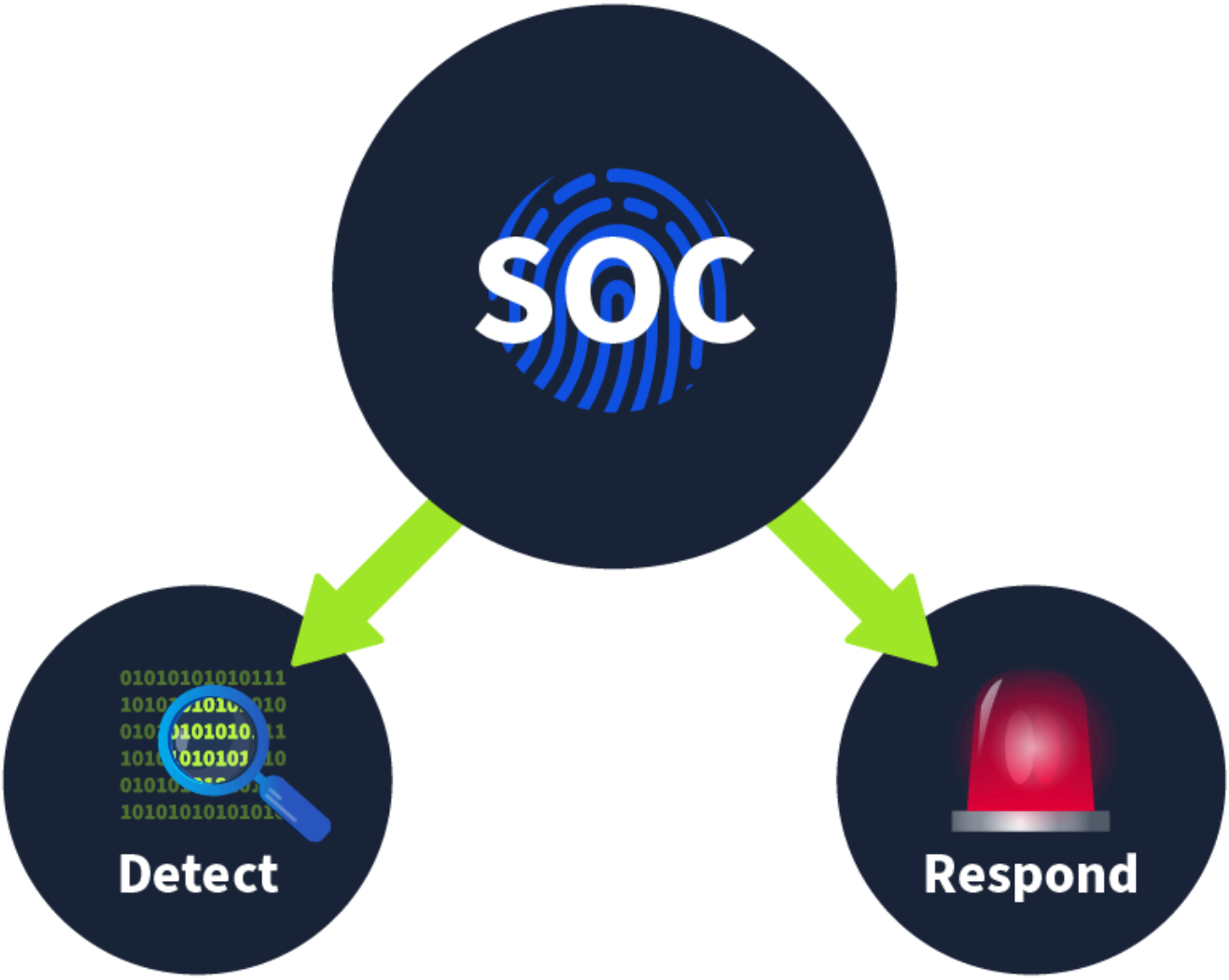
SOC Fundamentals

Introduction to SOC

A **SOC** (**S**ecurity **O**perations **C**enter) is a dedicated facility operated by a specialized security team. This team aims to continuously monitor an organization's network and resources and identify suspicious activity to prevent damage. This team works 24 hours a day, seven days a week.

Purpose and Componenets

The main focus of the SOC team is to keep **Detection** and **Response** intact



Detection:

Detect vulnerabilities: A vulnerability is a weakness that an attacker can exploit to carry out things beyond their permission level

Detect unauthorized activity: Consider the case where an attacker discovered the username and password of one of the employees and used them to log in to the company system. Many clues, such as geographic location, can help us detect this.

Detect policy violations: A security policy is a set of rules and procedures created to help protect a company against security threats and ensure compliance

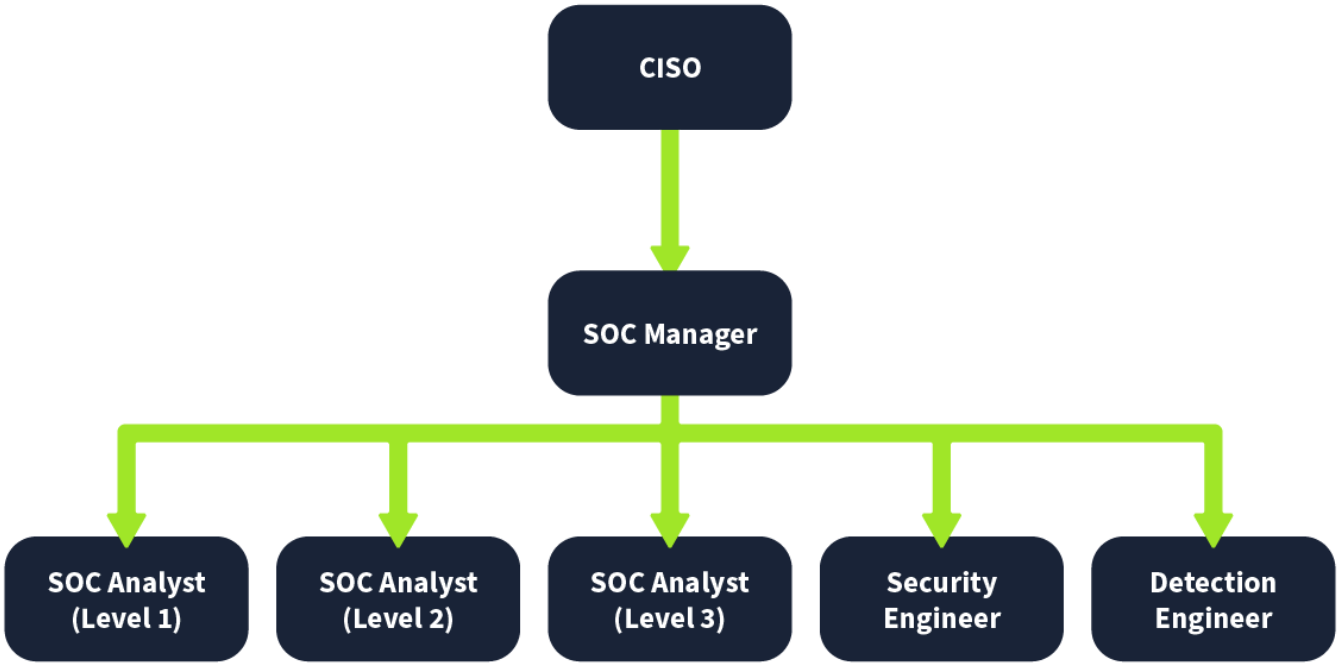
Detect intrusions: Intrusions refer to unauthorized access to systems and networks. One scenario would be an attacker successfully exploiting our web application.

Response:

-**Support with the incident response**: Once an incident is detected, certain steps are taken to respond to it. This response includes minimizing its impact and performing the root cause analysis of the incident. The SOC team also helps the incident response team carry out these steps.

People

The **People** are known as the SOC team. This team has the following roles and responsibilities.



SOC Analyst (Level 1): Anything detected by the security solution would pass through these analysts first. These are the first responders to any detection.

SOC Analyst (Level 2): While Level 1 does the first-level analysis, some detections may require deeper investigation

SOC Analyst (Level 3): Level 3 Analysts are experienced professionals who proactively look for any threat indicators and support in the incident response activities.

Security Engineer: All analysts work on security solutions. These solutions need deployment and configuration. Security Engineers deploy and configure these security solutions to ensure their smooth operation.

Detection Engineer: Security rules are the logic built behind security solutions to detect harmful activities

SOC Manager: The SOC Manager manages the processes the SOC team follows and provides support. The SOC Manager also remains in contact with the organization's CISO (Chief Information Security Officer) to provide them with updates on the SOC team's current security posture and efforts.

Process

Alert Triage

The first response to any alert is to perform the triage. The triage is focused on analysing the specific alert. This determines the severity of the alert and helps us prioritise it.


Who
What
Why
Where
When

Alert: Malware detected on Host: GEORGE PC

5 Ws	Answers
What?	A malicious file was detected on one of the hosts inside the organization's network.
When?	The file was detected at 13:20 on June 5, 2024.
Where?	The file was detected in the directory of the host: "GEORGE PC".
Who?	The file was detected for the user George.
Why?	After the investigation, it was found that the file was downloaded from a pirated software-selling website. The investigation with the user revealed that they downloaded the file as they wanted to use a software for free.

Reporting

The detected harmful alerts need to be escalated to higher-level analysts for a timely response and resolution. These alerts are escalated as tickets and assigned to the relevant people

Incident Response and Forensics

Sometimes, the reported detections point to highly malicious activities that are critical. In these scenarios, high-level teams initiate an incident response.

Technology

SIEM: Security Information and Event Management (SIEM) is a popular tool used in almost every SOC environment. This tool collects logs from various network devices, referred to as log sources.

Detection rules are configured in the SIEM solution, which contains logic to identify suspicious activity.

EDR: Endpoint Detection and Response (EDR) provides the SOC team with detailed real-time and historical visibility of the devices' activities. It operates on the endpoint level and can carry

out automated responses

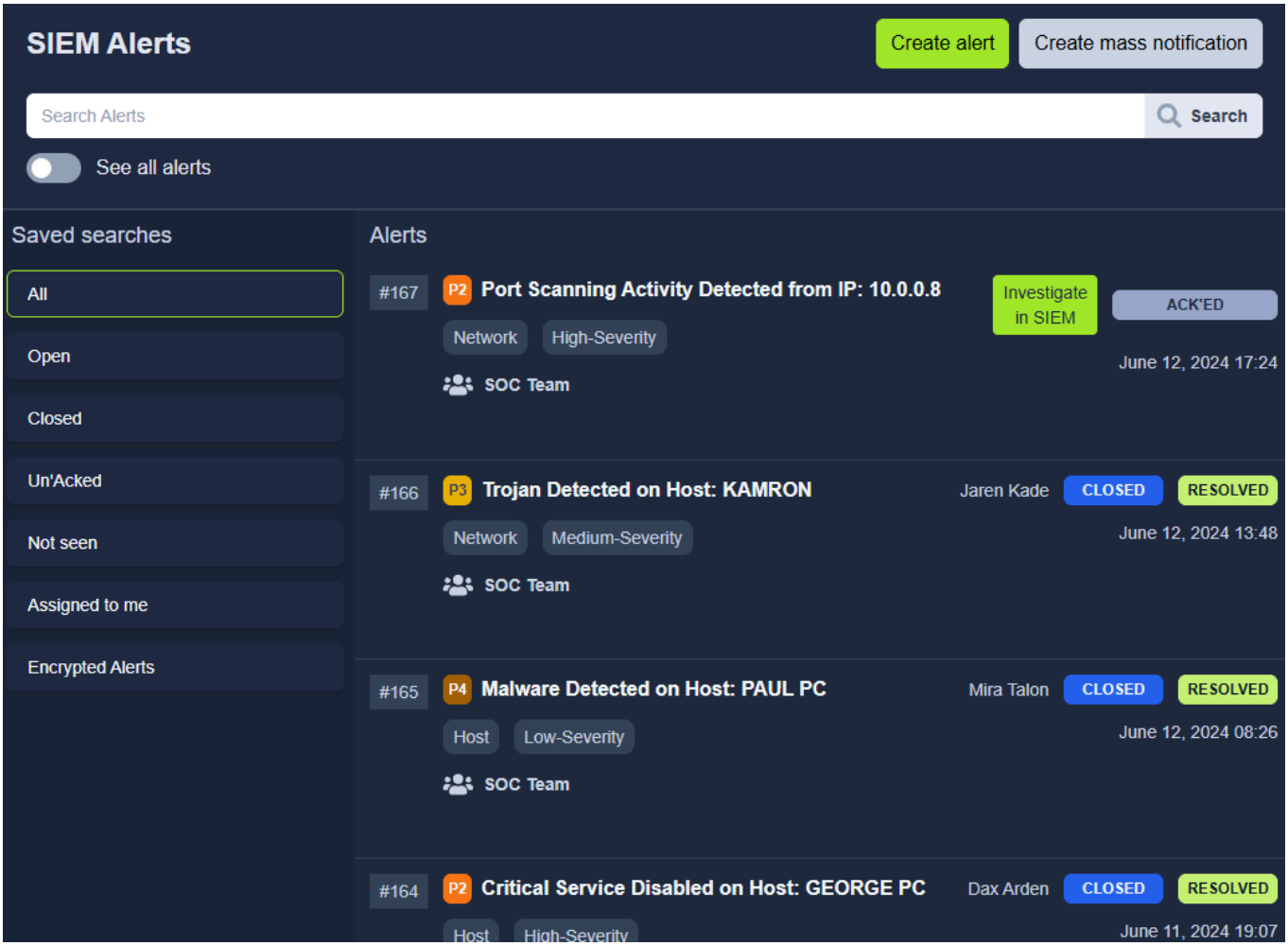
Firewall: A firewall functions purely for network security and acts as a barrier between your internal and external networks (such as the Internet). It monitors incoming and outgoing network traffic and filters any unauthorized traffic.

Several other security solutions play unique roles in a SOC environment, such as Antivirus, EPP, IDS/IPS, XDR, SOAR, and more

Practical Exercise of SOC

You receive an alert that a port scanning activity has been observed on one of the hosts in the network. You have access to the SIEM solution, where you can see all the associated logs for this alert

Note: The vulnerability assessment team notified the SOC team that they were running a port scan activity inside the network from the host: `10.0.0.8`



I had to analyse these logs

Time	Log Type	Source Range	Source IP	Destination IP	Source Port	Destination Port	Source Host Name	Destination Host Name
June 12, 2024 17:24	Traffic	Private	10.0.0.8	10.0.0.3	56927	443	NESSUS	JOE PC
June 12, 2024 17:24	Traffic	Private	10.0.0.8	10.0.0.3	56927	53	NESSUS	JOE PC
June 12, 2024 17:24	Traffic	Private	10.0.0.8	10.0.0.3	56927	22	NESSUS	JOE PC
June 12, 2024 17:24	Traffic	Private	10.0.0.8	10.0.0.3	56927	22	NESSUS	JOE PC
June 12, 2024 17:24	Traffic	Private	10.0.0.8	10.0.0.3	56927	22	NESSUS	JOE PC
June 12, 2024 17:24	Traffic	Private	10.0.0.3	10.0.0.8	22	56927	JOE PC	NESSUS

These logs show a port scan which triggered the alert i had to note down the date and time of the alert, Destination IP address, source host name and if the reason for the activity was intended or malicious

the vulnerability assessment team notified the SOC team that they were running a port scan activity inside the network from the host: 10.0.0.8