Security Information and Event Management (SIEM) and SOC Analyst Report

By Abdelrahman Wael Ibrahim

1. What is SIEM and Why is it Important?

Security Information and Event Management (SIEM) systems provide centralized collection, correlation, and analysis of log data from various devices—such as firewalls, servers, and endpoint protection tools—to detect and respond to threats in real time.

For example, if a user logs in from *Egypt at 9:00 AM* and from *Germany at 9:05 AM*, the SIEM system will flag this as an **impossible travel event** and trigger an alert.

Key Benefits:

- **Visibility:** Centralized view of all network and system activities.
- **Threat Detection:** Detects patterns of malicious behavior through event correlation.
- **Incident Response:** Enables faster investigation and containment.
- **Compliance:** Generates reports for frameworks like GDPR, ISO 27001, and PCI-DSS.

Source	Log Event	SIEM Action
Firewall	Blocked IP 192.168.10.5	Alert triggered
Windows Server	Login failure (3 times)	Correlated event
SIEM Dashboard	Multiple failures + foreign IP	Escalated to Tier 1 Analyst

2. Responsibilities of a SOC Tier 1 Analyst

A **SOC Tier 1 Analyst** acts as the organization's first line of cyber defense. They continuously monitor security alerts, identify suspicious activity, and escalate confirmed incidents for deeper investigation.

Main Responsibilities:

- Monitor SIEM alerts and dashboards 24/7.
- Perform **initial triage**—distinguish false positives from real threats.

- Investigate logs for context (user, IP, location, and time).
- Escalate confirmed incidents to Tier 2 analysts.
- Maintain accurate incident documentation and communication.

Illustrative Workflow:

```
SIEM Alert → Tier 1 Review → False Positive?
       ↓                    ↑
   Escalate to Tier 2     Close Alert
```

3. Main Challenges SOC Tier 1 Analysts Face Daily

- **Alert Fatigue:** Handling hundreds of daily alerts, many of which are false positives.
- **Time Pressure:** Quick decision-making to prevent data loss.
- **Complex Attack Surfaces:** Managing cloud, IoT, and hybrid networks.
- **Limited Context:** Incomplete log data during investigations.
- **Continuous Learning:** Adapting to new attack techniques daily.

Example: A PowerShell command execution alert appears on a user workstation. Without full endpoint visibility, the Tier 1 analyst must decide whether it's legitimate or part of a malware infection—leading to escalation.

4. Scenario: Responding to a Suspicious Login Alert

Situation: At 2:45 AM, the SIEM flags a login attempt for user `jane_admin` from a foreign IP address in Russia. The user normally logs in from Cairo, Egypt during working hours.

Response Steps:

1. **Validate the Alert:** Review details such as IP address, timestamp, and device.
2. **Gather Context:** Check login history and IP reputation databases (e.g., VirusTotal).
3. **Correlate Logs:** Analyze VPN and firewall data for repeated failed attempts.
4. **Containment:** Disable the suspicious account and isolate affected devices.

5. **Escalation:** Document findings and escalate to Tier 2 with full evidence.

6. **Post-Response Monitoring:** Continue watching for similar login patterns.

Step	Action	Tool Used	Purpose
1	Validate alert	SIEM	Confirm accuracy
2	Check IP	Threat Intelligence	Assess risk level
3	Correlate logs	Firewall, VPN	Find related events
4	Contain threat	AD, IAM Tools	Stop potential compromise
5	Escalate	Ticketing System	Handoff to Tier 2
6	Monitor	SIEM Dashboard	Detect recurrence

5. SOC Tier Hierarchy: Tier 1, Tier 2, Tier 3

A **Security Operations Center (SOC)** is divided into three levels or "tiers" based on expertise and responsibilities.

Tier 1 – Alert Monitoring and Triage

Role: First responder; monitors SIEM alerts and filters false positives. **Tools:** SIEM (Splunk, QRadar), Threat Intel (AbuseIPDB). **Goal:** Detect and escalate real incidents quickly.

Tier 2 – Investigation and Containment

Role: Performs deeper analysis, determines incident scope, and takes containment actions. **Tools:** EDR/XDR (CrowdStrike, SentinelOne), SOAR, network logs. **Goal:** Confirm and mitigate verified incidents.

Tier 3 – Forensics and Threat Hunting

Role: Handles advanced incidents, conducts digital forensics, and creates new detection rules. **Tools:** Wireshark, Volatility, Ghidra, MITRE ATT&CK. **Goal:** Identify root causes and strengthen detection systems.

Tier	Focus	Tools	Skill Level	Example Task
1	Monitoring & Triage	SIEM, Threat Intel	Beginner–Intermediate	Validate suspicious login
2	Investigation & Containment	EDR, Firewalls, SOAR	Intermediate–Advanced	Contain compromised host
3	Forensics & Threat Hunting	Wireshark, Ghidra, Volatility	Expert	Analyze malware & create rule

Conclusion

SIEM solutions form the backbone of modern cybersecurity operations by enabling real-time threat visibility and rapid response. SOC analysts across all tiers work collaboratively—Tier 1 detects, Tier 2 investigates, and Tier 3 hunts—to safeguard the organization from cyber threats efficiently and proactively.