POLITECNICO DI TORINO

Corso di Laurea Magistrale
in Ingegneria Gestionale

Tesi di Laurea

Analisi delle minacce connesse all'implementazione della blockchain in una supply chain di batterie elettriche

Relatore
prof. Guido Perboli

Candidato
Leonardo Tolla

Anno Accademico 2022-2023

A mia madre

Sommario

Nell'ambito della gestione delle catene logistiche, la tracciabilità del prodotto e l'attribuzione univoca delle responsabilità tra gli attori coinvolti rappresentano le principali sfide da affrontare. Tecnologie come la blockchain, caratterizzate dalla gestione decentralizzata di un database condiviso, forniscono una possibile soluzione a tali problemi. L'introduzione di una rete di questo tipo solleva però dubbi sulla sua affidabilità a fronte di minacce di natura informatica.

L'obiettivo del presente lavoro è quello di determinare se la tecnologia blockchain apporti un miglioramento o meno a quella che è la situazione attuale. A tal proposito, ci si è chiesto se gli attacchi dannosi fossero in grado di compromettere o meno la rete.

Per poter affrontare il problema è stato selezionato un caso d'uso come riferimento, rappresentato da una supply chain di batterie per cui è stata implementata una soluzione blockchain-based semplificata. Come strumento di supporto è stata utilizzata la piattaforma MISP, nata con l'intento di raccogliere e condividere dati sulle cyber minacce che ogni organizzazione subisce a livello globale. Da questo database è stata effettuata un'estrazione dei principali attacchi che sono stati poi sottosegmentati per livello di pericolosità. Infine, si è valutata qualitativamente la risposta del sistema blockchain agli attacchi estratti caratterizzati da un impatto medio/alto, includendo punti a favore e non. I risultati hanno evidenziato complessivamente una buona robustezza della soluzione proposta dato che gli effetti delle minacce si limitavano a livello locale, senza alterare globalmente il corretto funzionamento della rete.

Sulla base di quanto è emerso, la tecnologia blockchain appare come una concreta possibilità per far fronte alle principali sfide con cui la supply chain dovrà interfacciarsi. Tuttavia, l'adozione su larga scala di soluzioni di questo tipo è ancora alle fasi iniziali e le prospettive future indicano che sarà necessaria un'attenta valutazione circa l'effettivo ritorno dagli investimenti richiesti per la sua implementazione.

La presente tesi è stata organizzata come segue:

- **Capitolo 1:** introduzione alla tesi e background teorico sulla piattaforma MISP. In particolare, overview sulle sue principali features, il suo funzionamento e le piattaforme alternative presenti oggi.
- **Capitolo 2:** descrizione della supply chain presa in esame. Breve overview sulla blockchain e la sua integrazione nel caso di studio.

- **Capitolo 3:** valutazione della robustezza della soluzione prospettata attraverso l'analisi delle minacce presenti sulla piattaforma MISP.
- **Capitolo 4:** la conclusione della tesi, con le osservazioni finali e le prospettive future.

Ringraziamenti

Mi è doveroso dedicare questo spazio per ringraziare tutte le persone che, a vario titolo, mi hanno supportato nella realizzazione di questa tesi e nella mia crescita universitaria e personale.

Per prima cosa ringrazio il mio relatore Guido Perboli per i suoi consigli e per la disponibilità. Un sentito ringraziamento va anche a Vittorio Capocasale che mi ha guidato, con grande pazienza, nella stesura dell'elaborato.

Ringrazio la mia famiglia che non ha fatto mai mancare il suo supporto durante il mio percorso universitario e personale.

Ringrazio tutti gli amici di Potenza e in particolare Peppe e Giulio perchè fin dall'adolescenza sono stati la spalla ideale per affrontare la vita.

Un enorme ringraziamento va agli amici conosciuti a Torino.

In primis ringrazio Matteo e Peppe con i quali ho condiviso tutti i principali momenti della mia vita torinese. Ringrazio la vecchia roccia Andrea per i momenti di svago passati assieme e per la sua estrema puntualità nella consegna dei regali. Ringrazio Alessia ed Erica per essere costantemente una fonte d'ispirazione nell'affrontare con positività e maturità i momenti più bui. Ringrazio Federica perchè la sua leggerezza è un elemento indispensabile delle mie serate torinesi.

Ringrazio tutte le persone che, seppur marginalmente, sono entrate in contatto con me. Perché in fondo avete contribuito, in modo diverso, a farmi diventare ciò che sono oggi.

Indice

Elenco delle tabelle

Elenco delle figure

Capitolo 1

Introduzione generale

1.1 Principi generali

Negli ultimi dieci anni la gestione della supply chain, e cioè del flusso che dall'approvvigionamento di materiali permette di trasferire il prodotto finale al cliente, ha subito delle modifiche sostanziali.

La geografia della supply chain oggi è molto più complessa in quanto il numero di attori coinvolti è maggiore e questo perché progressivamente il concetto di integrazione verticale è diventato un vecchio paradigma. Le aziende oggi non realizzano più la maggior parte dei loro prodotti da sole, ma tendono per una serie di motivi (e.g. costi operativi inferiori, flessibilità operativa, risorse non disponibili internamente) all'outsourcing. Il trasferimento quindi di attività operative a soggetti esterni ha reso la supply chain globalmente più estesa e con un numero di attori coinvolti maggiore.

In questo contesto è evidente la necessità di gestire i rapporti tra le parti tipicamente attraverso i contratti, al fine di avere un'ottimizzazione dell'intera catena e non solo localmente. Tutto ciò però comporta una serie di costi aggiuntivi (e.g. contrattuali e operativi), oltre al rischio di comportamenti opportunistici delle parti, soprattutto in presenza di mercati dominati da pochi attori dove le long-lasting relationship sono necessità.

A questo bisogna aggiungere il fatto che la presenza di più aziende all'interno della catena rende necessaria la condivisione delle informazioni lungo tutti i nodi. Tipicamente però ogni compagnia gestisce i propri dati internamente, sul proprio sistema informativo e questo va a scapito sia dell'ottimizzazione della catena sia della possibilità di assegnare le responsabilità in caso di errori.

Una soluzione per far fronte ai problemi appena citati può essere rappresentata dalla tecnologia blockchain, che sempre maggiormente sta prendendo piede anche in questo settore.

Nella presente tesi verrà proprio valutata la robustezza dell'implementazione della blockchain all'interno di una supply chain di batterie per veicoli elettrici, in quello che è uno use

case definito. La valutazione verrà fatta a livello qualitativo, considerando quali attacchi di natura informatica la tecnologia risolve efficacemente e a quali è maggiormente esposta. Sulla base della gravità delle minacce residue si andrà a determinare se la soluzione prospettata rappresenta un miglioramento rispetto a quella attuale oppure no.

La base di partenza per questa analisi è stata la piattaforma MISP. Si tratta di un software progettato per la raccolta e la condivisione di attacchi informatici utilizzato sempre maggiormente dalle aziende e dalla pubblica amministrazione. Le minacce di rischio maggiore e alle quali la blockchain è passibile di attacco sono state estratte dal database della piattaforma. In seguito, sono stati considerati brevemente anche gli attacchi non rilevati sul MISP, ma che in qualche modo possono minare la validità della soluzione proposta.

La presente tesi è stata organizzata come segue:

- **Capitolo 1**: introduzione alla tesi e background teorico sulla piattaforma MISP. In particolare, overview sulle sue principali features, il suo funzionamento e le piattaforme alternative presenti oggi.
- **Capitolo 2**: descrizione della supply chain presa in esame. Breve overview sulla blockchain e la sua integrazione nel caso di studio.
- **Capitolo 3**: valutazione della robustezza della soluzione prospettata attraverso l'analisi delle minacce presenti sulla piattaforma MISP.
- **Capitolo 4**: la conclusione della tesi, con le osservazioni finali e le prospettive future.

1.2 Piattaforma MISP

Il Malware Information Sharing Platform (MISP) è una piattaforma per la raccolta, l'archiviazione, la distribuzione e la condivisione di indicatori di attacchi mirati, ma anche di informazioni su minacce, frodi finanziarie, vulnerabilità e persino informazioni antiterrorismo.

Questa piattaforma nasce dalla presa di coscienza che i cyber-attacchi hanno dinamiche e origini simili, al punto che condividerne gli schemi e le informazioni aiuta a combatterli. Tali informazioni, nel ramo della sicurezza informatica, sono principalmente raccolte sotto forma di Indicators of Compromise (IoC), ossia dati che indicano in qualche modo la presenza di un attacco o di una minaccia. Ci si rese ben presto conto dell'elevata numerosità di tali indicatori e della conseguente necessità di raccoglierli in una piattaforma unificata in modo da poterli consultare e aggiornare agevolmente. Su un'idea dell'informatico belga Christophe Vandeplas nacque, circa un decennio fa, il progetto MISP. Il lavoro di Vandeplas partì dalla fragilità che caratterizzava i metodi di condivisione delle informazioni in materia di cyber-security e ottenne l'approvazione dell'esercito belga prima e della NATO poi, che decise di impiegare suoi sviluppatori al potenziamento della piattaforma.[1]

A partire dal 2013 il MISP è diventato uno strumento fondamentale nell'ambito delle minacce informatiche e attualmente è finanziato dall'Unione Europea e dal Computer Incident Response Center Luxembourg (CIRCL). La robustezza della piattaforma ha fatto si che il suo utilizzo si estendesse a molteplici settori, tra cui quello finanziario. Infatti, a febbraio 2020 è stato siglato l'accordo "Cyber Information and Intelligence Sharing Initiative" (CIISI-EU) che vede coinvolti, tra gli altri, la Banca centrale europea e l'Europol. L'iniziativa prevede l'utilizzo della piattaforma MISP per la condivisione dei dati, con l'obiettivo di proteggere le informazioni di natura finanziaria.[1]

Il crescente utilizzo del MISP è imputabile sia alla peculiarità della piattaforma di esser totalmente open source (accessibile quindi pubblicamente) sia alla possibilità di gestire qualsiasi tipo di IoC. Ciò permette di avere una visione esaustiva delle minacce per poter così reagire in modo tempestivo ed efficace.

Un ulteriore punto di forza della piattaforma è rappresentato da un insieme di funzioni che agevolano la condivisione e l'esportazione dei dati attraverso molteplici opzioni come CSV, XML, JSON e testo puro.

1.2.1 MISP features

Dopo aver brevemente inquadrato le esigenze che hanno portato alla nascita del MISP e i principali motivi della sua affermazione nel mondo della cyber-security, è opportuno evidenziare le caratteristiche peculiari della piattaforma.

Le sue principali features sono elencate e descritte brevemente di seguito[2]:

- **Database di IoC:** la piattaforma permette l'archiviazione di indicatori tecnici e informativi relativi a campioni di malware e attacchi.
- **Correlazione automatica:** la piattaforma è dotata di un motore di correlazione per individuare in modo automatico le relazioni tra gli attacchi.
- **Condivisione:** la piattaforma offre funzionalità di filtraggio per consentire alle organizzazioni di indicare la visibilità e la distribuzione di ogni evento che inseriscono.
- **Interfaccia intuitiva:** la piattaforma consente agli utenti finali di creare e aggiornare eventi. Inoltre sono messe a disposizione funzionalità di filtraggio avanzate e una funzionalità di grafico degli eventi.
- **Esportazione:** la piattaforma offre molteplici modalità con cui esportare gli eventi tra cui i formati CSV, JSON (per l'integrazione con altri sistemi) e il testo semplice.
- **Importazione:** la piattaforma offre molteplici modalità con cui importare gli eventi tra cui quella multipla (batch-import), a testo libero e in formato CSV.
- **Tassonomia:** la piattaforma fornisce un set predefinito di schemi di classificazione degli eventi oltre a garantire la possibilità di etichettare gli eventi secondo i propri schemi.

- **MISP galaxy:** la piattaforma offre vocabolari di threat intelligence in cui vengono riportati gli autori degli attacchi e le minacce esistenti.

- **MISP Object:** la piattaforma fornisce degli oggetti di supporto che permettono di raggruppare attributi correlati, descrivendo le relazioni che intercorrono tra i dati di una minaccia.

Infine, occorre precisare che tassonomia, galaxy e object saranno oggetto di un approfondimento ulteriore nella sezione successiva. Questo è necessario in virtù della loro importanza in relazione alla creazione degli eventi e alla loro analisi.

1.2.2 Tassonomie MISP

Oltre al formato principale, la piattaforma mette a disposizione le tassonomie MISP. Si tratta di una feature che permette di classificare in modo efficiente eventi e attributi all'interno di un insieme di istanze MISP. Nella prima versione della piattaforma, l'etichettatura (tagging) era solamente locale, ma ci si rese conto che, per essere efficace, doveva essere utilizzata a livello globale. Dopo aver esplorato diverse soluzioni, venne costruito un nuovo schema che utilizzava il concetto di tag machine[3]. Si tratta di un tag espresso in modo tale da permettere ai sistemi di analizzarlo e interpretarlo. Il suo formato fu introdotto nel 2004 e di seguito possiamo visualizzare un esempio:

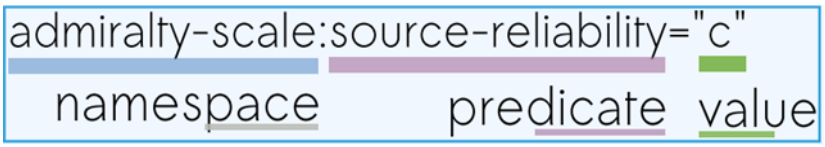

Figura 1.1. Esempio di tag machine (Fonte:[3])

Quando si utilizza la piattaforma MISP, le tassonomie sono disponibili liberamente e possono essere utilizzate in base alle regole della comunità. Inoltre possono essere consultate tramite il sito web e scaricabili in formato PDF o tramite il software MISP.

Di seguito vengono riportate alcune delle tassonomie esistenti messe a disposizione dalla piattaforma e appartenenti ad una lunga lista open source consultabile dalle organizzazioni[4]:

- **Open Source INTelligence (OSINT):** classificazione basata sulle fonti pubbliche, liberamente accessibili a chiunque.

- **Traffic Light Protocol (TLP):** tassonomia nata per facilitare il processo di condivisione delle informazioni sensibili e garantire una collaborazione più efficace tra le organizzazioni. TLP è un insieme di etichette standard utilizzate per definire i limiti alla condivisione che i destinatari delle informazioni devono applicare. Le etichette vengono elencate e descritte brevemente di seguito:

  - Red: etichetta utilizzata quando le informazioni non possono essere consultate senza rischi significativi per la privacy, la reputazione o le operazioni delle organizzazioni coinvolte. I destinatari quindi non possono quindi condividere le informazioni con nessun altro.
  - Amber: etichetta utilizzata quando è possibile condividere le informazioni con i membri della propria organizzazione, ma solo in caso di necessità. Infatti la divulgazione di questo tipo di dati, al di fuori delle comunità coinvolte, comporta rischi per la privacy e per la reputazione.
  - Green: etichetta utilizzata quando le informazioni non possono essere condivise al di fuori della comunità. In questo caso i destinatari delle informazioni non possono utilizzare canali pubblici, in quanto la condivisione è limitata alle organizzazioni partner presenti nella loro comunità.
  - White: etichetta utilizzata quando le informazioni comportano un rischio minimo o nullo di uso improprio. In questo caso quindi la divulgazione non è limitata.
  - Clear: etichetta utilizzata quando non ci sono limiti alla divulgazione. Conseguentemente, i destinatari possono diffondere le informazioni in tutto il mondo.

  In alcuni casi le informazioni possono essere estese con un tag specifico chiamato Chatham House Rule (CHR). Se il mittente decide di inserire questo tag aggiuntivo, la fonte dell'informazione non deve essere divulgata.

- **Pandemic:** si tratta di una particolare classificazione nata a seguito della diffusione della pandemia di Covid-19. Questa tassonomia include diversi tag; i principali vengono proposti di seguito:

  - Health: tag utilizzato per informazioni sul covid-19 e relative alla salute.
  - Cyber: tag legato alla combinazione Covid-19 e cybersecurity.
  - Disinformation: tag relativo ai fenomeni di disinformazione sulla pandemia.
  - Geostrategy: tag che mette in relazione le informazioni su COVID-19 con la geopolitica.

  Altre tassonomie esistenti che possiamo citare sono:

- **CIRCL taxonomy:** si tratta di una classificazione elaborata dal CIRCL e relativa al rilevamento degli incidenti e alle contromisure da adottare.
- **NATO classification markings:** relativo alle informazioni classificate NATO.
- **EUCI:** relativo alle informazioni classificate UE.

1.2.3 MISP galaxy

I MISP Galaxy rappresentano uno strumento essenziale per condivisione di attori, malware e dei Paesi obiettivo degli attacchi. Bisogna ricordare che la piattaforma nacque con l'obiettivo primario di condividere indicatori per lo più tecnici e nel corso del tempo divenne sempre crescente l'esigenza di avere un modo per descrivere attori, tools e caratteristiche comuni. Le tassonomie sono essenziali per la classificazione degli eventi, ma hanno il limite di essere poco descrittive, non consentendo quindi di collegare strutture più complesse ai dati. In questo contesto nasce il concetto di Galaxy, concepito come un semplice metodo per esprimere un oggetto di grandi dimensioni (cluster), composto da più elementi e che può essere allegato a eventi MISP o suoi attributi[5]. La piattaforma mette a disposizione, attraverso GitHub, Galaxy – cluster predefiniti. GitHub è sostanzialmente un servizio di hosting per progetti software in cui gli sviluppatori caricano il codice sorgente dei loro programmi e lo rendono scaricabile dagli utenti.

Riportiamo a titolo di esempio alcuni galaxy disponibili sulla piattaforma[6]:

- **Android:** si riferisce a malware per android. Tra questi possiamo citare:
  - RedAlert2: si tratta di un trojan che si nasconde finché l'utente non apre un'applicazione bancaria o di social media. Quando ciò accade, il trojan mostra all'utente un falso messaggio di errore, chiedendogli di effettuare nuovamente l'autenticazione. Red Alert raccoglie quindi le credenziali dell'utente e le invia al proprio server.
  - DoubleLocker: malware in grado di cambiare il PIN del dispositivo, impedendo l'accesso al proprio apparecchio. In seguito cripta i dati richiedendo un riscatto. Dopo essere stato installato, utilizza in modo improprio i servizi di accessibilità spacciandosi per Adobe Flash Player.
  - Andr/Dropr-FH: malware in grado di modificare file, registrare silenziosamente audio e video, monitorare testi e chiamate.

- **Target Information:** cluster galaxy che rappresenta una descrizione degli obiettivi dei threat actors. In questo caso viene riportato il paese geografico obiettivo dell'attacco.

- **Threat Actor**: cluster galaxy di gruppi noti o stimati che prendono di mira organizzazioni e dipendenti. Alcuni dei principali gruppi hacker sono riportati di seguito:
  - Codoso: gruppo di hacker che nel corso degli anni ha violato banche, studi legali e aziende tecnologiche.
  - Foxy Panda: gruppo che prende di mira le organizzazioni di telecomunicazioni e tecnologia.
  - Wekby: un gruppo attivo da diversi anni che prende di mira vari settori come la sanità, le telecomunicazioni, l'aerospaziale, la difesa e l'alta tecnologia.

1.2.4 MISP Objects

All'interno della piattaforma, uno strumento semplice ma potente per descrivere i dati è rappresentato dagli attributi. In MISP gli attributi possono essere indicatori di diversa natura e sono caratterizzati da un tipo, che indica il modo in cui viene descritto un attributo, e da una categoria che colloca l'attributo in un contesto. In questa ottica ci si rese conto della necessità di creare combinazioni avanzate di attributi[7]. Per far fronte a quest'esigenza sono stati definiti i MISP Objects, che aiutano gli analisti a descrivere le relazioni esistenti tra i dati di un evento. Per mantenere uniformità, gli objects sono descritti all'interno di un apposito template che utilizza il formato JSON. Il template contiene i seguenti elementi[8]:

- **Name:** rappresenta il nome dell'oggetto.
- **Meta-category:** è la categoria in cui rientra l'oggetto (e.g. file, rete, finanza...).
- **Description:** è un resoconto sintetico dell'oggetto.
- **Required:** è un array contenente gli attributi minimi per descrivere l'oggetto.
- **Version:** rappresenta il numero della versione e va incrementato ogni qual volta viene aggiornato l'object template.

Nella figura seguente si può notare quello che è un esempio di object template:

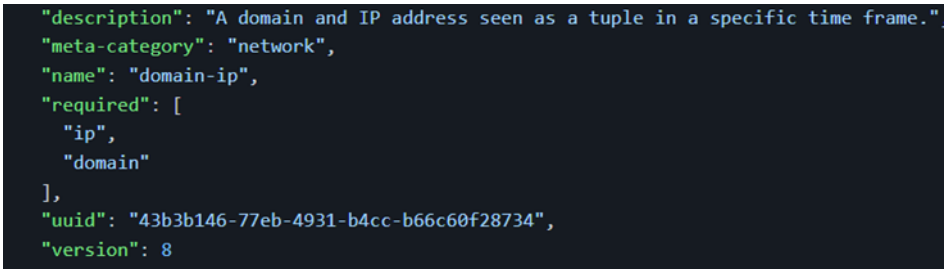

Figura 1.2. Esempio di un Object Template (Fonte:[8])

Infine, è opportuno elencare quelli che sono i principali objects presenti e disponibili sulla piattaforma[8]:

- **Bank-account:** si tratta di un object che descrive le informazioni relative a conti bancari.
- **File:** si tratta di un object generico che descrive un file.
- **Vulnerability:** si tratta di un object relativo a vulnerabilità per software, hardware o apparecchiature.
- **AIL-leak:** si tratta di un object che fa riferimento a fughe di informazioni.

1.2.5 Funzionamento generale della piattaforma

Una volta aver definito le main features della piattaforma, è fondamentale capire quello che è il funzionamento generale del MISP[9].

La piattaforma si compone di un'istanza centrale con cui i membri della rete possono interfacciarsi. Le modalità di accesso sono molteplici: dalla connessione con il proprio software tramite le interfacce fornite dal MISP, all'accesso diretto via browser. Le organizzazioni poi possono decidere di interagire attivamente, registrando gli eventi e condividendo i loro IoC, oppure semplicemente consultando le informazioni presenti. Il continuo aggiornamento dei dati è essenziale per le operazioni dei nodi della rete. Per questo motivo il MISP dispone di un sistema di notifiche che, tramite alert inviati ai membri della community, comunica la disponibilità di nuove informazioni.

Il MISP inoltre si serve di un provider di cyber threat intelligence come strumento di supporto. Questo provider ha accesso alla piattaforma e, sulla base dei dati presenti, effettua analisi sulle minacce e genera dei report. Attraverso questa integrazione, il database si arricchisce di dati e fornisce agli utenti un'esperienza più completa.

Le funzionalità descritte sono sintetizzate nella figura proposta di seguito:

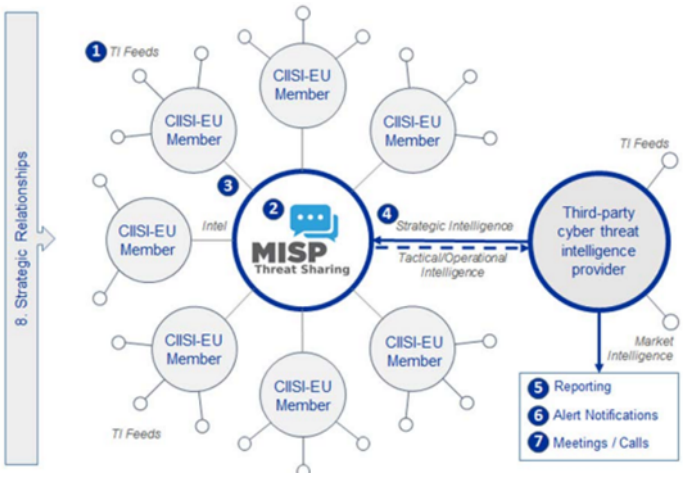

Figura 1.3. Funzionamento della piattaforma MISP (Fonte: Euro Cyber Resilience Board)

Abbiamo visto in sintesi quella che è l'architettura del MISP, ora ci occupiamo di cosa viene condiviso sulla piattaforma e di come avviene la stessa. Per quanto riguarda la prima, chiaramente gli oggetti della condivisione dipendono dal settore in cui opera ciascuna organizzazione che va a segnalare la minaccia. È naturale pensare che società finanziarie saranno interessate a minacce nel settore bancario mentre aziende di telefonia saranno maggiormente concentrate ad attacchi relativi al mondo delle telecomunicazioni.

Per quanto concerne le modalità di sharing è stato già evidenziato come la piattaforma metta a disposizione tassonomie, formato dati e protocolli per garantire una condivisione dei dati comune tra le varie organizzazioni.

1.2.6 Creazione di un evento

A questo punto della trattazione, è diventato evidente che il funzionamento della piattaforma gravita attorno alla creazione e alle condivisione degli eventi. In questa sezione viene mostrata la modalità di inserimento di una minaccia all'interno del MISP e il significato dei campi che il sistema richiede di valorizzare.

Cliccando sul pulsante *"Add Event"* all'interno della pagina principale della piattaforma, l'utente visualizza una schermata come quella proposta di seguito:

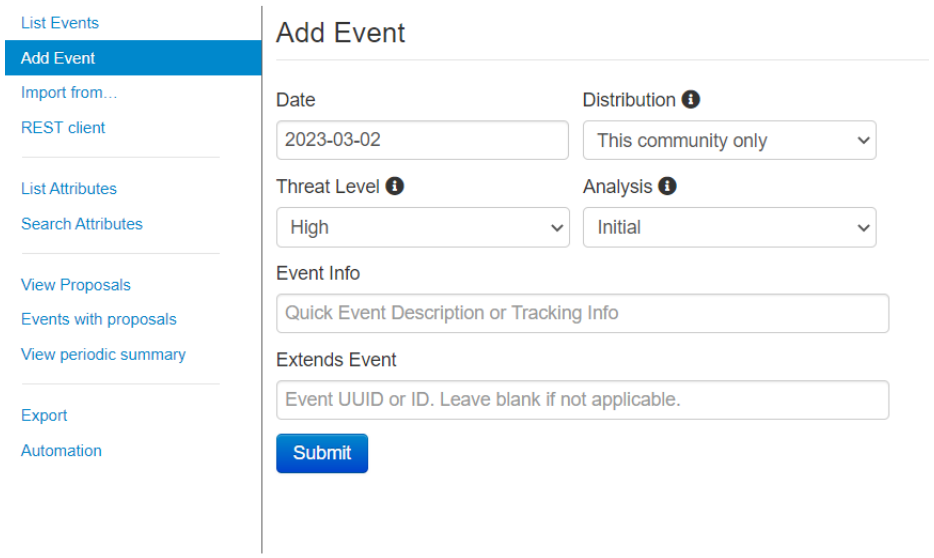

Figura 1.4. Schermata di creazione di un evento (Fonte: MISP Platform)

Dalla figura proposta, si nota come il sistema richieda di compilare una serie di campi per poter creare l'evento. In particolare, è necessario valorizzare[10]:

- **Date:** all'interno di questo campo viene inserita la data in cui è stato subito l'attacco.
- **Distribution:** è un campo che definisce il perimetro di condivisione dell'evento che si vuol creare. E' possibile scegliere tra le seguenti alternative:
  - Your organisation only: in questo caso solo i membri appartenenti all'organizzazione che sta inserendo l'evento saranno autorizzati ad esaminarlo.
  - This community only: in questo caso la condivisione della minaccia è limitata alle sole organizzazioni presenti sulla piattaforma MISP.
  - Connected communites: la visibilità dell'evento è estesa anche alle organizzazioni direttamente connesse alla community.
  - All communities: l'evento può essere liberamente propagato da un server al successivo.

- **Threat Level:** all'interno di questo campo è necessario specificare il livello della minaccia secondo tre differenti categorie di rischio:
  - Low: viene selezionato in presenza di mass malware, caratterizzati da impatto basso.
  - Medium: viene selezionato quando si è in presenza di malware come gli Advanced Persistent Threat (APT). Si tratta di minacce avanzate portate avanti da avversari dotati di elevate competenze tecniche e cospicue risorse tecnologiche.
  - High: viene selezionato soprattutto per attacchi quali APT sofisticati e 0 day attack. In particolare questi ultimi sono minacce non note e sono così definite in quanto gli sviluppatori hanno zero giorni per risolvere il problema prima dell'attacco.
  - Undefined: viene selezionato quando il livello della minaccia è sconosciuto o non definibile.
- **Analysis:** in questo campo si va a indicare lo stato attuale dell'analisi dell'evento. Le tre opzioni disponibili sono le seguenti:
  - Initial: in questo caso l'evento è stato appena creato ed è allo stato iniziale dell'analisi.
  - Ongoing: indica che l'analisi è ancora in corso.
  - Completed: il creatore dell'evento considera l'analisi completata
- **Event info:** in questo campo si riporta una breve descrizione della minaccia.
- **Extends Event:** consente di creare eventi completi che estendono un evento esistente. Questo campo quindi si può riempire inserendo l'identificativo dell'evento estensione di quello principale.

Il secondo step dopo aver creato l'evento è quello di popolarlo con eventuali attributi e attachment. Questa operazione può essere effettuata importando gli attributi da un formato esterno oppure manualmente. Soffermandoci su quest'ultimo caso possiamo vedere di seguito come si presenta l'apposita finestra di definizione degli attributi.

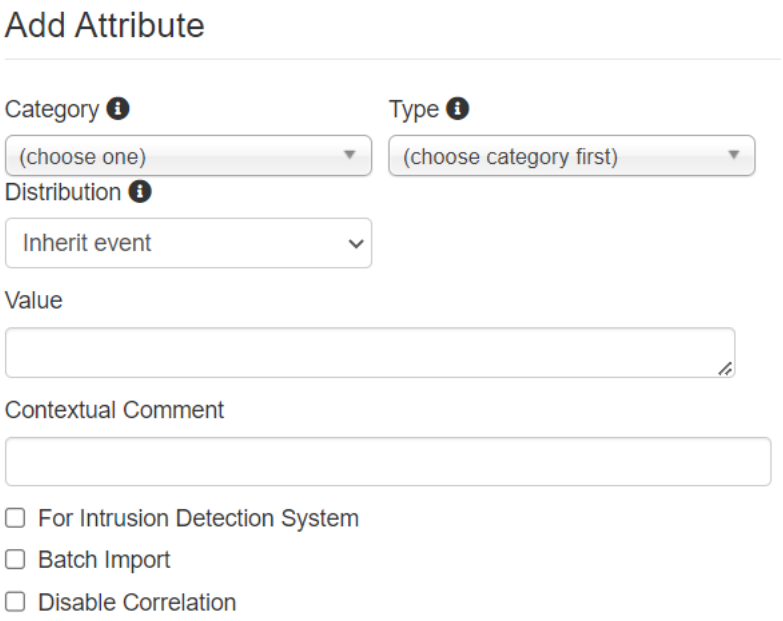

Figura 1.5. Inserimento degli attributi (Fonte: MISP Platform)

Dalla figura sopra mostrata si evince come la piattaforma richieda la compilazione di alcuni campi per poter aggiungere gli attributi all'evento. Di seguito viene descritto brevemente il loro significato[10]:

- **Category:** da un drop down menù è possibile indicare la categoria dell'attributo, ossia quale aspetto dell'evento è descritto dall'attributo corrente. Alcuni tipi di categorie selezionabili sono:
  - Financial fraud: è una categoria che fa riferimento ad indicatori relativi a frodi finanziarie.
  - Support tool: è una categoria che fa riferimento a strumenti di supporto all'analisi dell'evento.
  - Payload delivery: è una categoria che fa riferimento ad informazioni relative alla propagazione del malware.
- **Type:** da un drop down menù è possibile selezionare il mezzo con cui viene descritto un determinato aspetto dell'evento. Ad esempio, l'IBAN, il numero di conto corrente o il BIC sono tipi di attributo per la categoria Financial fraud.
- **Distribution:** esattamente come per gli eventi in questo elenco sarà possibile controllare chi potrà vedere l'attributo. Oltre ai livelli di distribuzione visti in fase di creazione dell'evento, è possibile selezionare la voce "Inherit event". In questo caso il livello di condivisione dell'attributo sarà lo stesso dell'evento al quale l'attributo è

associato. In presenza di più attributi si tiene conto dell'impostazione più restrittiva in termini di condivisione.

- **Value:** qui viene inserito il valore dell'attributo. Occorre precisare che i dati inseriti in questo campo devono essere coerenti con il tipo di attributo scelto.
- **Contextual Comment:** in questo campo è possibile inserire dei commenti relativi all'attributo ma puramente informativi.
- **Batch import:** opzione che consente di inserire più attributi dello stesso tipo.

Dopo aver confermato le scelte effettuate, l'evento può essere ulteriormente arricchito in base alle informazioni che si hanno a disposizione. In particolare, è possibile aggiungere un MISP Object selezionandolo da un drop down menù dedicato. Per ogni oggetto, posizionando il cursore del mouse sull'icona a lato dedicata, è possibile visualizzare una breve descrizione. Di seguito viene proposta la schermata relativa all'aggiunta di un object:

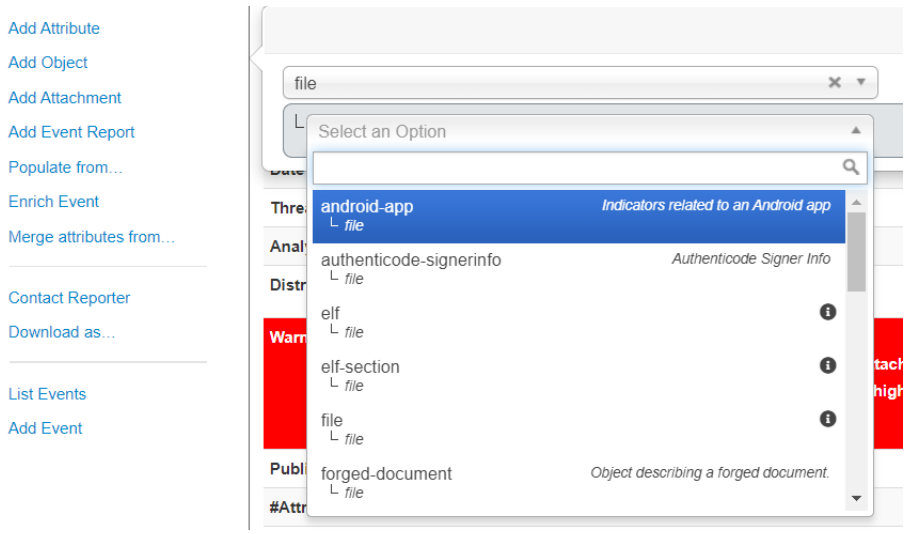

Figura 1.6. Inserimento di un Object (Fonte: MISP Platform)

L'evento può essere ulteriormente popolato importando IoC o caricando degli allegati come report di analisi. Quando tutte tutte le operazioni di arricchimento dell'evento sono terminate, è possibile pubblicare l'evento. A seguito di ciò, la piattaforma propaga l'evento sulla base del livello di distribuzione indicato in fase di creazione.

1.3 Piattaforme alternative: TIP ed HELK

Oltre al MISP, al momento, esistono altre due piattaforma utilizzate per la Cyber Threat Information Sharing. La prima di queste è la Threat Intelligence Platform (TIP). Si tratta di una piattaforma utilizzata principalmente per la condivisione delle informazioni e per l'analisi di dati interni ed esterni di un'organizzazione. A differenza del MISP, viene usata principalmente da società private per lo scambio di IoC e permette di importare dati anche in formati non strutturati (es. pdf, fogli di calcolo, e-mail)[11].

Nella figura seguente vengono inoltre evidenziate le differenti aree di copertura tra TIP e MISP nell'ambito del processo di Threat Intelligence:

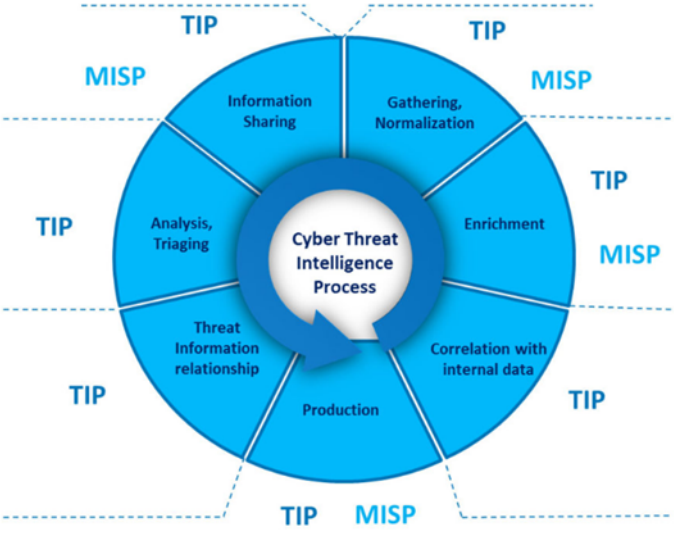

Figura 1.7. Aree di copertura MISP/TIP (Fonte:[11])

La seconda alternativa è rappresentata da uno strumento open source denominato The Hunting ELK (HELK).

HELK è una delle prime piattaforme di hunt, ossia di supporto alla ricerca di minacce all'interno dell'infrastruttura di rete prima che queste possono attaccare. HELK si serve, per raggiungere gli obiettivi di protezione e sicurezza, di strumenti come il linguaggio SQL, la creazione di grafici e l'apprendimento automatico. La piattaforma inoltre può fornire ulteriori informazioni sull'infrastruttura esistente e sulle difese di sicurezza necessarie.

Le principali features presenti sulla piattaforma HELK sono le seguenti[12]:

- **Kafka:** si tratta di un veloce sistema di messaggistica.
- **Elasticsearch:** si tratta di un motore di ricerca open source.
- **Logstash:** è un motore di raccolta dati con possibilità di esecuzione di istruzioni in tempo reale.
- **Kibana:** è una piattaforma open source di analisi e visualizzazione progettata per funzionare con Elasticsearch.
- **ES-Hadoop:** si tratta di una libreria open source indipendente e autonoma.
- **Quaderni Jupyter:** è un'applicazione web open-source che consente di creare e condividere documenti.

Capitolo 2

Caso di studio

2.1 Introduzione allo use case

Il principale obiettivo di questa tesi è quello di testare la robustezza della tecnologia blockchain nell'ambito di un case study già definito. In particolar modo tale caso d'uso pone l'attenzione su una Electric Vehicle (EV) Supply Chain, ispirata a quella di una automotive company.

Nelle sezioni seguenti, verrà descritta brevemente la parte di supply chain inerente alla produzione e al trasporto delle battery cells, e i relativi attori coinvolti. Inoltre, saranno elencati i principali problemi legati ad essa e che hanno portato alla definizione di una soluzione basata sulla blockchain.

Infine, attraverso la piattaforma MISP, si valuteranno quali attacchi (tra quelli di livello medio-alto) vengono superati dalla proposta ideata e quali non sono risolti, considerando quindi se il sistema implementato porta a un miglioramento rispetto alla situazione attuale.

2.1.1 Descrizione del processo

Nella descrizione dello use case in esame non vengono presi in considerazione le fasi di produzione e distribuzione dei veicoli elettrici, ma unicamente la gestione delle batterie elettriche, dalla fase di assemblaggio a quella di consegna delle stesse presso i concessionari. Di seguito, vengono riportati brevemente le fasi di processo[13]:

1. **Assemblaggio**: i moduli di ciascuna batteria vengono assemblati per formare un pacco batteria.
2. **Stoccaggio**: le batterie sono stoccate presso la warehouse del provider dei servizi di trasporto.
3. **Trasporto**: i battery packs vengono spediti presso l'impianto di montaggio della vettura.

4. **Assemblaggio e collaudo**: ciascun battery pack, una volta arrivato nella linea di produzione, viene assemblato e sottoposto a testing. In seguito, avviene l'attivazione della batteria e un ulteriore collaudo finale.

5. **Stoccaggio veicoli finiti**: dopo che il veicolo elettrico è stato caricato viene stoccato nell'area di parcheggio.

6. **Distribuzione veicoli finiti - 1° tappa**: il veicolo viene trasportato verso il porto dal quale partirà la spedizione verso il concessionario finale.

7. **Distribuzione veicoli finiti - 2° tappa** : una volta raggiunto il porto, il veicolo viene immagazzinato nell'attesa di esser imbarcato e vengono effettuate le operazioni portuali.

8. **Distribuzione veicoli finiti - 3° tappa**: il veicolo viene imbarcato sulla nave e spedito.

9. **Distribuzione veicoli finiti - 4° tappa**: il veicolo viene consegnato al concessionario e immagazzinato.

2.1.2 Attori coinvolti

Le fasi precedentemente descritte sono state elencate poiché in ciascuna di esse sono coinvolti diversi attori, che intervengono direttamente su quella che è la gestione delle batterie. Le operazioni che svolgono sono fondamentali per la nostra analisi, in quanto i problemi legati al loro tracciamento hanno portato alla soluzione blockchain-based. Di seguito vengono elencate, per ciascuna fase di processo, le attività effettuate sui battery packs[13]:

1. **Assemblaggio**: operatori dello stabilimento di assemblaggio ricaricano ciascun pacco batteria ad un livello di sicurezza.

2. **Stoccaggio**: gli operatori del centro di stoccaggio controllano che il livello di batteria rimanga in un range definito verificando che la temperatura dei pacchi non superi un valore soglia. In caso di situazioni anomale, possono intervenire ricaricando o isolando i pacchi.

3. **Trasporto**: questa fase vede coinvolti gli operatori nel monitoraggio delle batterie, come nella fase precedente.

4. **Assemblaggio e collaudo**: quando avviene il collaudo finale, gli operatori possono ricaricare i pacchi.

5. **Stoccaggio veicoli finiti**: in questa fase viene monitorata la carica del veicolo e, se necessario, viene ricaricato.

6. **Distribuzione veicoli finiti - 1° tappa**: se viene osservato un comportamento anomalo del veicolo e/o del pacco batteria, può intervenire direttamente l'operatore del provider di servizi logistici.

7. **Distribuzione veicoli finiti - 2° tappa** : questa fase vede coinvolto l'operatore nel medesimo modo della fase precedente.

8. **Distribuzione veicoli finiti - 3° tappa**: questa fase vede coinvolto l'operatore nel medesimo modo della fase precedente.

9. **Distribuzione veicoli finiti - 4° tappa**: in caso di anomalie in questo caso l'intervento viene effettuato direttamente dal concessionario o dall'operatore Autocare.

2.1.3 Limitazioni

Abbiamo visto nella sezione precedente che ci sono dei vincoli specifici per i vari processi che vanno ad impattare l'EV supply chain. Infatti, durante tutte le fasi è necessario monitorare costantemente i veicoli e i battery packs. Attraverso degli opportuni sensori, si vanno a rilevare parametri critici per quanto riguarda la qualità del trasporto come: temperatura, localizzazione e livello di vibrazione. Per la sicurezza degli operatori e l'utilizzabilità del veicolo invece va tenuto sotto controllo il livello di carica dei pacchi, evitando che scenda sotto un livello di guardia.

Abbiamo visto come il processo di monitoraggio coinvolga sia l'automotive company sia il provider dei servizi di trasporto, che intervengono sui battery packs in nodi distinti della catena logistica. Ciò fa sì che la raccolta e il tracciamento dei dati avvenga su sistemi informativi diversi, a seconda di quale tra le due parti ha effettuato la rilevazione e/o l'intervento. Questo rappresenta una delle principali limitazioni dell'EV supply chain che abbiamo preso in esame, in quanto è estremamente complesso ricostruire la catena di eventi che interessano una batteria. Infatti, nella situazione di sistemi informativi separati, non è possibile l'attribuzione delle responsabilità e ciascuna parte può pagare gli errori dell'altra, andando a compromettere la long term partnership.

Ulteriori limitazioni riguardano la sicurezza poiché è necessario garantire l'accesso ai sistemi aziendali a operatori fidati, ed evitare attacchi a stazioni di ricarica che possono compromettere l'integrità dei dati.

2.2 Soluzione blockchain based

L'introduzione della tecnologia blockchain nello use case appena descritto permette di ovviare alle limitazioni attuali del sistema analizzate nella sezione precedente.

Infatti, la soluzione prospettata consentirebbe di assegnare in modo univoco le responsabilità di ciascuna parte coinvolta collegando anomalie, batterie colpite, tempi e gli attori coinvolti. Inoltre, questo tracciamento decentralizzato delle informazioni permetterebbe di ridurre l'incertezza delle decisioni a carico dei partner e ne beneficerebbe la reputazione del marchio poiché, con maggiori dati a disposizione, sarebbe meno probabile che i veicoli tracciati necessitino di manutenzione[13].

In questa sezione verrà brevemente descritta la tecnologia blockchain e la sua implementazione nel caso di studio analizzato.

2.2.1 Tecnologia Blockchain

La blockchain è sostanzialmente un database strutturato come una catena di blocchi, ognuno dei quali contiene una serie di informazioni. La peculiarità di questo database (denominato ledger) è la sua decentralizzazione. Infatti, ogni membro di questo tipo di rete possiede una copia del ledger e su di essa ne ha il pieno controllo, ma lo stato globale del ledger è determinato dal contenuto della maggioranza delle copie e non è quindi modificabile da una qualche autorità centrale. Questa peculiarità distingue la blockchain dagli altri tipi di database ed è imputabile alla struttura di ogni blocco che è caratterizzato da tre elementi:

1. **Codice Hash**: si tratta di una rappresentazione alfanumerica di dati. È univoco e viene modificato se cambia anche uno solo dei dati relativi a quel blocco.
2. **Codice Hash del blocco precedente**: tale codice è necessario per mantenere l'ordine cronologico dei blocchi.
3. **Marca temporale**: è un riferimento temporale che individua il momento in cui il blocco è stato creato.

Figura 2.1. Struttura a blocchi della blockchain (Fonte: JavaBoss)

Appare evidente come il cambiamento di un blocco della catena porterebbe alla modifica del codice hash e della marca temporale di quel blocco. Come conseguenza anche il blocco successivo non avrebbe più come riferimento l'hash del blocco precedente e quindi si capirebbe immediatamente che la blockchain ha subito un'alterazione.

2.2.2 Byzantine Fault Tolerance e Meccanismi di consenso

Al di là di alcune eccezioni, abbiamo visto che la decentralizzazione è una peculiarità della tecnologia blockchain. In un sistema distribuito come questo, lo stato generale della blockchain è concordato periodicamente tra i membri del network. Chiaramente il consenso tra i partecipanti non è facile da raggiungere, specialmente se si tiene in conto

che alcuni nodi potrebbero fallire o agire in modo poco onesto. In questo contesto è opportuno introdurre il *Problema dei generali bizantini*.

Si tratta di un dilemma logico in cui ogni generale è a capo del proprio esercito e deve decidere se attaccare oppure ripiegare. La scelta tra le due opzioni non è rilevante, piuttosto l'obiettivo è che i generali concordino su una decisione comune. Il problema prevede inoltre che i generali possano comunicare tra loro e informare gli altri sulla scelta effettuata attraverso dei messaggeri; i messaggi possono però arrivare in ritardo, essere smarriti o piuttosto un generale potrebbe inviare una comunicazione falsa[14].

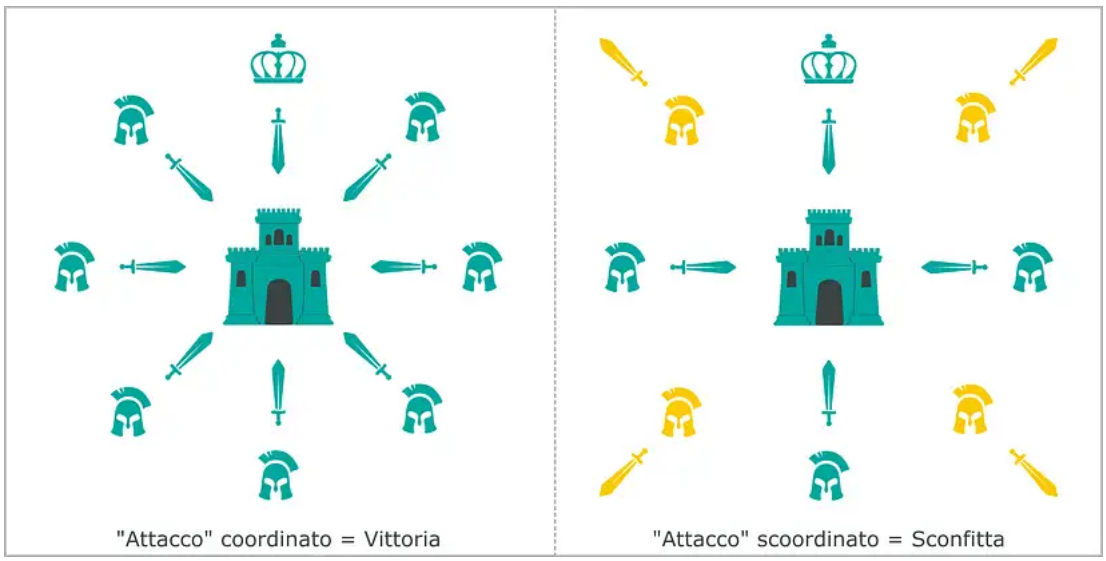

Figura 2.2. Problema dei generali bizantini

Nella tecnologia blockchain è evidente che i nodi rappresentano i generali e devono concordare sullo stato attuale del sistema; l'unico modo per poter concordare su una medesima scelta è necessario che almeno $\frac{2}{3}$ dei nodi siano onesti e affidabili.

La *Bizantine Fault Tolerance* (BFT) è proprio la capacità di un sistema di raggiungere il consenso tenendo conto che alcuni nodi potrebbero agire in modo dannoso. Tale capacità può essere raggiunta attraverso alcuni meccanismi denominati *algoritmi di consenso* di cui i più famosi sono la Proof of Work (POW) e la Proof of Stake (POS).

Il meccanismo POW è stato ideato e utilizzato per la prima volta per la blockchain Bitcoin e prevede dei quesiti matematici di varia difficoltà. La risoluzione di tali quesiti è deputata ai *miner* che sono appunto gli attori che partecipano alla creazione dei blocchi della catena. Nel momento in cui un miner ha individuato la soluzione al quesito la sottopone al resto della rete e, se più della metà della stessa la valida, viene creato il blocco. Un algoritmo di questo tipo richiede però un elevato calcolo computazione e tale limite ha portato poi all'ideazione del Proof of Stake. Nel POS non esistono i miner e i blocchi vengono convalidati dai cosiddetti *validator*. In questo meccanismo, la selezione dei

validator è legata alla quantità di valuta che ognuno di essi deposita nella rete blockchain. In genere più monete si bloccano, più è alta la probabilità di essere selezionati per la validazione dei blocchi. Con questo algoritmo il consumo energetico risulta essere molto basso; ma proprio per la quantità poco significativa delle risorse, le reti POS sono meno resistenti ad un eventuale attacco hacker.

Per il nostro use case, la rete blockchain creata utilizza un altro algoritmo di consenso, denominato IBFT 2.0[13]. Nelle reti IBFT 2.0 le transazioni e i blocchi sono approvati da validatori ed è necessaria una super maggioranza (maggiore o uguale a $\frac{2}{3}$) per inserire ogni blocco all'interno della catena. Inoltre in questo meccanismo di consenso i validatori esistenti propongono e votano per aggiungere o rimuovere validatori.

2.2.3 Oracles e Smart contracts

La tecnologia blockchain inoltre necessita quasi sempre della presenza degli *Oracles*. Si tratta di trusted third parties che forniscono alla tecnologia blockchain dati che, seppur non verificabili, non possono essere ottenuti in altro modo. Nel nostro use case gli oracles sono dei sensori che raccolgono gli onfield data; vanno cioè a rilevare i parametri critici delle batterie (temperatura, localizzazione, livello di vibrazione e carica)[13]. Con l'implementazione della tecnologia blockchain, le informazioni raccolte dai sensori durante le varie fasi del processo verrebbero memorizzate sulla blockchain stessa e rese disponibili a tutti i soggetti coinvolti.

Quando le parti si accordano sull'uso di tale tecnologia, si va a concordare il formato dei dati e come questi devono esser raccolti. A seguito di ciò, si procede alla definizione degli smart contracts.

Gli *smart contracts* sono dei programmi informatici che ciascun soggetto della rete esegue per poter aggiornare la propria copia del ledger. Nella soluzione prospettata sono usati solamente per controllare i permessi ed eseguire eventi[13] e, data la loro struttura, possono essere alterati solo in presenza di errori accidentali o intenzionali nell'ambito di esecuzioni indipendenti. Bisogna precisare che gli smart contracts di per sé non hanno valore legale ed è quindi necessario che le aziende si accordino, tipicamente attraverso i tradizionali contratti, per legittimarli.

2.2.4 Trilemma della blockchain

Occorre precisare che teoricamente ogni interazione all'interno della supply chain analizzata può essere basata su blockchain e smart contracts, a partire dalla richiesta delle celle al fornitore fino ad arrivare ai pagamenti. Nell'implementazione prospettata si è però deciso di tener traccia sulla blockchain solo delle info di tracking delle batterie e degli eventi negativi che potrebbero alterare la loro salute, questo a causa del cosiddetto *trilemma della scalabilità*[15].

Per spiegare meglio questo concetto, occorre tener presente che tre sono gli elementi desiderabili all'interno di una rete blockchain:

- **Decentralizzazione**: il controllo della rete è distribuito piuttosto che detenuto da una singola autorità centrale.
- **Sicurezza**: è necessario che una rete blockchain sia resistente alle minacce.
- **Scalabilità**: è un concetto legato alla capacità di gestire un numero sempre più elevato di transazioni senza che le prestazioni ne risultino inficiate.

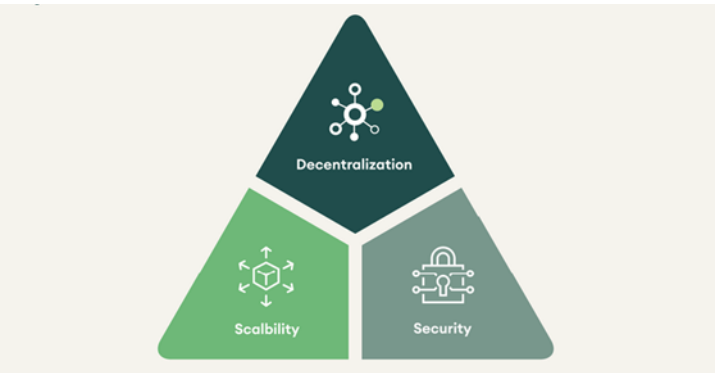

Figura 2.3. Trilemma della blockchain (Fonte: Business Insider India)

Il trilemma si riferisce al fatto che non è possibile per la rete blockchain raggiungere livelli ottimali di tutte e tre le caratteristiche contemporaneamente. Nel nostro caso aumentare la scalabilità porterebbe all'indebolimento di almeno una delle altre proprietà e questo spiega la quantità ridotta di dati che si è deciso di memorizzare sulla blockchain.

2.2.5 Framework Blockchain

Prima di entrare nel dettaglio della soluzione blockchain ideata per il caso d'uso trattato, è necessario descrivere brevemente i principali framework blockchain. Infatti per implementare una rete di questo tipo, è necessario velocizzare il processo di sviluppo, evitando di creare applicazioni da zero. I framework vengono incontro a questa esigenza in quanto sono piattaforme che fanno si che gli sviluppatori possano implementare i componenti specifici del software, a partire da moduli di base. Di seguito vengono elencati e brevemente descritti i principali framework blockchain presenti attualmente.

- **Hyperledger Fabric**: il progetto open source Hyperledger Fabric della Linux Foundation è il framework blockchain standard e modulare de facto per le piattaforme blockchain aziendali. L'architettura modulare aperta, che supporta lo sviluppo di applicazioni a livello aziendale e soluzioni industriali, utilizza componenti plug-and-play per un'ampia gamma di casi d'uso. Attraverso stringenti controlli sulla privacy, vengono resi visibili tra i partecipanti solo i dati che davvero si vuole condividere. Naturalmente tutto le transazioni sono tracciabili in modo da poter aumentare il

trusting tra le parti e i processi che si desidera automatizzare vengono documentati dagli smart contracts[16].

- **Hyperledger Sawtooth**: è una piattaforma blockchain aziendale per la creazione di applicazioni e reti di ledger distribuiti. Si caratterizza per un elevata modularità e per la capacità di semplificazione dello sviluppo delle applicazioni. Infatti, gli sviluppatori possono usare il linguaggio a propria scelta per definire le regole di business, senza dover conoscere il design del sistema centrale[17].
- **Hyperledger Besu**: si tratta di un client Ethereum Open Source, cioè una piattaforma per lo sviluppo e la distribuzione di progetti blockchain basati su Ethereum (piattaforma usata per la creazione e la pubblicazione degli smart contracts). Besu si caratterizza per la presenza dell'Ethereum Virtual Machine(EVM), ossia una macchina per l'esecuzione dei contratti intelligenti e per implementare vari tipi di algoritmi di consenso che sono coinvolti nella convalida delle transazioni, nella convalida dei blocchi e nella produzione degli stessi.
- **Quorum**: è una piattaforma blockchain privata creata nel 2016 presso JP Morgan Chase. Si tratta di una piattaforma che supporta transazioni pubbliche e private e permette la creazione di reti private protette; una funzionalità quest'ultima di grande importanza per la maggior parte delle aziende. Quorum si caratterizza per un'elevata velocità delle transazioni e per la privacy in quanto consente di controllare chi può accedere e visualizzare i dati.

Nel sistema blockchain scelto per il caso d'uso analizzato si è preferito il framework Hyperledger Besu. Ciò è stato dettato da un serie di fattori come la maggiore attivita della community di Besu su GitHub, essenziale per le tecnologie che devono essere usate nel lungo termine[13].

Inoltre come abbiamo appena visto Besu, essendo basato su Ethereum permette di sfruttare molti tools già sviluppati per la tecnologia Ethereum.

Capitolo 3

Analisi delle minacce e del loro impatto sul caso d'uso scelto

L'obiettivo del presente capitolo è quello di analizzare le minacce presenti sulla piattaforma MISP e il loro impatto sul caso d'uso scelto. Per prima cosa è stato individuato, a titolo di esempio, un evento registrato sul MISP, in modo da evidenziare i principali campi che lo compongono.

In seguito è stata effettuata un'estrazione degli eventi presenti sul database e conseguentemente una loro classificazione sulla base di varie dimensioni, per poter individuare i cluster più ricorrenti.

Infine sono state valutate, in relazione alla soluzione blockchain-based proposta, le minacce caratterizzate da un impatto medio - alto. A fronte di tali rischi è stata messa in luce la risposta della tecnologia blockchain, al fine di determinare se l'adozione della stessa all'interno della supply chain scelta potesse rappresentare un miglioramento rispetto allo stato attuale.

Nella sezione finale del capitolo è stata fornita una breve descrizione di quegli attacchi che, seppur non presenti sulla piattaforma, potessero avere un impatto rilevante in relazione all'implementazione proposta.

3.1 Analisi di un generico evento presente sul MISP

A titolo di esempio è stato individuato un evento tra quelli presenti nella lista della piattaforma MISP. Nel caso specifico, la minaccia presa in esame rientra in una famiglia di malware definita Tofsee. Si tratta di un modular spambot, ossia di un modulo usato principalmente per inviare spam tipicamente attraverso la diffusione di messaggi clickbait sui social network. Di seguito viene proposta la schermata dell'evento che appare sulla piattaforma MISP:

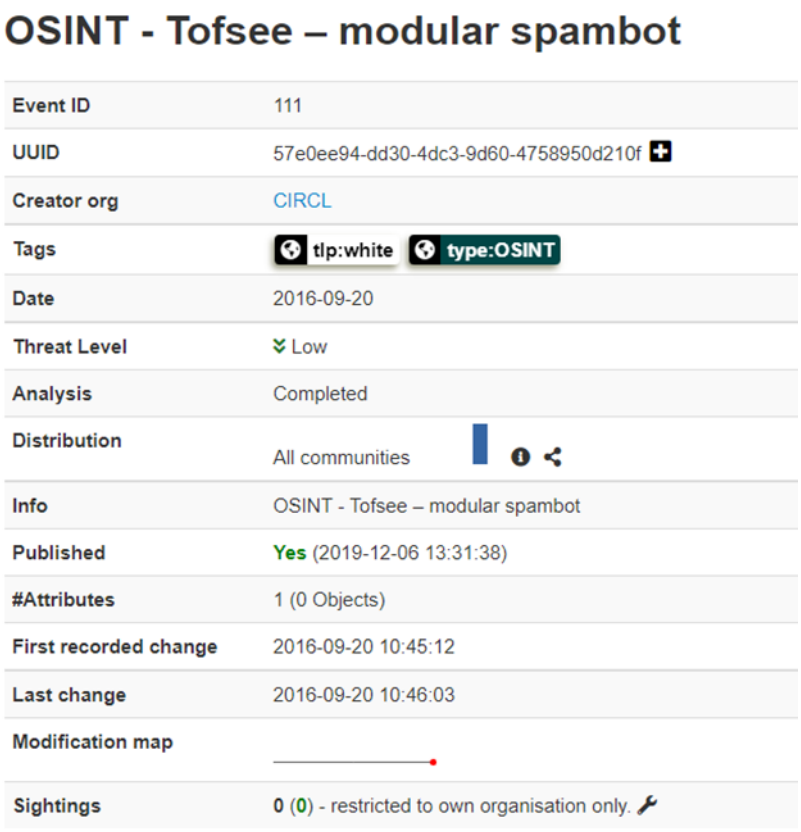

Figura 3.1. Esempio di un evento presente sulla piattaforma MISP (Fonte: MISP Platform)

La figura mostra come ciascun evento registrato sul database MISP sia caratterizzato da una serie di campi e attributi su cui è opportuno soffermarsi brevemente.

Per una visualizzazione più completa dell'evento è stata utilizzata la funzione "Download as" che ci permette di esportare l'evento in diversi formati e tra quelli proposti è stato selezionato il JavaScript Object Notation (JSON) che risulta essere il più semplice e il più pratico. Si tratta di un formato testuale per la strutturazione dei dati utilizzato per lo scambio di informazioni tra applicazioni client e server.

Di seguito è mostrato il JSON per l'evento d'esempio scelto:

Figura 3.2. JSON dell'evento mostrato in Figura 3.1

Nella porzione di codice presente in figura possiamo notare quelle che sono le principali caratteristiche dell'evento. Innanzitutto è presente l'ID dell'evento, l'identificativo dell'organizzazione creatrice dell'evento (rappresentato dal campo orgc_id) e il valore che identifica l'organizzazione che ha generato l'evento (rappresentato dal campo org_id).

In seguito, vengono riportate brevemente le info sulla minaccia e in questo caso si può notare la dicitura OSINT che rientra nelle tassonomie MISP. Si è già visto che la classificazione OSINT si riferisce alle attività volte alla ricerca ed all'acquisizione di informazioni tramite le cosiddette "fonti aperte", quindi fonti liberamente accessibili a chiunque.

Il valore booleano true posseduto dalla proprietà dell'evento "published" segnala che l'evento è stato pubblicato. La proprietà "attribute_count" invece esplica il numero di attributi relativamente a tale evento e nel caso preso in esame è presente un solo attributo.

Inoltre si può notare come il livello di minaccia, lo stato attuale dell'analisi e il livello di condivisione dell'evento vengono espressi tramiti valori numerici che codificano quelle che sono gli elenchi di opzioni già visti in fase di creazione di un evento. Per il "threat_level_id" il valore 1 indica minaccia alta, il 2 minaccia media, 3 minaccia bassa e 4 minaccia undefined. Nel nostro caso il livello della minaccia è Low.

Per quanto riguarda la proprietà analysis il valore 2 indentifica il fatto che il creatore dell'evento considera l'analisi completata. Infatti, il valore 0 viene utilizzato per uno stato di analisi iniziale, mentre il valore 1 per analisi ancora in corso. Infine, il campo distribution; in questo caso la numerazione va dallo 0 (condivisione dell'evento riservata solo ai membri dell'organizzazione) al 5 (inherit event). Il valore 3 assegnato indica che la condivisione è estesa a tutte le communities. Il campo sharing_group_id risulta essere settato a 0 in quanto assume un valore diverso da questo solo se per la proprietà distribution è stato settato il valore 4 che va proprio a definire un livello di condivisione dell'evento

limitato a organizzazioni definite nello sharing group. Notiamo poi due ulteriori proprietà dell'evento: timestamp e publish_timestamp che si riferiscono a quando l'evento è stato rispettivamente creato e pubblicato. Entrambe le proprietà hanno come valore stringhe numeriche, in quanto vengono espresse in secondi trascorsi da una data convenzionale conosciuta come Unix Epoch e corrispondente al 1° gennaio 1970. Infatti, nella figura iniziale viene riportato che l'evento è stato pubblicato in data 06/12/2019 alle 13:31:38 e corrisponde (partendo dal 1° gennaio 1970) a 1575635498 secondi che è proprio la stringa numerica riportata nel JSON.

Poiché non ci sono eventi completi che estendono l'evento principale, la proprietà extends_uuid risulta esser vuota. In caso contrario sarebbe stato presente l'identificativo dell'extends event. Infine, di particolare interesse è il valore false assegnato alla proprietà disable_correlation che sta ad indicare il fatto che la correlazione non è disabilitata. Ricordiamo che le correlazioni MISP sono un modo per trovare relazioni tra attributi e indicatori da malware o attacchi ed è un modo per indicare che un certo valore esiste in più di un evento.

L'analisi è ora estesa alla porzione di codice successiva che va a definire le proprietà (con i loro rispettivi valori) dell'organizzazione creatrice dell'evento e di quella che l'ha generato. Proponiamo di seguito il JSON corrispondente.

Figura 3.3. Organizzazioni legate all'evento mostrato in Figura 3.1

Si può notare come l'evento è stato generato da Telenor, multinazionale norvegese attiva nel settore delle telecomunicazioni e poi aggiunto sulla piattaforma MISP da CIRCL. Si tratta di un'organizzazione governativa progettata per raccogliere, esaminare, segnalare e rispondere a minacce e incidenti alla sicurezza informativa.

Di seguito invece viene proposto il JSON relativo agli attributi dell'evento scelto:

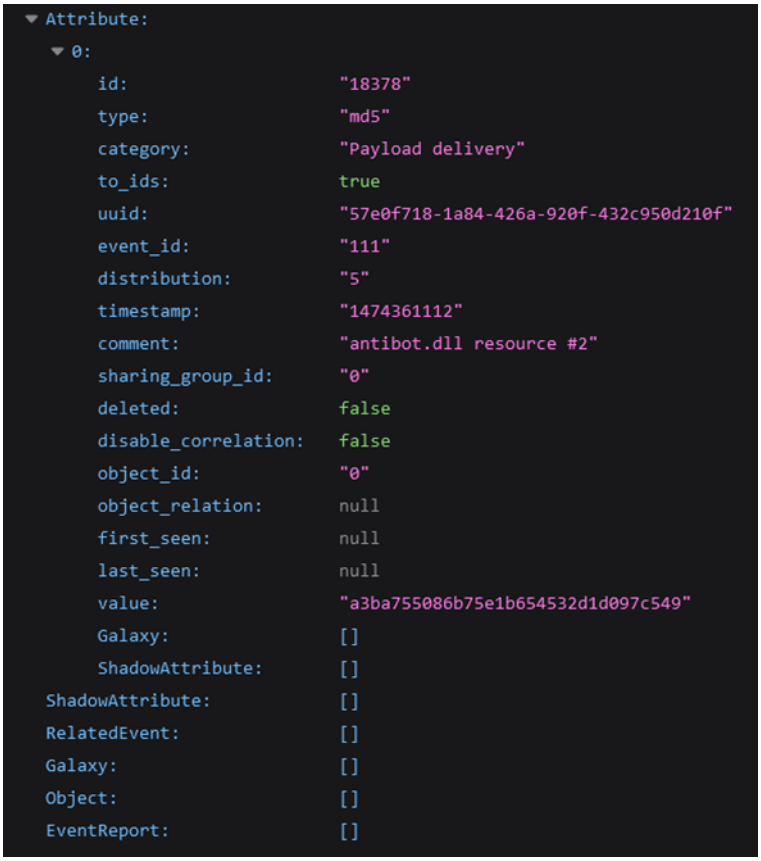

Figura 3.4. Attributi dell'evento mostrato in Figura 3.1

In figura è possibile notare le proprietà relative all'attributo e i corrispondenti valori assegnati. Emerge immediatamente che la minaccia è corredata da un solo attributo che rientra nella categoria payload delivery la quale fa riferimento al modo con cui il malware si propaga. Il type md5 ci chiarisce invece che la categoria precedente viene descritta attraverso il formato md5, mentre il value dell'attributo è l'hash md5 quindi una stringa che identifica univocamente il file.

Infine, abbiamo l'ultima parte di JSON riguardante i tag.

Nella fase iniziale di introduzione alla piattaforma, è stato evidenziato come il tag sia un metodo semplice per classificare un evento attraverso una semplice stringa. Oltre che sull'evento, i tag possono essere allegati anche agli attributi dello stesso, ma il miglior modo è quello di includere solo un tag specifico per gli attributi quando sono un'eccezione del tag settato per l'evento. Nel nostro caso abbiamo due tags relativi all'intero evento, come evidenziato dalla figura di seguito:

Figura 3.5. Tag dell'evento mostrato in Figura 3.1

Tra i subset di tags da usare per ogni evento troviamo il TLP che è proprio il primo tag del nostro evento in esame. In questo caso al campo "colour" è assegnato il valore "#ffffff" che corrisponde al colore white che indica, come già visto nella fase introduttiva, che le informazioni possono essere condivise pubblicamente in conformità con la legge. Infatti, il tlp di tipo white è utilizzato quando le informazioni comportano un rischio minimo o non prevedibile di uso improprio e ciò è in concordanza con il fatto che il livello di minaccia dell'evento è Low.

Per quanto riguarda il secondo tag è presente la tassonomia "type" che permette di descrivere diversi tipi di disciplina della raccolta delle informazioni. In questo caso, come visto all'inizio dell'analisi dell'evento, la raccolta delle info avviene da fonti aperte ed è per questo che è riportata la classificazione OSINT. Le principali altre tassonomie utilizzate per il tag "type" sono:

- **Sigint:** caratterizza i dati raccolti dall'intercettazione dei segnali.
- **Techint:** caratterizza i dati raccolti dall'analisi delle armi e degli equipaggiamenti utilizzati dalle forze armate.

- **Humint:** caratterizza i dati raccolti da un individuo fisico in un determinato luogo.
- **Medint:** caratterizza i dati raccolti da analisi di cartelle cliniche e/o esami fisiologici.
- **Imint:** caratterizza i dati raccolti da fotografie satellitare e aeree;
- **Finint**: caratterizza i dati raccolti dall'analisi di transazioni monetarie o finanziarie.

3.2 Interrogazione degli eventi attraverso il linguaggio JavaScript

Come è stato già detto, l'obiettivo primario di questa tesi è quello di individuare le minacce più rischiose presenti sulla piattaforma che possono in qualche modo minare l'integrazione blockchain-supply chain prospettata.

Per poter isolare le minacce di impatto maggiore è necessario avere a disposizione tutti gli eventi e i relativi attributi presenti sul MISP. La piattaforma mette a disposizione la possibilità di scaricare questi dati in diversi formati attraverso la funzione Export. Di seguito viene presentata la schermata con i vari formati disponibili per il download:

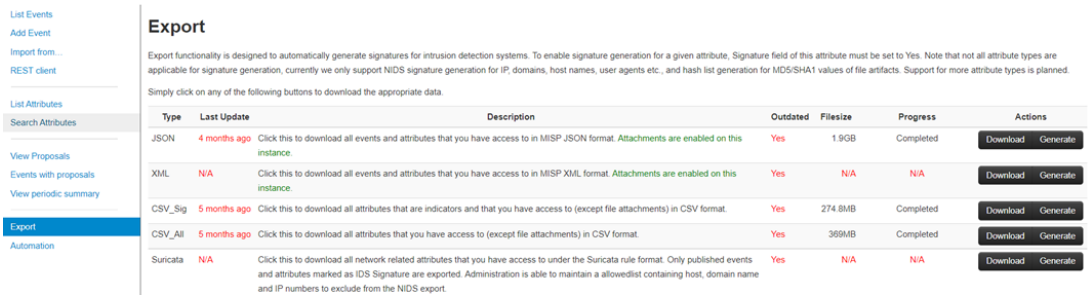

Figura 3.6. Funzione Export del MISP (Fonte: MISP Platform)

Per la nostra analisi è stato scelto il formato JSON. Come detto in precedenza, si tratta di un formato testuale utilizzato per lo scambio di dati comprensibile sia dall'essere umano sia dalla macchina che può interpretarlo senza difficoltà (quest' ultima operazione è definita parsing). Questo formato è caratterizzato da alcuni elementi di base:

- Proprietà: ogni proprietà possiede un nome e un valore che sono separati dal simbolo di due punti.
- Oggetto: è contenuto all'interno di una coppia di parentesi graffe ed è caratterizzato da un insieme di proprietà. Le proprietà di un oggetto sono separate da virgole.
- Array: è una sequenza di oggetti separati da virgole e racchiusa tra parentesi quadre. Gli oggetti spesso non sono caratterizzati dalla stessa struttura e questo rende il JSON estremamente flessibile.

Cliccando prima sul pulsante generate e poi su Download si ha a disposizione l'elenco degli eventi a cui è concesso l'accesso nel formato JSON. Nella miriade di eventi presenti, possiamo vedere di seguito un estratto (visualizzato su un JSON formatter) che permette di evidenziare immediatamente gli elementi caratteristici del formato che abbiamo appena descritto.


```
{
  "response":[
    {
      "Event":{
        "id":"2",
        "orgc_id":"3",
        "org_id":"2",
        "date":"2017-03-30",
        "threat_level_id":"3",
        "info":"OSINT - Carbon Paper: Peering into Turlaâ€™s second stage backdoor",
        "published":true,
        "uuid":"58dcfe62-ed84-4e5e-b293-4991950d210f",
        "attribute_count":"100",
        "analysis":"2",
        "timestamp":"1493403824",
        "distribution":"3",
        "proposal_email_lock":false,
        "locked":false,
        "publish_timestamp":"1569938882",
        "sharing_group_id":"0",
        "disable_correlation":false,
        "extends_uuid":"",
        "Org":{ },
        "Orgc":{ },
```


Figura 3.7. Estratto di JSON d'esempio

Il file JSON estratto comprende più di undicimila eventi ed oltre due milioni di attributi; molti di queste informazioni esulano da quello che è lo scopo della presente tesi e pertanto è necessario processare gli eventi ed effettuare una serie di classificazioni.

In tal senso si è reso indispensabile l'utilizzo di Javascript. Si tratta di un linguaggio di scripting, ossia di un linguaggio di programmazione per poter automatizzare dei compiti che altrimenti dovrebbero essere effettuati manualmente. L'idea di base è quella di usare tale linguaggio per poter interrogare il JSON e farci restituire le informazioni che di volta in volta si rendono necessarie per la nostra analisi. Di seguito viene presentato lo script realizzato, come vedremo successivamente, per sottosegmentare gli attacchi in base al loro livello di minaccia:

```
1  const fs = require('fs');
2
3
4  const JSONStream = require('JSONStream');
5  const getStream = () => {
6    const jsonData = "MISPevents.json";
7    const stream = fs.createReadStream(jsonData, { encoding: "utf8" });
8    const parser = JSONStream.parse(['response', true]);
9    return stream.pipe(parser)
10 };
11 main()
12
13 async function main() {
14    let tot=0;
15    const response=[]
16    getStream()
17    .on('data', function(data) {
18       if(tot==0){
19         console.log(data)
20         console.log(data.Event["threat_level_id"])
21       }
22       if (data.Event["threat_level_id"] ==1 || data.Event["threat_level_id"] ==2)
23       {
24                response.push(data)
25       }
26       tot++
27       })
28    .on("end", (err) => {
29      console.log("Events: "+response.length)
30      let out={response: response}
31      fs.writeFileSync('./threat.json', JSON.stringify(out))
32    })
33    .on("error", (err) => {
34      console.log(error)
35    });
36 }
```

Figura 3.8. Scripting per il livello di minaccia

L'idea di base in questo caso è quella di leggere il file scaricato in precedenza dal MISP con la funzione Export (rinominato MISPevents.json) e richiamare una funzione predefinita su ogni evento. Questa funzione deve memorizzare tutti gli eventi che rispettano una certa condizione (nel caso in figura un threatlevelid pari ad 1 o a 2 come si evince a partire dalla riga 22 del codice) e incrementare un contatore (tot++). Infine, vengono stampati su un file le statistiche finali (la riga di riferimento è la 31 e qui il file è stato nominato threat.json).

Per poter eseguire il codice Javascript appena mostrato ad ed avere così restituito in output il risultato della richiesta effettuata, è stato utilizzato Windows PowerShell. Si tratta si una shell, ossia di un programma che permette di interagire con il sistema attraverso un terminale e un'interfaccia Command Line (ossia l'interazione è possibile digitando comandi). Il metodo più veloce per avviarla è dato dai seguenti passaggi:

1. Vengono premuti sulla tastiera del computer i tasti **Windows** ed **R** contemporaneamente .
2. Si apre la finestra **Esegui** e nella casella Apri si digita **powershell**.
3. Si fa click su **OK**.

A questo punto si aprirà il Windows PowerShell e apparirà una schermata come quella mostrata nella figura seguente:

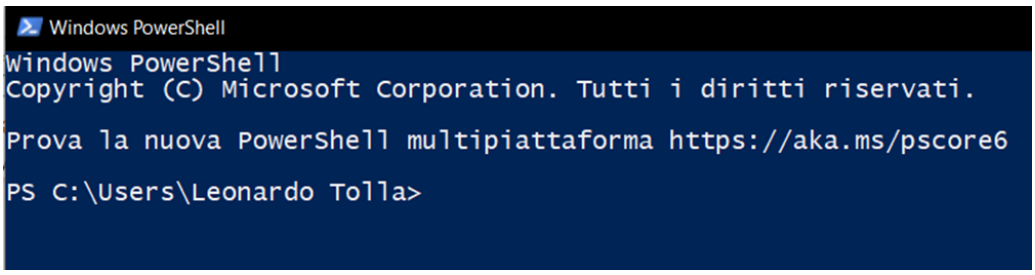

Figura 3.9. Powershell: schermata di apertura

A questo punto è necessario far sì che il sistema apra il codice Javascript e lo esegua; ciò si traduce sostanzialmente nei due passaggi seguenti:

1. Individuare la posizione del file Javascript all'interno del sistema.
2. Eseguire il codice Javascript.

Per effettuare queste due operazioni sono stati utilizzati due degli oltre cento comandi di sistema che sono disponibili e sono:

- **cd**: è un comando che imposta il percorso di lavoro su una posizione specificata.
- **node**: è un comando che permette di eseguire il file che si trova nella posizione definita con il cd.

La figura seguente mostra i comandi impartiti sul PowerShell, con main.js che è il nome che è stato dato al file Javascript eseguibile.

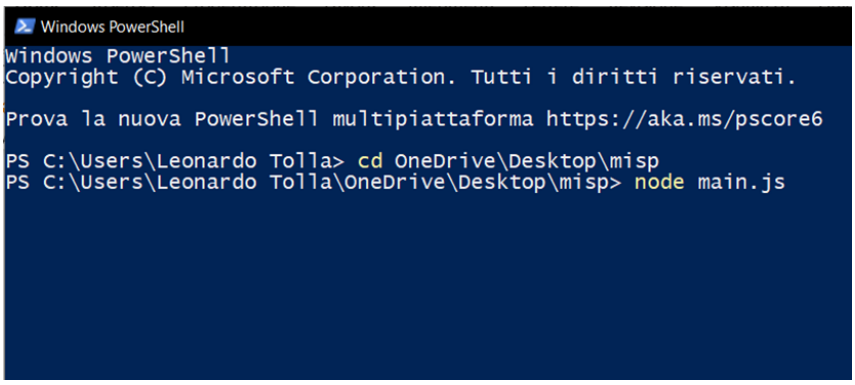

Figura 3.10. Powershell: comandi *cd* e *node*

Una volta cliccato il pulsante Invio verrà prodotto in output un file JSON contenente i risultati della richiesta che potrà esser visualizzato tramite browser o programmi di testo.

3.3 Classificazione degli eventi

Nella sezione precedente è stato evidenziato come, attraverso il linguaggio Javascript, sia possibile eseguire una cernita degli attacchi presenti sul MISP.

Nella presente sezione vengono descritte le principali classificazioni, effettuate sulla base delle seguenti dimensioni:

- **Threat Level:** sottosegmentazione degli eventi sulla base dell'impatto delle minacce.
- **Temporale:** sottosegmentazione degli eventi sulla base dell'anno di registrazione delle minacce sulla piattaforma.
- **Geografica:** sottosegmentazione degli eventi sulla base delle aree di provenienza delle organizzazioni che hanno segnalato gli attacchi.
- **Tags:** sottosegmentazione degli eventi sulla base dei tag allegati a ciascun evento.
- **Condivisione:** sottosegmentazione degli eventi sulla base del loro livello di visibilità.
- **Categorie di attributi:** sottosegmentazione degli eventi sulla base delle categorie di attributi associati.
- **Livello di analisi:** sottosegmentazione degli eventi sulla base dello stato attuale dell'analisi.

3.3.1 Classificazione per Threat Level

In fase di analisi del singolo evento abbiamo visto che il formato JSON prevede che il livello di minaccia venga espresso attraverso valori numerici, in particolare il valore 1 indica minaccia alta, il 2 minaccia media, il 3 minaccia bassa e il 4 minaccia undefined. È stata quindi effettuata una classificazione, adeguando il modello di scripting visto in precedenza, per evidenziare il numero di eventi per ciascun livello di impatto. I risultati ottenuti sono mostrati nella figura di seguito:

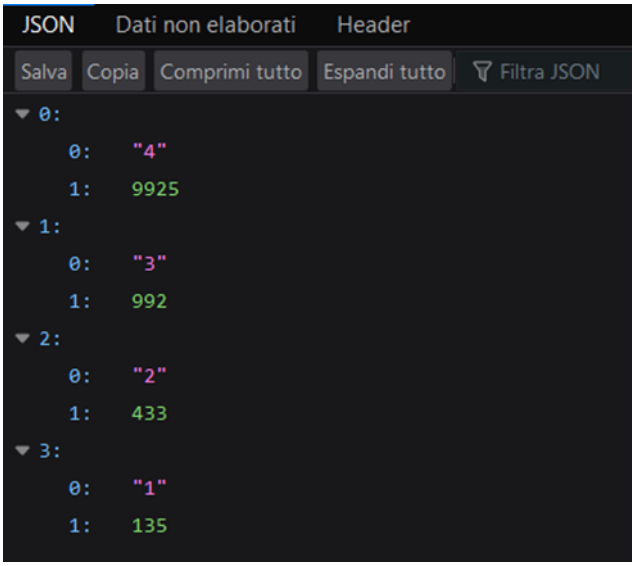

Figura 3.11. Risultati dello scripting per Threat Level

Emerge immediatamente che la maggior parte degli eventi presenta un livello della minaccia pari a 4; ciò in realtà significa che il threat level per quasi diecimila eventi è sconosciuto oppure non definibile. Il campo può essere però modificato in una data successiva, nel caso in cui si riesca in seguito a definire un opportuno livello di rischio tra quelli presenti sul MISP. I restanti eventi sono per lo più di livello Low, quindi tipicamente malware generici. Nell'ambito del presente lavoro, il focus sarà sugli eventi con impatto Medium/High e che ricorrono con numerosità minore.

Nel grafico successivo vengono sintetizzati i risultati ottenuti e rappresentati in forma percentuale:

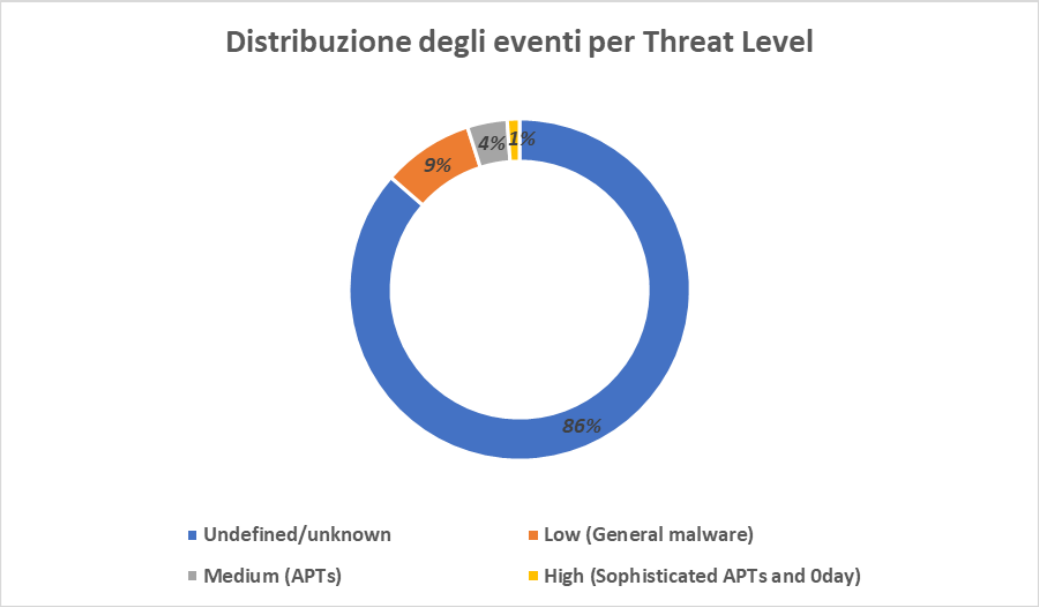

Figura 3.12. Distribuzione degli eventi per Threat Level

3.3.2 Classificazione temporale

Dopo la classificazione per livello di minaccia, con una seconda operazione di scripting, abbiamo registrato il numero di eventi occorsi nel corso del tempo, attraverso una suddivisione annuale che si basa sul momento in cui gli eventi stessi sono stati creati sulla piattaforma. Il risultato ottenuto è mostrato di seguito:

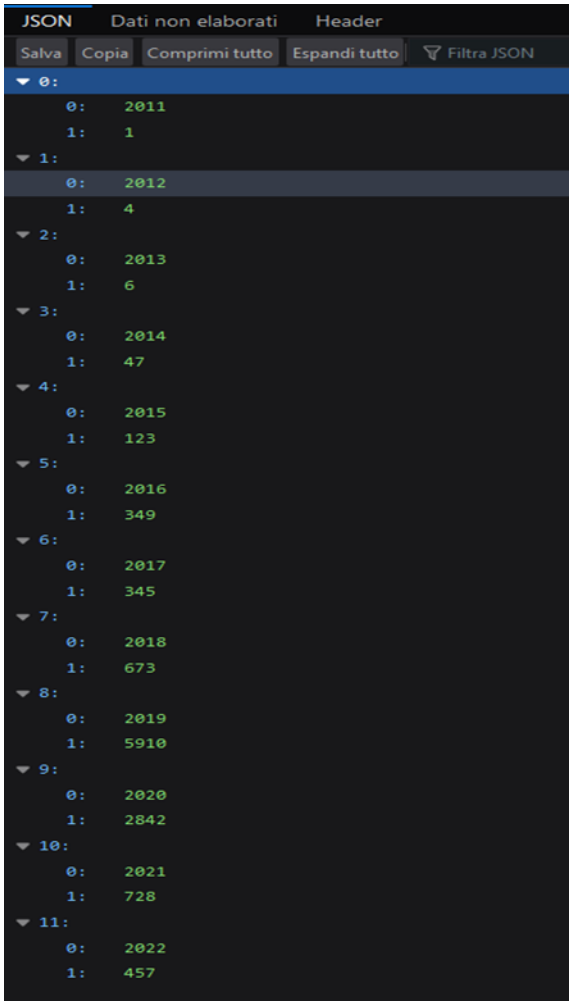

Figura 3.13. Risultati dello scripting per distribuzione temporale

Notiamo come il numero di eventi registrati sul MISP è tendenzialmente aumentato nel corso del tempo, sia per la crescente diffusione della piattaforma, sia per un utilizzo sempre maggiore dei dispositivi informatici che di fatto porta ad una maggiore registrazione di minacce.

Si nota però un picco di eventi creati negli anni 2019 e 2020; questo dato trova riscontro in quella che è stata la diffusione del virus SARS-CoV-2 con i relativi fenomeni di disinformazione e cyber minacce ad esso legato. Negli ultimi due anni il numero di eventi si è attestato a valori superiori a quelli degli anni pre-pandemia, ma ben distante dai picchi riscontrati.

Di seguito viene presentata graficamente la distribuzione temporale degli eventi :

Figura 3.14. Distribuzione temporale delle minacce

3.3.3 Classificazione geografica

Si è visto in fase di analisi di un evento che è possibile distinguere tra l'organizzazione che registra l'evento sulla piattaforma e quella che ha generato l'evento, ossia che ha subito l'attacco. In questo momento è interessante focalizzarci sulla seconda, in quanto si vuole valutare se ci sia una qualche occorrenza di tipo geografico nella distribuzione degli attacchi. Con questo obiettivo è stato effettuata una classificazione sulla base delle organizzazioni (e la loro relativa posizione geografica) che hanno generato gli eventi. Occorre tenere presente che sul MISP le organizzazioni vengono indicate attraverso valori numerici. Accedendo alla piattaforma si può reperire la lista delle organizzazioni, i loro ID e le loro posizioni geografiche. Di seguito sono mostrati i risultati ottenuti:

ID	Organizzazione	Posizione Geografica
2	Siemens AG	Germany
46	FORTH	Greece
7	Telenor	Norway
6	TelecomItalia	Italy
81	AI4HEALTHSEC	Europe
80	CyberSANE	Europe
9	CaixaBank	Spain
24	BitDefender	Romania

Tabella 3.1. Principali organizzazione che hanno registrato gli attacchi.

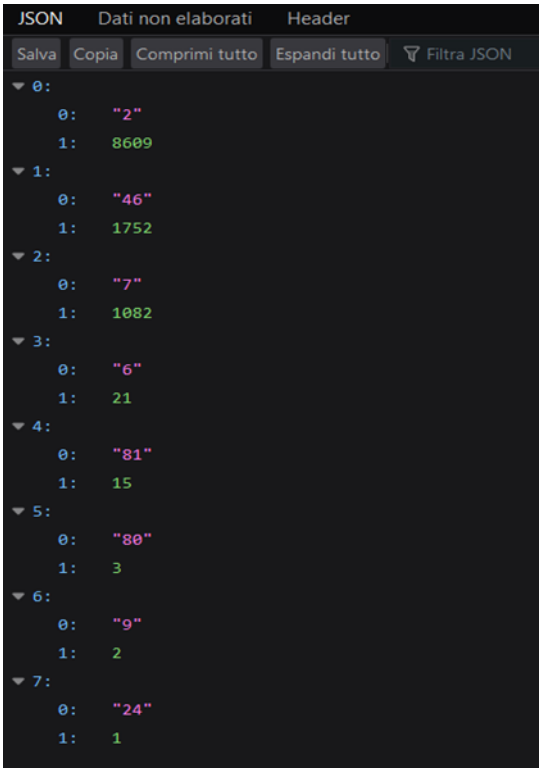

Figura 3.15. Risultati dello scripting per distribuzione geografica

Notiamo che la maggioranza degli attacchi si concentra in Germania, segnalati dalla Siemens, seguiti da FORTH, una dei maggiori centri di ricerca e sita in Grecia, e infine Telenor che opera nel settore delle telecomunicazioni norvegese. Le altre risultano essere pressoché irrilevanti. Abbiamo riportato in un istogramma la distribuzione geografica delle minacce:

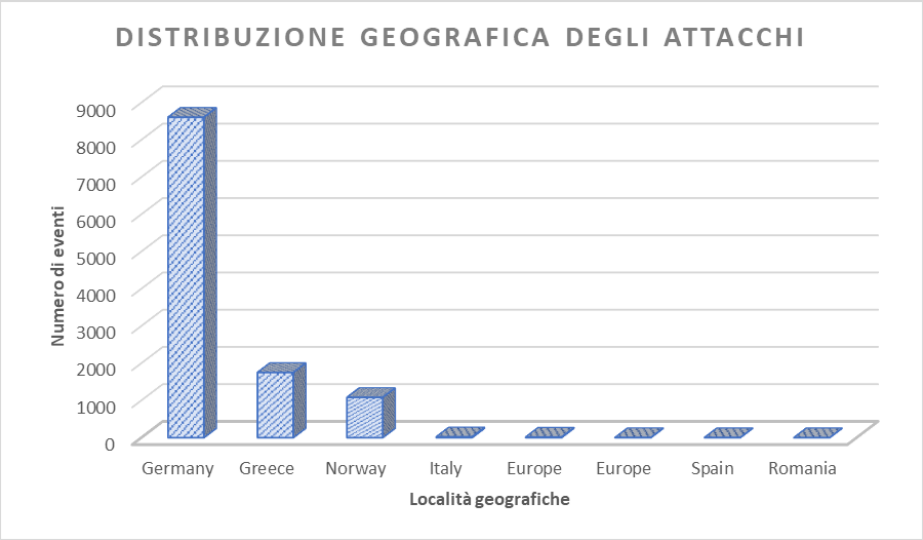

Figura 3.16. Distribuzione geografica degli attacchi

3.3.4 Classificazione per tags

Successivamente si è deciso di analizzare i tags allegati a ciascun evento per tener conto delle occorrenze più frequenti. In questo caso bisogna considerare che ogni evento può avere più di un tag e questo spiega l'elevata mole di questi ultimi rispetto a quella che è la numerosità delle minacce.

I risultati ottenuti hanno evidenziato che tag maggiormente presente è "tlp:white" il quale, lo ricordiamo, caratterizza informazioni che hanno divulgazione non limitate poiché comportano un rischio minimo e quindi possono essere condivise con il pubblico.

L'altro tag maggiormente presente è "malware: emotet". Si tratta di un malware che è nato originariamente per attaccare gli account bancari. La sua diffusione oggi però avviene principalmente tramite e-mail spam inviate a persone reali al cui interno si invita a scaricare un allegato che si rivela essere poi malevolo. Una volta infettato, il dispositivo della vittima viene aggiunto a una rete di computer infetti (botnet). Epoch 1, Epoch 2 ed Epoch 3 sono le denominazioni delle tre reti di server che controllano da remoto le operazioni del virus emotet e rientrano tra i tags più utilizzati sulla piattaforma con più di 7000 occorrenze totali.

Abbiamo poi numerose occorrenze di quella che è la classificazione OSINT, che fa riferimento a fonti pubbliche, nel nostro caso di tipo blog post e block-or-filter list. Infine ci sono più di 800 tags che fanno riferimento a informazioni riguardanti la pandemia di COVID-19.

I risultati ora descritti vengono riportati nella figura di seguito, dalla quale sono stati esclusi i tags con una rilevanza esigua rispetto al totale.

Figura 3.17. Risultati dello scripting per distribuzione dei tags

3.3.5 Classificazione per livello di condivisione

Si è già visto come, nel momento in cui si va a definire un evento sulla piattaforma, occorre anche indicare il livello di condivisione dello stesso, ossia andare a definire la visibilità della minaccia e quindi conseguentemente le organizzazioni che possono analizzarlo. Per quanto riguarda gli eventi estratti dalla piattaforma, il campo distribution è caratterizzato da soli due tipi di livelli di sharing.

In particolare, la quasi totalità degli eventi è caratterizzata dal valore "3", che indica che l'evento può esser condiviso con tutte le communities, propagando quindi l'evento da un server al successivo. I restanti eventi sono invece di livello distribution pari ad "1" e ciò limita la condivisione in quanto qualsiasi altra organizzazione connessa a server collegati MISP non potrà vedere l'evento.

I risultati appena descritti sono proposti nella figura seguente:

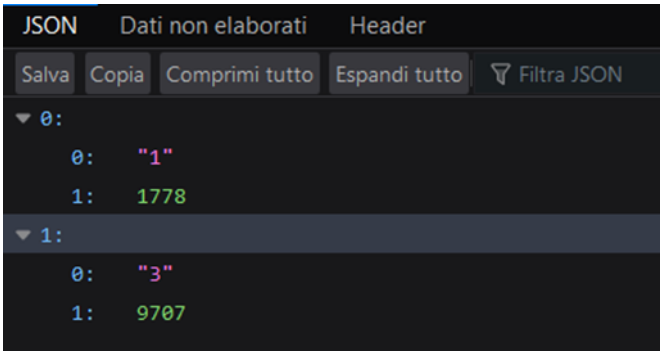

Figura 3.18. Risultati dello scripting per livello di condivisione

3.3.6 Classificazione per categorie di attributi

Come evidenziato all'inizio del presente elaborato, ciascun evento è caratterizzato da uno o più attributi e dalle sue categorie, ossia quale aspetto dell'evento è descritto da quel dato attributo. In questo senso è opportuno analizzare quelle che sono le principali categorie associate ai vari eventi e la loro numerosità. Anche in questo caso è stata effettuata un'operazione di scripting che ha permesso di individuare la numerosità delle varie categorie.

Le categorie individuate sono 15, ma sono state escluse quelle con una numerosità esigua rispetto al totale. Quelle presenti con una maggior frequenza vengono brevemente elencate di seguito:

- **Network activity:** categoria che fa riferimento alle informazioni sul traffico di rete generato dal malware.
- **Payload delivery:** categoria che fa riferimento a informazioni sulle modalità di distribuzione del malware.
- **Artifacts dropped:** categoria relativa a eventuali oggetti (e.g.file) rilasciati dal malware.
- **External analysis:** categoria che si riferisce a qualsiasi risultato derivante da un'analisi aggiuntiva del malware.
- **Payload installation:** categoria riguardante le informazioni su dove il malware si installa nel sistema.

Le categoria appena descritte e la loro numerosità relativa sono riportate nella figura seguente:

Figura 3.19. Risultati dello scripting per categorie di attributi

3.3.7 Classificazione per livello di analisi

L'ultima classificazione proposta riguarda il livello di analisi di ciascuna minaccia. In fase di creazione di un evento è emerso come il sistema richiede l'inserimento di quello che è l'attuale stato di analisi dell'evento. Anche in questo caso i tre stati di analisi possibili sono indicati attraverso altrettanti valori numerici.

La quasi totalità degli eventi vede il campo analysis valorizzato con lo 0 che indica che l'evento è stato appena creato e l'analisi sulla minaccia risulta ancora allo stato iniziale. I restanti invece sono caratterizzati dal valore 2 che si riferisce al fatto che il creatore dell'evento considera completata l'analisi della minaccia. Un'ultima quota di eventi, assolutamente modesta, è ancora in fase di analisi.

I risultati, quindi, certificano che attualmente le minacce sono registrate con una frequenza molto più elevata rispetto al passato, tanto che la quasi totalità delle minacce è

ancora in una fase di esaminazione preliminare. Ciò è concorde con quanto visto sulla distribuzione temporale degli eventi che evidenziava come la maggioranza degli eventi fosse stata registrata sulla piattaforma negli ultimi due anni.

Di seguito sono riportati i risultati appena descritti:

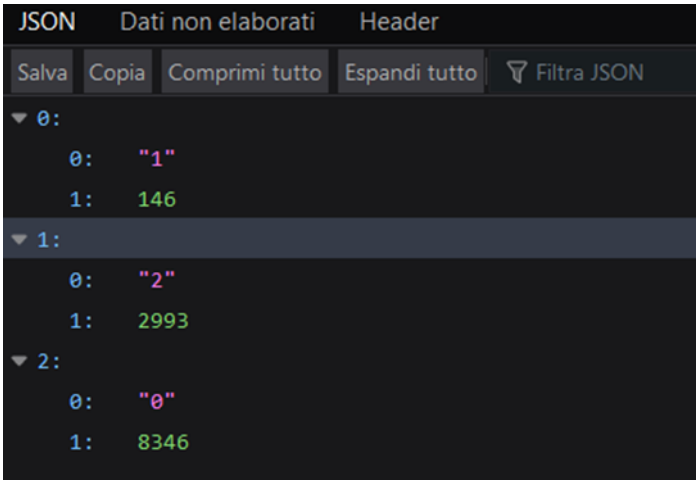

Figura 3.20. Risultati dello scripting per livello di analisi

3.4 Impatto dei rischi MISP sulla blockchain

3.4.1 Individuazione delle principali tipologie di attacco

Per quello che è l'obiettivo del presente lavoro, la classificazione maggiormente di interesse è quella relativa al threat level. Nella sezione precedente è emerso che sono più di 550 gli eventi con un impatto medio/alto.

Per questi eventi è necessario valutare la tipologia di attacco in modo da poter poi analizzare la risposta del sistema blockchain. In quest'ottica, la base di partenza è stata l'analisi dei tags degli eventi per poter ricavare maggiori informazioni sul tipo di minaccia. In particolare, le principali tipologie di attacco individuate sono riportate di seguito[6]:

- **Mirai:** si tratta di un malware che trasforma i dispositivi connessi ad internet in bot controllati a distanza che possono essere utilizzati, come parte di una botnet, per attacchi di rete su larga scala. La botnet Mirai è stata individuata per la prima volta nell'agosto 2016 ed è stata utilizzata in alcuni dei più grandi e pericolosi attacchi di tipo Distributed Denial of Service (DDoS).

- **Muhstik:** si tratta di una botnet che sfrutta delle vulnerabilità per accedere ad un URL specifico ed ottenere la possibilità di eseguire comandi su un server. A livello tecnico, Muhstik si è evoluto sulla base di Tsunami, un ceppo di malware utilizzato per anni per creare botnet infettando server Linux. La versione Muhstik amplia le

funzionalità di Tsunami, ma rimane principalmente utilizzata per lanciare attacchi DDoS. Gli autori di questi attacchi tipicamente poi richiedono un riscatto agli utenti colpiti.

- **Betabot:** si tratta di un malware acquistabile sul dark web, il che permette di lanciare botnet senza dover possedere particolari conoscenze tecniche. Quando infetta il dispositivo, è in grado di disabilitare fino a 30 diversi programmi antivirus e sicurezza. Di seguito alcuni dei comandi che possono essere impartiti alla botnet:
  - Lancio di un attacco DDoS contro un determinato obiettivo.
  - Download ed esecuzione di un file da un determinato URL.
  - Furto di informazioni da moduli visualizzati in un browser web.
- **Rootkit:** si tratta di software in grado di modificare le impostazioni e i permessi di un sistema informatico per prenderne il controllo completamente o in parte. I Rootkit si diffusero a partire da un caso eclatante che coinvolse la Sony BMG. Infatti nel 2005 l'azienda introdusse un rootkit nei propri CD musicali per limitare l'accesso da parte degli utenti e impedirne la duplicazione.
- **Ryuk ransomware:** è una famiglia di ransomware, di recente diffusione, che attacca principalmente grandi aziende. Quando Ryuk infetta un sistema per prima cosa arresta servizi e processi che potrebbero compromettere l'esecuzione dell'attacco. A quel punto crittografa file come foto, video, database, documenti e altri dati di interesse per gli utenti, mostrando poi sul sistema, sotto forma di file, le richieste di riscatto.
- **Egregor:** si tratta di un ransomware che, una volta entrato nel sistema, procede alla criptazione dei file. Egregor rende quindi documenti, archivi e database inutilizzabili, assegnando loro una nuova estensione (.random). Viene poi mostrata, solitamente in formato testuale, una nota di riscatto. Tale nota intima di pagare un ammontare ben preciso di bitcoin per ottenere la chiave di decrittazione.
- **Trick Bot:** inizialmente attaccava i sistemi attraverso e-mail di phishing. Queste false mail, provenienti apparentemente da istituzioni e aziende note, richiedevano alle vittime di aprire un allegato, esponendo loro all'infezione. Attualmente Trickbot è una botnet e un banking trojan in grado di rubare informazioni personali, credenziali e dettagli finanziari. In un attacco di questo tipo vengono prima disattivati i servizi Windows e le attività dei software anti-virus. Successivamente Trickbot utilizza vari metodi per estendere i privilegi amministrativi in modo da poter spiare sia il sistema che le reti, raccogliendo i dati dell'utente. Le informazioni raccolte dal malware vengono poi inoltrate a dispositivi esterni o agli autori dell'attacco.
- **Agent Tesla:** si tratta di un Remote Access Trojan (RAT), attivo dal 2014, che funziona come keylogger e password stealer. E' in grado di monitorare e raccogliere gli input da tastiera della vittima e appunti di sistema. Inoltre, può registrare screenshot e sottrarre le credenziali di accesso per molteplici software (inclusi Google Chrome, Mozilla Firefox e Microsoft Outlook).

3.4.2 Analisi dell'impatto degli attacchi sulla soluzione proposta

Dopo aver individuato le principali tipologie di attacco, l'obiettivo diventa quello di analizzare l'impatto degli stessi sul sistema blockchain proposto. In questo modo, sulla base del numero e della gravità degli attacchi dannosi, sarà possibile valutare l'effettiva sicurezza della soluzione ipotizzata e il livello di miglioramento rispetto alla situazione attuale. Per ciascun tipo di attacco identificato in precedenza è importante considerare sia il destinatario dello stesso sia l'entità dei danni che va a causare, evidenziando se e come il sistema blockchain riesce a contenerlo. Di seguito vengono proposte, per le tipologie di attacco individuate, le principali considerazioni effettuate:

1. Per le minacce causate dai ransomware come Egregor e Ryuk il sistema blockchain proposto risulta essere abbastanza robusto. Abbiamo visto che questa particolare famiglia di malware va a crittografare i file di interesse dell'utente-vittima, richiedendo un riscatto per la decrittazione. Nel sistema ipotizzato e descritto inizialmente, un attacco di questo tipo va a minacciare i nodi che condividono il database e che ne detengono una copia. In quello che è il nostro contesto, ciò si traduce nell'impossibilità di utilizzare una o più copie che sono risultate sotto attacco. In questo senso però la soluzione prospettata si dimostra efficace nel contenere questo rischio. Infatti, la crittografia della copia non va ad inficiare su quella che è l'integrità delle copie degli altri nodi della rete, a meno che il ransomware non agisse su tutte in maniera simultanea. Questo ultimo caso risulta essere però altamente improbabile e in ogni caso, rispetto alla situazione attuale, in cui si ha un'unica copia del database, si ha un improvement globale del sistema. Per quanto riguarda l'implementazione di contromisure ad attacchi di malware di questo tipo, sarebbe sufficiente creare uno o più backup della copia, in modo che l'attacco risulterebbe comunque inefficace e non altererebbe la funzionalità del sistema.

2. Per quanto riguarda invece attacchi di tipo keylogger e password stealer, come il RAT "Agent Tesla" analizzato in precedenza, il sistema blockchain ne risulta coinvolto solo in misura indiretta. Infatti, un trojan di questo tipo può raccogliere gli input da tastiera della vittima, quindi sicuramente nel nostro sistema i sensori e i nodi sono immuni a tale minaccia, essendone sprovvisti. Non può dirsi lo stesso però degli utenti che interagendo con il sistema blockchain utilizzano naturalmente dispositivi dotati di tastiera. In questo caso il keylogger va a registrare i caratteri inseriti da tastiera quando un utente digita la password. In questo caso le contromisure più efficaci sono rappresentate dall'utilizzo di una tastiera virtuale, che a differenza di quella fisica, non può essere attaccata dal malware, ma anche dal dotarsi di opportuni programmi che vanno a criptare tutto quello che viene digitato sulla tastiera.

3. Altre minacce individuate in precedenza e caratterizzate da un livello di rischio medio alto sono le botnet quali Mirai, Muhstik e BetaBot. E' emrso che questi malware sono sfruttati principalmente per inviare attacchi tipicamente DDoS. In questo tipo di minacce, dai computer compromessi partono contemporaneamente false richieste alla rete o al server per sovraccaricarli con un traffico eccessivo, portando così all'interruzione del servizio. Nel nostro sistema blockchain un attacco di questo tipo

comporterebbe l'impossibilità di accedere alla copia del database da parte del nodo che ha subito l'attacco, proprio a causa dell'elevato numero di finte domande di accesso. In ogni caso la caratteristica di decentralità della rete blockchain impedisce a un attacco DDoS di disabilitare il servizio agli utenti. Infatti, l'attacco a uno o più nodi non va ad inficiare l'integrità dell'intera rete e, come nel caso dei ransomware, attraverso un'altra copia è possibile bypassare l'inaccessibilità di quella che ha subito l'attacco.

4. Diverso è il discorso per malware come Rootkit e Trickbot. In questo caso tali software sono in grado di prendere il controllo di una macchina, grazie all'ottenimento dei permessi amministrativi dello stesso. Questo nel nostro caso in esame, si traduce con la possibilità, sfruttando eventuali bug o difetti nella configurazione dei nodi, nella perdita della copia del ladger. Emerge in maniera chiara che sugli attacchi che mirano a ottenere il controllo del nodo e a sottrarre informazioni il sistema blockchain risulta essere piuttosto debole.

3.5 Ulteriori attacchi al sistema blockchain

Abbiamo visto nella sezione precedente come la soluzione prospettata risulti essere sufficientemente robusta a fronte delle minacce più rischiose che sono presenti sulla piattaforma MISP. Bisogna però precisare che gli attacchi analizzati non esauriscono di certo le minacce a cui un sistema blockchain deve far fronte. In tal senso risulta quindi opportuno mostrare ed esaminare anche gli altri, con un focus particolare a quelli che maggiormente mettono a rischio l'integrità della soluzione proposta. Di seguito ne vengono descritti i principali:

- **51% Attack:** si tratta di un potenziale attacco a una rete blockchain in cui un'entità o organizzazione riesce a prendere il controllo della maggioranza del network. Questo permetterebbe all'autore dell'attacco di impedire la conferma delle transazioni. Non sarebbe comunque possibile impedire la trasmissione delle stesse al network o invertire le transazioni di altri utenti. Un 51% Attack risulta comunque abbastanza improbabile, soprattutto per i network più grandi in cui c'è una maggior protezione contro attacchi e manomissione di dati[18].

- **Sybil Attack:** in questo tipo di attacco gli hacker, utilizzando un singolo nodo, generano diversi falsi nodi attivi all'interno della catena blockchain. Le identità false servono per poter esercitare influenza nella rete e acquisire così la maggioranza dei consensi. Un 51% Attack sostanzialmente è un attacco Sybil effettuato su larga scala. Per prevenire una minaccia di questo tipo è possibile utilizzare algoritmi di consenso BFT. Si tratta di algoritmi implementati per risolvere il problema dei generali bizantini e che quindi mirano a mantenere la funzionalità del sistema anche a fronte di nodi dannosi o compromessi. In questo senso un algoritmo BFT è in grado di impedire o rendere inutile la creazione di identità multiple, rendendo di fatto inefficace un Sybil Attack.

3.5.1 Attacchi ai sensori

Infine, è opportuno citare brevemente anche i rischi che non coinvolgono direttamente la tecnologia blockchain, ma che in ogni caso possono avere un impatto negativo sul sistema. È il caso dei sensori che nella nostra soluzione rappresentano una trusted third part e che, se compromessi, forniscono in ingresso alla blockchain dei dati non validi. Essendo elementi fisici esterni, i sensori possono essere manomessi o addirittura spostati, portando ad errori di lettura. Per far fronte a questa limitazione, è possibile sfruttare la tecnologia Narrowband-IoT (uno standard per consentire la comunicazione sicura tra una serie di dispositivi interconnessi) e la collaborazione dei provider di servizi Internet (ISP). Un'altra limitazione è data dal fatto che se viene interrotta la comunicazione tra i sensori e la rete blockchain, ad esempio con l'uso di disturbatori di frequenze (jammers), la registrazione degli eventi negativi risulta compromessa.

Capitolo 4

Conclusioni

L'intento di quest'ultimo capitolo è quello di ricapitolare brevemente il lavoro svolto, da quelli che sono stati i dati di partenza fino a i risultati ottenuti, descrivendo sulla base degli stessi gli eventuali sviluppi futuri.

4.1 Osservazioni finali

L'attribuzione delle responsabilità all'interno di una supply chain così peculiare, come quella delle batterie per veicoli elettrici, è stato il catalizzatore dell'intero lavoro descritto nella presente tesi. Il costante monitoraggio e l'elevata frequenza degli interventi che richiedono le batterie durante il loro ciclo di vita hanno portato alla definizione di una soluzione che permettesse, in modo univoco, di tener traccia delle azioni compiute dagli attori coinvolti. Questo con l'obiettivo di ottenere un incremento del trust tra le parti interessate con conseguente ottimizzazione globale della rete.

La tecnologia Blockchain è emersa come uno strumento in grado di venire incontro a tali esigenze, introducendo però dei motivi di riflessione circa le capacità del sistema di contenere minacce di natura diversa rispetto a quelle presenti nella situazione attuale.

Il lavoro nel presente elaborato è stato quello di analizzare qualitativamente gli attacchi più rischiosi per la soluzione ideata che sono presenti nel panorama informatico. Per fare ciò ci siamo serviti della piattaforma MISP su cui vengono registrati le cyberminacce che quotidianamente vengono affrontate dalle organizzazioni internazionali. Sono stati estratti gli attacchi maggiormente rischiosi ed è stato valutato singolarmente il loro impatto sul sistema blockchain.

I risultati ottenuti hanno evidenziato che la rete risponde bene ai rischi in quanto nella maggior parte dei casi le compromissioni sono temporanee e a livello locale, mentre globalmente la tecnologia non ne risulta impattata. Questo suggerisce che la strada blockchain-based può rappresentare una prospettiva concreta per quel che riguarda il tracciamento di un prodotto nell'ambito logistico e la trasparenza delle operazioni ad esso connesso.

Inoltre, bisogna tener presente che il tasso di globalizzazione crescente nell'ultimo decennio ha investito anche il mondo della supply chain. Questo ha fatto si che le catene di approvvigionamento e distribuzione diventassero più estese, ma anche maggiormente esposte a nuovi rischi come quelli ambientali, etici, sanitari o di natura geopolitica. Basti pensare alla pandemia virale da Covid-19 che ha messo in luce tutte le fragilità e le vulnerabilità delle catene, venendo meno la capacità di tracciare i flussi e la trasparenza con i fornitori. In un panorama di questo tipo che vede la logistica andare nella direzione di processi geograficamente sempre più estesi e complessi, la blockchain può rappresentare un valido aiuto in quanto va a contenere i nuovi rischi a cui esposta la global supply chain.

4.2 Prospettive future

4.2.1 Miglioramento della scalabilità del sistema

La rete blockchain analizzata nel presente elaborato risulta essere piuttosto semplificata. Per via della scalabilità all'interno del trilemma della blockchain, la soluzione ideata tiene traccia delle sole informazioni di monitoraggio legate alle batterie. Questo apre sicuramente alla possibilità di migliorare il sistema in termini requisiti di archiviazione e scalabilità. A tal proposito un'eventuale soluzione può esser rappresentata dall'integrazione dell'InterPlanetary File System.

L'IPFS è un protocollo peer to peer per l'archiviazione e la condivisione dei dati. Quando viene aggiunto un file a IPFS, questo viene scomposto in più parti, crittografato e ne viene assegnata un'impronta digitale unica (CID). Gli altri nodi cercano tale file chiedendo chi sta memorizzando il contenuto con quello specifico CID e, dopo aver scaricato il file, ne mettono in cache una copia diventando così a loro volta fornitori di quel contenuto. Un nodo può conservare un file e fornirlo ad altri per sempre oppure eliminarlo per salvare spazio, memorizzando quindi solo ciò a cui è realmente interessato. Quando viene caricata una nuova versione del file su IPFS, essa riceve un nuovo CID in modo da risultare immune a ogni tipo di manomissione poiché qualsiasi modifica al contenuto non sovrascrive l'originale. Un protocollo di questo tipo integrato nella blockchain permetterebbe di archiviare file di grandi dimensioni fuori dalla catena e di inserire link permanenti nelle transazioni in modo da proteggere i contenuti senza dover inserire i dati stessi all'interno della rete[19].

4.2.2 Estensione della blockchain all'intera SC

Un'ulteriore possibile prospettiva futura può esser rappresentata dall'estensione della rete blockchain a tutte le operazioni connesse alla supply chain. Ad esempio gli smart contracts, che nel nostro caso d'uso erano limitati al controllo dei permessi e all'emissioni di eventi legati ai battery packs, potrebbero essere usati per gestire i pagamenti tra le parti. Quello che solitamente accade oggi è che il pagamento ai fornitori viene dilazionato nel tempo dopo che la merce è stata già consegnata, aumentando cosi il capitale circolante. Attraverso gli smart contracts sarebbe possibile digitalizzare i contratti coinvolgendo sia gli operatori logistici che gli istituti bancari. Con questa soluzione l'avvenuta ricezione

della merce verrebbe registrata immediatamente nella rete blockchain e contestualmente emessa la fattura di pagamento, semplificando drasticamente le operazioni finanziarie[20].

4.2.3 Limiti agli sviluppi futuri

Un report del Capgemini Research Institute dal titolo "Does blockchain hold the key to a new age of supply chain transparency and trust?"[21] fornisce una panoramica delle aziende che stanno investendo nell'implementazione della blockchain e prevede che entro il 2025 tale tecnologia sarà utilizzata massivamente nell'ambito della supply chain. Questo report però evidenzia anche alcuni ostacoli che possono frenare l'adozione futura della rete blockchain nel settore logistico; i principali vengono mostrati nella figura riportata di seguito:

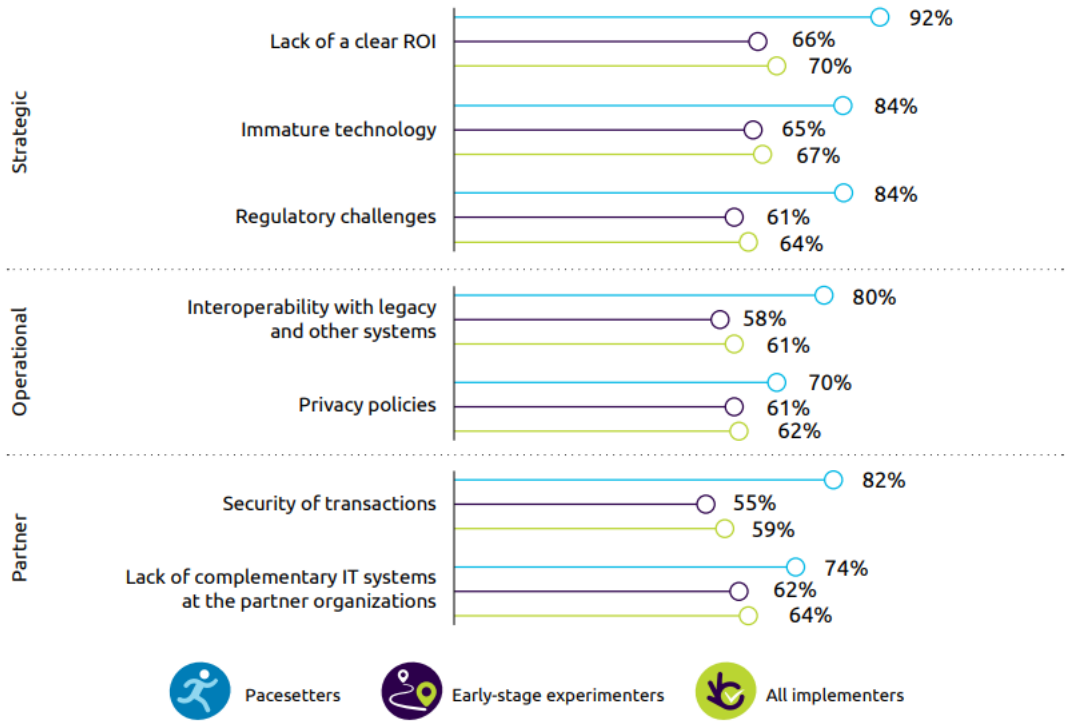

Figura 4.1. Ostacoli principali all'implementazione della Blockchain (Fonte:[21])

Dal grafico emerge come il 92% delle organizzazioni pioniere dell'implementazione della blockchain (pacesetters) ritiene che il ROI sia la principale sfida da affrontare per l'adozione della rete nel proprio business. Infatti questo indice, che misura il reddito generato dal capitale investito nel tempo, non è stato ancora quantificato per applicativi di questo tipo e per questo rappresenta un freno allo sviluppo di tale tecnologia.

Un'altra significativa fonte di preoccupazione è rappresentata dal fatto che i modelli e i processi di business di ogni supply chain dovranno essere riprogettati per favorire l'adozione della blockchain. Inoltre, secondo il report "Using blockchain to drive supply chain innovation"redatto dall'azienda di servizi di consulenza Deloitte, ci sarebbero altri potenziali rischi da monitorare[22]. Oggi le aziende utilizzano strumenti digitali (Barcode, Tag RFID ...) per tracciare i prodotti fisici e in quest'ottica sarebbe necessaria una revisione delle practices aziendali per una loro implementazione all'interno della rete. Inoltre la tecnologia blockchain richiede la migrazione verso un network completamente diverso dalle attuali soluzioni, il che rende perplessi utenti e operatori su una sua eventuale adozione.

Quanto detto finora fa capire i motivi per cui oggi sono ancora molto limitate le implementazioni su larga scala, come si evince chiaramente dal grafico mostrato di seguito

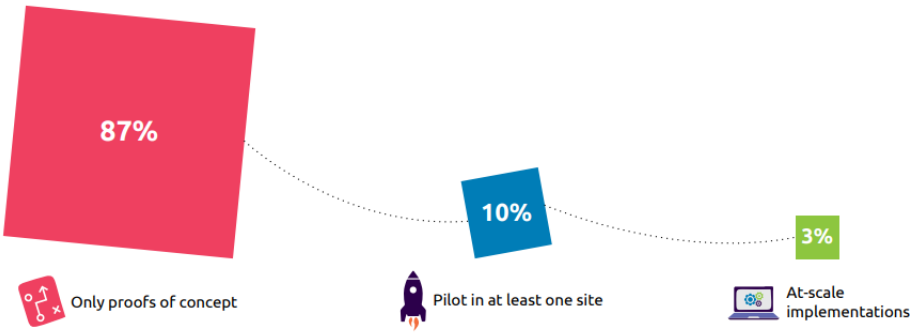

Figura 4.2. Livello di implementazione della Blockchain (Fonte:[21])

Il Capgemini Research Institute ha analizzato la maturità di implementazione della blockchain e, come evidenziato dalla figura, la stragrande maggioranza (87%) si trova in una fase di sperimentazione o di proof of concepts. Il 10% in una fase avanzata di test con almeno un progetto pilota avviato e solamente il 3% delle aziende stanno sperimentando su larga scala.

Per concludere, le companies dovrebbero prestare attenzione agli stakeholders della supply chain e ai competitors nel loro settore che hanno iniziato a sperimentare l'utilizzo della blockchain. Questo perché, come evidenzia ancora Deloitte, la rete beneficia del cosiddetto *Network Effect*. Si tratta dell'effetto economico per cui un bene o servizio aumenta di valore in base al numero di utenti. Una volta raggiunta una certa massa critica è più facile per gli altri utenti entrare nel sistema e ottenerne i benefici[22]. Ecco perchè il timing relativo allo sviluppo della rete blockchain sarà un aspetto cruciale per far si che questa tecnologia venga coinvolta sempre di più all'interno della gestione delle catene di fornitura.

Bibliografia

[1] Aruba. Sharing delle informazioni tra gestori: indicatori di compromissione e misp. URL https://www.aruba.it/magazine/pec/sharing-delle-informazioni-tra-gestori-indicatori-di-compromissione-e-misp.aspx.

[2] MISP Project. Features of misp, the open source threat sharing platform, . URL https://www.misp-project.org/features/.

[3] MISP Project. Information sharing and taxonomies, . URL https://www.misp-project.org/misp-training/3-misp-taxonomy-tagging.pdf.

[4] MISP Project. Misp taxonomies and classification as machine tags, . URL https://www.misp-project.org/taxonomies.html.

[5] MISP Project. Misp galaxy, . URL https://www.misp-project.org/misp-training/3.2-misp-galaxy.pdf.

[6] MISP Project. Misp galaxy clusters, . URL https://www.misp-project.org/galaxy.html#_android.

[7] MISP Project. Misp object template, . URL https://www.misp-project.org/misp-training/3.3-misp-object-template.pdf.

[8] MISP Project. Format of misp object template, . URL https://github.com/MISP/misp-objects.

[9] Michele Petito. Misp: l'unione fa la sicurezza. URL https://www.garrnews.it/cybersecurity-24/893-misp-l-unione-fa-la-sicurezza.

[10] CIRCL. Using the system. URL https://www.circl.lu/doc/misp/using-the-system/.

[11] Mattia Siciliano. La cyber threat information sharing: differenze di approccio tra malware information sharing platform (misp) e threat intelligence platform (tip). URL https://www.ictsecuritymagazine.com/articoli/la-cyber-threat-information-sharing-differenze-di-approccio-tra-misp-e-tip/.

[12] Roberto Rodriguez. The helk. URL https://thehelk.com/intro.html.

[13] Bruni; Capocasale; Costantino; Musso; Perboli. Decentralizing electric vehicle supply chains: Value proposition and system design.

[14] Binance Academy. La byzantine fault tolerance spiegata, . URL https://academy.binance.com/it/articles/byzantine-fault-tolerance-explained.

[15] Binance Academy. Cos'è il trilemma della blockchain?, . URL https://academy.binance.com/it/articles/what-is-the-blockchain-trilemma.

[16] IBM. Cos'è hyperledger fabric? URL https://www.ibm.com/it-it/topics/hyperledger.

[17] Hyperledger sawtooth. URL https://sawtooth.hyperledger.org/docs/1.2/.

[18] Binance Academy. Cos'è un 51% attack?, (2018). URL https://academy.binance.com/it/articles/what-is-a-51-percent-attack.

[19] How ipfs works. URL https://ipfs.tech/.

[20] Blockchain per la supply chain - smart contracts. URL https://www.logisticaefficiente.it/qantica/management/blockchain-per-la-supply-chain.html#:~:text=Applicazioni%20della%20blockchain%20nella%20supply,per%C3%B2%20sminuire%20le%20sue%20potenzialit%C3%A0.

[21] Capgemini Research Institute. Does blockchain hold the key to a new age of supply chain transparency and trust? URL https://www.capgemini.com/gb-en/wp-content/uploads/sites/5/2022/05/Digital-Blockchain-in-Supply-Chain-Report-1.pdf.

[22] Deloitte. Using blockchain to drive supply chain innovation. URL https://www2.deloitte.com/content/dam/Deloitte/us/Documents/process-and-operations/us-blockchain-to-drive-supply-chain-innovation.pdf.