Security Operations Center (SOC)

Index

Introduction

A Security Operations Center (SOC) is a centralized unit that deals with security issues on an organizational and technical level. It includes people, processes, and technology to monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents. This document covers essential components of a SOC, including SIEM, EDR, NDR, XDR, SOAR, offense management, SOC analysis, and data visualization. A step-by-step lab guide is also provided for practical learning.

SIEM (Security Information and Event Management)

SIEM technology supports threat detection, compliance, and security incident management through the collection and analysis of security events, as well as a wide variety of other log and event data sources.

Key Functions

1. **Log Collection**: Aggregates log data generated throughout the organization's technology infrastructure.
2. **Normalization and Parsing**: Converts raw data into a common format for easier analysis.
3. **Correlation**: Identifies relationships between different data points to detect suspicious activities.
4. **Alerting**: Generates alerts based on predefined rules.
5. **Reporting**: Creates reports for compliance and management.

Scenario Example

- **Scenario**: Detecting unauthorized access attempts.
    - **Setup**: Configure SIEM to collect logs from firewalls, intrusion detection systems (IDS), and Windows event logs.
    - **Implementation**: Create a correlation rule to detect multiple failed login attempts followed by a successful login.

EDR (Endpoint Detection and Response)

EDR solutions focus on monitoring and responding to threats on endpoints, such as desktops, laptops, and mobile devices.

Key Functions

1. **Real-Time Monitoring**: Continuously monitors endpoint activities.
2. **Threat Detection**: Uses behavioral analysis to detect suspicious activities.

3. **Response Capabilities**: Provides tools to contain and remediate threats.
4. **Forensics and Investigation**: Collects detailed information for post-incident analysis.

Scenario Example

- **Scenario**: Detecting and responding to malware on a workstation.
    - **Setup**: Deploy EDR agents on all endpoints.
    - **Implementation**: Configure EDR to alert on suspicious file execution patterns and enable automated isolation of compromised endpoints.

NDR (Network Detection and Response)

NDR solutions monitor network traffic to detect and respond to threats that bypass perimeter defenses.

Key Functions

1. **Traffic Analysis**: Inspects network traffic in real-time.
2. **Anomaly Detection**: Identifies deviations from normal network behavior.
3. **Incident Response**: Provides tools for investigating and responding to network-based threats.

Scenario Example

- **Scenario**: Detecting data exfiltration.
    - **Setup**: Deploy NDR sensors at strategic points in the network.
    - **Implementation**: Configure NDR to alert on large outbound data transfers to unfamiliar IP addresses.

XDR (Extended Detection and Response)

XDR is an integrated suite of security products that provide broad visibility, detection, and response capabilities across endpoints, networks, servers, and cloud environments.

Key Functions

1. **Unified Visibility**: Centralizes security data from multiple sources.
2. **Advanced Threat Detection**: Uses AI and machine learning to detect sophisticated threats.
3. **Automated Response**: Enables coordinated response actions across different security layers.

Scenario Example

- **Scenario**: Coordinating response to a ransomware attack.
    - **Setup**: Integrate EDR, NDR, and other security tools into an XDR platform.
    - **Implementation**: Configure XDR to detect ransomware patterns and automate the containment and remediation processes.

SOAR (Security Orchestration, Automation, and Response)

SOAR platforms help manage and automate security operations, coordinate incident response, and improve efficiency.

Key Functions

1. **Playbooks**: Automate response workflows.
2. **Case Management**: Centralize incident handling and tracking.
3. **Orchestration**: Integrate and coordinate actions across multiple security tools.

Scenario Example

- **Scenario**: Automating phishing response.
    - **Setup**: Develop a SOAR playbook for phishing incidents.
    - **Implementation**: Configure SOAR to automatically extract indicators from phishing emails, query threat intelligence sources, and quarantine affected user accounts.

Offense Management

Offense management involves prioritizing, analyzing, and responding to security incidents based on their potential impact.

Key Functions

1. **Prioritization**: Rank incidents by severity and potential impact.
2. **Analysis**: Investigate the root cause and scope of incidents.
3. **Response**: Take appropriate actions to mitigate and remediate threats.

Scenario Example

- **Scenario**: Managing a multi-stage attack.
    - **Setup**: Use SIEM and SOAR for comprehensive offense management.

- **Implementation**: Prioritize incidents based on risk, analyze attack vectors, and execute coordinated response actions.

SOC Analysis

SOC analysts play a critical role in monitoring, detecting, and responding to security threats.

Key Functions

1. **Threat Monitoring**: Continuously monitor security tools and dashboards.
2. **Incident Analysis**: Investigate alerts and determine the scope and impact of incidents.
3. **Threat Hunting**: Proactively search for signs of compromise.

Data Visualization with Pivots and Databases

Data visualization is crucial for understanding security data and identifying trends.

Key Techniques

1. **Pivot Tables**: Summarize and analyze complex datasets.
2. **Dashboards**: Create visual representations of key metrics and trends.
3. **Search Processing Language (SPL)**: Query and analyze data in SIEM platforms like Splunk.

Scenario Example

- **Scenario**: Visualizing attack patterns.
    - **Setup**: Use Splunk to collect and index security logs.
    - **Implementation**: Create pivot tables and dashboards to visualize failed login attempts, suspicious IP addresses, and data transfer volumes.

Generating Alerts

Generating alerts is a fundamental function of a SOC to notify analysts of potential security incidents.

Key Steps

1. **Define Alert Criteria**: Specify the conditions that trigger an alert.
2. **Configure Alerting Tools**: Set up alerts in SIEM, EDR, and other platforms.
3. **Alert Management**: Review and triage alerts to determine their significance.

Lab Guide

Prerequisites

- Access to SIEM, EDR, NDR, and SOAR platforms (e.g., Splunk, CrowdStrike, Darktrace, Palo Alto Networks Cortex XSOAR).
- Basic knowledge of security operations and incident response.

Step-by-Step Lab Guide

Step 1: Setting Up SIEM

1. **Install Splunk**:
    - Download and install Splunk on a server or use Splunk Cloud.
    - Configure data inputs for logs from firewalls, IDS, and Windows event logs.
2. **Create a Correlation Rule**:
    - Navigate to the "Search & Reporting" app.
    - Create a new correlation search to detect multiple failed login attempts.

spl

index=main sourcetype=windows:security EventCode=4625 | stats count by src_ip | where count > 5

Step 2: Deploying EDR

1. **Install CrowdStrike Falcon**:
    - Deploy CrowdStrike agents on all endpoints.
    - Configure policies for threat detection and response.
2. **Create an Alert for Malware Detection**:
    - Navigate to the "Detection" tab.
    - Create a rule to alert on suspicious file executions.

Step 3: Configuring NDR

1. **Install Darktrace**:
    - Deploy Darktrace sensors in the network.
    - Configure traffic analysis and anomaly detection settings.
2. **Create an Alert for Data Exfiltration**:

- Navigate to the "Threat Visualizer".
- Create an alert for large outbound data transfers to unfamiliar IPs.

Step 4: Integrating XDR

1. **Set Up Palo Alto Networks Cortex XDR**:
   - Integrate EDR, NDR, and other security tools.
   - Configure unified visibility and detection rules.
2. **Create an Automated Response for Ransomware**:
   - Navigate to the "Incident Management" tab.
   - Configure an automated playbook to isolate infected endpoints and block malicious IPs.

Step 5: Automating with SOAR

1. **Install Cortex XSOAR**:
   - Deploy Cortex XSOAR on a server.
   - Integrate with SIEM, EDR, and other tools.
2. **Create a Phishing Response Playbook**:
   - Navigate to the "Playbooks" tab.
   - Create a playbook to extract indicators from emails, query threat intelligence, and quarantine user accounts.

Step 6: Offense Management and SOC Analysis

1. **Prioritize and Analyze Incidents**:
   - Use Splunk for offense management.
   - Prioritize incidents based on risk and analyze the root cause.
2. **Perform Threat Hunting**:
   - Use Splunk's SPL to search for signs of compromise.

spl

index=main sourcetype=windows:security | search "privilege escalation"

Step 7: Data Visualization

1. **Create Dashboards in Splunk**:
   - Navigate to the "Dashboards" tab.

- Create visualizations for key metrics like failed logins and data transfer volumes.

2. **Use Pivot Tables**:
    - Navigate to the "Pivot" tab.
    - Create pivot tables to analyze complex datasets.

Step 8: Generating Alerts

1. **Define Alert Criteria in Splunk**:
    - Navigate to the "Search & Reporting" app.
    - Create a new alert for unusual login activity.

spl

index=main sourcetype=windows:security EventCode=4624 | stats count by src_ip | where count > 10

2. **Configure Alert Notifications**:
    - Set up email notifications for alerts.
    - Configure integration with SOAR for automated response.

Conclusion

Understanding the components and functions of a SOC is crucial for effective security operations and incident response. By following the outlined concepts and the provided lab guide, you can develop and utilize SOC tools and techniques effectively. Regular practice and exploration of advanced features will further enhance your skills and capabilities in managing and securing a SOC.