



Domain 4: Security Operations (28%)

◆ 4.1 Incident Response



Incident Response Process (NIST 800-61)

1. Preparation

- Create policies, procedures, IR plans.
- Train employees.
- Ensure logging and alerting are enabled.

2. Detection & Analysis

- Identify signs of compromise.
- Confirm if it's truly an incident (false positives?).
- Tools: IDS/IPS, SIEM, antivirus, EDR.

3. Containment

- Stop the spread (short-term vs long-term).
- Quarantine affected systems.

4. Eradication


- Remove malware, close vulnerabilities.

5. Recovery

- Restore systems from backups.
- Monitor for re-infection.

6. Lessons Learned

- Create after-action reports (AAR).
- Improve policies and detection mechanisms.

 **Tip:** Know the **order** and **purpose** of each phase. Containment happens **before** eradication!


◆ 4.2 Detection and Monitoring

Security Tools

Tool	Description
SIEM	Collects and analyzes logs for alerting
SOAR	Automates incident response playbooks
NDR	Network-based detection
EDR	Detects suspicious endpoint behavior
UEBA	Detects anomalies based on user behavior

Log Sources

- Firewalls, IDS/IPS, endpoints
- Windows Event Logs
- Syslog (Linux, network devices)
- Cloud logs (AWS CloudTrail, Azure Monitor)

 Enable **centralized log collection**, set **retention policies**, and monitor **critical events** like logins, privilege escalation, or config changes.

Alerting and Tuning

- **False positive:** Normal activity incorrectly flagged as malicious.
 - **False negative:** Malicious activity missed by the system.
 - **Tuning:** Adjust detection rules to reduce noise and improve accuracy.
-

◆ 4.3 Threat Hunting and Intelligence

Threat Hunting

- Proactive activity to find threats **not detected by tools**.
- Uses hypothesis-based approach.
- Based on:
 - Indicators of Compromise (IOCs)
 - Tactics, Techniques, Procedures (TTPs)
 - Threat intelligence feeds

Threat Intelligence Types

Type	Description	Example
Strategic	High-level trends	Nation-state targeting finance
Tactical	TTPs of threat actors	MITRE ATT&CK use of PowerShell
Operational	Current campaigns	Malware spreading via phishing
Technical	IPs, hashes, URLs	Blacklisted IP 188.166.x.x

✓ Understand **how** and **why** threat intel is used — especially in **SIEMs** and **hunting**.


◆ 4.4 Vulnerability Management

Process Overview

1. **Identify** assets and vulnerabilities (use scanners)
2. **Prioritize** based on risk and criticality
3. **Remediate** vulnerabilities (patches, configs)
4. **Verify** fixes are successful
5. **Report** and improve process

Vulnerability Scanners

- Tools: Nessus, OpenVAS, Qualys
- Look for:
 - Outdated software
 - Missing patches
 - Misconfigurations

 False positives are common! Not every finding is exploitable.

◆ 4.5 Patch and Change Management

🧩 Patch Types

Patch Type	Description
Security	Fixes vulnerabilities
Bug fix	Resolves functional issues
Feature update	Adds functionality

🔄 Patch Management Process

1. Test in dev environment
2. Approve through change control
3. Deploy to production
4. Document changes

✅ Patching must follow a **formal change management policy** to avoid breaking systems.


◆ 4.6 Digital Forensics

🔍 Forensic Process

1. **Identify** what needs to be collected
2. **Preserve** evidence (write blockers, hash verification)
3. **Collect** data from devices
4. **Examine** for artifacts (browser history, logs, registry)
5. **Analyze** connections, time stamps, file access
6. **Report** findings (maintain chain of custody)

Evidence Types

- **Volatile:** RAM, network sessions — must be collected first.
- **Non-volatile:** Hard drives, USBs — persists after shutdown.

 Always maintain **chain of custody** — document who accessed what and when!

◆ 4.7 Response to Common Threats

Common Threat Types

Threat	Description	Example
Phishing	Email-based deception	Fake login pages
Ransomware	Encrypts files for ransom	WannaCry
DDoS	Disrupts availability	Botnet floods
Insider Threat	Employee misuse	Sabotage, data theft
Supply Chain	Compromise through 3rd parties	SolarWinds attack

 Know **how to detect** and **respond** to these threats using logs, alerts, containment plans.

◆ 4.8 Security Assessments

Assessment Types

Type	Description
Vulnerability Scan	Automated scan, non-intrusive
Penetration Test	Simulates real attacks
Red Team	Offensive testers (simulate adversary)
Blue Team	Defensive analysts
Purple Team	Collaboration between red and blue

 Pen testing **requires written authorization** and must follow scope rules.

◆ 4.9 Data Loss Prevention (DLP)

- Prevents unauthorized **transfer of sensitive data**.
- Can monitor:
 - **Data in use** (on endpoint)
 - **Data in motion** (on network)
 - **Data at rest** (on storage)
- Alerts or blocks actions like:
 - Uploading customer data to cloud
 - Copying files to USB

Key Takeaways for Domain 4

- Understand **incident response steps** clearly (NIST model).
 - Know the difference between **SIEM, SOAR, EDR, NDR, UEBA**.
 - Be able to identify vulnerabilities, prioritize, and patch correctly.
 - Know how to perform basic **forensics** and **threat hunting**.
 - Understand **common attack types** and proper responses.
 - Be familiar with **DLP, change control, and threat intelligence types**.
-