V CONFERENZA NAZIONALE

Partenariato cybersecurity privacy

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

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

01 Create a plan

02 Know who all need the Intelligence

03 Involve the right people

04 Implement the right TTP (Tools, Tecniques, and Procedures)

05 Understand the difference between Threat Data and Threat Intelligence

06 Integrate with the Organization's Security Technologies

07 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 shraing 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