Title: WEEK 3 TASK

1) Correlate logs, detect anomalies, enrich data

Tools: Elastic Security, Security Onion (Elastic-based), Google Sheets

1. Log correlation (4625 ↔ outbound traffic)

1. Ingest sample logs. Import Windows Security logs (e.g., BOTS/Splunk sample or your own EVTX) into Elastic via Winlogbeat/Elastic Agent (windows/security). Use Event ID 4625 (failed logon) for correlation. (What 4625 means and fields to watch. ManageEngine)
2. Correlate to outbound. In Elastic's Discover (data view logs-* / winlogbeat-* / logs-windows.*), run a KQL like: event.code: "4625"

| keep @timestamp, winlog.event_data.IpAddress, user.name, host.name

Document (paste into Sheets)

| Timestamp | Event ID | Source IP | Destination IP | Notes |

|---|---|---|---|---|

| 2025-08-18 12:00:00 | 4625 | 192.168.1.100 | 8.8.8.8 | Suspicious DNS request |

Anomaly detection: high-volume egress

Create a Custom query rule (Elastic Security → Rules → Create new → *Custom query*). Query example (ECS): trigger when outbound volume bursts:

network.direction: "outbound" and network.bytes >= 1048576

---

2) Threat intelligence integration

Tools: Wazuh, AlienVault OTX, TheHive

Import an OTX feed into Wazuh

Configure Wazuh TI integrations to pull IOCs (OTX). Many deployments sync OTX alongside VirusTotal/MISP to match alerts with IP/domain indicators. (Wazuh + OTX/MISP/VT capability overview.

Tip: Also enable VirusTotal hash lookups in Wazuh for file alerts. (Official Wazuh VT integration.

Test IOC: Temporarily treat 192.168.1.100 as a mocked “malicious IP” via a local list or custom OTX pulse in a lab.

Alert enrichment with OTX

When Wazuh flags an event with a matched IP, enrich with OTX reputation. (OTX/VT lookup patterns**.**

Document (paste into sheet):

| Alert ID | IP | Reputation | Notes |

|---|---|---|---|

| 003 | 192.168.1.100 | Malicious (OTX) | Linked to C2 server |

Hunt for T1078 – Valid Accounts

In Wazuh’s Kibana app, search for non-system interactive/network logons to find suspicious use of valid creds, e.g.:

event.category: "authentication" and user.name != "SYSTEM"

Focus on odd hours, new sources, or lockouts. (Technique definition/intent)

---

3) Incident escalation practice

Tools: TheHive, Google Docs, (optional) Splunk SOAR/Phantom

TheHive – create/escalate a case

Create a High severity case for “Unauthorized access on Server-Y”, tag T1078. Assign Tier-2 and set tasks: *Contain host*, *Pull volatile data*, *Reset credentials*, *User validation*. (General TheHive case creation workflow; assign/notify team.)

SITREP (Google Docs)

Title: Unauthorized Access on Server-Y
Summary: Detected at 2025-08-18 13:00, IP 192.168.1.200, MITRE T1078 (Valid Accounts).
Actions: Isolated Server-Y at the switch, escalated to Tier-2, initiated credential resets, began forensic collection and timeline reconstruction, enabled additional detections for suspicious authentication.

Workflow automation (Splunk SOAR/Phantom)

Create a simple playbook: if severity == High → assign owner = Tier-2 queue, add tag Needs-IR, post Slack/Email to on-call.

---

4) Alert triage with threat intel

Tools: Wazuh, VirusTotal, AlienVault OTX

Triage simulation

Alert example in Wazuh:

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	192.168.1.101	High	Open

Checklist: verify command line, parent proc, user, lateral targets, recent logons, and any IOC hits.

IOC validation (VT + OTX)

- VirusTotal: IP/file/hash lookup (API v3 ip_addresses/{ip}, files/{sha256}). (VT refs)
- OTX: Check pulse hits/reputation and related indicators. (OTX usage)

---

5) Evidence preservation & analysis

Tools: Velociraptor, FTK Imager

Volatile data (Velociraptor)

From the Windows endpoint, run a collection with a query equivalent to:

SELECT * FROM netstat

using Velociraptor client/GUI to export CSV (network connections). (Netstat artifact usage pattern)

Memory acquisition & hashing

- **Acquire RAM via Velociraptor's Artifact.Windows.Memory.Acquisition or FTK Imager memory capture. (Velociraptor + FTK usage overview. Elasticsearch Python Client)**
- **Compute SHA-256 (sha256sum or FTK's hashing) and record in chain-of-custody.**

Evidence log (paste into doc):

| Item | Description | Collected By | Date | Hash Value |

|---|---|---|---|---|

| Memory Dump | Server-Y Dump | SOC Analyst | 2025-08-18 | <SHA256> |

---

6) Capstone: full SOC workflow simulation

Tools: Metasploit, Wazuh, CrowdSec, TheHive, Google Docs

Exploit Samba usermap_script on the target (Metasploitable 2):

Detection & triage (Wazuh)

Ensure Wazuh rules flag the exploit/lateral movement. Document:

| Timestamp | Source IP | Alert Description | MITRE Technique |

|---|---|---|---|

| 2025-08-18 14:00:00 | 192.168.1.101 | Samba exploit | T1210 |

(T1210 definition/context)