multinet
INFOSTRUCTURE FOR THE NATION

SOC ANALYST STUDY NOTES

Prepared by: Rohan Khan

multinet
INFOSTRUCTURE FOR THE NATION

CHAPTER 1
SOC Analyst Essentials

Key Concepts in Security Operations Center (SOC) Analysis

Definitions

- SIM (Security Information Management)

Definition: SIM is a system that focuses on the long-term storage, analysis, and reporting of security data. It enables organizations to retain historical security information and use it for compliance reporting, forensics, and in-depth analysis of past incidents.

- SEM (Security Event Management)

Definition: SEM is designed for the real-time monitoring, correlation, and notification of security events. It provides immediate insights into ongoing security incidents, allowing for faster detection and response to potential threats.

- SIEM (Security Information and Event Management)

Definition: SIEM combines the capabilities of SIM and SEM into a single solution that offers both historical data analysis and real-time monitoring. It centralizes the collection and management of security data across the organization, allowing for comprehensive threat detection, compliance management, and incident response.

CHAPTER 2

Functions of SIEM

SIEM systems provide a wide range of essential functionalities:

- Log Collection: Gather logs from various sources
- Log Aggregation: Combine logs for easier analysis
- Rule-based Alerts: Trigger alerts based on predefined rules
- Artificial Intelligence: Use AI to enhance detection capabilities
- Response: Enable timely response to incidents
- Parsing: Process logs into structured formats
- Normalization: Standardize log data across sources
- Categorization: Classify logs by type and severity
- Enrichment: Add context to logs for deeper insights
- Indexing: Organize data for efficient searching
- Storage: Safely retain log data for compliance and analysis

CHAPTER 3

Roles and Responsibilities of SOC Analysts

Definition:

SOC stands for Security Operations Center, a centralized unit dedicated to monitoring, detecting, and responding to cybersecurity threats

Functions of a SOC:

- Threat Monitoring: Continuous observation of security events and network activity.
- Alert Investigation: Analysis of alerts to assess their impact and urgency.
- Incident Response: Coordinating actions to mitigate and remediate identified security incidents.

Technologies Utilized in SOC:

- SIEM (Security Information and Event Management): Collects and analyzes security data from across the organization.
- EDR (Endpoint Detection and Response): Provides real-time endpoint monitoring and threat detection.
- TIP (Threat Intelligence Platform): Aggregates and analyzes threat intelligence data to improve defenses.
- SOAR (Security Orchestration, Automation, and Response): Streamlines incident management through automated workflows.
- Ticketing Systems (e.g., Service Now, Jira): Tracks and manages security incidents and tasks.
- MDR (Managed Detection and Response): Outsourced service providing advanced threat detection and remediation

multinet
INFOSTRUCTURE FOR THE NATION

Tasks of an L1 SOC Analyst:

1. Alert Triage: Prioritize and categorize alerts based on severity and relevance.
2. First Line of Defense: Act as the initial point of contact for threat detection and mitigation.
3. Identifying Anomalies: Detect unusual patterns or suspicious activities within systems.
4. Whitelist Management: Raise requests to whitelist legitimate applications or IP addresses.
5. Preliminary Investigations: Conduct initial analysis to validate threats before escalation

Tasks of an L2 SOC Analyst

1. Monitoring Alerts: Continuously observe security alerts and notifications for potential threats.
2. Threat Hunting: Actively search for indicators of compromise within the network to identify threats that bypass traditional security measures.
3. Resource Mentoring: Provide guidance and support to junior analysts, helping them develop their skills.
4. Whitelist Management: Create and approve whitelists to allow safe applications or IPs while minimizing false positives.
5. Handling Escalated Investigations: Take over complex security incidents escalated from L1 analysts, providing deeper analysis and resolution.

Tasks of an L3 SOC Analyst

1. Client Onboarding: Facilitate the onboarding of new clients by setting up security protocols and ensuring proper integration with the SOC.
2. Incident Management: Oversee and coordinate responses to major security incidents, ensuring effective mitigation and documentation.
3. Report and Documentation: Prepare detailed reports and maintain documentation for compliance and record-keeping.
4. Stakeholder Communication: Communicate technical information to stakeholders, keeping them informed of incident statuses and resolutions.

Security Technologies Used in SOAR (Security Orchestration, Automation, and Response)

Ticketing Systems: Track and manage security incidents from identification through resolution.

Data Loss Prevention (DLP): Protect sensitive data from unauthorized access and data breaches.

SIEM (Security Information and Event Management): Collect and analyze data from multiple sources for real time threat detection.

EDR (Endpoint Detection and Response): Monitor endpoint devices for suspicious activities and potential threats.

CTI/TIP (Cyber Threat Intelligence/Threat Intelligence Platform): Gather and analyze threat intelligence to improve security posture.

Email and Web Gateways: Protect against malicious email and web-based threats.

Network Security: Secure the organization's network from unauthorized access and cyberattacks.

Vulnerability Management: Identify and mitigate vulnerabilities within systems and applications

Cloud Tools: Manage and secure cloud-based environments and resources.

IAM/PAM (Identity and Access Management / Privileged Access Management): Control and monitor access to critical systems, limiting exposure to potential threats

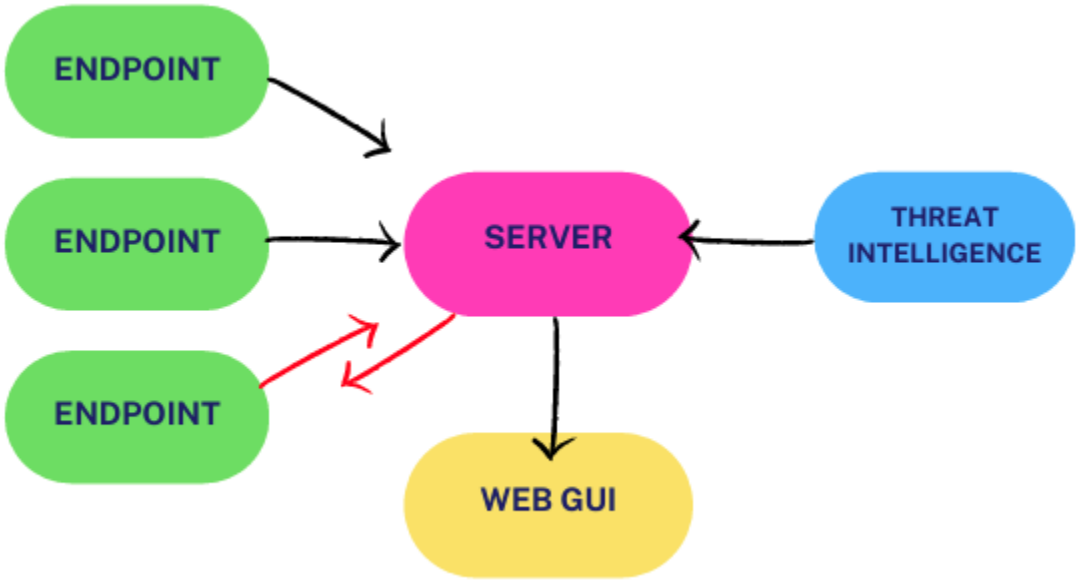
In summary, the roles and responsibilities within a Security Operations Center (SOC) are layered and demand a structured approach to ensure effective cybersecurity. L2 and L3 SOC analysts play distinct yet complementary roles, from monitoring alerts and managing escalations to overseeing client onboarding and stakeholder communication. Leveraging a suite of advanced security technologies, such as SIEM, EDR, and SOAR tools, enables SOC teams to proactively detect, respond to, and mitigate security threats. Understanding these roles and technologies is crucial for building a resilient cybersecurity infrastructure that safeguards an organization's assets and reputation in an increasingly complex threat landscape.

CHAPTER 4

Endpoint Detection and Response (EDR)

EDR Architecture Overview

- Endpoints: Devices such as computers, servers, and mobile devices, each monitored by the EDR system.
- Server: Acts as the central hub, collecting and processing data from endpoints.
- Web GUI: A graphical user interface that provides security analysts with real-time access to EDR data and controls.
- Threat Intelligence: Integration with threat intelligence sources to enhance detection accuracy and provide context for potential threats



Key Functions of EDR

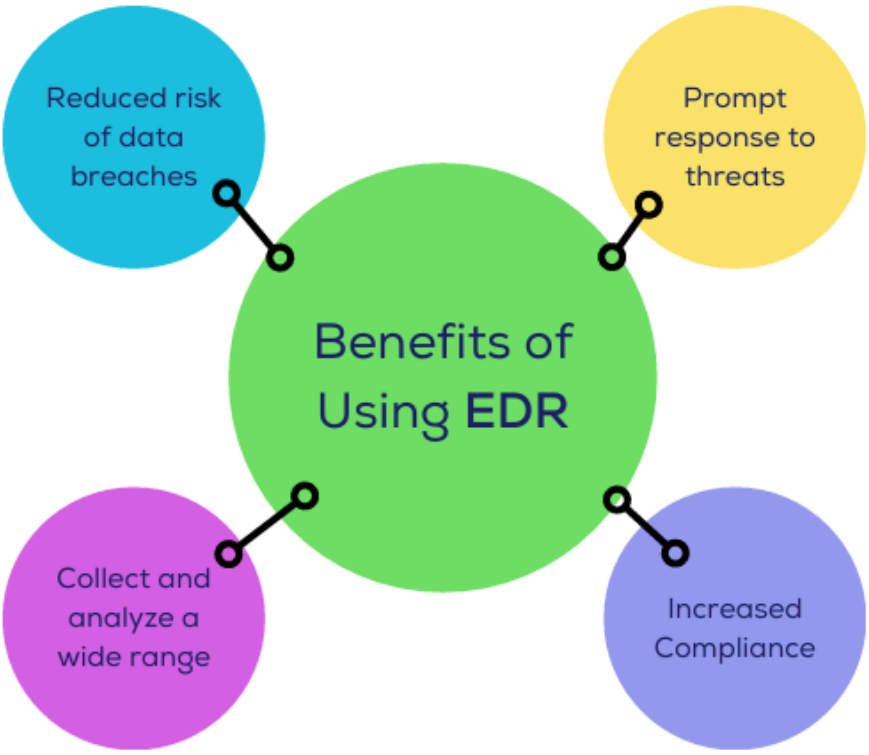
- Real-time Continuous Monitoring: Monitors endpoints for suspicious activities, whether online or offline, to provide ongoing security visibility.
- Endpoint Data Collection: Gathers detailed data from each endpoint, including system activities and behaviors.
- Signature-less Detection: Identifies threats using behavioral analysis rather than relying on known threat signatures, allowing detection of novel threats.
- Rules-based Automated Response: Triggers predefined responses to detected threats in real-time, minimizing the response time for known threats.

Data Collected by EDR

EDR systems collect a variety of endpoint data to support threat detection and incident response:

- Network Connections: Tracks outgoing and incoming network connections to identify unusual patterns.
- Process Execution: Monitors the execution of processes to detect potentially malicious behavior.
- Registry Modifications: Observes changes in the system registry, which could indicate unauthorized modifications
- Currently Running Processes: Keeps an inventory of active processes for real-time visibility into system activities.
- Cross-process Events: Tracks interactions between processes to detect suspicious behavior, such as process injection.

multinet
INFOSTRUCTURE FOR THE NATION



CHAPTER 5

Incident Response Frameworks & Automation Techniques

Automation is essential to enhance efficiency in managing cyber incidents. Key areas include:

- Triage: Prioritizing and categorizing incidents for effective response
- Enrichment: Enhancing incident data with additional context
- Threat Intelligence (TI) Gathering: Collecting relevant threat data for informed decisions
- Validation Across Detection Tools: Ensuring consistency and accuracy in detection
- False Positive Closure: Reducing unnecessary alerts to avoid resource waste
- Email Notifications: Informing users about potential threats or actions required
- Blocking IPs: Preventing further intrusion by blocking suspicious IP addresses
- Administrator Alerts: Notifying administrators of critical incidents for prompt action

NIST Incident Response Framework The National Institute of Standards and Technology (NIST) outlines a structured approach to incident response:

- Preparation: Establishing tools, policies, and teams for incident management.
- Detection and Analysis: Identifying potential incidents and analyzing their impact.
- Containment, Eradication, and Recovery: Containing the threat, eliminating it from the environment, and restoring normal operations.
- Post-Incident Activity: Reviewing the incident and improving future responses.

SANS Incident Response Framework

The SANS framework emphasizes a more granular approach to incident response:

- Preparation: Ensuring readiness with appropriate tools, training, and procedures.
- Identification: Detecting and confirming the incident.
- Containment: Limiting the scope and impact of the incident.
- Eradication: Removing the threat from the environment.
- Recovery: Restoring systems to their normal operation.

Eradication & Recovery Process

Eradication ensures that the threat is completely removed. Key steps include:

- Removing Artifacts: Deleting any remnants of the attack.
- Identifying All Hosts: Ensuring that all affected systems are accounted for.
- Updating Configurations: Making changes to prevent reoccurrence.
- Patching Vulnerabilities: Applying patches to close security gaps.
- Documentation: Recording all steps for future reference and compliance.

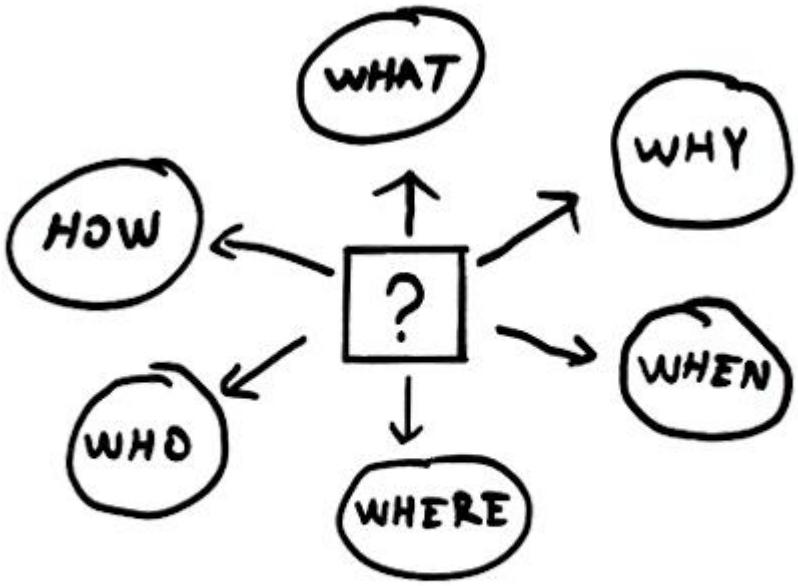
Recovery focuses on returning to normal operations:

- Restoration: Rebuilding affected systems and data.
- Normal Operations: Returning systems to their operational state.
- Activities Monitoring: Continuously monitoring for potential threats.
- Documentation: Recording recovery steps for accountability.
- Prevent Reinfection: Implementing measures to prevent future incidents

Lessons Learned

After an incident, reviewing what happened is crucial for improvement:

- Meetings: Discussing what went wrong and what went well.
- 5W+H (Who, What, When, Where, Why, and How): Analyzing the incident in depth.
- Way Forward: Developing strategies to improve response in the future.
- Documentation: Ensuring all actions taken are well documented for future reference



5WIH Method for a systematic breakdown of an incident

CHAPTER 6

Practice Websites for Blue Team Labs

These platforms provide valuable resources for practicing cybersecurity defense techniques:

Cyber Defenders Platform

Blue Team Level 1

Lets Defend

For network security use:

Netcat

Nmap

tcpdump

For malware analysis use:

Virus Total

ANY.RUN

Ghidra