Armaan Shamsaasef

Gap Analysis

Notes: Gap Analysis (SY0-701 - 1.2)

Core Concept: A Gap Analysis is a formal assessment that compares an organization's current security posture ("where we are") against a desired set of standards, regulations, or best practices ("where we want to be"). The goal is to identify the "gaps" that need to be addressed.

The Purpose & Process

- Goal: To find the differences between the current state and a target state.
- Outcome: A report that identifies deficiencies and provides a roadmap for implementing controls to close those gaps.
- Process:
    1. Define the desired state (the standard or framework).
    2. Document the current security state.
    3. Compare the two to identify gaps.
    4. Create a plan to address the gaps.

Key Examples of Target Standards (The "Where we want to be")

Professor Messer highlights that a gap analysis can be performed against various benchmarks:

- Industry Standards: PCI DSS, HIPAA, ISO 27001.
- Government Regulations: NIST Cybersecurity Framework, NIST SP 800-53.
- Internal Policies: The company's own security policy.

Detailed Examples from the Video

The video provides a clear, running example to illustrate the process:

Scenario: A company performs a gap analysis against the PCI DSS (Payment Card Industry Data Security Standard).

Example Gap 1: Data Encryption

- Requirement (Target State): All stored cardholder data must be encrypted.
- Current State: The company finds that cardholder data in their database is stored in plain text.
- The Gap: A complete lack of encryption for sensitive data.
- Remediation Plan: Implement database encryption technologies.

Example Gap 2: Vulnerability Management

- Requirement (Target State): Internal and external vulnerability scans must be performed regularly.
- Current State: The company performs internal scans but has no process for external vulnerability scans.
- The Gap: Missing a critical component of the vulnerability management program.
- Remediation Plan: Begin performing quarterly external vulnerability scans.

Example Gap 3: Security Policy

- Requirement (Target State): A formal security policy must be in place.
- Current State: The company has no official, documented security policy.
- The Gap: A complete lack of a foundational security document.
- Remediation Plan: Create and formally adopt a corporate security policy.

Key Takeaway

A Gap Analysis is a proactive and systematic tool for security improvement. It provides a clear, prioritized list of actions needed to achieve compliance with a standard or to reach a higher level of security maturity. The identified "gaps" become the foundation for the organization's security project plan.