**THEORY**

**1. Advanced Log Analysis**

**Core Concepts**

* **Log Correlation:** The process of connecting events from multiple sources (firewall, endpoint, application logs) to identify coordinated malicious activity.
  + Example: Several failed login attempts on Windows (Event ID 4625) from 192.168.204.137 immediately followed by successful login attempts and large outbound transfers.
* **Anomaly Detection:** Identifying behaviors that deviate from normal baselines, such as logins from 192.168.204.138 at unusual hours or excessive Hydra brute-force attempts.
* **Log Enrichment:** Adding contextual metadata (geolocation of IP, user account type, device hostname) to raw logs to make them actionable.

**Expanded Learning Objectives**

* Build the ability to **cross-reference logs** to discover hidden attack patterns.
* Reduce **false positives** by applying correlation and enrichment.
* Understand how to spot **multi-stage attacks** by piecing together log trails.

**Practical Activities**

1. **Set up log forwarding** from the Debian VM (Suricata + system logs) and Windows 11 agent (Windows Event Logs).
2. **Simulate brute force attack** using Hydra from Debian (hydra -l admin -P rockyou.txt ssh://192.168.204.138).
3. Collect logs in Wazuh or Elastic.
4. Correlate Suricata alerts with Windows Event 4625 entries.

**Deliverables**

* A **correlation report** showing failed login attempts and Suricata alerts tied to the same attacker IP.
* Annotated diagrams illustrating how the logs fit together.

**2. Threat Intelligence Integration**

**Core Concepts**

* **Types of Threat Intel:**
  + Indicators of Compromise (IOCs) → IP addresses, hashes, domains.
  + TTPs (Tactics, Techniques, and Procedures) → adversary behavior mapped to **MITRE ATT&CK**.
  + Threat feeds (STIX/TAXII) → structured intel streams for SOCs.
* **SOC Integration:** Enhance alerts by automatically tagging them with intel (e.g., “IP 192.168.204.137 matches known brute-force activity in OTX feed”).
* **Proactive Hunting:** Using intelligence to form hypotheses, such as searching for **T1078 (Valid Accounts misuse)** when unusual logins are detected.

**Expanded Learning Objectives**

* Learn how to **ingest threat feeds** into Wazuh/Elastic.
* Develop the skill to **map detections to ATT&CK techniques**.
* Perform proactive hunting using external IOCs and observed logs.

**Practical Activities**

1. Connect AlienVault OTX threat feed to Wazuh.
2. Run enrichment on attacker IP (192.168.204.137) to see if it exists in public feeds.
3. Use MITRE ATT&CK Navigator to align Hydra brute force attempts with **T1110 (Brute Force)**.
4. Create a custom rule in Wazuh to trigger on IOC matches.

**Deliverables**

* Threat intel report showing how Hydra brute force attempts align with MITRE ATT&CK techniques.
* IOC list used in hunting activities.
* Dashboard screenshot of alerts enriched with threat intelligence.

**3. Incident Escalation Workflows**

**Core Concepts**

* **SOC Tiers:**
  + **Tier 1 (Triage):** Initial alert review and filtering.
  + **Tier 2 (Investigation):** Correlation, deeper analysis, and escalation.
  + **Tier 3 (Advanced):** Threat hunting, malware analysis, and forensic response.
* **Communication Protocols:** SITREPs, escalation templates, and manager briefings.
* **SOAR Automation:** Tools like Splunk SOAR auto-assign high-severity alerts, attach IOCs, and escalate to Tier 2 without manual input.

**Expanded Learning Objectives**

* Be able to **recognize escalation triggers** (e.g., Hydra brute force successful login).
* Draft structured SITREPs for management.
* Use **automation** to streamline escalation.

**Practical Activities**

1. Simulate unauthorized access from Debian VM (192.168.204.137) into Windows VM (192.168.204.138) using Hydra.
2. Generate a SITREP in Google Docs:
   * Title: *Unauthorized Access on Windows Agent*
   * Summary: Attack detected at 2025-09-16 13:00. Source: 192.168.204.137 → Destination: 192.168.204.138. Technique: MITRE T1110 (Brute Force).
   * Actions: Account isolated, case escalated to Tier 2.
3. Create a TheHive case with severity **High**.
4. Build a Splunk SOAR playbook that automatically escalates high-priority alerts.

**Deliverables**

* A SITREP in Google Docs (200 words).
* TheHive case JSON import file for the incident.
* SOAR playbook (screenshot or JSON export).