Topic 5 Discussion 1

Discuss the systems/methods/software/services required to detect a breach or an intrusion. Discuss elements necessary within the security architecture to isolate corporate assets should an intrusion occur (e.g., ransomware).

Hello Class,

Detecting a breach or intrusion is critical for maintaining the integrity and security of corporate assets. Organizations typically employ a combination of systems, methods, software, and services to achieve this. Key components include:

Intrusion Detection Systems (IDS) - These systems monitor network traffic for suspicious activity and known threats. They can be host-based or network-based, providing real-time alerts when potential breaches are detected.

Security Information and Event Management (SIEM) - SIEM solutions aggregate and analyze security data from across the organization, enabling the detection of anomalies and potential threats through correlation of events.

Endpoint Detection and Response (EDR) - EDR tools focus on monitoring and responding to threats on endpoints, such as workstations and servers. They provide visibility into endpoint activities and can automate responses to detected threats.

Vulnerability Management Tools - Regularly scanning for vulnerabilities helps organizations identify and remediate weaknesses before they can be exploited by attackers.

Threat Intelligence Services - These services provide organizations with up-to-date information on emerging threats and vulnerabilities, allowing them to proactively defend against potential attacks.

In terms of security architecture, several elements are essential for isolating corporate assets during an intrusion, particularly in the case of ransomware:

Network Segmentation - Dividing the network into segments can limit the spread of malware and contain breaches to specific areas, protecting critical assets(Ilyin, 2025).

Access Controls - Implementing strict access controls ensures that only authorized personnel can access sensitive data and systems, reducing the risk of insider threats and unauthorized access.

Data Backup and Recovery Solutions - Regularly backing up data and having a robust recovery plan in place is crucial for minimizing the impact of ransomware attacks(Benmalek, 2024). This allows organizations to restore data without paying ransoms.

Incident Response Plan - A well-defined incident response plan outlines the steps to take in the event of a breach, including containment, eradication, and recovery processes. This plan should be regularly tested and updated.

User Education and Awareness Training - Educating employees about security best practices and the risks of phishing and other social engineering attacks can significantly reduce the likelihood of successful intrusions(CISA, 2023).

In summary, a multi-layered approach combining advanced detection systems, proactive security measures, and a strong incident response framework is essential for effectively managing and mitigating the risks associated with breaches and intrusions, especially ransomware attacks.

References:

Benmalek, M. (2024). Ransomware on cyber-physical systems: Taxonomies, Case studies, Security gaps, and Open Challenges. *Internet of Things and Cyber-Physical Systems*, *4*, 186–202. https://doi.org/10.1016/j.iotcps.2023.12.001

CISA. (2023, May). *I’ve Been Hit By Ransomware!* Www.cisa.gov. https://www.cisa.gov/stopransomware/ive-been-hit-ransomware

Ilyin, Stepan. (2025, July 17). *Ransomware Detection*. Wallarm.com; Wallarm. https://www.wallarm.com/what/ransomware-detection