Advanced Log Analysis

Core Concepts

1. **Log Correlation**
    - **Definition**: Log correlation involves analysing logs from multiple sources (e.g., firewalls, endpoints, applications) to identify patterns indicative of an attack.
    - **Example**:
        - Failed login attempts (Event ID 4625 in Windows) followed by unusual outbound traffic could indicate a brute-force attack followed by data exfiltration.
        - Tools like SIEMs (e.g., Splunk, ELK Stack) automate correlation by aggregating logs and applying rules.
2. **Anomaly Detection**
    - **Techniques**:
        - **Statistical Methods**: Baseline normal behavior (e.g., average logins per hour) and flag deviations.
        - **Rule-Based Methods**: Define rules (e.g., "alert if >10 failed logins in 5 minutes").
    - **Example**:
        - A user logging in at 3 AM from a foreign country when they typically work 9-5.
3. **Log Enrichment**
    - **Purpose**: Add context to raw logs to improve analysis.
    - **Methods**:
        - Geolocation for IPs.
        - User role mapping (e.g., admin vs. regular user).
        - Threat intelligence feeds (e.g., tagging known malicious IPs).

Key Objectives

- Reduce false positives by contextualizing alerts.
- Uncover multi-stage attacks by linking disparate log events.

How to Learn

- **Resources**:
    - SANS Reading Room: Search for papers like "Effective Log Analysis."
    - Elastic’s documentation on anomaly detection.
    - Case studies (e.g., CISA’s Equifax breach report).

2. Threat Intelligence Integration

Core Concepts

1. **Threat Intelligence Types**
    - **Indicators of Compromise (IOCs)**: Malicious IPs, file hashes, domains.
    - **Tactics, Techniques, and Procedures (TTPs)**: How attackers operate (e.g., MITRE ATT&CK framework).
    - **Threat Feeds**: STIX/TAXII standards for sharing intelligence.
2. **Integration in SOC**
    - **Process**:
        - Automatically enrich SIEM alerts with threat intelligence (e.g., tagging an IP as "known C2 server").
        - Example: Matching a suspicious IP in logs to a threat feed.
3. **Threat Hunting with Intelligence**
    - **Approach**:
        - Proactively search for TTPs (e.g., T1078 - Valid Accounts misuse).
        - Use tools like MISP or AlienVault OTX to gather intelligence.

Key Objectives

- Enhance detection by leveraging external intelligence.
- Proactively hunt for threats rather than waiting for alerts.

How to Learn

- **Resources**:
    - MITRE ATT&CK: Study TTPs and map them to defenses.
    - OASIS Cyber Threat Intelligence: Learn STIX/TAXII standards.
    - AlienVault OTX: Explore real-world threat feeds.

3. Incident Escalation Workflows

Core Concepts

1. **Escalation Tiers**
    - **Tier 1 (Triage)**: Initial alert assessment (e.g., false positive filtering).
    - **Tier 2 (Investigation)**: Deep dive into confirmed incidents.
    - **Tier 3 (Advanced Analysis)**: Handle complex threats (e.g., APTs).
2. **Communication Protocols**
    - **SITREP (Situation Reports)**: Summarize incident details for stakeholders.
    - **Stakeholder Briefings**: Tailor communication to technical vs. non-technical audiences.
3. **Automation in Escalation**
    - **SOAR Tools**: Automate tasks like ticket assignment, alert enrichment, and response playbooks.
    - Example: Splunk SOAR auto-assigning high-severity alerts to Tier 2.

Key Objectives

- Streamline incident response with clear workflows.
- Ensure timely and effective communication.

- **Resources**:
  - NIST SP 800-61: Incident handling guidelines.
  - SANS Incident Handler's Handbook: Templates for reports.
  - Splunk SOAR documentation: Learn automation use cases.

Summary of Steps to Master These Areas

1. **Log Analysis**:
   - Study correlation techniques and anomaly detection.
   - Practice with SIEM tools and real-world logs.
2. **Threat Intelligence**:
   - Learn MITRE ATT&CK and STIX/TAXII.
   - Integrate feeds into a lab SIEM for hands-on experience.
3. **Incident Escalation**:
   - Map workflows using NIST/SANS frameworks.
   - Simulate escalations in a lab environment with SOAR tools.

Would you like recommendations for hands-on labs or specific tools to practice these concepts?

Master Core Concepts

Log Correlation

- **Practical Exercise**:
  1. Collect sample logs from multiple sources:
     - Firewall (e.g., Suricata logs).
     - Endpoint (Windows Event ID 4625).
     - Application (Apache/Nginx logs).
  2. Use a SIEM (Elastic Security/Splunk) to:
     - Write a query to link **Event ID 4625** (failed logins) with outbound traffic spikes (e.g., **destination_ip != internal_range**).
     - Example output:

bash
index=logs (EventCode=4625) AND destination_ip=8.8.8.8

Anomaly Detection

- **Hands-On Task**:
  - In Elastic Security, create a detection rule for:
    - Unusual login times (e.g., **WHERE hour(timestamp) NOT BETWEEN 8 AND 18**).
    - High-volume transfers (e.g., **bytes_out > 1MB/sec**).
  - Use **Kibana Machine Learning** to baseline normal behavior._

Log Enrichment

- **Tool Implementation**:
  - Add GeoIP to Elastic/Kibana:

bash
 # Configure Logstash GeoIP filter
filter {
  geoip { source => "client_ip" }
}

- Enrich logs with user roles (e.g., map **username** to **department** via CSV lookup).

2. Learning Resources

- **SANS Reading Room**: Study "Effective Log Analysis".
- **Elastic Documentation**: Anomaly Detection Guide.
- **Case Study**: CISA's Equifax Report (Focus on log correlation gaps).

Threat Intelligence Integration

1. Core Practice

Threat Feeds & IOCs

- **Lab Setup**:
  1. Import AlienVault OTX feeds into Wazuh:

```
# OTX API integration in Wazuh
curl -XPOST "http://localhost:9000/otx?api_key=YOUR_KEY"
```

  2. Test with a known malicious IP (e.g., **185.183.96.231**).

Alert Enrichment

- **Example**:
  - In Wazuh/Splunk, auto-tag alerts with OTX data:

```
python
# Pseudocode for alert enrichment
if alert.ip in otx_malicious_ips:
  alert.add_tag("C2 Server")
```

Threat Hunting (MITRE ATT&CK)

- **Procedure**:
  - Hunt for **T1078** (Valid Accounts):

```
sql
SELECT * FROM logs WHERE user.activity = "off-hours" AND user.role = "admin";
```

2. Learning Resources

- **MITRE ATT&CK**: T1078 Technique.
- **STIX/TAXII**: OASIS CTI Docs.
- **AlienVault OTX**: Public Threat Feeds.

Incident Escalation Workflows

1. SOC Tier Workflow

Tier 1 (Triage):

- **Automated Playbook**:
  - Use Splunk SOAR to:
    - Assign **High** severity alerts to Tier 2.
    - Enrich alerts with VulnDB lookup.

Tier 2 (Investigation):

- **Case Study**:
  - Simulate a phishing incident:
    1. Escalate to Tier 2 with:
       - User email, attachment hash, sender IP.
    2. Document in **TheHive**:

markdown

Phishing Case

****IOC**: Email from "support@malicious.tld"**

****Action**: Block sender, scan endpoints.**

Tier 3 (Advanced):

- **Example**:
  - Analyze an APT incident:
    - Use **Velociraptor** to collect memory dumps.
    - Cross-reference with **VirusTotal**.

2. Communication Protocols

- **SITREP Template**:

****Title**: Unauthorized Database Access**

****Timeline**: 2025-09-21 14:00 - 14:30 UTC**

****Impact**: PII data exposure risk**

****Action**: Isolated DB, initiated forensics.**

3. Learning Resources

- **NIST SP 800-61**: Incident Handling Guide.
- **SANS Handbook**: Incident Handler's Templates.
- **Splunk SOAR**: Automation Use Cases._

Final Capstone Project

1. **Simulate an Attack**: Trigger a Metasploit exploit (**multi/samba/usermap_script**).
2. **Detect & Escalate**:
   - Wazuh alerts → TheHive case → SOAR playbook.
3. **Report**:

Executive Summary

****Attack**: Samba usermap exploit (MITRE T1210).**

****Response**: Contained via IP blocking.**

****Recommendation**: Patch Samba (CVE-2025-XXXX).**

Toolkit Checklist

Category	Tools
Log Analysis	Elastic, Splunk, Security Onion
Threat Intel	Wazuh, OTX, MISP
Escalation	TheHive, Splunk SOAR
Forensics	Velociraptor, FTK Imager