Security Operations Center (SOC)

Rohan Idiculla Abraham

21BEC1080

A security operations center (SOC) – sometimes called an information security operations center, or ISOC – is an in-house or outsourced team of IT security professionals that monitors an organization's entire IT infrastructure, 24/7, to detect cybersecurity events in real time and address them as quickly and effectively as possible.

What does a SOC Team Member do?

Members of a SOC team are responsible for a variety of activities, including proactive monitoring, incident response and recovery, remediation activities, compliance, and coordination and context.

- **Proactive Monitoring:**

This includes log file analysis. Logs can come from end points or from network resources, such as routers, firewalls, intrusion detection system (IDS) applications and email appliances.

- **Incident Response and Recovery:**

A SOC coordinates an organization's ability to take the necessary steps to mitigate damage and communicate properly to keep the organization running after an incident.

- **Remediation Activities:**

SOC team members provide data-driven analysis that helps an organization address vulnerabilities and adjust security monitoring and alerting tools.

- **Compliance:**

Organizations secure themselves through conformity to a security policy, as well as external security standards, such as ISO 27001x, the NIST Cybersecurity Framework (CSF) and the General Data Protection Regulation (GDPR). Organizations need a SOC to help ensure that they are compliant with important security standards and best practices.

- **Coordination and Context:**

Above all, a SOC team member helps an organization coordinate disparate elements and services and provide visualized, useful information. Part of this coordination is the ability to provide a helpful, useful set of narratives for activities on the network. These narratives help shape a company's cybersecurity policy and posture for the future.

Key SOC roles and responsibilities:

- SOC manager
- Compliance auditor

- Incident Responder
- SOC analyst
- Threat hunter

SOC as a service (SOCaaS)

SOCaaS is a security model that allows a third-party vendor to operate and maintain a fully managed SOC on a subscription basis. This service includes all of the security functions performed by a traditional, in-house SOC, including network monitoring; log management; threat detection and intelligence; incident investigation and response; reporting; and risk and compliance. The vendor also assumes responsibility for all people, processes and technologies needed to enable those services and provide 24/7 support.

SIEM solutions in SOC

Security information and event management (SIEM) solutions are a type of security solution that helps businesses monitor and analyze their security data in real time. SIEM solutions collect data from multiple sources, including network devices, applications and user activity, and use analytics to detect potential threats.

SIEM solutions allow businesses to respond quickly to security incidents and take corrective action. For many SOCs, this is the core monitoring, detection and response technology utilized to monitor and aggregate alerts and telemetry from software and hardware on the network and analyze the data for potential threats.

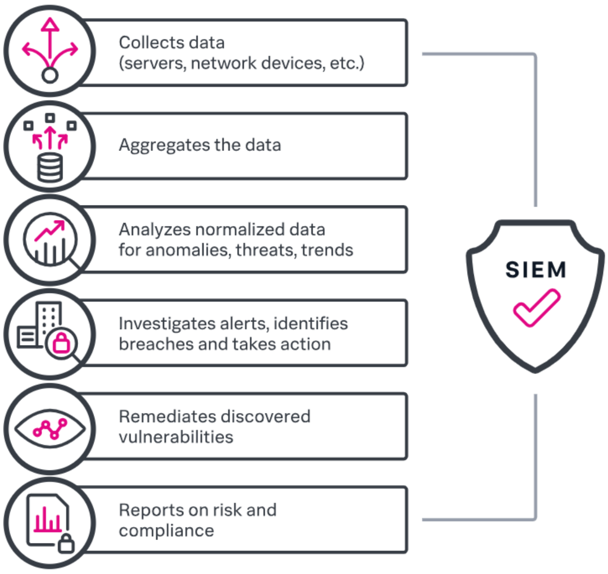
Working of SIEM:

At the most basic level, all SIEM solutions perform some level of data aggregation, consolidation and sorting functions in order to identify threats and adhere to data compliance requirements.

Main functionality:

- Log Management
- Event Correlation and Analytics
- Incident Monitoring and Security Alerts
- Compliance Management and Reporting

A SIEM solution aggregates event data across disparate sources within your network infrastructure, including servers, systems, devices and applications, from perimeter to end user, and including cloud, multicloud and hybrid environments, as well as on-premises. Ultimately, a SIEM solution offers a centralized view with additional insights, combining context information about your users, assets and more. It consolidates and analyzes the data for deviations against behavioural rules defined by your organization to identify potential threats.



IBM QRadar

The IBM QRadar SIEM can be deployed as a hardware, software or virtual appliance-based product. The product architecture includes event processors for collecting, storing and analyzing event data and event collectors for capturing and forwarding data. The SIEM product also includes flow processors to collect Layer 4 network flows, QFlow processors for performing deep packet inspection of Layer 7 application traffic, and centralized consoles for Security Operations Center (SOC) analysts to utilize when managing the SIEM. Flow processors offer similar capabilities to event processors, but are for network flows, and consoles are for people to utilize when using or managing the SIEM.

There are three layers of functionality

- Data Collection

Data collection is the first layer, where data such as events or flows is collected from your network. The All-in-One appliance can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QRadar QFlow Collectors to collect event or flow data.

- Data Processing

After data collection, the second layer or data processing layer is where event data and flow data are run through the Custom Rules Engine (CRE), which generates offenses and alerts, and then the data is written to storage.

- Data Searches

In the third or top layer, data that is collected and processed by QRadar is available to users for searches, analysis, reporting, and alerts or offense investigation. Users can search, and manage the security admin tasks for their network from the user interface on the QRadar Console.

Use Cases

- Real Time threat Intelligence

Scenario

Security operation centers faced with overwhelming amounts of data must narrow the funnel and accelerate throughput without creating false positives to effectively mitigate a threat. Less noise allows analysts to focus on the critical events and IOCs.

Scheduled database queries give attackers the chance to do more damage but real time monitoring enables faster detection. Real time event processing provides immediate notification before an attack spreads, and real-time event log enrichment specifies critical environmental data.

Solution

- Discovers, interprets and classifies network assets, devices, users and applications automatically

- Analyzes and correlates across multiple data sources to identify known and unknown threats automatically

- Reduces and prioritizes events into a few actionable offenses, according to their importance and business impact

- Allows for custom rules and tailored anomaly detection settings

- Identify Patient Zero

Scenario

Security teams must find the initial point of attack and figure out how the malicious payload was disseminated beyond the point of entry.

Compromised entities need to be quarantined to prevent the spread of the attack. What, if any, peripheral actions were taken to circumvent cleanup activities.

Solution

- Searches historical network activity to identify anomalous communications (I,e., patient zero)

- Reconstructs raw network data back to its original form and retraces the security incident

- Identifies suspect or unexpected content and activity in network communications

- Generates multiple views of data including relationships, timelines, source and threat category

- Uses data pivoting and follow data linkages

- Abnormal Connection Behaviour

Scenario

Unusual or illogical volume, time or geography in connection can indicate an attack, which can be through rogue services and systems, malware and worm propagation, communication with IP blacklist and unauthorized or tunneled services.

Hosts exhibiting infection behaviors must be addressed and remote attackers blocked before they make it into the network. Back scatter must be identified as well as traffic that's allowed from and/or to known blacklisted sources. Ports should be scanned to verify security policies.

Solution

- Customizes default rules to detect unusual network activity.

- Generates alerts and offenses based on:

    - Clean/quarantine events from a single IP Address
    - Existing services that have stopped or crashed
    - When a highly valued server suddenly starts using new applications or communicates with outside assets
    - Multiple firewall drop/reject/deny events and IDS alerts from a single IP Address
    - Multiple failed events from a single IP Address that is not part of the known internal network
    - Allowed events from an IP Address that are not part of the known network and are known to have/use malware
    - Appearance of new hosts and services on the network

- DNS attack

Scenario

Many organizations do not monitor their DNS traffic for malicious activity. But DNS as a tunnel can be established while hiding data inside the DNS requests, which can be turned into real data on the destination DNS server.

Malicious software uses DNS to get data out of the company network or receive commands/updates from a command and control server.

Solution

- Utilize QNI flows or logs with domain information from other devices including:
    - DNS Servers
    - Proxies
    - Apache Webservers
    - Other BIND compatible devices
- Detect and monitor outbound requests to malicious sites
- Drill down and identify DNS trends and activity using DNS analyzer dashboard
- Detect DGA, tunneling or squatting domains being accessed from within network