



V CONFERENZA NAZIONALE



Foto Informatica

GT 50

Posteitaliane



Profice



Texi Solutions

Cybersecurity: stato dell'arte, sistemi di difesa e resilienza

Roma, Palazzo Wedekind, Piazza Colonna 366, 4 aprile 2022

Cyber Threat Intelligence

Corrado Aaron Visaggio

What is Cyber Intelligence and why do you need it?

E' l'analisi di dati attraverso l'uso di strumenti e tecniche per generare **informazione utile** ad individuare (e contrastare) le minacce (emergenti) che possono riguardare un'organizzazione

Essa serve ad identificare, contrastare e prevenire gli attacchi

Senza la comprensione delle vulnerabilità, degli indicatori, degli attori e di come un attacco è condotto, non è possibile contrastare né prevenire gli attacchi.

Incident Management Cycle

CHECK

If No, go to Remediate and take further actions
If Yes, start to post-incident evaluate and inform relevant parties and continue to Observe

Has the deviant behavior, message, appearance disappeared?

Are there triggers or alerts that justify incident response?

Extract contextual information: What is the deviant behavior, message, appearance? Where does it occur? Verify if event is known false positive or related to planned activities (test, audit, changes,...)

OBSERVE

Find related events (e.g., by checking functional mailbox)
Check if event is related to an already open incident.
What is working as expected?

Determine whether an alert is in scope or not
If Yes: Continue with Triage
If No: Determine to which stakeholder alert belongs and Inform relevant stakeholder

REMEDIATE

Check if expected effects are the same as the actual effects observed
If Yes: Continue to Check

If expected effects are not the same as the actual effects observed, go to Investigate and select a different cause and take actions by referring to cheat sheets or Quick Reference Cards for that specific cause

Take actions to remediate for a specific incident (cause)

Note down expected effects of actions. Note down actual effects observed.

POST-INCIDENT EVALUATE

Know what has happened, learn the right lessons, successes as well as failures, adjust standing procedures and playbooks.

What are unexpected technical observations?

What are expected technical observations?
Get more contextual information & find online references

TRIAGE

Declare true positive, suspected, false positive, or near miss

If True Positive or Suspected: Continue to Investigate
If False Positive or Near Miss: Close ticket

CONTAIN

Inform other relevant parties within or outside the organization of the incident and mitigating measures

Verify effectiveness of containment/mitigation, if Yes: Continue with remediate

Prioritize the security incident. If the security incident has a high priority, create containment/mitigation plan and escalate to higher level management
Take mitigating measures to contain the most likely cause listed

What may have caused parts of the network, services, systems, website, or applications to not work as expected?

What parts of the network, services, systems, website, or applications work as expected?

INVESTIGATE

Involve and communicate with asset owner/management and technical contact(s)

List cause(s) (e.g. DDoS, data leakage, etc.) and continue to Contain

TTP (Tactics, Techniques and Procedures) for Threat Data Collection

OSINT: motori di ricerca, Web services, Website Footprint, Emails, Whois Lookup, DNS Interrogation

HUMINT: Social Engineering, Interviste

CCI: honeypots, Passive DNS Monitoring, Pivoting Off Adversary's Infrastructure, Malware Sinkholes, YARA

IoC: evidenza sugli indicatori di attacco

Malware Analysis: evidenza derivante dall'analisi di agenti malevoli

Advanced Persistent Threats (APT)

E' un attacco nel quale un utente non autorizzato ottiene accesso ad una rete e rimane al suo interno per un periodo di tempo lungo

Kill Chain

E' una serie di passi che tracciano le fasi di un attacco dalla reconnaissance fino all'esfiltrazione.

Threat Intelligence types

Strategic Threat Intelligence

Fornisce una panoramica delle minacce che riguardano l'organizzazione.
Vulnerabilità e rischi in termini di: azioni preventive, attori, severità dei rischi

Tactical Threat Intelligence

Dettagli su TTP e serve a comprendere i vettori di attacco
Fornisce le informazioni per costruire una strategia difensiva
Serve a rafforzare i controlli esistenti ed i meccanismi di difesa.

Technical Threat Intelligence

Si focalizza su evidenze specifiche di un attacco
Ricerca di indicatori di compromissione

Operational Threat Intelligence

Fornisce dettagli sulla natura, la finalità, le tempistiche e le modalità di un attacco specifico.
Realizzata per lo più attraverso infiltrazione.

Golden Rules for Implementing a Cyber Threat Intelligence Program



Create a plan



Know who all need the Intelligence



Involve the right people



Implement the right TTP (Tools, Techniques, and Procedures)



Understand the difference between Threat Data and Threat Intelligence



Integrate with the Organization's Security Technologies



Communication

Challenges

Tempestività.

Molti malware sono presenti sulle piattaforme pubbliche (anyrun, Malware Bazaar, VirusTotal) 30/40 giorni prima del loro effettivo utilizzo.

Attendibilità.

Molti IoC devono essere verificati (tipicamente IP e url).

Pluralità di Piattaforme.

Si può usare Twitter? Ed il Darkweb?

Secondo l'ENISA vi sono 80 iniziative ed organizzazioni e più di 50 CSIRT coinvolti nel CTI sharing a livello Europeo

Convergere verso una tipologia universale di scambio.

STIX-TAXII, OpenTPX, MAEC, IODEF, VERIS

Automazione della raccolta.

Conclusions

Passare da una difesa di tipo reattivo ad una di tipo preventivo e adattivo

Avere CTI efficace ed efficiente

La CTI deve essere verticalizzata sui settori di attività

La CTI deve integrarsi con l'infrastruttura di controllo e di difesa

Passare da un approccio di tipo statico ad uno di tipo dinamico