Critical Infrastructure and Security for Health

CSP008

PRESENTATION BY: STYLIANOS KARAGIANNIS (PDMFC, PORTUGAL)

Cyberattack Scenarios

Lockbit

Lockbit ransomware infiltrates the healthcare network through phishing emails or unpatched systems, targeting critical assets such as the Windows Domain Controller (DC) and Windows Hosts. Once inside, Lockbit encrypts sensitive data, rendering it inaccessible, and demands ransom payment for decryption keys.

Incidents: Data encryption, disruption of services, potential data loss, extortion demands.

IDS/IPS: Detects anomalous network activity associated with ransomware encryption processes, triggering alerts for immediate investigation and response.

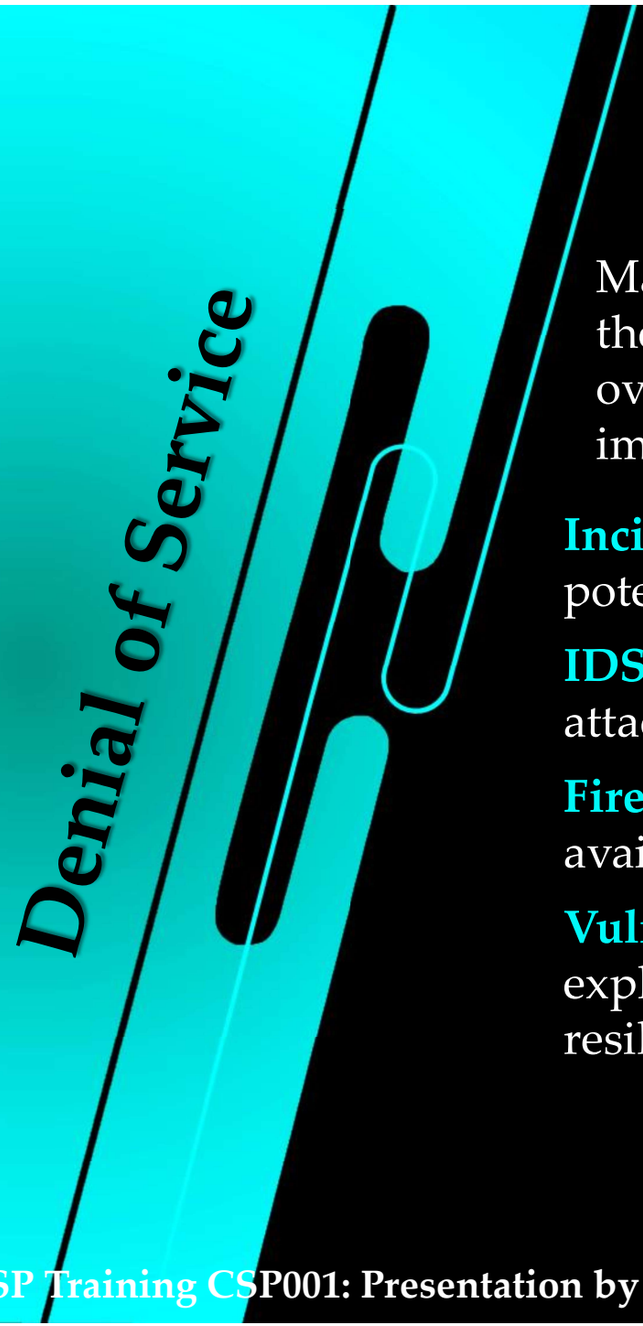
SIEM: Centralizes logs and alerts from affected systems, enabling security teams to correlate events and respond swiftly to the incident.

Firewall: Blocks unauthorized network connections and prevents lateral movement of ransomware within the network, containing the spread of infection.

Vulnerability Assessment: Identifies and patches vulnerabilities exploited by ransomware, reducing the risk of future infections and data breaches.

Cyberattack Scenarios Pt.2

Denial of Service



Malicious actors launch a distributed denial of service (DDoS) attack against the Picture Archiving and Communication System (PACS), flooding it with an overwhelming volume of traffic. This results in the unavailability of medical imaging data and disrupts healthcare services.

Incidents: Service disruption, denial of access to medical imaging data, potential impact on patient care.

IDS/IPS: Detects and mitigates abnormal traffic patterns indicative of a DoS attack, preventing the system from becoming overwhelmed.

Firewall: Filters and blocks malicious traffic aimed at PACS, ensuring its availability and integrity.

Vulnerability Assessment: Identifies vulnerabilities in PACS that could be exploited in DoS attacks, allowing for preemptive measures to strengthen resilience.

Thank you

Presenter: Stylianos Karagiannis (PDMFC, Portugal)

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