Exam Cram Notes: Security Monitoring

1. Overview

Security monitoring involves **continuous observation, analysis, and detection** of suspicious activities, unauthorized access, and potential threats within an organization's IT environment. Effective monitoring helps in **early detection of incidents, compliance, and rapid response to security breaches**.

---

2. Security Monitoring Components

A. Log Management & Analysis

✅ **Centralized Log Collection –** Aggregates logs from various sources (servers, firewalls, applications) into a central repository.
✅ **Log Retention Policies –** Determine how long logs are kept based on compliance and forensic needs (e.g., GDPR, HIPAA).
✅ **Log Analysis** – Identifies unusual patterns, errors, or security incidents.

🔷 **Tools:** Syslog, Windows Event Viewer, Fluentd

B. Network Monitoring

✅ **NetFlow & Packet Capture –** Analyzes network traffic for anomalies.
✅ **Intrusion Detection Systems (IDS) –** Monitors network traffic for known attack signatures.
✅ **Intrusion Prevention Systems (IPS) –** Actively blocks detected threats.
✅ **Anomaly-Based Detection** – Identifies deviations from normal traffic behavior.

🔷 **Tools:** Wireshark, SolarWinds, Snort, Suricata

C. Endpoint Monitoring

✅ **Endpoint Detection & Response (EDR) –** Provides real-time visibility into endpoint activities, detecting and responding to threats.
✅ **Host-Based Intrusion Detection Systems (HIDS) –** Monitors system files and logs for suspicious changes.
✅ **Application Whitelisting –** Only allows authorized applications to run, blocking unauthorized software.

🔷 **Tools:** CrowdStrike, Carbon Black, Microsoft Defender for Endpoint

D. User Activity Monitoring

✅ **User Behavior Analytics (UBA) –** Detects anomalies in user behavior that may indicate insider threats or compromised accounts.
✅ **Privileged Access Management (PAM) –** Monitors activities of users with elevated

privileges.
✅ **Session Recording –** Records user sessions for auditing and forensic purposes.

🔷 **Tools:** Splunk UBA, SolarWinds UAM, ObserveIT

---

3. Security Information and Event Management (SIEM)

A. Key Features of SIEM

✅ **Log Aggregation –** Collects logs from multiple sources for centralized analysis.
✅ **Correlation Rules** – Identifies complex attack patterns by correlating events across systems.
✅ **Real-Time Alerts –** Notifies administrators of potential security incidents.
✅ **Threat Intelligence Integration –** Enriches alerts with external threat data.
✅ **Automated Response (SOAR) –** Responds to incidents using pre-defined playbooks.

🔷 **Tools:** Splunk, ArcSight, IBM QRadar, Microsoft Sentinel

B. Common Use Cases

✅ **Detecting Brute Force Attacks –** Multiple failed login attempts from different IPs.
✅ **Identifying Data Exfiltration –** Unusual outbound data transfer volumes.
✅ **Monitoring Suspicious User Behavior –** Login attempts from unfamiliar locations.
✅ **Detecting Malware Infections –** Communication with known malicious IPs.

---

4. Network Traffic Analysis

A. Traffic Analysis Techniques

✅ **Deep Packet Inspection (DPI) –** Examines packet contents for threats.
✅ **NetFlow Analysis –** Tracks source/destination, bandwidth, and protocol usage.
✅ **Signature-Based Detection** – Identifies known attack patterns (e.g., SQL injection, DDoS).
✅ **Behavioral Analysis –** Learns normal behavior to identify anomalies (e.g., unusual port usage).

🔷 **Tools:** Wireshark, NetFlow Analyzer, Zeek (Bro)

B. Common Threats Detected

✅ **DDoS Attacks –** High-volume traffic aimed at overwhelming services.
✅ **Man-in-the-Middle (MitM) Attacks –** Eavesdropping or altering communications.
✅ **Lateral Movement –** Attackers moving within the network to access critical systems.
✅ **Unauthorized Protocol Use –** Detection of Telnet, FTP, or other insecure protocols.

---

5. Threat Intelligence & Hunting

A. Threat Intelligence

✅ **Indicators of Compromise (IoCs) –** Known malicious IPs, URLs, file hashes.
✅ **Threat Feeds –** External data sources providing information on emerging threats (e.g., STIX/TAXII, VirusTotal).
✅ **Reputation Services –** Evaluate the risk level of IPs, domains, and files.

🔷 **Sources:** MITRE ATT&CK, AlienVault OTX, Recorded Future

B. Threat Hunting

✅ **Proactive Search for Threats –** Goes beyond automated detection, looking for hidden threats.
✅ **Hypothesis-Driven Investigation –** Based on potential attack scenarios.
✅ **YARA Rules** – Identify and classify malware based on patterns.

🔷 **Tools:** ThreatHunter, Velociraptor, GRR Rapid Response

---

6. Monitoring Cloud Environments

✅ **Cloud Access Security Brokers (CASB) –** Monitor and control cloud application usage.
✅ **Cloud Security Posture Management (CSPM) –** Detects misconfigurations in cloud environments (e.g., AWS, Azure).
✅ **Cloud Logging Services –** AWS CloudTrail, Azure Monitor, Google Cloud Operations.

---

7. Incident Response & Reporting

A. Incident Response Process

1. **Detection & Analysis** – Identify and assess incidents.
2. **Containment, Eradication, Recovery –** Limit impact, remove threats, restore services.
3. **Post-Incident Activities –** Document lessons learned, update response plans.

B. Reporting & Compliance

✅ **Regulatory Compliance –** Ensure adherence to GDPR, HIPAA, PCI-DSS.
✅ **Security Dashboards & Reports –** Provide insights into security posture for stakeholders.

---

8. Key Exam Takeaways

✅ **Centralize log collection and use SIEM** for correlation and analysis.
✅ **Monitor network traffic** with DPI, IDS/IPS, and NetFlow analysis.
✅ **Implement endpoint monitoring** with EDR and HIDS solutions.
✅ **Utilize threat intelligence feeds** to stay ahead of emerging threats.
✅ **Perform proactive threat hunting** to discover hidden attackers.
✅ **Regularly test incident response plans** and report security metrics.