CISSP Domain 7: Security Operations

1. Introduction to Security Operations

- **Definition:** Security Operations focuses on the continuous monitoring, management, and enhancement of security measures to safeguard organizational assets and information.
- **Goals:**
    1. Maintain **Confidentiality, Integrity, and Availability (CIA)**.
    2. Minimize downtime.
    3. Optimize security responses.
- **Key Principles:**

    1. Least Privilege: Grant only the permissions necessary for job functions.
    2. Need-to-Know: Restrict access to sensitive information based on operational necessity.

---

2. Incident Management and Response

- **Incident Response Lifecycle (NIST SP 800-61):**

    1. **Preparation:** Develop incident response policies, procedures, and training.
    2. **Detection & Analysis:** Identify incidents through tools like IDS, IPS, SIEM, or anomaly detection.
    3. **Containment:** Prevent the spread of the incident (e.g., isolate infected systems).
    4. **Eradication:** Remove the root cause (e.g., delete malware, apply patches).
    5. **Recovery:** Restore systems and validate normal functionality.
    6. **Post-Incident Activities:** Conduct lessons learned and update policies.

- **Types of Incidents:**

    - **Malware:** Viruses, ransomware, worms.
    - **Insider Threats:** Misuse of privileges by employees.
    - **Phishing:** Social engineering to steal sensitive information.
    - **Distributed Denial-of-Service (DDoS):** Overloading systems to disrupt availability.
    - **Advanced Persistent Threats (APTs):** Long-term, stealthy attacks.
- **Legal Considerations:**

    - **Chain of Custody:** Maintain evidence integrity.
    - Admissibility of Evidence: Ensure compliance with jurisdictional laws.

---

3. Investigation and Forensics

- **Digital Forensics Process:**

    1. **Data Acquisition:** Collect evidence using forensically sound methods (e.g., imaging tools).
    2. **Examination:** Search for relevant artifacts (e.g., logs, file metadata).
    3. **Analysis:** Interpret findings to draw conclusions.
    4. **Reporting:** Document results for stakeholders or legal proceedings.

- **Tools:** FTK, EnCase, Sleuth Kit.
- **Log Management:** Collection, retention, and analysis of logs for accountability and troubleshooting.
- **E-Discovery:** Identifying, collecting, and delivering electronic evidence.

---

4. Resource Protection

- **Media Management:**

    - Storage: Use encrypted and labeled storage devices.
    - Transportation: Secure transit of sensitive data.
    - Disposal: Use secure methods (e.g., degaussing, shredding).
- **Physical Security:**

    - Perimeter Defenses: Fences, gates, guards.
    - Secure Areas: Access-controlled server rooms.
    - Environmental Controls: HVAC systems, fire suppression (e.g., clean agents like FM-200).

---

5. Change and Patch Management

- **Change Management:**

    - **Configuration Management:** Maintain secure baseline configurations and track changes.
    - **Change Control Board (CCB):** Formal review and approval of changes.
- **Patch Management:**

    - Evaluate vulnerabilities and prioritize patches based on risk.
    - Test patches before deployment to avoid disruptions.

6. Disaster Recovery (DR) and Business Continuity Planning (BCP)

- **Disaster Recovery Planning:**
    - **Recovery Time Objective (RTO):** Maximum acceptable time to restore operations.
    - **Recovery Point Objective (RPO):** Maximum acceptable data loss in terms of time.
    - **Maximum Tolerable Downtime (MTD):** Total time a system can be offline without significant harm.
- **BCP Strategies:**
    - **Hot Site:** Fully operational with real-time replication.
    - **Warm Site:** Partially prepared with some equipment.
    - **Cold Site:** Basic infrastructure, requiring setup before use.
- **Testing Plans:**
    - Full-Interruption Tests: Complete system shutdowns.
    - Simulation Tests: Mimic actual events without disruption.
    - Tabletop Exercises: Team discussions on response scenarios.

---

7. Backup Strategies

- **Types of Backups:**
    - Full Backup: Complete copy of all data.
    - Incremental Backup: Copies only data changed since the last backup.
    - Differential Backup: Copies all changes since the last full backup.
- **Backup Locations:**
    - On-Site, Off-Site, and Cloud-Based.
- **Frequency:** Depends on data criticality and RPO requirements.

---

8. Vulnerability and Threat Management

- **Vulnerability Assessments:** Identify and evaluate potential security weaknesses.
- **Patch Management:** Regularly apply updates to address known vulnerabilities.
- **Threat Intelligence:** Proactively identify adversary tactics and potential threats.

---

9. Security Operations Center (SOC)

- **SOC Functions:**
    - Centralized monitoring of network activity.
    - Log aggregation and analysis.
    - Real-time incident response.
- **SOC Models:**
    - In-House: Full control, resource-intensive.
    - Outsourced: Cost-effective but less control.
    - Hybrid: Combination of in-house and outsourced resources.

---

10. Personnel Safety and Security

- **Safety Concerns:** Include workplace violence, natural disasters, and pandemics.
- **Personnel Screening:** Background checks, role-based access control.
- **Awareness Training:** Regular security education for staff to mitigate risks.

---

11. Preventive and Detective Measures

- **Preventive Controls:**
    - Firewalls, Access Controls, Encryption, Anti-Malware Solutions.
- **Detective Controls:**
    - Intrusion Detection Systems (IDS), Security Audits, CCTV Surveillance.

---

12. Key Metrics and Monitoring

- **Metrics to Measure:**
    - SLA Compliance.
    - MTTR (Mean Time to Repair): Time to resolve an incident.
    - MTTD (Mean Time to Detect): Time to identify an incident.
- **Tools:** SIEM, Dashboards, and Ticketing Systems.

One-Page Summary of Key Points

1. **Incident Response:** Six stages: Preparation, Detection, Containment, Eradication, Recovery, Post-Incident.
2. **Logging and Monitoring:** Use SIEM to aggregate logs for analysis; ensure audit trails are intact.
3. **Vulnerability Management:** Conduct scans and apply patches methodically.
4. **Backup Types:** Full, incremental, differential; test backups regularly.
5. **BCP and DRP:** Key terms: RTO (Recovery Time Objective) and RPO (Recovery Point Objective).
6. **Physical Security:** Protect systems using environmental controls and secure perimeters.
7. **Legal and Forensics:** Preserve evidence integrity with chain of custody.
8. **Advanced Threats:** Use IDPS and threat intelligence for proactive defenses.

Exam Preparation Summary

- **Incident Response Lifecycle:** Preparation, Detection, Containment, Eradication, Recovery, Post-Incident Review (NIST SP 800-61).
- **Key Metrics:**
    - RTO (How quickly to restore operations).
    - RPO (Acceptable data loss in time).
    - MTD (Maximum tolerable downtime).
- **Forensic Practices:** Chain of custody, tools (EnCase, FTK).
- **Backup Types:** Full, Incremental, Differential.
- **DRP/BCP:** Hot, Warm, Cold sites for recovery.

Exam Tips and Mnemonics

1. **Incident Response Stages (Mnemonic): Prepare Dogs Carry Emergency Rations Post-incident.**
2. **Backup Hierarchy: Full > Incremental > Differential** (Full is largest, incremental is smallest).
3. **Key Differences:**
    - **RTO:** How quickly you restore operations.
    - **RPO:** How much data loss is acceptable.

4. **Forensics Rule:** Always maintain the **Chain of Custody**.
5. **SOC Models: In-house** (control) vs. **Outsourced** (cost-effective).

Expected Questions and Answers (Beginner to Advanced)

Beginner-Level Questions:

Q: What is the primary goal of least privilege?
A: To limit user access to only the information and resources necessary for their job responsibilities.

Q: What are the six stages of the incident response lifecycle?
A: Preparation, Detection & Analysis, Containment, Eradication, Recovery, and Post-Incident Activities.

Q: What is the difference between a hot site and a cold site?
A: A hot site is a fully operational alternate facility with near-real-time replication, while a cold site is a facility with basic infrastructure but no pre-installed systems or data.

Q: Define "change management."
A: A systematic process to ensure that changes to IT systems are reviewed, approved, and tested before implementation.

Q: What is an audit trail used for?
A: To track system activities for accountability, troubleshooting, and forensic investigations.

Intermediate-Level Questions:

Q: What is a SIEM and why is it important?
A: A Security Information and Event Management (SIEM) system aggregates, analyzes, and correlates logs from multiple sources to detect and respond to security incidents.

Q: How does job rotation improve security?
A: By exposing employees to different roles, it reduces the risk of collusion and fraud while improving knowledge transfer.

Q: What is chain of custody, and why is it critical in digital forensics?
A: Chain of custody documents the handling of evidence to ensure its integrity for legal proceedings.

Q: Explain the difference between a vulnerability scan and a penetration test.
A: A vulnerability scan identifies potential weaknesses, while a penetration test actively exploits vulnerabilities to assess their impact.

Q: What are incremental and differential backups?
A: Incremental backups save only data changed since the last backup, while differential backups save all data changed since the last full backup.

Advanced-Level Questions:

Q: What is a playbook in incident response?
A: A predefined set of procedures tailored to respond to specific incident types.

Q: What is data masking, and when is it used?
A: Data masking obscures sensitive information, often used in non-production environments to protect data integrity.

Q: How does an Intrusion Prevention System (IPS) differ from an Intrusion Detection System (IDS)?
A: An IPS actively blocks malicious activities, while an IDS only detects and alerts on suspicious behavior.

Q: What is the purpose of job rotation and separation of duties?
A: To reduce fraud risk, detect collusion, and promote knowledge transfer.

Q: Describe the role of threat intelligence in security operations.
A: Threat intelligence provides insights into adversary tactics, techniques, and procedures (TTPs) to improve proactive defenses.

Scenario-Based Questions:

Scenario: Your organization has detected ransomware on critical servers. How would you respond?

1. Preparation: Verify IRP and gather response team.
2. Detection/Analysis: Analyze ransomware type, assess scope.
3. Containment: Disconnect infected systems from the network.
4. Eradication: Remove ransomware and patch vulnerabilities.
5. Recovery: Restore systems from backups.
6. Post-Incident: Conduct lessons learned to prevent recurrence.

Scenario: A team member with privileged access is suspected of unauthorized data access. What steps would you take?

A: Log analysis, privilege review, isolate suspected accounts, and notify HR/legal.

Scenario: A company experiences frequent DDoS attacks. Suggest mitigation techniques.

A: Implement rate-limiting, use anti-DDoS services, configure firewalls to block malicious traffic, and monitor network traffic patterns.

Scenario: Your backup restoration process fails during a DR drill. What actions should you take?

A: Validate backup integrity, review DRP steps, test alternate backups, and update DRP documentation.

Scenario: An insider shares sensitive data with a competitor. What steps should be taken?

A: Investigate through log analysis, preserve evidence, engage legal/HR, and implement stricter controls.

Numerical Questions:

Q: If a company's RTO for a critical system is 4 hours and the system fails at 2:00 PM, by what time must the system be restored?
A: By 6:00 PM.

Q: Calculate RPO: If the last backup was at 10:00 AM and the system failed at 4:00 PM, how much data could be lost?
A: Up to 6 hours of data could be lost.

Q: What is the total time to recover if RTO is 4 hours and RPO is 2 hours?
A: Recovery involves restoring within 4 hours and restoring up to 2 hours of lost data.

Q: If a vulnerability scan identifies 200 vulnerabilities, and the remediation team addresses 20% per week, how many vulnerabilities remain after 2 weeks?
A: 200 x 0.8 x 0.8 = 128 vulnerabilities.

Q: During an incident, logs show a spike in traffic from IP 192.168.1.100 generating 10,000 requests per second. How would you mitigate this?
A: Block the IP at the firewall, analyze traffic patterns, and verify legitimate users.