SOC Week 3 Notes

Prepared by: Kartheek

Theoretical Knowledge

1. Objectives

This report contains the details of the task includes Advanced Log Analysis, Threat Intelligence Integration, and Incident Escalation flows. The goal of this task is to:

- Develop skills to analyze and correlate logs to uncover complex threats and reduce
  false positives.
- Build Proficiency in leveraging threat intelligence to enhance detection and response.
- Master workflows for escalating incidents and communicating with stakeholders efficiently.

2. Advanced Log Analysis

Advanced Log Analysis means in depth analysis of logs and that includes Log Correlation, Anomaly Detection, and Log Enrichment.

2.1 Log Correlation

Log correlation means linking logs from different sources that includes firewalls, endpoints, and applications to identify attack patterns (e.g., linking failed logins – Event ID 4625 – with suspicious outbound traffic). In simple words analyzing logs from different sources to identify pattern of events. It helps in troubleshooting complex issues, and identifying security threats across the network. In the SANS Reading-Room the techniques used for correlating logs includes OLAP (Online Analytical Processing performed on the datasets.

2.2 Anomaly Detection

Anomaly detection is a process of identifying unusual patterns. It is a critical approach of finding errors, and potential threats such as network intrusion, malicious files or malwares across networks. Learning techniques to detect anomalies (e.g., unusual login times, high-volume data transfers) using statistical or rule-based methods. With the Equifax case-study analysis I detected one major anomaly is that there is no patch update done by IT department created a massive attack with phishing, and Identity theft.

2.3 Log Enrichment

Adding context to logs (e.g., geolocation for IPs, user roles) to enhance analysis. The process of adding additional information to raw log data to make it more meaningful for analysis, security, and for troubleshooting.

3. Threat Intelligence Integration

It is a process of improving organizations security and to automate defense process. Threat intelligence integration includes the core concepts they are Threat Intelligence types, Integration in SOC, and Threat Hunting with Intelligence.

3.1 Threat Intelligence Types

Understanding indicators of compromise (IOCs) (e.g., malicious IPs, hashes).

Tactics: The action or strategy used by threat actor to achieve a specific end.

Techniques: Methods used by the threat actor to achieve tactics.

Procedures: The step-by-step implementation of techniques to achieve the specific end.

Threat feeds: Continuous stream of data about threats to protect the organizations data. STIX/TAXII are used for data sharing as a cyber threat information.

3.1 Integration in SOC

Integration in SOC improves security, threat detection, and faster response times. This is achieved by integrating Threat Intelligence feeds into security tools like SIEMs, using automation to streamline workflow. Learning integration of threat intelligence into SIEMs for automated alert enrichment.

Example: Matching a suspicious IP toa known C2 server.

3.2 Threat Hunting with Intelligence

Using intelligence as a proactive approach for searching threats (e.g., hunting for T1078 – Valid account misuse). Threat intelligence used as guide and prioritize proactive threat hunting within a network.

4. Incident Escalation Workflows

Incident escalation workflows meant a systemized automated process for handling critical issues, and threats by automatically routing them to the correct authority or team with required context.

4.1 Escalation Tiers

Understanding SOC tier structure (Tier 1: Triage, Tier2: Investigation, Tier3: Advanced Analysis) and escalation criteria (e.g., severity, complexity). Escalation is very important because a threat should be handover to a right authority to mitigate and defend the threat to the organization.

4.2 Communication Protocols

Communication protocols defined as a set of rules that need to be followed for the escalation. Learning structured communication for escalation (e.g., SITREP situation Reports) and stakeholder briefings. The report to be understand by non-technical users.

4.3 Automation in Escalation

To automate the escalation process SOAR tools used (e.g., ticket assignment, alert enrichment). Automation of escalation done by using pre-determined rules to move a problem automatically to the higher authority without manual intervention.

Practical Application

1. Advanced Log Analysis

Tools – Elastic Security, Security Onion, Google Sheets.

1.1 Log Correlation

Ingesting sample logs (e.g., from Boss of the SOC dataset) into Elastic Security. Correlating failed logins (Event ID 4625) without outbound traffic.

Documenting the metadata like timestamp, event ID, Source IP, Destination IP, and Notes.

1.2 Anomaly Detection

Creating an elastic rule to detect high-volume data transfers (e.g., bytes_out > 1MB in 1 minute). Testing it with a mock file transfer.

1.3 Log Enrichment

Using a GeoIP plugin in Elastic to add geolocation to an IP address. Later that summarizing the findings when performing log enrichment.

2. Threat Intelligence Integration

Tools – Wazuh, Alienvault OTX, and TheHive.

2.1 Threat Feed Import

Importing AlienVault OTX feed into Wazuh to match Indicators of Compromise (IOCs) (e.g., malicious IPs, file hashes). Testing with a mock IP (e.g., 192.168.1.100).

2.2 Alert Enrichment

Enriching a Wazuh alert with OTX data (e.g., IP reputation). Documenting its metadata like Alert ID, IP, Reputation, and Notes.

2.3 Threat Hunting

Threat hunting means finding the threats. For example, hunt for T1078 (Valid Accounts) in Wazuh logs using a query (e.g., user.name !=”system”). Finally summarizing the findings for threat hunting.

3. Incident Escalation Practice

Tools – TheHive, and Google Docs.

3.1 Escalation Simulation

Creating a TheHive case for High-priority alert (e.g., unauthorized access). Escalate it to Tier2 team with a brief summary and that should be in a proper and easy context so everyone can easily understand.

3.2 SITREP Draft

SITREP stands for Situation Report and it should be written in Google Docs for a mock incident and that report contains the metadata like Title, Summary, and Actions. These are very important in the report.

3.3 Workflow Automation

Creating a simple Splunk Phantom playbook for auto-assigning of High-prioirty alerts to Tier2 team. Testing it with a mock alert.

4. Alert Triage with Threat

Tools – Wazuh, VirusTotal, and AlienVault OTX.

4.1 Triage Simulation

Analyzing a mock alert (e.g., “Suspicious PowerShell Execution”) in Wazuh. Documenting the findings that contains metadata like Alert ID, Description, Source IP, Priority, and Status.

4.2 IOC Validation

IOC stands for Indicators of Compromise cross-reference the alert’s IP or hash with Threat Intelligence tools like VirusTotal, and Alienvault OTX. Summarizing the findings.

5. Evidence Preservation and Analysis

Evidence preservation is very important for the future references and also its analysis helps to find in depth details. Evidence should be submitted in the court for the legal proceedings that should not be changed by the threat actor for this reason only the evidence preserved.

Tools – Velociraptor, and FTK Imager.

5.1 Volatile Data Collection

Using Velociraptor tool for collecting network connections (SELECT * FROM netstat) from a Windows VM. Then saving it to a CSV file.

5.2 Evidence Collection

Collecting a memory dump (SELECT * FROM Artifact.Windows.Memory.Acquisition) and hashing it using SHA256sum. Finally documenting it with some metadata it includes Item, Description, Collected By, Date, and Hash value.

6. Capstone Project

Capstone project a full SOC workflow simulation that it includes simulation of attack, detection of attack, triage, respond, escalate, and report.

Tools – Metasploit, Wazuh, Crowdsec, TheHive, and Google Docs.

6.1 Attack Simulation

Performing attack with msfconsole on Metasploitable2. Exploiting a Metasploitable2 vulnerability with Metasploit (e.g., Samba usermap script: use exploit/multi/samba/usermap_script).

6.2 Detection and Triage

Configuring Wazuh to alert on the attack and documenting it with the metadata like Timestamp, Source IP, Alert, Description, and MITRE Technique.

6.3 Response and Containment

Performing an isolation on the Virtual Machine and blocking the IP address of attacker with CrowdSec tool. Verifying with a ping test.

6.4 Escalation

Escalating it to a Tier 2 team via TheHive with a brief description of case summary.

6.5 Reporting

Writing a detailed report using SANS template, including Executive Summary this includes the title, who is handling, and where it is detected. Timeline a series of event occurred and the recommendations.

6.6 Briefing

Writing a report is not only understand to the technical users but also for the non-technical manager, summarizing the incident like how it is happened, where it is happened, and its impact, and actions.