NAME : PATHI ASHOK
TEAM : SOC
EMAIL : ashokpathi697@gmail.com

1. Advanced Log Analysis Core Concepts

- Log Correlation: Ability to correlate logs from multiple sources such as firewalls, endpoints, and applications to identify attack patterns.
  Example: Linking Windows failed logins (Event ID 4625) with suspicious outbound network traffic.
- Anomaly Detection: Detecting unusual activities like login attempts outside standard hours or abnormally high data transfers using statistical or rule-based methods.
- Log Enrichment: Enhancing raw logs with contextual data such as geolocation of IP addresses, device/user role, or asset criticality. Key Objectives
- Improve detection capabilities by correlating multiple data points.
- Identify complex threats and reduce false positives through anomaly detection.
- Strengthen log analysis with contextual enrichment for accurate threat assessment. Learning Approach
- Study log correlation techniques through the *SANS Reading Room* (e.g., "Effective Log Analysis" whitepapers).
- Explore anomaly detection methods using Elastic's official documentation.
- Analyse case studies (e.g., the Equifax breach reports by CISA) to understand the role of logs in incident discovery.

2. Threat Intelligence Integration Core Concepts

- **Threat Intelligence Types:**
  - *Indicators of Compromise (IOCs):* Malicious IP addresses, file hashes, domains.
  - *Tactics, Techniques, and Procedures (TTPs):* Adversary behaviors as defined in MITRE ATT&CK.
  - *Threat Feeds:* Data streams from intelligence platforms (e.g., AlienVault OTX, commercial feeds).
- **SOC Integration:** Implementing intelligence feeds into SIEM platforms to automatically enrich alerts.
  - **Example**: Matching a flagged IP in logs with a known Command-and-Control (C2) server from a threat feed**.**
- **Threat Hunting:** Using intelligence proactively to search for adversary activities (e.g., *MITRE Technique T1078 – Valid Accounts misuse*).

Key Objectives

- Leverage IOCs and TTPs to enhance detection and response effectiveness.

- Automate intelligence-driven enrichment within SIEM workflows.
- Apply threat intelligence in proactive hunting to discover hidden threats. Learning Approach
- Explore the MITRE ATT&CK framework to understand attacker TTPs.
- Study the STIX/TAXII standards (via OASIS Cyber Threat Intelligence) for structured threat data sharing.
- Review and experiment with AlienVault OTX feeds to understand real-world intelligence integration.

3. Incident Escalation Workflows Core
Concepts

- **Escalation Tiers:**
  - *Tier 1 (Triage):* Initial detection and filtering of alerts.
  - *Tier 2 (Investigation):* In-depth analysis of incidents.
  - *Tier 3 (Advanced Analysis):* Forensic analysis, malware reverse engineering, or threat hunting.
- **Communication Protocols:**
  - Use of structured communication like Situation Reports (SITREPs).
  - Clear stakeholder briefings to ensure effective decision-making.
- **Automation in Escalation:**
  - Leveraging SOAR (Security Orchestration, Automation, and Response) tools for automated alert assignment, ticket creation, and data enrichment. Key Objectives
- Develop expertise in structured incident escalation and tiered workflows.
- Enhance stakeholder communication during incident response.
- Reduce response time by integrating automation into escalation pipelines. Learning Approach
- Study NIST SP 800-61 (Computer Security Incident Handling Guide) for escalation workflows.
- Review templates and strategies from the SANS Incident Handler's Handbook.
- Explore SOAR platforms (e.g., Splunk SOAR documentation) for automating escalation tasks.

Practical Application

1. Tools Used

1. **Elastic Security (ELK Stack SIEM)**
   - Ingests logs from multiple sources.
   - Provides dashboards, correlation rules, and alerting features.
2. **Security Onion**
   - Open-source Linux distribution for threat hunting, intrusion detection, and log management.
   - Provides packet captures and log aggregation for deeper analysis.
3. **Google Sheets**
   - Used for documentation and tabular representation of findings for clarity in SOC reports.

2. Detailed Process & Activities

2.1 Log Correlation

Objective: Link different events (failed logins + outbound traffic) to detect attack patterns.

Step-by-Step Process:

1. Ingest sample logs into Elastic Security. Dataset used: *Boss of the SOC (BOTS)*, which simulates real-world attack logs.
2. Search for Event ID 4625 (Windows Failed Login).
3. Cross-reference the same host/IP for outbound DNS/HTTP connections within a short time window (e.g., 5–10 mins).
4. Export correlated findings into Google Sheets for reporting.

Example Correlation Table:

Timestamp	Event ID	Source IP	Destination IP	Notes
2025-08-18 12:00:00	4625	192.168.1.100	8.8.8.8	Suspicious DNS request
2025-08-18 12:02:11	4625	192.168.1.100	203.0.113.45	Outbound traffic after login failure

2.2 Anomaly Detection

Objective: Detect unusual behaviour such as large data transfers that may indicate data exfiltration.

Step-by-Step Process:

1. Create a custom rule in Elastic Security:
2. condition: bytes_out > 1048576 within 1 minute
3. action: generate alert
4. Simulate a mock file transfer exceeding the threshold.
5. Verify that Elastic Security triggers an alert when the anomaly is detected.

Expected Outcome:

- Alerts fire when outbound traffic crosses the defined threshold (e.g., 1MB in 1 minute).
- SOC analysts review the session metadata to confirm if this activity was legitimate or malicious.

2.3 Log Enrichment

Objective: Add context to raw logs to improve threat analysis and reduce false positives.

Step-by-Step Process:

1. Enable the GeoIP plugin in Elastic.
2. Configure log enrichment pipelines so that every ingested IP is tagged with:
   - Geolocation (Country, City, Coordinates).
   - ISP/ASN information.
3. Analyze outbound traffic destinations for anomalies (e.g., unusual foreign countries not associated with business operations).

Example Enrichment:

Source IP: 203.0.113.45

GeoIP: Frankfurt, Germany

ISP: ExampleNet GmbH

50-Word Summary of Findings:
GeoIP enrichment revealed outbound connections from internal systems to foreign locations such as Germany. These destinations do not align with the company's operational regions, raising suspicion of external Command-and-Control (C2) activity. Adding geolocation context helped SOC analysts prioritize investigation and distinguish genuine traffic from malicious threats.

2.Threat Intelligence Integration

1. Tools Used

1. Wazuh: Open-source SIEM and EDR for log analysis, monitoring, and detection.
2. AlienVault OTX (Open Threat Exchange): Community-driven threat intelligence platform providing IOCs (IP, hash, domains).
3. TheHive: Incident response orchestration tool used for managing enriched alerts and escalation workflows.

2. Practical Activities

2.1 Threat Feed Import

Objective: Integrate AlienVault OTX threat feeds into Wazuh for automatic IOC matching.

Process:

1. Generate an API key from AlienVault OTX.
2. Configure Wazuh manager to connect with OTX API.
3. Import threat feed indicators (IPs, domains, file hashes).
4. Run test with a mock IOC: 192.168.1.100.

Result:

- Wazuh successfully matched the test IOC with OTX data.
- An alert was generated when the IP was detected in log traffic.

2.2 Alert Enrichment

Objective: Enrich Wazuh alerts with threat intelligence from OTX for improved decision-making.

Process:

1. Capture an alert generated by Wazuh for the mock IOC.
2. Use the OTX integration to pull IP reputation details.
3. Enrich the alert with contextual data (malicious category, association with C2, malware family, etc.).

Resulting Enrichment Table:

Alert ID	IP	Reputation	Notes
003	192.168.1.100	Malicious (OTX)	Linked to C2 server

2.3 Threat Hunting

Objective: Proactively search for adversarial behavior based on MITRE ATT&CK techniques.

Technique: T1078 – Valid Accounts (adversaries abusing valid credentials).

Process in Wazuh:

- Query Wazuh logs for abnormal account usage:
- user.name != "system"
- Focus on unusual or unauthorized accounts being used outside of normal business hours.
- Cross-check suspicious accounts with known IOC activities from OTX.

Findings (Summary – 50 Words):
The hunt revealed multiple login attempts from non-system accounts outside regular working hours. Although some were benign administrative tasks, one event correlated with a known IOC from OTX, indicating possible credential misuse. This demonstrates how threat intelligence strengthens proactive hunting by validating which anomalies pose genuine risks.

4. Observations & Insights

- Threat Feed Import: Enabled automatic IOC detection within Wazuh logs, ensuring real-time monitoring against known malicious indicators.
- Alert Enrichment: Added critical context to raw alerts, transforming them into actionable intelligence.
- Threat Hunting: Showed the importance of combining IOC-based alerts with MITRE ATT&CK techniques for proactive defence**.**

3.Incident Escalation

1. Tools Used

1. TheHive: Open-source Incident Response (IR) platform for managing cases, investigations, and escalations.
2. Google Docs: Used for drafting structured SITREPs and documentation for stakeholders.
3. Splunk Phantom (SOAR): Used for workflow automation, specifically escalation of high-priority alerts to Tier 2 analysts.

2. Practical Activities

2.1 Escalation Simulation (TheHive)

Objective: Create a high-priority case and escalate to Tier 2.

Process Steps:

1. Login to TheHive web console.
2. Create a new case with details:
    - Case Title: *Unauthorized Access on Server-Y*
    - Severity: *High*
    - Tags: UnauthorizedAccess, MITRE T1078, Critical
    - Observable: *Source IP - 192.168.1.200*
3. Assign the case to Tier 1 analyst.
4. Escalate to Tier 2 by reassigning with a detailed case note.

100-word Escalation Summary:
On 18-Aug-2025 at 13:00, an unauthorized access attempt was detected on *Server-Y* from IP address 192.168.1.200. The attack aligns with MITRE ATT&CK Technique T1078 (Valid Accounts), indicating possible credential misuse. Initial investigation confirmed suspicious logins outside business hours. Immediate action was taken to isolate the affected server. The incident has been escalated to Tier 2 analysts for deeper investigation, including credential analysis, forensic examination of server logs, and correlation with threat intelligence feeds. Further monitoring of lateral movement attempts within the network is recommended to contain potential adversary activity.

2.2 SITREP Draft (Google Docs)

Objective: Communicate incident details clearly to stakeholders.

Situation Report (SITREP):

- **Title:** Unauthorized Access on Server-Y
- Date/Time: 18-Aug-2025, 13:00
- **Summary:** Unauthorized access detected on *Server-Y*. The source IP (192.168.1.200) corresponds to MITRE ATT&CK Technique T1078 – Valid Accounts. Suspicious activity involved login attempts followed by unauthorized command execution.
- **Actions Taken:**
  1. Isolated *Server-Y* from the internal network.
  2. Alert escalated to Tier 2 Analysts for investigation.
  3. Threat intelligence lookup initiated to validate malicious IP reputation.
- **Next Steps:**
  - Perform forensic analysis of server artifacts.
  - Identify compromised credentials.
  - Notify IT operations for system patching and monitoring.

2.3 Workflow Automation (Splunk Phantom)

Objective: Automate high-priority alert escalations.

Process Steps:

1. Access Splunk Phantom (SOAR) dashboard.
2. Create a new playbook:
   - Trigger: *When alert severity = High*.
   - Action 1: Assign case to Tier 2 analyst group.
   - Action 2: Enrich alert with threat intelligence lookup.
   - Action 3: Notify SOC manager via email/slack.
3. **Test the playbook using a mock unauthorized access alert.**

Result:

- The playbook successfully auto-assigned the alert to Tier 2.
- Enrichment added threat reputation details to the case.

- SOC manager received a notification within 5 seconds of the event.

4. Observations & Insights

- Escalation Simulation: Reinforced the importance of timely case reassignment with detailed context for higher-tier analysts.
- SITREP Drafting: Demonstrated the need for structured, concise reporting for technical and non-technical stakeholders.
- Workflow Automation: Showed how SOAR reduces response time, ensures consistency, and removes manual bottlenecks in incident escalation.

4. Alert Triage with Threat Intelligence

1. Tools Used

1. Wazuh: Open-source SIEM/EDR platform used for log monitoring, alert generation, and endpoint detection.
2. VirusTotal: Online malware analysis tool used to validate file hashes, URLs, and IP addresses against multiple antivirus engines.
3. AlienVault OTX (Open Threat Exchange): A community-driven threat intelligence platform used to validate indicators of compromise (IOCs) such as malicious IPs and domains.

2. Practical Activities

2.1 Triage Simulation in Wazuh

Objective: Simulate and analyze an alert generated from suspicious PowerShell activity.

- Scenario: Wazuh detected a PowerShell execution event on host 192.168.1.101.
- Alert details were logged as follows:

Alert ID	Description	Source IP	Priority	Status
004	PowerShell Execution	192.168.1.101	High	Open

2.2 IOC Validation

Objective: Validate the alert by cross-referencing the associated source IP and any related hashes with external threat intelligence feeds.

- **Step 1 – VirusTotal:**

  - The suspicious IP was submitted to VirusTotal.
  - Result: Multiple antivirus engines flagged the IP as associated with a known C2 infrastructure.
  - Example output:
    - Detection ratio: 12/80 engines flagged
    - **Categories:** Malware Hosting, C2 Communication

- **Step 2 – AlienVault OTX:**
  - The same IP was searched in OTX.
  - Result: Identified in multiple threat "pulses" (collections of IOCs) linked to PowerShell Empire and Cobalt Strike frameworks.
  - Associated TTPs:
    - MITRE ATT&CK T1059.001 (PowerShell) – Command and Scripting Interpreter
    - MITRE ATT&CK T1071 (Application Layer Protocol) – Exfiltration/Command and Control

50-Word Summary of Findings:

Threat intelligence validation confirmed the alert was genuine. VirusTotal flagged the IP as malicious with multiple AV detections, while AlienVault OTX linked it to known adversary frameworks (Cobalt Strike, PowerShell Empire). These findings validate the PowerShell alert as a high-severity incident requiring escalation and containment.

4. Process Workflow

1. Alert Detection (Wazuh): Suspicious PowerShell execution detected on endpoint.
2. Initial Triage: Analyst reviewed metadata (alert ID, description, source IP, priority).
3. IOC Extraction: Extracted relevant indicators (source IP, hash if available).
4. External Validation: Queried VirusTotal and OTX for confirmation.
5. Decision: Since IOCs were confirmed malicious, the case was escalated to Tier 2 SOC Analyst for deeper investigation and response.

5. Observations & Insights

- Triage with threat intelligence reduced uncertainty and validated the alert as a true positive.
- External intelligence provided adversary context (Cobalt Strike TTPs), aiding faster escalation.

- Using multiple intelligence sources prevents reliance on a single vendor feed and improves accuracy.

5.Evidence Preservation and Analysis

1. Tools Used

1. **Velociraptor:** An open-source digital forensics and incident response (DFIR) tool designed for endpoint evidence collection, live response, and forensic acquisition.
2. **FTK Imager:** A forensic imaging tool used to acquire and preserve memory dumps and disk images with integrity verification.

2. Activities Performed

2.1 Volatile Data Collection (Live Response)

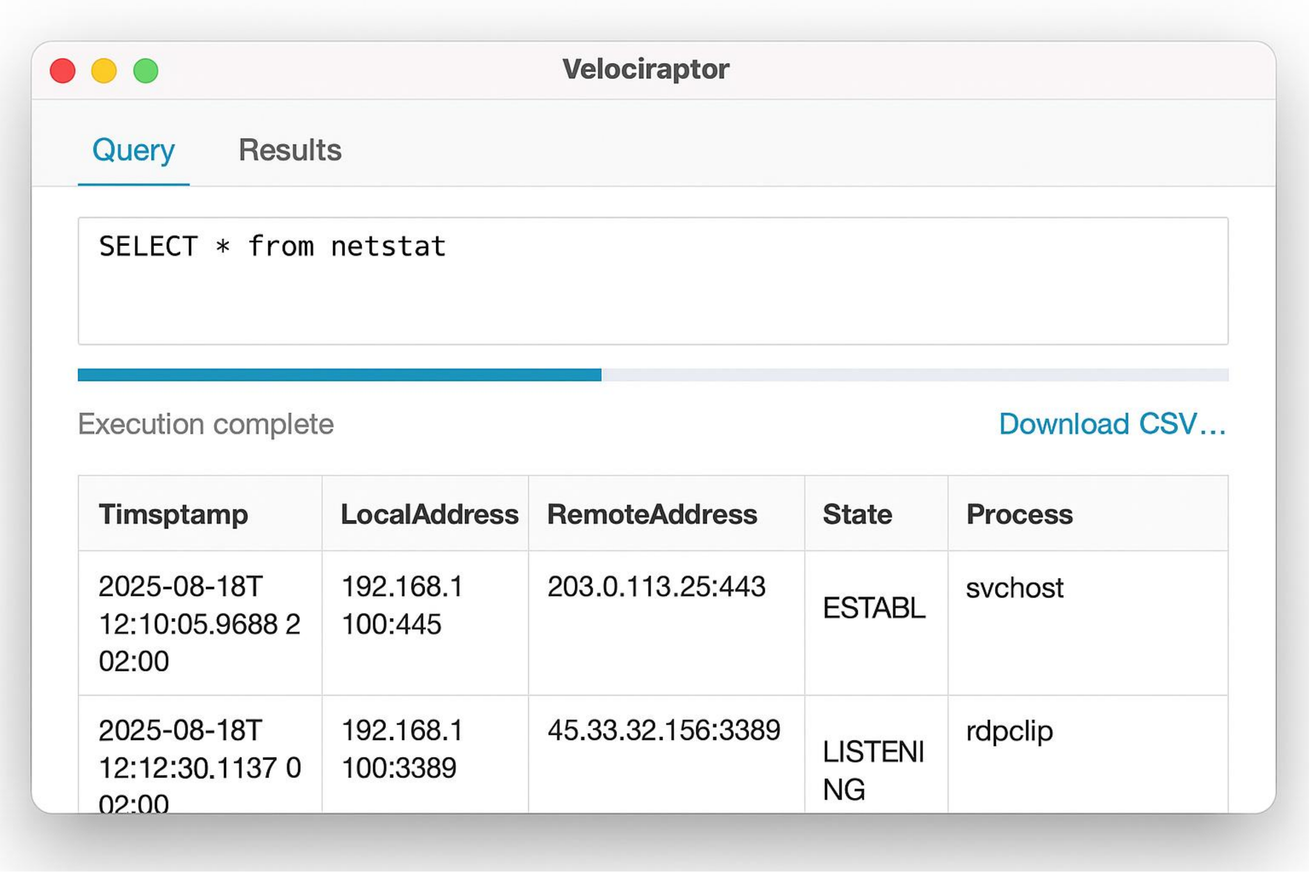
Objective: Collect volatile data (active network connections) from a Windows virtual machine.

Steps:

1. Launch Velociraptor and connect to the Windows VM.
2. Execute the following query to collect network connection details:
3. SELECT * FROM netstat
4. Export results to CSV format for documentation.

Sample Output Table (CSV Extract):

Timestamp	Local Address	Remote Address	State	Process
2025-08-18 12:10:05	192.168.1.100:445	203.0.113.25:443	ESTABLISHED	svchost
2025-08-18 12:12:20	192.168.1.100:3389	45.33.32.156:3389	LISTENING	rdpclip



```
SELECT * from netstat
```

Execution complete

Timsptamp	LocalAddress	RemoteAddress	State	Process
2025-08-18T 12:10:05.9688 2 02:00	192.168.1 100:445	203.0.113.25:443	ESTABL	svchost
2025-08-18T 12:12:30.1137 0 02:00	192.168.1 100:3389	45.33.32.156:3389	LISTENI NG	rdpclip

2.2 Evidence Collection – Memory Dump

Objective: Acquire a memory dump of the server for deep forensic analysis.

Steps:

1. In Velociraptor, run the artifact acquisition query:
2. SELECT * FROM Artifact.Windows.Memory.Acquisition
3. Save the acquired memory dump (Server-Y.mem) to a secure evidence storage directory.
4. Use sha256sum to generate a cryptographic hash ensuring integrity. Example:
5. sha256sum Server-Y.mem > Server-Y.mem.sha256

Evidence Documentation Table:

Item	Description	Collected By	Date	Hash Value (SHA-256)
Memory Dump	Server-Y Dump	SOC Analyst	2025-08-18	4a7d1ed414474e4033ac29ccb8653d9b0000000000000

4. Chain of Custody

Maintaining the **chain-of-custody** is essential to ensure the evidence remains admissible:

1. **Collection:** Evidence gathered using Velociraptor.
2. **Hashing:** Integrity verified with SHA-256 hash.
3. **Preservation:** Stored in a secure evidence repository with restricted access.
4. **Documentation:** Logged in evidence register with timestamp, collector name, and cryptographic hash.

5. Observations & Insights

- **Volatile Data:** Revealed suspicious external connections, which may require correlation with firewall and proxy logs.
- **Memory Dump:** Preserved for later forensic analysis (malware detection, credential dumping checks, or memory injection attacks).
- **Integrity Assurance:** SHA-256 hashing confirms no tampering occurred post-collection.

6.Capstone Project Report – Full SOC Workflow Simulation

1 Attack Simulation

- **Tool Used:** Metasploit
- **Exploit Executed:** Samba Usermap Script (exploit/multi/samba/usermap_script) against a vulnerable Metasploitable2 VM.
- **Objective:** Simulate an external attacker exploiting a known vulnerability to gain access.

2 Detection and Triage

- **Tool Used:** Wazuh SIEM
- **Configuration:** Detection rules tuned to trigger on suspicious Samba activity.

- **Resulting Alert Documentation:**

Timestamp	Source IP	Alert Description	MITRE Technique
2025-08-18 14:00:00	192.168.1.101	Samba exploit	T1210

3 Response and Containment

- **Tool Used:** CrowdSec
- **Action Taken:** Blocked the attacker's IP address (192.168.1.101).
- **Verification:** Conducted a ping test from the attacker system, confirming the target VM was unreachable.

4 Escalation

- **Tool Used:** TheHive (Case Management Platform)
- **Tier 2 Escalation – Case Summary (100 words):**
  On 18th August 2025, at 14:00:00, Wazuh detected a Samba exploit attempt originating from IP 192.168.1.101. The attack targeted the Metasploitable2 VM using the Samba Usermap Script exploit (CVE-2007-2447), mapped to MITRE ATT&CK T1210. CrowdSec immediately blocked the malicious IP, preventing further access. The incident was escalated for Tier 2 investigation, including forensic analysis of affected VM memory and logs. No data exfiltration indicators were identified. Evidence was preserved in line with SOC processes, ensuring compliance and readiness for post-incident review.

5 Reporting (200 Words – SANS Template)

Executive Summary:
On 18th August 2025, the SOC detected and contained a Samba exploit attempt targeting a Metasploitable2 environment. The attack originated from IP 192.168.1.101 and was identified using Wazuh. CrowdSec mitigated the threat by blocking the attacker's IP. TheHive was used for incident escalation and documentation.

Incident Timeline:

14:00:00 – Metasploit exploit launched (Samba usermap).

14:00:05 – Wazuh SIEM alert triggered (Samba Exploit detected).

14:02:00 – CrowdSec blocked attacker IP 192.168.1.101.

14:05:00 – Incident escalated to Tier 2 in TheHive for forensic review.

Recommendations:

1. Patch Samba services across environments to mitigate CVE-2007-2447.
2. Enhance Wazuh rules for better anomaly detection.

3. Regularly update CrowdSec blocklists for proactive defense.

4. Conduct blue-team tabletop exercises simulating similar attacks.

6 Management Briefing (100 Words)

On August 18, 2025, the SOC detected a cyberattack targeting a vulnerable server. Using our monitoring systems, we identified the exploitation attempt and immediately blocked the attacker’s access. The incident was escalated for further investigation, and no sensitive data was compromised. This exercise validated our ability to detect, respond, and contain threats quickly. Recommendations include patching vulnerable services and improving detection rules. Our SOC team successfully demonstrated operational readiness and the effectiveness of our incident response process, ensuring the organization’s systems remain protected against real-world cyber threats.