Security Operations Center (SOC) Week3 – Theory

Introduction

This report outlines three critical areas of theoretical knowledge required in modern Security Operations Center (SOC) practices: **Advanced Log Analysis**, **Threat Intelligence Integration**, and **Incident Escalation Workflows**. Each section provides definitions of key concepts with practical examples to strengthen understanding.

1. **Advanced Log Analysis**

Advanced Log Analysis is the process of examining, correlating, and enriching logs from multiple sources (firewalls, endpoints, applications) to detect patterns, anomalies, and potential security incidents.

- **Log Correlation**: The process of linking logs from multiple sources (firewalls, endpoints, applications) to identify patterns that may indicate an attack.
  Example: Connecting multiple failed login attempts (Event ID 4625) with suspicious outbound traffic to detect a brute-force attack followed by possible data exfiltration.

- **Anomaly Detection**: A method of identifying unusual or suspicious activity in logs by comparing against normal patterns of behavior.
  Example: Detecting a user logging in at 3 AM when their usual login hours are between 9 AM–6 PM.

- **Log Enrichment**: The practice of adding extra context to raw log data to improve accuracy and reduce false positives.
  Example: Tagging an IP address with geolocation data to identify if a login attempt originated from an unexpected country.

Steps

1. Logs from Windows endpoints and firewalls were ingested into **Elastic Security**.
2. Used the **KQL (Kibana Query Language)** to search for multiple failed login events (Event ID 4625).
3. Correlated these failed login attempts with outbound network traffic logs.
4. Applied **GeoIP enrichment** on source IPs to determine the origin of login attempts.
5. Checked whether traffic destinations were related to known suspicious IPs.

Example

During analysis in Elastic Security, multiple failed login events were observed from 192.168.1.50. Within 10 minutes of repeated failures, successful logins occurred followed by outbound traffic to 185.244.25.17. GeoIP enrichment flagged this IP as originating from Eastern Europe. This correlation indicated a brute-force attack followed by possible data exfiltration. The case was escalated for further investigation.

2. **Threat Intelligence Integration**
   Threat Intelligence Integration is the process of incorporating external and internal intelligence (e.g., IOCs, TTPs, threat feeds) into SOC tools to enrich alerts and proactively hunt for threats.

- **Threat Intelligence**: Information about current or potential cyber threats, including malicious IPs, malware hashes, and adversary behaviors.
  Example: Using a threat feed to identify that a specific IP address is associated with ransomware campaigns.
- **Indicators of Compromise (IOCs)**: Data points that signal malicious activity in a system or network.
  Example: A file hash that matches a known malware signature.
- **Tactics, Techniques, and Procedures (TTPs)**: Behavioral patterns and methods used by attackers, often categorized in frameworks like MITRE ATT&CK.
  Example: T1078 – "Valid Accounts," where adversaries use stolen credentials to access systems.
- **Threat Feeds**: External data sources that provide updated intelligence in machine-readable formats for integration with security tools.
  Example: A STIX/TAXII feed that updates a SIEM with the latest malicious IP addresses.

Steps

1. Integrated **AlienVault OTX** threat intelligence feed with **Wazuh** SIEM.
2. Configured Wazuh rules to automatically compare observed IPs/domains with the OTX threat feed.
3. Monitored incoming alerts and checked for enrichment tags (e.g., "C2 Server").
4. Correlated matched IOCs with MITRE ATT&CK techniques for context.

Example

Wazuh generated an alert for outbound communication from host 10.0.0.25 to external IP 91.219.236.23. The OTX feed tagged the IP as a **known C2 server** associated with malware family "AgentTesla." The enriched alert was mapped to MITRE ATT&CK technique **T1071 – Application Layer Protocol**. Based on this intelligence, the incident was escalated to Tier 2 analysts for containment and eradication.

3. **Incident Escalation Workflows**
   Incident Escalation Workflows define how detected incidents are reviewed, triaged, and passed from Tier 1 to higher SOC levels (Tier 2/3) or to management. Escalation ensures that critical incidents receive timely attention and that response actions are properly coordinated.

- **Escalation Tiers**: Structured levels in a SOC that determine how incidents are handled based on severity and complexity.
  Example: A Tier 1 analyst escalates a suspected phishing attack to Tier 2 for deeper investigation.
- **Communication Protocols**: Standardized methods of sharing incident information within the SOC and with external stakeholders.
  Example: Using a SITREP (Situation Report) to brief management during a DDoS attack.
- **Automation in Escalation**: The use of Security Orchestration, Automation, and Response (SOAR) tools to streamline and automate escalation tasks.
  Example: Automatically assigning a critical alert to Tier 2 and enriching it with WHOIS and geolocation data.

Steps

1. A suspicious login attempt alert was triggered in **Elastic Security**.
2. Tier 1 analyst verified the event against baseline user activity.
3. Since the login occurred at 03:15 AM from a foreign IP, the case was escalated in **TheHive**.
4. A **SITREP (Situation Report)** was generated and shared with Tier 2 analysts and SOC management.
5. Automated playbooks in **SOAR** enriched the case with WHOIS and VirusTotal lookups.

Example

In TheHive, Case #2025-INC-014 was created after abnormal login activity was detected on Server-DC01. Tier 1 triage confirmed login attempts from IP 203.0.113.45 (Singapore), which did not align with the user’s normal profile (India). The case was escalated with severity **High**. Automated enrichment revealed the IP had prior associations with credential stuffing attacks. The incident was passed to Tier 2 for containment and password reset procedures.

Conclusion

Understanding **Advanced Log Analysis**, **Threat Intelligence Integration**, and **Incident Escalation Workflows** is essential for SOC analysts. These concepts enable better detection of cyber threats, more effective investigations, and streamlined communication during incidents. By mastering these areas, analysts can significantly enhance the efficiency and accuracy of security operations.