STUDENT HANDOUT · WEEK 12

Security Monitoring and Enterprise Capabilities

SY0-701 objectives 4.4, 4.5. Notes, exercises, review questions, and the lab.

Name	
Date	

THIS WEEK YOU WILL

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.

KEY IDEAS

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	Alert tuning
Isolate the host or file so it cannot spread	Too many false positives cause alert fatigue
Confirm whether the alert is a true positive	Adjust thresholds, add context, suppress known good
Remediate, then validate the system is clean	Never tune away a whole class of real attacks
Record what happened in the ticket	Retest the rule after every change

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	Centralized proxy
Software on each device enforces the policy	All web traffic passes one filtering point
Works at home, in hotels, anywhere	One place to manage policy and logs
Must be deployed and updated on every device	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 1: 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.

#	Prompt	Your answer
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	

EXERCISE 2: 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.

#	Prompt	Your answer
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 QUESTIONS

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?

KEY TAKEAWAYS

- **Collect it, then correlate it.** A SIEM turns scattered logs into alerts a person can act on.
- **Tune alerts or lose them.** Noisy rules teach analysts to ignore alerts, including the real ones.
- **Layer the gateway controls.** Firewall, IPS, web, DNS, and email filters each stop different attacks.
- **Watch endpoints and users.** FIM, EDR, DLP, NAC, and UBA catch what the perimeter misses.

LAB 12: LOG ANALYSIS AND ALERT TRIAGE IN A SIEM

60 MINUTES

Use the free Wazuh virtual machine (OVA) from wazuh.com with your Ubuntu and Windows lab VMs as agents, or a free Elastic trial. If your computer cannot run a SIEM, use the sample auth.log and Windows Security log export your instructor provides. Generate test attacks only against your own lab VMs.

Steps

1. Import the Wazuh OVA into your hypervisor, start it, and open the dashboard in a browser at the address shown on its console. Give it at least 8 GB of memory if you can.
2. Install the Wazuh agent on your Ubuntu and Windows VMs with the commands the dashboard's deploy new agent page generates, and confirm both agents show as active.
3. Generate events. From your second VM, run ssh fakeuser@UBUNTU_IP and enter a wrong password ten times. On Windows, fail five logins, then run net user labtest * /add (it prompts for a password) and net localgroup Administrators labtest /add.
4. In the dashboard, find those events. Search for Windows event IDs 4625 (failed logon), 4720 (account created), and 4732 (member added to a security-enabled local group), and for the sshd failed password events from Ubuntu.
5. Without a SIEM, or as a cross-check, count failed SSH logins by source address in the log: grep 'Failed password' auth.log | awk '{print $(NF-3)}' | sort | uniq -c | sort -rn.
6. Triage three alerts. For each, record the time, source, account, what happened, true or false positive, severity, and the next action you would take.
7. Tune one rule. Pick a noisy or low-value alert and write the change you would make, such as a higher threshold, an exclusion for a known good source, or a higher severity for admin accounts, and the risk that change accepts.
8. Remove the test account with net user labtest /delete, then shut down or snapshot the SIEM VM, since it uses a lot of memory.

Hand in

A short triage report: screenshots of the events you found, a table of three triaged alerts with your decisions, and one paragraph describing the rule you would tune and why.

Questions to answer in your report

1. Which of your generated events would you treat as most serious in a real clinic, and why?
2. How did correlating events from two systems change your conclusion about any alert?
3. What risk does your tuning change accept, and how would you watch for it?
4. Which log source missing from your lab would you add first at Lakeside Family Clinic, and what would it show?