A - Z

OF

SECURITY OPERATIONS CENTER (SOC)

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to
next slide ➔

A ALERTING

SOC teams set up alerts to quickly identify and respond to security incidents.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

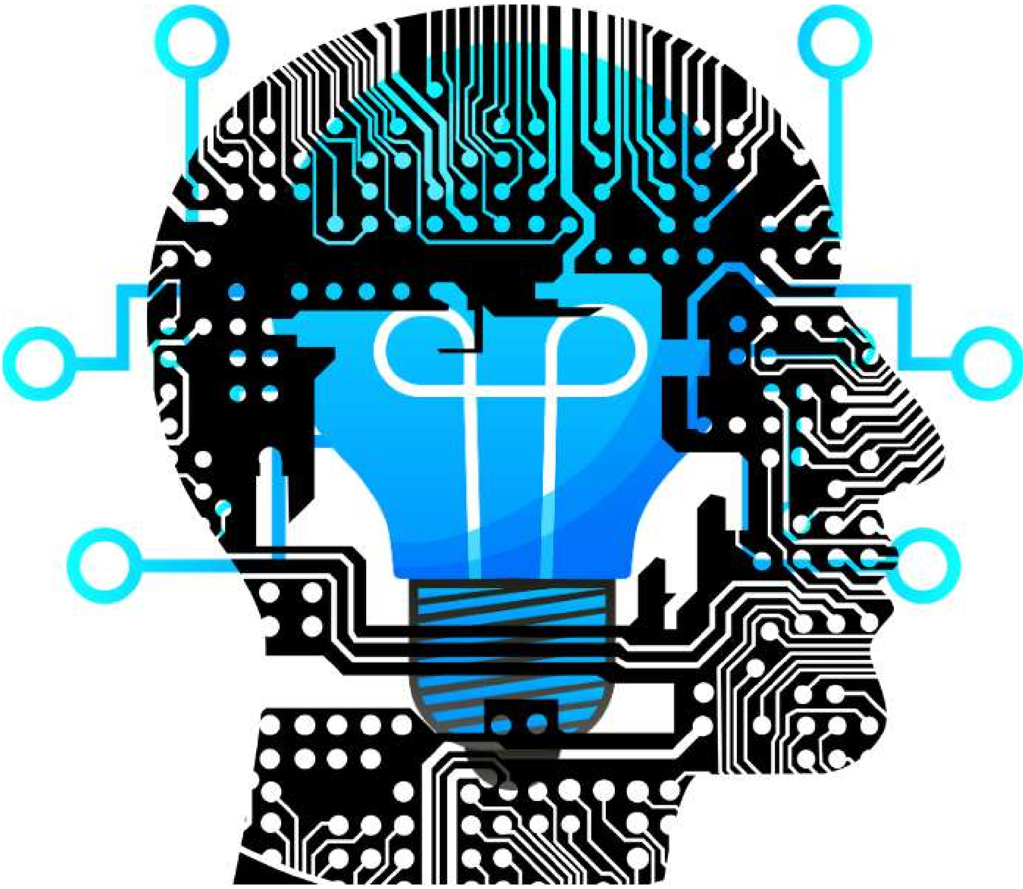
B

BLUE TEAM

The defensive cybersecurity team within a SOC focused on protecting systems and networks.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔



C

CYBER THREAT INTELLIGENCE

SOC analysts utilize threat intelligence to proactively defend against potential cyber threats.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

D DETECTION

SOC's primary function is to detect and respond to cybersecurity incidents.

Elizabeth Ekedoro
@ElizabethEkedoro

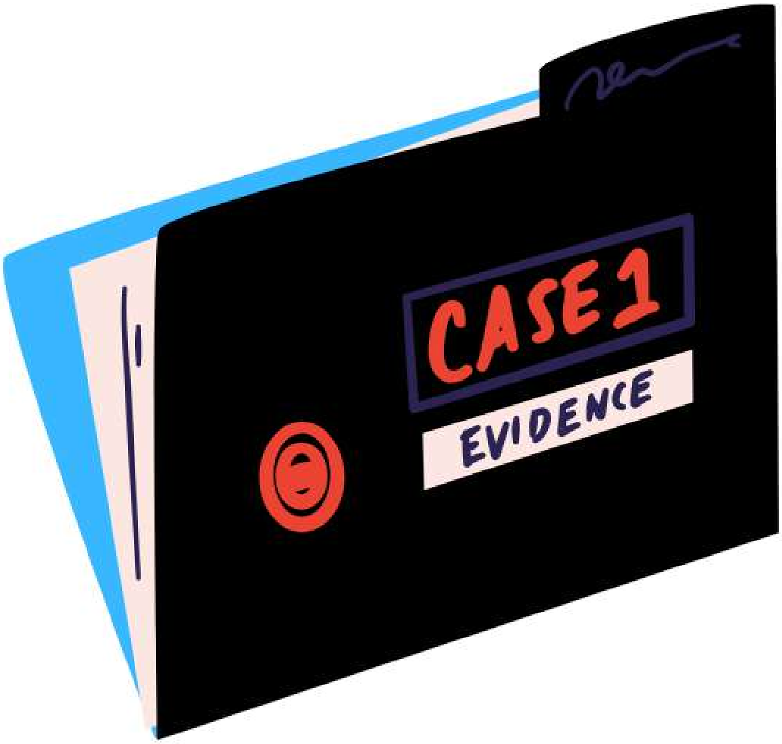
Swipe to next slide →

E ENDPOINT SECURITY

SOC analysts monitor and secure endpoints such as laptops, desktops, and servers to prevent security breaches.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide



F

FORENSICS

SOC teams conduct digital forensics to investigate security incidents and identify root causes.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide →

G

GATEWAY

SOC teams use gateways as a defense mechanism to monitor, detect, and block potential threats before they reach the internal network.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

H

HONEYPOT

SOC analysts deploy decoy systems to lure and study attackers' behavior in a controlled environment.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔

INCIDENT RESPONSE

SOC analysts React to and resolve security incidents efficiently to minimize the impact.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

J

JUST-IN-TIME TRAINING

Providing SOC analysts with timely and relevant training to enhance their skills and response capabilities.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

K KEY PERFORMANCE INDICATORS (KPIS)

Metrics used to measure the effectiveness and performance of a SOC.

Elizabeth Ekedoro
@ElizabethEkedoro

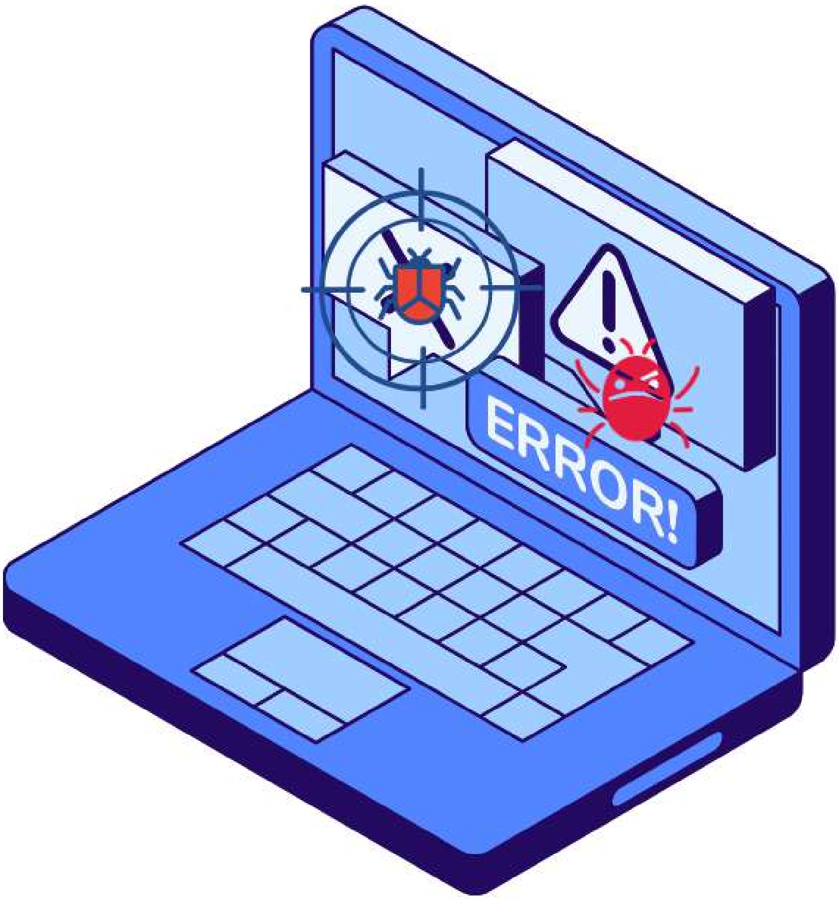
Swipe to next slide

L LOG MONITORING

SOC teams analyze log data from various sources to identify potential security incidents.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔



M MALWARE ANALYSIS

SOC analysts study malware samples to understand their behavior, origins, and potential impact.

Elizabeth Ekedoro
@ElizabethEkedoro

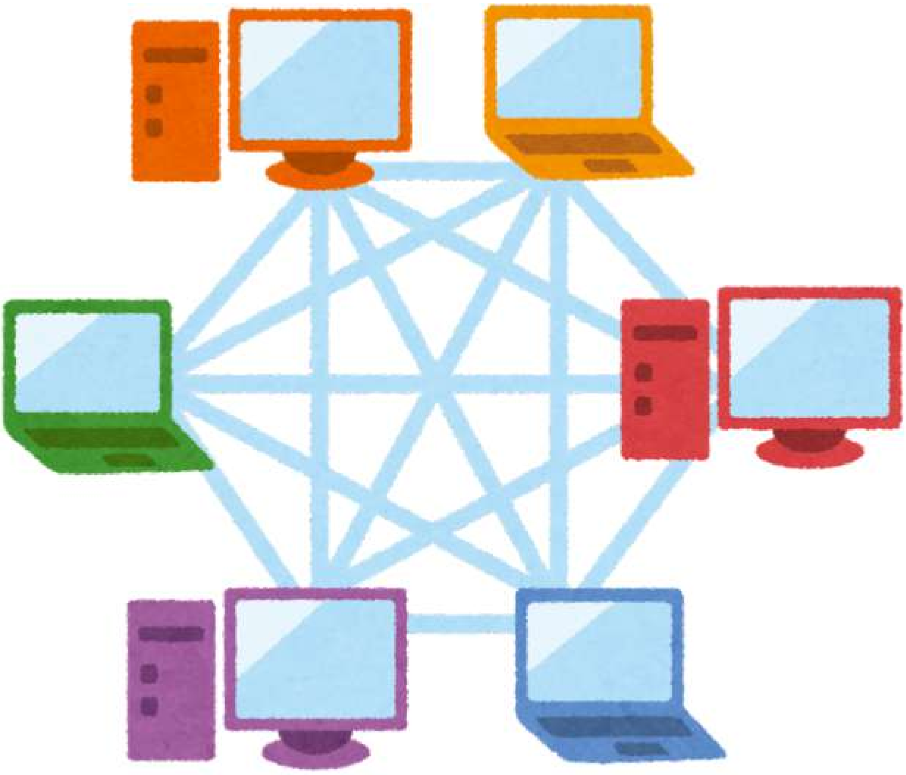
Swipe to next slide

O ORCHESTRATION

SOC analysts automate and orchestrate security processes to streamline incident response and management.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔

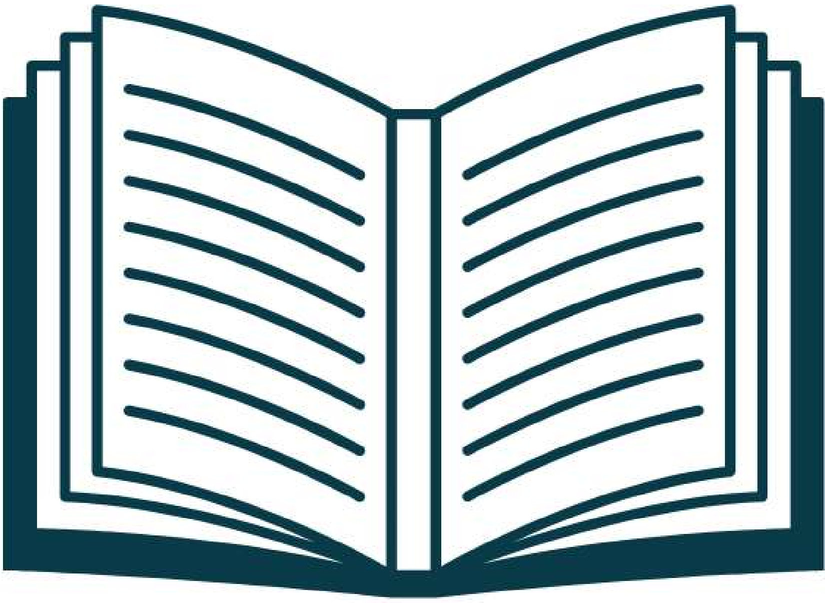


N NETWORK SECURITY

SOC teams monitor and secure network traffic to identify and block threats.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔



P

PLAYBOOKS

Pre-defined response procedures and workflows used by SOC analysts during incident response.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

Q

QUERY

SOC analysts use queries to search for particular patterns, behaviors, or indicators of compromise within the vast amount of data collected by various security tools.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide →

R REPORTING

SOC analysts compile incident reports and communicate findings to senior management. Their insights help stakeholders make informed decisions regarding security enhancements.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔

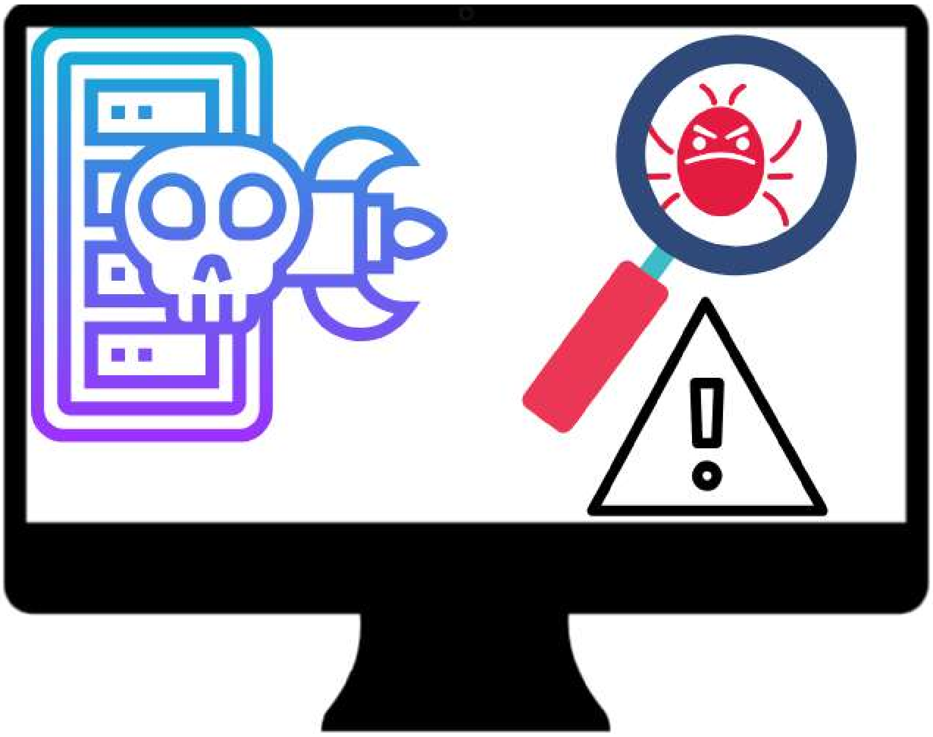
S

SIEM (SECURITY INFORMATION AND EVENT MANAGEMENT)

Platforms used by SOCs to centralize and analyze security alerts and data e.g Splunk

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide



THREAT HUNTING

SOC analysts proactively search for and identify threats within network and system data.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

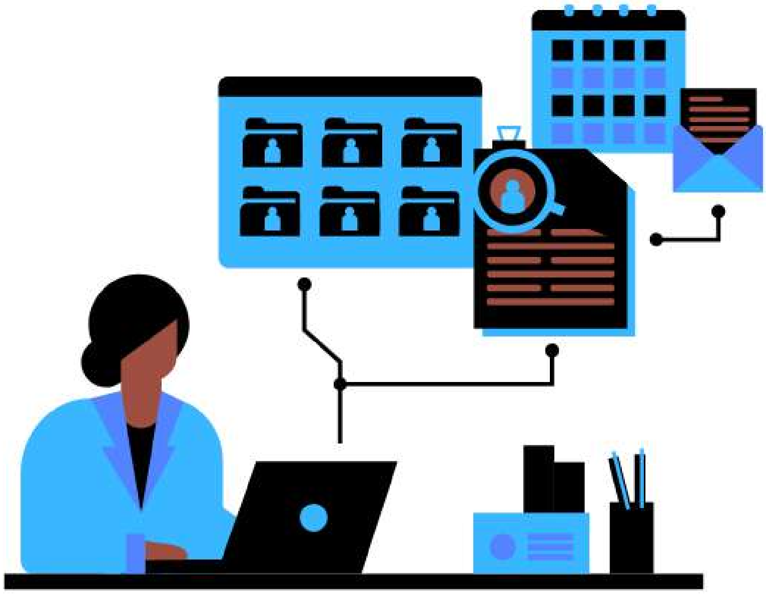
U

UBA (USER BEHAVIOR ANALYTICS)

SOC teams are responsible for monitoring and analyzing user behavior to detect insider threats and anomalous activities.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔



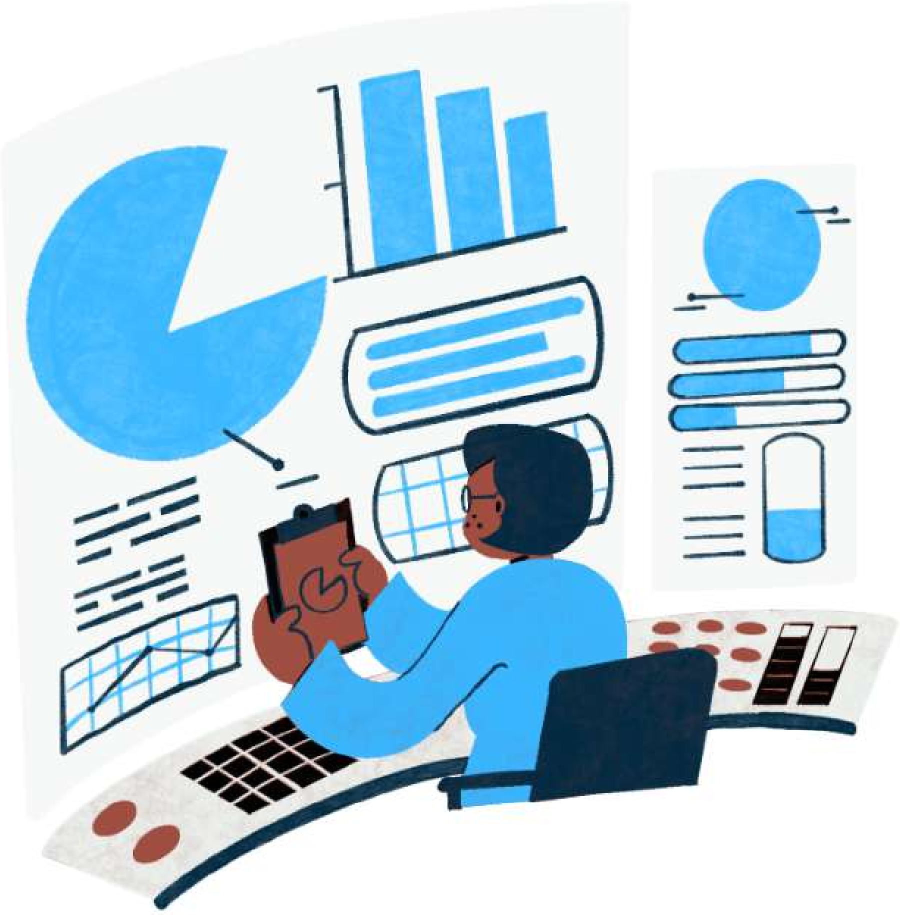
V

VULNERABILITY MANAGEMENT

SOC teams are responsible for Identifying and mitigating vulnerabilities in systems and applications to prevent cyberattacks.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide ➔



W WORKSTATION

This is a specialized set-up SOC analysts use for monitoring network security, analyzing potential threats, and responding to cybersecurity Incidents.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

X

XDR (EXTENDED DETECTION AND RESPONSE)

A powerful security solution used by SOCs for monitoring, analyzing, and responding to security incidents across multiple environments.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide

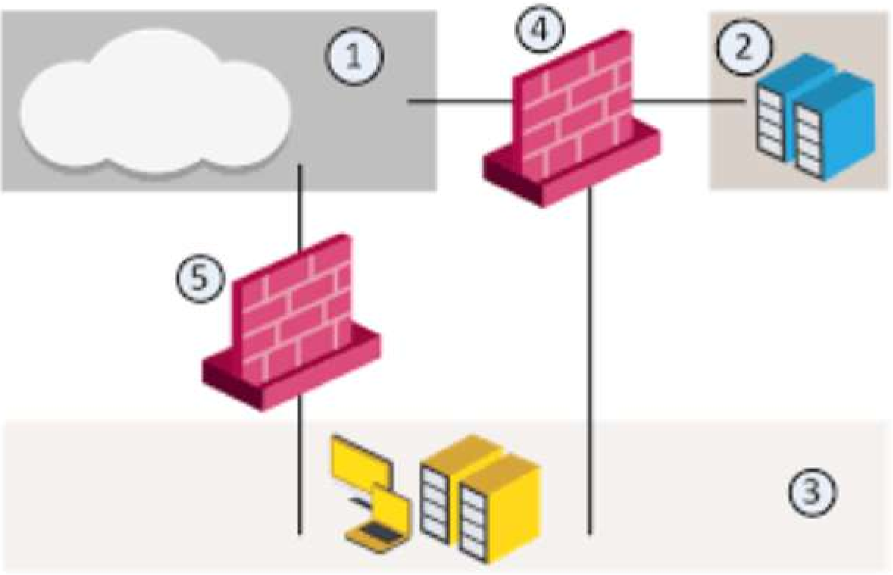
Y

YARA RULE

SOC analysts use YARA rules to detect the presence of malware within a set of files, assess the security of a potentially compromised system, and pinpoint shared characteristics among malware samples.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to next slide



Z ZONED SECURITY

This is a strategy that involves dividing a network or information system into different security zones based on the sensitivity of the data and the level of access required.

Elizabeth Ekedoro
@ElizabethEkedoro

Swipe to
next slide

Save if you like this post

Follow me for more:

@ElizabethEkedoro