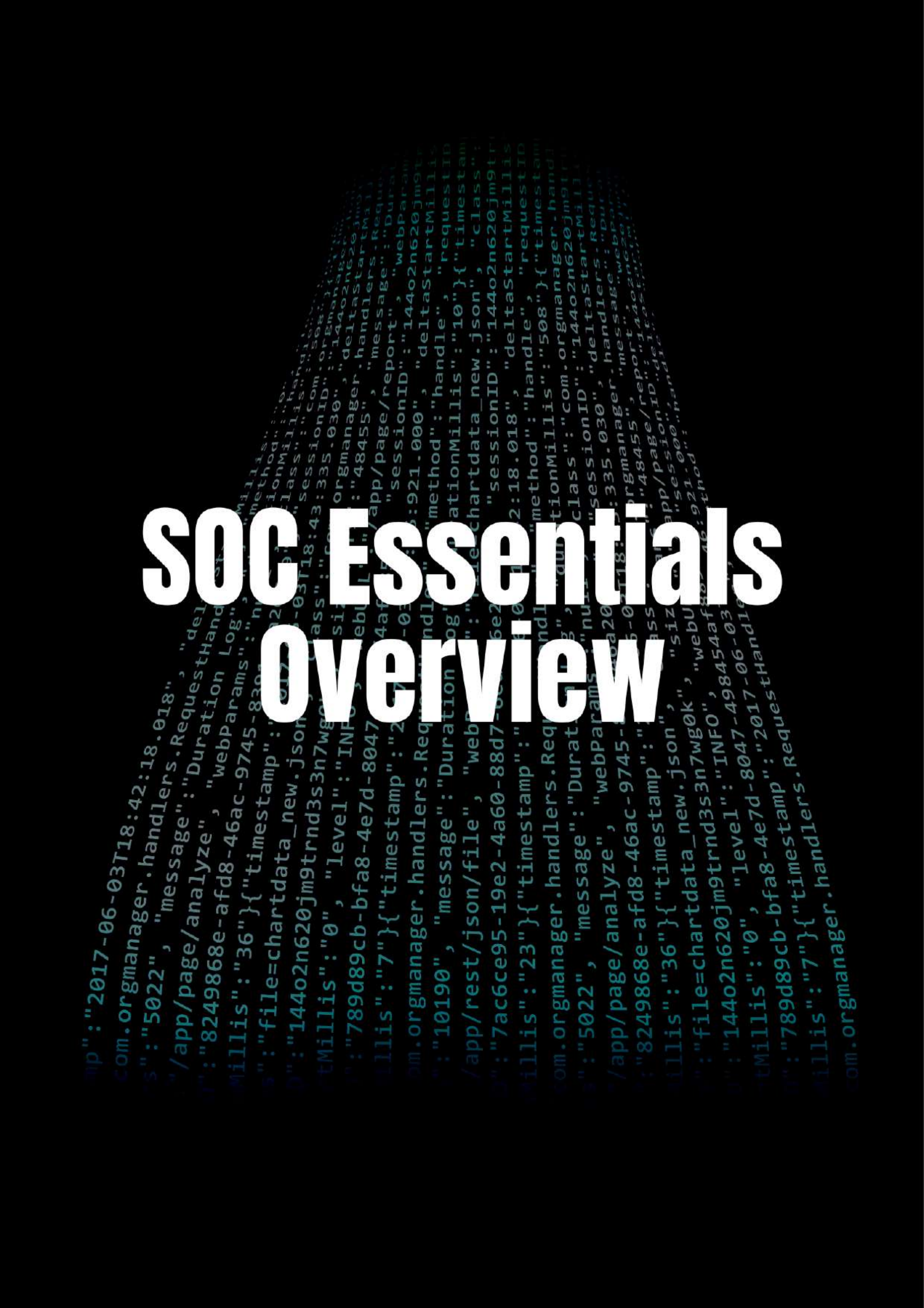

SOC Essentials
Overview

Introduction to SOC

If you want to become a SOC Analyst

If becoming a SOC Analyst is your career goal, we recommend you focus on SOC tools such as SIEM, Log Management, and EDR, and take notes.

SOC types & roles

What is SOC

A Security Operation Center (SOC) is a facility where the information security team continuously monitors and analyzes the security of an organization. The primary purpose of the SOC team is to detect, analyze, and respond to cybersecurity incidents using technology, people, and processes.

Types of SOC Models

- In-house SOC
- Virtual SOC
- Co-Managed SOC
- Command SOC

1. In-house SOC

This team is formed when an organization builds its cybersecurity team. Organizations considering an internal SOC should have a budget to support its continuity.

2. Virtual SOC

This type of SOC team does not have a permanent facility and often works remotely in various locations.

3. Co-Managed SOC

The Co-Managed SOC consists of internal SOC staff working with an external Managed Security Service Provider (MSSP). Coordination is key in this type of model.

4. Command SOC

This SOC team oversees smaller SOCs across a large region. Organizations using this model include large telecommunications providers and defense agencies.

People, Process & Technology

Building a successful SOC requires serious coordination. Most importantly, there should be a strong relationship between people, processes, and technology.

Simply put, we will discuss the people, processes, and technologies required for SOC.

1. People

A strong SOC team requires highly trained personnel who are familiar with security alerts and attack scenarios. Because attack types are constantly changing, you need team members who can easily adapt to new attack types and are willing to conduct research.

2. Processes

To further develop your SOC structure, you need to align it with many different types of security requirements, such as NIST, PCI, and HIPAA. All processes require extreme standardization of actions to ensure nothing is left out.

3. Technology

The team needs to have different products for many tasks, such as penetration testing, detection, prevention, and analysis, and they need to follow the market and technology closely to find the best solution for the organization. Sometimes the best product on the market may not be the best product for your team. Remember to consider other factors such as the organization's budget.

SOC Roles

- SOC Analyst
- Incident Responder
- Threat Hunter
- Security Engineer
- SOC Manager

1. SOC Analyst

This role can be categorized as Level 1, 2, and 3 according to the SOC structure. A security analyst classifies the alert, looks for the cause, and advises on remediation.

2. Incident Responder

An Incident Response Officer is an individual responsible for threat detection. This role performs the initial assessment of security breaches.

3. Threat Hunter

A Threat Hunter is a cybersecurity professional who proactively seeks out and investigates potential threats and vulnerabilities within an organization's network or system. They use a combination of manual and automated techniques to detect, isolate, and mitigate advanced persistent threats (APTs) and other sophisticated attacks that may evade traditional security measures. Threat hunters typically have a deep understanding of the organization's IT infrastructure and security posture, as well as knowledge of emerging threats and attack tactics. They aim to find and eliminate threats before they can damage or disrupt the business.

4. Security Engineer

Security engineers are responsible for maintaining the security infrastructure of Security Information and Event Management (SIEM) solutions and security operations center (SOC) products. For example, a security engineer builds the connection between SIEM and Security Orchestration, Automation, and Response (SOAR) products.

5. SOC Manager

A SOC manager takes on management responsibilities such as budgeting, strategizing, managing staff, and coordinating operations. They deal with operational rather than technical issues.

SOC Analyst & their Responsibilities

In this section, we will discuss what a SOC Analyst is, where they fit into the SOC team, and the general responsibilities of the role. It is important to review these sections carefully before learning about the technical side of the role. In this way, aspiring SOC Analyst candidates can get an idea of what their future career might look like.

A SOC Analyst is the first person to investigate threats to a system. If the situation demands it, they escalate incidents to their supervisors so they can mitigate threats. The SOC Analyst plays an important role on the SOC team because they are the first person to respond to a threat.

The Advantages of being a SOC Analyst

There are many various techniques for attack vectors and malicious software and they increase more and more every day. As an analyst you will get greater enjoyment from investigating these varying types of incidents. Even though the operating systems, security products, etc. that you use will be the same the job will feel less monotonous because you will be analyzing different incidents. Also, you may not encounter such techniques (not every week or every day).

A day in the life of a SOC analyst

Throughout the day, a SOC analyst typically reviews alerts in the SIEM and determines which ones are real threats. To reach a conclusion, they use various security and protection products such as Endpoint Detection and Response (EDR), Log Management, and SOAR. We will explain in detail why and how these products are used later in the training program.

To be a successful SOC analyst who is not dependent on security products and can correctly analyze SIEM alerts, you must have the following skills and abilities.

Operating Systems

To determine what is abnormal in a system, you first need to know what is accepted as normal. For example, there are many services within the Windows operating system, and it is difficult to know which ones are suspicious without knowing which ones are or could be considered normal Windows services. Therefore, you should be familiar with how Windows/Linux operating systems work.

Network

First and foremost, in this role, you will be dealing with a lot of malicious IPs and URLs, so you need to confirm that there are no devices on the network trying to connect to those addresses. Once you accomplish that, it will set the direction of the analysis.

This step is a bit more complicated because you may have to find a potential data leak on the network. To perform all of these functions, you need to understand the basics of networking.

Malware analysis

When dealing with most threats, you are likely to encounter some type of malicious software. To understand the real purpose of these malicious programs (they sometimes display different behaviors to fool analysts), you need to have malware analysis skills.

It is important to at least determine what the command and control center of the malicious file is and whether or not there is a device communicating with that address.

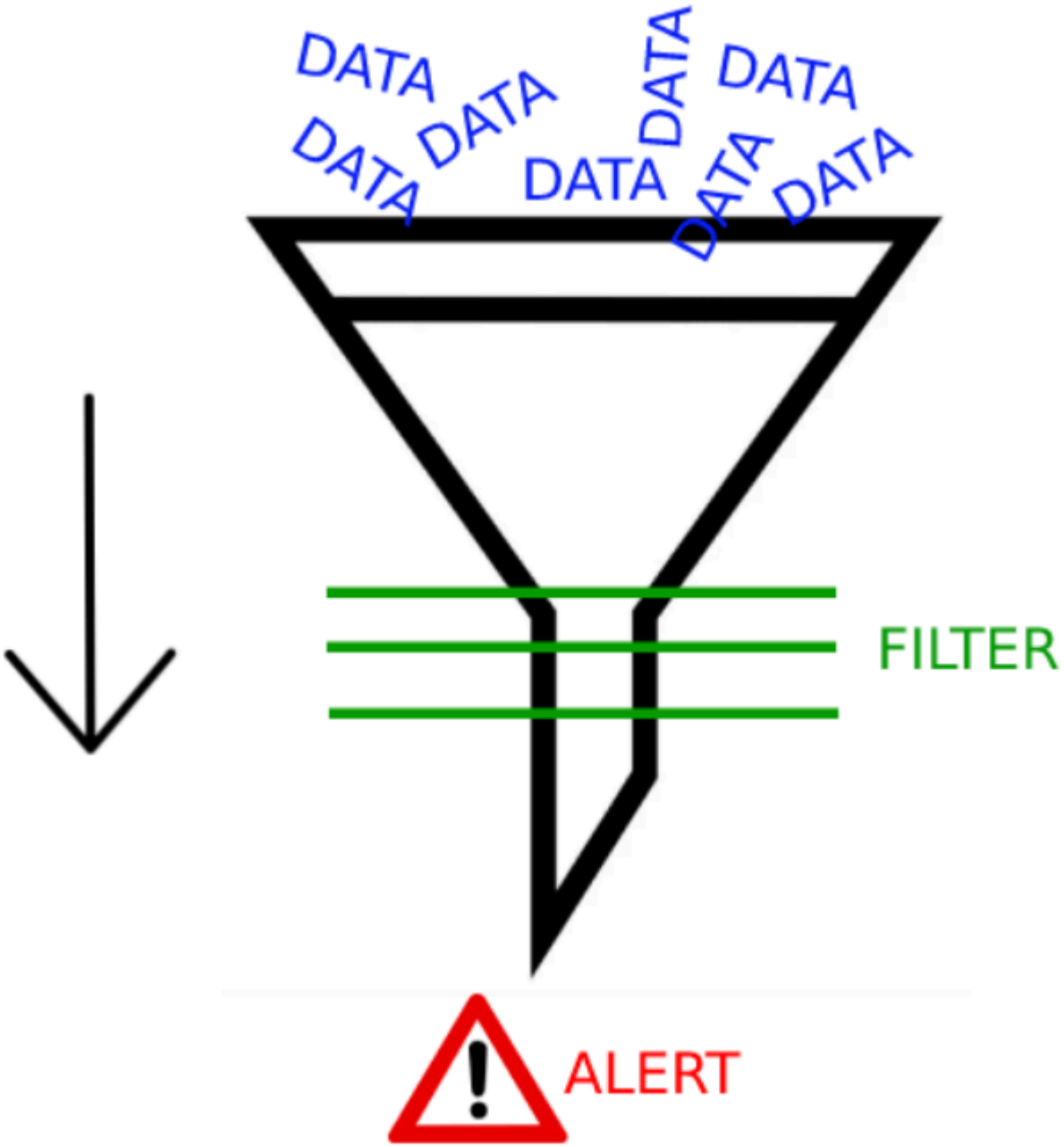
SIEM & Analyst Relationship

SIEM

SIEM is a security solution that combines security information and event management, which involves real-time logging of events in an environment. The ultimate purpose of event logging is to detect security threats.

Overall, SIEM products have a lot of features. The ones that interest us most as SOC analysts are those that collect and filter data and provide alerts for suspicious events.

Example alert: If someone on a Windows operating system tries to enter 20 incorrect passwords in 10 seconds, this is suspicious activity. It is unlikely that someone who has forgotten their password would try to re-enter it that many times in such a short period of time. So we create a SIEM rule/filter to detect such activity that exceeds the threshold. Based on this SIEM rule, an alert will be generated when such a situation occurs.



Some popular SIEM solutions

- IBM QRadar
- ArcSight ESM
- FortiSIEM
- Splunk

Relationship between a SOC analyst & SIEM

Although SIEM solutions have many features, SOC analysts typically only track alerts. There are other groups/people responsible for developing configurations and rule correlations.

As mentioned above, alerts are generated from data that passes through filters. Alerts are first analyzed by a SOC analyst. This is where a SOC analyst's job in the security operations center begins. In essence, they have to determine whether the generated alert is a real threat or a false alert.

Log Management

As a SOC Analyst, you will perform a lot of log analysis. For this reason, it is important to be familiar with "Log Management" systems/solutions. It doesn't matter what product you use, it's about knowing what to look for and where to look for it.

What is Log Management ?

As the name implies, Log Management provides access to all logs in an environment (web logs, OS logs, firewall, proxy, EDR, etc.) and allows you to manage them in one place. This increases efficiency and saves time.

If you can't access the logs from one place, then the same request (e.g., the goal is to determine all users on letsdefend.io) would have to be sent to different devices. This would increase your margin for error and the amount of time you would need to spend.

Purpose of Log Management

SOC analysts use Log Management to check for communication with specific addresses and to view details of that communication. For example:

1. If they find malware communicating with "xyz.io," they can search for "xyz.io" in their logs to see if any devices have communicated with this command & control center.
2. If a SIEM alert shows a device leaking data to IP address 122[.]194[.]229[.]59, they can isolate the device and investigate further. They should also use Log Management to check if other devices are communicating with the suspicious IP, ensuring nothing is missed.

EDR (Endpoint Detection & Response)

A SOC analyst must spend a significant amount of time using EDR when performing analysis on an endpoint device. The following sections discuss why EDR is beneficial to SOC analysts and how to use it effectively.

EDR

Endpoint Detection and Response (EDR) is a security solution that continuously monitors and collects data from endpoints (like computers and devices) in real-time. It uses automated rules to detect and respond to threats. (Source: mcafee.com)

Analysis with EDR

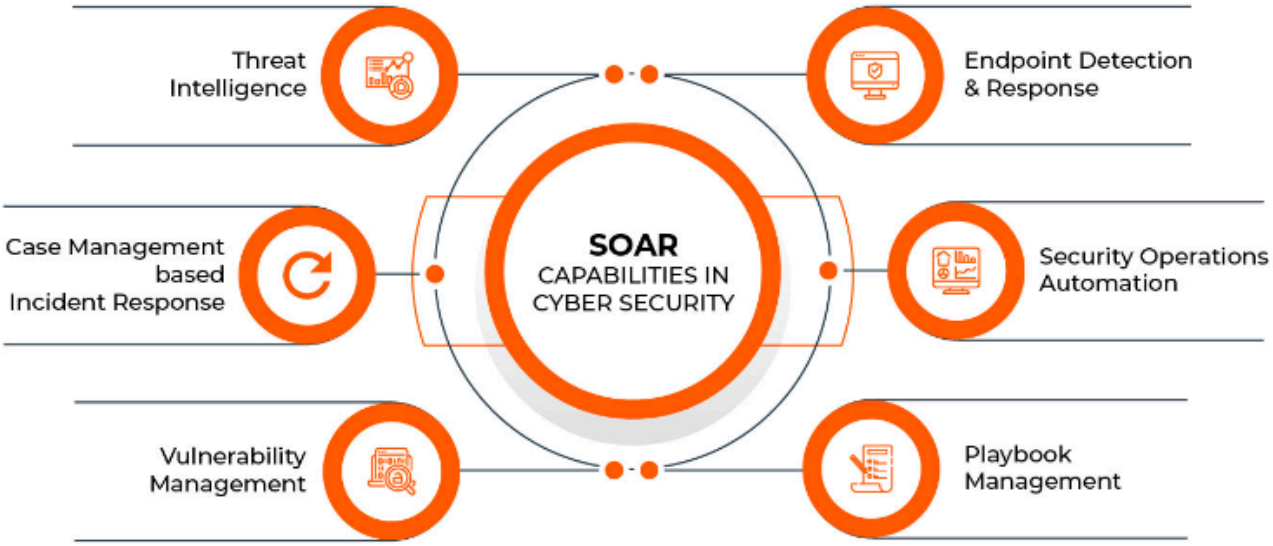
Some EDR solutions commonly used in the workplace: CarbonBlack, SentinelOne, and FireEye HX.

SOAR

SOAR (Security Orchestration, Automation, and Response) helps different security tools work together and automates tasks to make SOC operations more efficient. For example, it can automatically check VirusTotal for details about an IP address in a SIEM alert, saving time for SOC analysts.

Popular SOAR Tools:

- **Splunk Phantom**
- **IBM Resilient**
- **Logsign**
- **Demisto**



Saves you time

SOAR saves time with workflows that automate processes. Some common workflows are:

- IP address reputation control
- Hash query
- Scanning an acquired file in a sandbox environment

Centralization (A single plateform for everything you need)

Playbooks

SOAR allows you to investigate SIEM alerts using predefined **playbooks** that guide you through different scenarios. Even if you forget some steps, you can follow the playbook to perform the analysis correctly.

Playbooks also help ensure consistency among SOC team members. For instance, if checking IP reputation is required, including this step in the playbook ensures everyone follows the same process, avoiding any inconsistencies.

Threat Intelligence Feed

A SOC team should be immediately aware of the latest threats and take the necessary precautions. To meet this need, threat intelligence feeds are created. As a SOC analyst, you can use these feeds to guide your investigations.

A Threat Intelligence Feed is data (such as malware hashes, C2 (Command&Control) domain/IP addresses etc.) provided by a third party company.

Threat intelligence feeds provide data on past malicious activities, such as malware hashes or IP addresses of command and control centers. As a SOC analyst, you use these feeds to check if a specific hash or IP has been involved in previous attacks.

Free and Popular Sources:

- **VirusTotal**
- **Talos Intelligence**

If data you run through feeds does not show up

Let's say you ran a hash of an .exe in VirusTotal and in the past you didn't find anything suspicious about it. In this case, you should not just assume that the file is clean, that would be a mistake. A SOC analyst should carefully perform the necessary file analysis (static/dynamic).

We shouldn't forget that IP addresses can change hands

For example, let's say an attacker created a server on AWS (Amazon Web Services) and used it as a command and control center. Then various threat intelligence feeds listed that IP address as a malicious address.

2 months later, the attacker shut down the server and someone else moved their personal blog to that server. This doesn't mean that people who visited the blog were exposed to malicious content. The fact that this IP address has been used for malicious purposes in the past does not mean that it contains malicious content.

Common mistakes made by SOC analyst

Like everyone else, SOC analysts can make mistakes. In this section, we will discuss common mistakes made by SOC analysts and how to avoid making them yourself.

- Over-reliance on VirusTotal Results
- Hasty Analysis of Malware in a Sandbox
- Inadequate Log Analysis
- Overlooking VirusTotal Dates

Over-reliance on VirusTotal Results

Sometimes we can rely on the result displayed on VirusTotal's green screen after analyzing a file's URL and seeing that the address is harmless. However, there is a new malicious software developed using an AV (AntiVirus) bypass technique that may not be detected by VT (VirusTotal). For this reason, we should accept VirusTotal as a supporting tool and perform our analyses with this in mind.

Hasty analysis of malware in a sandbox

A 3-4 minute analysis in a sandbox environment may not always yield accurate results. Here are the reasons why:

Malware might be able to detect a sandbox environment and will not activate itself.

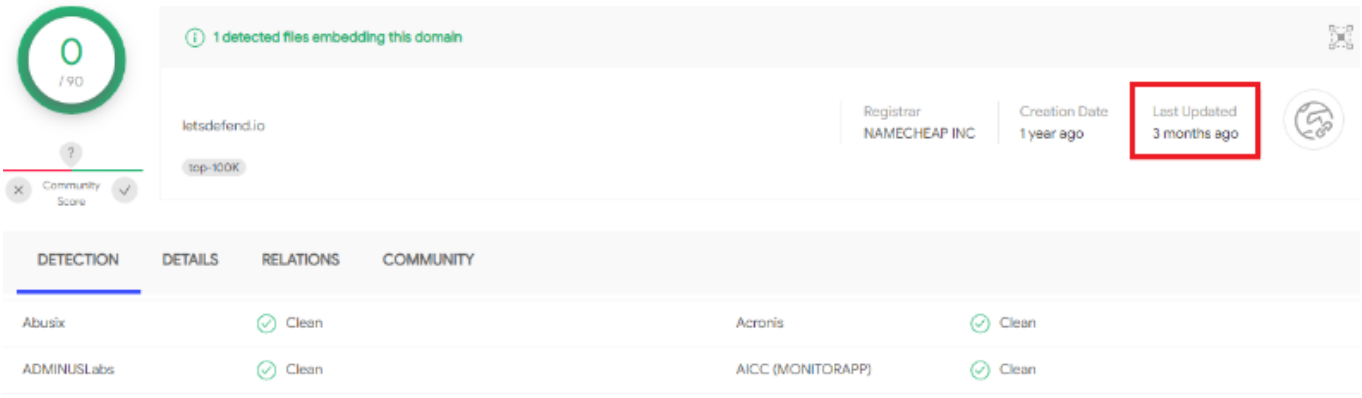
Malware may not become active for 10 to 15 minutes after the operation is performed.

For this reason, the duration of the analysis should be kept as long as possible and it should take place in a real environment, if possible.

Inadequate Log analysis

Occasionally we see that some log analysis is not performed properly. For example, let's say that a piece of malware has been detected on a machine with the hostname "LetsDefend", and that malware is secretly sending data to the address "letsdefend.io". As a SOC analyst, you should use Log Management solutions to determine if any other device is also attempting to connect to this address.

Overlooking VirusTotal Dates



An attacker could simply search a clean URL on VirusTotal and replace it with malicious content. This is why you should not just look at the search cache, but conduct a new search.