Cyber Threat Intelligence (CTI) for Health

CSP006

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Threat Intelligence

Practical Aspects of CTI

Threat Indicators (IOC)

Healthcare organizations can use CTI to monitor for threat indicators such as suspicious network traffic, abnormal user behavior, and malware signatures in DICOM, PACS, HL7 FHIR, and Active Directory logs.

- **Analyzing Threat Data:** CTI enables healthcare security teams to analyze threat data and identify patterns or trends that may indicate potential security incidents or vulnerabilities within their systems.
- **Incident Response and Mitigation Strategies:** With CTI, healthcare organizations can develop robust incident response and mitigation strategies to effectively respond to and mitigate cyber threats, including ransomware attacks, data breaches, and insider threats.
- **Detection of Malware Targeting DICOM Systems:** CTI can help healthcare organizations detect and mitigate malware targeting DICOM systems by monitoring for suspicious file transfers, unauthorized access attempts, and unusual network activity.
- MISP facilitates the sharing and analysis of threat intelligence data among healthcare security professionals. Practical aspects of CTI include monitoring for threat indicators, analyzing threat data, and implementing incident response and mitigation strategies.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

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