Critical Infrastructure and Security for Health

CSP008

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Introduction

Healthcare Domain

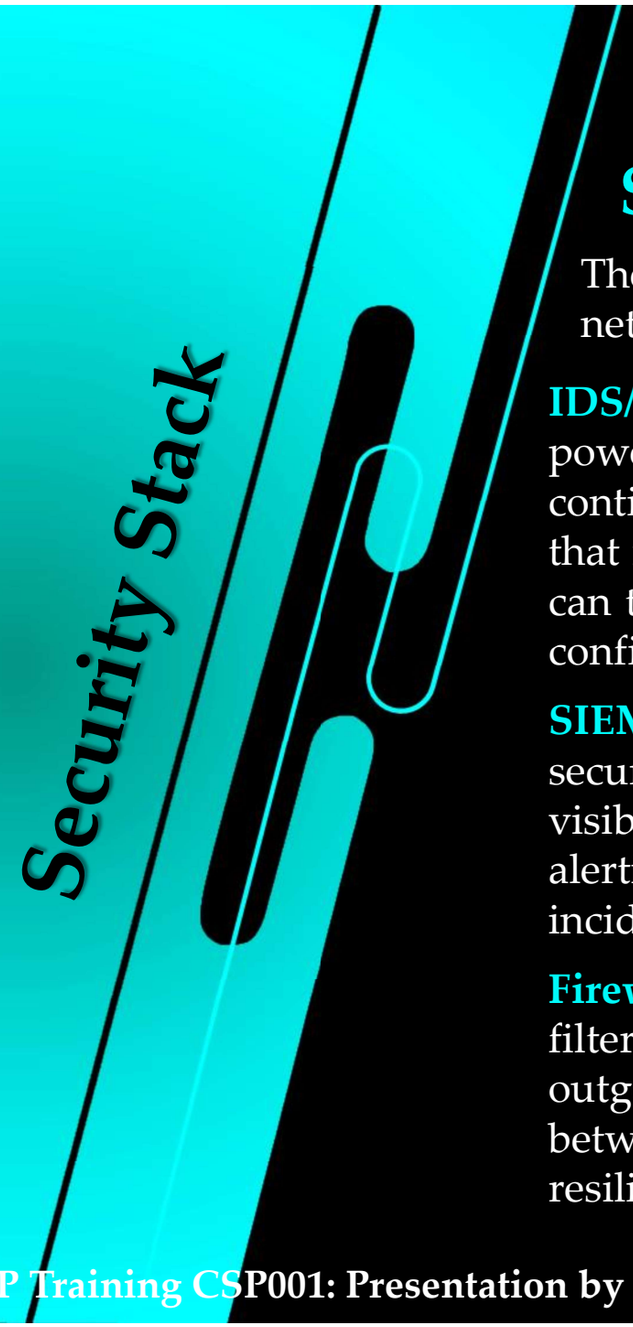
In the healthcare environment, assets like the Windows Domain Controller, Health Information System, Laboratory Information System, Picture Archiving and Communication System, DICOM-Enabled Modality, and Windows Host are interconnected via Ethernet VLAN, facilitating seamless data exchange and enabling critical functions such as authentication, patient record management, diagnostic imaging, and general data processing.

Assets and Protocols in Healthcare

- **DICOM (Digital Imaging and Communications in Medicine):** DICOM is a standard for transmitting, storing, and sharing medical imaging data such as X-rays, MRIs, and CT scans. It is widely used in healthcare for the exchange of medical images between different systems and facilities.
- **PACS (Picture Archiving and Communication System):** PACS is a system used for storing, retrieving, and distributing medical images. It integrates with DICOM and provides healthcare professionals with access to patient images and related data.
- **HL7 FHIR (Health Level Seven Fast Healthcare Interoperability Resources):** HL7 FHIR is a standard for exchanging electronic healthcare information. It enables interoperability between different healthcare systems and facilitates the exchange of patient data such as medical records, lab results, and clinical observations.
- **Domain Controller - Active Directories:** Active Directory is a directory service developed by Microsoft for managing user identities, permissions, and access to resources within a network. In healthcare organizations, Active Directory is used to manage user accounts, access controls, and authentication.

Healthcare Security

Security Stack



The security stack in healthcare comprises essential components aimed at fortifying the network infrastructure and protecting sensitive patient data.

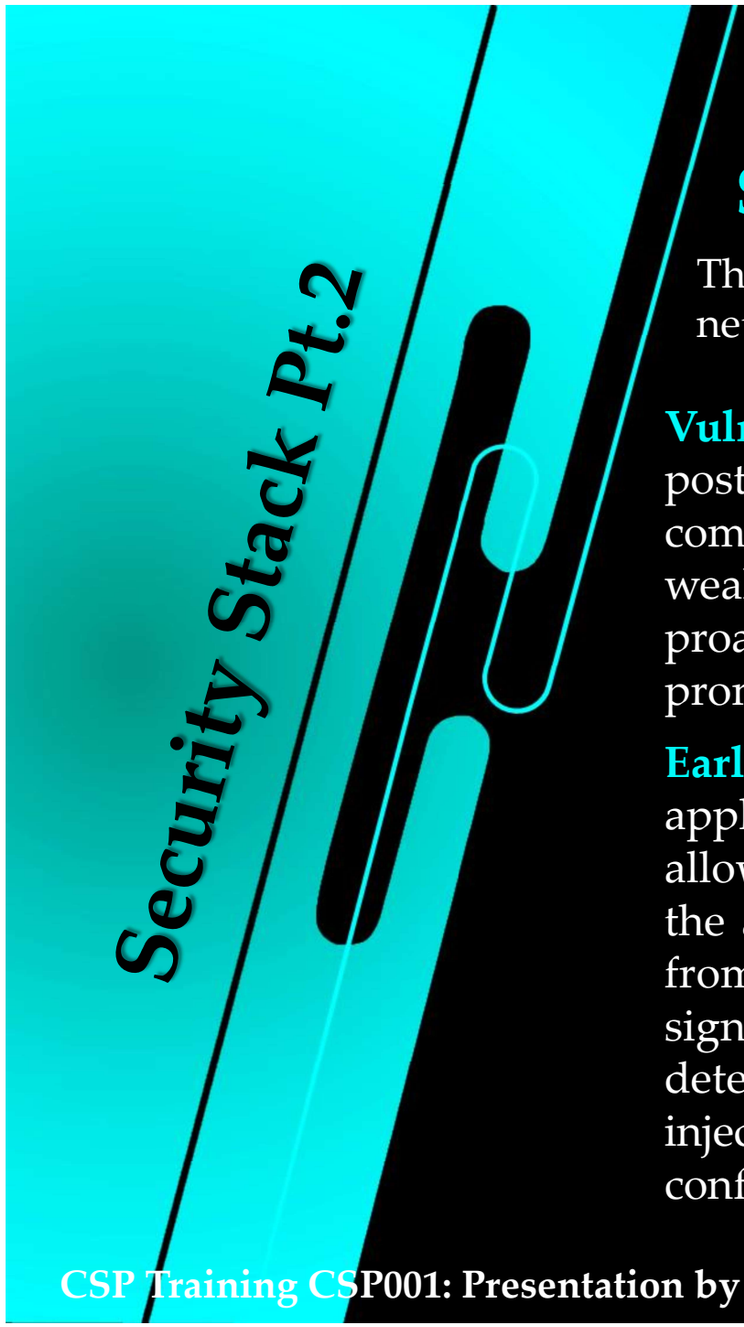
IDS/IPS (Intrusion Detection System/Intrusion Prevention System): The IDS/IPS, powered by Suricata, serves as a vigilant guardian of the healthcare network. It continuously monitors network traffic, analyzing it for suspicious patterns or anomalies that may indicate a potential security threat. In the event of a detected threat, the system can take proactive measures to prevent it from compromising the network's integrity or confidentiality.

SIEM (Security Information and Event Management): It aggregates and correlates security event data from various sources across the network, providing real-time visibility into potential threats or suspicious activities. With advanced analytics and alerting capabilities, the SIEM empowers security teams to respond swiftly to security incidents, minimizing potential impact.

Firewall: It fortifies the healthcare network's perimeter defenses. With robust rule-based filtering capabilities, the firewall will enforce security policies, regulate incoming and outgoing traffic, and thwart unauthorized access attempts. By creating a secure barrier between the internal network and external threats, the firewall enhances the overall resilience of the healthcare infrastructure.

Healthcare Security

Security Stack Pt.2



The security stack in healthcare comprises essential components aimed at fortifying the network infrastructure and protecting sensitive patient data.

Vulnerability Assessment: Tools like Velociraptor, empowers proactive security posture management within the healthcare environment. By conducting comprehensive scans and assessments, Velociraptor identifies potential security weaknesses or vulnerabilities in systems, applications, and configurations. This proactive approach enables security teams to prioritize and address vulnerabilities promptly, minimizing the risk of exploitation and data breaches.

Early Detection of Vulnerabilities: SAST tools analyze the source code of applications statically, meaning they inspect the code without executing it. This allows them to detect vulnerabilities early in the development lifecycle, even before the application is deployed. Early detection is crucial in preventing vulnerabilities from being introduced into production environments, where they can pose significant risks to patient data and system integrity. SAST tools are designed to detect a wide range of common security flaws, such as injection vulnerabilities (SQL injection, XSS), authentication issues, insecure data storage, and insecure configurations.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

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