Cyber Threat Intelligence (CTI) for Health

CSP006

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Example Cyberattack Pt.1

Cyber Attack on Healthcare Organization

Example for CTI Pt. 1

A healthcare organization has been targeted by a cyber attack aimed at stealing patient data from its electronic health record (EHR) system. The attack, initiated through a phishing email containing a malicious attachment, resulted in the compromise of several user accounts within the organization's network.

1. **Initial Indicator Sharing:** Upon discovery of the phishing email and suspicious attachments, the healthcare organization's security team uploads relevant indicators of compromise (IOCs) to their local instance of MISP. These IOCs include: a) Malicious email sender addresses, b) Email subject lines and content, c) Filename and hash of the malicious attachment.
2. **Threat Analysis and Correlation:** The MISP platform automatically correlates the uploaded IOCs with existing threat intelligence feeds and databases. This process helps identify known malware signatures, malicious domains, and IP addresses associated with similar cyber attacks targeting healthcare organizations globally.
3. **Triage and Prioritization:** Based on the severity and impact of the cyber attack, the healthcare organization's security analysts prioritize actionable IOCs for further investigation and response. This may involve flagging high-risk indicators, such as compromised user accounts or network connections to known malicious IP addresses, for immediate remediation.

Example Cyberattack Pt.2

Cyber Attack on Healthcare Organization

4. Information Sharing and Collaboration: Leveraging MISP's information sharing capabilities, the healthcare organization securely shares relevant threat intelligence data, including IOCs and analysis reports, with trusted external partners such as other healthcare providers, government agencies, and cybersecurity industry groups. This collaborative approach enhances situational awareness and enables a coordinated response to the cyber attack across the healthcare sector.

5. Enhanced Detection and Prevention: By integrating MISP with their security infrastructure, the healthcare organization implements automated threat detection and prevention measures based on shared threat intelligence. This includes updating firewall rules, intrusion detection systems (IDS), and endpoint security solutions to block malicious traffic, quarantine compromised systems, and prevent further spread of the cyber attack within their network.

Outcome

Through proactive threat intelligence sharing and collaboration enabled by MISP, the healthcare organization effectively mitigates the cyber attack, containing its impact and preventing unauthorized access to patient data. By leveraging shared threat intelligence, the organization strengthens its cyber resilience and enhances its ability to defend against future cyber threats targeting the healthcare sector.

Use Case #1: Analysis

Use Case #1 - Cyber Threat Intelligence Analysis

MISP for Analysts

- Use MISP to collect, analyze, and share information about cyber threats. MISP serves as a central repository for collecting and sharing intelligence across organizations and industries.
- Once analysis is complete, analysts distribute information using MISP's advanced sharing features.

- **In Healthcare:** Analysts gather threat intelligence manually or automatically using MISP's ingestion capabilities. MISP provides enrichment integrations to provide additional context to events automatically.
- IOCs can be pushed to security solutions to be blocked.
- Reports can be generated and shared with executives.
- MISP events can be automatically shared with the wider cybersecurity community.

Use Case #2: Research

Use Case #2 - Security Research

MISP for Researchers

- Security researchers use MISP to collect and share information about vulnerabilities, exploits, and threats. MISP's integrations and support for CTI taxonomies/frameworks allow researchers to use a common language when describing threats.

- **In Healthcare:** Researchers investigate new forms of malware and list IOCs, MITRE ATT&CK techniques used, and CVEs exploited.
- Shared information helps organizations block IOCs, write detections for specific MITRE ATT&CK techniques, and prioritize patching CVEs.
- IOCs such as file hashes, IP addresses, and domain names are essential for identifying and blocking malicious activity associated with the ransomware strain.

Use Case #3: Incident Response

Use Case #3 - Incident Response

MISP for Response

- Incident responders use MISP to share information about incidents they have experienced or are resolving. MISP's correlation engine is ideal for sharing incident data as it allows responders to quickly see related incidents.
- **In Healthcare:** Responders share information about new threat actors, malware strains, phishing campaigns, etc.
- Correlation engine helps responders quickly identify related incidents and take appropriate actions to minimize impact.
- Incident responders use MISP to share details of the phishing campaign, including email sender addresses, malicious attachments, and compromised user accounts.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

Please send all questions to:
stylianos.karagiannis@pdmfc.com