COMPTIA SECURITY+ SY0-701 · WEEK 12

Security Monitoring and Enterprise Capabilities



Objectives 4.4 and 4.5 · 90-minute lesson

Presenter: Trapper Brown

What you will be able to do in 90 minutes

1. Describe the monitoring activities from log aggregation and alerting to archiving and alert response.
2. Compare monitoring tools such as SIEM, SCAP, NetFlow, SNMP traps, agents, and agentless collection.
3. Triage alerts, choose between quarantine and tuning, and explain why alert fatigue is a risk.
4. Modify firewall rules, access lists, IDS and IPS settings, and web and DNS filters for a scenario.
5. Explain how SPF, DKIM, DMARC, and an email gateway work together against spoofed mail.
6. Select secure protocols and ports, and apply Group Policy and SELinux to harden operating systems.
7. Match FIM, DLP, NAC, EDR, XDR, and user behavior analytics to the problems they solve.

AGENDA

9 min	What we monitor and how
10 min	Monitoring tools
6 min	Alert response, quarantine, and tuning
10 min	Exercise 1: triage the clinic's alerts
9 min	Firewalls, access lists, and IDS and IPS
7 min	Web filtering
9 min	Email security and DNS filtering
9 min	Operating system security and secure protocols
9 min	FIM, DLP, NAC, EDR, XDR, and UBA
9 min	Exercise 2: match the problem to the capability
3 min	Wrap-up

Collect, alert, report, archive, and respond

1. **Aggregate** — Collect logs from systems, apps, and network gear
2. **Alert** — Rules and correlation flag events worth a look
3. **Scan** — Check systems against baselines and known flaws
4. **Report** — Summarize trends and compliance for owners
5. **Archive** — Keep logs for the retention period, tamper-proof
6. **Respond** — Triage, quarantine, validate, and tune the rule

Each monitoring tool sees a different slice

Tool	What it does
SIEM	Aggregates and correlates logs, raises alerts
SCAP and benchmarks	Standard, automated checks against a baseline
Agents and agentless	Software on the host vs remote collection
SNMP traps	Device pushes an alert to the manager, UDP 162
NetFlow	Who talked to whom, when, and how much
AV, DLP, vuln scanners	Malware, data leaving, and known flaws

Contain the threat, then fix the noise

Quarantine and validate

- Isolate the host or file so it cannot spread
- Confirm whether the alert is a true positive
- Remediate, then validate the system is clean
- Record what happened in the ticket

Alert tuning

- Too many false positives cause alert fatigue
- Adjust thresholds, add context, suppress known good
- Never tune away a whole class of real attacks
- Retest the rule after every change

Exercise 1: triage the clinic's SIEM alerts



8

MINUTES · SMALL GROUPS

For each alert, decide true or false positive, severity, and the next action. Note any rule that needs tuning.

1. 1: 42 failed logins for jsmith from one external IP in 3 minutes
2. 2: A successful login for jsmith from that same IP right after
3. 3: AV flags a file on the billing PC and quarantines it
4. 4: Backup server sends 80 GB to the cloud backup provider at 2 a.m.
5. 5: NetFlow shows a front desk PC sending DNS to an unknown server
6. 6: SNMP trap: switch port 14 goes down and up 30 times an hour
7. 7: The same printer alert fires 300 times a day, every day

Rules decide what passes; IDS and IPS watch it

Firewall rules

Read top to bottom; first match wins; implicit deny

Access lists

Permit or deny by source, destination, and port

Ports and protocols

Open only what a service needs, nothing more

Screened subnet

Public servers sit apart from the internal network

Signatures

Match known attack patterns; miss new ones

Trends

Flag departures from normal behavior over time

Filter the web at the device or at the gateway

Agent-based

- Software on each device enforces the policy
- Works at home, in hotels, anywhere
- Must be deployed and updated on every device

Centralized proxy

- All web traffic passes one filtering point
- One place to manage policy and logs
- Misses devices that leave the network

Prove mail is real and block bad domains

Control	What it does	Where it lives
SPF	Lists servers allowed to send for the domain	DNS TXT record
DKIM	Signs messages so changes can be detected	Mail header, public key in DNS
DMARC	Policy for failures: none, quarantine, reject	DNS TXT record at _dmarc
Email gateway	Filters spam, malware, and phishing links	In front of the mail service
DNS filtering	Refuses to resolve known bad domains	Resolver or DNS security service

Choose the secure protocol and its port

Insecure	Secure choice	Port
Telnet	SSH	TCP 22
FTP	SFTP (over SSH) or FTPS	TCP 22, or TCP 990 for FTPS
HTTP	HTTPS (HTTP over TLS)	TCP 443
LDAP	LDAPS	TCP 636
SNMPv1 and v2c	SNMPv3	UDP 161, traps on UDP 162
POP3 and IMAP	POP3S and IMAPS	TCP 995 and TCP 993

Watch files, data, devices, and behavior

FIM

Alerts when a watched file or setting changes

DLP

Finds and blocks sensitive data leaving

NAC

Checks a device's identity and health before it joins

EDR

Records endpoint activity, detects, and responds

XDR

Correlates endpoint, network, cloud, and email data

UBA

Learns each user's normal and flags changes

Exercise 2: match the problem to the capability



7

MINUTES · PAIRS

For each clinic problem, name the objective 4.5 capability that fits best and one setting you would change.

1. Spoofed email claims to come from the clinic's own domain
2. Staff click links to newly registered phishing domains
3. A contractor plugs an unpatched laptop into an exam room jack
4. Someone changed the web server's login page overnight
5. Patient record numbers are being sent to personal webmail
6. A billing account downloads ten times its normal records
7. Admins still manage the firewall over Telnet
8. Ransomware ran on a laptop; you need to see what else it touched

REVIEW

Five questions: write your answers first

1. What is the difference between agent-based and agentless monitoring?
2. What does NetFlow record, and what does it not record?
3. Name the three DNS-based email authentication controls and what each does.
4. Why is alert tuning a security task and not just a convenience?
5. How does EDR differ from XDR?

TAKEAWAYS

Four things to take with you

01

Collect it, then correlate it

A SIEM turns scattered logs into alerts a person can act on.

02

Tune alerts or lose them

Noisy rules teach analysts to ignore alerts, including the real ones.

03

Layer the gateway controls

Firewall, IPS, web, DNS, and email filters each stop different attacks.

04

Watch endpoints and users

FIM, EDR, DLP, NAC, and UBA catch what the perimeter misses.

NEXT Lab 12: Log analysis and alert triage in a SIEM