Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

CSP006_S_E

PRESENTAZIONE DA PARTE DI:
DR. STEFAN SCHAUER
DR. ABDELKADER SHAABAN
AIT ISTITUTO AUSTRIACO DI TECNOLOGIA

Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

Cyber Threat Intelligence e Threat Hunting nel settore dell'energia

Panoramica

- Argomento-1: Introduzione all'intelligence delle minacce e alla caccia alle minacce
- Argomento-2: Fonti e raccolta dei dati
- Argomento 3: Attori e tattiche di minaccia
- Argomento 4: Modellazione pratica delle minacce e indagini sulla sicurezza

Ordine del giorno

01. Informazioni sulle minacce

02. Fonti di intelligence

03. Caccia alle minacce

OBIETTIVI

Al termine di questa sessione, dovreste essere in grado di ...

1. Identificare i diversi tipi di avversari che rappresentano una minaccia per i nostri sistemi informatici.

2. Identificare i diversi tipi di intelligence che possiamo utilizzare per caratterizzare le minacce.

3. Esplorare diversi strumenti open-source che ci permettono condividere le informazioni e automatizzare le risposte.

4. Riconoscere l'ampia gamma di prodotti pubblici
   fonti disponibili di minaccia informatica
   Intelligenza

Informazioni sulle minacce

Cos'è l'intelligence sulle minacce informatiche CTI)

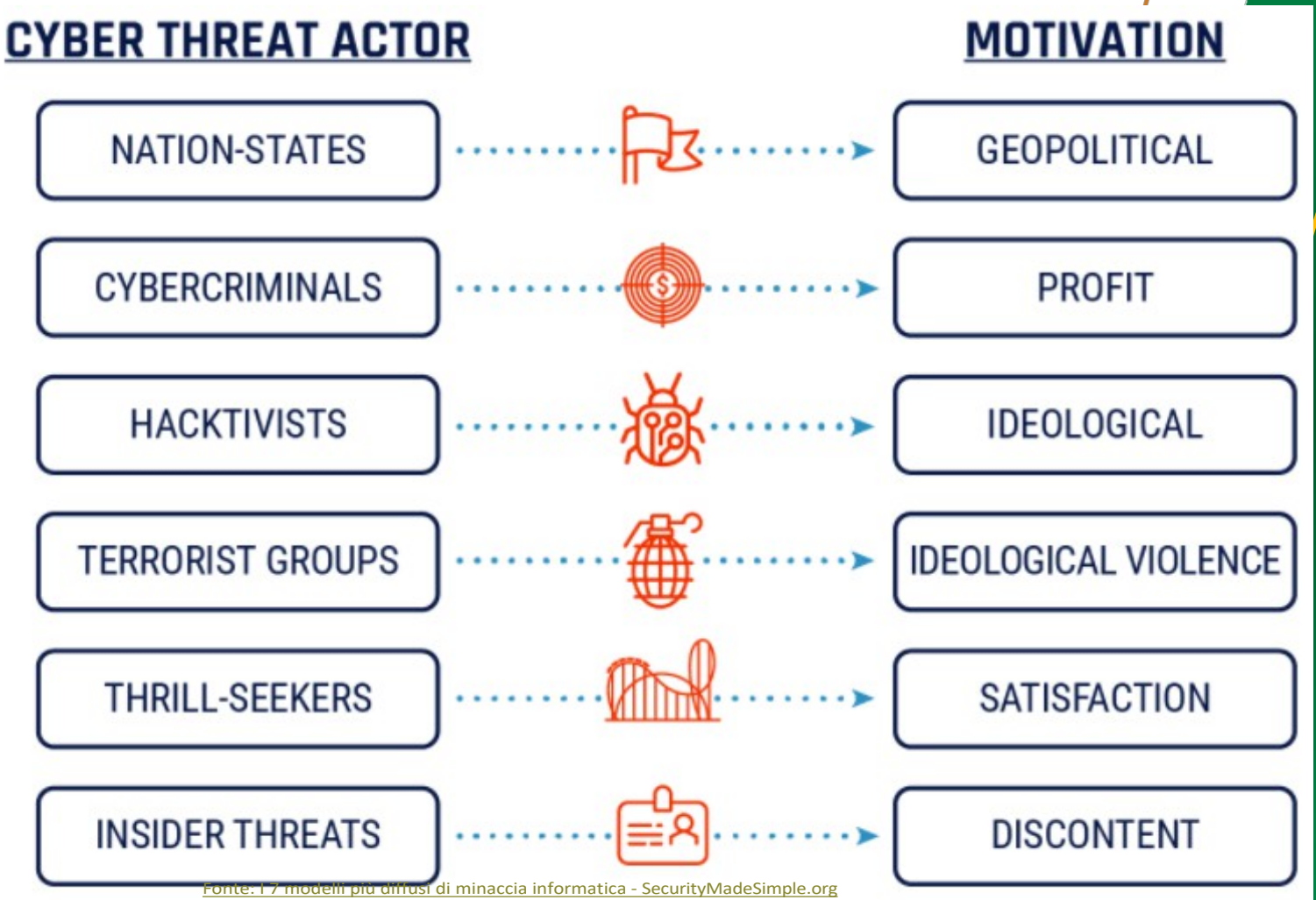
L'uso di competenze, conoscenze ed esperienze per raccogliere e valutare l'affidabilità delle informazioni relative agli attori delle minacce/avversari, comprese le loro intenzioni, capacità e potenziali opportunità, al fine di mitigare i possibili attacchi informatici e i danni che potrebbero causare.

Gli avversari vogliono attaccare i sistemi informatici, è importante capire le loro intenzioni:

- Motivazioni politiche?
- Hacktivismo?
- Guadagno economico?

Le loro capacità sono altrettanto importanti. Gli avversari sono un gruppo di hacker sponsorizzato dallo Stato, criminali tecnicamente qualificati o script kiddies che giocano con nuovi strumenti? Le capacità di questi gruppi sono molto varie. Alcune potrebbero non essere rilevanti.

Tipi di attori delle minacce in natura



Fonte: I 7 modelli più diffusi di minaccia informatica - SecurityMadeSimple.org

Concetti chiave

Avversario / Attore di minaccia

La persona o il gruppo di persone dietro tastiera, che esegue l'attacco informatico. Può essere in modo generico, ad esempio l'*Unità militare 26165*, o un individuo specifico, ad l'*Unità militare 26164*.

Kevin Mitnick.

Campagna

Operazioni dannose prolungate di un avversario che si concentrano su un unico obiettivo o fine, ad esempio compromettere il servizio online di un'azienda o sabotare una raffineria di petrolio e gas.

Tattiche, tecniche e procedure (TTP)

Un modo per descrivere un metodo o un insieme di metodi utilizzati dagli avversari per compromettere una macchina o un sistema.

Indicatori di compromissione (IoC)

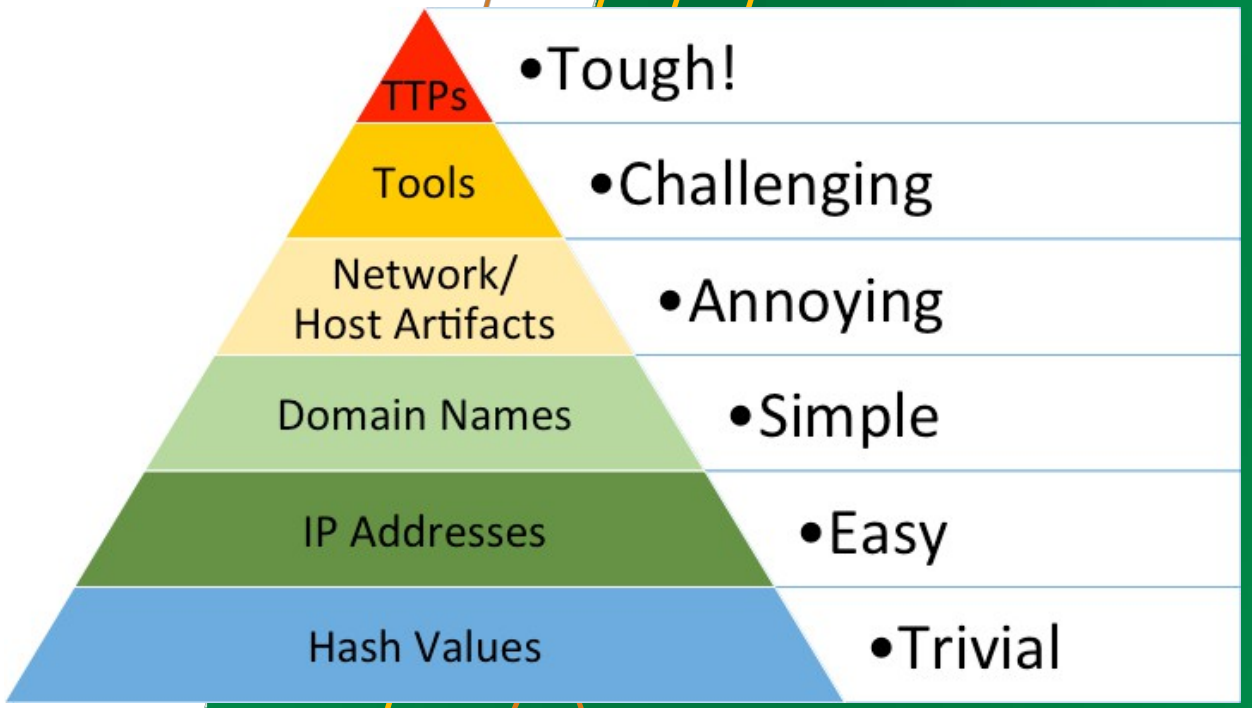
Frammenti di dati forensi, presenti nei registri di sistema, nei file, nelle acquisizioni di pacchetti di rete e così via, che identificano un'attività dannosa su un sistema o una rete di computer.

Piramide del dolore dell'Istituto SANS

Il dolore si riferisce alla sofferenza che si può causare a un avversario, se si è in grado di individuare e identificare gli elementi di quel livello della piramide.

Più si sale nella piramide, più *dolorosa* per gli aggressori.

Più la sezione della piramide è ampia, più le informazioni sono accurate e fruibili.



SANS è l'acronimo di SysAdmin, Audit, Network e Security.

Valori Hash

Gli algoritmi di hashing producono un **digest del messaggio** a partire da un dato input e vengono utilizzati per verificare l'integrità di un software, per assicurarsi che non siano state apportate modifiche dannose.

Gli algoritmi di hashing più comuni sono **SHA1**, **MD5** e **SHA256**.

Gli algoritmi di hashing sono funzioni unidirezionali*.

La modifica di anche un solo bit dell'input produce un hash diverso.

Input	Input
Hello	Hallo
Output	**Output**
8b1a9953c4611296a827abf8c47804d7	1de11cf8b803fb31cacb13ce23c0b361

▸ Audacity 3.1.2 64 bit installer

SHA256 Checksum:

```
6a3f5f7c1801d30de40e02477be87b429336e3ed42d65cf6f12cdb9a101d1906
```

▸ Audacity 3.1.2 64 bit zip file

SHA256 Checksum:

```
3d1d4e097c48b7d685c8061920b84ac4ac0257d40ae17567de223d75f41bbb40
```

IP, dominio, artefatti di rete

- I domini ci permettono di utilizzare nomi leggibili per i siti web e i servizi online.
- Gli indirizzi IP sono un elemento molto preciso, ma I domini possono essere utilizzati per ingannare gli esseri umani.
- Molte famiglie di malware utilizzano algoritmi di generazione dei domini (DGA) per creare e registrare i domini in modo procedurale.
- In questo modo il malware impiantato ha la possibilità di trovare una connessione con gli aggressori.

```
Standard query 0x6c4f  A pivuogusodtoku.ddns.net
Standard query 0xb48b  A onogibuluremg.ddns.net
Standard query 0x66fc  A geevheuqsemaif.ddns.net
Standard query 0x7b8c  A egisrihuwuwoom.ddns.net
Standard query 0x6660  A enaxontugahoun.ddns.net
Standard query 0xb015  A vauqomadassaeb.ddns.net
Standard query 0x56da  A opdeikixaxec.ddns.net
Standard query 0xa24e  A oticrivievhuow.ddns.net
Standard query 0x6644  A uqodupegbo.ddns.net
Standard query 0x63d0  A xisenuun.ddns.net
Standard query 0x0243  A omexithamisi.ddns.net
Standard query 0xbeca  A uxtoleite.ddns.net
Standard query 0x12b6  A uglaweedipwaho.ddns.net
Standard query 0x57dc  A ahtilenearo.ddns.net
Standard query 0x3e8c  A niesivaxumo.ddns.net
Standard query 0xd3f6  A iricilec.ddns.net
Standard query 0x734a  A uqadvoduurgeuhi.ddns.net
Standard query 0x94b1  A ehwepikeisi.ddns.net
Standard query 0xc9e9  A ehukguaggox.ddns.net
Standard query 0x292f  A onwaukfitamia.ddns.net
Standard query 0x2975  A idxoebsad.ddns.net
Standard query 0xac37  A ihneuwvaixq.ddns.net
Standard query 0x8b92  A subaukewoktalev.ddns.net
```

Tattiche, tecniche e procedure (TTP)

I TTP sono classificazioni gerarchiche del comportamento degli avversari. L'uso delle TTP in La combinazione con il MITRE ATT&CK Framework rende più facile "prendere le impronte digitali" di una gruppo di minacce.

Una **tattica** è il metodo di più alto livello per raggiungere un obiettivo tramite un attacco informatico.

Ad esempio, *infezione con malware tramite Spear Phish* (accesso iniziale).

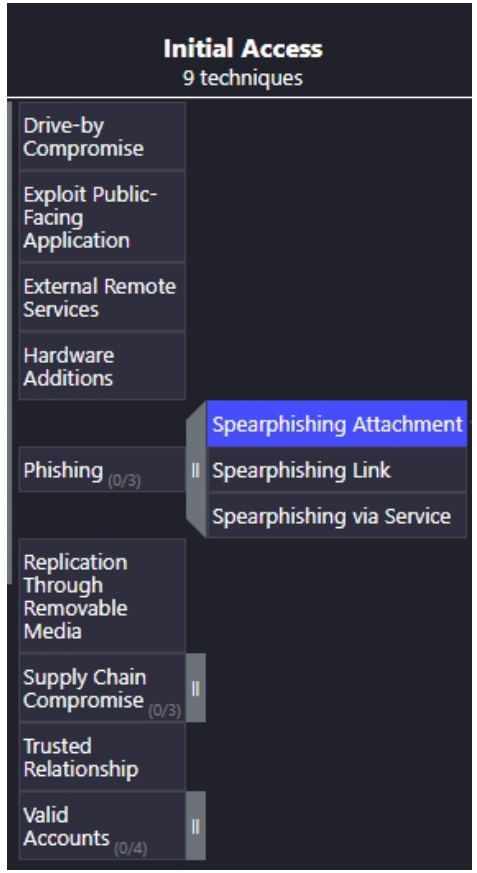
Una **tecnica** è il modo in cui viene impiegata la tattica.

Ad esempio, la creazione di un exploit dannoso all'interno di un file PDF (T1566.001). Una **procedura** è il modo in cui viene fornita la tecnica.

Ad esempio, i comandi utilizzati per creare il PDF e inviare l'e-mail. Il termine TTP viene talvolta utilizzato per descrivere in generale il modo in cui opera un avversario.

MITRE ATT&CK Framework

L'ATT&CK Framework di MITRE consente di identificare e condividere facilmente i TTP.



Procedure Examples

ID	Name	Description
G0018	admin@338	admin@338 has sent emails with malicious Microsoft Office documents attached.[1]
S0331	Agent Tesla	The primary delivered mechaism for Agent Tesla is through email phishing messages.[2]
G0130	Ajax Security Team	Ajax Security Team has used personalized spearphishing attachments.[3]

Detection

ID	Data Source	Data Component
DS0015	Application Log	Application Log Content
DS0022	File	File Creation
DS0029	Network Traffic	Network Traffic Content
		Network Traffic Flow

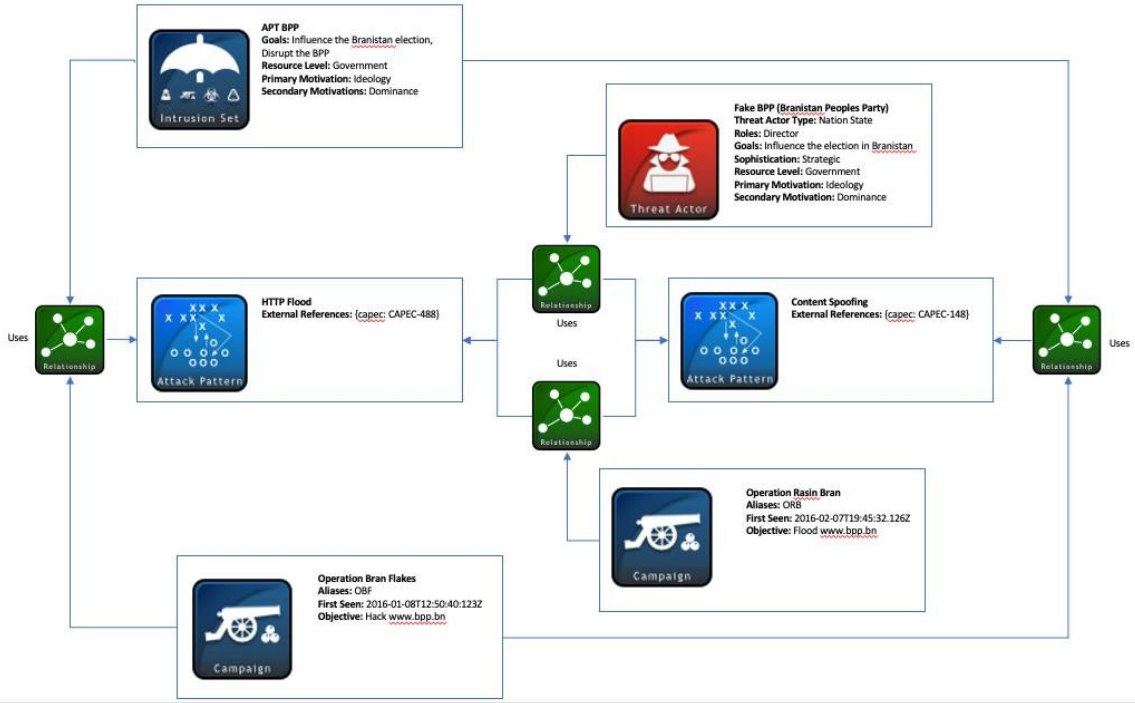
Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can also automatically quarantine suspicious files.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments can be used to block activity.

Espressione strutturata delle informazioni sulle minacce (STIX)

Linguaggio e formato di serializzazione per lo scambio di CTI

Può essere rappresentato visivamente per un analista o memorizzato come JSON.




```
{
    "type": "bundle",
    "id": "bundle--56be2a3b-1534-4bef-8fe9-602926274089",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.1",
            "id": "indicator--d81f86b9-975b-4c0b-875e-810c5ad45a4f",
            "created": "2014-06-29T13:49:37.079Z",
            "modified": "2014-06-29T13:49:37.079Z",
            "name": "Malicious site hosting downloader",
            "description": "This organized threat actor group operates
            "indicator_types": [
                "malicious-activity"
            ],
            "pattern": "[url:value = 'http://x4z9arb.cn/4712/']",
            "pattern_type": "stix",
            "valid_from": "2014-06-29T13:49:37.079Z"
        },
```

Piattaforma di condivisione delle informazioni sulle minacce informatiche (MISP)

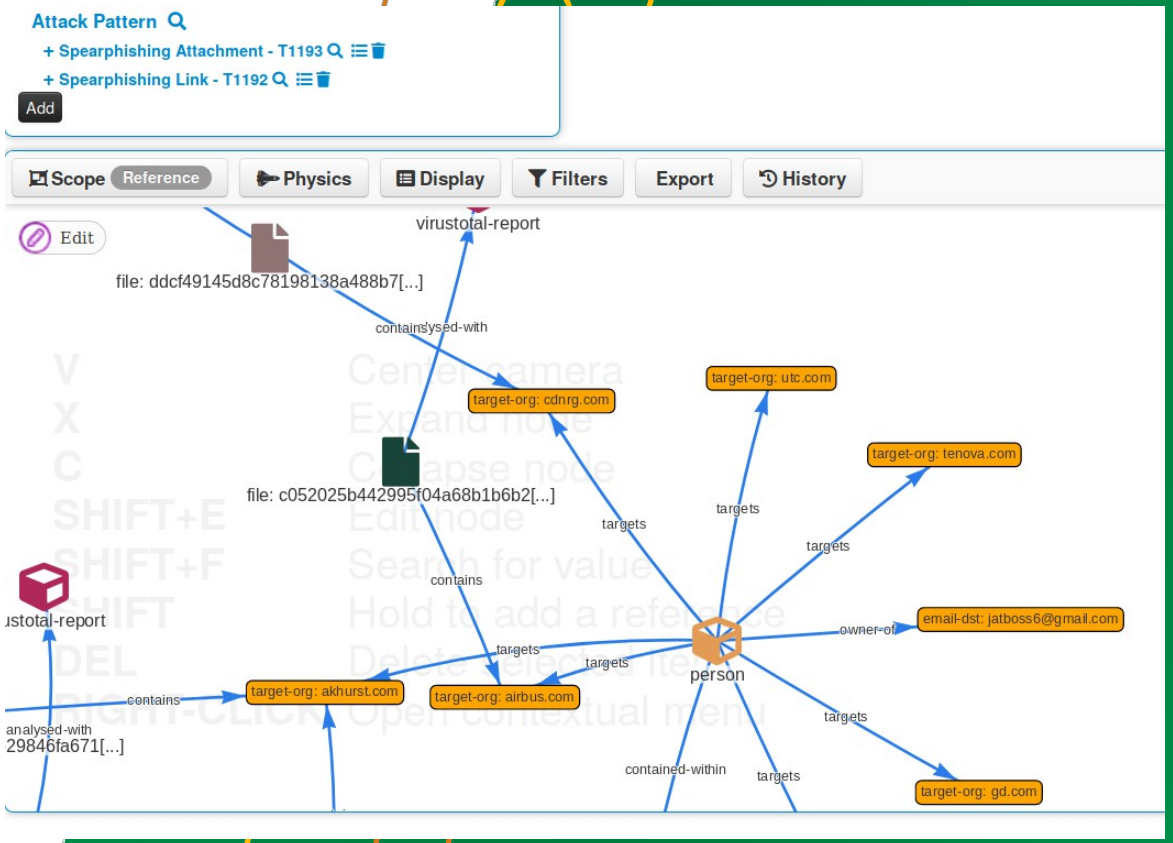
Piattaforma open source di intelligence sulle minacce.

Può eseguire automaticamente le regole di Snort, Suricata, Bro, Zeek IDS.

Può esportare in STIX, OpenIOC, testo o csv.

Sono disponibili librerie Python, Ruby, Go e HTTP.

Può integrarsi con ElasticSearch/Logstash/Kibana (ELK).



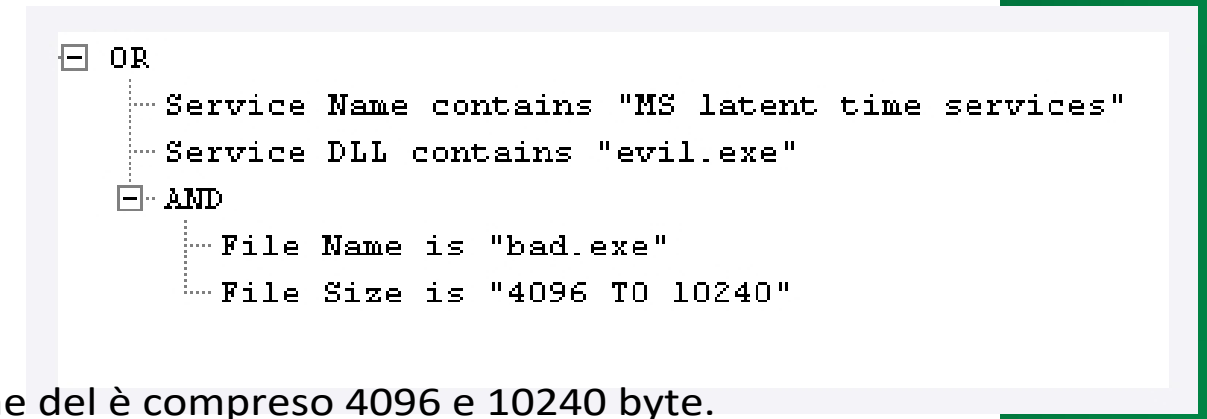
APERITIVO

Un altro standard aperto per la condivisione di informazioni su attività dannose.

Il nome di un servizio è "Servizi a tempo latente MS".

- **o**

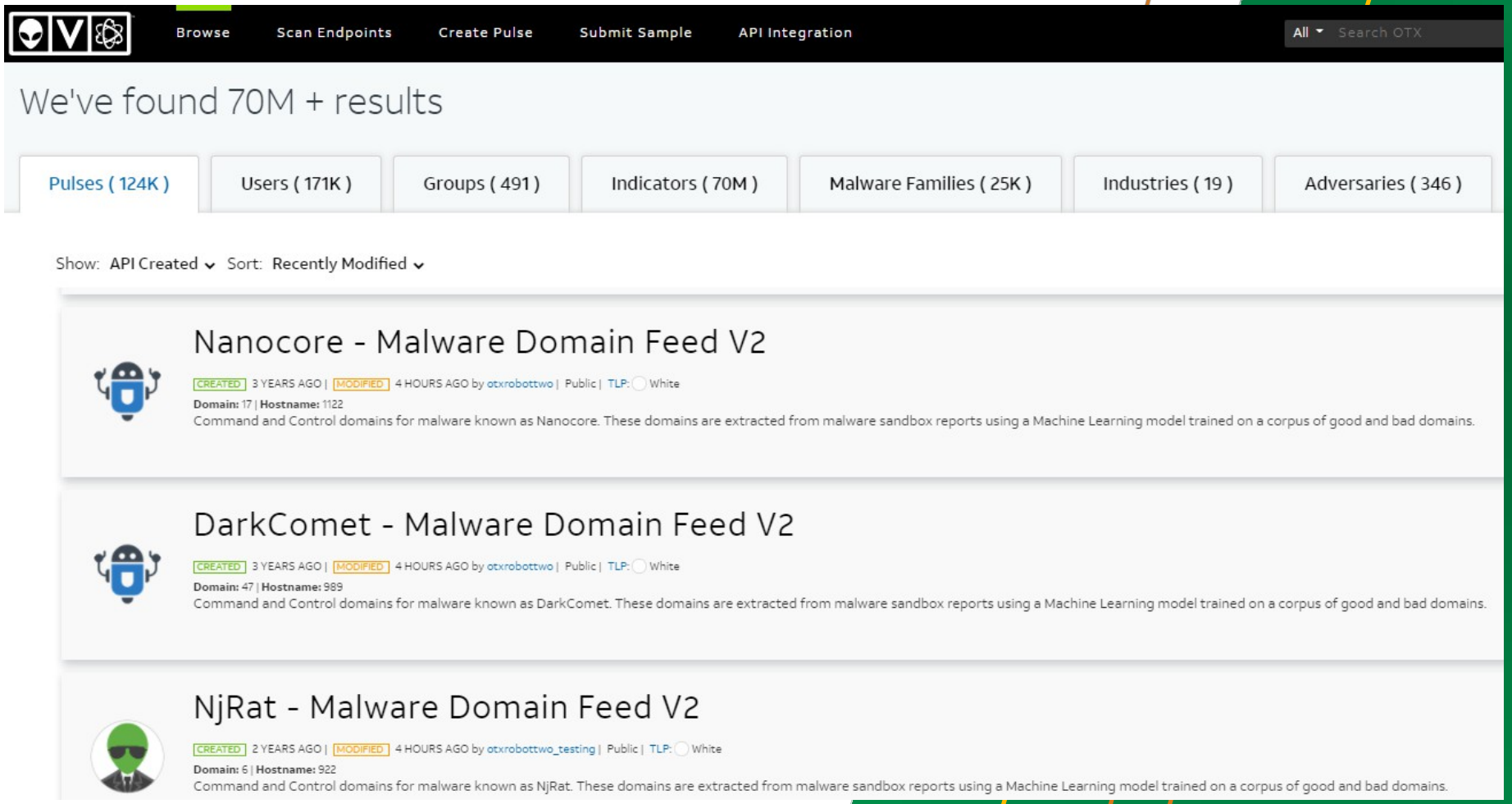
Il nome del ServiceDLL contiene "evil.exe".



- **o**

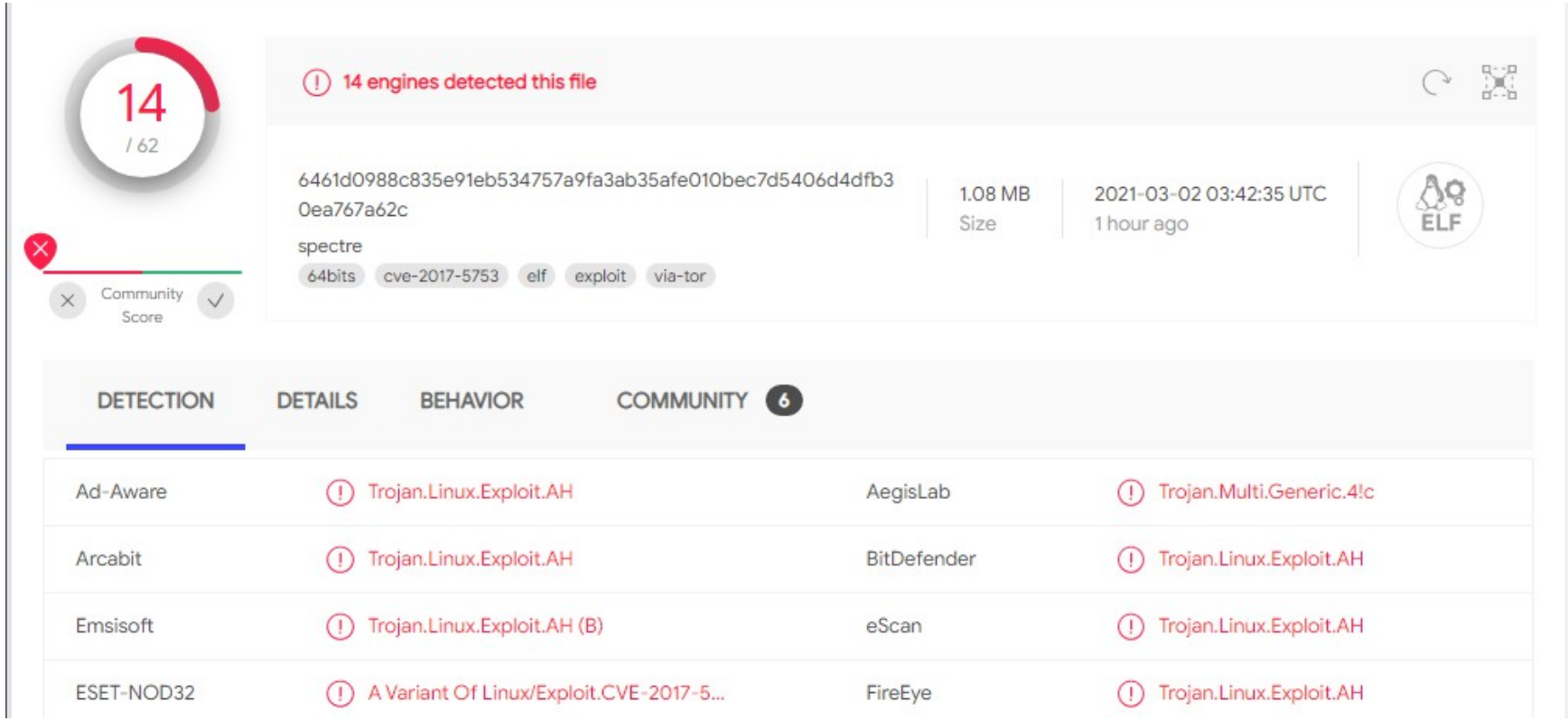
Il nome del file è "bad.exe" **E** l'attributo della dimensione del è compreso 4096 e 10240 byte.

AlienVault Scambio aperto di minacce (OTX)

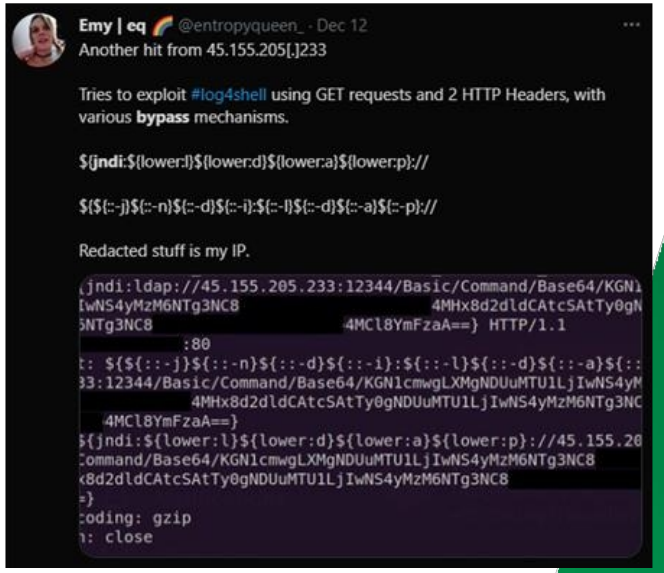


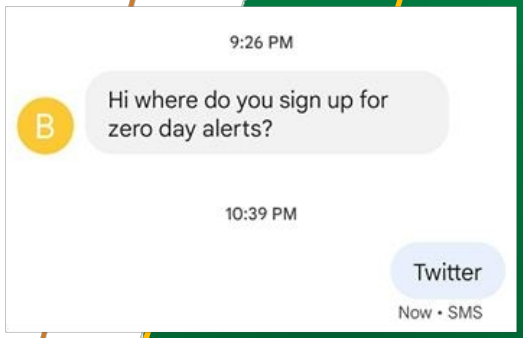
Virustotal

Caricate qualsiasi file e VirusTotal lo confronterà con una serie di strumenti antivirus tra i migliori al mondo.



Social media





Fonti di intelligence

Fonti di intelligence

Caccia alle minacce

Che cos'è la caccia alle minacce?

Definire cosa si intende per caccia alle minacce

Ha qualche esperienza?

Vi state interfacciando con i cacciatori di minacce, ad es. fornendo loro informazioni?

Come vengono rilevate le nuove minacce nel vostro ambienti? Attivi o passivi?

Caccia alle minacce

L'arte di cercare nelle reti e nei sistemi individuare e isolare le minacce.

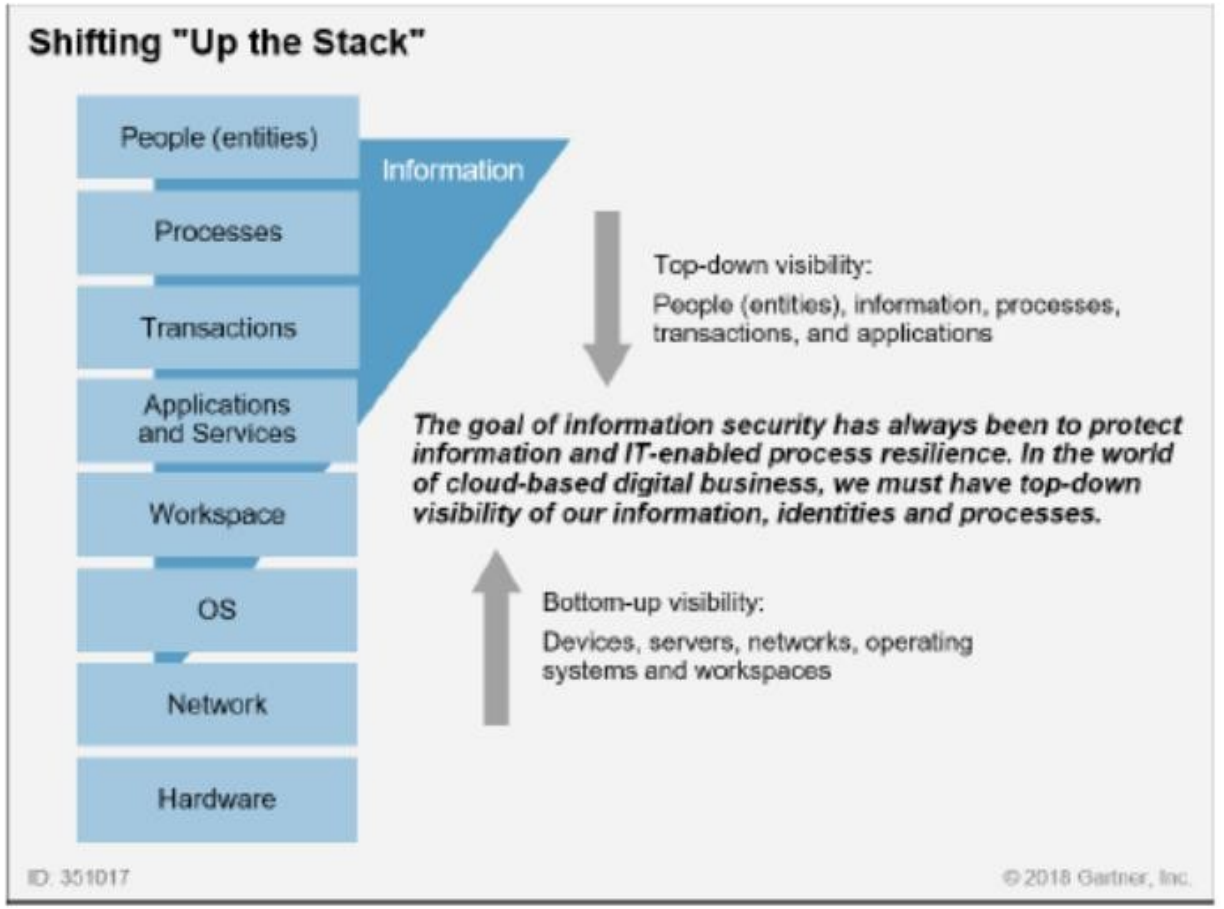
- È una misura proattiva
- Si rivolge alle minacce avanzate
- Presuppone la violazione delle soluzioni di sicurezza in atto.

La caccia alle minacce viene tipicamente effettuata senza una richiesta esplicita di indagine.

- Fatto senza una vera causa
- Le cacce si ripetono

La caccia alle minacce spesso si basa sul monitoraggio della sicurezza, ma non è la stessa cosa.

Perché la caccia alle minacce?



Un po' di vocabolario

Dwell Time - Numero di giorni in cui un aggressore è presente in un sistema vittima prima di essere rilevato.

Ipotesi - Una domanda di ricerca che può posta all'inizio caccia - Successivamente si valutano i dati e gli indicatori che supportano o meno l'ipotesi.

TTP: tattiche, tecniche e procedure.

Vantaggi

In base al principio di base, cerchiamo gli aggressori che hanno avuto successo, in modo da poterli trovare.

- La supervisione completa di un'organizzazione tipica non è possibile a questo punto.

Migliora le capacità di rilevamento

- Affina in modo permanente le competenze
- Supporta il rilevamento precoce di potenziali vettori di attacco
- Aumenta la consapevolezza della superficie di attacco

Migliora la raccolta dei dati

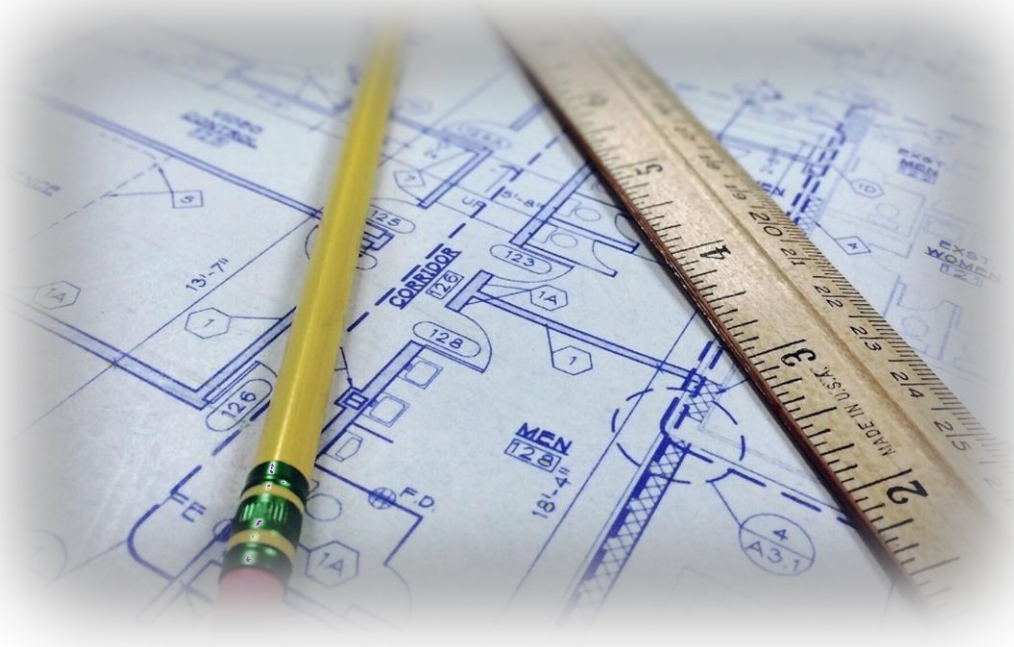
Piani di risposta agli incidenti informatici

Approccio strutturato alla preparazione

- Quali sono le misure da e le informazioni da raccogliere?
- Cosa fare in caso di incidente?
- Informazioni di contatto
- Sulla base dell'analisi dei rischi e della BIA.
- Diverse forme di attacco

Esigenza

- Analisi approfondita
- Manutenzione regolare
- Sensibilizzazione e formazione



Prontezza di risposta agli incidenti informatici

Valutare la prontezza di risposta agli incidenti informatici

- Esistono approcci strutturati

Un buon esempio:

- Liste di controllo sviluppate dal governo australiano
- Semplice e utilizzabile

https://www.cyber.gov.au/sites/default/files/2022-07/ACSC%20Cyber%20Incident%20Readiness%20Checklist_A4.pdf

Prontezza di risposta agli incidenti informatici

☐	Up-to-date hard copy versions of the Cyber Incident Response Plan and playbooks are stored in a secure location (in case of electronic or hardware failure) and are accessible to authorised staff members.
☐	Specific playbooks to supplement the Cyber Incident Response Plan have been developed, that define step-by-step guidance for response actions to common incidents, and roles and responsibilities.
☐	A Cyber Incident Response Team (CIRT) and a Senior Executive Management Team (SEMT) – or equivalents - have been formed to manage the response, with approved authorities.
☐	All relevant IT and OT Standard Operating Procedures (SOPs) are documented and have been reviewed or tested in an exercise to ensure they remain current and responsible personnel are aware of their roles, responsibilities and processes.
☐	Arrangements for service providers, including cloud and software as a service, to provide and retain logs have been established and tested to ensure these include useful data and can be provided in a timely manner.
☐	Log retention for critical systems have been configured adequately and tested to confirm that they capture useful data. Refer to the ACSC publications including Windows Event Logging and Forwarding for specific guidance.

Il modello di maturità della caccia alle minacce

Descrive

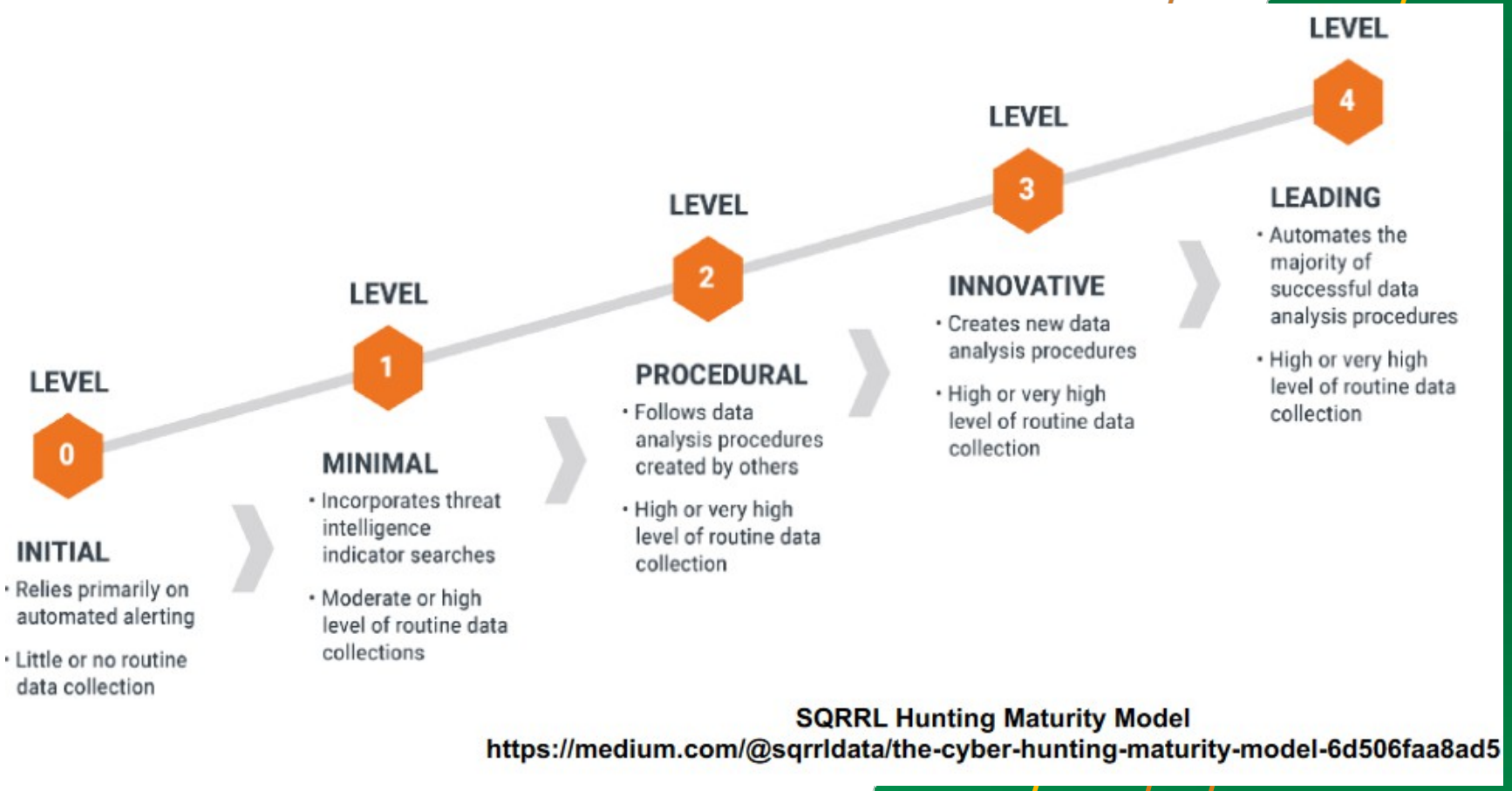
- Livelli di sviluppo
- Possibilità associate

Suddiviso in tre livelli da 0 a 4 In base a tre fattori

chiave

- Quantità e qualità dei dati
- Le modalità di visualizzazione e analisi delle diverse fonti di dati
- Automazione dell'arricchimento dei dati con le fonti, ad Threat Intelligence o DNS.

Il modello di maturità della caccia alle minacce



SQRRL Hunting Maturity Model
https://medium.com/@sqrrldata/the-cyber-hunting-maturity-model-6d506faa8ad5

Il modello di maturità della caccia alle minacce

I livelli più alti non possono essere raggiunti solo con gli strumenti.

- Richiede ai team di trovare nuovi attori delle minacce
- Si basa sulla creatività umana e sul pensiero fuori dagli schemi.

  scatola
- In combinazione con l'automazione delle attività non creative e l'acquisizione e l'arricchimento delle informazioni di base.
- Lavorare in gruppo

Il modello di maturità può essere utilizzato come tabella di marcia per migliorare i team di caccia alle minacce.

KPI per la caccia alle minacce

Gli indicatori di prestazione chiave (KPI) aiutano ad analizzare e visualizzare il successo di un sistema di caccia alle minacce.

Le metriche possono supportare i decisori

- come meccanismo di avvertimento che le cose vanno male
- nel prendere la decisione giusta grazie ai risultati effettivi paragonabili a quelli teorici

Metriche come queste non dovrebbero mai essere utilizzate

- Come unico meccanico per la remunerazione
- Per confrontare diversi analisti

KPI per la caccia alle minacce

KPI basati sullo sforzo

- Cosa abbiamo fatto per migliorare le nostre cacce?

KPI basati sul successo

- Come riusciti a portare a termine le nostre battute di caccia?

KPI basati sulla gestione

- Come viene integrato il Threat Hunting nell'organizzazione?

Alcuni esempi nelle seguenti diapositive

KPI basati sullo sforzo

Numero di Caccia alle minacce completate

Numero di fonti di dati collegate

Numero di analisti coinvolti dopo una caccia alle minacce completata Tempo

medio dedicato ad una caccia alle minacce

Numero di cacce alle minacce incomplete

Numero di ipotesi che sono state (non) trovate dal modello di caccia alle minacce utilizzato

Numero di risultati non dannosi per categoria (rischio di sicurezza, vulnerabilità di registrazione, autorizzazioni utente errate, errata configurazione dello strumento, ecc.)

KPI basati sul successo

Riduzione del numero di falsi positivi

Numero e tipo di riscontri (dannosi, non dannosi)

Numero di risultati non dannosi per categoria (rischio di sicurezza, vulnerabilità di registrazione), permessi utente non corretti, errata configurazione dello strumento, ecc.)

Ridurre le dimensioni del record filtrando le attività non dannose rilevate Numero di nuove tecniche di attacco rilevate

Numero di nuovi rilevamenti generati

Tempo di permanenza dei risultati (tempo trascorso fino al rilevamento)

Numero di incidenti rilevati in modo proattivo rispetto a quelli rilevati in modo reattivo - Gravità degli incidenti

Il numero di sistemi compromessi, non protetti o mal configurati individuati

Numero di risultati risolti per gravità

KPI basati sulla gestione

Budget per la gestione della caccia alle minacce

Modello di dati e processo di garanzia della qualità dei dati stabiliti

Tutte le cacce alle minacce sono guidate da informazioni sulle minacce rilevanti per l'organizzazione. Il team Threat Hunting lavora a stretto contatto con altri team.

implementati costantemente nuovi meccanismi di rilevamento.

Tutte le cacce alle minacce effettuate sono adeguatamente documentate.

Tutti i rilevamenti generati sono adeguatamente automatizzati. Miglioramenti apportati al processo di ricerca delle minacce

Sintesi

- Una minaccia è una combinazione di capacità, opportunità e intento malevolo.
- Gli avversari hanno molte motivazioni e possono provenire da qualsiasi parte: dall'interno dell'organizzazione vittima o da una potenza straniera.
- Esistono molti modi per catalogare e condividere le informazioni sulle minacce utilizzando strumenti open-source: STIX, MISP, OpenIOC
  - Alcuni di questi strumenti forniscono interfacce di programmazione per automatizzare le configurazioni di firewall e IDS/IPS.
- Esistono informazioni pubblicamente disponibili da parte di organizzazioni del settore pubblico e privato.
  - Aziende di sicurezza informatica, organizzazioni che si occupano di big data, enti governativi, ecc.

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Co-funded by the European Union

Co-funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or HADEA. Neither the European Union nor the granting authority can be held responsible for them.

Project Agreement no. 101083594

Grazie

Si prega di inviare tutte le domande a:
Stefan SchauerStefan.Schauer@ait.ac.at
Abdelkader Shaaban,
abdelkader.Shaaban@ait.ac.at