www.wisemancybersec.com
info@wisemancybersec.com

CISSP Domain 7:

SECURITY OPERATIONS — EXAM-READY CHEATSHEET

WISEMAN CYBERSEC
BE WISE , BE SECURE

Core Concept

- Security Operations ensures that day-to-day security tasks are performed to protect information assets, detect incidents, and maintain resilience.
- **Focus areas:** Monitoring, Incident Handling, Forensics, Logging, Recovery, Investigations, and Continuous Improvement.

Key Principles of Security Operations

Principle	Description	Example
Least Privilege	Give users only the access necessary for their role	Admin rights only for system changes
Separation of Duties	Split tasks to prevent fraud/errors	One person initiates, another approves
Job Rotation	Rotating roles to prevent collusion and detect fraud	Network admin shifts every 6 months
Mandatory Vacations	Absence may reveal hidden fraud or malpractice	Policy in financial or admin roles
Need-to-Know	Access only to data required for specific tasks	HR doesn’t see financial records
Change Management	Formal process to evaluate and approve changes	All system changes logged & approved

Logging, Monitoring & Detection

- **SIEM (Security Information and Event Management):** Correlates logs from multiple systems to detect anomalies.
- **Log Management:** Retain logs based on regulatory needs (e.g., PCI DSS = 1 year).
- **Monitoring Types:**
  - *Real-time monitoring* (live alerts)
  - *Passive monitoring* (review later)
- **Detection Methods:**
  - Signature-based (known threats)
  - Anomaly-based (behavioral deviation)
  - Heuristic (AI/ML-driven detection)

Incident Response (IR) Process

Step	Description
1. Preparation	Build IR team, define procedures, tools, contacts
2. Detection & Analysis	Identify unusual activity, verify incident
3. Containment	Isolate affected systems to prevent spread
4. Eradication	Remove root cause (malware, vulnerabilities)
5. Recovery	Restore systems and monitor for reoccurrence
6. Lessons Learned	Document incident, improve response process

IR Roles:

- Incident Manager (coordinates actions)
- Forensic Analyst (collects evidence)
- Comms Officer (handles internal/external info)

Digital Forensics Basics

Phase	Key Activity
Identification	Recognize potential evidence
Preservation	Secure and protect evidence integrity
Collection	Gather data using forensic tools
Examination	Analyze to extract relevant info
Analysis	Interpret evidence for conclusions
Reporting	Document findings for legal/disciplinary use

Chain of Custody:

- Chronological documentation of evidence handling — who, what, when, where, and how.

Tools: EnCase, FTK, Autopsy, Volatility, Wireshark.

Disaster Recovery (DR) & Business Continuity (BC)

Key Concepts

- **RTO (Recovery Time Objective):** Time to restore after disruption.
- **RPO (Recovery Point Objective):** Acceptable data loss measured in time.
- **MTD (Maximum Tolerable Downtime):** Total downtime business can handle before failure.

Backup Strategies

Type	Description
Full	Entire data set copied each time
Incremental	Copies only data changed since last backup
Differential	Copies data changed since last *full* backup

Recovery Sites

Type	Features	Activation Time
Hot Site	Fully operational mirror site	Minutes–Hours
Warm Site	Partially equipped, requires config	Hours–Days
Cold Site	Empty facility, needs full setup	Days–Weeks
Mobile Site	Portable recovery setup	Flexible

Security Operations Center (SOC)

SOC Functions:

- Continuous monitoring
- Threat intelligence integration
- Incident triage and escalation
- Log correlation
- Metrics reporting

SOC Tiers:

Tier	Role
Tier 1	Alert monitoring & triage
Tier 2	Deep analysis, correlation
Tier 3	Threat hunting, forensics, remediation

Vulnerability & Patch Management

Process	Description
Identification	Use scanners like Nessus, Qualys
Assessment	Prioritize by CVSS score and business impact
Remediation	Apply patches, mitigations
Verification	Validate successful application
Reporting	Track closure and exceptions

CISSP Tip: Know CVSS base metrics: Exploitability, Impact, Temporal, Environmental.

Change & Configuration Management

- **Configuration Control:** Baseline known-good system state.
- **Change Control:** All modifications must be authorized and documented.
- **Rollback Plan:** Always have a fallback procedure before changes.

Preventive & Detective Controls

Type	Example
Preventive	Firewalls, Access Controls, Encryption
Detective	IDS/IPS, SIEM, Log Audits
Corrective	Backup Restore, Antivirus Cleanup
Compensating	Temporary MFA until patch applied
Deterrent	Security Awareness Training

Personnel Security & Awareness

- **Background Checks:** Before hiring sensitive positions.
- **Termination Procedures:** Immediately revoke access, conduct exit interview.
- **Security Awareness Training:** Phishing, reporting, data handling.
- **Privileged Account Management:** Rotate, monitor, and log all admin activity.

Monitoring Tools & Metrics

Tool	Purpose
SIEM (Splunk, QRadar)	Log correlation, alerts
SOAR	Automate incident workflows
EDR/XDR	Endpoint visibility & response
NDR	Network anomaly detection

KPIs: MTTR (Mean Time to Respond), MTBF (Mean Time Between Failures), Incident Frequency, SLA Compliance.

Third-Party & Outsourced Security

- Include security clauses in **SLAs** (response time, breach notification).
- Conduct **vendor risk assessments** regularly.
- Ensure **data handling and destruction policies** align with regulations.

Environmental & Physical Security

- **HVAC** (Temperature/Humidity Control)
- **Fire Suppression:**
  - Water (non-electrical), CO_2, FM-200, Halon alternatives
- **Power:** UPS, Generators, Redundancy
- **Personnel Safety:** Emergency exits, CCTV, Access badges

Exam Traps & Quick Tips

- *Know sequence*: IR → DR → BC.
- Understand difference: **Hot vs. Warm vs. Cold Site.**
- Memorize **Evidence Handling Steps** and **Chain of Custody**.
- Be familiar with **Backup Types & Restoration Sequence.**
- Differentiate **Incident vs. Event vs. Alert.**
- *CISSP mindset*: Always choose answers that **protect confidentiality, integrity, and availability** while **minimizing business disruption**.

Key Takeaway

Security Operations is the “heartbeat” of cybersecurity — where plans become actions, and incidents become lessons.
Master this domain to **connect theory with real-world defense** — exactly what the CISSP exam tests.