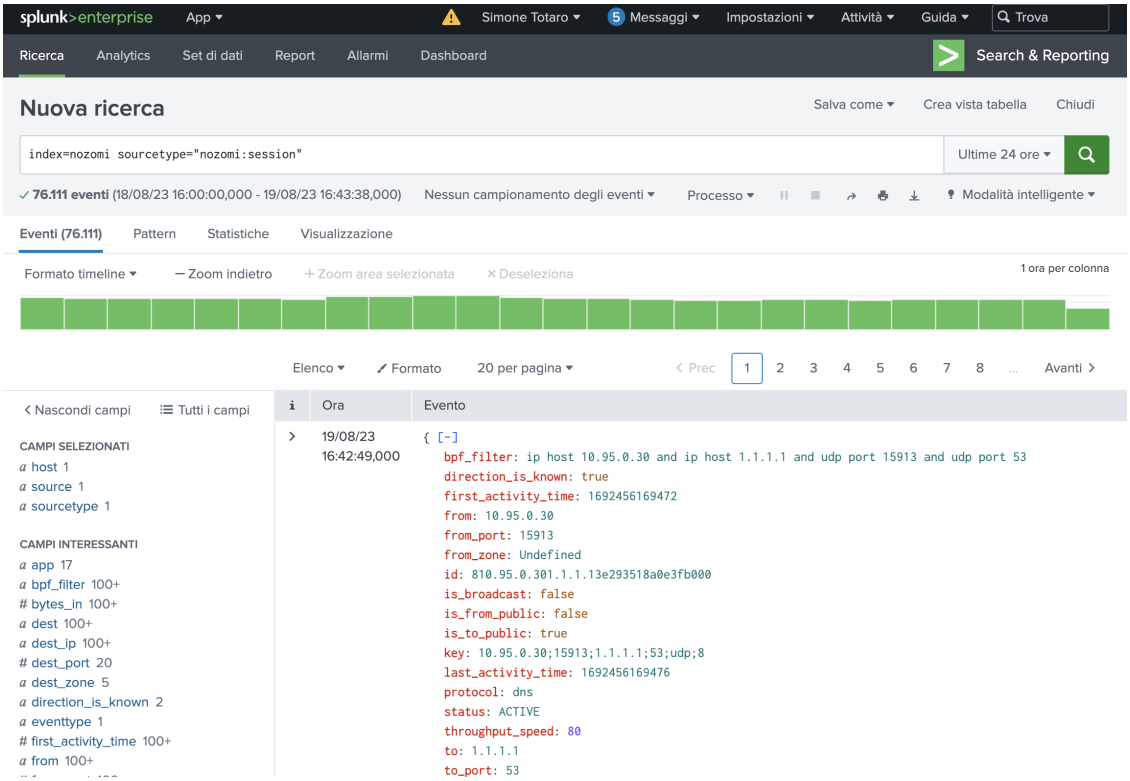


Figura 3.7. Esempio di una semplice query SPL

La ricerca ha restituito oltre 76.000 eventi nelle ultime 24 ore, ognuno dei quali avente una serie di campi che contengono determinati valori, come ad esempio user, src_ip e dest_ip (indirizzi IP sorgente e destinazione), e così via. In particolare, Splunk effettua una suddivisione dei campi in due categorie, ovvero **Selected Fields** (campi selezionati) e **Interesting Fields** (campi interessanti).

A sinistra dell'elenco degli eventi vediamo dunque la barra laterale relativa ai Campi. Gli Interesting Fields sono campi che compaiono in almeno il 20% degli eventi, mentre i Selected Fields sono i campi principali che vengono estratti in ogni ricerca, ovvero:

- **Host**: indica il nome della macchina o del dispositivo da cui proviene l'evento.
- **Source**: rappresenta la fonte fisica dell'evento, come un file, una porta di rete o uno script da cui proviene l'evento.
- **Sourcetype**: definisce il tipo di dati dell'evento, aiutando a categorizzarli per una migliore analisi.

Facendo clic su un campo si visualizzano un elenco di valori per quel campo, un conteggio dei valori e una percentuale degli eventi in cui viene visualizzato il valore. Inoltre, cliccando sopra una determinata coppia campo-valore essa verrà aggiunta alla ricerca.

Sono presenti tre diverse modalità per definire il livello di dettaglio che verrà utilizzato durante l'esecuzione di una ricerca (opzione in alto a destra in Figura 3.7):

1. **Fast Mode (Modalità Veloce)**: Esegue la ricerca nel modo più rapido possibile, sacrificando alcuni dettagli nell'elaborazione, infatti, l'individuazone automatica dei campi è disattivata. È la modalità ideale per eseguire ricerche veloci su grandi volumi di dati quando non è fondamentale la precisione dei dettagli.
2. **Smart Mode (Modalità Intelligente)**: Buon compromesso tra velocità e completezza dei risultati. Alcune funzionalità di elaborazione avanzate saranno abilitate, consentendo di ottenere risultati più completi rispetto alla modalità veloce. È un'ottima scelta quando si desidera ottenere risultati accurati in tempi ragionevolmente rapidi.
3. **Verbose Mode (Modalità Dettagliata)**: Questa modalità restituisce risultati estremamente dettagliati e completi ed è l'opzione migliore in scenari in cui la precisione dei risultati è fondamentale, anche se richiede più tempo.

Esempio di query SPL concatenate

L'operatore di pipe "|" è utilizzato per concatenare comandi in una sequenza e per trasferire i risultati della prima parte della ricerca alla successiva, in modo da costruire ricerche complesse.

Aggiungendo alla ricerca precedente i comandi: *stats count by transport_protocol*, la query completa diventerà:

```
index=nozomi sourcetype=nozomi:session
| stats count by transport_protocol
```

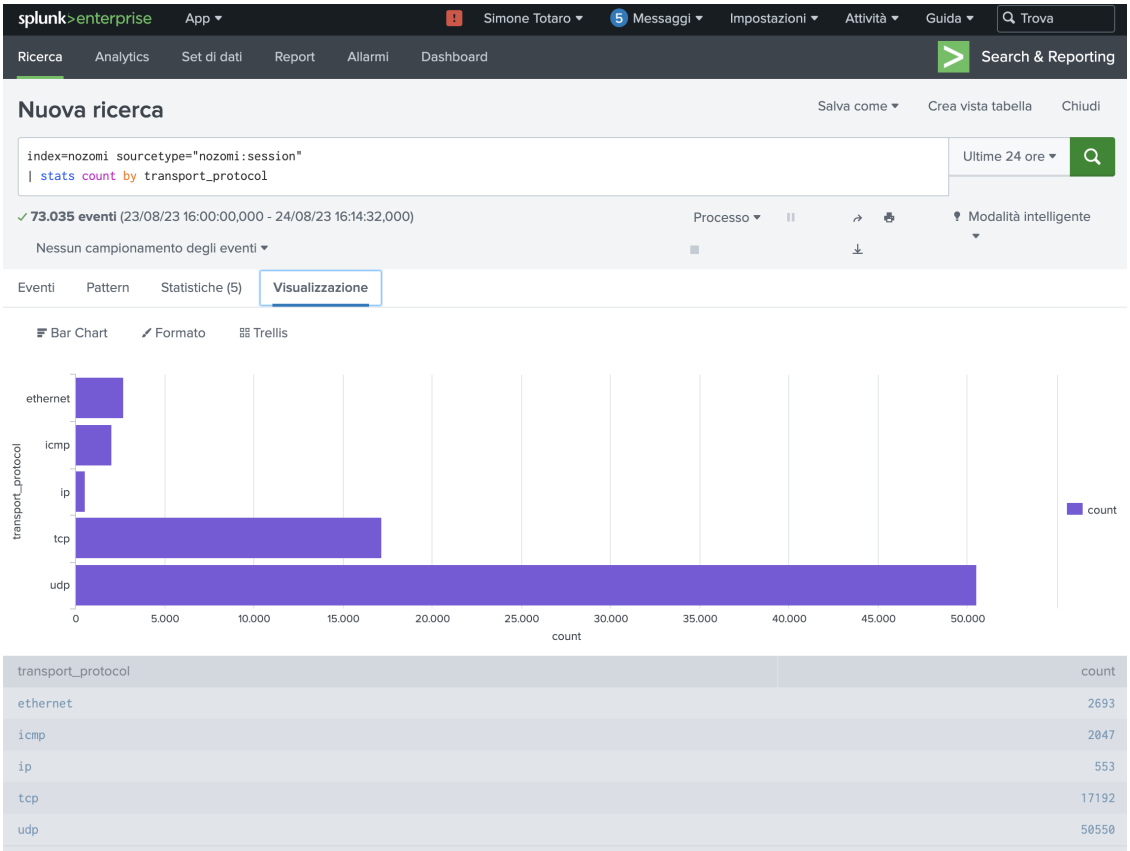


Figura 3.8. Esempio del comando "stats"

Così, dopo aver filtrato gli eventi con *index=nozomi* e *sourcetype="nozomi:session"*, con il comando *stats* calcoliamo il conteggio di eventi per ogni protocollo di trasporto.

Nella sezione "Visualizzazione" vediamo una tabella (Figura 3.8) che riporta tutti i valori del campo *transport_protocol* nella prima colonna, mentre nella seconda i rispettivi conteggi calcolati attraverso la ricerca.
Se scegliamo la visualizzazione "Bar Chart", potremo osservare gli stessi dati tramite un diagramma a barre, dove i conteggi sono rappresentati sull'asse x e i valori del campo *transport_protocol* sull'asse y.

Scriviamo invece la seguente query:

```
index=nozomi sourcetype=nozomi:session
| timechart span=1h count
```

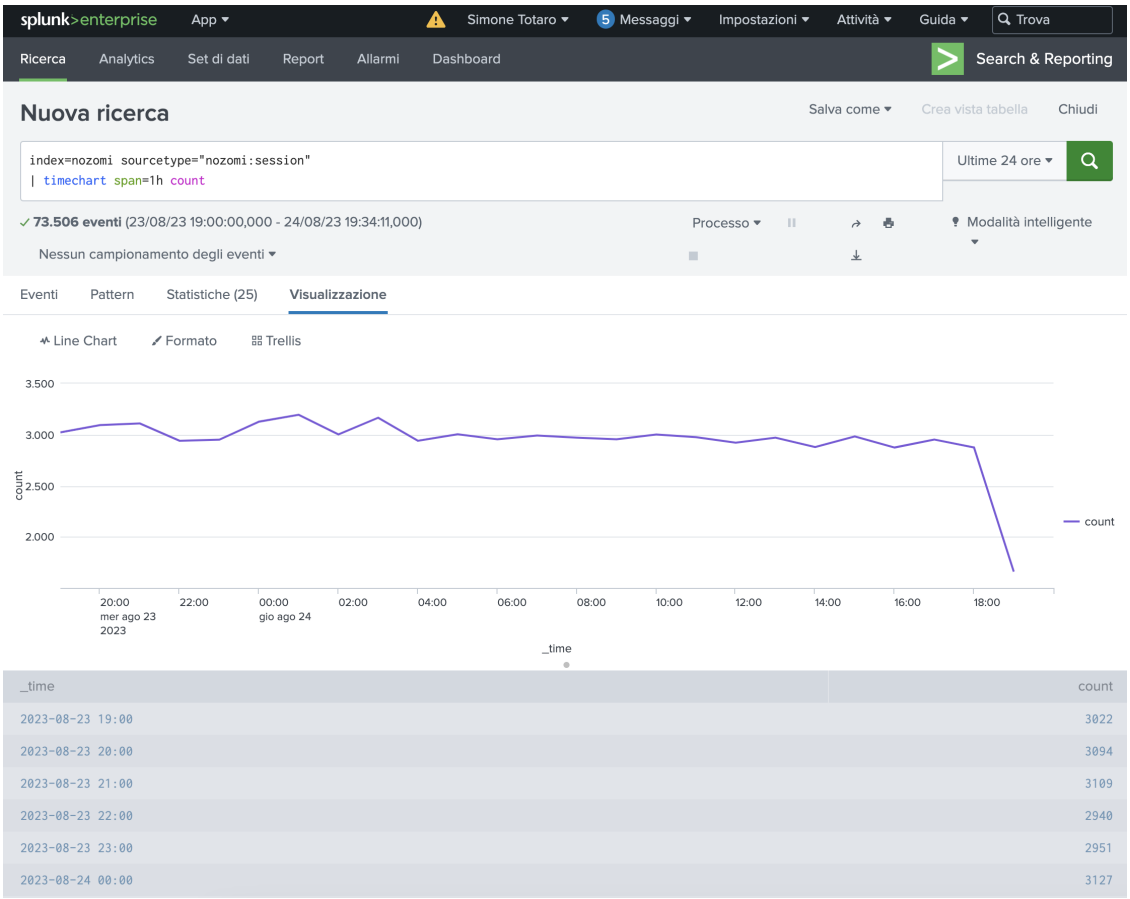


Figura 3.9. Esempio del comando "timechart"

In questo caso, la ricerca inizia con il filtraggio degli eventi e, utilizzando il comando *timechart*, viene creato un grafico che mostra il conteggio degli eventi ogni ora, utilizzando la visualizzazione "Line Chart".

Possiamo specificare l'ampiezza di ciascun intervallo di tempo attraverso il parametro "span=1h", ad esempio, se volessimo generare un grafico con intervalli giornalieri potremmo scrivere "span=1d", oppure un grafico settimanale scrivendo "span=7d", e così via.

Possiamo vedere infine il conteggio degli eventi nella tabella sottostante il grafico, accanto a ciascun timestamp.

3.4 Elastic Stack: caratteristiche e differenze con Splunk

Tra le diverse alternative a Splunk, una delle più interessanti da considerare è Elastic Stack, ovvero un insieme di tre software ampiamente utilizzati per la gestione e l'analisi dei dati: Elasticsearch, Logstash e Kibana. Questi lavorano insieme per consentire la raccolta, l'archiviazione, la ricerca e la visualizzazione dei dati in modo efficiente e intuitivo.

Ecco una breve panoramica di ciascun componente [19]:

1. **Elasticsearch**: è un motore di ricerca e analisi distribuito, progettato per gestire grandi quantità di dati e renderli facilmente accessibili e ricercabili in tempo reale. Utilizza un modello di indicizzazione basato su documenti JSON e offre potenti capacità di ricerca testuale e analitica.

2. **Logstash** è uno strumento di importazione ed elaborazione dati che permette di raccogliere dati da una varietà di fonti, trasformarli e inviarli alla destinazione desiderata, come Elasticsearch. È in grado di elaborare e normalizzare dati provenienti da log, metriche, eventi e altre sorgenti, grazie a una serie di plug-in predefiniti per supportare diverse sorgenti di dati.

3. **Kibana**: è un'interfaccia utente che permette di visualizzare e interagire con i dati archiviati in Elasticsearch, con il quale è possibile creare dashboard, grafici, mappe e visualizzazioni personalizzate per analizzare i dati in modo visivo e intuitivo.

Sostanzialmente il funzionamento di Elastic Stack è il seguente: innanzitutto Logstash importa, trasforma e invia i dati ad Elasticsearch, il quale indicizza, analizza e ricerca i dati importati ed infine Kibana visualizza i risultati dell'analisi. Tale funzionamento ricorda molto l'architettura di Splunk, descritta nel paragrafo 3.2.2.

Poiché condividono molte somiglianze in diversi aspetti, vedi ad esempio lo screenshot di Kibana in Figura 3.10 simile alla visualizzazione degli eventi di Splunk, la preferenza tra i due software dipende principalmente dal contesto specifico in cui vengono impiegati e dai casi d'uso.

Un punto di forza di Splunk rispetto ad Elastic è sicuramente la velocità nell'analisi ed elaborazione dei dati, grazie soprattutto al fatto che si tratta di un software a pagamento, a differenza di Elastic che è stata sviluppata come opzione open source ed è relativamente nuova sul mercato, dunque ancora in via di sviluppo [20].

In termini di versatilità, Splunk può accettare qualsiasi formato di dati come .csv, file di registro, JSON, ecc. ed è molto flessibile per l'integrazione con altri plug-in o strumenti. Elastic ha invece delle limitazioni, supportando principalmente dati JSON, risultando quindi meno flessibile e adattabile. Elastic inoltre utilizza la sintassi di Apache Lucene per le sue query, mentre Splunk utilizza il suo linguaggio "Search Processing Language" (SPL).

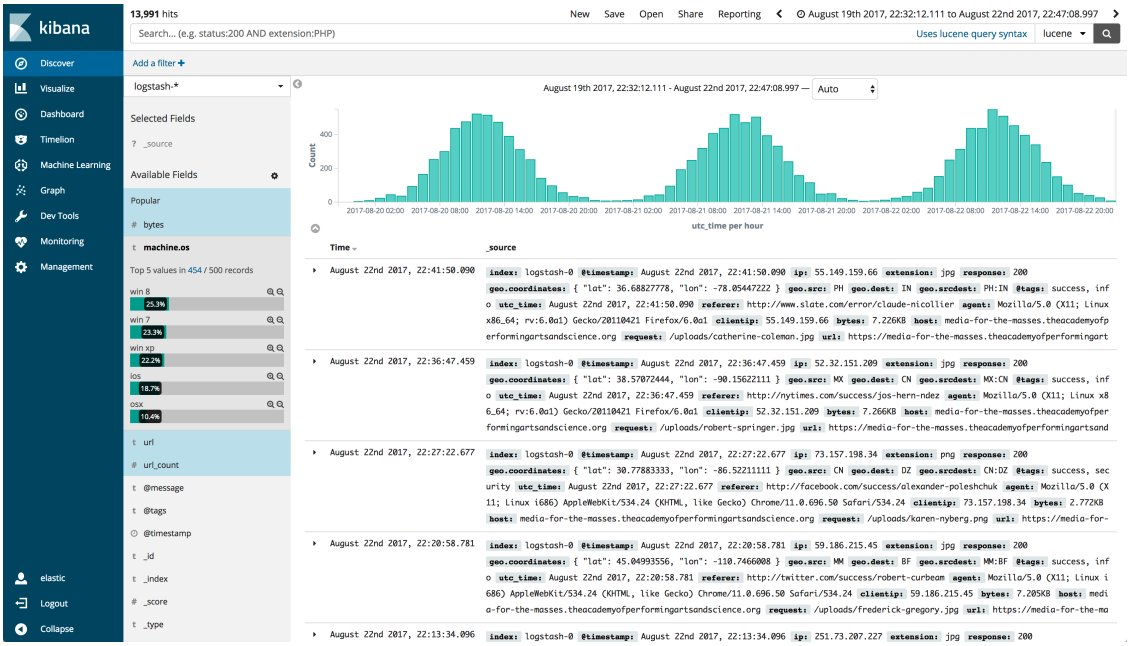


Figura 3.10. Visualizzazione eventi con Kibana

Nel contesto dell'integrazione con Nozomi Networks, Splunk risulta essere la scelta migliore grazie alla presenza di un add-on disponibile su Splunkbase, garantendo una connessione diretta tra le due piattaforme.
Dall'altro lato, attualmente non esiste un'app ufficiale o un add-on specifico su Elastic simile a quello di Splunk per implementare un'integrazione diretta con Nozomi Networks, dunque richiederebbe la creazione di un meccanismo più generico e complesso per gestire l'integrazione tra le piattaforme.

Splunk si distingue anche per via della presenza di applicazioni specifiche per la sicurezza, come InfoSec e Security Essentials.

L'app InfoSec, ad esempio, fornisce varie dashboard che offrono una visualizzazione immediata delle metriche di sicurezza chiave, consentendo di monitorare l'attività delle minacce, la presenza di malware, vulnerabilità, ecc.

L'app Security Essentials include invece ricerche, report e dashboard preconfigurati che aiutano a individuare velocemente tentativi di compromissione e anomalie nei dati. Questa include in particolare il MITRE ATT&CK Framework, ovvero uno dei principali modelli di riferimento per la mappatura delle tattiche e delle tecniche utilizzate dagli aggressori nelle fasi di attacco. L'integrazione con questo framework consente di definire ricerche SPL personalizzate per individuare potenziali attacchi e implementare un sistema di allarme per notificarne la presenza. Elastic, al momento, non offre un equivalente in questo senso.

In definitiva, nel contesto della tesi, Splunk si presenta come la scelta più idonea e conveniente.

Capitolo 4

Integrazione tra le due piattaforme

4.1 Creazione e utilizzo di chiavi API per l'integrazione dei dati

È possibile effettuare un'integrazione di Nozomi Guardian con applicazioni di terze parti sfruttando OpenAPI, in modo da poter aggiornare i dati in Guardian o ricevere dati da esso. Per autenticare tali applicazioni, Guardian utilizza una chiave API, la quale deve essere prima generata, insieme ad un token, all'interno di Guardian stesso. La chiave ed il token devono essere fornite dall'applicazione al Guardian per effettuare con successo l'autenticazione.

È importante notare che ogni chiave API è associata a un utente specifico di Guardian e rimane valida fino a quando non viene revocata o finché l'utente non viene eliminato.

Quando si definisce un utente da associare alla chiave API, è essenziale definire con attenzione l'accesso consentito, infatti è possibile limitare l'ambito, le autorizzazioni e gli intervalli IP consentiti per questo utente. Queste misure di sicurezza sono fondamentali per controllare le azioni che le applicazioni di terze parti possono eseguire in Guardian, garantendo una gestione sicura e controllata dell'accesso ai dati.

Per effettuare una connessione tra Splunk Enterprise e Nozomi Networks Guardian utilizzando OpenAPI, è dunque sufficiente seguire i seguenti passaggi:

1. **Creazione utente e concessione delle autorizzazioni**: creare su Nozomi Guardian un nuovo utente da associare alla chiave API, definendo le autorizzazioni consentite [21].
2. **Creazione chiave API in Guardian**: generare una chiave API ed un token all'interno di Nozomi Guardian, andando a specificare l'intervallo di indirizzi IP consentiti, se necessario.
3. **Installazione del Nozomi Networks add-on per Splunk**: scaricare ed installare il componente aggiuntivo da Splunkbase, il quale ci consentirà di effettuare a tutti gli effetti l'integrazione tra le due piattaforme per la ricezione dei dati da Nozomi.
4. **Autenticazione tramite API**: configurare il Nozomi Networks Add-on per Splunk, impostando il nome dell'utente, la chiave API e il token per potersi autenticare con Guardian.

4.1.1 Creazione utente e concessione delle autorizzazioni

Innanzitutto, creiamo un utente da associare all'applicazione di terze parti: apriamo dunque Nozomi Guardian ed effettuiamo l'accesso.
Navighiamo in Amministrazione → Impostazioni → Utenti e clicchiamo su "Aggiungi". Qui ci verrà richiesto di inserire il nome utente, la password, il gruppo in cui inserire l'utente (per le autorizzazioni concesse) e di specificare la sorgente, scegliendo tra *Locale*, *Active Directory*, *LDAP* e *SAML*.

La scelta della "Sorgente" si riferisce all'origine dell'utente e al sistema di autenticazione utilizzato per consentire loro l'accesso al sistema:

- **Locale**: indica che l'utente è creato e gestito direttamente nel sistema Guardian ed è un'opzione utile per la gestione degli utenti interni, come gli amministratori o gli operatori dedicati.
- **Active Directory**: è un servizio di directory di Microsoft utilizzato per gestire le identità e le risorse di rete in un ambiente Windows. Scegliendo questa opzione, significa che l'utente verrà autenticato tramite il sistema Active Directory dell'organizzazione.
- **LDAP (Lightweight Directory Access Protocol)**: è un protocollo di comunicazione utilizzato per autenticare utenti da un servizio di directory esterno. Usando questa opzione, l'utente verrà autenticato tramite un servizio di directory LDAP specifico, che potrebbe essere fornito da un provider esterno.
- **SAML (Security Assertion Markup Language)**: è uno standard per l'autenticazione basata su token utilizzato in scenari di autenticazione single sign-on (SSO). Con questa opzione, Guardian utilizzerà SAML per autenticare l'utente attraverso un'identità federata o un provider di servizi di autenticazione SAML esterno.

La scelta della sorgente dipende principalmente dalle esigenze di autenticazione. Nel nostro caso, vogliamo gestire gli utenti specificamente all'interno di Guardian, dunque scegliamo l'opzione "Locale".

Dopo aver creato un nuovo utente, possiamo procedere alla definizione del suo gruppo di appartenenza (Figura 4.1). In questa fase si ha la possibilità di configurare le autorizzazioni dell'utente, ad esempio se avrà privilegi amministrativi, se potrà configurare specifici elementi della rete e anche a quali dati avrà accesso, come Asset, Vulnerabilità, ecc.
Nel nostro caso, ai fini di un'integrazione completa, utilizzeremo il gruppo *admin*, con tutti i privilegi di amministratore.

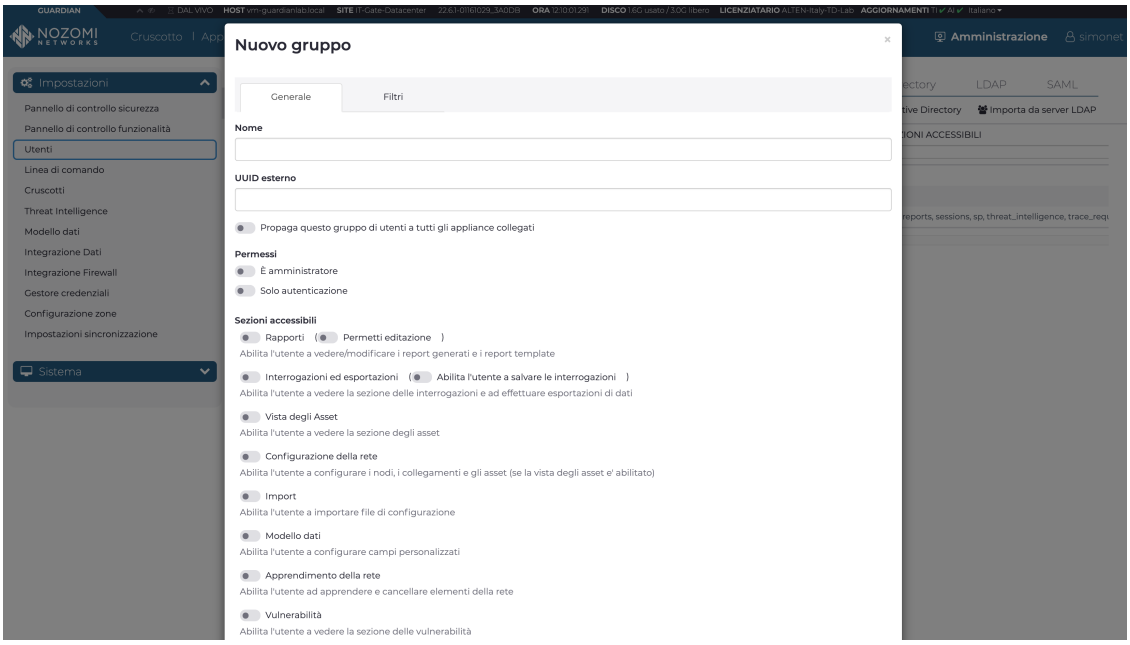


Figura 4.1. Creazione di un gruppo in Nozomi Guardian

4.1.2 Generazione chiave API in Guardian

Dopo aver creato l'utente ed il gruppo di appartenenza, possiamo procedere con la generazione della chiave API in Guardian.
Una volta effettuato l'accesso con l'utente che vogliamo sia proprietario della chiave, apriamo il menu utente nella parte superiore di qualsiasi pagina di Guardian e navighiamo in: Altre azioni → Modifica chiavi OpenAPI.

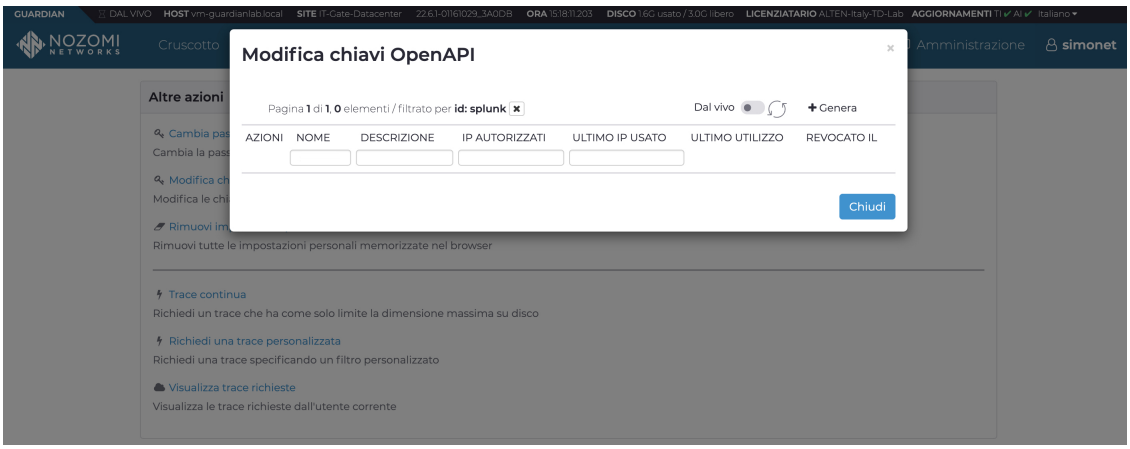


Figura 4.2. Configurazione chiavi OpenAI

Clicchiamo su Genera ed inseriamo una descrizione della chiave e l'intervallo degli indirizzi IP consentiti. Nozomi consiglia di includere nella descrizione il nome dell'applicazione che si connetterà utilizzando questa chiave. Definendo invece un intervallo IP, solo le applicazioni in esecuzione nell'intervallo specificato potranno connettersi utilizzando questa chiave.

Cliccando dunque nuovamente su Genera verrà restituito il nome (univoco) e la chiave segreta appena creata, la quale deve essere copiata e tenuta in un posto sicuro in quanto non sarà mai più possibile visualizzarla in seguito. Perdendo tale chiave sarà necessario generarne una nuova; inoltre, una volta creata, una chiave API non può essere modificata, ma solo essere revocata.

Una volta generata la chiave, è necessario definire un nuovo Endpoint all'interno di Guardian, in modo da specificare lo Splunk Forwarder che dovrà ricevere i dati di Nozomi.

Navighiamo su Amministrazione → Integrazione Dati e poi clicchiamo su Aggiungi.

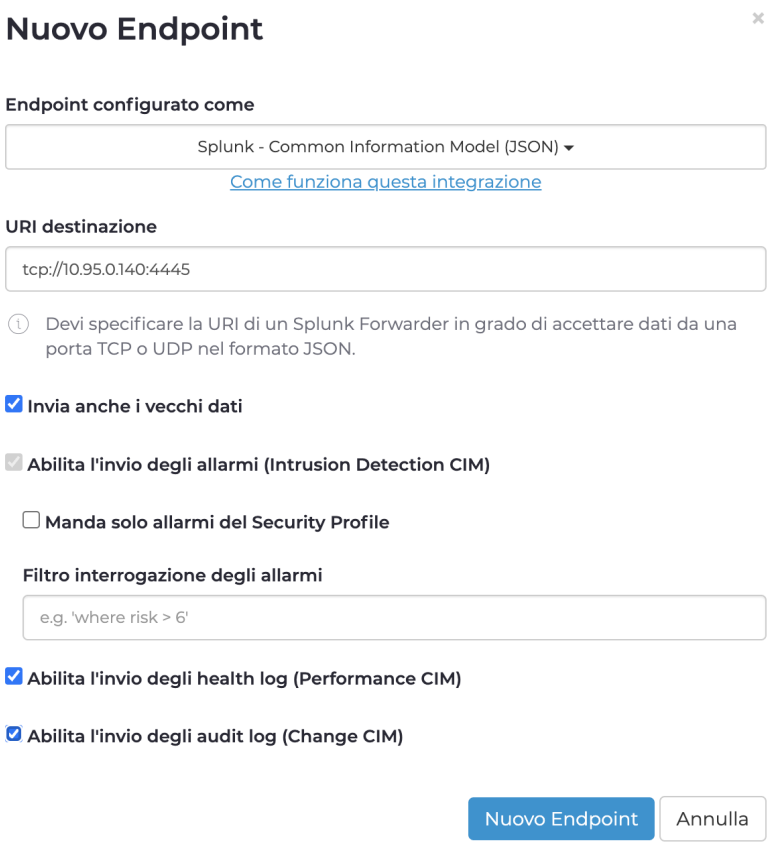


Figura 4.3. Definizione di un nuovo Endpoint

Tra le varie configurazioni disponibili dobbiamo scegliere "Splunk - Common Information Model (JSON)", indicando che i dati verranno inviati a Splunk in formato JSON. Ci verrà richiesto di inserire anche l'URI (Uniform Resource Identifier) destinazione, dunque inseriamo quello relativo al nostro Splunk Forwarder.

Infine possiamo scegliere se attivare determinate opzioni per inviare dati vecchi, o anche dati relativi agli health e audit logs. L'invio degli allarmi è attivo di default e non può essere disattivato.

Dopo aver creato l'Endpoint possiamo monitorare lo stato della connettività (figura 4.4) per vedere se la configurazione è andata a buon fine.

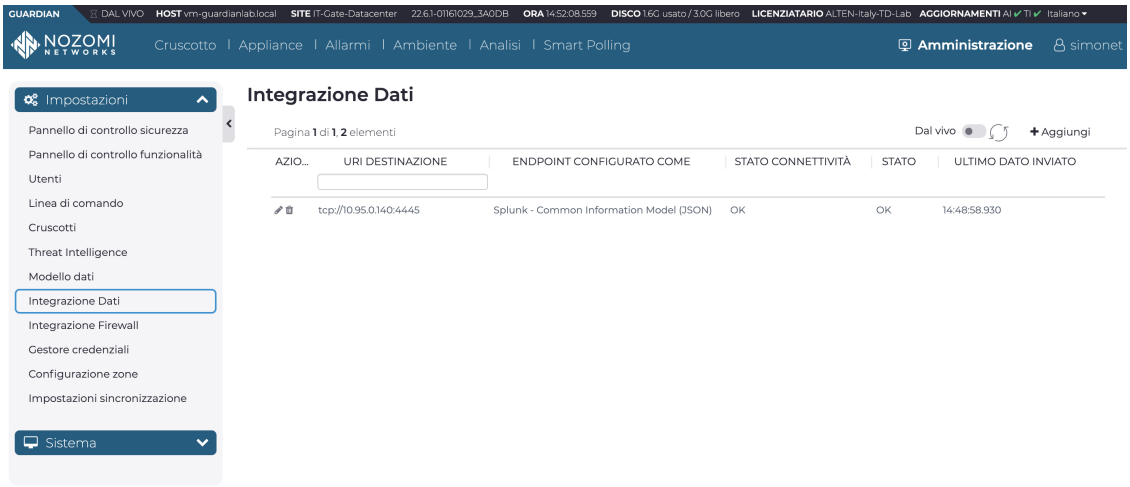


Figura 4.4. Integrazione Dati Nozomi Guardian

4.1.3 Installazione Nozomi Networks Sensor Add-on per Splunk

Adesso procediamo con l'installazione del componente aggiuntivo "Nozomi Networks Sensor Add-on", cercando tale componente nello store Splunkbase, o accedendo direttamente al seguente link: Nozomi Networks Sensor Add-on - Splunkbase [22].

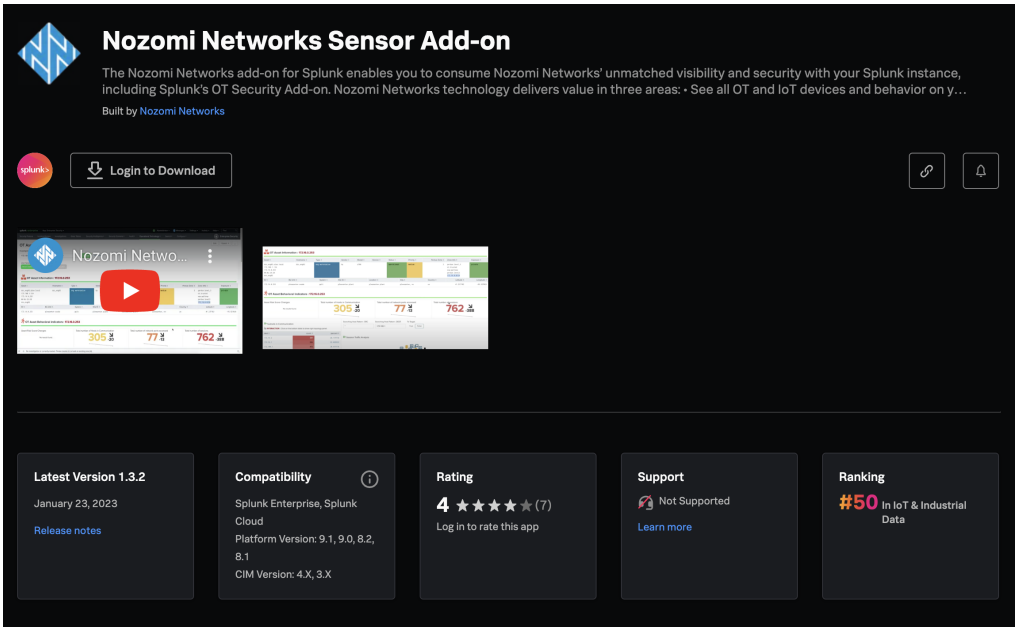


Figura 4.5. Download del Nozomi Networks Sensor Add-on

Per un corretto funzionamento dell'applicazione è importante verificarne prima la compatibilità con la propria versione di Splunk Enterprise installata (vedi riquadro "Compatibility" in figura 4.5).
Clicchiamo dunque su "Login to Download" per scaricare l'add-on, inserendo le nostre credenziali di Splunk. Verrà scaricato un file in formato ".tgz" che dobbiamo installare manualmente su Splunk Enterprise, accedendo alla piattaforma ed andando su:
App → Gestisci app → Installa app da file.

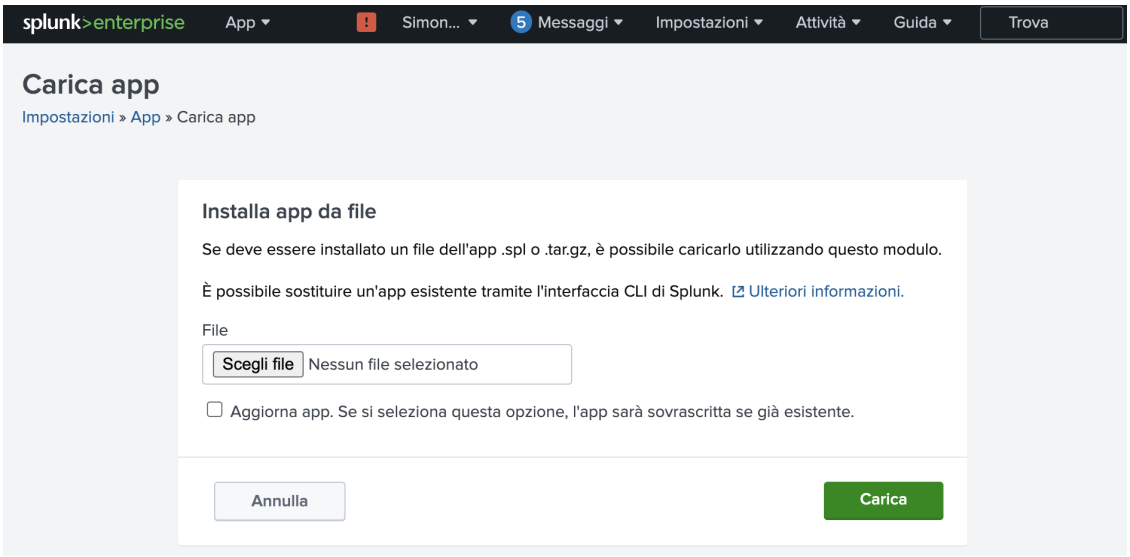


Figura 4.6. Installazione app da file su Splunk Enterprise

Qui scegliamo il file scaricato e poi clicchiamo su Carica. Successivamente, al termine dell'installazione del componente, riavviamo la nostra istanza Splunk andando su Impostazioni → Comandi del server → Riavvia Splunk.

4.1.4 Configurazione add-on e autenticazione tramite API

Procediamo ora alla configurazione dell'add-on per consentire l'autenticazione a Nozomi Guardian. Apriamo l'app appena installata (Apps → Nozomi Networks Add-on dal menu in alto) e apriamo la schermata "Configurazione". Cliccando su "Aggiungi" ci verrà chiesto di inserire le credenziali, ovvero un nome univoco per l'account (a nostra scelta), un username ed una password. Username e password non sono altro che la chiave API che abbiamo generato prima su Nozomi Guardian, ovvero il nome ed il token della chiave.

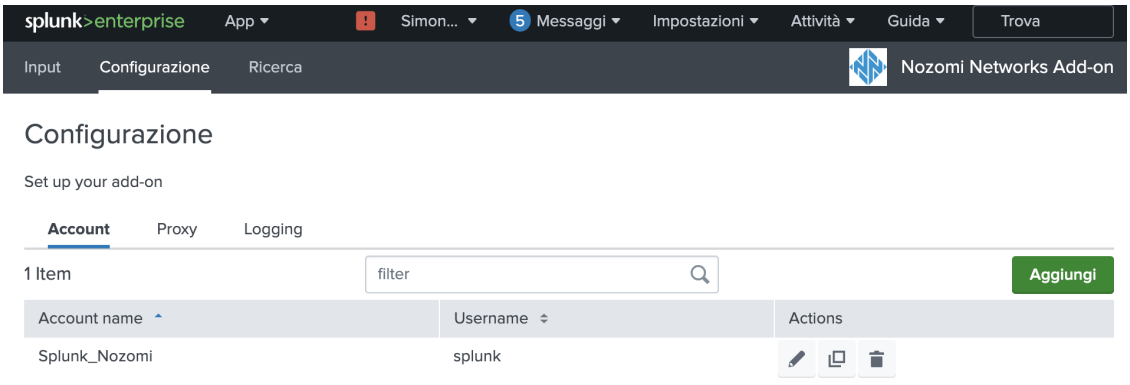


Figura 4.7. Nozomi Networks Add-on

Inseriti dunque i dati richiesti avremo completato l'autenticazione tramite API.

4.1.5 Configurazione input per ricezione dati da Nozomi Guardian

Per abilitare la ricezione delle varie tipologie di dati da Nozomi Guardian, è necessario creare nuovi input di dati all'interno del Nozomi Networks Add-on. Apriamo dunque la schermata "Input" e clicchiamo su "Create New Input", dove potremo scegliere la tipologia di dati che vogliamo ricevere, tra cui *Alerts*, *Sessions*, *Assets*, ecc. Iniziamo selezionando *Alert*.

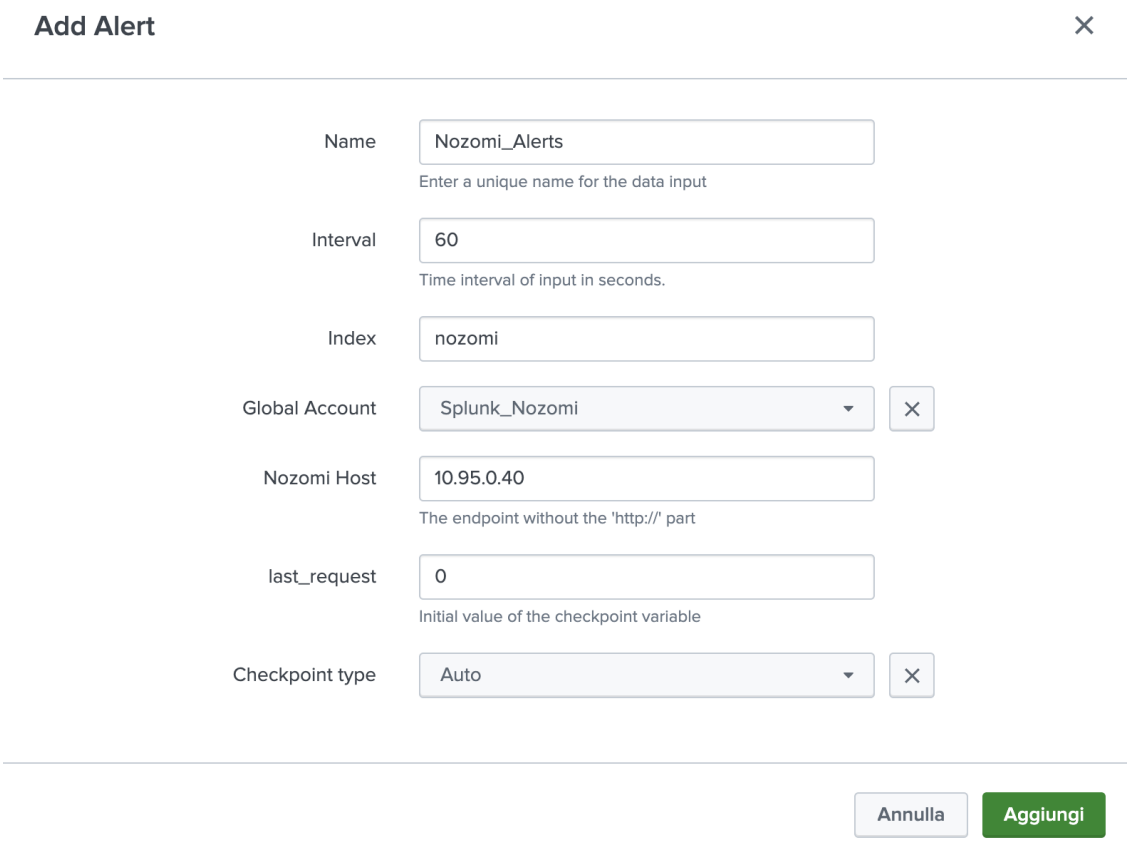


Figura 4.8. Nozomi Networks Add-on

Aggiungiamo ora le informazioni necessarie, ovvero il nome dell'input, l'intervallo in secondi in cui Splunk acquisirà i dati da Nozomi, l'indice "nozomi", l'account globale creato precedentemente, ed infine l'host di Nozomi. Manteniamo i valori predefiniti per le due informazioni finali. Ripetiamo nuovamente la stessa procedura per "Assets", "Nodes", "Sessions" e qualsiasi altro input che vogliamo includere.

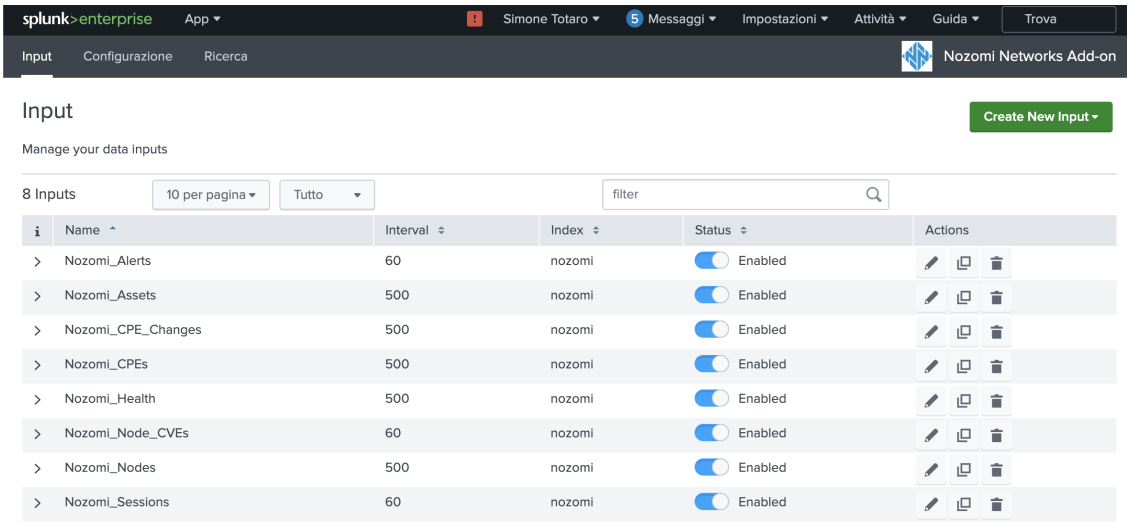


Figura 4.9. Elenco input per ricezione dati su Splunk

Per verificare il funzionamento della connessione, verifichiamo la presenza dei dati di Nozomi all'interno dell'ambiente Splunk eseguendo una ricerca. Per farlo, apriamo la scheda "Ricerca" e inseriamo una semplice query SPL, ad esempio "index=nozomi".

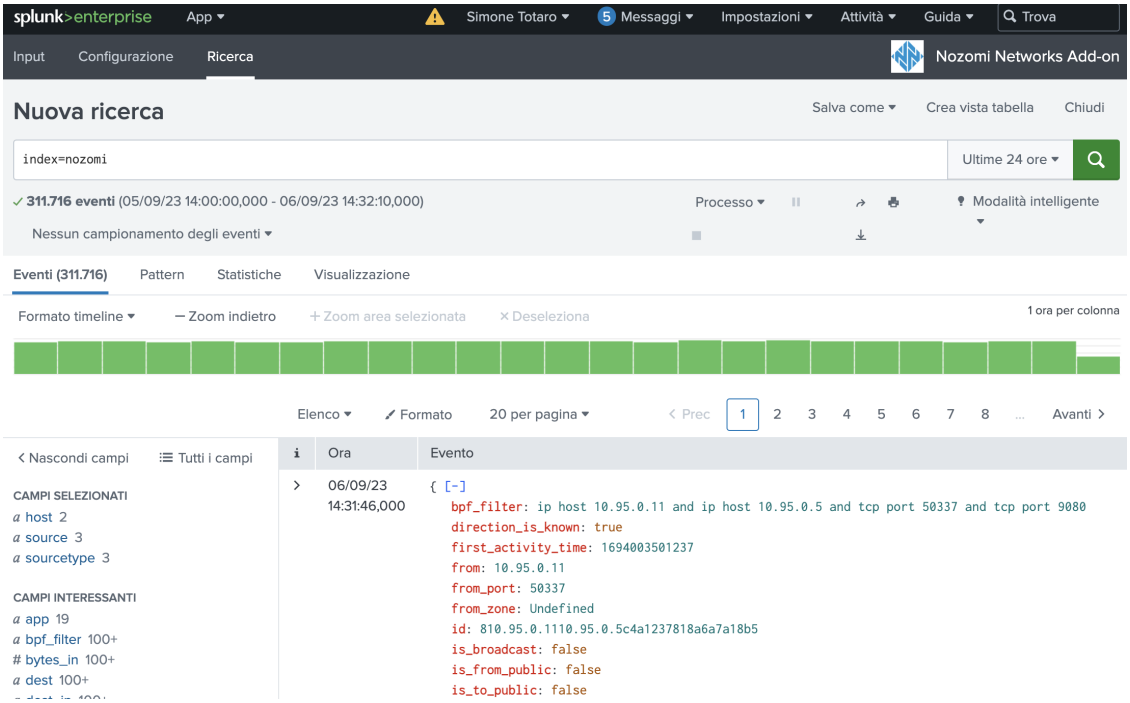


Figura 4.10. Ricerca generica per verificare il funzionamento

Notiamo che vengono restituiti eventi relativi alle ultime 24 ore, dunque la connessione ha funzionato correttamente.

4.2 Ricerca e confronto Asset per verifica correttezza dati

Dopo aver completato con successo la configurazione delle due piattaforme, procediamo con una fase iniziale di confronto dei dati, per esaminare innanzitutto il formato in cui Splunk riceve i dati e per verificare se le informazioni ricevute corrispondono a quelle presenti su Nozomi Guardian.

4.2.1 Confronto Asset di Livello 1

Come è possibile vedere nella sezione "Panoramica Asset" della schermata "Cruscotto" di Guardian (Figura 2.4), sono presenti 136 Asset totali di Livello 1, in particolare 53 di tipo "Controller" e 83 di tipo "OT Device". In questa fase possiamo effettuare un primo controllo per verificare che Splunk riceva lo stesso numero di asset per entrambe le tipologie.

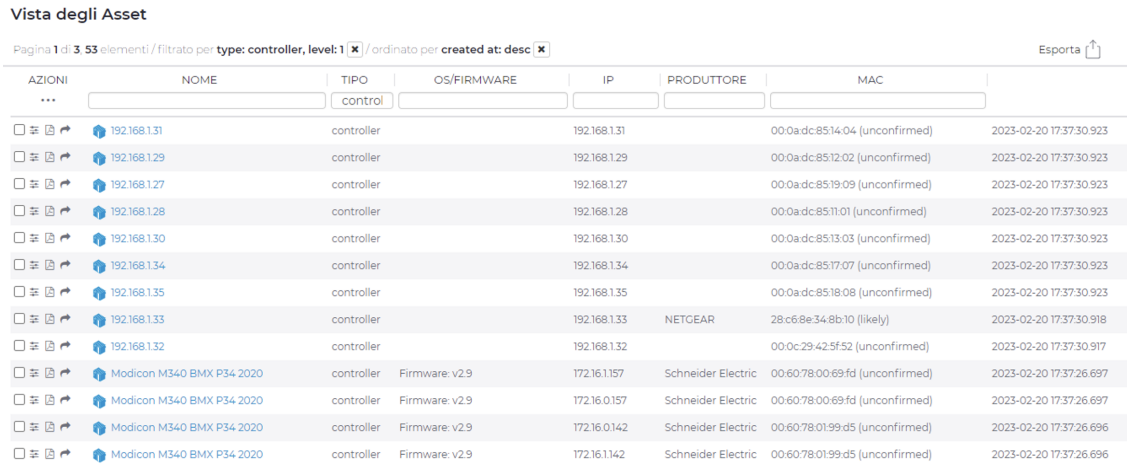


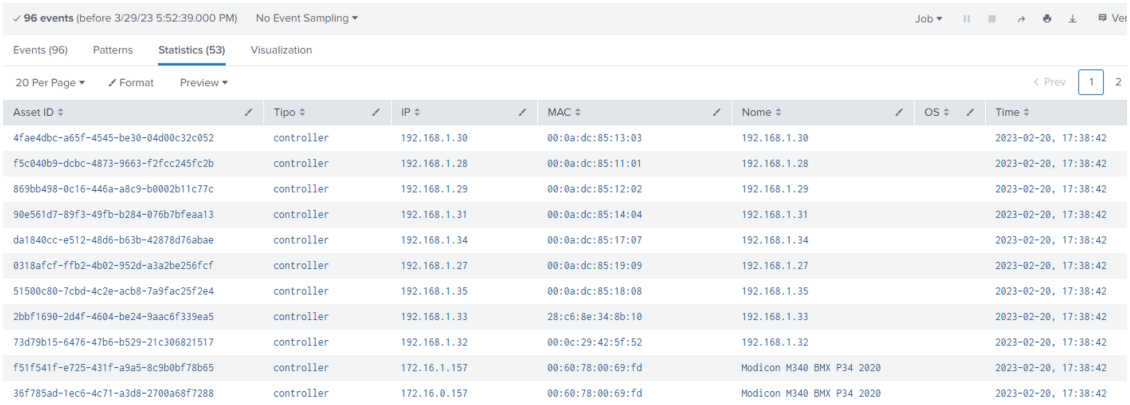
Figura 4.11. Vista degli Asset di tipo "controller" su Guardian

Nella Figura 4.11 vediamo gli asset di tipo "Controller" presenti sulla rete. Scriviamo una query SPL per cercare le stesse informazioni su Splunk.

```
(index="nozomi") sourcetype="*asset*" type=controller
| eval Time = strftime(_time, "%F, %T")
| rename ip{} as IP, mac_address{} as MAC, asset_id as "Asset ID",
   name as Nome, os as OS
| dedup IP
| table "Asset ID" IP MAC Nome OS Time
| sort -Time
```

Questa query filtra gli eventi nell'indice "nozomi" con sourcetype contenente la parola "asset" e tipo "controller". Tramite il comando *eval* viene creato un nuovo campo chiamato "Time" utilizzando la funzione 'strftime' per formattare il campo *_time* nel formato "AAAA-MM-GG, HH:MM:SS".

Con *rename* rinominiamo alcuni campi per renderli più leggibili, mentre con *dedup* eliminiamo le righe duplicate basate sul campo "IP". Infine creiamo una tabella con i vari campi elencati nel comando *table* e la ordiniamo in base al campo "Time" in ordine decrescente.



✓ 96 events (before 3/29/23 5:52:39.000 PM) No Event Sampling — Job

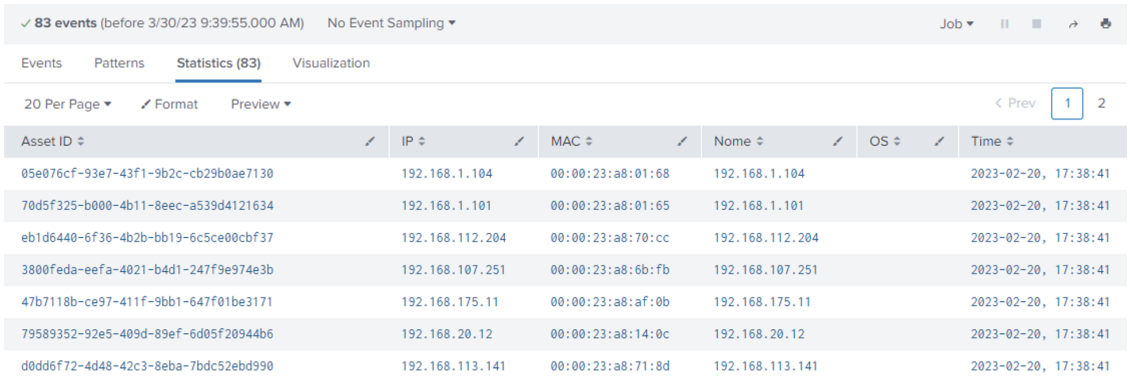
Events (96) | Patterns | Statistics (53) | Visualization

20 Per Page | Format | Preview — Prev 1 2

Asset ID	Tipo	IP	MAC	Nome	OS	Time
4fae4dbc-a65f-4545-be30-04d00c32c052	controller	192.168.1.30	00:0a:dc:85:13:03	192.168.1.30		2023-02-20, 17:38:42
f5c040b9-dcbc-4873-9663-f2fcc245fc2b	controller	192.168.1.28	00:0a:dc:85:11:01	192.168.1.28		2023-02-20, 17:38:42
869bb498-0c16-446a-a8c9-b0002b11c77c	controller	192.168.1.29	00:0a:dc:85:12:02	192.168.1.29		2023-02-20, 17:38:42
90e561d7-89f3-49fb-b284-076b7bfeaa13	controller	192.168.1.31	00:0a:dc:85:14:04	192.168.1.31		2023-02-20, 17:38:42
da1840cc-e512-48d6-b63b-42878d76abae	controller	192.168.1.34	00:0a:dc:85:17:07	192.168.1.34		2023-02-20, 17:38:42
0318afcf-ffb2-4b02-952d-a3a2be256fcf	controller	192.168.1.27	00:0a:dc:85:19:09	192.168.1.27		2023-02-20, 17:38:42
51500c80-7cbd-4c2e-acb8-7a9fac25f2e4	controller	192.168.1.35	00:0a:dc:85:18:08	192.168.1.35		2023-02-20, 17:38:42
2bbf1690-2d4f-4604-be24-9aac6f339ea5	controller	192.168.1.33	28:c6:8e:34:8b:10	192.168.1.33		2023-02-20, 17:38:42
73d79b15-6476-47b6-b529-21c306821517	controller	192.168.1.32	00:0c:29:42:5f:52	192.168.1.32		2023-02-20, 17:38:42
f51f541f-e725-431f-a9a5-8c9b0bf78b65	controller	172.16.1.157	00:60:78:00:69:fd	Modicon M340 BMX P34 2020		2023-02-20, 17:38:42
36f785ad-1ec6-4c71-a3d8-2700a68f7288	controller	172.16.0.157	00:60:78:00:69:fd	Modicon M340 BMX P34 2020		2023-02-20, 17:38:42

Figura 4.12. Ricerca Asset di tipo "controller" su Splunk

La ricerca (eseguita su time range "Sempre") ha restituito gli stessi 53 asset presenti su Guardian, come è possibile vedere confrontando i dati delle figure 4.11 e 4.12. Modificando leggermente la query, scrivendo *type="OT_device"*, cerchiamo tutti gli eventi relativi agli asset di tipo "OT_device".



✓ 83 events (before 3/30/23 9:39:55.000 AM) No Event Sampling — Job

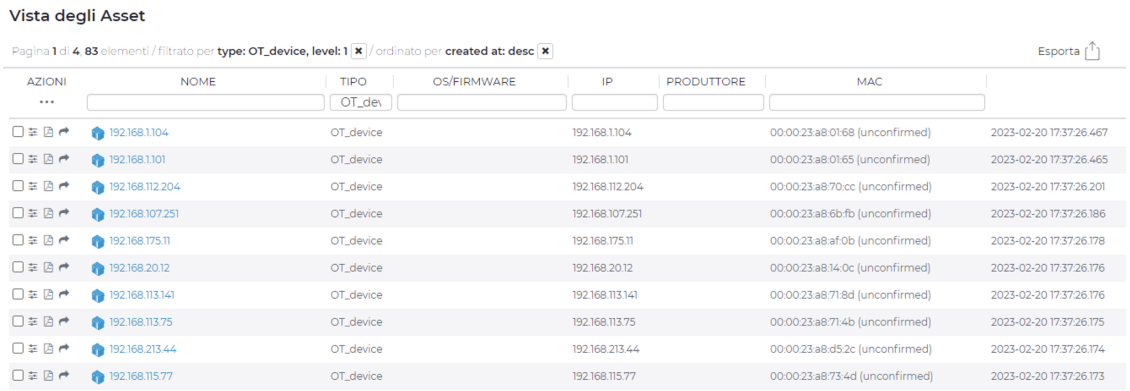
Events | Patterns | Statistics (83) | Visualization

20 Per Page | Format | Preview — Prev 1 2

Asset ID	IP	MAC	Nome	OS	Time
05e076cf-93e7-43f1-9b2c-cb29b0ae7130	192.168.1.104	00:00:23:a8:01:68	192.168.1.104		2023-02-20, 17:38:41
70d5f325-b000-4b11-8eec-a539d4121634	192.168.1.101	00:00:23:a8:01:65	192.168.1.101		2023-02-20, 17:38:41
eb1d6440-6f36-4b2b-bb19-6c5ce00cbf37	192.168.112.204	00:00:23:a8:70:cc	192.168.112.204		2023-02-20, 17:38:41
3800feda-eefa-4021-b4d1-247f9e974e3b	192.168.107.251	00:00:23:a8:6b:fb	192.168.107.251		2023-02-20, 17:38:41
47b7118b-ce97-411f-9bb1-647f01be3171	192.168.175.11	00:00:23:a8:af:0b	192.168.175.11		2023-02-20, 17:38:41
79589352-92e5-409d-89ef-6d05f20944b6	192.168.20.12	00:00:23:a8:14:0c	192.168.20.12		2023-02-20, 17:38:41
d0dd6f72-4d48-42c3-8eba-7bdc52ebd990	192.168.113.141	00:00:23:a8:71:8d	192.168.113.141		2023-02-20, 17:38:41

Figura 4.13. Ricerca Asset di tipo "OT_device" su Splunk

Anche in questo caso la ricerca ha restituito gli stessi 83 asset di tipo OT_device presenti su Guardian (vedi figure 4.13 e 4.14).



Vista degli Asset

Pagina **1** di **4**, **83** elementi / filtrato per **type: OT_device, level: 1** / ordinato per **created at: desc** — Esporta

AZIONI	NOME	TIPO	OS/FIRMWARE	IP	PRODUTTORE	MAC	
...		OT_dev					
	192.168.1.104	OT_device		192.168.1.104		00:00:23:a8:01:68 (unconfirmed)	2023-02-20 17:37:26.467
	192.168.1.101	OT_device		192.168.1.101		00:00:23:a8:01:65 (unconfirmed)	2023-02-20 17:37:26.465
	192.168.112.204	OT_device		192.168.112.204		00:00:23:a8:70:cc (unconfirmed)	2023-02-20 17:37:26.201
	192.168.107.251	OT_device		192.168.107.251		00:00:23:a8:6b:fb (unconfirmed)	2023-02-20 17:37:26.186
	192.168.175.11	OT_device		192.168.175.11		00:00:23:a8:af:0b (unconfirmed)	2023-02-20 17:37:26.178
	192.168.20.12	OT_device		192.168.20.12		00:00:23:a8:14:0c (unconfirmed)	2023-02-20 17:37:26.176
	192.168.113.141	OT_device		192.168.113.141		00:00:23:a8:71:8d (unconfirmed)	2023-02-20 17:37:26.176
	192.168.113.75	OT_device		192.168.113.75		00:00:23:a8:71:4b (unconfirmed)	2023-02-20 17:37:26.175
	192.168.213.44	OT_device		192.168.213.44		00:00:23:a8:d5:2c (unconfirmed)	2023-02-20 17:37:26.174
	192.168.115.77	OT_device		192.168.115.77		00:00:23:a8:73:4d (unconfirmed)	2023-02-20 17:37:26.173

Figura 4.14. Vista degli Asset di tipo "OT Device" su Guardian

4.2.2 Eventi e verifica informazioni ricevute su Splunk

Dopo aver confrontato il numero di asset tra le due piattaforme, procediamo a un'analisi più dettagliata delle informazioni relative a un singolo asset. Iniziamo esaminando le informazioni su un asset specifico, prima su Nozomi Guardian e successivamente tramite una ricerca su Splunk.

Per fare ciò, apriamo una scheda di dettaglio di un asset su Guardian, ad esempio l'asset con l'indirizzo IP "192.168.95.15":

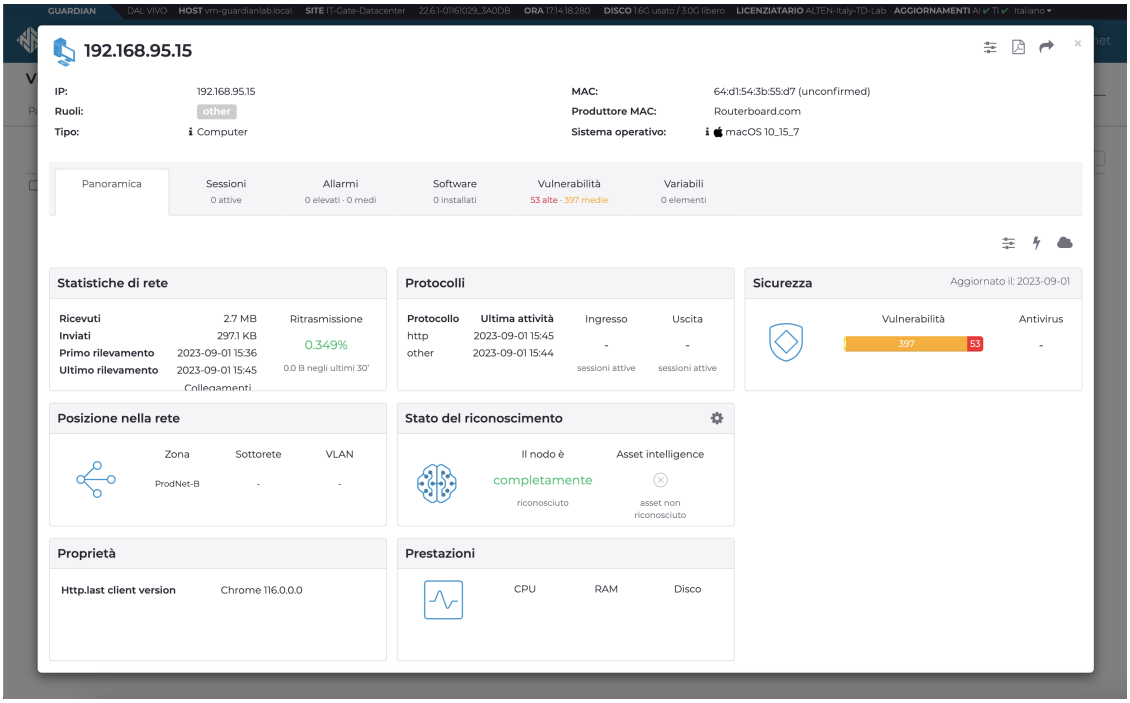


Figura 4.15. Panoramica di un asset su Guardian

Guardian ci fornirà diverse informazioni, tra cui gli indirizzi IP e MAC della macchina, il sistema operativo installato, i protocolli attivi, e altro ancora.
Ora procediamo a cercare le stesse informazioni su Splunk. Per individuare un singolo asset, basta aggiungere l'indirizzo IP specifico alla ricerca; in questo modo, Splunk restituirà soltanto gli eventi con quella particolare informazione all'interno. In alternativa, è possibile cercare direttamente una corrispondenza campo-valore scrivendo *ip="192.168.95.15"*.

Non ci interessa in questo caso visualizzare i dati in formato tabellare, dunque rimuoviamo dalla query precedente i comandi successivi alla prima *pipe*:

```
index="nozomi" sourcetype="*asset*" "192.168.95.15"
```

Visualizzando i risultati della nostra ricerca in modalità "Dati non elaborati" vediamo i dati grezzi per come vengono inviati da Nozomi, ovvero in formato JSON (figura 4.16). Le varie informazioni viste su Guardian sono dunque presenti anche su Splunk, con l'aggiunta di alcuni dati, come l'*id*, non direttamente visibili su Nozomi.

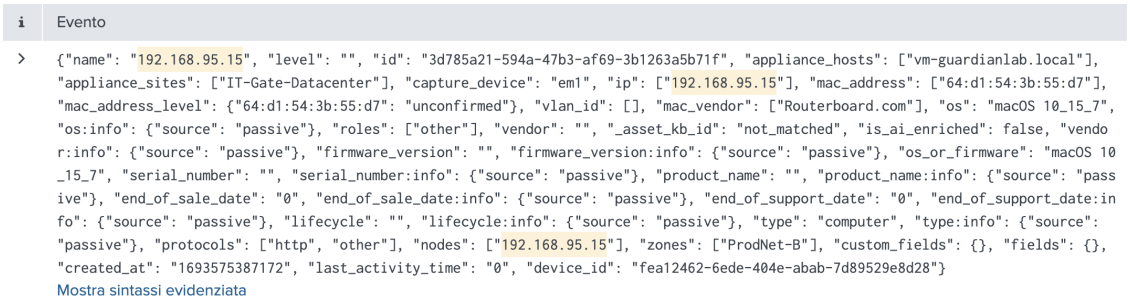


Figura 4.16. Evento Splunk in formato JSON

Se scegliamo la modalità di visualizzazione "Elenco", possiamo osservare i dati in maniera più chiara, e risulta interessante notare come avvenga l'estrazione automatica dei campi.

Figura 4.17. Evento Splunk con estrazione dei campi

Nella figura 4.17, sulla sinistra, sono evidenziati gli *Interesting Fields* (Campi Interessanti), ovvero i campi a cui Splunk assegna automaticamente dei valori durante la ricerca (a search time). È possibile aggiungere un valore specifico alla ricerca semplicemente facendo clic su di esso, direttamente dal pannello dei campi laterali oppure dall'evento stesso.

Se desideriamo creare nuovi campi personalizzati basati sui valori presenti negli eventi, abbiamo la possibilità di creare dei "Calculated Fields"(Campi Calcolati). Esploreremo questa opzione nei paragrafi successivi.

4.3 Nozomi Networks App per Splunk

Procediamo adesso a sviluppare un'applicazione dedicata all'analisi dei dati provenienti da Nozomi. Questa applicazione includerà diverse schermate e dashboard progettate per visualizzare informazioni cruciali per la sicurezza, ovvero gli accessi alla piattaforma, asset sulla rete, allarmi generati da Nozomi, vulnerabilità rilevate e altro ancora.

4.3.1 Creazione di un'applicazione su Splunk

Per creare una nuova applicazione su Splunk, accediamo alla piattaforma e navighiamo in: *App* → *Gestisci app* e clicchiamo su *Crea app*.

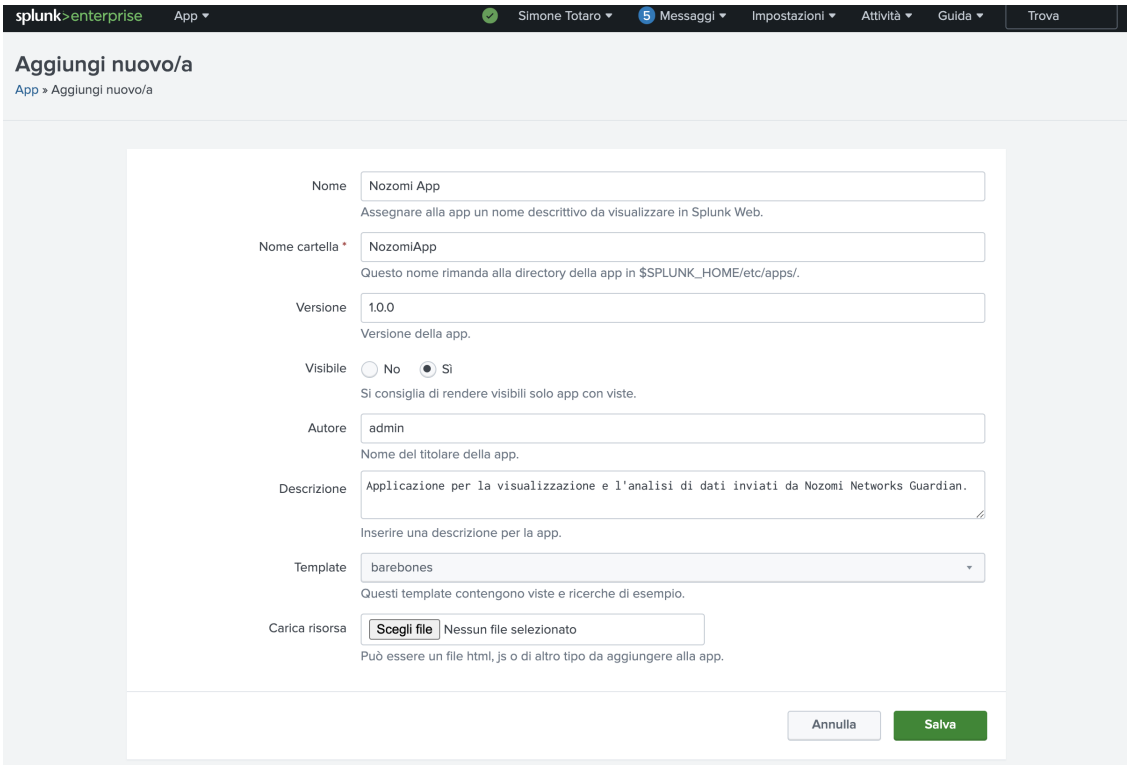


Figura 4.18. Creazione di una nuova app su Splunk

Diamo un nome all'applicazione e scegliamo il nome della cartella che verrà creata nella directory *$SPLUNK_HOME/etc/apps/*. Successivamente, scegliamo una versione per l'app, decidiamo se vogliamo renderla visibile o meno, specifichiamo l'autore, inseriamo una breve descrizione e selezioniamo infine un template (possiamo mantenere quello predefinito). Clicchiamo infine su *Salva* per creare l'applicazione.

4.3.2 Dashboard principali: illustrazione e funzionamento

L'applicazione appena creata sarà vuota, quindi ora è necessario personalizzarla aggiungendo widget e dashboard per visualizzare i dati di nostro interesse.

Per farlo, possiamo creare nuove "Viste", ovvero delle dashboard dedicate a ciascun tipo di dati che vogliamo monitorare.
Questo può essere fatto in due modi: direttamente dall'interfaccia utente di Splunk o modificando alcuni file all'interno dell'applicazione stessa. Per leggere e modificare questi file, possiamo utilizzare l'esplora risorse del nostro computer, oppure usare un'app chiamata "Config Explorer," che è disponibile su Splunkbase al seguente link: Config Explorer - Splunkbase [23].

Per creare una nuova vista, accediamo alle impostazioni dell'interfaccia utente di Splunk e, nella sezione "Viste," clicchiamo su "Nuova vista." Inseriamo un nome per la vista e definiamo la struttura della pagina utilizzando il linguaggio XML con i vari tag come "form," "panel," "row," e altri. I vari widget possono essere aggiunti anche dall'interfaccia utente, modificando la vista stessa senza scrivere il codice XML, il quale verrà generato in automatico.

Una volta create le viste, configuriamo la barra di navigazione della nostra app aggiungendo le diverse viste che abbiamo creato.

Per accedere ai file relativi all'interfaccia utente della nostra applicazione, possiamo navigare nella seguente directory:

$SPLUNK_HOME/etc/apps/NozomiApp/local/data/ui/.

Qui troveremo due cartelle, *views* e *nav*: all'interno di *views* troviamo i singoli file XML, ognuno relativo ad una determinata vista che abbiamo creato, mentre all'interno di *nav* troviamo un file chiamato "default.xml", contenente la struttura della nostra barra di navigazione.

Per l'app di Nozomi Networks, il codice XML della navbar è il seguente:

```
<nav search_view="search">
  <view name="cruscotto" default='true' />
  <view name="autenticazioni" />
  <view name="assets" />
  <view name="nodi" />
  <view name="allarmi" />
  <view name="sessioni" />
        <view name="vulnerabilita" />
  <collection label="Search">
        <view name="search" />
        <view name="analytics_workspace" />
        <view name="datasets" />
        <view name="reports" />
        <view name="alerts" />
        <view name="dashboards" />
  </collection>
</nav>
```

Esploreremo ora le dashboard principali realizzate per l'applicazione di Nozomi Networks. Per semplicità, verranno mostrate solo alcune implementazioni dei widget che le compongono, spiegando come sono stati aggiunti e definiti a livello di interfaccia utente e query SPL.

È importante sottolineare che diverse funzionalità non sono state inserite all'interno di quest'applicazione, in quanto già presenti sull'applicazione "InfoSec", illustrata in seguito.

Dashboard "Cruscotto"

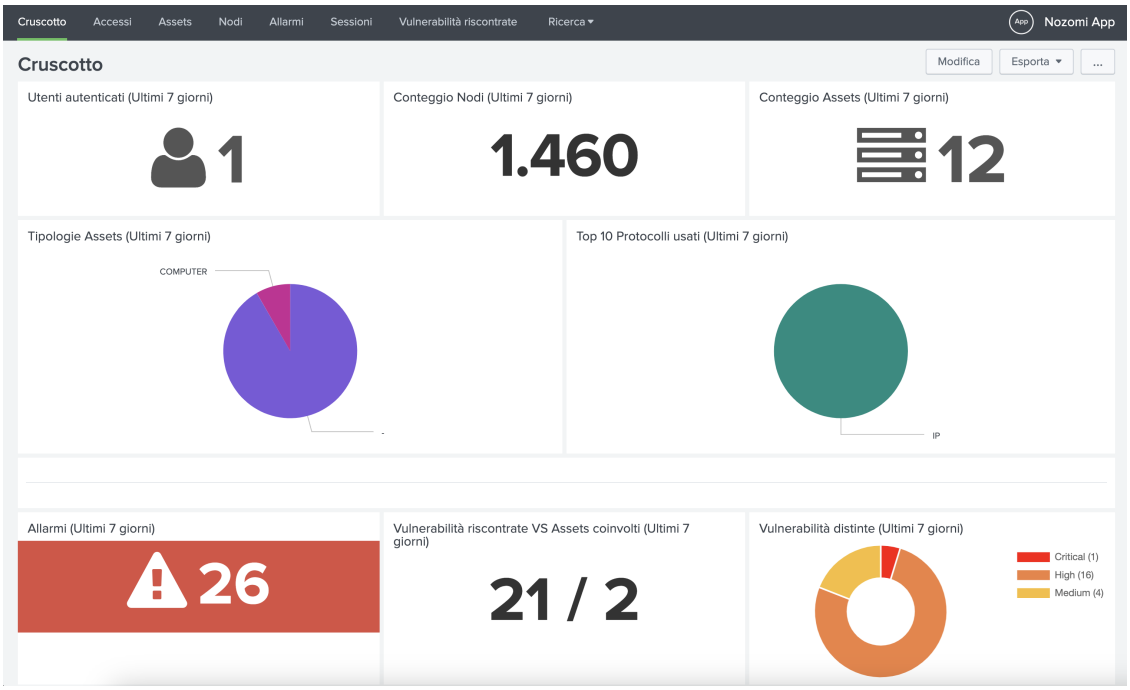


Figura 4.19. Dashboard "Cruscotto"

Notiamo innanzitutto la barra di navigazione in alto (figura 4.19), definita attraverso il codice XML riportato precedentemente.

La prima vista è un cruscotto composto da diversi widget, che consentono di consultare rapidamente alcune delle informazioni più rilevanti degli ultimi 7 giorni, quali il numero di utenti autenticati, il conteggio dei nodi e degli asset, le diverse tipologie di asset e i protocolli più utilizzati, ed infine alcuni dati sulla sicurezza come il numero di allarmi generati da Nozomi, le vulnerabilità riscontrate sugli asset e il livello di rischio associato.

Un widget interessante da analizzare è quello relativo alle "Vulnerabilità distinte", dunque vediamo come è stato aggiunto alla dashboard.
Per modificare la vista, bisogna cliccare sul pulsante "Modifica" in alto a destra, e poi su "Aggiungi pannello". A questo punto bisogna cercare la tipologia di pannello desiderata, in questo caso "Semicircle donut". Una volta selezionato, va impostato l'intervallo temporale relativo alla ricerca: questo può essere fatto scegliendo manualmente l'intervallo, oppure utilizzando un "token", i quali verranno utilizzati e spiegati in seguito.

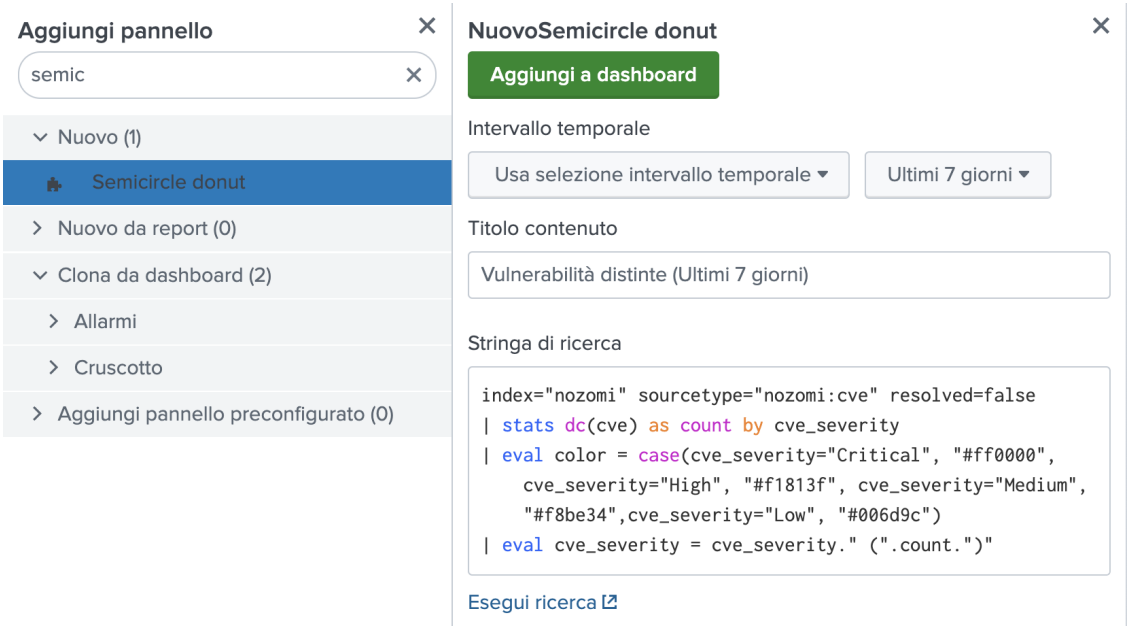


Figura 4.20. Aggiunta di un nuovo pannello

Nell'area "Stringa di ricerca" va inserita infine la query SPL che servirà per generare i valori da fornire al pannello. La query è la seguente:

```
index="nozomi" sourcetype="nozomi:cve" resolved=false
| stats dc(cve) as count by cve_severity
| eval color = case(cve_severity="Critical", "#ff0000",
   cve_severity="High", "#f1813f", cve_severity="Medium",
   "#f8be34",cve_severity="Low", "#006d9c")
| eval cve_severity = cve_severity." (".count.")"
```

Questa query analizza i dati provenienti dall'indice "nozomi" con sourcetype "nozomi:cve", selezionando solamente gli eventi in cui il campo "resolved" è impostato su "false", per indicare che stiamo cercando vulnerabilità non risolte.
Dopo il filtraggio, utilizziamo il comando *stats* per contare il numero di vulnerabilità univoche (*dc(cve) as count*) raggruppate per il campo "cve_severity", che rappresenta la gravità delle vulnerabilità. Questo ci darà il numero di vulnerabilità per ciascun livello di gravità.
Con il comando *eval* assegniamo un colore a ciascun livello di gravità delle vulnerabilità, ad esempio, se la gravità è "Critical", assegniamo il colore rosso (#ff0000).
Infine usiamo nuovamente il comando *eval* per modificare la colonna "cve_severity", aggiungendo tra parentesi il numero di vulnerabilità per ciascun livello di gravità.

Abbiamo la possibilità di definire l'azione da eseguire quando clicchiamo su un widget. Per esempio, possiamo configurarlo in modo da avviare una ricerca SPL in una nuova pagina, consentendo così la visualizzazione degli eventi correlati.
In questo caso, impostiamo il widget in modo che, al clic, venga aperta la dashboard relativa alle vulnerabilità rilevate. Per farlo, clicchiamo nuovamente su "Modifica" e successivamente su "Modifica drilldown".

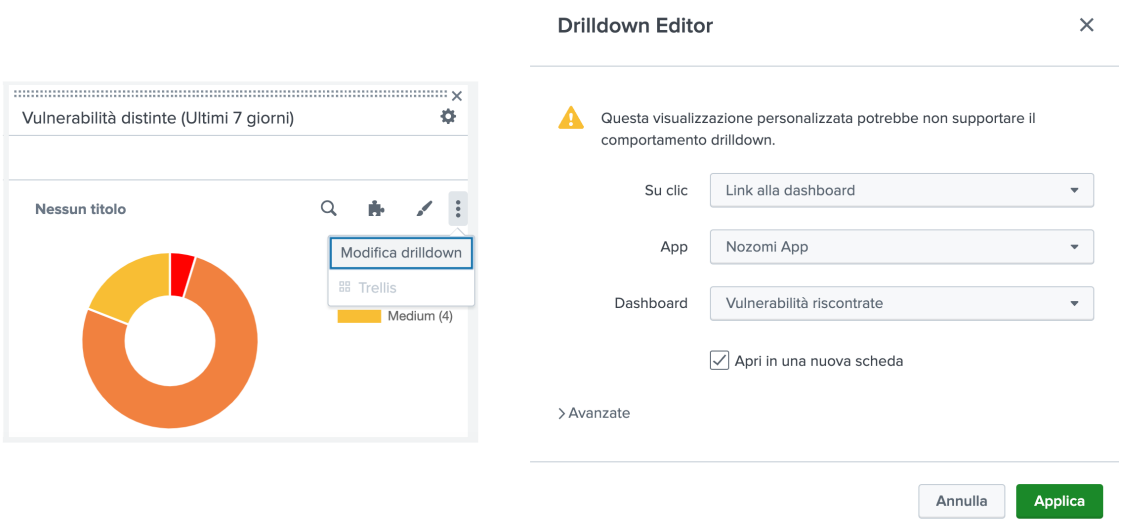


Figura 4.21. Drilldown Editor di un pannello

Qui selezioniamo "Link alla dashboard" tra le varie opzioni e poi scegliamo l'applicazione e la dashboard che vogliamo aprire.
Selezionando invece "Link alla ricerca" potremmo eseguire in una nuova scheda la ricerca SPL definita all'interno del pannello, o in alternativa definire una nuova query e un nuovo time range, se necessario.

Dashboard "Accessi"

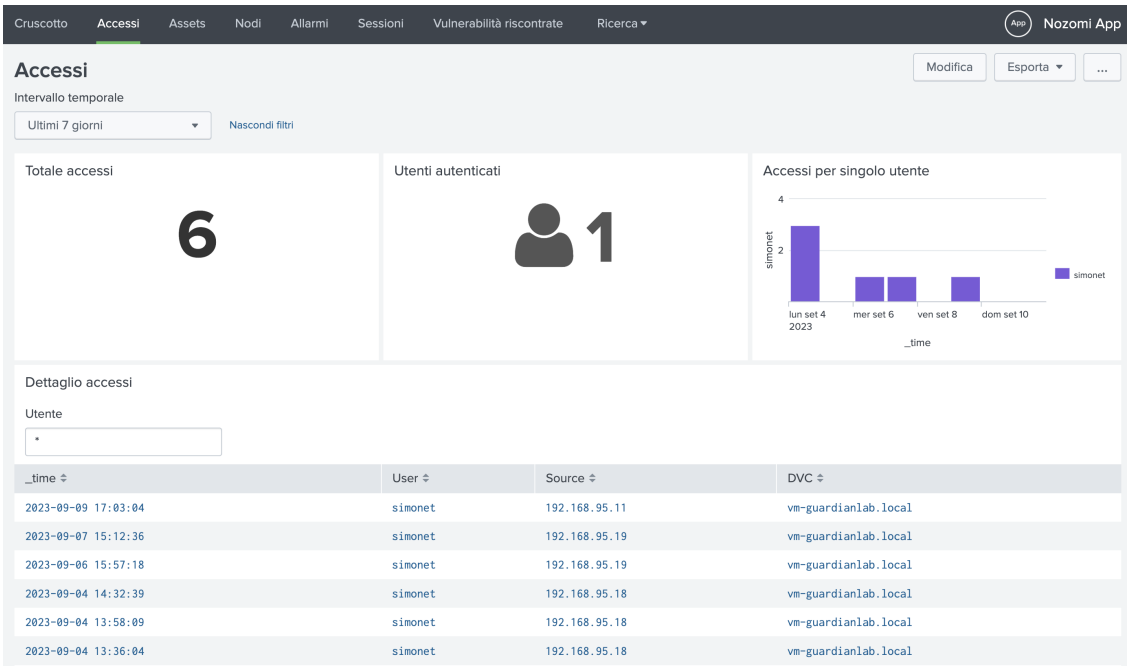


Figura 4.22. Dashboard "Accessi"

Questa dashboard è stata realizzata per il monitoraggio degli accessi alla piattaforma Nozomi Guardian nell'intervallo di tempo selezionato, riportando: il numero totale di accessi, il numero di utenti univoci autenticati, un istogramma che mostra il numero di accessi per ciascun utente, ed infine una tabella che elenca tutti gli accessi alla piattaforma. Tale tabella presenta il timestamp dell'accesso, il nome dell'utente, l'indirizzo IP della macchina utilizzata e il dispositivo.

Dashboard "Assets"

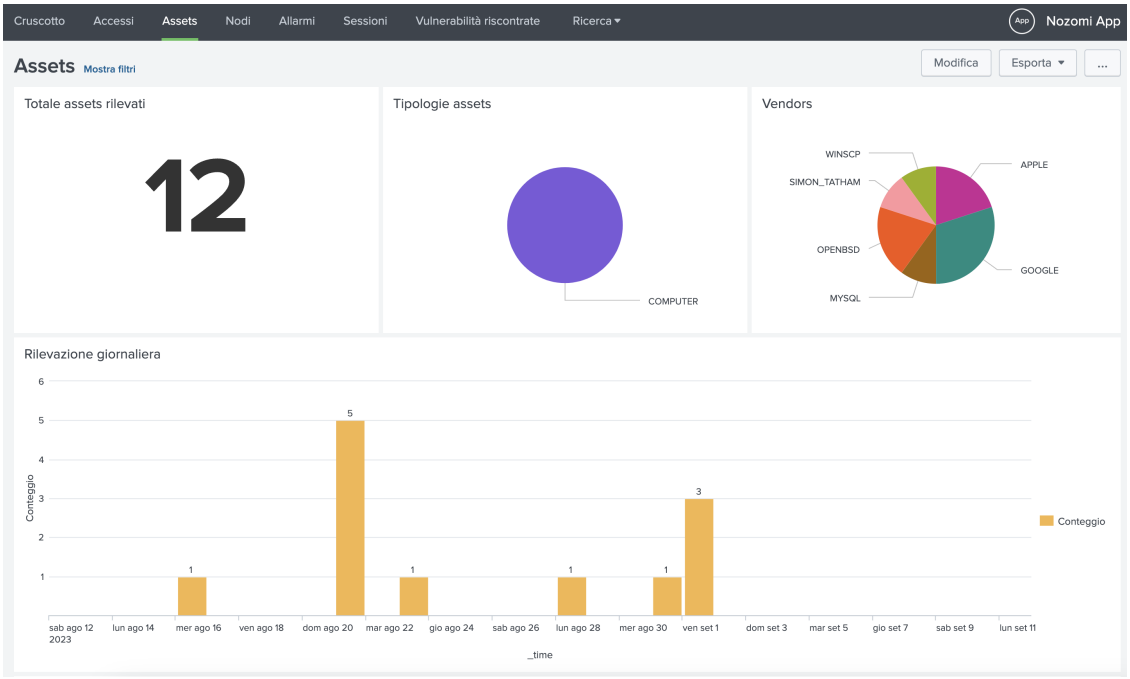


Figura 4.23. Dashboard "Assets"

Questa dashboard consente di tenere traccia dei nuovi asset rilevati su Nozomi durante l'intervallo di tempo selezionato, mostrando il conteggio totale, le tipologie, i venditori ed un conteggio giornaliero.

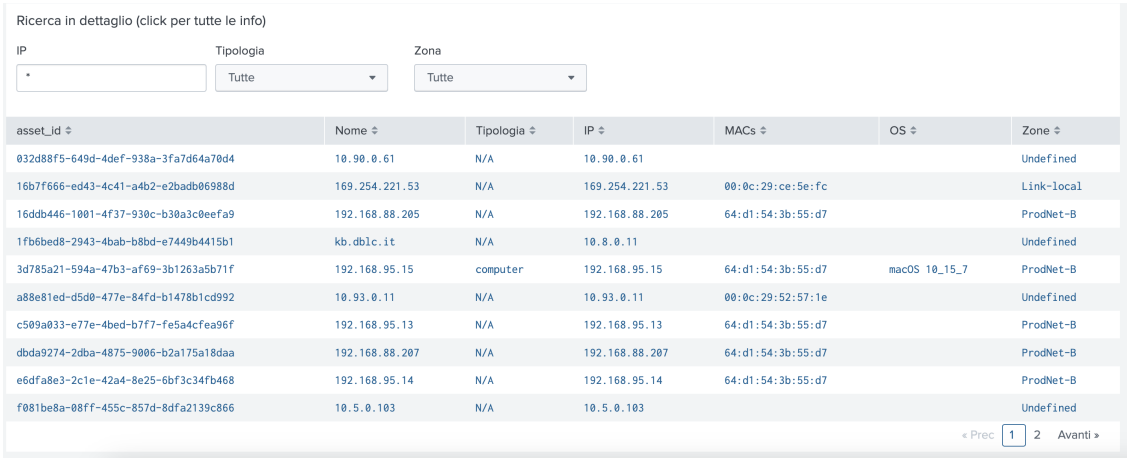


Figura 4.24. Widget per ricerca dettagliata asset

È stato aggiunto anche un widget per effettuare una ricerca rapida di un asset, filtrando per indirizzo IP, tipologia e zona. La tabella mostra dunque le informazioni più rilevanti di ciascun asset, con la possibilità di selezionarne uno per effettuare una ricerca dettagliata nella stessa scheda. Vediamo dunque come è stato realizzato questo widget.

La query di ricerca utilizzata è la seguente:

```
index=nozomi ((sourcetype="nozomi:nn_asset" "zones{}"="$zona_tok$"
    "ip{}"="*$ip_tok$*" ) OR (sourcetype="nozomi:node_cpe"
    cpe_vendor="*"))
| fillnull asset_type value="N/A"
| search asset_type="$tipologia_tok$"
| fields name,cpe_vendor, product_name,asset_type, os, mac_address{},
    zones{}, ip{}, asset_version, asset_id
| stats values(*) as * by asset_id
| search asset_id!="" AND name=*
| rename ip{} as IP, mac_address{} as MACs, asset_version as
    "Versione", product_name as Prodotto, name as Nome, asset_type as
    Tipologia, os as OS, "zones{}" as Zone, cpe_vendor as Vendor
| table asset_id, Nome, Tipologia, IP, MACs, OS, Zone
```

Questa query, attraverso un filtro condizionale, estrae eventi da due tipi di sourcetype, ovvero *nozomi:nn_asset* e *nozomi:node_cpe*:

- Per *nozomi:nn_asset* vengono cercati eventi in cui il campo *zones{}* è uguale al valore specificato nella variabile *$zona_tok$* ed eventi in cui il campo *ip{}* contiene il valore specificato nella variabile *ip_tok**.
- Per *nozomi:node_cpe*, viene cercato qualsiasi evento che abbia il campo *cpe_vendor* definito.

Il comando *fillnull asset_type value="N/A"* sostituisce i valori nulli nel campo *asset_type* con "N/A".

Con *search asset_type="$tipologia_tok$"* vengono filtrati ulteriormente gli eventi in base al valore specificato nella variabile *$tipologia_tok$* nel campo *asset_type*.

Con *stats values(*) as * by asset_id* vengono poi raggruppati i risultati in base al campo *asset_id*.

All'interno della query di ricerca sono stati utilizzati i **token**, identificati dai campi specificati tra i simboli "$". I token possono essere paragonati alle variabili nei linguaggi di programmazione, in quanto rappresentano valori variabili, come ad esempio le selezioni effettuate dagli utenti in un modulo di input. Questi valori possono essere passati tra diversi pannelli per creare dashboard interattive [24].
Alcuni token sono predefiniti in Splunk per fornire informazioni sull'ambiente, ad esempio sugli eventi di clic dell'utente, oppure possono essere creati token personalizzati.

Per utilizzarli all'interno della ricerca, tali token devono prima essere definiti all'interno dei filtri che abbiamo creato, ovvero IP, Tipologia e Zona. All'interno del pannello di ciascun filtro, va specificato il token che vogliamo utilizzare, come possiamo vedere nella figura 4.25 per il filtro Tipologia.

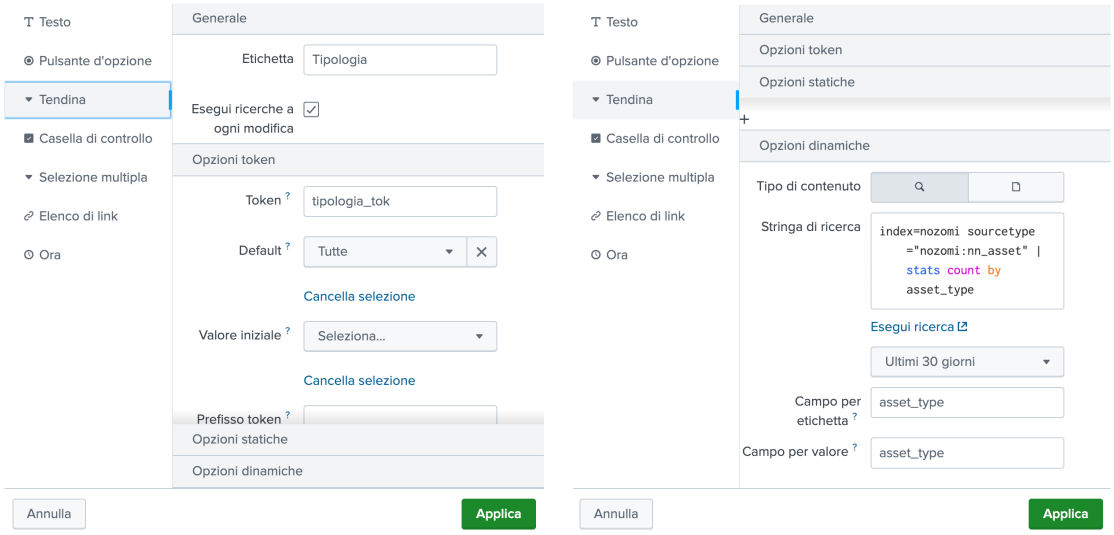


Figura 4.25. Filtro asset per tipologia

Si inserisce dunque il token e si imposta un valore di default e un valore iniziale, dopo aver inserito anche la stringa di ricerca relativa al filtro stesso. Ad esempio, per ottenere un menu dropdown con le varie tipologie degli asset, è stata scritta la seguente query:

```
index=nozomi sourcetype="nozomi:nn_asset"
| stats count by asset_type
```

In questo modo, una volta selezionato un valore dal filtro Tipologia, cambierà il valore del token *$tipologia_tok$* ed in tempo reale cambieranno i risultati della ricerca per la lista degli asset. Lo stesso è stato fatto anche per i filtri IP e Zona.

Dashboard "Nodi"

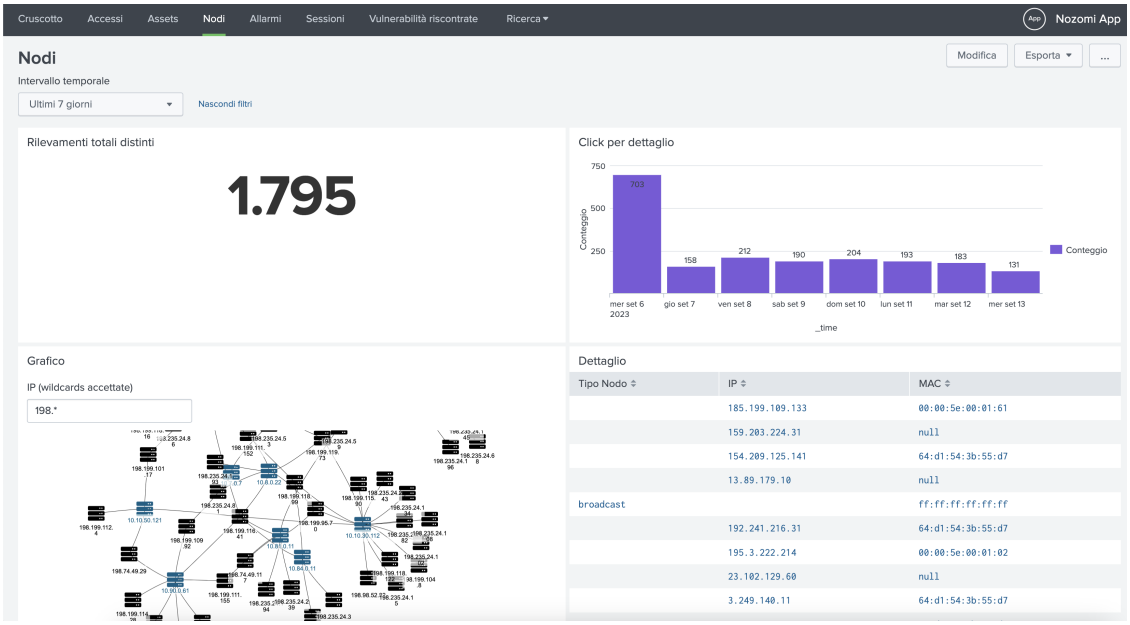


Figura 4.26. Dashboard "Nodi"

Per la dashboard "Nodi" sono stati creati quattro pannelli per monitorare i nodi rilevati nel periodo temporale specificato. I primi due pannelli mostrano rispettivamente il conteggio totale dei nodi e il conteggio giornaliero. Il terzo pannello presenta un diagramma di rete interattivo che consente di applicare filtri su un indirizzo IP specifico. Il quarto pannello fornisce una tabella completa con l'elenco di tutti i nodi.

Dashboard "Allarmi"

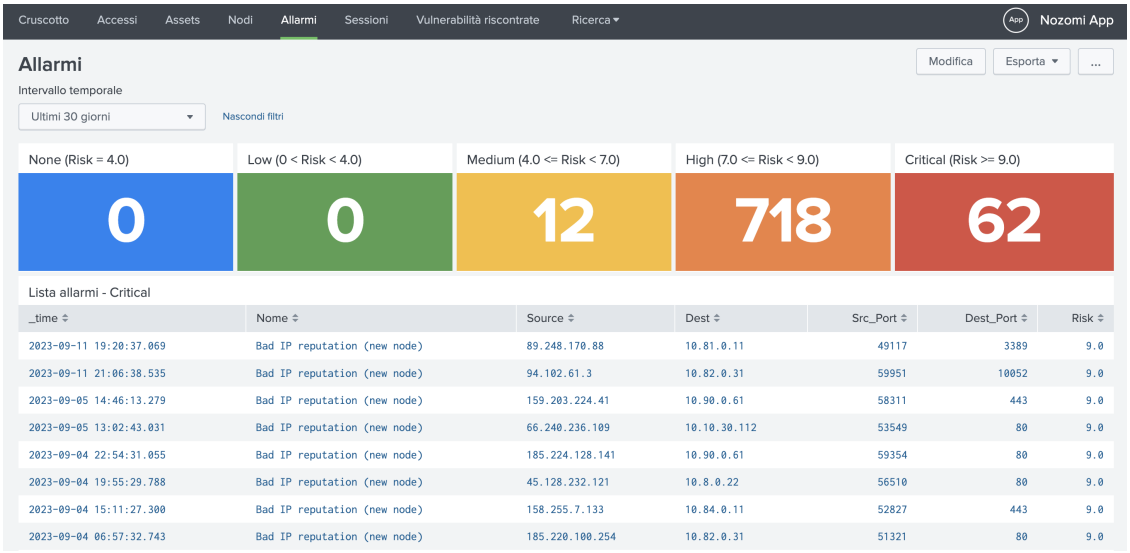


Figura 4.27. Dashboard "Allarmi"

Per il monitoraggio degli allarmi è stata sviluppata una dashboard più elaborata che include cinque pulsanti rappresentanti i diversi livelli di criticità degli allarmi. Ogni pulsante visualizza il conteggio degli allarmi corrispondenti e utilizza un colore specifico per indicare il livello di criticità. Cliccando su uno qualsiasi di questi pulsanti, il valore del token *$risk_token$* viene assegnato dinamicamente e funge da filtro per la lista degli allarmi visualizzata sotto i pulsanti. Ad esempio, se si fa clic sul pulsante relativo al livello di criticità "Critical", la lista degli allarmi viene aggiornata in tempo reale, mostrando diverse informazioni come il timestamp, il nome, gli indirizzi IP sorgente e destinazione, le porte sorgente e destinazione, e un punteggio di rischio per ciascun allarme.

Per semplificare il filtraggio degli allarmi in base al livello di criticità, è stato definito un **Calculated Field** chiamato *risk_severity*, il cui valore dipende dal campo numerico *risk*. Tale campo *risk* è estratto automaticamente da Splunk durante la ricerca e rappresenta il grado di rischio associato a ciascun allarme, variando da 0 a 10.0.

L'obiettivo è definire un nuovo campo che utilizzi valori di tipo stringa per rappresentare i livelli di criticità, ad esempio, se il campo *risk* è compreso tra 4.0 e 7.0, al campo *risk_severity* verrà assegnato il valore "Medium", e così via per gli altri intervalli di valori.

Per creare un campo calcolato è sufficiente navigare su Impostazioni → Campi → Campi calcolati → Nuovo campo calcolato:

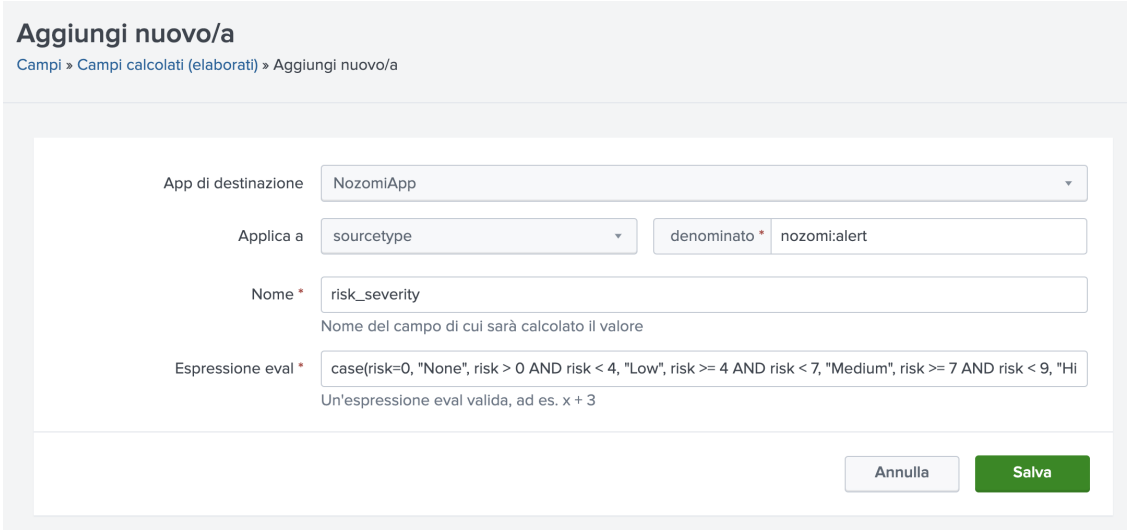


Figura 4.28. Definizione di un campo calcolato

Una volta scelta l'applicazione di destinazione, dobbiamo indicare il sourcetype al quale applicare il nuovo campo, il nome del campo stesso e definire l'espressione eval. Per il nostro scopo, creiamo l'espressione utilizzando la funzione "case" nel seguente modo:

```
case(risk=0, "None", risk > 0 AND risk < 4, "Low", risk >= 4 AND risk
   < 7, "Medium", risk >= 7 AND risk < 9, "High", risk>= 9,
   "Critical")
```

Dunque, se risk è uguale a 0, viene assegnato il valore "None" al nuovo campo, se è maggiore di 0 e minore di 4, viene assegnato il valore "Low", e così via.
In questo modo, per cercare solamente gli allarmi con uno specifico livello di rischio, è sufficiente utilizzare il nuovo campo *risk_severity* all'interno della query. Ad esempio, per effettuare il conteggio degli allarmi con rischio "Medium", la query sarà:

```
index=nozomi sourcetype="nozomi:alert" risk_severity=Medium
| stats count
```

La dashboard include anche un riquadro che visualizza il conteggio giornaliero degli allarmi, suddivisi per categoria, nonché il conteggio totale di ciascun tipo di allarme e una lista simile alla precedente (figura 4.29).
È possibile applicare dei filtri basati sugli indirizzi IP di origine e destinazione e sulla categoria degli allarmi. Inoltre, i widget sono interattivi: ad esempio, selezionando una categoria di allarmi nel widget per il conteggio totale, si aggiornano istantaneamente i dati mostrati nei pannelli circostanti.

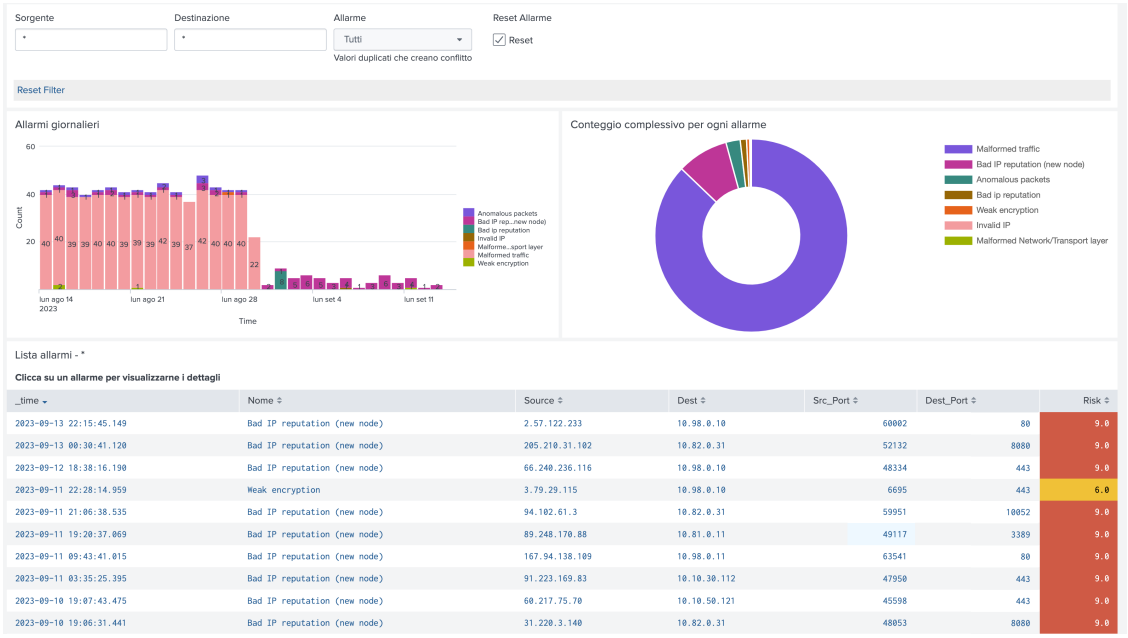


Figura 4.29. Filtraggio allarmi per categoria

Dashboard "Sessioni"

Attraverso questa dashboard, è possibile effettuare un monitoraggio delle sessioni di rete, ovvero le attuali connessioni o le comunicazioni attive tra vari dispositivi o nodi all'interno dell'infrastruttura.

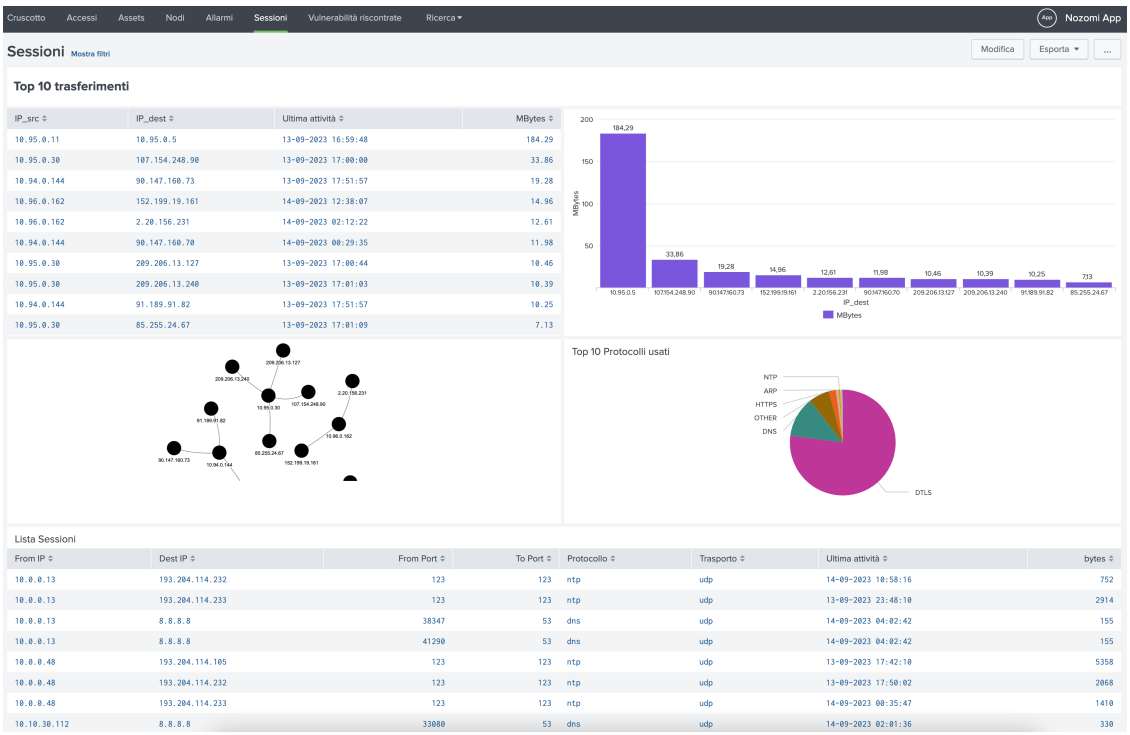


Figura 4.30. Dashboard "Sessioni"

I primi due pannelli ci permettono di esaminare le 10 sessioni con il più alto volume di dati (in megabyte) scambiati tra due dispositivi o nodi, identificati attraverso i loro indirizzi IP. Queste sessioni possono anche essere visualizzate tramite un diagramma di rete interattivo, mentre attraverso un grafico a torta possiamo esplorare i 10 protocolli più utilizzati all'interno del sourcetype "nozomi:session".

Infine, l'ultimo pannello mostra un elenco di tutte le sessioni all'interno dell'intervallo di tempo specificato, mostrando gli indirizzi IP di origine e destinazione, le porte di origine e destinazione, i protocolli utilizzati durante la sessione, l'orario dell'ultima attività registrata e la quantità di dati (in byte) scambiata tra i dispositivi.

Nel primo pannello, la quantità di dati trasferiti durante una sessione è stata rappresentata in megabyte, tuttavia Nozomi non invia questa informazione a Splunk, bensì invia i dati solamente in byte. È stato quindi necessario effettuare una conversione tramite il comando eval.

La query completa è:

```
index=nozomi sourcetype="nozomi:session"
| rename transferred.bytes as bytes
| fields *
| eval last_activity_time = strftime(strptime(last_activity_time,
    "%s%3N"), "%d-%m-%Y %H:%M:%S")
| stats last(last_activity_time) as last_activity_time sum(bytes) as
    bytes by from, to
| sort 10 - bytes
| rename to as IP_dest, from as IP_src, last_activity_time as "Ultima
    attivita"
| eval MBytes = round(bytes/1024/1024, 2)
| fields - bytes
```

Dopo aver estratto gli eventi dall'indice *nozomi* e sourcetype *nozomi:session*, usiamo la prima *eval* per convertire il timestamp complesso (ad esempio "1630741800000") in un formato più comprensibile di data e orario in Splunk, usando le due funzioni *strptime* e *strftime*. La prima converte il timestamp in un oggetto riconosciuto da Splunk, mentre la seconda lo formatta successivamente in un nuovo formato, come "gg-mm-aaaa HH:MM:SS".

Con la funzione *stats* calcoliamo due statistiche: la prima, *last(last_activity_time) as last_activity_time*, restituisce l'ultima data e ora dell'attività rilevata per ciascuna sessione, mentre la seconda, *sum(bytes) as bytes*, calcola la somma dei byte trasferiti in ogni sessione. I risultati sono raggruppati per gli indirizzi IP di origine ("from") e di destinazione ("to").

Con *sort 10 - bytes* ordiniamo i risultati in base al campo "bytes" in ordine decrescente, prendendo solo le prime 10 righe.

Infine con *eval MBytes = round(bytes/1024/1024, 2)* definiamo il campo "MBytes", che rappresenta il numero di megabyte trasferiti, calcolati dividendo i byte per 1024 due volte e arrotondando il risultato a due decimali.

fields - bytes semplicemente rimuove il campo "bytes" dal risultato finale, in quanto sostituito dal campo "MBytes".

Dashboard "Vulnerabilità riscontrate"

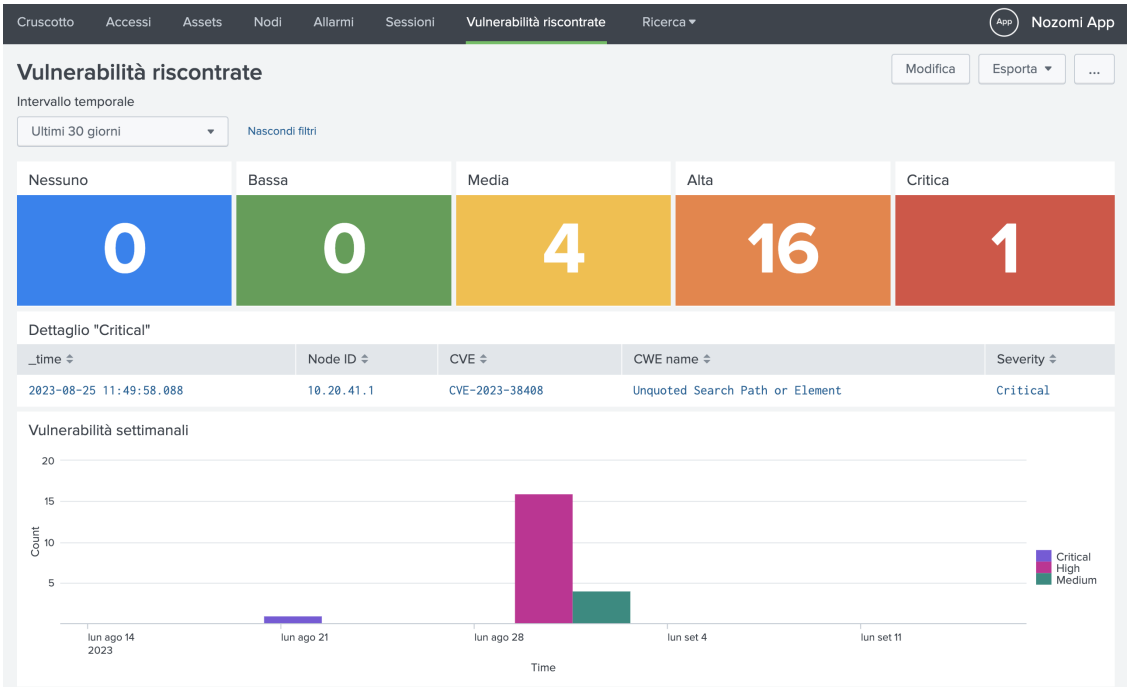


Figura 4.31. Dashboard "Vulnerabilità riscontrate"

L'ultima dashboard è stata progettata per il monitoraggio delle vulnerabilità rilevate sui nodi della rete. La sua interfaccia è simile a quella utilizzata per la gestione degli allarmi ed è costituita da cinque pulsanti che rappresentano i diversi livelli di criticità delle vulnerabilità, basandosi sul valore contenuto nel campo *cve_severity*. Utilizzando il token *$form.severity_tok$*, è possibile controllare la lista sottostante, che visualizza tutte le vulnerabilità in base alla loro tipologia.
Con un istogramma monitoriamo invece il conteggio di tutte le vulnerabilità settimanali per ciascun livello di criticità.

È presente inoltre una lista completa delle vulnerabilità (figura 4.32), con possibilità di filtrare i risultati in base all'indirizzo IP del nodo, al CVE (Common Vulnerabilities and Exposures) di riferimento, al valore CWE (Common Weakness Enumeration) e alla severità.

Fare clic su qualsiasi riga della tabella aprirà un nuovo pannello in cui verrà eseguita una nuova ricerca Splunk specifica per la vulnerabilità selezionata. Questo permette di esaminare in dettaglio l'evento correlato, visualizzando i valori per ciascun campo, il tutto senza la necessità di avviare una nuova ricerca in una scheda separata.

Per rendere interattivi i due pannelli, abbiamo nuovamente utilizzato i token. In particolare, abbiamo definito tre token per i campi *cve*, *cve_severity* e *node_id*, rispettivamente *$cve2_tok$*, *$severity2_tok$* e *$nodo2_tok$*.

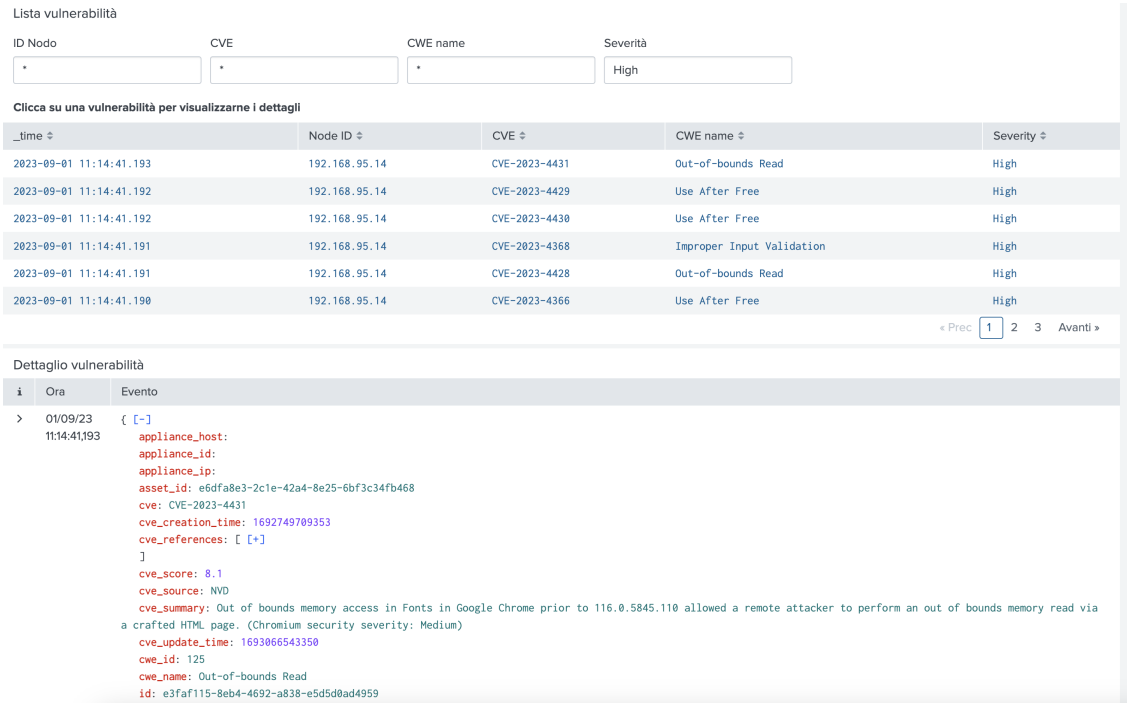


Figura 4.32. Lista completa vulnerabilità riscontrate con filtraggio

Nel "Drilldown Editor" del pannello relativo alla lista delle vulnerabilità, abbiamo configurato questi tre token, assegnando a ciascuno di essi i valori dei campi corrispondenti. Abbiamo utilizzato la notazione "row.field_name" per indicare che desideriamo utilizzare i valori contenuti nei campi della riga selezionata.

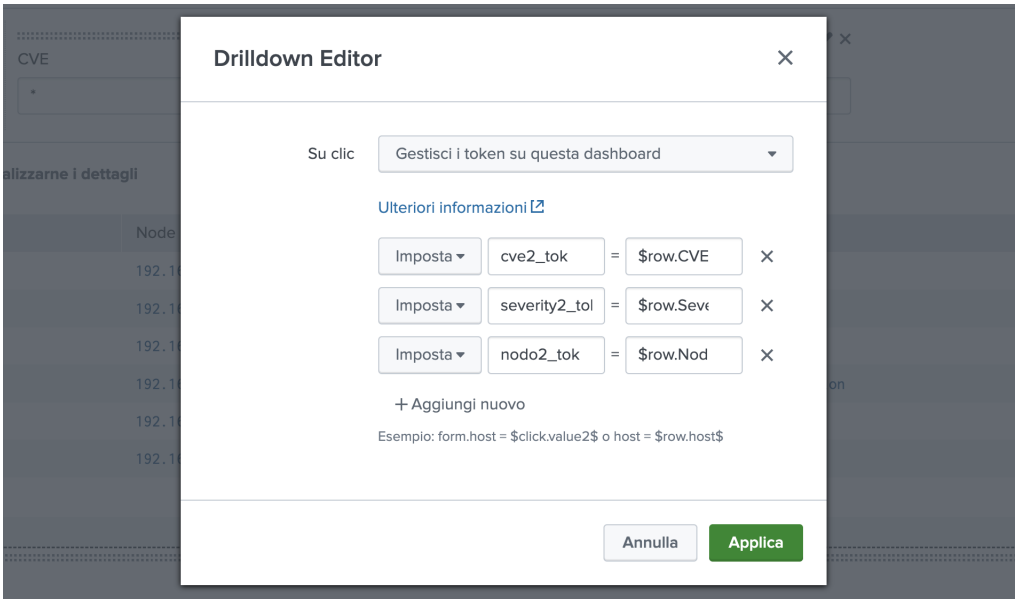


Figura 4.33. Definizione token per vulnerabilità dettagliate

La query di ricerca degli eventi che sfrutta tali token è dunque la seguente:

```
index=nozomi sourcetype="nozomi:cve" node_id="$nodo2_tok$"
    cve_severity="$severity2_tok$" cve="$cve2_tok$"
```

4.4 App InfoSec di Splunk

InfoSec è un'applicazione gratuita per Splunk progettata per affrontare i problemi di sicurezza più comuni, come il monitoraggio continuo e le indagini sulla sicurezza. Si può scaricare e installare gratuitamente tramite Splunkbase seguendo questo link: InfoSec App for Splunk - Splunkbase [25].

Questa app è stata pensata per semplificare l'utilizzo di Splunk, offrendo diverse dashboard complete che permettono di avere una visione unificata degli eventi e che aiutano nell'analisi degli allarmi, del traffico e di altri dati.

Un punto interessante di InfoSec è la sua capacità di gestire casi d'uso avanzati legati al rilevamento delle minacce, infatti è possibile ampliare le sue funzionalità utilizzando ulteriori risorse di sicurezza, come l'applicazione *Security Essentials*. Quest'app offre una vasta gamma di controlli di sicurezza che possono essere facilmente integrati nell'app InfoSec.

Per un corretto funzionamento dell'applicazione, è richiesta la configurazione di due componenti principali, ovvero i *Data Model* e il *Common Information Model (CIM)*. Questa configurazione è necessaria per una corretta normalizzazione dei dati degli eventi che vengono inseriti in Splunk.

4.4.1 Data Model e il Common Information Model (CIM)

I **data model** sono una categoria di "knowledge object" che servono per semplificare e accelerare l'analisi dei dati, in quanto consentono di organizzare i dati in modo logico e strutturato [26]. Ciascun data model rappresenta una categoria specifica di dati di eventi, come ad esempio i dati di sicurezza, di autenticazione, di rete o di sistema.

Man mano che continuamente inseriamo dati in Splunk, alcuni di questi solitamente seguono schemi o pattern specifici, ad esempio, potremmo raccogliere dati di autenticazione da varie fonti come registri SSH, Windows Event Logs o Syslogs, e ognuna di queste fonti di dati segue determinate regole o pattern. In tali situazioni, i data model diventano estremamente utili poiché semplificano notevolmente la ricerca e l'analisi dei dati in base alla tipologia degli eventi, indipendentemente dalla loro origine, che potrebbe essere rappresentata da diversi index e sourcetype. Sono quindi particolarmente utili quando si ha a che fare con grandi quantità di dati eterogenei provenienti da diverse fonti.

Grazie a queste strutture, gli utenti possono accedere semplicemente ai dati di loro interesse, ad esempio, invece di scrivere query complesse per ottenere dettagli dai log di sicurezza, è possibile usare il data model di sicurezza predefinito di Splunk per recuperare facilmente le informazioni desiderate. Questo semplifica notevolmente anche la creazione di report interattivi e dashboard.

I **dataset** sono suddivisioni logiche dei dati all'interno di un data model e rappresentano categorie specifiche o sottoinsiemi di eventi all'interno di una categoria di dati più ampia, raggruppando eventi simili o correlati. Per esempio, all'interno di un data model relativo alla sicurezza, potremmo avere diversi dataset relativi a categorie specifiche di eventi di sicurezza, come "Accessi non autorizzati", "Autenticazioni riuscite", "Autenticazioni fallite", ecc.
L'utilizzo dei dataset semplifica ulteriormente l'analisi dei dati, consentendo agli utenti di concentrarsi su categorie specifiche di eventi senza dover considerare l'intero data model. Ciò facilita la creazione di ricerche, report e dashboard mirate a un particolare aspetto dei dati, migliorando l'efficienza e la comprensione delle informazioni.

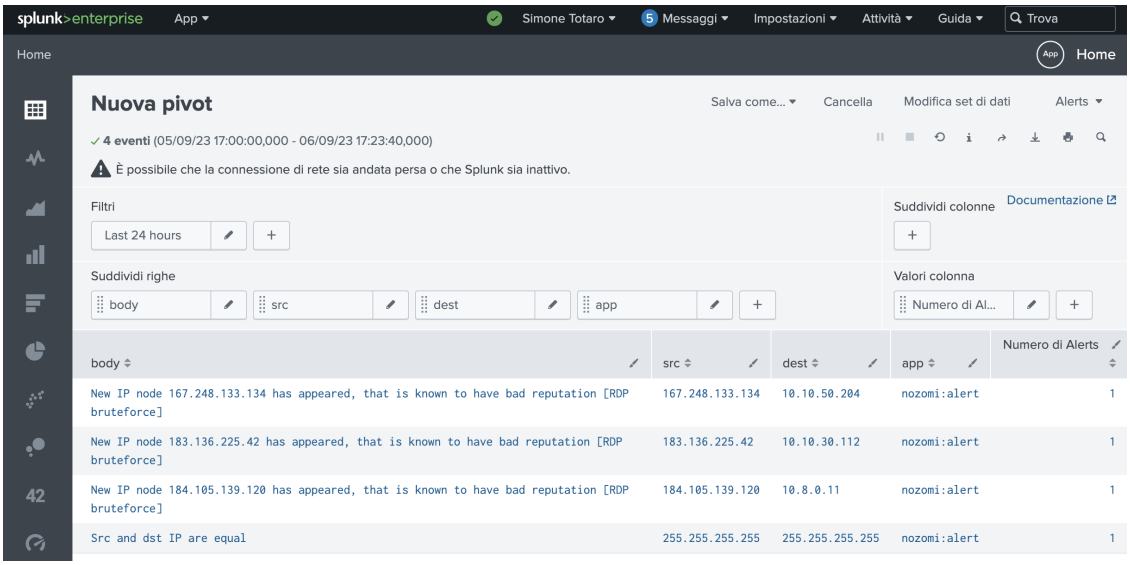


Figura 4.34. Nuovo pivot per il data model "Alerts"

I data model e i dataset permettono di utilizzare un potente tool di Splunk chiamato "Pivot" [27], il quale consente di estrarre ed elaborare i propri dati senza progettare le ricerche SPL che li generano.

Selezionando uno specifico data model, è possibile analizzare i dati di un particolare dataset e, tramite un'interfaccia drag-and-drop, generare tabelle statistiche, grafici e visualizzazioni in base alle configurazioni di colonne e righe selezionate.
Se ad esempio si è definito un data model per gestire i dati relativi a server di posta elettronica, con dataset per le email inviate e quelle ricevute, è sufficiente creare un nuovo pivot e selezionare il relativo data model e data set d'interesse per analizzare solamente determinati dati, ad esempio solo le email ricevute.

Nella figura 4.34 è stato generato un nuovo pivot per il data model "Alerts", estraendo per ciascun allarme vari campi, tra cui il corpo dell'evento, indirizzi IP sorgente e destinazione, il relativo sourcetype ed il numero di allarmi generati, senza scrivere alcuna query SPL. Nella barra laterale sono inoltre disponibili diversi tool per creare grafici, tabelle e altre visualizzazioni sui dati estratti.

Tra le principali funzioni dei data model vi è l'ottimizzazione delle ricerche, in quanto Splunk è in grado di pre-elaborare i dati all'interno dei data model, creando una cache che aumenta notevolmente la velocità ed l'efficienza delle ricerche e generando quello che si chiama data model "accelerato".
Splunk accelera i data model attraverso ricerche pianificate regolari, generalmente ogni 5 minuti, sui dati sottostanti agli eventi, generando sintesi dei dati in background.

Per garantire il corretto funzionamento dell'app InfoSec, questa si basa sul **Common Information Model (CIM)**, un modello semantico utilizzato per l'interpretazione dei dati [28]. InfoSec, per essere in grado di lavorare con una vasta gamma di produttori e fornitori, fa affidamento su questo modello. Il CIM può essere considerato come una sorta di schema in cui sono definiti vari campi, alcuni dei quali devono essere obbligatoriamente presenti, mentre altri sono considerati opzionali. In pratica, è necessaria una fase di normalizzazione o "mapping" dei dati in modo che siano allineati con i campi definiti in questo modello.

4.4.2 Configurazione di InfoSec

Per consentire a InfoSec di generare report accurati basati sui dati in Splunk, tali dati devono essere organizzati all'interno di specifici data model, in conformità con il CIM. Di conseguenza, per utilizzare questo modello è necessario installare l'applicazione "Splunk Common Information Model" da Splunkbase, la quale può essere scaricata tramite il seguente link: Splunk Common Information Model (CIM) - Splunkbase [29].

L'installazione di questa applicazione aggiungerà automaticamente a Splunk una serie di data model preconfigurati, ciascuno composto da un set di campi e tag e tutti essenziali per il corretto funzionamento di InfoSec. Questi data model possono essere utilizzati per normalizzare e validare i dati durante le ricerche, accelerare le ricerche e le dashboard o creare nuovi report e visualizzazioni utilizzando Pivot.

In aggiunta all'app Common Information Model, è necessario installare i seguenti add-on per configurare correttamente InfoSec. Ciascuno di essi è scaricabile da Splunkbase:

- Punchcard - Custom Visualization
- Force Directed App For Splunk
- Splunk App for Lookup File Editing

Verifichiamo adesso lo stato di "salute" dell'app Infosec, aprendo l'applicazione e navigando nella schermata Health [30].

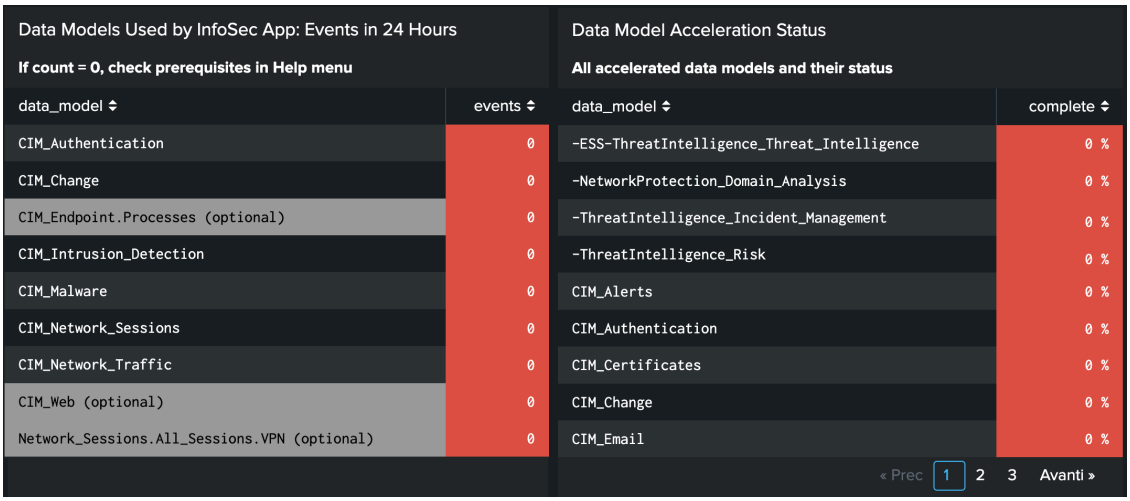


Figura 4.35. Salute dei Data Model su InfoSec

Un primo pannello mostra il numero di eventi ricevuti nelle ultime 24 ore su ciascuno dei data model utilizzati dall'app. Inizialmente, per ciascun data model, il numero di eventi rilevati è 0, in quanto non è stato ancora effettuato il mapping al CIM.

Il secondo pannello mostra invece lo stato di accelerazione di ciascun data model. Attualmente nessuno è accelerato, dunque dobbiamo abilitare l'accelerazione per tutti i data model che ricevono dati.

Possiamo visionare tutti i data model aggiunti in seguito all'installazione dell'app, navigando in *Impostazioni* → *Modelli di dati* e filtrando per App, selezionando "Splunk Common Information Model (Splunk_SA_CIM)".

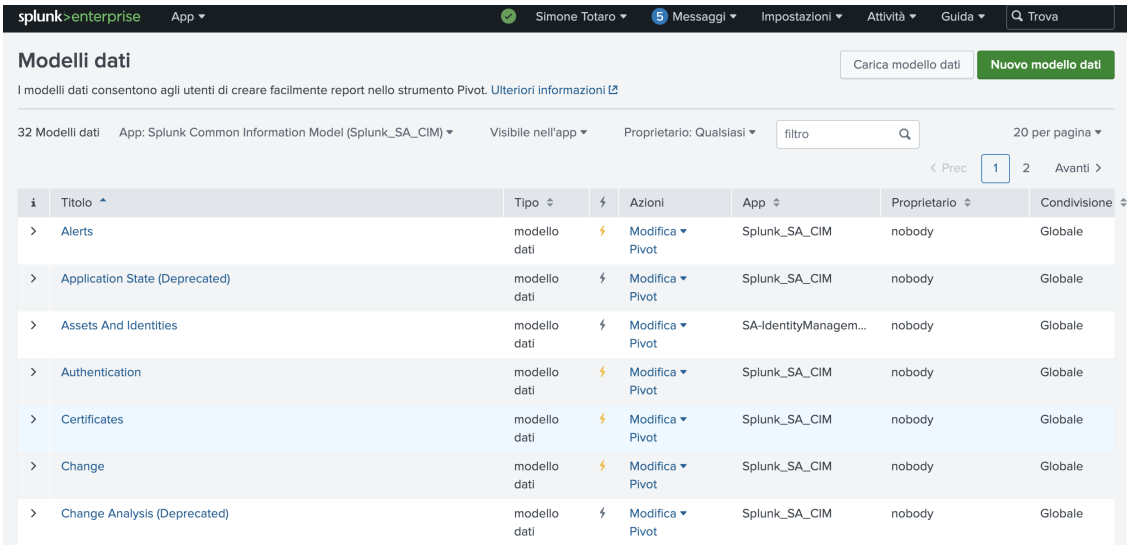


Figura 4.36. Data Model aggiunti con l'applicazione del CIM

I data model di nostro interesse, ovvero quelli necessari a InfoSec, sono i seguenti:

- Authentication
- Change
- Endpoint (opzionale)
- Intrusion_Detection
- Malware
- Network_Sessions
- Network_Traffic
- Web (opzionale)

Per ciascuno di essi clicchiamo su Modifica → Modifica Accelerazione e selezioniamo Accelera. Per indicare che il data model è accelerato comparirà un'icona di un fulmine giallo.

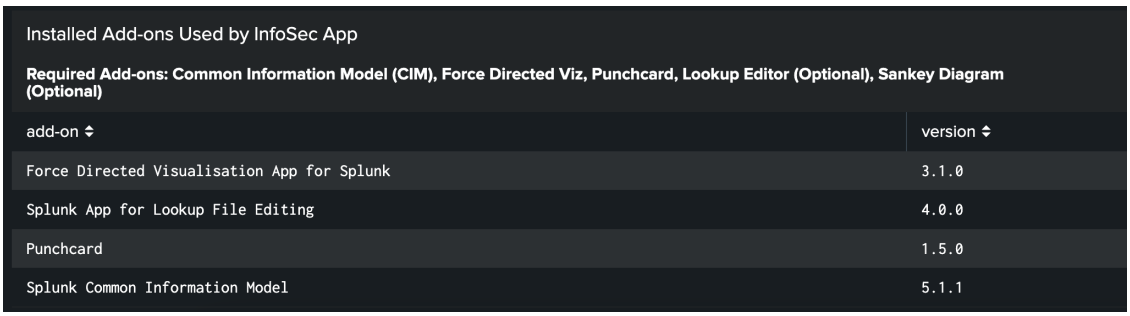


Figura 4.37. Add-on installati per l'applicazione InfoSec

Il terzo pannello mostra infine lo stato di installazione per ciascun add-on richiesto per InfoSec. In figura 4.37 la dashboard segnala che tutti i componenti aggiuntivi richiesti sono installati.

4.4.3 Mapping dati in modo conforme al Common Information Model

La scelta di quale data model utilizzare, e dunque di quali dati mappare al CIM, dipende principalmente dal tipo di dati che vogliamo analizzare. L'obiettivo è stato infatti quello di capire quali tra questi data model avesse senso utilizzare per i dati ricevuti da Nozomi Networks, in quanto alcuni potrebbero non essere necessari.

Mapping del data model "Authentication"

Cominciamo analizzando il data model "Authentication" che tratta i dati relativi all'autenticazione. Vediamo come configurarlo e come identificare i dati da inserire in questo data model. Dall'elenco visto precedentemente (vedi figura 4.36) selezioniamo "Authentication", dove troveremo una sezione chiamata "VINCOLI" che contiene la ricerca Splunk che identifica gli eventi destinati a popolare questo data model.

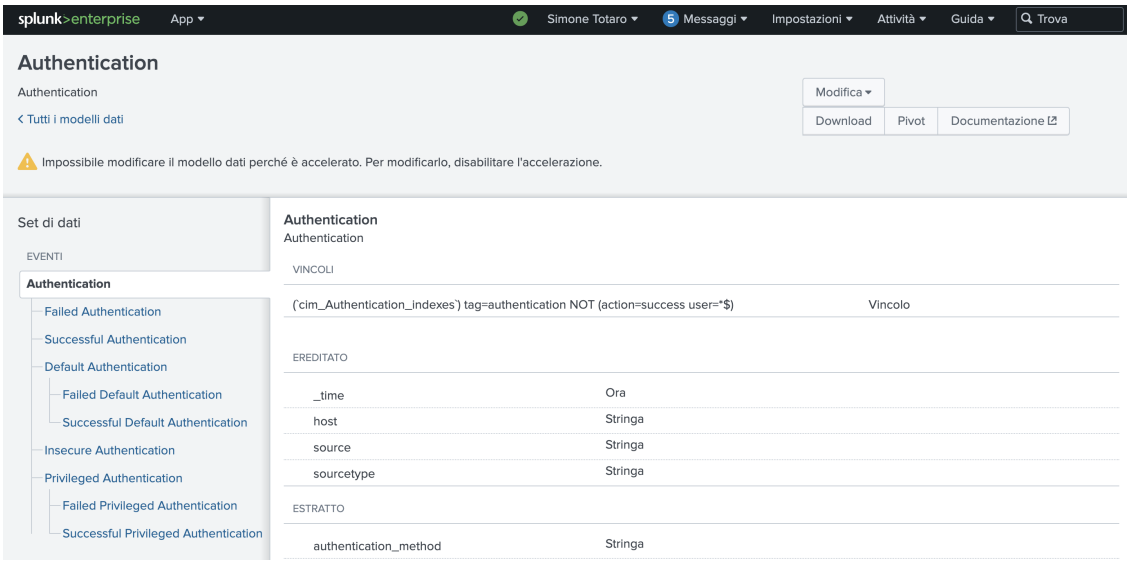


Figura 4.38. Data model "Authentication"

All'interno della ricerca notiamo la presenza di "cim_Authentication_indexes", ovvero una *macro* che non è altro che un insieme di indici specifici.
La condizione *tag=authentication* restringe la ricerca per restituire solo gli eventi con questo tag, mentre *(NOT (action=success user=*$))* esclude gli eventi che contengono il campo "action" con valore "success" e il campo "user" con un valore che termina con il carattere "$".

Vogliamo scoprire quali dati abbiamo in Splunk che potrebbero adattarsi a questa ricerca, dunque dobbiamo capire quali siano gli indici da associare alla macro. Apriamo l'app Search & Reporting, rimuoviamo la macro dalla ricerca e includiamo un conteggio per indice e sourcetype, aggiungendo *stats count by index, sourcetype*.

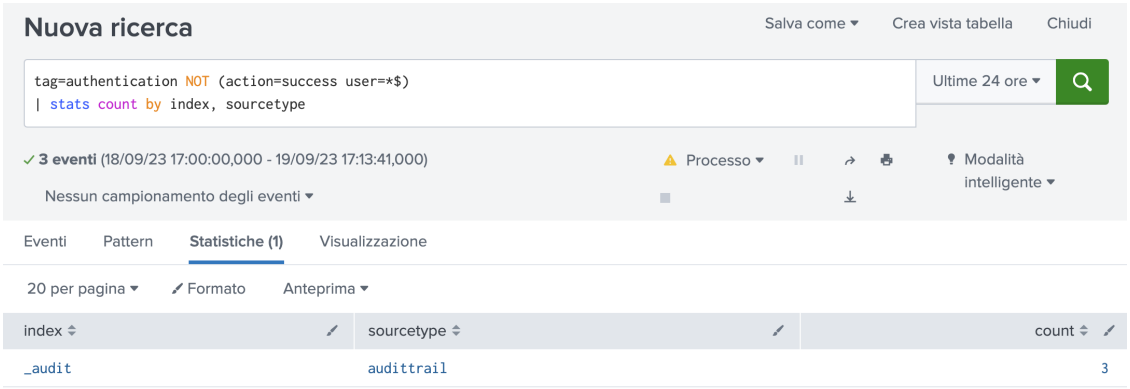


Figura 4.39. Ricerca dati di autenticazione

Notiamo che la ricerca restituisce dati provenienti dall'indice _audit, dunque sono presenti eventi con il tag "authentication". Tale indice fa però riferimento agli accessi effettuati su Splunk, ma noi vogliamo solamente i dati relativi agli accessi di Nozomi. Vogliamo dunque aggiungere ulteriori dati al nostro data model, ai quali dobbiamo applicare questo tag. Nel nostro caso, vogliamo aggiungerlo agli eventi di autenticazione appartenenti alla seguente ricerca:

```
index=nozomi sourcetype="json_nozomi" nozomi_source=audit_log user=*
```

Per taggare correttamente i dati relativi a questa ricerca bisogna creare un "event type" ovvero un campo definito dall'utente che rappresenta una categoria di eventi. Accediamo alle impostazioni, clicchiamo su "Event type" e poi su "Nuovo Event Type".

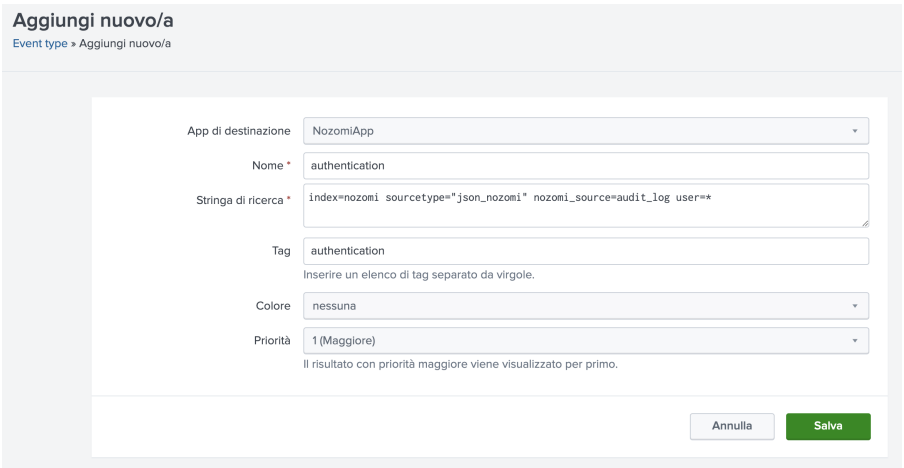


Figura 4.40. Creazione di un nuovo Event Type

Assegniamo un nome all'event type, ad esempio "authentication", e come app di destinazione selezioniamo "NozomiApp" (la scelta è indifferente). Come "Stringa di ricerca" inseriamo la query precedente e nel campo "Tag" inseriamo "authentication".
Salviamo l'event type e assicuriamoci che la visualizzazione sia impostata per tutte le app e che siano assegnati i corretti privilegi di lettura e scrittura agli utenti. Ora, tutti gli eventi relativi a questa stringa di ricerca, e dunque a questo event type, saranno taggati con il tag "authentication".

Adesso abbiamo l'indice da assegnare alla macro, ovvero *nozomi*. L'indice *_audit* non lo includiamo in quanto non fa riferimento ai dati di Nozomi. Accediamo a "Ricerca avanzata" dal menu "Impostazioni", apriamo "Macro di ricerca" e cerchiamo la macro *cim_Authentication_indexes*. Clicchiamo sul nome della macro per aprire la finestra di Configurazione CIM per il data model "Autenticazione".

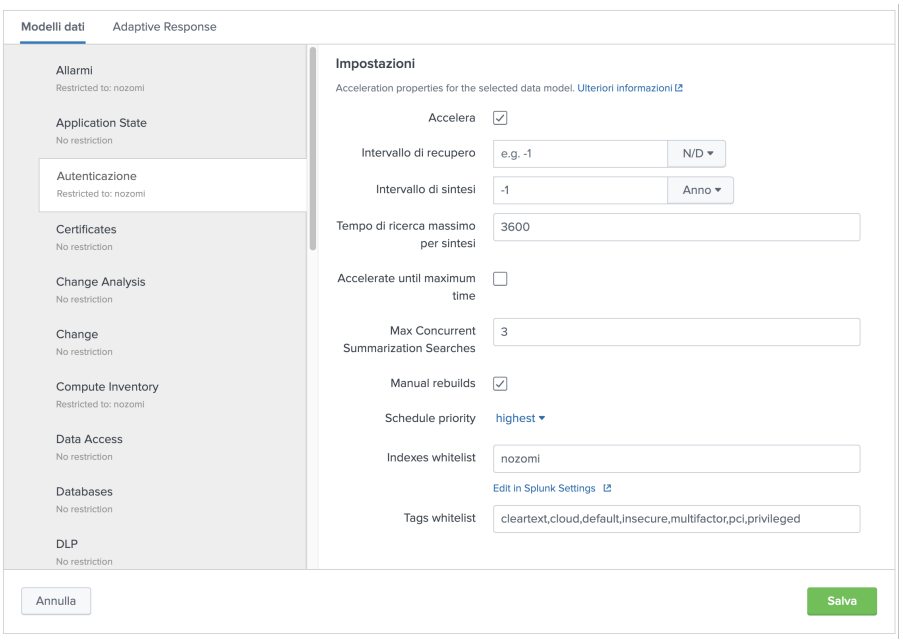


Figura 4.41. Aggiunta indici alla macro di autenticazione

Aggiungiamo l'indice alla "Indexes whitelist" e salviamo le modifiche. Per verificare che la modifica abbia esito positivo, eseguiamo nuovamente la ricerca del data model.

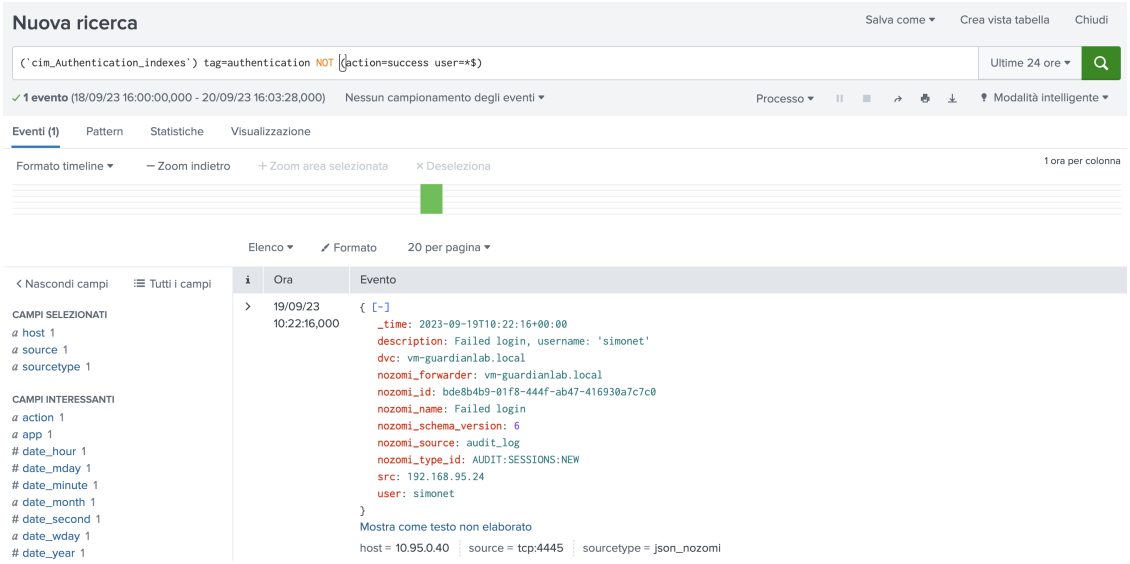


Figura 4.42. Eventi inseriti nel data model "Authentication"

La ricerca ora restituisce gli eventi che ci aspettiamo. Questa procedura va fatta per tutti i data model d'interesse.

L'ultimo passo è il mapping o normalizzazione dei campi in conformità con il CIM. Questa fase è necessaria in quanto i dati possono provenire da diversi sourcetype e quindi essere rappresentati da campi con nomi diversi, ma che indicano la stessa informazione, ad esempio, un sourcetype potrebbe chiamare gli indirizzi IP sorgente "source" mentre un altro potrebbe chiamarli "src_ip". Il CIM fornisce campi standardizzati per risolvere questo problema e renderli compatibili con l'app InfoSec.

Per conoscere i nomi dei campi secondo il CIM, useremo la documentazione ufficiale di Splunk. Per ciascun data model, è disponibile una tabella con i nomi dei campi secondo il CIM.

La tabella completa per il data model "Authentication" è disponibile a questo link: Authentication - Common Information Model Add-on Manual

Dataset name	Field name	Data type	Description	Notes
Authentication	`action`	string	The action performed on the resource.	Prescribed values: `success`, `failure`, `pending`, `error` Recommended. Also, required for pytest-splunk-addon

Authentication	`app`	string	The application involved in the event.	`ssh`
				`splunk`
				`win:local`
				`signin.amazonaws.com`
				Recommended.
				Also, required for pytest-splunk-addon

Authentication	`authentication_method`	string	The method used to authenticate the request.	Optional
Authentication	`authentication_service`	string	The service used to authenticate the request.	`Okta`, `ActiveDirectory`, `AzureAD` Optional
Authentication	`dest`	string	The target involved in the authentication. You can alias this from more specific fields.	`dest_host`, `dest_ip`, `dest_nt_host` Recommended
Authentication	`dest_bunit`	string	The business unit of the authentication target.	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.
Authentication	`dest_category`	string	The category of the authentication target.	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons. `email_server` or `SOX-compliant`
Authentication	`dest_nt_domain`	string	The name of the Active Directory used by the authentication target, if applicable.	
Authentication	`dest_priority`	string	The priority of the authentication target.	This field is automatically provided by asset and identity correlation features of applications like Splunk Enterprise Security. Do not define extractions for this field when writing add-ons.
Authentication	`duration`	number	The amount of time for the completion of the authentication event, in seconds.	
Authentication	`reason`	string	The human-readable message associated with the authentication action (`success` or `failure`).	
Authentication	`response_time`	number	The amount of time it took to receive a response in the authentication event, in seconds.	
Authentication	`signature`	string	A human-readable signature name.	

Figura 4.43. Tabella mapping CIM "Authentication"data model

Nella tabella vedremo il nome del campo, la sua tipologia (ad esempio, stringa o numero), una descrizione di cosa dovrebbe rappresentare il campo e alcuni esempi di valori. Ad esempio, il campo "app" rappresenta l'applicazione coinvolta nell'evento, e alcuni esempi di valori per questo campo sono "ssh" o "splunk".

Non è obbligatorio mappare tutti i campi, infatti alcuni sono indicati come "Recommended" mentre altri come "Optional". Un buon punto di partenza è iniziare a mappare i campi raccomandati. Nel nostro caso, vogliamo valutare quali campi ha senso mappare, in quanto potremmo non ricevere tutti i tipi di dati da Nozomi, quindi il mapping potrebbe non essere necessario per alcuni campi.

Per verificare immediatamente i valori dei campi e lo stato complessivo della normalizzazione, possiamo utilizzare il tool "CIM Validator" tramite l'app "SIM-cim_vladiator," scaricabile gratuitamente da questo link: SA-cim_vladiator - Splunkbase [31].
L'app permette di esaminare i campi di ciascun data model e visualizzare la percentuale di campi mappati con successo al CIM.

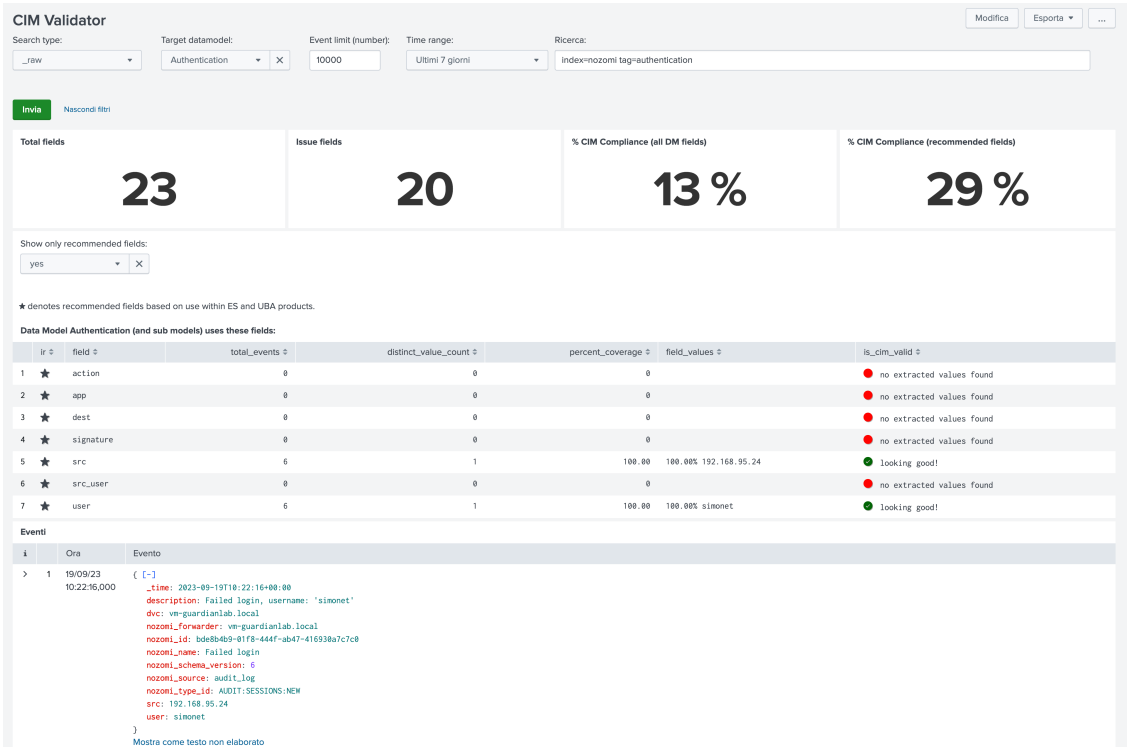


Figura 4.44. CIM Validator - Authentication data model

Apriamo l'app, selezioniamo il data model "Authentication", e effettuiamo una ricerca sugli ultimi 7 giorni, ad esempio "index=nozomi tag=authentication". Per semplicità, restringiamo la visualizzazione solamente ai campi raccomandati. Otteniamo una "CIM Compliance" solo del 29% per i campi raccomandati, mentre del 13% per tutti i campi. Notiamo inoltre che alcuni campi non restituiscono risultati, mentre "src" e "user" sono già mappati correttamente di default.

I campi che non restituiscono risultati sono "action", "app", "dest", "signature" e "src_user", dunque consultiamo la tabella del data model per vedere che tipo di dati dovrebbero rappresentare. È buona prassi eseguire la ricerca in una nuova scheda per visualizzare gli eventi restituiti e i relativi campi estratti.

Il campo "action" dovrebbe rappresentare l'esito dell'autenticazione, dunque dovrebbe contenere valori come "success", "failure", "pending" o "error". Nel nostro caso, l'esito è rappresentato dal campo "nozomi_name" come una stringa, ad esempio "User signed in" per indicare che l'autenticazione ha avuto successo. Dobbiamo quindi definire manualmente un nuovo campo andando su Impostazioni → Campi → Campi calcolati → Aggiungi nuovo.

Scegliamo l'app di destinazione, applichiamolo al sourcetype "json_nozomi," nominiamo il campo "action" e come espressione eval scriviamo "case(nozomi_name = "User signed in", "success", nozomi_name = "Failed login", "failure")". Questa assegnerà dunque i valori "success" o "failure" al campo "action" in base all'esito dell'autenticazione.

Salviamo, impostiamo la visibilità come globale e assegniamo i permessi di lettura e scrittura agli utenti.

Il campo "app", come visto prima, dovrebbe rappresentare l'applicazione coinvolta nell'evento. Poiché non c'è un campo che contenga direttamente questa informazione nella ricerca, che nel nostro caso è semplicemente una stringa "nozomi", dovremo definire nuovamente un nuovo campo. Assegniamo "app" come nome e "nozomi" come espressione eval, tra virgolette per indicare che si tratta di una stringa.

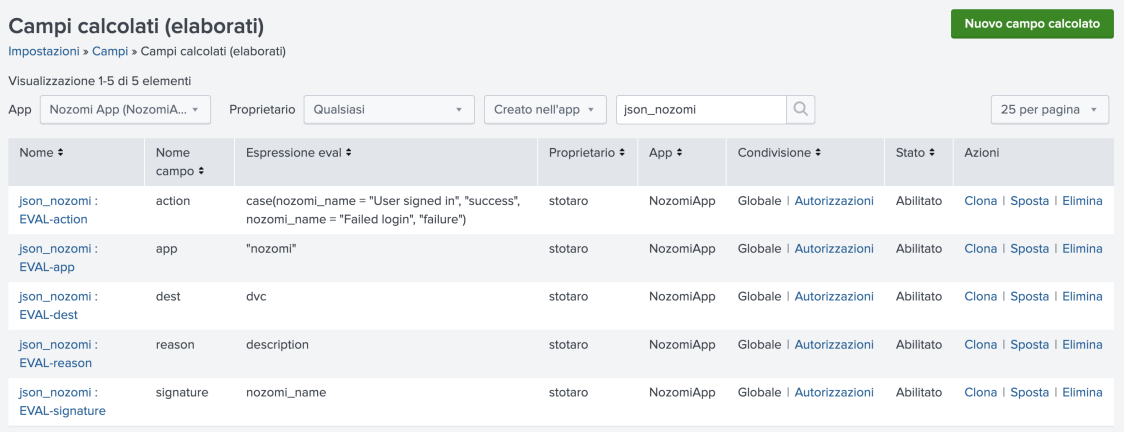


Figura 4.45. Campi calcolati per il data model "Authentication"

Nell'immagine sono elencati tutti i campi calcolati definiti per questo data model. Alcuni di essi sono solo alias per altri campi, ad esempio "signature" secondo la tabella CIM rappresenta le stesse informazioni del campo "nozomi_name".

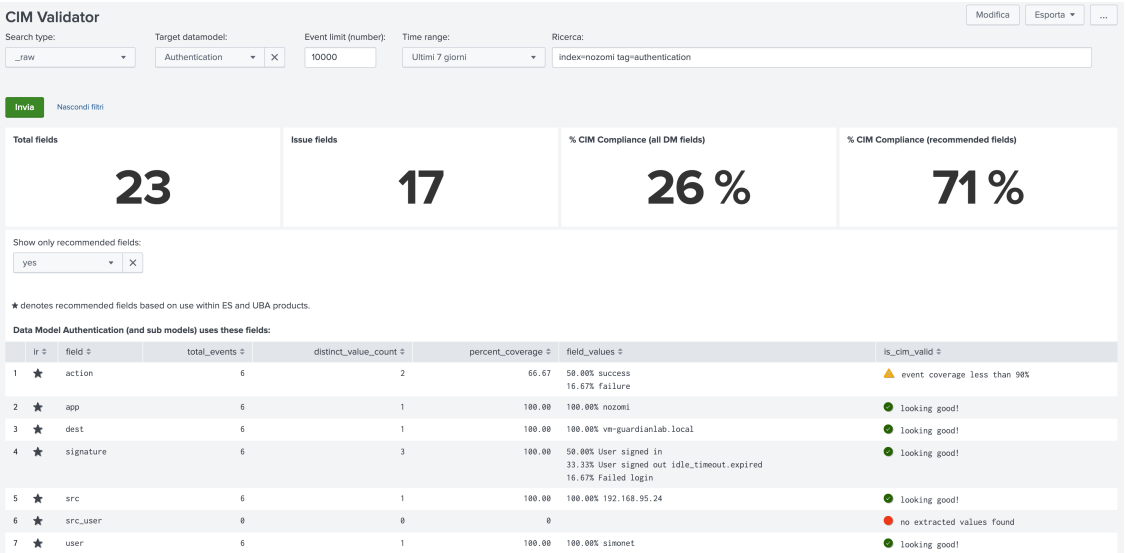


Figura 4.46. Mapping CIM effettuato su Authentication data model

Al termine di questa procedura, vedremo che la "CIM Compliance" per i campi raccomandati sarà aumentata al 71%, e ai vari campi saranno associati eventi. Non è stato effettuato il mapping per il campo "src_user" in quanto potrebbe non essere necessario a meno che non ci siano casi di "privilege escalation".

Mapping del data model "Network Traffic"

Il prossimo data model che possiamo analizzare e configurare è "Network Traffic", il quale richiede il seguente vincolo:

```
(‘cim_Network_Traffic_indexes‘) tag=network tag=communicate
```

Anche in questo caso desideriamo utilizzare l'index "nozomi" per popolare il data model. Dunque, modifichiamo la macro *cim_Network_Traffic_indexes*, aggiungendo "nozomi" all'Indexes whitelist.

Gli eventi che desideriamo siano taggati con "network" e "communicate" sono quelli che appartengono alla seguente ricerca:

```
index=nozomi sourcetype=nozomi:session
```

Definiamo quindi un nuovo event type chiamato "traffic" al quale applichiamo questa query e assegniamo i due tag. Eseguendo ora tale ricerca, vengono restituiti dati, confermando che gli eventi sono stati taggati correttamente.

Procedendo ora con la normalizzazione dei campi, abbiamo nuovamente consultato il CIM Validator, il quale ha restituito una CIM compliance di soli l'8%.

Alcuni campi di particolare interesse riguardano gli indirizzi IP e MAC sorgente e destinazione. Le informazioni su tali indirizzi sono contenute nei campi "from" e "to". Tuttavia, secondo la tabella CIM del data model, ci sono quattro campi per rappresentare questi indirizzi: "src_ip" e "src_mac" per gli indirizzi IP e MAC sorgente, e "dest_ip" e "dest_mac" per gli indirizzi IP e MAC destinazione.

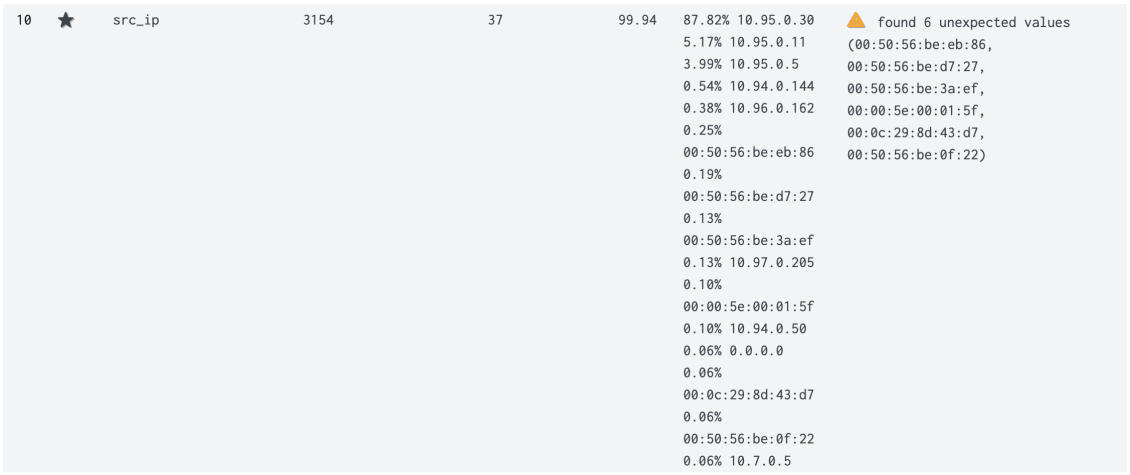


Figura 4.47. Mapping campo "src_ip" con valori errati

Tentando ad esempio di mappare il campo "src_ip" al campo "from", avviene che tutti gli indirizzi IP e MAC vengono inseriti insieme nel campo "src_ip". Questo lo notiamo consultando il CIM Validator e analizzando i valori del campo "from" tramite una ricerca.

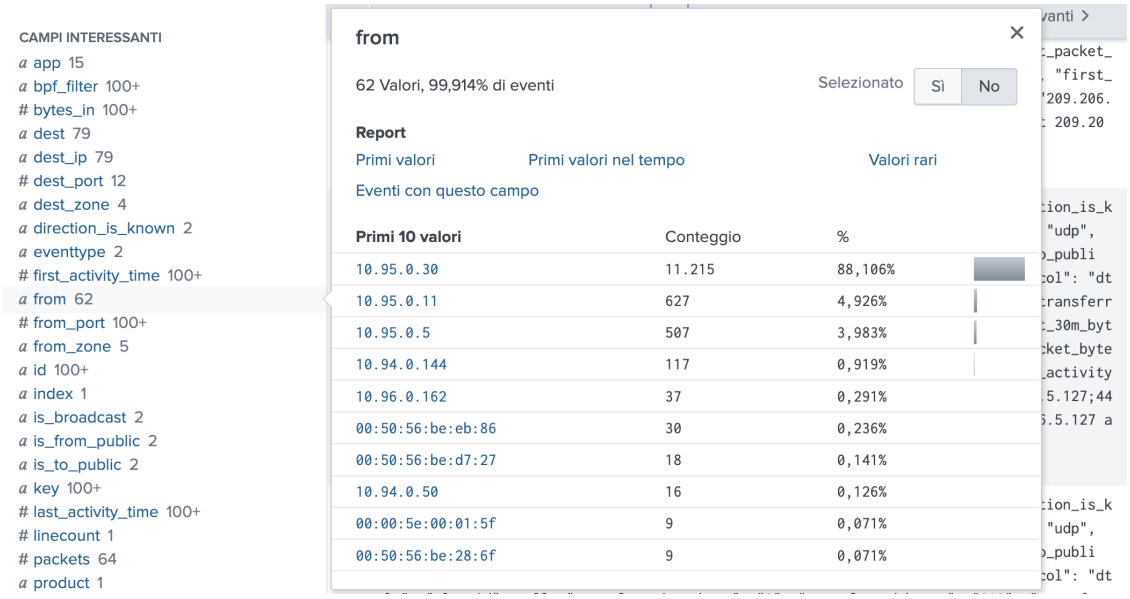


Figura 4.48. Valori campo "src_ip" con indirizzi IP e MAC

Risulta quindi necessario eseguire il mapping utilizzando espressioni regolari in grado di filtrare gli indirizzi IP e MAC, poiché attualmente non vi è una distinzione tra di essi.

Per scrivere le espressioni regolari, possiamo avvalerci del sito regex101.com [32]. Nell'area "regular expression" inseriamo la nostra regex, mentre nell'area "test string" inseriamo un evento Splunk in formato raw per visualizzare in tempo reale quali campi verranno inclusi nell'espressione che vogliamo definire.

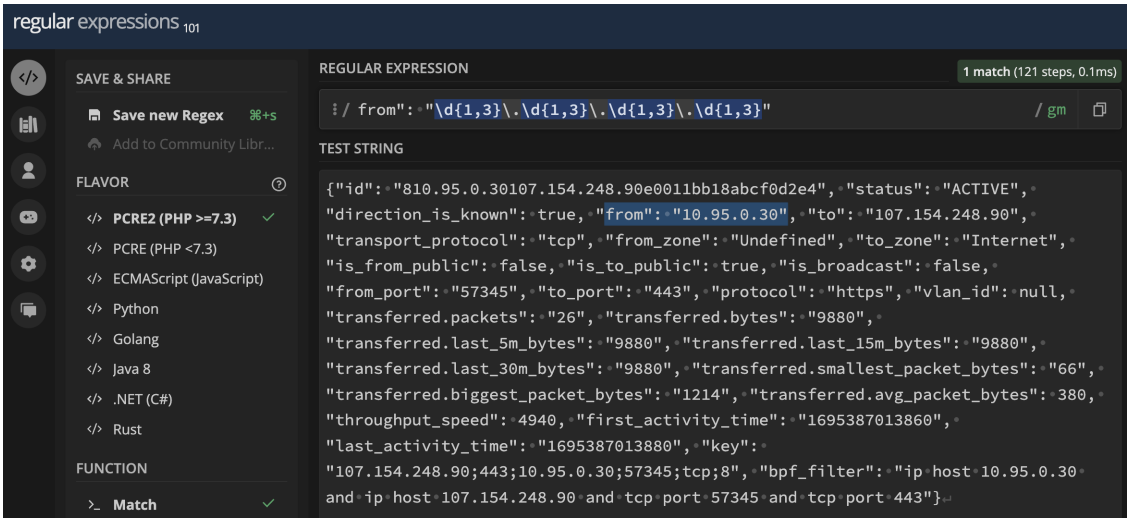


Figura 4.49. Espressione regolare per indirizzi IP

L'espressione regolare per estrarre esclusivamente gli indirizzi IP dall'evento è la seguente: **"\d{1,3}.\d{1,3}.\d{1,3}.\d{1,3}"**, dove \d è una classe di caratteri che corrisponde a qualsiasi cifra (0-9), {1,3} è un quantificatore che corrisponde al carattere precedente tra 1 e 3 volte ed infine "." corrisponde letteralmente al carattere del punto. Questo pattern viene ripetuto quattro volte per corrispondere ai quattro gruppi di cifre separati da punti negli indirizzi IP.

Ora possiamo creare un nuovo campo calcolato chiamato "src_ip" per cui l'espressione regolare sarà:

if (match(to, "\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}\"), to, null)

Questo codice controlla se il campo "to" contiene un indirizzo IP e, in caso di corrispondenza, restituirà il valore del campo "to", altrimenti restituirà null.

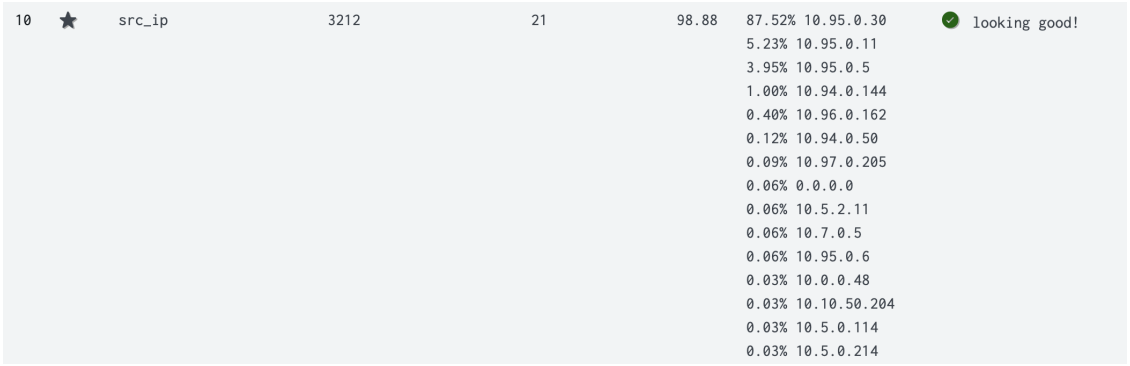


Figura 4.50. Mapping "src_ip" con valori corretti

Consultando adesso il CIM Validator, vediamo che vengono estratti correttamente solo gli indirizzi IP.

Analogamente, possiamo creare un campo calcolato chiamato "src_mac" e definire la seguente espressione regolare:

if (match(to,"[a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-]"), to, null)

dove [a-fA-F0-9]{2} corrisponde a qualsiasi carattere (ripetuto due volte) che sia una lettera minuscola da "a" a "f", una lettera maiuscola da "A" a "F" o una cifra da "0" a "9", e [\:\-] corrisponde a due punti o un trattino.

Nome	Nome campo	Espressione eval
nozomi:session : EVAL-app	app	protocol
nozomi:session : EVAL-bytes_in	bytes_in	'transferred.bytes'
nozomi:session : EVAL-dest	dest	if (match(to,"\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"), to, null)
nozomi:session : EVAL-dest_mac	dest_mac	if (match(to,"[a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}"), to, null)
nozomi:session : EVAL-dest_zone	dest_zone	to_zone
nozomi:session : EVAL-packets	packets	'transferred.packets'
nozomi:session : EVAL-product	product	"Guardian"
nozomi:session : EVAL-protocol	protocol	"ip"
nozomi:session : EVAL-src	src	if (match(from,"\d{1,3}\.\d{1,3}\.\d{1,3}\.\d{1,3}"), from, null)
nozomi:session : EVAL-src_mac	src_mac	if (match(from,"[a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}[\:\-][a-fA-F0-9]{2}"), from, null)
nozomi:session : EVAL-src_port	src_port	from_port
nozomi:session : EVAL-src_zone	src_zone	from_zone
nozomi:session : EVAL-transport	transport	transport_protocol
nozomi:session : EVAL-vendor	vendor	"Nozomi"
nozomi:session : EVAL-vendor_product	vendor_product	"Nozomi Guardian"
nozomi:session : EVAL-vlan	vlan	vlan_id

Figura 4.51. Campi calcolati per il Network Traffic data model

In figura sono elencati tutti i campi calcolati definiti per il Network Traffic data model.

Mapping dei data model "Malware" e "Intrusion Detection"

Il Malware data model è vincolato come segue:

```
(‘cim_Malware_indexes‘) tag=malware tag=attack
```

Analogamente, il vincolo per l'Intrusion Detection data model è definito come:

```
(‘cim_Intrusion_Detection_indexes‘) tag=ids tag=attack
```

Anche in questo caso è necessario aggiungere l'index "nozomi" alle rispettive whitelist.

Nozomi Networks Guardian raggruppa le intrusioni e i malware in una singola categoria di allarmi. Infatti, esiste già un event type chiamato "nozomi_all_alerts" definito con l'installazione del Nozomi Networks Add-on. Questo event type utilizza il sourcetype "nozomi:alert" nella sua stringa di ricerca, consentendo agli eventi contrassegnati con i tag "attack" e "ids" di utilizzare lo stesso sourcetype.

Per distinguere in modo più accurato i malware scambiati tra due nodi della rete, è possibile utilizzare la seguente stringa di ricerca e assegnare il tag "malware" agli eventi correlati:

```
index=nozomi sourcetype=nozomi:alert threat_name!=""
```

Con questa query, si specifica che ci si desidera riferire esclusivamente agli allarmi in cui il campo "threat_name" è definito e contiene valori. Poiché non esiste un campo specifico negli eventi per distinguere i malware da altre tipologie di allarmi legati alle intrusioni, "threat_name" rappresenta il campo più idoneo per questa distinzione. Successivamente, è possibile creare un event type denominato "malware" incorporando questa query e assegnando il tag "malware" ad esso.

Un campo di particolare interesse è "action". Esaminando la tabella del CIM, possiamo leggere i valori previsti per questo campo. Tale campo fa riferimento all'azione intrapresa dal dispositivo e i valori attesi dovrebbero essere "allowed", "blocked", "deferred", o simili. Va notato che questa tipologia di informazione non è originariamente presente nei nostri eventi, in quanto Nozomi Guardian non prende azioni dirette sugli allarmi ma invece inoltra semplicemente tutti gli eventi a Splunk per la visualizzazione e l'analisi.

Se desideriamo utilizzare InfoSec per una visione completa dei dati trasmessi da Nozomi, possiamo assegnare un valore generico al campo "action" per i nostri eventi, ad esempio "sniffed" per indicare che il dispositivo ha semplicemente catturato questi dati. Pertanto, creiamo un campo calcolato chiamato "action" per il sourcetype "nozomi:alert" con il valore "sniffed".

Alcuni campi, come "file_name" e "file_path", non sono presenti negli eventi inviati da Nozomi, dunque possiamo non effettuarne il mapping. Tali campi si applicano a entrambi i data model, dato che entrambi operano utilizzando lo stesso sourcetype.

Data model rimanenti e "rebuild"

Per il data model "Network Sessions" è stato eseguito un processo di mappatura simile a quello visto in precedenza per il data model "Network Traffic". Questo è dovuto al fatto che entrambi fanno riferimento agli eventi con sourcetype "nozomi_session".

Per quanto riguarda i rimanenti data model, ovvero "Change", "Endpoint", e "Web" è importante notare che essi si basano su dati che non vengono trasmessi da Nozomi, di conseguenza non è necessario effettuare alcuna mappatura dei loro campi.

Dopo aver completato il processo di mappatura per ciascun data model, è importante ricordare di attivare l'accelerazione per ciascuno di essi, altrimenti InfoSec non sarà in grado di utilizzarli per la creazione delle proprie dashboard.

Inoltre, se dopo aver eseguito la mappatura non si visualizzano alcuni dati all'interno delle dashboard, potrebbe essere necessario eseguire un'operazione di "rebuild" dei data model. Questa operazione ha lo scopo di aggiornare i dati all'interno dei data model e di rendere effettive le modifiche apportate. Dato che i data model accelerati fanno riferimento a dati preesistenti risalenti al momento della mappatura iniziale, l'esecuzione del "rebuild" diventa necessaria per assicurarsi che i dati siano allineati con le modifiche recenti e correttamente elaborati.

Figura 4.52. Rebuild di un data model

Per eseguire il rebuild, navighiamo in Impostazioni → Modelli di dati, troviamo il data model d'interesse e clicchiamo prima su Ricrea e poi su Aggiorna. Raggiunto lo stato di "100% completato" vedremo i dati aggiornati con l'ultimo mapping.

4.4.4 Funzionamento e dashboard di InfoSec

L'app InfoSec fornisce diverse dashboard per coprire tre ambiti principali: autenticazione, malware/antivirus e sessioni/traffico di rete.

La dashboard "Security Posture" offre una panoramica di alto livello del proprio ambiente, includendo indicatori per le statistiche di rilevamento delle intrusioni, antivirus e malware. Mostra anche le tendenze negli host, nei dispositivi e negli account monitorati. Inoltre, sono disponibili pannelli per avvisi di intrusione per informazioni su account e asset. Questi strumenti forniscono informazioni dettagliate sullo stato della sicurezza e sulle potenziali aree di rischio.

La dashboard "Health" controlla lo stato dell'ambiente Splunk in relazione ai requisiti dell'app InfoSec. Rileva infatti potenziali problemi che potrebbero influenzare il funzionamento di InfoSec, identifica le fonti di dati indicizzati e mostra lo stato dei data model necessari.

Ulteriori dashboard riguardano gli accessi Windows, le attività dei firewall, le sessioni VPN e molto altro ancora.

4.4.5 Monitoraggio autenticazioni

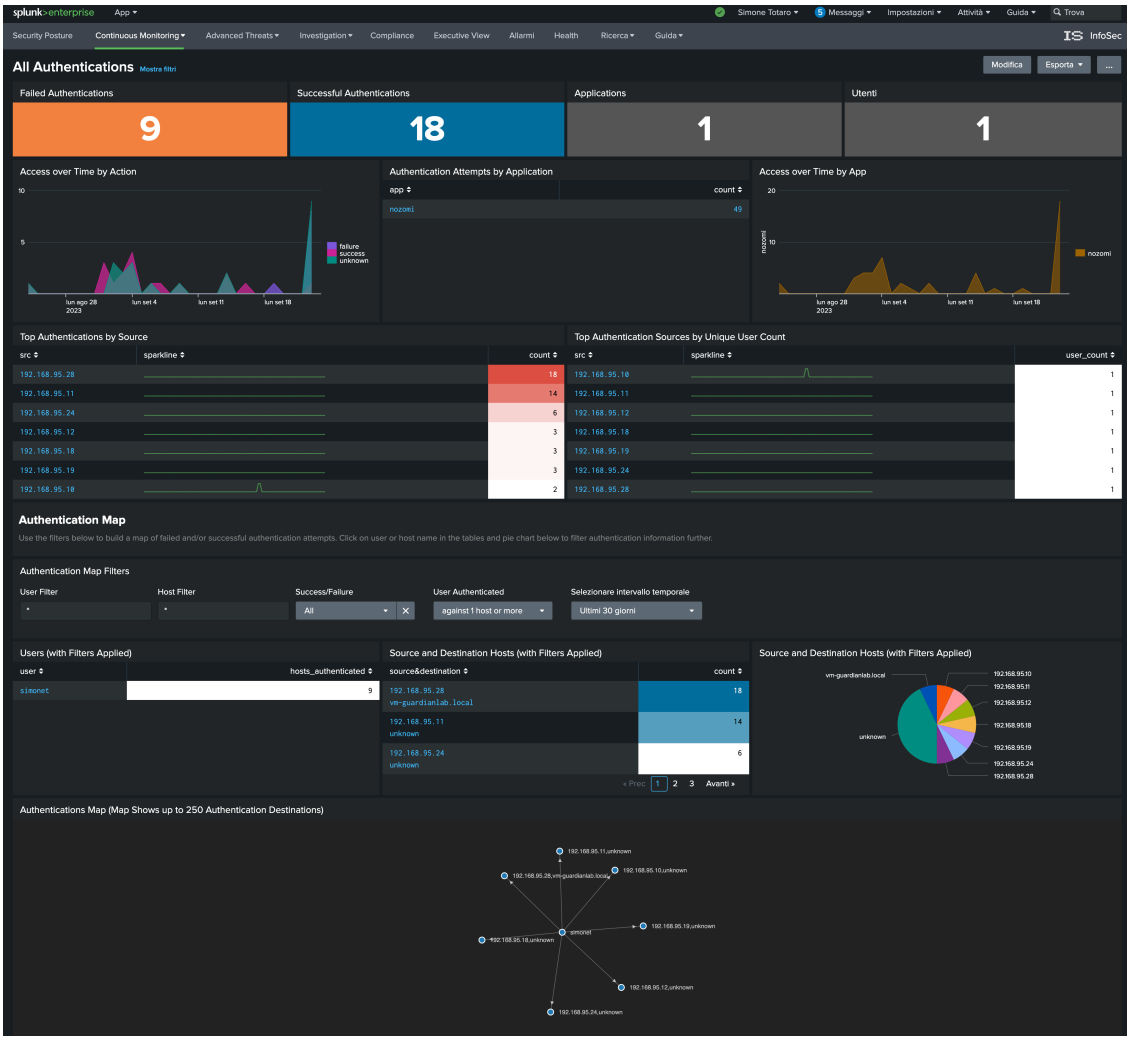


Figura 4.53. Dashboard InfoSec per le autenticazioni

Questa dashboard offre una panoramica unica delle attività di autenticazione degli utenti provenienti da diverse fonti di dati. Consente di monitorare sia le autenticazioni riuscite che quelle fallite e fornisce una rappresentazione grafica dell'andamento nel tempo del numero di accessi. Inoltre, è presente un pannello per visualizzare il conteggio delle autenticazioni per ciascuna sorgente, identificata tramite l'indirizzo IP.

Con questa dashboard potremo identificare le anomalie di autenticazione nel nostro ambiente o gli account problematici che non riescono ripetutamente ad accedere.

Nella parte sottostante possiamo filtrare per utente, host, azione (autenticazioni fallite o riuscite), e criteri di frequenza (ad esempio "Autenticazioni con 5 o più host").

È possibile estendere il monitoraggio delle autenticazioni non solo per Nozomi ma anche per altre applicazioni. Ad esempio, è possibile includere anche gli accessi degli utenti alla piattaforma Splunk semplicemente aggiungendo l'index "_audit" all'elenco degli indici consentiti nel data model "Authentication".

4.4.6 Monitoraggio traffico di rete

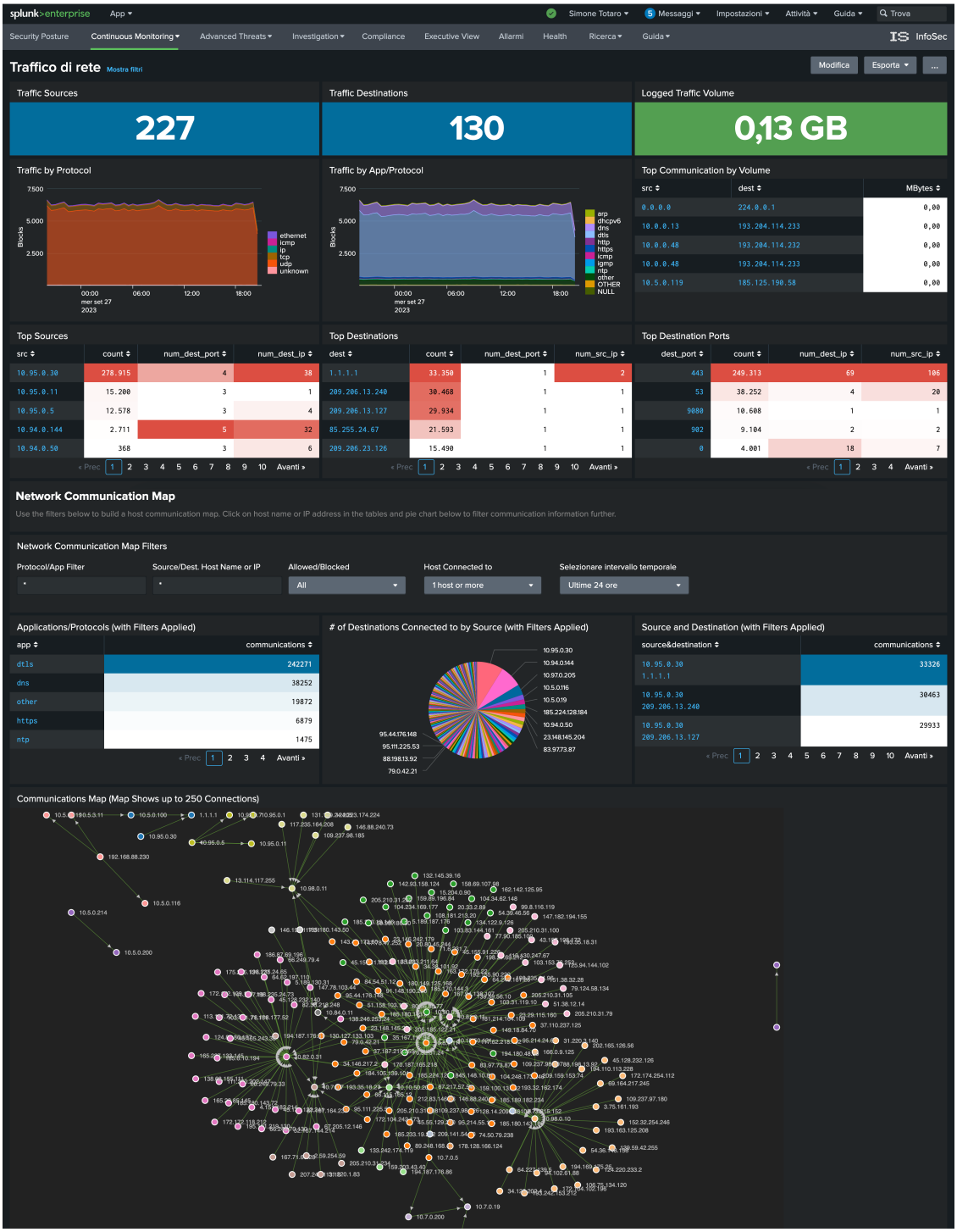


Figura 4.54. Dashboard InfoSec per il traffico di rete

Questa dashboard offre un monitoraggio completo del traffico di rete. Possiamo vedere il numero di sorgenti e destinazioni, con dettagli sugli indirizzi IP e porte di rete, oltre alla quantità di traffico scambiata nelle sessioni. I dati sono presentati attraverso grafici per ogni protocollo di rete.

Si possono applicare diversi filtri per controllare pannelli interattivi e visualizzare informazioni come il numero di destinazioni raggiunte da una sorgente specifica o il conteggio delle comunicazioni tra diverse coppie sorgente-destinazione. Inoltre, attraverso una mappa delle comunicazioni sono mostrati tutti i collegamenti tra i nodi della rete.

4.4.7 Monitoraggio malware e intrusioni

Con le seguenti dashboard possiamo monitorare i dati relativi a malware e intrusioni rilevati nella rete nelle ultime 24 ore, facenti parte del sourcetype "nozomi:alert".

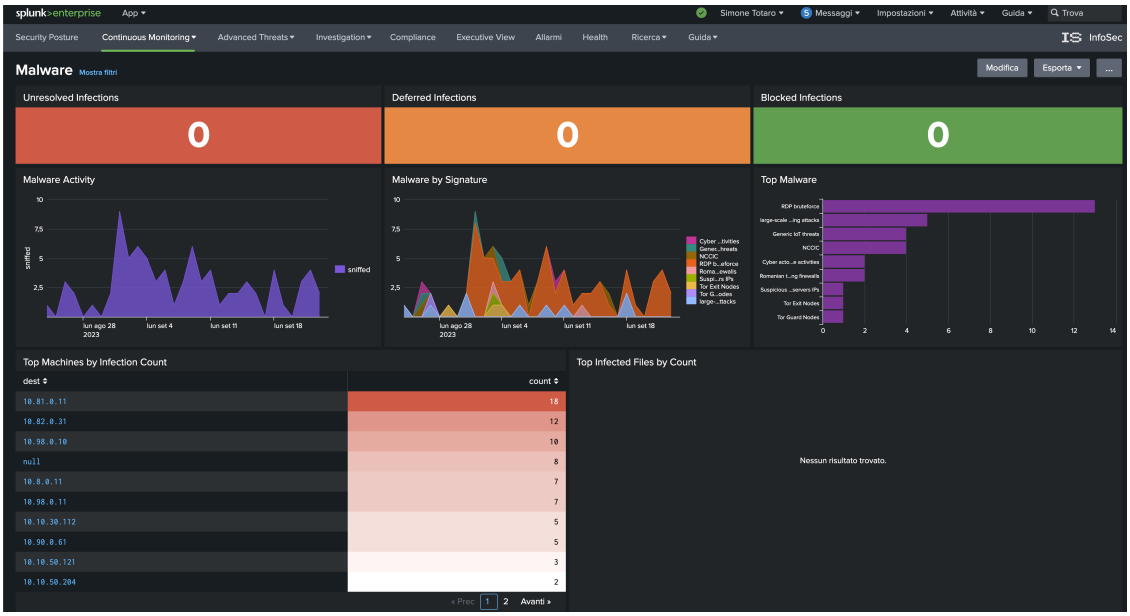


Figura 4.55. Dashboard InfoSec per i malware

Nella parte superiore della dashboard "Malware", vengono mostrati i conteggi per infezioni non risolte, differite e bloccate, basati sui valori del campo "action". Tuttavia, poiché Nozomi Guardian non intraprende azioni dirette sugli allarmi e abbiamo mappato il campo "action" al valore "sniffed", questi contatori non mostreranno alcuna informazione.

I pannelli successivi sono più informativi, mostrando il numero di malware rilevati nei giorni precedenti, i malware più frequentemente rilevati e le macchine con il maggior numero di malware rilevati. Selezionando un qualsiasi elemento all'interno dei pannelli, visualizzeremo i risultati in una nuova finestra di ricerca Splunk.

È importante notare che nella sezione "Top Infected Files by Count" non vedremo alcun valore. Questo è normale poiché Nozomi Guardian non raccoglie informazioni sui file presenti sulle macchine, ma si concentra principalmente sulla monitoraggio della rete. Pertanto, non rileva specificamente malware sui dispositivi, ma segnala le minacce trasferite nella rete tra vari nodi. Per la rilevazione vera e propria di malware e minacce sui file, è necessario utilizzare Nozomi Arc, un altro software di Nozomi Networks progettato per la raccolta di informazioni dettagliate su file, software, driver, adattatori e periferiche USB [33]. Questo software è specializzato nella rilevazione di minacce nei file, mentre Guardian si concentra principalmente sul rilevamento di minacce nella rete.

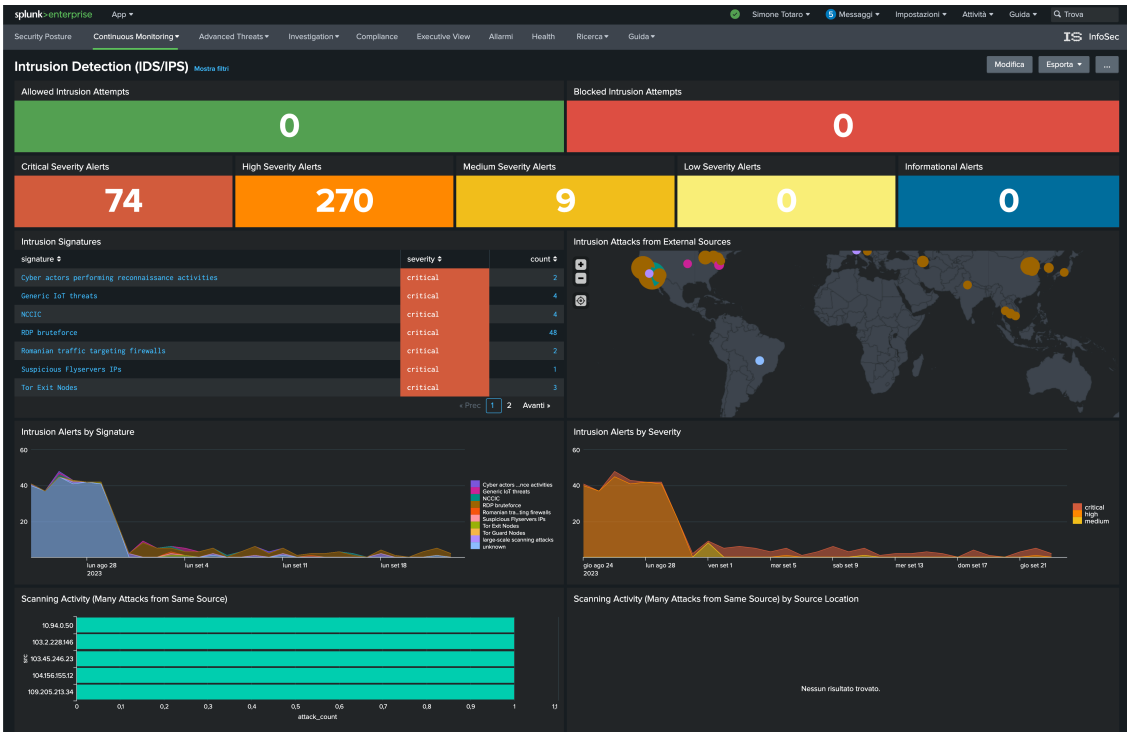


Figura 4.56. Dashboard InfoSec per il rilevamento delle intrusioni

La dashboard "Intrusion Detection" fornisce una panoramica completa dei sistemi IDS/IPS nel proprio ambiente. Gli eventi totali sono categorizzati per gravità, consentendo l'analisi specifica delle intrusioni in base alla criticità, ad esempio possiamo focalizzarci solo sugli alert ad alta severità.

Oltre a elenchi e grafici che rappresentano le intrusioni di rete, la dashboard include una mappa per identificare rapidamente le sorgenti d'attacco in base alla localizzazione degli indirizzi IP di origine. Il codice SPL del pannello "Intrusion Attacks from External Sources" è il seguente:

```
| tstats summariesonly=true allow_old_summaries=true count from
    datamodel=Intrusion_Detection.IDS_Attacks where *
    IDS_Attacks.severity="*" by IDS_Attacks.src, IDS_Attacks.signature
| rename "IDS_Attacks.*" as "*"
| iplocation src
| geostats sum(count) by signature globallimit=20 binspanlat=10
    binspanlong=10
```

La prima parte del codice utilizza il comando *tstats* per recuperare il conteggio di eventi dal data model "Intrusion_Detection", filtrando gli eventi con qualsiasi severità. Il risultato viene raggruppato per indirizzo IP sorgente e firma.

Il comando *iplocation* viene utilizzato per aggiungere ai dati informazioni sulla localizzazione geografica in base all'indirizzo IP sorgente. Questo comando estrae le informazioni sulla localizzazione dagli indirizzi IP consultando database di terze parti, ad esempio il database "MaxMind". Sono supportati sia gli indirizzi IPv4 che IPv6 e le subnet che utilizzano la notazione CIDR.

Il comando *geostats* somma per ciascuna firma il conteggio degli eventi in base alle coordinate geografiche degli indirizzi IP sorgenti, limita la visualizzazione ai 20 risultati

più significativi e usa celle quadrate di 10 gradi di latitudine e longitudine per aggregare i dati.

Infine è disponibile un pannello che mostra il numero di attacchi provenienti da vari indirizzi IP, permettendo di individuare le sorgenti con il maggior numero di attacchi.

4.4.8 Generazione e monitoraggio di allarmi

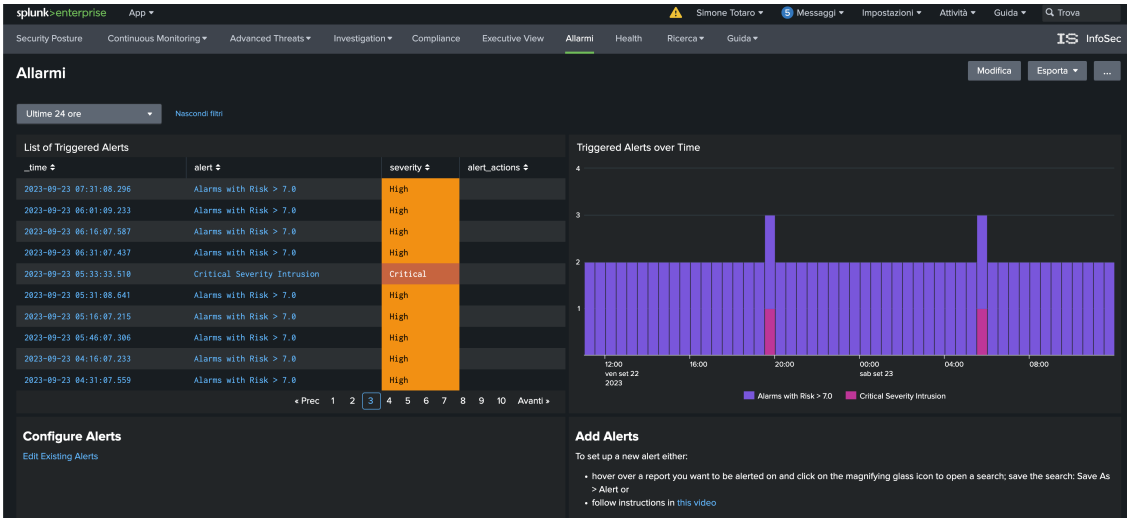


Figura 4.57. Dashboard InfoSec per gli allarmi

La dashboard "Allarmi" offre un'interfaccia per il monitoraggio e la gestione degli allarmi generati dall'app InfoSec. Gli allarmi eseguono regolarmente ricerche programmate per individuare eventi corrispondenti nei dati. Si possono esaminare gli attuali allarmi definiti nell'app InfoSec e modificarli o aggiungerne di nuovi tramite questa dashboard.

In Splunk, è possibile trasformare qualsiasi ricerca creata in un allarme, e ognuno deve includere una pianificazione della ricerca. Infatti, quando si crea un allarme, Splunk offre opzioni per specificare gli orari in cui si desideri che la ricerca venga eseguita.

È importante notare che per il data model "Alert" non è stato necessario un mapping CIM, poiché le ricerche fanno riferimento all'indice *_audit*, che è l'indice predefinito utilizzato da Splunk per memorizzare eventi di audit relativi all'attività di sistema e alle modifiche all'interno della piattaforma Splunk. Questo indice registra eventi come accessi e disconnessioni degli utenti, modifiche ai ruoli e alle autorizzazioni degli utenti e altro ancora.

A differenza della dashboard realizzata per la Nozomi App, la dashboard "Allarmi" di InfoSec si riferisce dunque agli allarmi generati da Splunk anziché da Nozomi. È possibile configurare avvisi personalizzati definendo ricerche SPL specifiche.

Generazione allarme per allarmi Nozomi con rischio elevato

Possiamo ad esempio creare un allarme che scatti quando vengono rilevati allarmi di Nozomi con un valore di rischio superiore a 7.0, indicando una criticità elevata. Possiamo fare in modo che la ricerca sia eseguita in automatico ogni 15 minuti e faccia riferimento ai dati delle ultime 24 ore.

La ricerca che vogliamo pianificare è la seguente:

```
‘nozomi_indexes‘ sourcetype="nozomi:alert" risk>7.0
| fields *
| fillnull value="N/A" id_dst, id_src
| search id_src="***" id_dst="***"
| table id, _time name, id_src, id_dst, port_src, port_dst, risk
| rename id_src as Source, id_dst as Dest, port_src as Src_Port,
   port_dst as Dest_Port, risk as Risk, name as Nome
```

Per creare un alert, iniziamo eseguendo la ricerca su Splunk e poi selezionando Salva come → Alert.

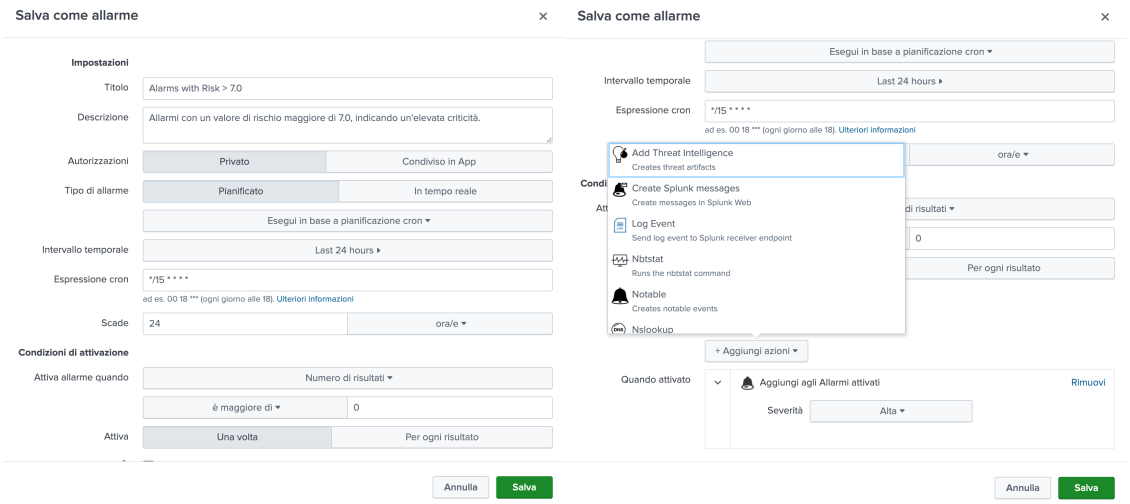


Figura 4.58. Generazione di un allarme Splunk

Qui avremo l'opportunità di personalizzare l'alert che stiamo creando. Inseriamo un titolo, impostiamo i permessi su "Privato" e scegliamo la tipologia "Pianificato". Selezioniamo quindi "Esegui in base a pianificazione cron". Come intervallo temporale impostiamo "Ultime 24 ore" e come espressione Cron inseriamo: */15 * * * *. Questa espressione significa "esegui la ricerca ogni 15 minuti". Per generare facilmente un'espressione Cron, è possibile utilizzare il sito Crontab.guru.

Nella sezione "Attiva azioni", facciamo clic su "Aggiungi azioni". Qui avremo l'opzione di selezionare varie azioni da eseguire ogni volta che l'avviso viene generato, come ad esempio inviare un log event a un endpoint di ricezione Splunk, inviare una email, eseguire uno script, e così via. In questo caso, selezioniamo solamente "Aggiungi agli Allarmi attivati".
Possiamo anche definire la gravità dell'allarme, in questo caso scegliamo "Alto".

Gli allarmi generati saranno infine visibili sull'app InfoSec, come possiamo vedere in figura 4.57.

4.5 Generazione di allarmi adoperando il MITRE ATT&CK Framework

Uno degli aspetti distintivi di Splunk è la sua capacità di integrarsi con il **MITRE ATT&CK Framework**, un modello ampiamente riconosciuto per la classificazione delle tattiche e delle tecniche utilizzate dagli aggressori nel campo della cybersecurity.

Grazie a questa integrazione, gli amministratori di sistema possono creare ricerche personalizzate basate sul MITRE ATT&CK Framework per rilevare attività sospette e comportamenti malevoli all'interno delle reti OT e IoT.

L'implementazione di regole di allarme basate su questo framework consente di generare notifiche immediate in caso di potenziali minacce, consentendo una risposta tempestiva e mirata per proteggere le infrastrutture industriali.

4.5.1 Il MITRE ATT&CK Framework

Il MITRE ATT&CK è un modello che si focalizza sull'analisi del comportamento degli avversari informatici in diverse fasi degli attacchi e sulle piattaforme che solitamente vengono prese di mira, concentrandosi su come gli avversari compromettono e operano all'interno delle reti. Può essere utilizzato per valutare gli strumenti e le difese di un'organizzazione, infatti, può essere usato ad esempio per valutare l'efficacia del SOC (Security Operations Center) dell'organizzazione, nel rilevare, analizzare e gestire le intrusioni.

È importante notare che non è possibile ottenere una copertura del 100% per ogni tecnica di ATT&CK, infatti non tutti i comportamenti degli avversari dovrebbero generare allarmi. Ad esempio, determinate azioni mirate semplicemente a risolvere problemi di rete potrebbero essere erroneamente rilevate come tentativi di attacco, ma queste attività non dovrebbero generare allarmi. [34]

L'obiettivo dunque dovrebbe essere concentrarsi sulla raccolta di informazioni e sull'implementazione di strategie di difesa per affrontare le diverse minacce nel tempo.

Il MITRE ATT&CK comprende tre elementi principali: tattiche, tecniche e sub-tecniche.

- Le **tattiche** rappresentano gli obiettivi degli avversari durante un attacco, ovvero la ragione per cui compiono una determinata azione, ad esempio scoprire informazioni, muoversi lateralmente, eseguire file ed estrarre dati.
- Le **tecniche** descrivono i comportamenti utilizzati dagli avversari per raggiungere tali obiettivi tattici, dunque rappresentano come un avversario raggiunge un obiettivo compiendo varie azioni.
- Le **sub-tecniche** infine suddividono ulteriormente i comportamenti descritti dalle tecniche in descrizioni più specifiche su come viene utilizzato il comportamento per raggiungere un obiettivo.

La correlazione tra tattiche, tecniche e sub-tecniche viene visualizzata attraverso la **Matrice ATT&CK**, riportata nella figura 4.59 della pagina seguente.

Matrice del MITRE ATT&CK Framework

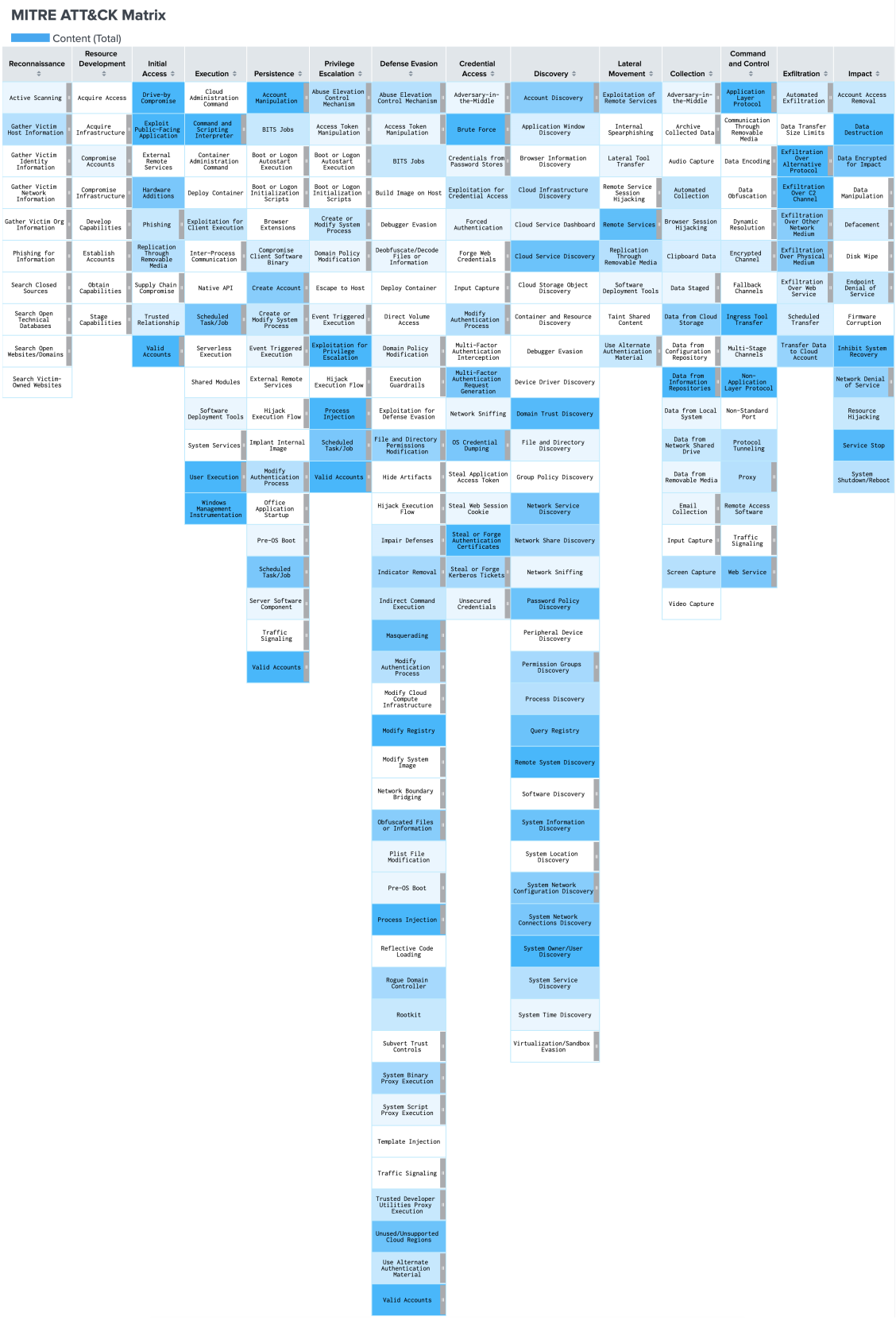


Figura 4.59. Matrice del MITRE ATT&CK su Splunk Security Essentials

MITRE ha suddiviso ATT&CK in tre matrici diverse: *Enterprise* per rappresentare reti aziendali tradizionali (con sistemi operativi Windows, Linux e MacOS) e tecnologie cloud, *Mobile* per dispositivi mobili, e *ICS* per sistemi di controllo industriale. Ciascuna di queste matrici contiene a sua volta tattiche e tecniche associate al dominio di quella matrice.

Le tattiche sono considerate come "etichette" all'interno della matrice, in cui una tecnica o sub-tecnica è associata a una o più categorie di tattiche.

Un esempio di tattica è il *movimento laterale*, ovvero una strategia usata dagli attaccanti per muoversi all'interno di una rete dopo aver ottenuto l'accesso iniziale, in modo da ottenere dati sensibili o privilegi speciali. Per ottenere con successo il movimento laterale in una rete, gli attaccanti dovranno impiegare una o più tecniche elencate nella colonna "Lateral Movement" della matrice.

ATT&CK fornisce molti dettagli sulle diverse tattiche e tecniche, fornendo descrizioni, esempi e suggerimenti relativi al rilevamento e alla mitigazione. Per accedere a informazioni più approfondite, è sufficiente visitare il sito ufficiale di MITRE [35] e fare clic su una cella della matrice d'interesse.

4.5.2 Ricerca dei Security Content su Splunk Security Essentials

Per l'integrazione con il MITRE ATT&CK, Splunk incorpora la Matrice Enterprise nell'applicazione Security Essentials, che serve per esplorare vari scenari di sicurezza e affrontare diverse minacce. Tale applicazione può essere scaricata e installata gratuitamente dal seguente link di Splunkbase: Splunk Security Essentials - Splunkbase. [36]

Dopo l'installazione di Security Essentials, è possibile accedere alla matrice navigando su Analytics Advisor → MITRE ATT&CK Framework. Per ciascuna tecnica all'interno della matrice, Splunk ha definito diverse query SPL denominate "Security Content", le quali possono essere personalizzate e utilizzate per generare allarmi in Splunk.

La prima fase dell'integrazione ha comportato un'analisi dei vari Security Content disponibili per ciascuna tattica, con lo scopo di determinare, in base ai dati provenienti da Nozomi, quali fossero le query più appropriate da attivare in Splunk per generare allarmi. Questi allarmi possono essere successivamente visualizzati nell'app InfoSec, con la possibilità di inviare notifiche agli amministratori di sistema, ad esempio, tramite email.

Per esaminare i vari Security Content disponibili per una determinata tecnica, selezioniamo una cella nella matrice e scorriamo verso la parte inferiore della pagina, dove troveremo vari filtri e opzioni di visualizzazione.

Prendiamo ad esempio in considerazione la tecnica "Network Service Discovery" appartenente alla tattica "Discovery" (figura 4.60). Questa tecnica si riferisce ai metodi utilizzati dagli attaccanti, come la scansione delle porte e delle vulnerabilità, per raccogliere elenchi dei servizi in esecuzione sui dispositivi di rete in modo da trovare potenziali servizi vulnerabili. [37]

Security Essentials mostrerà un elenco dei vari Security Content disponibili per la tecnica selezionata, assegnando un colore diverso per ciascuno di essi in base allo stato, il quale può essere: *Active* se rappresenta un contenuto attualmente in esecuzione, *Available* se si dispongono i dati per poter attivare il contenuto, oppure *Needs data* se è un contenuto per il quale sono necessari ulteriori dati per l'attivazione.

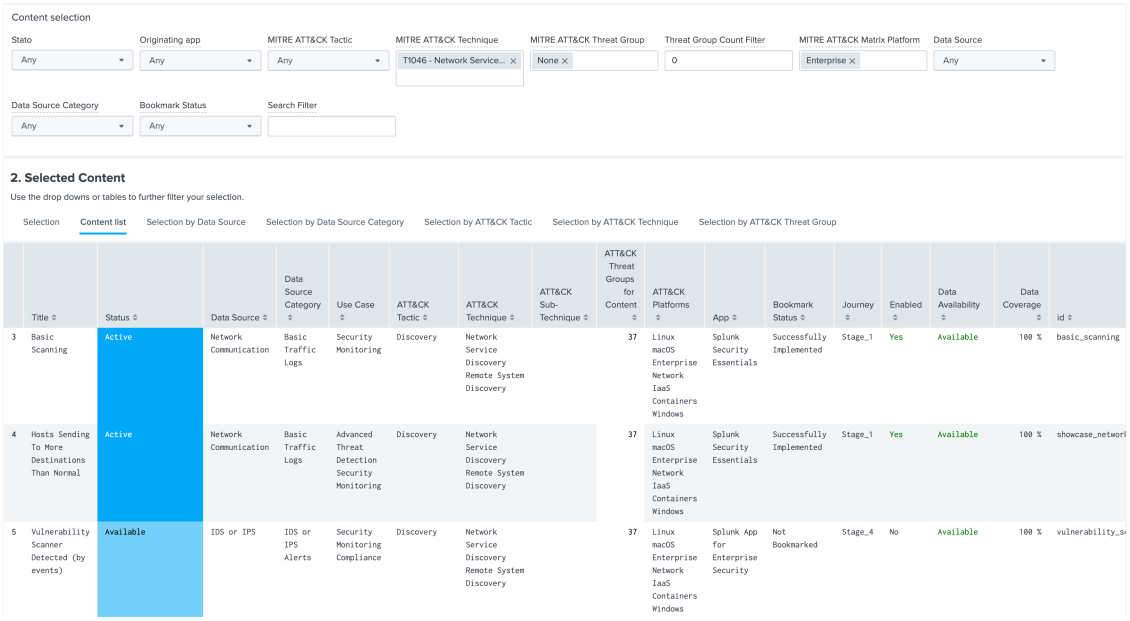


Figura 4.60. Elenco di alcuni Security Content per la tecnica "Network Service Discovery"

Per ciascuna voce sono riportati vari dettagli, quali la categoria della sorgente dati, il caso d'uso, le tattiche e le tecniche associate. È importante notare che, in alcuni casi, un contenuto può anche essere correlato a più tecniche all'interno del framework ATT&CK. La descrizione include inoltre le piattaforme su cui possono verificarsi gli attacchi, ad esempio Linux o MacOS, e il numero di *gruppi* associati a quel particolare contenuto.

I **gruppi** sono noti avversari o gruppi di attaccanti che sono stati identificati, monitorati e documentati da organizzazioni pubbliche e private. Ciascun gruppo è identificato da un nome e collegato a una serie di tattiche, tecniche e sub-tecniche che utilizzano nelle loro operazioni. Questa associazione consente di comprendere meglio il comportamento degli avversari e di avere informazioni sulle tattiche e le tecniche che potrebbero essere utilizzate da un determinato gruppo.

Per esaminare ulteriormente i contenuti sulla sicurezza, clicchiamo in fondo alla pagina sul tasto "Drill down to content selection" per visualizzare tutti i security content in una nuova pagina.

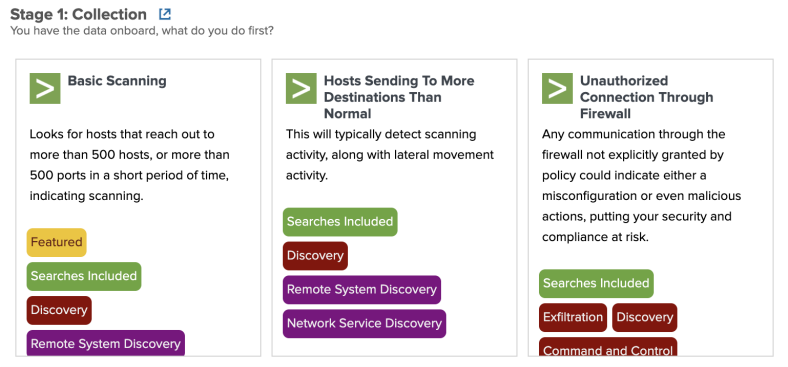


Figura 4.61. Security Content di Network Service Discovery

Security Content "Basic Scanning"

Esaminiamo ora il contenuto "Basic Scanning," il quale si focalizza sulla rilevazione di host che effettuano comunicazioni con più di 1000 host diversi o coinvolgono più di 1000 porte diverse in un breve periodo di tempo. Questo è un indicatore di potenziali tentativi di scansione di rete, le quali permettono agli aggressori di scoprire la superficie di attacco di un'organizzazione e di prepararsi per le fasi successive di un attacco. In generale, le scansioni dovrebbero avvenire solo da fonti autorizzate, quindi è importante rilevare eventuali tentativi non autorizzati.

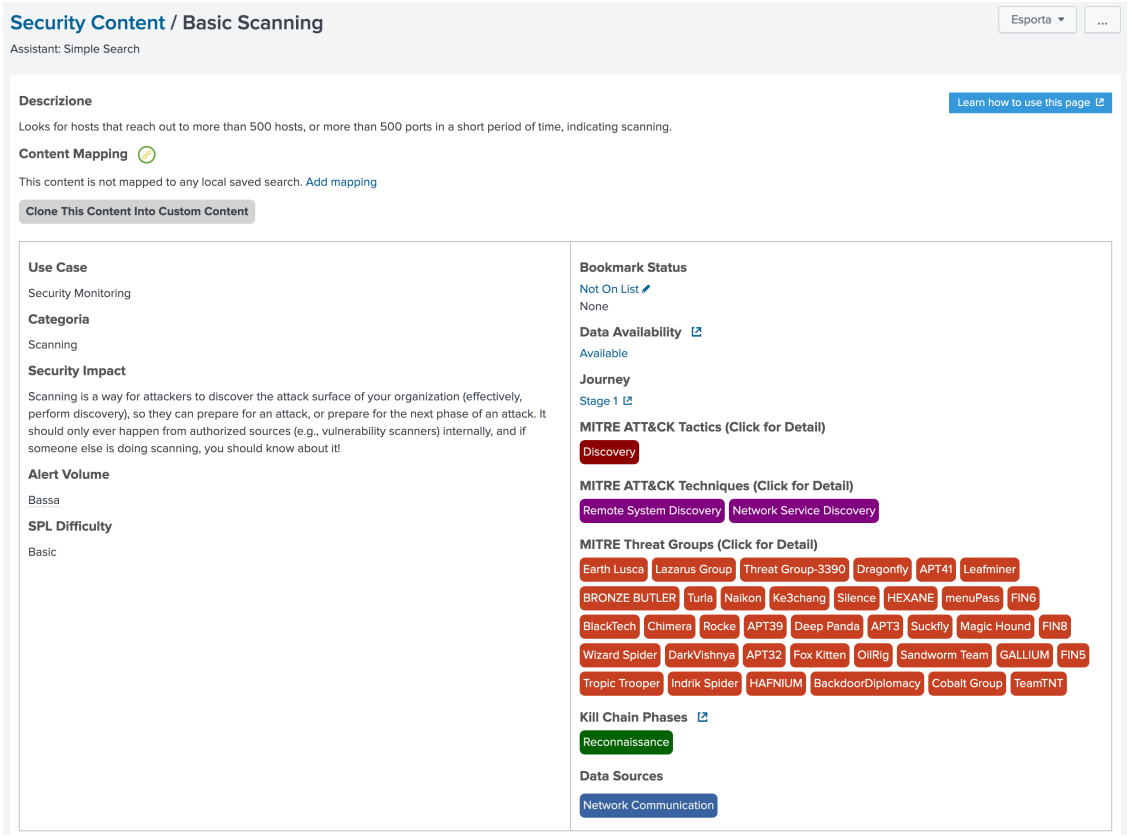


Figura 4.62. Analisi del Security Content "Basic Scanning"

Security Essentials fornisce informazioni dettagliate sul Security Content, inclusa una breve descrizione dell'attività dannosa che mira a identificare, l'impatto sulla sicurezza che questa attività potrebbe avere, il livello di rischio associato all'allarme e altre informazioni pertinenti fornite dal MITRE, come l'elenco di tutti i gruppi correlati, come ad esempio "Earth Lusca", "Lazarus Group", ecc.

Security Essentials include anche i requisiti necessari per configurare la query come un allarme (figura 4.63). In questo specifico caso, è necessario avere dati provenienti dai firewall all'interno di Splunk. Inoltre, affinché la query funzioni correttamente, i campi "dest_ip" e "dest_port" devono essere definiti. Infatti, i dati devono essere conformi al Common Information Model, il che richiede il mapping come già eseguito in precedenza.

In seguito, è fornita la query SPL da utilizzare come riferimento per l'attivazione dell'allarme, in quanto è necessario personalizzarla in base agli indici e ai sourcetype relativi ai dati di nostro interesse.

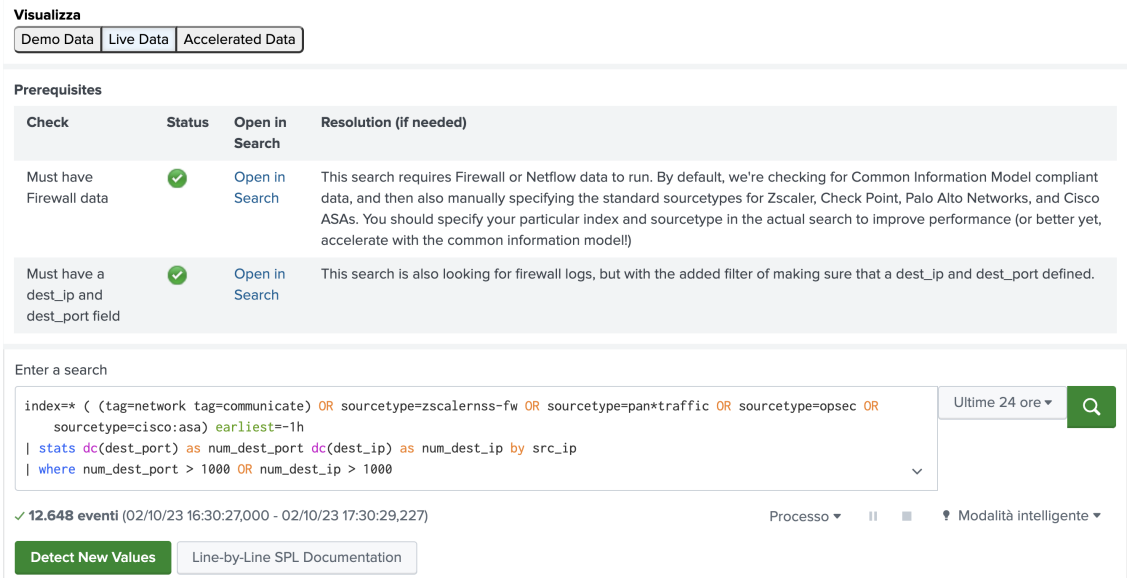


Figura 4.63. Requisiti e query del Security Content "Basic Scanning"

La query suggerita dal Security Content inizia cercando in tutti gli indici, filtrando dati da diversi sourcetype e da eventi contrassegnati con i tag "network" e "communicate" e limitando la ricerca agli eventi verificatisi nell'ultima ora. Per ogni indirizzo IP sorgente, calcola il numero di porte di destinazione uniche ("num_dest_port") e il numero di indirizzi IP di destinazione unici ("num_dest_ip"). Infine, mostra solo i risultati in cui il numero di porte di destinazione uniche o il numero di indirizzi IP di destinazione unici sono superiori a 1000, identificando dunque quegli indirizzi IP sorgenti che comunicano con un numero insolitamente elevato di porte o indirizzi IP di destinazione.

A questo punto, è possibile personalizzare la query in base ai nostri dati. Ad esempio, è possibile limitare la ricerca all'indice *nozomi* e ai tag *network* e *communicate*, rimuovendo le diverse tipologie di sourcetype elencate nell'operatore OR.

Successivamente è possibile attivare l'allarme, eseguendo la ricerca in una nuova scheda utilizzando l'applicazione "Search & Reporting" e seguendo la procedura illustrata nella sezione 4.4.8. Clicchiamo dunque su "Salva come" e poi su "Alert", assegniamo un nome all'allarme, impostiamo l'intervallo temporale in modo che la ricerca venga eseguita ogni 15 minuti relativamente ai dati delle ultime 24 ore e definiamo la severità dell'allarme (in questo caso, "Bassa" come suggerito dal Security Content).

Infine, è possibile selezionare l'azione desiderata, in questo caso scegliamo solamente di aggiungere l'allarme agli allarmi attivati. Da questo momento in poi, ogni volta che l'allarme si attiverà, sarà visibile nella dashboard "Allarmi" nell'applicazione InfoSec.

Security Content "Hosts Sending To More Destinations Than Normal"

Appartenente alla stessa tecnica "Network Service Discovery" del MITRE è il Security Content "Hosts Sending To More Destinations Than Normal", il quale mira a rilevare, come l'alert precedente, attività dannose di scansione della rete, insieme ad attività di movimento laterale.

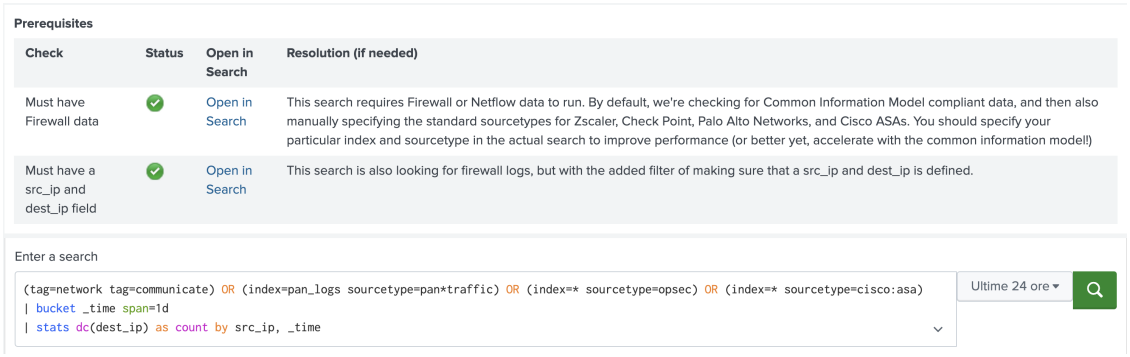


Figura 4.64. Requisiti e query del Security Content "Hosts Sending To More Destinations Than Normal"

La query riportata nel Security Content è progettata per trovare attività anomale relative all'invio di dati da parte di host a un numero insolitamente elevato di destinazioni in un breve periodo di tempo, il che potrebbe indicare un comportamento sospetto, ad esempio un'esplorazione non autorizzata della rete per raccogliere informazioni su di essa.

Tale query crea degli insiemi (bucket) di dati temporali, suddividendo gli eventi in gruppi in base a una finestra temporale di un giorno ("span=1d"). Successivamente con il comando *stats* conta quante destinazioni diverse sono state raggiunte da ogni host in un giorno specifico.

Alla fine della query possiamo aggiungere $|where\ count > 500$, in modo da filtrare i risultati per mostrare solo le righe in cui il conteggio di destinazioni supera un determinato valore, in questo esempio 500. Questo significa che la query identificherà gli host che hanno comunicato con più di 500 destinazioni uniche nel periodo di tempo specificato. Valori adeguati per il filtro *where* e per l'intervallo temporale che vogliamo considerare andrebbero scelti in seguito ad un'analisi approfondita del proprio traffico di rete, per capire come correttamente configurare l'alert.

Security Content "Basic Brute Force Detection"

Esaminiamo ora il Security Content chiamato "Basic Brute Force Detection", che rientra nella tecnica "Brute Force" e nella tattica "Credential Access". Questa tattica consiste di tecniche che mirano a scoprire le credenziali degli utenti, inclusi nomi utente e password.

Tali tecniche di forza bruta sono utilizzate per ottenere l'accesso agli account, provando ad indovinare le password deboli utilizzando un meccanismo ripetitivo o iterativo, tentando centinaia di password comuni. Vengono usate non solo quando le password sono sconosciute, ma anche quando vengono ottenuti gli hash delle password.

La query suggerita utilizza controlla semplicemente se all'interno dei propri log è presente un numero elevato di accessi non riusciti e almeno un accesso riuscito dalla stessa sorgente.

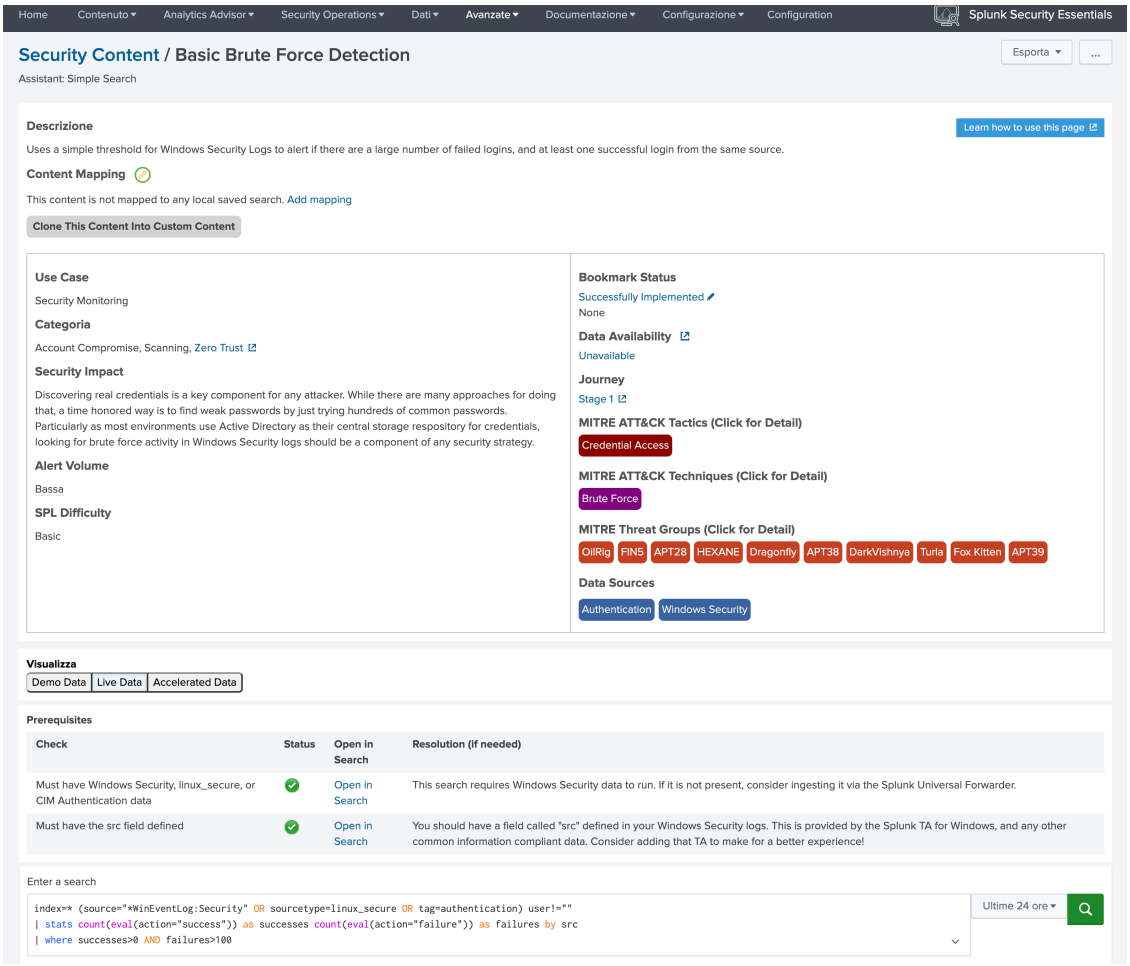


Figura 4.65. Analisi del Security Content "Basic Brute Force Detected"

Notiamo che la ricerca si basa su un sorgente relativo ai Windows Security Logs (che non è rilevante per noi) o sugli eventi etichettati con il tag "authentication." In precedenza, avevamo già mappato il data model "Authentication" e definito un Event Type con i tag appropriati per concentrarci esclusivamente sui tentativi di autenticazione in Nozomi. Inoltre, la query richiede un campo "src" definito nei nostri dati.

Eseguiamo ora questa query e salviamola come allarme, configurando il range temporale per le ultime 24 ore e impostando la frequenza a ogni 5 minuti. Questa volta vogliamo che l'allarme invii automaticamente una email a un utente specifico, ad esempio a un amministratore di sistema. Perciò, come prima azione di trigger, selezioniamo "Aggiungi agli Allarmi Attivati" con una severità "Bassa", mentre come seconda azione impostiamo "Invia email".

In questa sezione (figura 4.66) è possibile inserire l'indirizzo di destinazione al quale verranno inviate le email contenenti gli allarmi e definire la priorità, l'oggetto e il corpo del messaggio. Di default, viene utilizzato il token *$name$* per utilizzare il nome dell'allarme stesso.

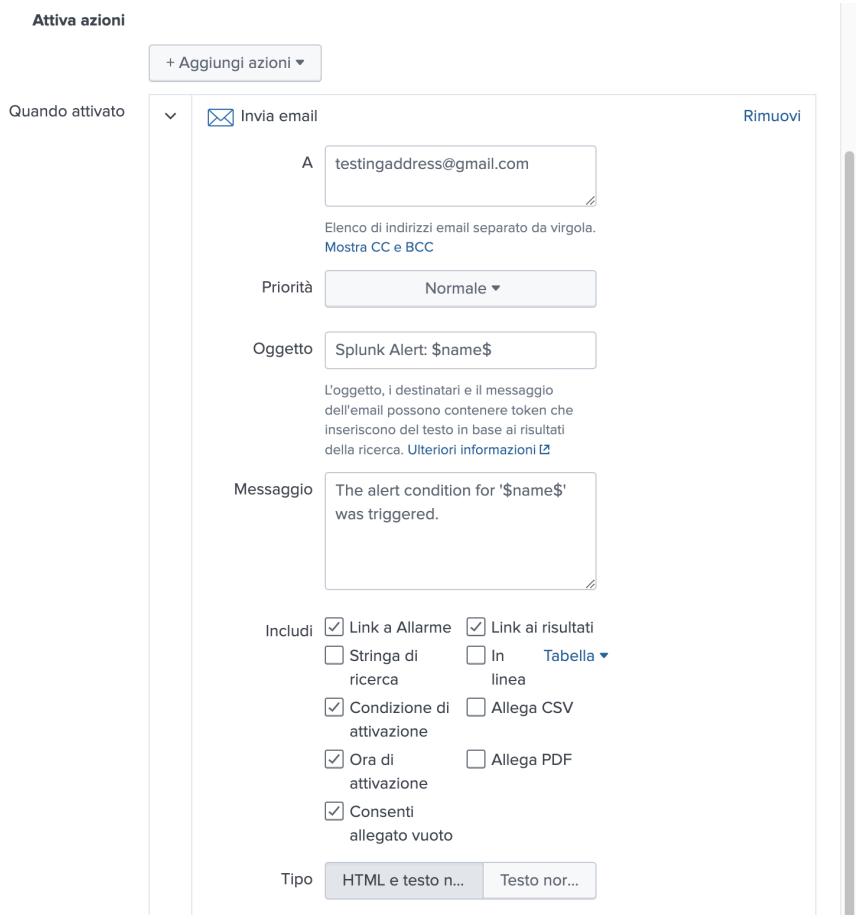


Figura 4.66. Configurazione email automatica per allarme

In aggiunta, è possibile selezionare quali informazioni includere nell'email, come ad esempio un link diretto all'allarme su Splunk, la stringa di ricerca e la condizione che ha scatenato l'allarme, l'orario di attivazione e un link ai risultati. Inoltre, è possibile allegare un file CSV o PDF contenente un report dettagliato sull'allarme.

Figura 4.67. Configurazione per l'invio di email da Splunk

Per configurare Splunk per l'invio di email tramite un account Gmail, è necessario seguire i seguenti passaggi:

1. Andare su Impostazioni → Impostazioni Server → Impostazioni Email
2. Nel campo "Host di posta", inserire "smtp.gmail.com:587".
3. Selezionare l'opzione "Abilita TLS" nel campo "Protezione email".
4. Nel campo "Nome utente" inserire l'indirizzo email da cui si desidera inviare le email.
5. Per quanto riguarda la password, non inserire la password del proprio indirizzo Gmail. Bisogna creare una nuova password specifica per Splunk e salvarla direttamente nella configurazione di Gmail.
6. Successivamente, è possibile personalizzare il formato dell'email, ad esempio, aggiungendo un testo a piè di pagina. Inoltre, vi è la possibilità di definire completamente il formato dei report in formato PDF, nel caso si desiderasse allegarli alle email.

Per creare una password appositamente per Splunk, accediamo alle impostazioni del nostro account Gmail, andando sulla pagina "Gestisci il tuo Account Google" e poi su Sicurezza. Qui dobbiamo innanzitutto attivare e configurare la "verifica in due passaggi" di Google, ovvero l'autenticazione a due fattori, necessaria per aggiungere un livello di sicurezza extra all'account. Una volta completata la configurazione della verifica in due passaggi, bisogna accedere alla sezione "Password per le app".

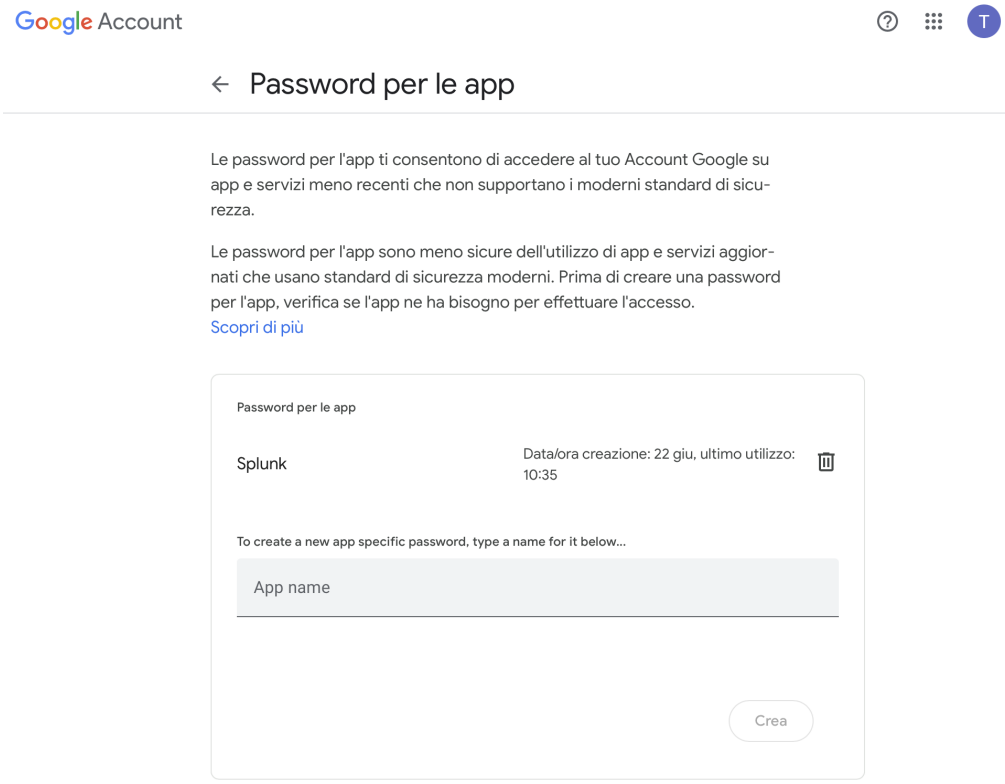


Figura 4.68. Password per le app su Gmail

Questo passaggio è necessario in quanto determinati servizi meno recenti, tra cui Splunk, potrebbero non essere completamente allineati ai moderni standard di sicurezza di Google. Dunque, creiamo qui una nuova app specificamente per Splunk e generiamo una password. Completata questa procedura, potremo inserire questa password nelle "Impostazioni server di posta" di Splunk visto precedentemente.

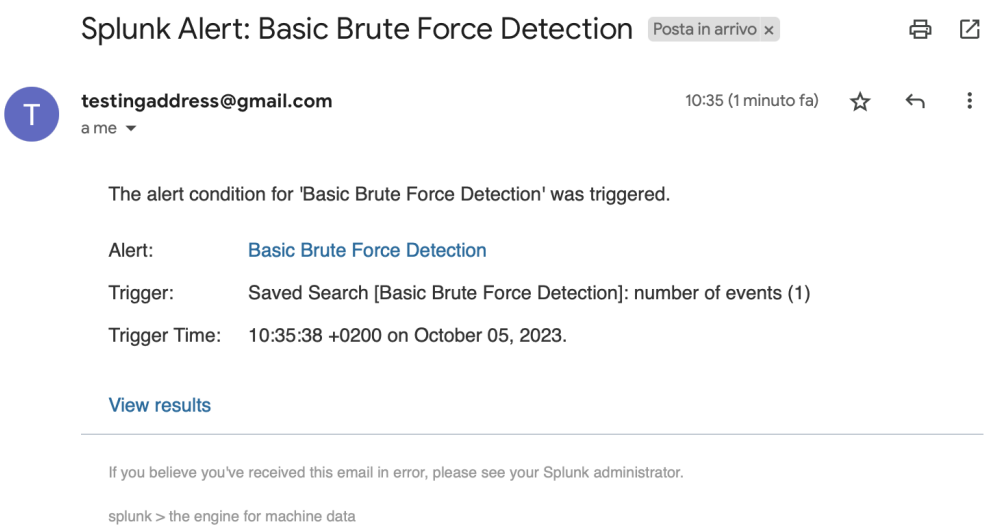


Figura 4.69. Invio email automatica per allarme Brute Force

Nell'immagine è presentato un esempio di email inviata a un account di test in risposta a un allarme generato da un tentativo di attacco a forza bruta su Nozomi Guardian.

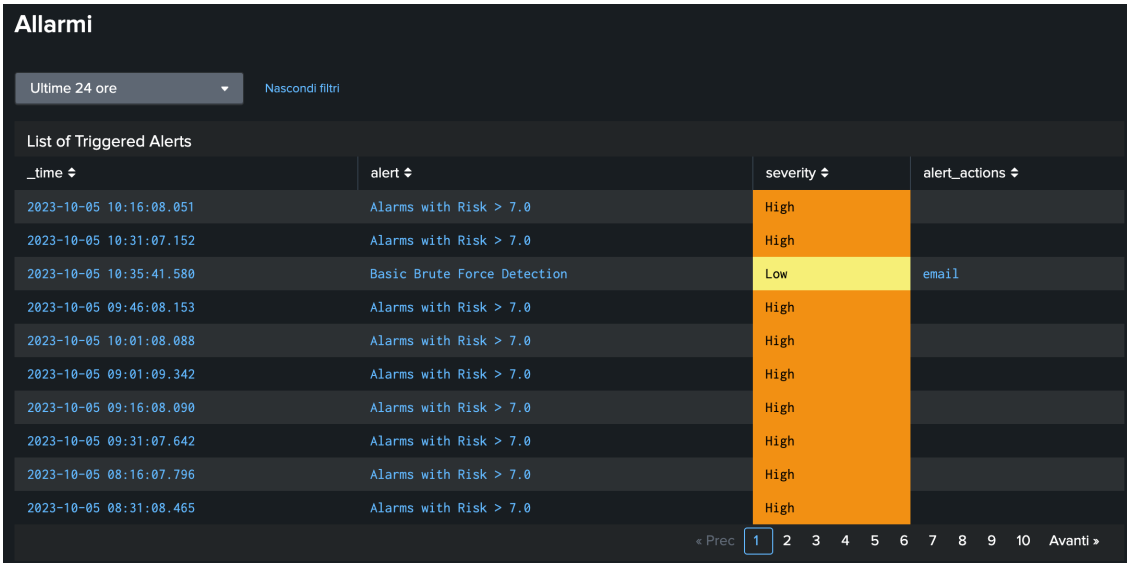


Figura 4.70. Allarme Brute Force visibile su InfoSec

Notiamo inoltre che il nuovo allarme appena generato è ora visibile anche tramite l'applicazione InfoSec, dunque la configurazione ha funzionato correttamente.

Capitolo 5

Conclusione

5.1 Risultati ottenuti

L'integrazione di Nozomi Networks con Splunk è stata quindi eseguita con successo. I dati sono ora correttamente visibili all'interno dell'ambiente Splunk, sfruttando le varie dashboard delle due applicazioni, Nozomi App e InfoSec. Questa integrazione permette ad un'organizzazione di estendere notevolmente la visibilità dell'intera infrastruttura, consentendo un'analisi più approfondita dei propri dati di log. Tale sviluppo rappresenta un passo significativo nella protezione dell'organizzazione da possibili minacce, sia da parte di singoli che di gruppi di attaccanti.

Un aspetto importante di questa integrazione è stato inoltre l'utilizzo del MITRE ATT&CK Framework, che consente la generazione di allarmi utilizzando le numerose query fornite da Security Essentials. Questo aspetto è fondamentale poiché fornisce un metodo efficace per monitorare costantemente il proprio ambiente di rete.

Ad esempio, alcuni security content adatti ai dati di Nozomi, non analizzati nel capitolo precedente, permettono di verificare se vengono utilizzate porte considerate proibite in particolari collegamenti di rete. Questo consentirebbe di individuare dispositivi di rete potenzialmente compromessi o configurati in modo errato, rientrando nella tecnica "Command and Control" della matrice ATT&CK.

Altri contenuti consentono invece di analizzare se nel traffico di rete vi sono casi in cui un protocollo di alto livello non coincide con la porta attualmente in uso. Ad esempio, questo contenuto dovrebbe identificare se sulla porta TCP 80 sono in esecuzione protocolli diversi da HTTP. Ciò indicherebbe tentativi di aggirare le restrizioni del firewall, oppure tentativi di nascondere comunicazioni dannose su porte e protocolli tipicamente consentiti ma non correttamente monitorati. Una situazione simile rientrerebbe nella tecnica di "Exfiltration" della matrice.

In conclusione, questa integrazione migliora notevolmente la capacità dell'organizzazione di monitorare, rilevare e mitigare potenziali minacce, rappresentando un importante passo avanti nella strategia di sicurezza complessiva dell'azienda.

5.2 Sviluppi futuri

Tutti i dati utilizzati per la realizzazione di questa tesi sono stati ottenuti da ambienti di laboratorio e simulati mediante l'uso di macchine virtuali. Questo è stato necessario per

comprendere e testare l'integrazione tra Nozomi e Splunk e per dimostrarne il potenziale in un ambiente controllato.

Il prossimo passo di questa integrazione sarebbe quindi l'utilizzo di dati reali, dunque provenienti da dispositivi OT e IoT all'interno dell'infrastruttura di un'organizzazione e raccolti direttamente da Nozomi Networks, per poi visualizzarli tramite le dashboard realizzate appositamente per questa piattaforma. Di conseguenza, utilizzando dati reali sarà necessario estendere la normalizzazione in conformità con il Common Information Model ai dati che non sono stati simulati utilizzando l'ambiente di laboratorio. In particolare, si potrebbe adoperare il software "Nozomi Arc" per la raccolta e l'analisi di informazioni su file, driver e periferiche USB, in aggiunta all'utilizzo di Nozomi Guardian.

5.2.1 Elevare la sicurezza con Splunk Enterprise Security

In prospettiva, si potrebbe inoltre pensare di utilizzare Enterprise Security, ovvero una soluzione avanzata e a pagamento di Splunk che, in confronto a InfoSec, introduce una serie di funzionalità che rendono la gestione del livello di rischio molto più automatizzata.

Per fare un esempio, possiamo considerare un evento, come un tentativo di attacco a forza bruta, che si verifica costantemente, per esempio ogni notte. In questo caso l'indice *severity*, ovvero il livello di rischio dell'evento, può essere considerato basso dal punto di vista del Security Operations Center (SOC) dell'organizzazione, dunque potremmo inizialmente ritenere che non sia necessaria alcuna azione da parte nostra, in quanto tali tentativi sono piuttosto comuni e non richiedono una risposta immediata. La situazione cambia però quando iniziamo a notare un aumento significativo di eventi correlati, come scansioni insolite della rete o errori provenienti da pagine web.

In questo scenario, come in InfoSec, tutti gli eventi che vengono generati vengono raccolti e presentati in una dashboard. Tuttavia, in Enterprise Security vi è la possibilità di assegnare specifici eventi a utenti o operatori del SOC, consentendo a un determinato utente di esaminare l'evento in dettaglio, verificare se richiede ulteriori azioni oppure determinare se è stato già risolto. In tal caso, l'utente avrebbe la possibilità di automatizzare determinate azioni in risposta a tali eventi, come ad esempio effettuare il blocco di certi indirizzi IP.

Enterprise Security introduce anche le "Correlation Searches", ovvero delle query di ricerca più complesse rispetto a quelle disponibili in Security Essentials, in quanto consentono di eseguire analisi più approfondite del traffico di rete. Queste query rappresentano un potente strumento quando combinate con il MITRE ATT&CK Framework, poiché permettono di identificare pattern e comportamenti sospetti che potrebbero rimanere inosservati con le query più semplici di Security Essentials.

Tali query sfruttano il Data Enrichment di Enterprise Security, ovvero una funzionalità che consente di arricchire i dati con informazioni esterne utilizzando file di lookup, aggiungendo ai dati di log informazioni sugli asset aziendali e sulle identità degli utenti. Ad esempio, è possibile categorizzare determinati dispositivi come "scanner", riducendo i falsi positivi, comprenderne meglio la provenienza, assegnare priorità in base a categorie come "server" o "PC", e molto altro.

Trattandosi dunque di una soluzione a pagamento, risulta importante condurre un'analisi dettagliata all'interno dell'organizzazione, per valutare se siano realmente necessarie le funzionalità più avanzate offerte da Enterprise Security, oppure se sia sufficiente utilizzare InfoSec per ottenere una sorveglianza e un monitoraggio dei dati più semplice attraverso le sue varie dashboard e strumenti disponibili.

Ringraziamenti

Desidero esprimere la mia profonda gratitudine a coloro che hanno contribuito alla realizzazione di questa tesi.

Innanzitutto, desidero ringraziare il mio Relatore, il Professore Guido Marchetto, e il mio Correlatore, l'Ingegnere Alessio Sacco, per il loro inestimabile aiuto e supporto durante la stesura di questa tesi.

Un caloroso ringraziamento va ad Alten Italia per avermi concesso l'opportunità di svolgere il tirocinio e la tesi in un contesto aziendale. In particolare, desidero esprimere la mia gratitudine al mio tutor aziendale, Paolo Seghetti, che non solo mi ha fornito una solida formazione in azienda ma ha anche fornito preziose indicazioni per la realizzazione di questa tesi.

Voglio anche dedicare un sentito ringraziamento a tutti i miei amici che hanno reso questa esperienza universitaria a Torino davvero indimenticabile e a coloro che mi hanno offerto il loro costante sostegno anche a distanza.

Infine, ma soprattutto, desidero esprimere la mia profonda riconoscenza ai miei genitori, che hanno reso possibile la mia esperienza a Torino e mi hanno sostenuto in ogni fase del mio percorso accademico, specialmente nei momenti di difficoltà. Grazie a mia sorella per essere stata sempre presente, anche a distanza, e auguri a lei e a Kevin per l'arrivo di Cassandra. Dedico quindi questo lavoro a tutta la mia famiglia, vi voglio bene.

Con affetto,

Simone Totaro

Bibliografia

[1] Nozomi Networks, "Guardian - Unlock Visibility Across OT, IoT and IT", https://www.nozominetworks.com/products/guardian/

[2] Zscaler, "What is the Purdue Model for ICS Security?", https://www.zscaler.com/resources/security-terms-glossary/what-is-purdue-model-ics-security

[3] IoT e IIoT – Significato, soluzioni e applicazioni, https://www.copadata.com/it/prodotti/platform-editorial-content/significato-di-iot-e-iiot-industrial-internet-of-things/

[4] TIBCO, "Cos'è l'Internet of things industriale (IIoT)?", https://www.tibco.com/it/reference-center/what-is-industrial-internet-of-things-iiot

[5] Introduction to Nozomi Networks, https://academy.nozominetworks.com/introduction-to-nozomi-networks

[6] Nozomi Networks, "Guardian Sensors Specification Sheet", https://www.nozominetworks.com/downloads/US/Nozomi-Networks-Guardian-Specifications-Sheet.pdf

[7] NIST National Vulnerability Database, "CVE-2021-3739 Detail", 2020, https://nvd.nist.gov/vuln/detail/CVE-2021-3739

[8] Splunk, "ICS Cybersecurity", 2020, https://www.splunk.com/en_us/form/ics-cybersecurity.html

[9] Center for Strategic & International Studies, "Significant Cyber Events List", 2020, https://csis-website-prod.s3.amazonaws.com/s3fs-public/200528_Significant_Cyber_Events_List.pdf

[10] About Splunk Enterprise, https://docs.splunk.com/Documentation/Splunk/9.1.0/Overview/AboutSplunkEnterprise

[11] Scale your deployment with Splunk Enterprise components, https://docs.splunk.com/Documentation/Splunk/9.1.0/Deploy/Distributedoverview

[12] About Splunk Enterprise deployments, https://docs.splunk.com/Documentation/Splunk/9.1.0/Overview/AboutSplunkEnterprisedeployments

[13] About deployment server and forwarder management, https://docs.splunk.com/Documentation/Splunk/9.0.4/Updating/Aboutdeploymentserver

[14] Splunk, "Splunk Enterprise architecture and processes", December 2019, https://docs.splunk.com/Documentation/Splunk/8.0.0/Installation/Splunksarchitectureandwhatgetsinstalled

[15] Cloudian, "Splunk Architecture: Components and Best Practices", https://cloudian.com/guides/splunk-big-data/splunk-architecture-data-flow-components-and-topologies/

[16] Splunk Enterprise Installation Manual, https://docs.splunk.com/Documentation/Splunk/9.1.0/Installation/Whatsinthismanual

[17] Splunk Knowledge Objects: What They Are & How to Use Them, https://kinneygroup.com/blog/know-your-knowledge-objects-in-splunk/

[18] Use fields to search, https://docs.splunk.com/Documentation/Splunk/9.1.0/SearchTutorial/Usefieldstosearch
[19] Cos'è lo stack ELK?, https://aws.amazon.com/it/what-is/elk-stack/
[20] EDUCBA, "Kibana vs Splunk", https://www.educba.com/kibana-vs-splunk/
[21] Nozomi Networks, "Creating and Using API Keys for Data Integration", https://help.vantage.nozominetworks.io/docs/api-key-config
[22] Nozomi Networks Sensor Add-on, https://splunkbase.splunk.com/app/5316
[23] Config Explorer, https://splunkbase.splunk.com/app/4353
[24] Token usage in dashboards, https://docs.splunk.com/Documentation/Splunk/9.1.1/Viz/tokens
[25] App InfoSec for Splunk, https://splunkbase.splunk.com/app/4240
[26] About data models, https://docs.splunk.com/Documentation/SplunkCloud/latest/Knowledge/Aboutdatamodels
[27] Introduction to Pivot, https://docs.splunk.com/Documentation/Splunk/9.1.1/Pivot/IntroductiontoPivot
[28] Overview of the Splunk Common Information Model, https://docs.splunk.com/Documentation/CIM/5.2.0/User/Overview
[29] Splunk Common Information Model (CIM), https://splunkbase.splunk.com/app/1621
[30] InfoSec App for Splunk Documentation, https://splunk-infosec-documentation.readthedocs.io/en/latest/
[31] SA-cim_vladiator, https://splunkbase.splunk.com/app/2968
[32] Regex101, https://regex101.com/
[33] Nozomi Networks, "Nozomi Arc Endpoint Sensor", https://uploads-ssl.webflow.com/645a4534705010e2cb244f50/649508a14bea1b9f57db436e_Nozomi-Networks-Arc-Endpoint-Sensor.pdf
[34] Blake E. Strom, Andy Applebaum, Doug P. Miller, Kathryn C. Nickels, Adam G. Pennington, Cody B. Thomas, "MITRE ATT&CK: Design and Philosophy", MITRE, March 2020, https://attack.mitre.org/docs/ATTACK_Design_and_Philosophy_March_2020.pdf
[35] The MITRE Corporation, "Enterprise Matrix", https://attack.mitre.org/matrices/enterprise/
[36] Splunk Security Essentials, https://splunkbase.splunk.com/app/3435
[37] The MITRE Corporation, "Network Service Discovery", 30 March 2023, https://attack.mitre.org/techniques/T1046/