2025 CISSP Mentor Program

CHAPTER 16 & 17

Brad Nigh
FRSecure

CISSP® MENTOR PROGRAM – SESSION TEN

FRSECURE CISSP MENTOR PROGRAM LIVE STREAM

THANK YOU!

Quick housekeeping reminder.

- The online/live chat that's provided while live streaming on YouTube is for constructive, respectful, and relevant (about course content) discussion **ONLY**.
- At **NO TIME** is the online chat permitted to be used for disrespectful, offensive, obscene, indecent, or profane remarks or content.
- Please do not comment about controversial subjects, and please **NO DISCUSSION OF POLITICS OR RELIGION**.
- Failure to abide by the rules may result in disabling chat for you.
- **DO NOT share or post copywritten materials (pdf of book)**

CISSP® MENTOR PROGRAM – SESSION TEN

QUESTIONS.

The most common questions:

Check your email for links

- Discord channels https://discord.gg/FWfjPnAZ
  - Use it for more in-depth questions / discussions
  - Before you ask a question, check
    - If it's been asked
    - The isc2.com website
- Live session links & recording
- Instructor slide deck https://learn.frsecure.com/
- Other Resources

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Before we get too deep into this.

How about a dumb dad joke?

I've just accepted a senior position at the Old McDonald's Farm.

I'll be the new CIEIO

CISSP® MENTOR PROGRAM – SESSION TEN

INTRODUCTION

Before we get too deep into this.

How about a dumb dad joke?

I've just accepted a senior position at the Old McDonald's Farm.

I'll be the nev

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE

- **Domain 2.0: Asset Security**
  - 2.3 Provision information and assets securely
    - 2.3.1 Information and asset ownership
    - 2.3.2 Asset inventory (e.g., tangible, intangible)
  - 2.3.3 Asset management
- **Domain 3: Security Architecture and Engineering**
  - 3.1 Research, implement and manage engineering processes using secure design principles
    - 3.1.2 Least privilege
    - 3.1.6 Segregation of Duties (SoD)
  - 3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
    - 3.5.6 Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
    - 3.5.11 Serverless

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE

- **Domain 7: Security Operations**
  - 7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation)
  - 7.4 Apply foundational security operations concepts
    - 7.4.1 Need-to-know/ least privilege
    - 7.4.2 Segregation of Duties (SoD) and responsibilities
    - 7.4.3 Privileged account management
    - 7.4.4 Job rotation
    - 7.4.5 Service-level agreements (SLA)
  - 7.5 Apply resource protection
    - 7.5.1 Media management
    - 7.5.2 Media protection techniques
    - 7.5.3 Data at rest/ data in transit

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE

- **Domain 7: Security Operations**
  - 7.8 Implement and support patch and vulnerability management
  - 7.9 Understand and participate in change management processes
  - 7.15 Address personnel safety and security concerns
    - 7.15.1 Travel
    - 7.15.2 Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)
    - 7.15.3 Emergency management
    - 7.15.4 Duress

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

THE CISSP TOPICS COVERED IN THIS CHAPTER INCLUDE

- **Domain 8: Software Development Security**
  - 8.4 Assess security impact of acquired software
    - 8.4.4 Managed services (e.g., enterprise applications)
    - 8.4.5 Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- Need-to-Know and Least Privilege
  - Need-to-Know Access
  - The Principle of Least Privilege
- Segregation of Duties (SoD) and Responsibilities
- Two-Person Control

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- Security operations include implementing risk management, incident response, access controls, and monitoring to ensure data protection and operational resilience.
- Due care and due diligence
- Confidentiality, Integrity, Availability (CIA Triad)
  - Ensures security across systems.
- Defense-in-Depth
  - Multiple layers of security to reduce vulnerabilities.
- Continuous Monitoring
  - Identifies security threats in real time.
- Incident Response and Recovery
- Effective strategies to mitigate attacks and restore operations.

- **Need-to-Know and Least Privilege**
  - **Need-to-Know Access**
  - **The Principle of Least Privilege**
- **Segregation of Duties (SoD) and Responsibilities**
- **Two-Person Control**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

Concept	Definition	Purpose	Examples
Due Care	Acting responsibly and taking reasonable steps to protect assets, employees, and customers.	Ensures organizations apply **practical security measures** to reduce risks.	Implementing **firewalls**, securing **physical access**, encrypting **sensitive data**.
Due Diligence	Conducting thorough investigations and assessments before making security decisions.	Identifies risks in advance, preventing **negligence** in security planning.	Performing **risk assessments**, vetting **third-party vendors**, reviewing **security audit reports**.

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Need-to-Know and Least Privilege**
  - **Need-to-Know Access**
    - Users receive access only to information relevant to their job role.
    - Prevents data leakage and insider threats.
    - Used in classified environments (military, government, corporate security).
  - **The Principle of Least Privilege**
- **Segregation of Duties (SoD) and Responsibilities**
- **Two-Person Control**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Need-to-Know and Least Privilege**
  - **Need-to-Know Access**
  - **The Principle of Least Privilege**
    - Users and processes should have the minimum permissions needed to perform their tasks.
    - Reduces attack surface and prevents unauthorized privilege escalation.
    - Enforced through role-based access control (RBAC), multi-factor authentication (MFA), and zero-trust models.
- **Segregation of Duties (SoD) and Responsibilities**
- **Two-Person Control**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Need-to-Know and Least Privilege**
  - **Need-to-Know Access**
  - **The Principle of Least Privilege**
- **Segregation of Duties (SoD) and Responsibilities**
  - Ensures **no single individual has complete control over a critical security process**, reducing the risk of fraud or errors.
  - Examples of SoD:
    - System administrators should not approve security policies—separate governance oversight.
    - Financial transactions require separate roles for authorization and execution—reduces fraud risks.
    - Security auditors should not also handle security configurations—ensures independent assessments.
- **Two-Person Control**

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Need-to-Know and Least Privilege**
  - **Need-to-Know Access**
  - **The Principle of Least Privilege**
- **Segregation of Duties (SoD) and Responsibilities**
- **Two-Person Control**
  - Two-person control (or **dual control**) requires **two individuals to authorize or execute a sensitive operation**.
    - Prevents unauthorized actions by requiring mutual verification.
    - Enhances security in high-risk operations (e.g., nuclear codes, financial transactions, cryptographic key management).
    - Used to prevent insider threats and fraud.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- Job Rotation
- Mandatory Vacations
- Privileged Account Management
- Service-Level Agreements (SLAs)

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Job Rotation**
  - Involves periodically moving employees into different roles within an organization to reduce security risks and prevent fraud.
    - Prevents insider threats by ensuring no single person controls critical operations for extended periods.
    - Enhances employee cross-training, increasing organizational resilience.
    - Reduces the risk of long-term fraudulent activities.
- **Mandatory Vacations**
- **Privileged Account Management**
- **Service-Level Agreements (SLAs)**

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Job Rotation**
- **Mandatory Vacations**
  - Require employees to take leave periodically, allowing organizations to review their activities for suspicious behavior.
    - Malicious activity often becomes visible when an employee is absent.
    - Reduces burnout, improving overall security awareness and productivity.
    - Enhances audit and monitoring effectiveness by allowing fresh oversight.
- **Privileged Account Management**
- **Service-Level Agreements (SLAs)**

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Job Rotation**
- **Mandatory Vacations**
- **Privileged Account Management**
  - Controls and monitors high-privilege accounts, reducing the risk of unauthorized access to sensitive systems.
    - Prevents unauthorized administrative actions that could compromise security.
    - Helps detect privilege escalation attacks.
    - Improves accountability and auditability of administrative activity.
- **Service-Level Agreements (SLAs)**

Chapter 16 Managing Security Operations

Apply Foundational Security Operations Concepts

- **Job Rotation**
- **Mandatory Vacations**
- **Privileged Account Management**
- **Service-Level Agreements (SLAs)**
  - Defines security expectations, service availability, and compliance terms between vendors and organizations.
    - Ensures vendors meet security and uptime commitments.
    - Defines responsibilities for incident response and recovery.
    - Provides a framework for auditing third-party security compliance.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Sensitive Data
  - Malware and Monitoring Devices
  - Free Wi-Fi
  - VPNs
- Emergency Management

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- **Duress**
  - Refers to situations where an individual is forced or coerced into taking an action against their will, often under threat of harm.
    - **Duress Codes & Signals**
    - **Duress Alarms**
    - **Training & Awareness**
    - **Access Control Measures**
- **Travel**
  - **Sensitive Data**
  - **Malware and Monitoring Devices**
  - **Free Wi-Fi**
  - **VPNs**
- **Emergency Management**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Involves mitigating risks that employees face while traveling for business, especially when handling sensitive information or working in high-risk environments.
    - **Pre-Travel Planning**
    - **Secure Communication & Devices**
    - **Physical Security & Awareness**
    - **Emergency Response & Duress Protocols**
    - **Access Control & Identity Protection**
  - Sensitive Data
  - Malware and Monitoring Devices
  - Free Wi-Fi
  - VPNs
- Emergency Management

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Sensitive Data
    - Minimize Data Exposure
    - Encryption & Secure Storage
    - Physical Security
  - Malware and Monitoring Devices
  - Free Wi-Fi
  - VPNs
- Emergency Management

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Sensitive Data
  - Malware and Monitoring Devices
    - Avoid Public or Untrusted Devices
    - Use Endpoint Protection
    - Check for Unauthorized Surveillance
  - Free Wi-Fi
  - VPNs
- Emergency Management

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Sensitive Data
  - Malware and Monitoring Devices
  - Free Wi-Fi
    - Security Risks
    - Avoid Automatic Connections
    - Use Secure Alternatives
  - VPNs
- Emergency Management

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- **Duress**
- **Travel**
  - **Sensitive Data**
  - **Malware and Monitoring Devices**
  - **Free Wi-Fi**
  - **VPNs**
    - Types of VPNs
      - **Remote-access VPNs:** Used by individuals to securely connect to a corporate network from outside.
      - **Site-to-site VPNs:** Connect entire networks together, for example, linking two branch offices securely.
      - **Client-based vs. clientless VPNs:** Important distinction for implementation and access control.
- **Emergency Management**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- **Duress**
- **Travel**
  - **Sensitive Data**
  - **Malware and Monitoring Devices**
  - **Free Wi-Fi**
  - **VPNs**
    - VPN Protocols
      - **IPSec:** Widely used; operates at the network layer; supports encryption and authentication (AH/ESP).
      - **SSL/TLS:** Often used for browser-based VPNs; operates at the transport layer.
      - **PPTP, L2TP:** Older protocols, less secure, typically only discussed for historical or comparative context.
  - **Emergency Management**

Cha ations

Addres

- Dur
- Trav
  - S
  - I
  - I
  - V
  - I

Protocol	Layer Operated On	Encryption Support	Authentication Support	Notes / CISSP Focus
IPSec	Network (Layer 3)	Strong (e.g., AES)	Yes (pre-shared key, certs)	Supports AH & ESP; widely used for site-to-site VPNs; robust, but complex setup
SSL/TLS	Transport (Layer 4)	Strong	Yes (certificates, MFA)	Common in clientless/ browser-based VPNs; easier to deploy; increasingly popular
L2TP	Data Link (Layer 2)	None on its own	No (used with IPSec for both)	Typically paired with IPSec; encapsulates packets; adds overhead
PPTP	Data Link (Layer 2)	Weak	Weak	Outdated and insecure; may appear in CISSP as a deprecated example
IKEv2	Network (Layer 3)	Strong	Yes	Often used with mobile devices; stable and reconnects well after dropped signals

on and

ort

or

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Address Personnel Safety and Security

- Duress
- Travel
  - Sensitive Data
  - Malware and Monitoring Devices
  - Free Wi-Fi
  - VPNs
- Emergency Management
  - Focuses on preparing for, responding to, and recovering from security incidents, natural disasters, cyber threats, or other emergencies.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Provision Resources Securely

- Information and Asset Ownership
  - Asset Management
    - Tangible assets
    - Intangible assets
  - Hardware Asset Inventories
  - Software Asset Inventories

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - Information Ownership
    - In cybersecurity, designated owners are responsible for classifying, protecting, and managing information assets. Ownership ensures accountability for securing sensitive data.
  - Asset Ownership
    - Organizations assign ownership roles to individuals or departments to manage, maintain, and ensure the security of IT assets. Owners define security policies, access controls, and compliance measures.
  - **Asset Management**
    - **Tangible assets**
    - **Intangible assets**
  - **Hardware Asset Inventories**
  - **Software Asset Inventories**

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - **Asset Management**
    - Identification & Classification
    - Lifecycle Management
    - Risk Assessment
    - **Tangible assets**
    - **Intangible assets**
  - **Hardware Asset Inventories**
  - **Software Asset Inventories**

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - **Asset Management**
    - **Tangible assets**
      - **Physical** components used in IT and security operations
        - Servers, networking equipment, workstations
        - Security devices like firewalls, biometric scanners, and surveillance systems
        - Physical storage media such as hard drives and backup tapes
    - **Intangible assets**
  - **Hardware Asset Inventories**
  - **Software Asset Inventories**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - **Asset Management**
    - **Tangible assets**
    - **Intangible assets**
      - **Non-physical** elements essential to cybersecurity and business operations
        - Intellectual property (patents, trademarks, proprietary algorithms)
        - Sensitive data (customer records, trade secrets)
  - **Hardware Asset Inventories**
  - **Software Asset Inventories**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - **Asset Management**
    - **Tangible assets**
    - **Intangible assets**
  - **Hardware Asset Inventories**
    - Asset visibility & tracking
      - Organizations must maintain an up-to-date record of all hardware, including ownership details, locations, and security statuses.
    - Patch & maintenance management
      - Regular updates and security patches help prevent vulnerabilities in hardware assets.
    - End-of-life planning
      - Organizations must securely decommission hardware to prevent data leaks and unauthorized access.
  - **Software Asset Inventories**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Provision Resources Securely

- **Information and Asset Ownership**
  - **Asset Management**
    - **Tangible assets**
    - **Intangible assets**
  - **Hardware Asset Inventories**
  - **Software Asset Inventories**
    - License compliance
      - Avoiding unauthorized software usage that could lead to legal or security issues.
    - Vulnerability management
      - Identifying outdated or unsupported software that may introduce security risks.
    - Access control & authorization
      - Defining who can install, modify, or access certain software applications.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- Media Management
- Media Protection Techniques
- Controlling USB Flash Drives
- Tape Media
- Mobile Devices

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Media Management**
  - Involves tracking, storing, and disposing of data storage devices to prevent unauthorized access.
    - Data Classification
    - Inventory Tracking
    - Secure Disposal
- **Media Protection Techniques**
- **Controlling USB Flash Drives**
- **Tape Media**
- **Mobile Devices**

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Media Management**
- **Media Protection Techniques**
  - Protecting media ensures that sensitive information is not exposed to unauthorized individuals.
    - Encryption
    - Access Control
    - Physical Security
- **Controlling USB Flash Drives**
- **Tape Media**
- **Mobile Devices**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- Media Management
- Media Protection Techniques
- Controlling USB Flash Drives
  - Disabling USB Ports
  - Using Encrypted Drives
  - Endpoint Protection
- Tape Media
- Mobile Devices

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Media Management**
- **Media Protection Techniques**
- **Controlling USB Flash Drives**
- **Tape Media**
  - While older, tape media is still used for archival storage and disaster recovery.
    - Data Encryption
    - Access Controls
    - Secure Transportation
- **Mobile Devices**

Chapter 16 Managing Security Operations

Apply Resource Protection

- Media Management
- Media Protection Techniques
- Controlling USB Flash Drives
- Tape Media
- Mobile Devices
  - Mobile Device Management (MDM)
  - Strong Authentication
  - Remote Wipe Capability

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managing Media Lifecycle**
  - Reusable media is subject to a mean time to failure (MTTF)
    - Covered in chapter 10 (session 5)
  - Some tapes include specifications saying they can be reused as many as 250 times or last up to 30 years under ideal conditions.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managing Media Lifecycle**

MTTF is different from mean time between failures (MTBF). MTTF is normally calculated for items that will not be repaired when they fail, such as a tape. In contrast, MTBF refers to the amount of time expected to elapse between failures of an item that personnel will repair, such as a computer server.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- Managed Services in the Cloud
- Shared Responsibility with Cloud Service Models

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managed Services in the Cloud**
  - Refers to outsourcing certain IT functions to a **Managed Service Provider (MSP)**. These providers handle aspects such as security, monitoring, backup, and compliance to ensure smooth cloud operations.
    - Improved Security
    - Cost Efficiency
    - Automated Compliance
- **Shared Responsibility with Cloud Service Models**

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managed Services in the Cloud**
- **Shared Responsibility with Cloud Service Models**
  - Cloud security follows a shared responsibility model, meaning cloud providers and customers each have security responsibilities. The division varies based on the type of cloud service:
    - Cloud Provider Responsibilities
      - Maintain the security of infrastructure, networks, and physical data centers.
    - Customer Responsibilities
      - Configure security settings, manage access controls, and protect application-level data.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managed Services in the Cloud**
- **Shared Responsibility with Cloud Service Models**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managed Services in the Cloud**
- **Shared Responsibility with Cloud Service Models**
  - Software as a Service (SaaS)
    - Delivers **ready-to-use applications** over the internet, eliminating the need for local installation.
      - Data Protection
      - Identity Management
      - Vendor Lock-in Risks
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Managed Services in the Cloud**
- **Shared Responsibility with Cloud Service Models**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
    - Offers a **development environment** where organizations can build and deploy applications without managing infrastructure.
      - Secure Application Development
      - Access Control
      - Cloud Database Security
  - Infrastructure as a Service (IaaS)

Chapter 16 Managing Security Operations

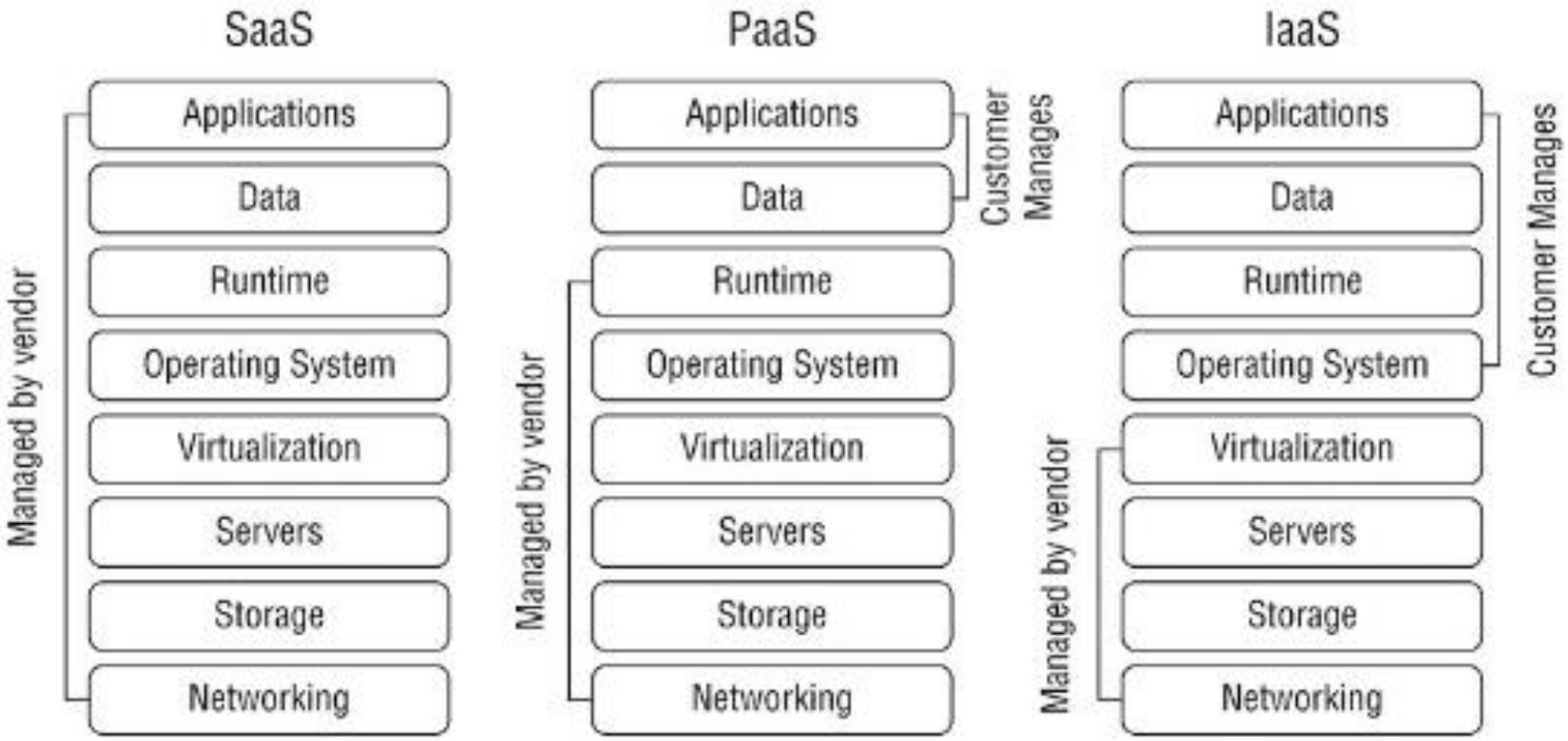
Apply Resource Protection

- **Managed Services in the Cloud**
- **Shared Responsibility with Cloud Service Models**
  - Software as a Service (SaaS)
  - Platform as a Service (PaaS)
  - Infrastructure as a Service (IaaS)
    - Provides **virtualized computing resources**, including servers, storage, and networking.
      - Cloud Network Security
      - Virtual Machine (VM) Security
      - Data Encryption

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection



Chapter 16 Managing Security Operations

Apply Resource Protection

- **Cloud deployment model**
  - Public cloud
  - Private cloud
  - Community cloud
  - Hybrid cloud

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Cloud deployment model**
  - Public cloud
    - Definition
      - A cloud environment hosted and managed by a third-party provider, accessible to multiple organizations or individuals over the internet.
    - Examples
      - Amazon Web Services (AWS), Microsoft Azure, Google Cloud Platform (GCP).
    - Security Considerations
      - Strong access controls and encryption are required since data is stored in a shared infrastructure.
      - Organizations must ensure compliance with regulations like GDPR, HIPAA, or SOC 2 when using public cloud services
  - Private cloud
  - Community cloud
  - Hybrid cloud

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Cloud deployment model**
  - Public cloud
  - Private cloud
    - Definition
      - A cloud infrastructure dedicated to a single organization, either hosted internally or managed by a third-party provider with exclusive access.
    - Security Considerations:
      - Greater control over data, security configurations, and compliance.
      - Requires robust identity and access management to protect sensitive information.
      - Typically used by enterprises with strict security or regulatory requirements.
  - Community cloud
  - Hybrid cloud

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Cloud deployment model**
  - Public cloud
  - Private cloud
  - Community cloud
    - Definition
      - A cloud environment shared among multiple organizations with similar interests, requirements, or regulatory concerns (e.g., healthcare, government, or financial institutions).
    - Security Considerations:
      - Offers enhanced security tailored to industry-specific standards.
      - Requires clear governance policies for shared infrastructure and access control.
      - Used by organizations that require collaboration while maintaining strict security protocols.
  - Hybrid cloud

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Cloud deployment model**
  - Public cloud
  - Private cloud
  - Community cloud
  - Hybrid cloud
    - Definition
      - A combination of public and private cloud environments that enables organizations to balance scalability with security.
    - Security Considerations:
      - Requires secure data transfer between private and public environments.
      - Organizations must implement strong interoperability controls and encryption.
      - Frequently used by businesses that want flexibility, allowing sensitive workloads to remain in a private cloud while utilizing public cloud resources for scalability.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Apply Resource Protection

- Scalability and Elasticity
- Perform Configuration Management (CM)
- Managing Change

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Scalability and Elasticity**
  - **Scalability**
    - Refers to the ability of a system to handle increased workloads by adding resources (e.g., more servers, storage, or computing power). It ensures **long-term** performance improvements without disruptions.
  - **Elasticity**
    - Allows a system to dynamically adjust resource allocation in **real time** based on demand. Cloud environments often use elasticity to scale resources up or down automatically.
- **Perform Configuration Management (CM)**
- **Managing Change**

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Scalability and Elasticity**
- **Perform Configuration Management (CM)**
  - The practice of maintaining **consistent system settings** to ensure security and stability.

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Scalability and Elasticity**
- **Perform Configuration Management (CM)**
  - Provisioning
    - **Deploying and configuring resources** such as hardware, software, and network devices in a controlled manner. This ensures that systems are set up correctly and securely from the start.
  - Baselining
  - Automation

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Scalability and Elasticity**
- **Perform Configuration Management (CM)**
  - Provisioning
  - Baselining
    - Establishes **a standard configuration** that systems must adhere to in order to maintain security and compliance.
  - Automation

Chapter 16 Managing Security Operations

Apply Resource Protection

- **Scalability and Elasticity**
- **Perform Configuration Management (CM)**
  - Provisioning
  - Baselining
  - Automation
    - Enhances efficiency and security by **reducing manual errors and ensuring consistent enforcement** of configuration management policies.

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
  - **Approve/reject the change.**
  - **Test the change.**
  - **Schedule and implement the change.**
  - **Document the change.**

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
    - Any proposed change must be formally submitted with clear details on why the change is needed.
    - Requests should include security implications, expected outcomes, and affected assets.
    - Organizations often use change request forms or ticketing systems to initiate and track changes.
  - **Review the change.**
  - **Approve/reject the change.**
  - **Test the change.**
  - **Schedule and implement the change.**
  - **Document the change.**

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
    - The change request undergoes a review process to assess potential security risks, operational impact, and compatibility.
    - Security teams analyze whether the change aligns with policies, compliance regulations, and best practices.
    - Stakeholder input (e.g., IT, security, and management) ensures a well-rounded assessment.
  - **Approve/reject the change.**
  - **Test the change.**
  - **Schedule and implement the change.**
  - **Document the change.**

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
  - **Approve/reject the change.**
    - Based on the review, the change request is either approved or rejected.
    - Approval may require management and security team consent, ensuring the change does not introduce vulnerabilities.
    - Rejection occurs if the change poses excessive risk or lacks sufficient justification.
  - **Test the change.**
  - **Schedule and implement the change.**
  - **Document the change.**

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
  - **Approve/reject the change.**
  - **Test the change.**
    - Before full implementation, testing is conducted in a controlled environment (such as a staging or sandbox system).
    - Testing helps identify potential issues before deployment to production systems.
    - Security controls are evaluated to ensure the change does not create vulnerabilities or compliance violations.
  - **Schedule and implement the change.**
  - **Document the change.**

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
  - **Approve/reject the change.**
  - **Test the change.**
  - **Schedule and implement the change.**
    - Once tested and approved, the change is scheduled to minimize disruption (e.g., off-peak hours).
    - Implementation follows a structured approach, documenting each action taken.
    - Rollback plans are prepared in case unexpected issues arise.
  - **Document the change.**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Managing Change

- **Change Management**
  - **Request the change.**
  - **Review the change.**
  - **Approve/reject the change.**
  - **Test the change.**
  - **Schedule and implement the change.**
  - **Document the change.**
    - After implementation, all modifications must be logged, detailing:
      - The exact changes made
      - Who implemented them
      - Any security impacts
      - Results of post-change assessments
    - Proper documentation ensures accountability, auditing, and traceability, helping with future troubleshooting.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Managing Change

- Versioning
- Configuration Documentation
- Managing Patches and Reducing Vulnerabilities
- Systems to Manage

Chapter 16 Managing Security Operations

Managing Change

- **Versioning**
  - Tracking and managing changes in software, systems, and configurations through version numbers or identifiers.
- **Configuration Documentation**
- **Managing Patches and Reducing Vulnerabilities**
- **Systems to Manage**

Chapter 16 Managing Security Operations

Managing Change

- **Versioning**
- **Configuration Documentation**
  - Involves maintaining detailed records of how systems and applications are set up and what their current state is.
- **Managing Patches and Reducing Vulnerabilities**
- **Systems to Manage**

Chapter 16 Managing Security Operations

Managing Change

- **Versioning**
- **Configuration Documentation**
- **Managing Patches and Reducing Vulnerabilities**
  - The practice of applying updates to correct software flaws and bolster security.
  - Should include identification, testing, approval, and deployment of patches.
- **Systems to Manage**

Chapter 16 Managing Security Operations

Managing Change

- **Versioning**
- **Configuration Documentation**
- **Managing Patches and Reducing Vulnerabilities**
- **Systems to Manage**
  - All devices and platforms within an organization's IT environment that need to be controlled and protected.
  - Servers, endpoints, network devices, virtual machines, mobile devices, IoT devices.

Chapter 16 Managing Security Operations

Managing Change

- Patch Management
  - Evaluate patches
  - Test patches
  - Approve the patches
  - Deploy the patches
  - Verify that patches are deployed

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - Refers to the organized process of identifying, acquiring, testing, deploying, and verifying software updates (patches) to fix vulnerabilities, improve performance, or enhance functionality.
  - **Evaluate patches**
  - **Test patches**
  - **Approve the patches**
  - **Deploy the patches**
  - **Verify that patches are deployed**

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - **Evaluate patches**
    - This step involves:
      - Identifying newly released patches from vendors.
      - Assessing the relevance of those patches based on your environment.
      - Evaluating risk exposure if the patch is not applied (e.g., exploitability, severity scores like CVSS).
  - **Test patches**
  - **Approve the patches**
  - **Deploy the patches**
  - **Verify that patches are deployed**

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - **Evaluate patches**
  - **Test patches**
    - Before deploying a patch organization-wide, it should be thoroughly tested to avoid disruptions:
      - Use test/staging environments that mimic production setups.
      - Check for compatibility with existing systems, applications, and configurations.
      - Monitor for side effects like performance issues or conflicts.
  - **Approve the patches**
  - **Deploy the patches**
  - **Verify that patches are deployed**

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - **Evaluate patches**
  - **Test patches**
  - **Approve the patches**
    - Once a patch is evaluated and successfully tested:
      - Formal approval is obtained from IT/security leadership or a Change Advisory Board (CAB).
      - Change management procedures ensure the patch aligns with business objectives and won't impact critical operations.
  - **Deploy the patches**
  - **Verify that patches are deployed**

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - **Evaluate patches**
  - **Test patches**
  - **Approve the patches**
  - **Deploy the patches**
    - With approval:
      - Patches are rolled out to production environments using automation tools if possible (e.g., SCCM, WSUS, or third-party patching platforms).
      - Deployment schedules should minimize downtime and business disruption—often during off-hours or maintenance windows.
  - **Verify that patches are deployed**

Chapter 16 Managing Security Operations

Managing Change

- **Patch Management**
  - **Evaluate patches**
  - **Test patches**
  - **Approve the patches**
  - **Deploy the patches**
  - **Verify that patches are deployed**
    - Confirm success and detect issues.
    - Use patch status scans, agent reports, or endpoint logs.
    - Document outcomes and follow up on exceptions or failed installations.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 16 Managing Security Operations

Managing Change

- Vulnerability Management
- Vulnerability Scans
- Common Vulnerabilities and Exposures

Chapter 16 Managing Security Operations

Managing Change

- **Vulnerability Management**
  - The **continuous process of identifying, assessing, prioritizing, and remediating security weaknesses** in systems, applications, and networks.
  - Key phases include:
    - Discovery: Identifying assets and software in your environment.
    - Assessment: Analyzing those assets for known vulnerabilities.
    - Prioritization: Assigning risk levels based on exploitability and asset value.
    - Remediation: Applying patches, configuration changes, or mitigation techniques.
    - Verification: Re-testing to ensure the vulnerability has been resolved.
- **Vulnerability Scans**
- **Common Vulnerabilities and Exposures**

Chapter 16 Managing Security Operations

Managing Change

- **Vulnerability Management**
- **Vulnerability Scans**
  - **Automated tools used to detect known weaknesses** in your systems or applications.
  - Vulnerability scanners (e.g., Nessus, Qualys, OpenVAS) compare systems against databases of known weaknesses and help identify gaps **before attackers can exploit them**.
- **Common Vulnerabilities and Exposures**

Chapter 16 Managing Security Operations

Managing Change

- **Vulnerability Management**
- **Vulnerability Scans**
- **Common Vulnerabilities and Exposures**
  - CVE is a standardized dictionary of **publicly known cybersecurity vulnerabilities**.
  - Managed by MITRE Corporation with support from the U.S. Department of Homeland Security.
  - Each CVE entry has a unique identifier (e.g., CVE-2024-12345), a brief description, and references to related advisories and patches.

Chapter 16 Managing Security Operations

Exam Essentials

- Know the difference between need to know and the least privilege principle.
- Understand separation of duties and job rotation.
- Know about monitoring privileged operations.
- Understand service-level agreements.
- Describe personnel safety and security concerns.
- Understand secure provisioning concepts.
- Know how to manage and protect media.

Chapter 16 Managing Security Operations

Exam Essentials

- Know the difference between SaaS, PaaS, and IaaS.
- Recognize security issues with managed services in the cloud.
- Explain configuration and change control management.
- Understand patch management.
- Explain vulnerability management.

WHEN DOES A JOKE BECOME A DAD JOKE?

WHEN IT BECOMES APPARENT!

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

- Domain 7.0: Security Operations
  - 7.2 Conduct logging and monitoring activities
  - 7.2.1 Intrusion detection and prevention
  - 7.2.2 Security Information and Event Management (SIEM)
  - 7.2.3 Continuous monitoring
  - 7.2.4 Egress monitoring
  - 7.2.5 Log management
  - 7.2.6 Threat intelligence (e.g., threat feeds, threat hunting)

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

- Domain 7.0: Security Operations
  - 7.6 Conduct incident management
  - 7.6.1 Detection
  - 7.6.2 Response
  - 7.6.3 Mitigation
  - 7.6.4 Reporting
  - 7.6.5 Recovery
  - 7.6.6 Remediation
  - 7.6.7 Lessons learned

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

- Domain 7.0: Security Operations
  - 7.7 Operate and maintain detective and preventative measures
  - 7.7.2 Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
  - 7.7.3 Whitelisting/blacklisting 7.7.4 Third-party provided security services
  - 7.7.5 Sandboxing
  - 7.7.6 Honeypots/honeynets
  - 7.7.7 Anti-malware
  - 7.7.8 Machine learning and Artificial Intelligence (AI) based tools Domain
- Domain 8.0: Software Development Security
  - 8.2 Identify and apply security controls in software development ecosystems
  - 8.2.7 Security Orchestration, Automation, and Response (SOAR)

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Defining an Incident
  - An **incident** is any event that has a negative effect on the confidentiality, integrity, or availability of an organization's assets.
  - A **computer security incident** (sometimes called just security incident) commonly refers to an incident that is the result of an attack or the result of malicious or intentional actions on the part of users.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps

FIGURE 17.1 Incident management

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident management does not include a counterattack against the attacker. Launching attacks on others is counterproductive and often illegal.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
  - **Reporting**
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
    - Identifying potential security incidents through logs, alerts, anomaly detection systems, intrusion detection systems (IDS), or reports from users.
  - **Response**
  - **Mitigation**
  - **Reporting**
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
    - Activating the incident response team, classifying the incident, and initiating containment actions.
    - Goal: Confirm the incident and stop it from spreading or worsening.
  - **Mitigation**
  - **Reporting**
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
    - Implementing short-term controls to limit harm and preserve evidence for forensic analysis.
    - Goal: Prevent further damage while keeping critical systems operational.
  - **Reporting**
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
  - **Reporting**
    - Documenting the incident, detailing its scope, impact, timeline, and actions taken.
    - Goal: Ensure transparency, support legal requirements, and coordinate external communication if necessary.
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
  - **Reporting**
  - **Recovery**
    - Bringing systems back online, monitoring them for unusual behavior, and confirming that they're free from threats.
    - Goal: Return to business as usual with confidence the threat is eliminated.
  - **Remediation**
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
  - **Reporting**
  - **Recovery**
  - **Remediation**
    - Fixing vulnerabilities, applying long-term patches, updating configurations or security tools.
    - Goal: Close the door that the attacker used — for good.
  - **Lessons Learned**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Incident Management Steps
  - **Detection**
  - **Response**
  - **Mitigation**
  - **Reporting**
  - **Recovery**
  - **Remediation**
  - **Lessons Learned**
    - Conducting a post-incident review or retrospective with stakeholders.
    - Goal: Improve incident response by identifying what worked, what didn't, and what needs to change.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Implementing Detective and Preventive Measures
  - Preventive Control
  - Detective Control

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Implementing Detective and Preventive Measures**
  - Together, these controls help organizations:
    - Prevent incidents from occurring
    - Identify issues when prevention fails
    - Respond quickly to minimize impact
  - **Preventive Control**
  - **Detective Control**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Implementing Detective and Preventive Measures**
  - **Preventive Control**
    - **Proactive** measures intended to **stop security incidents before they happen**.
    - Examples include:
      - Firewalls and network access controls
      - User authentication mechanisms (e.g., MFA)
      - Security awareness training
      - Encryption and secure configurations
      - Physical barriers (e.g., locked doors, biometrics)
  - **Detective Control**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Implementing Detective and Preventive Measures**
  - **Preventive Control**
  - **Detective Control**
    - **Reactive** measures designed to **identify and alert** on suspicious or unauthorized activity **after it occurs**.
    - Examples include:
      - Intrusion detection systems (IDS)
      - Security Information and Event Management (SIEM) tools
      - Audit logs and monitoring systems
      - Video surveillanceFile integrity checking

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - Keep systems and applications up to date
  - Remove or disable unneeded services and protocols
  - Use intrusion detection and prevention systems
  - Use up-to-date antimalware software.
  - Use firewalls
  - Implement configuration and system management processes

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
    - Regularly apply vendor-issued patches and updates for operating systems, applications, and firmware.
    - Patch management and vulnerability reduction are critical for maintaining secure system baselines.
  - **Remove or disable unneeded services and protocols**
  - **Use intrusion detection and prevention systems**
  - **Use up-to-date antimalware software.**
  - **Use firewalls**
  - **Implement configuration and system management processes**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
  - **Remove or disable unneeded services and protocols**
    - Disable default ports, services, and legacy protocols that aren't essential (e.g., Telnet, SMBv1).
    - Follows the principle of least functionality—systems should run only what's necessary.
  - **Use intrusion detection and prevention systems**
  - **Use up-to-date antimalware software.**
  - **Use firewalls**
  - **Implement configuration and system management processes**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
  - **Remove or disable unneeded services and protocols**
  - **Use intrusion detection and prevention systems**
    - Deploy IDS/IPS at network perimeters and critical points. Regularly review alerts and update detection rules.
    - Combines detective and preventive controls for stronger incident response posture.
  - **Use up-to-date antimalware software.**
  - **Use firewalls**
  - **Implement configuration and system management processes**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
  - **Remove or disable unneeded services and protocols**
  - **Use intrusion detection and prevention systems**
  - **Use up-to-date antimalware software.**
    - Ensure antimalware solutions are installed, running, and auto-updating signatures.
    - Essential for endpoint protection and maintaining defense-in-depth strategies.
  - **Use firewalls**
  - **Implement configuration and system management processes**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
  - **Remove or disable unneeded services and protocols**
  - **Use intrusion detection and prevention systems**
  - **Use up-to-date antimalware software.**
  - **Use firewalls.**
    - Configure firewalls to enforce least privilege access, monitor connections, and block unauthorized traffic.
    - Core to network security architecture and access control policies.
  - **Implement configuration and system management processes**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Basic Preventive Measures**
  - **Keep systems and applications up to date**
  - **Remove or disable unneeded services and protocols**
  - **Use intrusion detection and prevention systems**
  - **Use up-to-date antimalware software.**
  - **Use firewalls.**
  - **Implement configuration and system management processes**
    - Use configuration management tools to enforce system baselines, track changes, and maintain consistency.
    - Tied to change management, provisioning, baselining, and overall system hardening efforts.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Understanding Attacks
  - Botnets
  - Denial-of-Service Attacks
  - Distributed reflective denial-of-service (DRDoS)
  - SYN Flood Attack
  - TCP Reset Attack

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Botnets**
    - A network of compromised devices (bots or zombies) controlled by a threat actor, often through a command-and-control (C2) server.
    - Botnets are like an army of hijacked computers silently obeying an attacker's orders without the owner's knowledge.
  - **Denial-of-Service Attacks**
  - **Distributed reflective denial-of-service (DRDoS)**
  - **SYN Flood Attack**
  - **TCP Reset Attack**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Botnets**
  - **Denial-of-Service Attacks**
    - The aim to disrupt services by overwhelming a system with traffic or resource requests.
    - The goal is to make applications, servers, or networks unavailable to legitimate users.
  - **Distributed reflective denial-of-service (DRDoS)**
  - **SYN Flood Attack**
  - **TCP Reset Attack**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Botnets**
  - **Denial-of-Service Attacks**
  - **Distributed reflective denial-of-service (DRDoS)**
    - A type of amplified DDoS attack that uses third-party servers to reflect traffic toward a target.
    - Attackers spoof the victim's IP address in requests to vulnerable servers (like DNS, NTP), which then send large responses to the victim.
    - Imagine yelling someone's name into a canyon, and the echoes collapse their eardrums—that's DRDoS in cyber terms.
  - **SYN Flood Attack**
  - **TCP Reset Attack**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Understanding Attacks
  - Botnets
  - Denial-of-Service Attacks
  - Distributed reflective denial-of-service (DRDoS)
  - SYN Flood Attack
    - Exploits the TCP handshake process (SYN, SYN-ACK, ACK).
    - An attacker sends many SYN requests without completing the handshake, leaving the server with half-open connections.
  - TCP Reset Attack

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Botnets**
  - **Denial-of-Service Attacks**
  - **Distributed reflective denial-of-service (DRDoS)**
  - **SYN Flood Attack**
  - **TCP Reset Attack**
    - An adversary sends a forged TCP reset (RST) packet to interrupt an active connection.
    - It's often used to force disconnections in VPNs or encrypted channels like TLS.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Understanding Attacks
  - Smurf and Fraggle Attacks
  - Ping Flood
  - Legacy
  - Zero-Day Exploit

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Smurf and Fraggle Attacks**
    - Both are types of **Denial-of-Service (DoS)** attacks, but they use slightly different methods to flood a target with traffic
  - **Ping Flood**
  - **Legacy**
  - **Zero-Day Exploit**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Smurf and Fraggle Attacks**
    - **Smurf Attack**: This exploits the Internet Control Message Protocol (ICMP). An attacker sends an ICMP echo request (like a "ping") to a broadcast address of a network with the spoofed IP address of the target. All devices on the network reply to the target, overwhelming it with traffic.
  - **Ping Flood**
  - **Legacy**
  - **Zero-Day Exploit**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Smurf and Fraggle Attacks**
    - **Fraggle Attack**: A variation of Smurf, but it uses UDP (User Datagram Protocol) instead of ICMP. The attacker sends spoofed UDP packets to port 7 (echo) or port 19 (character generator protocol) causing the devices to flood the target.
  - **Ping Flood**
  - **Legacy**
  - **Zero-Day Exploit**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Smurf and Fraggle Attacks**
  - **Ping Flood**
    - Also known as an **ICMP Flood**, this attack involves sending a large number of ping requests to a target machine very rapidly.
  - **Legacy**
  - **Zero-Day Exploit**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Understanding Attacks
  - Smurf and Fraggle Attacks
  - Ping Flood
  - Legacy
    - Ping of Death
    - Teardrop
    - LAND
  - Zero-Day Exploit

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

Attack Name	How It Works	Targeted Protocol	Impact
Ping of Death	Sends oversized or malformed ping packets (>65,535 bytes) that overflow memory buffers on the target machine.	ICMP	System crashes, reboots, or freezes.
Teardrop	Sends overlapping or fragmented IP packets that crash systems when the OS tries to reassemble them improperly.	IP Fragmentation	Blue screen, system instability.
LAND	Sends a spoofed TCP SYN packet where both the source and destination IP address are the victim's, confusing the host and causing a crash or loop.	TCP	System lock-up or denial of service.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Smurf and Fraggle Attacks**
  - **Ping Flood**
  - **Legacy**
  - **Zero-Day Exploit**
    - Targets a previously unknown vulnerability in software or hardware. It's called “zero-day” because:
      - Developers have had zero days to fix the flaw.
      - It’s a race against time before patches are released.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Understanding Attacks
  - Man-in-the-Middle/ On-path Attacks
  - Sabotage

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Man-in-the-Middle/ On-path Attacks**
    - Occurs when a malicious actor secretly intercepts or alters communication between two parties who believe they are directly communicating with each other.
      - Session Hijacking: Taking over a legitimate user session after obtaining session tokens.
      - HTTPS Spoofing / SSL Stripping: Downgrading secure HTTPS to plain HTTP to sniff credentials.
      - ARP Spoofing: Misleading devices on a local network to route traffic through the attacker's machine.
  - **Sabotage**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Understanding Attacks**
  - **Man-in-the-Middle/ On-path Attacks**
  - **Sabotage**
    - A form of insider threat where a disgruntled or malicious employee intentionally harms the organization. It may involve:
      - Deleting or corrupting critical data
      - Modifying systems to fail or backdoor them for future exploitation
      - Leaking confidential or proprietary information

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection and Prevention Systems
  - Knowledge- and Behavior-Based Detection
  - False Positive or True Negative?

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Intrusion Detection and Prevention Systems**
  - **Intrusion Detection System (IDS)**
    - Monitors traffic or system activities and alerts administrators to suspicious behavior. It does not block threats—it's more like a surveillance camera.
  - **Intrusion Prevention System (IPS)**
    - Actively blocks or mitigates detected threats, often by dropping malicious packets, blocking IPs, or resetting connections.
    - Typically sits inline with traffic (unlike IDS, which is passive)
  - **Knowledge- and Behavior-Based Detection**
  - **False Positive or True Negative?**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection and Prevention Systems
  - Intrusion Detection System (IDS)
  - Knowledge- and Behavior-Based Detection
    - Knowledge-Based Detection (a.k.a. Signature-Based):
      - Relies on known attack patterns, like virus signatures or known exploits.
      - Pros: Accurate for known threats, low false positives.
      - Cons: Cannot detect zero-day attacks or new/unseen threats.
  - False Positive or True Negative?

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Intrusion Detection and Prevention Systems**
  - **Intrusion Detection System (IDS)**
  - **Knowledge- and Behavior-Based Detection**
    - **Behavior-Based Detection (a.k.a. Anomaly-Based):**
      - Establishes a baseline of normal activity, then flags deviations.
      - Pros: Can detect unknown or novel threats, like zero-days.
      - Cons: Prone to false positives (e.g., an unusual but legitimate behavior might raise an alert)
  - **False Positive or True Negative?**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection and Prevention Systen
  - Intrus m (IDS)
  - Know -Based Detec
  - False ative?

	Detected	Not Detected
Incident Occurred	True Positive	False Negative
No Incident	False Positive	True Negative

IDPSs

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Intrusion Detection and Prevention Systems**
  - **IDS Response**
    - **Passive Response**
      - Monitors and logs suspicious activity, then alerts administrators. It's like a security camera.
    - **Active Response**
      - Goes a step further—it can automatically respond to threats. Think of it as a security guard who sees something suspicious and acts on it.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection Systems
  - IDS Response
    - Passive Response
      - What it does: Logs the event and sends alerts to administrators—no intervention occurs.
      - Tools used: Email alerts, SNMP traps, syslog messages.
      - Use Case: Ideal for environments where false positives must be carefully vetted before acting.
    - Active Response

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection Systems
  - IDS Response
    - Passive Response
    - Active Response
      - Block the attacker's IP address.
      - Terminate a suspicious session.
      - Reconfigure firewall rules in real time.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection Systems
  - IDS Response
    - Passive Response
    - Active Response

For CISSP exam purposes, it's important to note that **IDS is typically considered passive**, while **IPS (Intrusion Prevention System)** is the one associated with active responses.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Detection and Prevention Systems
  - Host- and Network-Based IDSs

Cha nding to Inc

Doma

- I tion
  - S

Feature	Host-Based IDS (HIDS)	Network-Based IDS (NIDS)
Deployment Location	Installed on individual hosts/ endpoints	Deployed at strategic points in the network
Scope of Visibility	Monitors activity on a *single host*	Monitors *network traffic* across multiple systems
Detection Focus	File integrity, system logs, process behavior	Packet headers, payloads, protocol anomalies
Resource Usage	Uses host resources (CPU, RAM, storage)	Operates on dedicated hardware/appliance
Encryption Awareness	Can inspect encrypted local activity	Cannot inspect encrypted traffic without decryption
Evasion Resistance	Less prone to evasion via encryption/tunneling	Can be bypassed by encrypted or obfuscated traffic
Response Capability	Granular—can kill processes, block local changes	Typically more passive or requires integration to act
Management Overhead	High in large environments—needs per-host config	Easier to scale—centralized monitoring across hosts

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Prevention Systems
  - Specific Preventive Measures
    - Honeypots and Honeynets
    - Warning Banners
    - Anti-malware

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Intrusion Prevention Systems**
  - **Specific Preventive Measures**
    - **Honeypots and Honeynets**
      - Deception tools used to lure attackers and study their tactics:
      - **Honeypot:** A decoy system designed to look vulnerable and attract attacks.
      - **Honeynet:** A full network of honeypots simulating a larger environment.
    - **Warning Banners**
    - **Anti-malware**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

The use of honeypots raises the issue of enticement versus entrapment.

Entrapment - **Inducing someone to commit a crime** they otherwise wouldn't have.

Honeypots are *detective* and *research-based controls*, implementing them without a **risk-informed legal and operational strategy** can backfire.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Intrusion Prevention Systems
  - Specific Preventive Measures
    - Honeypots and Honeynets
    - Warning Banners
      - **Legal disclaimers** and messages shown to users when accessing systems.
      - Play a role in **legal preparedness**—they support the admissibility of evidence and reinforce organizational policy awareness.
    - Anti-malware

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Intrusion Prevention Systems**
  - **Specific Preventive Measures**
    - **Honeypots and Honeynets**
    - **Warning Banners**
    - **Anti-malware**
      - Defends against **malicious code** like viruses, worms, spyware, ransomware, and more.
      - Types of detection:
        - Signature-based (known patterns)
        - Heuristic/behavior-based (suspicious behavior)
        - Cloud-based threat intel

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Whitelisting and Blacklisting**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- ~~Whitelisting and Blacklisting~~
- Allowlisting and Denylisting

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Allowlisting and Denylisting**
  - **Allowlisting**
    - A restrictive approach where **only explicitly approved entities are permitted**—everything else is blocked by default.
      - Applications: Only approved software can run on a system.
    - Pros:
      - High security: Great for reducing exposure to unknown threats.
      - Tight control: Especially valuable in high-security or regulated environments.
    - Cons:
      - Administrative overhead: Requires constant updates and management.
      - Usability: Can impede legitimate activity if not maintained carefully.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Allowlisting and Denylisting**
  - **Denylisting**
    - A permissive model where **known malicious or unwanted items are blocked**, but everything else is allowed by default.
      - Blocking known malware domains or file hashes.
      - Preventing access to dangerous or inappropriate websites.
    - Pros:
      - *Easy to implement*: Especially when threat intelligence feeds are integrated
      - *User-friendly*: Less likely to block normal behavior.
    - Cons:
      - *Reactive approach*: It only blocks *known* threats.
      - *Gaps in coverage*: Zero-day threats or novel attacks can slip through.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Firewalls**
  - Block directed broadcasts on routers
  - Block private IP addresses at the border
  - Second-generation
    - Application-level gateway firewall
    - Circuit-level gateway firewalls
  - Third-generation firewalls
    - Also called stateful inspection firewalls
  - Next-generation firewall (NGFW)
    - Functions as a unified threat management (UTM)

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Sandboxing**
  - A technique used to **run code or applications in a controlled, isolated environment**—a "sandbox"—where they can't affect the host system or broader network.
  - Purpose:
    - Observe and analyze suspicious or untrusted programs (e.g., email attachments, scripts) without risk.
    - Prevent malware or exploits from compromising production systems.
- **Third-Party Security Services**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Sandboxing**
- **Third-Party Security Services**
  - **External providers that deliver security capabilities or expertise** that an organization may lack internally.
    - Managed Security Service Providers (MSSPs): Monitor networks, manage firewalls, and respond to incidents.
    - Cloud-based security solutions: Like DDoS protection, anti-spam services, or cloud access security brokers (CASBs).
    - Penetration testing and risk assessments: Conducted by specialized security firms.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types
  - Protecting Log Data

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

Concept	What You Should Know
Log Retention	Retain logs for a defined period based on business, legal, and regulatory requirements.
Time Synchronization	Use NTP (Network Time Protocol) to ensure timestamps are consistent across systems.
Log Protection	Logs should be **read-only**, protected from tampering, and access-controlled.
Log Analysis	Use SIEM tools to correlate and alert on suspicious activity across multiple systems.
Legal Considerations	Ensure you warn users (e.g., via warning banners) and comply with privacy laws.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types
    - Security Logs
    - System Logs
    - Application Logs
    - Firewall Logs
    - Proxy Logs
    - Change Logs
  - Protecting Log Data

CISSP

Ch onding to In

Dom

Log Type	Purpose	Typical Contents	Primary Use in Security
Security Logs	Track security-related events on systems and networks	Logins/logouts, authentication attempts, policy violations	**Auditing, incident detection, compliance**
System Logs	Record OS-level events and internal operations	System startups, shutdowns, errors, service status	**Troubleshooting, uptime monitoring**
Application Logs	Monitor activity and errors in specific software applications	App-specific events, user actions, failures	**Application-level security and performance**
Firewall Logs	Track allowed and denied traffic across network perimeters	Source/destination IPs, ports, protocols, action taken	**Traffic analysis, threat detection, policy audit**
Proxy Logs	Monitor and record web traffic flowing through proxy servers	URLs accessed, user identities, timestamps, HTTP methods	**Web usage control, malware detection, forensics**
Change Logs	Document system or configuration changes	Time/date of changes, user making the change, before/after states	**Change management, rollback support, accountability**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types

OS	Log file location
Microsoft	C:\Windows\System32\winevt\Logs\
Linux/Unix	/var/log/
macOS	/var/log, ~/Library/Logs, /Library/Logs/

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Logging and Monitoring**
  - **Logging Techniques**
  - **Common Log Types**
  - **Protecting Log Data**
    - Integrity
      - Ensure that logs cannot be altered by unauthorized users or malicious actors.
      - Use cryptographic hashing, digital signatures, and read-only storage formats to preserve integrity.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types
  - Protecting Log Data
    - Legal & Regulatory Considerations
      - Logs may contain personally identifiable information (PII) or other sensitive data, so ensure compliance with GDPR, HIPAA, or other laws.
      - Logs used in investigations should be collected legally and must maintain a valid chain of custody to be admissible in court.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Logging and Monitoring**
  - **Logging Techniques**
  - **Common Log Types**
  - **Protecting Log Data**
    - Time Synchronization
      - Synchronize all systems with a trusted time source (e.g., NTP) to ensure accurate timestamps across the environment.
      - Accurate time is essential for incident reconstruction and correlation across multiple systems.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types
  - Protecting Log Data
    - Retention and Storage
    - Synchronize all systems with a trusted time source (e.g., NTP) to ensure accurate timestamps across the environment.
      - Accurate time is essential for incident reconstruction and correlation across multiple systems.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Logging and Monitoring**
  - **Logging Techniques**
  - **Common Log Types**
  - **Protecting Log Data**
    - Access Control and Monitoring
      - Restrict log access to authorized personnel only.
      - Monitor access attempts to logs to detect tampering or unauthorized review.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Logging and Monitoring**
  - **Logging Techniques**
  - **Common Log Types**
  - **Protecting Log Data**
    - Centralization and Analysis
      - Use centralized log management or a SIEM (Security Information and Event Management) system.
      - Enables real-time correlation, alerting, forensic analysis, and compliance reporting.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Logging Techniques
  - Common Log Types
  - Protecting Log Data
    - Testing & Validation
      - Regularly test your logging infrastructure to confirm logs are collected, protected, and usable.
      - Include this in security assessments and audits.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accaccountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
    - A chronological record of system activities
      - Logins/logouts
      - File access
      - Privileged operations
      - Configuration changes
  - Monitoring and Accountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
    - Supports **non-repudiation**, **accountability**, and **forensics**
    - Must be protected for **integrity and confidentiality**
  - Monitoring and Accountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accountability
    - The processes and tools used to **track user and system activity** in order to hold individuals **accountable** for their actions
      - Logs, alerts, and audit trails enable attribution of activity to specific users.
      - Paired with authentication controls (e.g., MFA, unique IDs) and access logs
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accountability
  - Monitoring and Investigations
    - The **ongoing surveillance** and the ability to investigate when something suspicious or harmful occurs
      - Real-time and retrospective log analysis
      - Use of SIEM (Security Information and Event Management) tools
      - Digital forensics to examine logs, memory, and file systems
      - Coordination with legal and HR if internal threat is suspected
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
    - Detecting **misconfigurations**, **performance issues**, and **system failures**
      - Identifying failing hardware or software
      - Pinpointing performance bottlenecks
      - Discovering unauthorized changes
  - Monitoring and Tuning Techniques

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques
    - Ensures your monitoring tools remain **effective, efficient, and relevant**
      - Tuning SIEMs to reduce false positives and negatives
      - Updating rule sets based on current threat intelligence
      - Adjusting alert thresholds and triggers
      - Retiring outdated or noisy alerts

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Logging and Monitoring
  - Audit Trails
  - Monitoring and Accaccountability
  - Monitoring and Investigations
  - Monitoring and Problem Identification
  - Monitoring and Tuning Techniques
    - Log analysis involves **examining collected log data** to uncover patterns, detect suspicious behavior, troubleshoot issues, and support incident response. Logs serve as a **forensic record** of activity, helping analysts understand what occurred and when.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Security Information and Event Management
- Syslog
- Sampling
- Clipping Levels

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Security Information and Event Management**
  - A centralized platform that aggregates, normalizes, correlates, and analyzes **log data and security events** from various sources like firewalls, IDS/IPS, servers, and applications
- **Syslog**
- **Sampling**
- **Clipping Levels**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Security Information and Event Management**
- **Syslog**
  - **RFC 5424**
  - A **standardized protocol** used to send **log or event messages** to a central server or logging infrastructure.
  - Uses UDP (default) or TCP on port 514
  - Common in Unix/Linux systems and supported by many network appliances
  - Includes fields like timestamp, severity, facility, and message content
- **Sampling**
- **Clipping Levels**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Security Information and Event Management**
- **Syslog**
- **Sampling**
  - The practice of analyzing a **subset of data** rather than every single record. It helps optimize performance and reduce overhead
    - Network monitoring: Examine only some packets or flows
    - Log analysis: Alert on a percentage of logs matching criteria
    - Audits: Review a statistical sample of access records
- **Clipping Levels**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Security Information and Event Management**
- **Syslog**
- **Sampling**
- **Clipping Levels**
  - **Thresholds** set to reduce the noise in monitoring and alerting. Only events that **exceed the clipping level** are flagged for attention.
    - Example: Only alert on failed login attempts after 5 consecutive failures within 10 minutes.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Other Monitoring Tools
  - Keystroke Monitoring
  - Traffic Analysis and Trend Analysis
  - Log Management
  - Egress Monitoring

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Other Monitoring Tools**
  - **Keystroke Monitoring**
    - Logging or analyzing every key a user types.
    - Treated as a high-sensitivity monitoring control.
    - Raises privacy and legal concerns—must be disclosed to users (e.g., via warning banners).
    - Used sparingly, with clear policy and legal justification.
  - **Traffic Analysis and Trend Analysis**
  - **Log Management**
  - **Egress Monitoring**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Other Monitoring Tools
  - Keystroke Monitoring
  - Traffic Analysis and Trend Analysis
    - Examining **network communication patterns** over time to understand usage, detect anomalies, and identify potential threats.
    - Traffic analysis
      - Focuses on volume, source/destination addresses, protocols, and timing.
    - Trend analysis
      - Looks for patterns or deviations (e.g., sudden spikes in outbound traffic might indicate data exfiltration).
  - Log Management
  - Egress Monitoring

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Other Monitoring Tools
  - Keystroke Monitoring
  - Traffic Analysis and Trend Analysis
  - Log Management
    - The structured approach to **collecting, storing, analyzing, and disposing of log data** from across the enterprise.
      - Centralized logging (e.g., via syslog or agents)
      - Retention policies aligned with legal/regulatory needs
      - Secure storage with tamper protections
      - Regular review and alerting via SIEMs
  - Egress Monitoring

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Other Monitoring Tools
  - Keystroke Monitoring
  - Traffic Analysis and Trend Analysis
  - Log Management
  - Egress Monitoring
    - **Monitoring outbound network traffic** to detect
      - Data exfiltration
      - Unauthorized communications
      - Malware “call home” behavior
      - Policy violations (e.g., sending sensitive files externally)

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
  - **Machine Learning and AI Tools**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
    - Refers to a set of tools and processes that allow security teams to:
    - Orchestrate: Integrate multiple security technologies and data sources into unified workflows.
    - Automate: Execute routine tasks (like user blocking or log parsing) without human intervention.
    - Respond: Manage incidents and alerts more efficiently, often reducing dwell time and manual workload.
  - **Machine Learning and AI Tools**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
    - Playbook
    - Runbook
  - **Machine Learning and AI Tools**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
    - Playbook
      - Helps reduce response time from hours to minutes and ensures a repeatable, defensible process is followed every time.
    - Runbook
  - **Machine Learning and AI Tools**

Chapter 17 Preventing and Responding to Incidents

Playbook example

1. Ingestion & Trigger

- Event Source: A user reports a suspicious email via a “Report Phishing” button, or it’s flagged by the email gateway.
- Trigger: SOAR receives the alert and starts the phishing playbook.

2. Email Enrichment

- Extract details:
  - Sender address
  - URLs and attachments
  - Subject line, timestamps
- Use threat intelligence sources to check:
- Reputation of sender and domain
- Hashes of attachments
- Destination of embedded links (is it malicious?)

3. Automated Decision Point

- If indicators are known malicious, skip to response.
- If suspicious but unknown, proceed to sandboxing.

4. Sandboxing and Analysis

- Detonate attachments or URLs in a controlled sandbox.
- Log results (e.g., if they drop malware or redirect to credential harvesters).

Chapter 17 Preventing and Responding to Incidents

Playbook example

5. Containment Actions

- If confirmed malicious:
  - Quarantine the email from all affected inboxes.
  - Block sender domain at the email gateway and firewall.
  - Disable or reset credentials for users who clicked links.
  - Alert impacted users with next steps.

6. Notification & Escalation

- Notify:
  - Security team (via SIEM, Slack, email, etc.)
  - Helpdesk for user follow-up
  - Compliance team if sensitive data may be at risk

7. Post-Incident Tasks

- Tag incident with metadata for reporting.
- Auto-generate a ticket in the case management system.
- Document everything: timeline, actions, outcomes.
- Feed new IOCs (Indicators of Compromise) back into threat intel tools.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
    - Playbook
    - Runbook
      - While a **playbook** defines the overall strategy and automated workflow for handling incidents, a **runbook** dives into the **step-by-step actions an analyst or system should take** to execute that playbook.
  - **Machine Learning and AI Tools**

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Runbook example

Step 1: Ingest Alert

- Triggered from: Endpoint Detection & Response (EDR) or SIEM
  - Action:
    - Record time of detection
    - Gather alert metadata: file hash, filename, path, affected user/device

Step 2: Enrichment

- Actions:
  - Check file hash against threat intelligence databases (VirusTotal, internal IOC lists)
  - Query EDR for file execution history and affected processes
  - Pull user info from Active Directory (who's logged in, group memberships)
  - Extract network activity during time of alert

Step 3: Triage and Decision

- Actions:
  - If hash is known malicious → proceed to containment
  - If hash is unknown or suspicious → upload sample to sandbox for detonation
  - Log analyst decision rationale

Step 4: Containment

- Automated if severity is high:
  - Isolate endpoint from the network (via EDR)
  - Block hash in AV/EDR tools
  - Quarantine file
  - Notify user and helpdesk

Chapter 17 Preventing and Responding to Incidents

Runbook example

Step 5: Investigation and Impact Assessment

- Identify lateral movement or propagation to other hosts
- Check for exfiltration indicators
- Collect additional logs (e.g., DNS, proxy, firewall) for context

Step 6: Remediation

- Remove malicious file and associated registry keys or scheduled tasks
- Restore affected files from backup (if needed)
- Reconnect endpoint to the network

Step 7: Notification and Documentation

- Send incident summary to SecOps and Management
- Update ticket with:
  - Timeline of actions
  - Indicators of compromise (IOCs)
  - Response actions taken
- Tag incident in SIEM for metrics and trend analysis

Step 8: Closure and Lessons Learned

- Run post-mortem and update detection rules if gaps were found
- Feed new IOCs into threat intelligence platform
- Update runbook/playbook if improvements are identified

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
  - **Machine Learning and AI Tools**
    - Emerging technologies that support detection, analysis, and prediction.
    - **Machine learning** is a part of artificial intelligence and refers to a system that can improve automatically through experience.
    - **Artificial intelligence** is a broad field that includes ML. It gives machines the ability to do things that a human can do better or allows a machine to perform tasks that we previously thought required human intelligence.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Understanding SOAR**
  - **Machine Learning and AI Tools**
    - **ML is the brain behind pattern recognition**, while **AI brings in the reasoning and automation** to make actionable decisions based on those insights.

Chap nding to Incid

Domain 7

- Au
  -
  -

Category	Machine Learning (ML)	AI Tools (Broader AI)
Definition	Algorithms trained on data to make predictions or detect patterns	Systems that simulate human intelligence, including ML, NLP, and more
Use in Security	Anomaly detection, behavior analysis, spam/phishing identification	Automated threat hunting, response (via SOAR), fraud detection
Learning Type	Supervised, unsupervised, or reinforcement learning	May include ML + logic systems, expert systems, natural language tools
CISSP Domains Impacted	Security Operations, Communication & Network Security	Security & Risk Mgmt, Security Engineering, Security Operations
Strengths	Detects unknown threats through behavior deviation	Enhances automation, decision-making, and response accuracy
Challenges/ Risks	Requires quality training data; risk of bias, drift	Explainability issues, over-reliance, and data privacy concerns
Examples	UEBA (User & Entity Behavior Analytics), ML-based DLP	SOAR, NLP-driven threat intel tools, AI-enhanced SIEMs

, analysis,

ence and
cally

udes ML. It
human
tasks that
ence.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Threat Intelligence**
    - Refers to the **collection, analysis, and application of information** about potential or current threats targeting an organization. It's not just raw data—it's **contextualized, actionable knowledge** that supports defense decisions.
      - Prioritize security controls based on likely threats
      - Enrich alerts and logs for better incident response
      - Feed into SIEM and SOAR systems for automated actions
  - **Understanding the Kill Chain**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Threat Intelligence**
  - **Understanding the Kill Chain**
    - Describes the **phases of a typical cyberattack**, helping defenders **detect and disrupt** adversaries at each stage.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Threat Intelligence**
  - **Understanding the Kill Chain**
    - Kill Chain Phases:
      - Reconnaissance – Attacker gathers intel on target (e.g., scanning open ports, researching employees).
      - Weaponization – Crafting a malicious payload (e.g., malware + exploit).
      - Delivery – Transmitting the payload (e.g., phishing email, malicious link).
      - Exploitation – Code executes by exploiting a vulnerability.
      - Installation – Malware is installed to gain persistence.
      - Command & Control (C2) – Attacker establishes remote access/control.
      - Actions on Objectives – Attacker completes goal (e.g., data theft, disruption).

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **The MITRE ATT&CK Matrix**
  - Created by MITRE and viewable at http:// attack.mitre.org
  - A knowledge base of identified tactics, techniques, and procedures (**TTPs**)
  - The matrix is structured like a table:
    - Rows = Tactics – the "why" of an attacker's action (i.e., their objectives).
    - Columns = Techniques (and Sub-techniques) – the "how" the attacker achieves each tactic.

The MITRE ATT&CK Matrix

Chapter 17 Preventing and Responding to I

Tactic (Goal)	Examples of Techniques
Initial Access	Phishing, Drive-by Compromise
Execution	PowerShell, Scheduled Tasks
Persistence	Registry Run Keys, Account Manipulation
Privilege Escalation	Exploitation for Privilege Escalation
Defense Evasion	Obfuscated Files, Disabling Security Tools
Credential Access	Keylogging, Credential Dumping
Discovery	System Information Discovery, Network Scanning
Lateral Movement	Remote Services, Pass-the-Hash
Collection	Screen Capture, Clipboard Collection
Exfiltration	Exfil via Web, Cloud Storage
Command & Control	Beaconing, Domain Fronting
Impact (Enterprise)	Data Destruction, Resource Hijacking

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Automating Incident Response
  - Threat Feeds
  - Threat Hunting

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **Threat Feeds**
    - A real-time or regularly updated stream of **threat intelligence data** that includes indicators of compromise (IOCs), tactics and techniques, and emerging attack trends.
  - **Threat Hunting**

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Types of data in a threat feed:
  - Malicious IP addresses and URLs
  - File hashes associated with malware
  - Known phishing domains
  - Attack signatures and behaviors (e.g. MITRE ATT&CK techniques)

Automating Incident Response

Threat Feeds

- Sources:
  - Open-source intelligence (OSINT)
  - Government agencies (e.g., US-CERT)
  - Commercial threat intel providers
  - Industry ISACs (Information Sharing and Analysis Centers)

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Automating Incident Response
  - Threat Feeds
  - Threat Hunting
    - A **proactive and hypothesis-driven approach** to detecting threats that may have slipped past traditional defenses.
    - Instead of waiting for alerts, hunters go looking for anomalies and patterns that indicate compromise.
      - Based on behavioral baselines and anomalies
      - Often uses MITRE ATT&CK as a reference
      - Leverages logs, endpoint telemetry, threat intel, and network traffic

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **The Intersection of SOAR, Machine Learning, AI, and Threat**

Element	Role in the Ecosystem
Threat Feeds	Provide **real-time intelligence** (e.g., malicious IPs, file hashes, threat actor TTPs).
Machine Learning (ML)	Learns patterns and detects **anomalies or unknown threats** across large datasets.
Artificial Intelligence (AI)	Drives **automated analysis, prioritization, and decision-making**.
SOAR	**Executes and orchestrates response workflows**, often fueled by the other components.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **The Intersection of SOAR, Machine Learning, AI, and Threat**
    - When orchestrated together:
      - Threat feeds update ML/AI tools with new Indicators of Compromise (IOCs).
      - ML/AI analyze inbound data, user behavior, or endpoint logs to identify suspicious activity.
      - SOAR ingests alerts, enriches them using threat intelligence, and executes automated containment steps like blocking IPs or isolating hosts.

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- **Automating Incident Response**
  - **The Intersection of SOAR, Machine Learning, AI, and Threat**
    - Imagine an attacker launches a phishing campaign. A **threat feed** flags the domain, **ML/AI** detect suspicious email patterns, **SOAR** kicks in to quarantine emails and block domains—all before users even notice.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- List and describe incident management steps.
- Know about third-party provided security services.
- Know about denial-of-service (DoS) attacks.
- Understand zero-day exploits.
- Understand man-in-the-middle attacks.
- Understand intrusion detection and intrusion prevention.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Describe honeypots and honeynets.
- Understand the methods used to block malicious code.
- Know the types of log files.
- Understand monitoring and uses of monitoring tools.

CISSP® MENTOR PROGRAM – SESSION TEN

Chapter 17 Preventing and Responding to Incidents

Domain 7.0: Security Operations

- Be able to explain audit trails.
- Understand how to maintain accountability.
- Describe threat feeds and threat hunting.
- Know the benefits of SOAR.

CISSP® MENTOR PROGRAM – SESSION TEN

SESSION 11 - FIN

We made it! Next Session Info

Session 11 – Chapter 18/Chapter 19 (pg. 869-945)

Lesson

- Disaster Recovery Planning
- Investigations and Ethics

Instructor: Ryan Cloutier

Lesson Release: 6/25 (after Session 10)

Live Mentor Session: 7/2