**Week 04: SOC TASKS  
Theoretical Summary**

**Advanced Log Analysis**

Log analysis is a cornerstone of modern security operations. Every digital system, whether a firewall, endpoint, or application produces logs that record activities, both normal and malicious. While individual logs provide useful insights, they often tell only part of the story. Advanced log analysis is about connecting the dots across multiple sources, identifying anomalies, and enriching raw data with additional context to uncover complex threats that might otherwise go unnoticed.

**Core Concepts**

**Log Correlation**

Security analysts rarely rely on a single log source. For example, a failed login attempt (Windows Event ID 4625) on its own might look harmless, but when correlated with suspicious outbound traffic, it could signal a brute-force attempt followed by successful compromise. Log correlation is the process of linking related events across systems to build a more complete narrative of attacker behavior. This approach reduces the chance of missing subtle but critical indicators of attack.

**Anomaly Detection**

Attackers frequently try to blend into normal activity. Detecting anomalies means identifying patterns that deviate from what is expected, such as unusual login times, repeated logins from unfamiliar geographies, or sudden spikes in data transfers. Analysts can use statistical baselines or rule-based alerts to flag such behavior. For instance, if a user who normally transfers a few kilobytes suddenly uploads gigabytes of data, this could point to exfiltration.

**Log Enrichment**

Raw logs are often too technical and lack sufficient context for fast decision-making. Enrichment adds valuable metadata to make analysis more meaningful. For example, attaching geolocation data to IP addresses, mapping user roles to account activity, or identifying whether a hash matches known malware in a threat feed all make logs more actionable. Enrichment transforms isolated data points into intelligence that can support quicker, more confident decisions.

**Key Objective**

The primary goal of advanced log analysis is to equip analysts with the ability to identify genuine threats while minimizing false positives. By correlating logs, detecting unusual behaviors, and enriching information with context, security teams can prioritize alerts, respond more effectively, and understand the broader picture of an incident.

**Advanced Log Analysis**

Log analysis is a cornerstone of modern security operations. Every digital system whether a firewall, endpoint, or application, produces logs that record activities, both normal and malicious. While individual logs provide useful insights, they often tell only part of the story. Advanced log analysis is about connecting the dots across multiple sources, identifying anomalies, and enriching raw data with additional context to uncover complex threats that might otherwise go unnoticed.

**Core Concepts**

**Log Correlation**

Security analysts rarely rely on a single log source. For example, a failed login attempt (Windows Event ID 4625) on its own might look harmless, but when correlated with suspicious outbound traffic, it could signal a brute-force attempt followed by successful compromise. Log correlation is the process of linking related events across systems to build a more complete narrative of attacker behavior. This approach reduces the chance of missing subtle but critical indicators of attack.

**Anomaly Detection**

Attackers frequently try to blend into normal activity. Detecting anomalies means identifying patterns that deviate from what is expected, such as unusual login times, repeated logins from unfamiliar geographies, or sudden spikes in data transfers. Analysts can use statistical baselines or rule-based alerts to flag such behavior. For instance, if a user who normally transfers a few kilobytes suddenly uploads gigabytes of data, this could point to exfiltration.

**Log Enrichment**

Raw logs are often too technical and lack sufficient context for fast decision-making. Enrichment adds valuable metadata to make analysis more meaningful. For example, attaching geolocation data to IP addresses, mapping user roles to account activity, or identifying whether a hash matches known malware in a threat feed all make logs more actionable. Enrichment transforms isolated data points into intelligence that can support quicker, more confident decisions.

**Key Objective**

The primary goal of advanced log analysis is to equip analysts with the ability to identify genuine threats while minimizing false positives. By correlating logs, detecting unusual behaviors, and enriching information with context, security teams can prioritize alerts, respond more effectively, and understand the broader picture of an incident.

**Incident Escalation Workflows**

Incident escalation is the bridge between detection and resolution. In any security operations center (SOC), analysts constantly face a flood of alerts, not all of which are critical. Without a structured escalation process, serious incidents can be overlooked, miscommunicated, or delayed—leading to major consequences. Incident escalation workflows ensure that potential threats are systematically evaluated, prioritized, and communicated to the right people at the right time.

**Core Concepts**

**SOC Tier Structure**

Most SOCs operate in tiers, with responsibilities divided to maximize efficiency:

* **Tier 1 (Triage**): Frontline analysts review incoming alerts, dismiss false positives, and escalate suspicious activity.
* **Tier 2 (Investigation):** Analysts dig deeper into escalated cases, correlating logs, applying threat intelligence, and determining scope and impact.
* **Tier 3 (Advanced Analysis/Threat Hunting):** Senior analysts handle highly complex cases, perform malware reverse engineering, or respond to sophisticated adversaries.
* This tiered structure ensures that simple tasks don’t consume senior resources, while complex attacks receive expert attention.

**Escalation Criteria**

Not every alert needs escalation. Analysts decide based on:

* **Severity:** Potential business impact if the activity is malicious.
* **Complexity:** Whether Tier 1 tools/processes can resolve the issue.
* **Confidence:** Level of certainty based on evidence (correlated logs, threat intel matches, anomaly detection).

**Communication Protocols**

Escalation is not just technical—it’s also about clear communication. Standardized formats like Situation Reports (SITREPs) summarize what happened, when it was detected, affected systems, and actions taken so far. These reports allow Tier 2/3 analysts and managers to quickly understand the situation without sifting through raw logs.

**Automation in Escalation**

Security Orchestration, Automation, and Response (SOAR) platforms streamline escalation by:

* Automatically enriching alerts (e.g., attaching threat intel lookups).
* Assigning cases to the appropriate tier based on severity.
* Notifying stakeholders through integrated ticketing systems.

This reduces response time and ensures consistency in handling incidents.

**Example Workflow**

A simplified escalation workflow can be visualized as follows:

1. **Alert Generated** → SIEM flags suspicious login activity.
2. **Tier 1 Triage** → Analyst reviews logs:
   * Confirms login attempts came from unusual geolocation.
   * Sees correlation with failed logins (Event ID 4625).
   * Checks enrichment (IP flagged as malicious in OTX).
   * Marks case as “Suspicious” and escalates.
3. **Tier 2 Investigation** → Receives SITREP with key details. Analyst:
   * Correlates with firewall logs (outbound traffic to same IP).
   * Confirms multiple accounts involved.
   * Assesses business impact (critical server access).
   * Escalates to Tier 3 for containment.
4. **Tier 3 Analysis** → Senior analyst performs deeper investigation:
   * Collects volatile memory, reviews artifacts.
   * Engages IR team for containment (isolate server, revoke compromised credentials).
   * Communicates with management on risk.
5. **Management Notification** → Clear, non-technical briefing provided to decision-makers.
6. **Case Closure** → Incident documented, lessons learned fed back into playbooks.

This workflow ensures no critical step is missed and each escalation level adds more value without duplicating efforts.

**Key Objective**

The main objective of escalation workflows is to ensure that every incident receives the right level of attention, with the right information, at the right time. Proper workflows reduce alert fatigue, prevent delays in response, and maintain trust between SOC analysts, technical teams, and business stakeholders.