SOC Fundamentals (Let’s Defend Course)

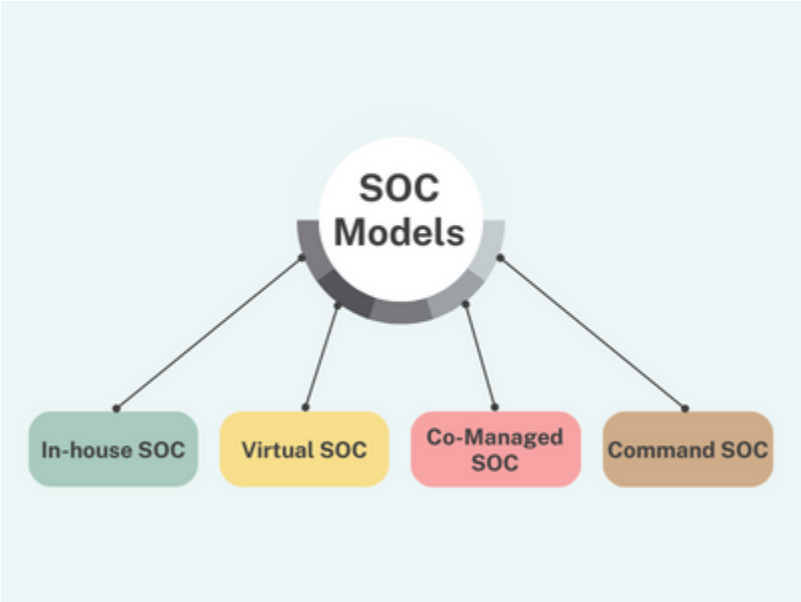
What is a SOC?

A Security Operation Center (SOC) is a facility where the information security team continuously monitors and analyzes the security of an organization.

What is Purpose of SOC ?

The purpose of a Security Operations Center (SOC) is to effectively **detect**, **analyze**, and **respond** to cybersecurity **incidents** by leveraging a combination of **technology**, **skilled personnel**, and established **processes**.

Types of SOC Models :



SOC Model	Description
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.

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

	Description
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.
Process	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.
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 ：

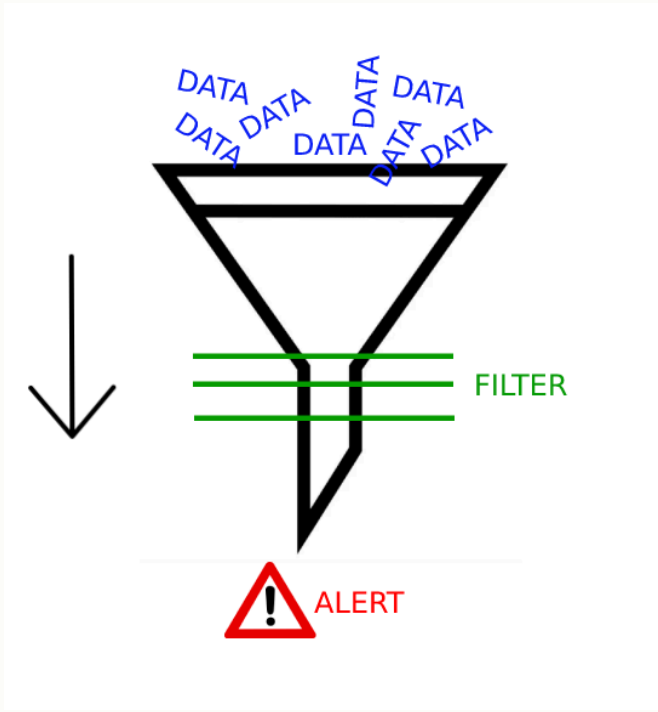
SOC Role	Description
SOC Analyst	This role can be categorized as Level 1, 2, and 3 according to the SOC structure. A security analyst classifies the alert, looks for the cause, and advises on remediation.
Incident Responder	An Incident Response Officer is an individual responsible for threat detection. This role performs the initial assessment of security breaches.
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.
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.

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.

SIEM and Analyst Relationship

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.

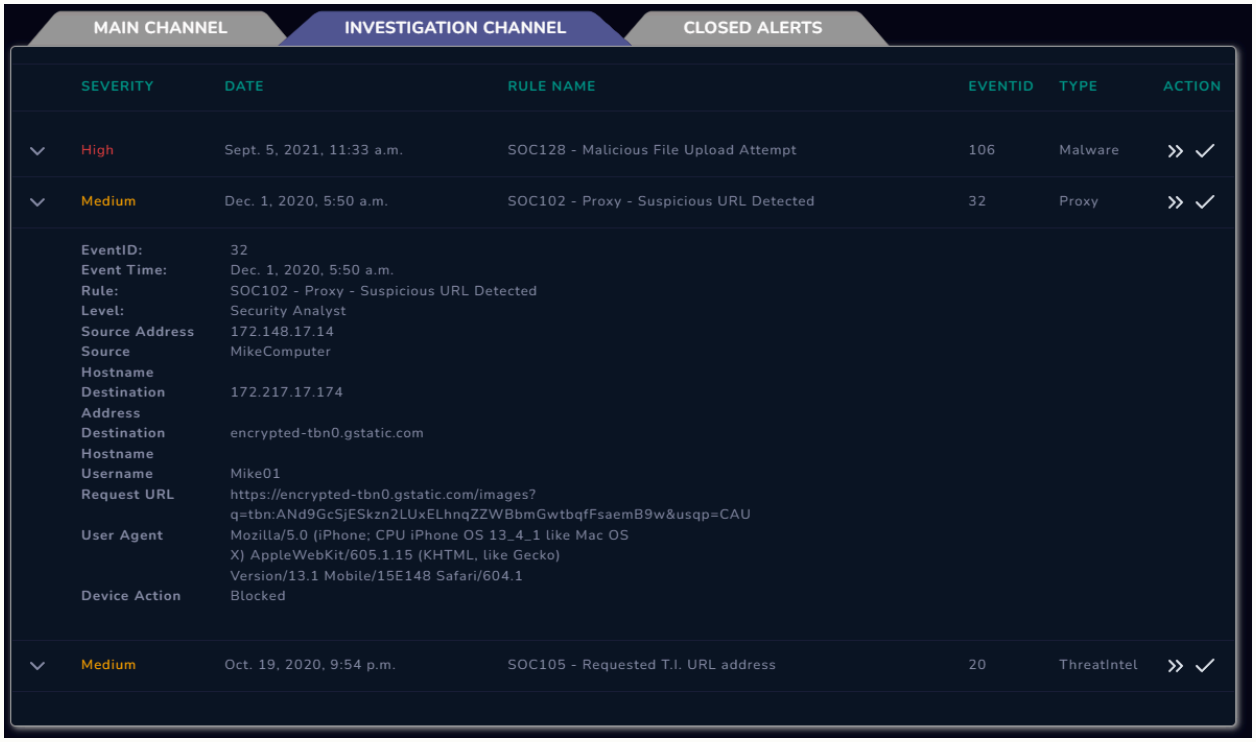


Some popular SIEM solutions: IBM QRadar, ArcSight ESM, FortiSIEM, Splunk, etc.

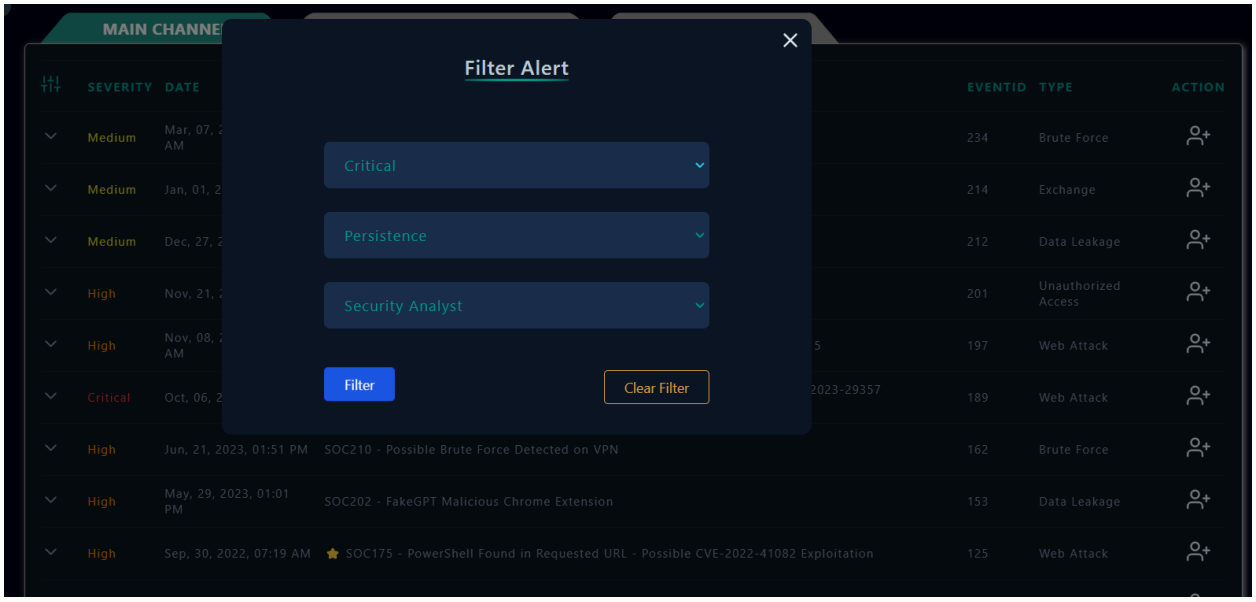
Relationship Between a SOC Analyst and SIEM

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.

For a better understanding, let's go back to the "Monitoring" page; as you can see below, there are various alerts on the SIEM interface. A SOC analyst should analyze the details related to these alerts with the help of other SOC products (such as EDR, Log Management, Threat Intelligence Feed, etc.) and ultimately determine whether they are real threats or not.



You can view newly created alerts in the "Main Channel" and think of this channel as a shared channel. Your teammates are not visible in this simulation, but in a real work scenario, your teammates will be able to see this panel. After you select the alert you want to work on, click the Take Ownership button in the Action area to take ownership of the alert and direct it to the Investigation Channel.



What is Log Management?

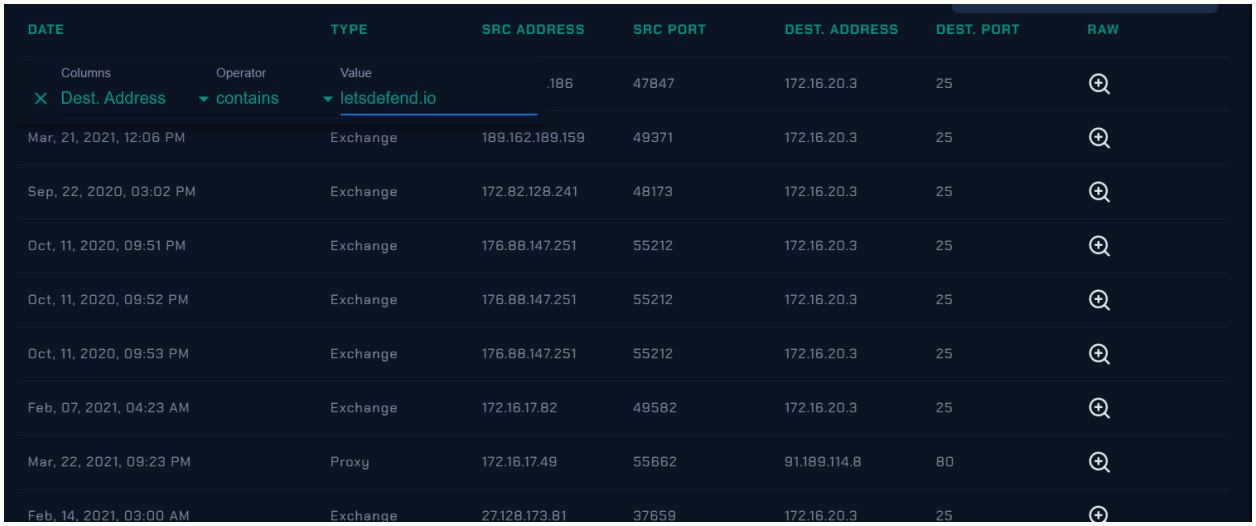
As the name implies, Log Management provides access to all logs in an environment (web logs, OS logs, firewall, proxy, EDR, etc.) and allows you to manage them in one place. This increases efficiency and saves time.

Show Filter

Search

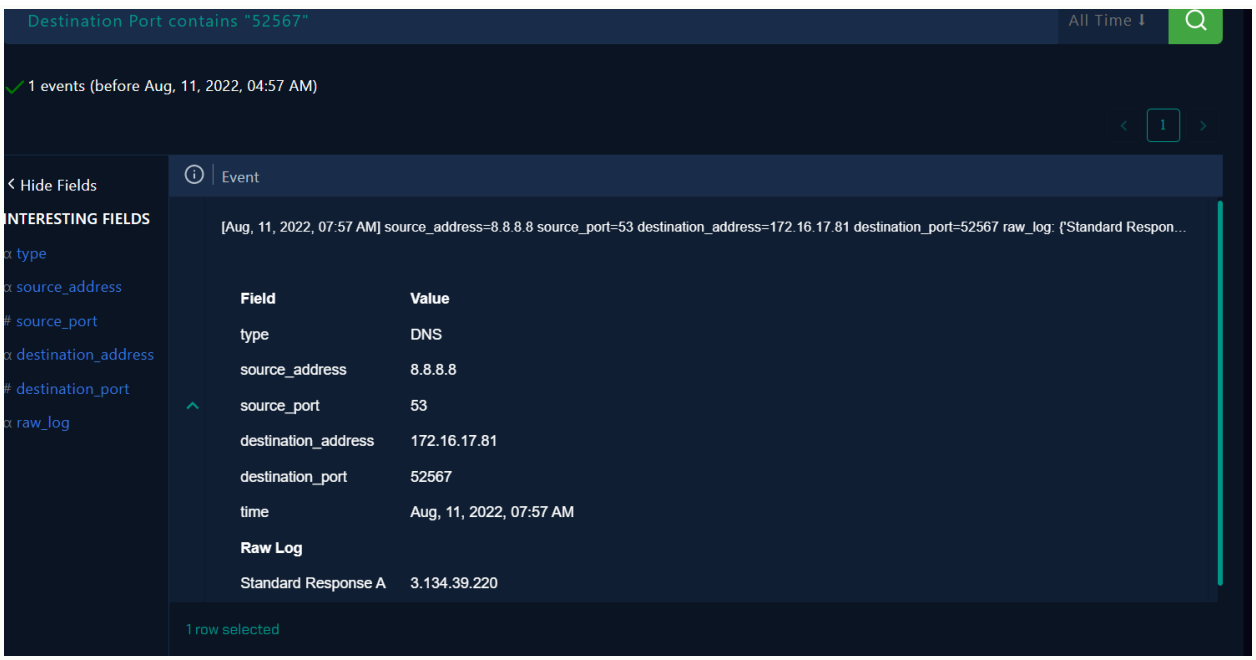
DATE	TYPE	SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
Aug, 29, 2020, 10:28 PM	Proxy	172.16.17.14	47741	198.100.45.154	80	
Aug, 29, 2020, 10:32 PM	Proxy	172.16.17.14	57441	67.68.210.95	80	
Oct, 11, 2020, 09:41 PM	Proxy	172.16.17.47	41221	172.217.17.238	443	
Aug, 29, 2020, 11:00 PM	Exchange	63.35.133.186	47847	172.16.20.3	25	
Aug, 29, 2020, 11:09 PM	Proxy	172.16.17.88	23477	81.169.145.105	80	
Feb, 06, 2021, 12:42 PM	Firewall	172.16.17.34	23512	49.233.160.217	443	
Feb, 06, 2021, 03:40 PM	Firewall	172.16.17.35	56442	172.16.17.45	21	
Feb, 14, 2021, 12:13 PM	Proxy	172.16.17.49	14474	67.68.210.95	80	
Feb, 22, 2021, 04:31 PM	Proxy	49.234.71.65	42212	172.16.20.4	80	
Feb, 21, 2021, 05:02 PM	Proxy	172.16.20.4	80	49.234.71.65	33212	

SOC analysts typically rely on Log Management to determine if there is any communication with a particular address and to view the details of that communication. Let's say you came across a piece of malware and after running it, you found that it was communicating with and executing commands from the "letsdefend.io" address. In this situation, the command&control center is "letsdefend.io", you can search for "letsdefend.io" in your company's log management to see if any devices have attempted to communicate with the command&control center.

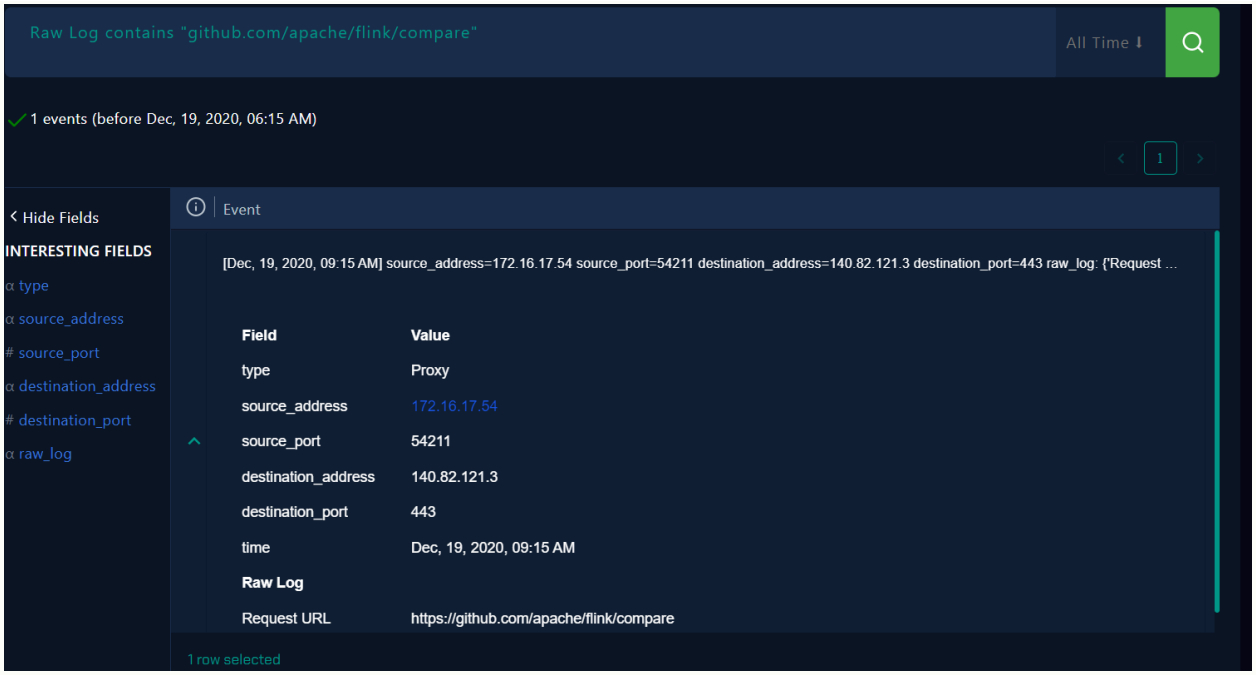


Example :

1. What is the type of log that has a destination port number of 52567?



2. What source IP address entered the URL 'https://github.com/apache/flink/compare'?



EDR - Endpoint Detection and Response :

Endpoint Detection and Response (EDR), also known as Endpoint Threat Detection and Response (ETDR), is an integrated endpoint security solution that combines continuous, real-time monitoring and collection of endpoint data with rules-based automated response and analysis capabilities. (Definition source: mcafee.com)

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

Search Anything...

- Eddie 172.16.17.182
- SSHDevServer01 172.16.17.121
- Shirley 172.16.20.191
- Diya 172.16.17.209
- Hilary 172.16.17.197
- Nathan 172.16.17.152

Endpoint Information

Host Information

Hostname:	SSHDevServer01
Domain:	LetsDefend
IP Address:	172.16.17.121
Bit Level:	64
OS:	Ubuntu 20.04.02
Primary User:	LetsDefend
Client/Server:	Server

Action

Containment:

Remote Access: Go to Lab

Processes 151 | Network Action 22 | Terminal History 16 | Browser History 20 | Results: 10

EVENT TIME	PROCESS ID	PROCESS NAME	PARENT PROCESS	COMMAND LINE
Apr 4 2024 09:55:19	2864	svchost.exe	services.exe	C:\Windows\s...
Apr 4 2024 09:55:27	928	services.exe	wininit.exe	C:\Windows\s...
Apr 4 2024 09:56:00	720	GoogleUpdate...	GoogleUpdate...	"C:\Program F...
Apr 4 2024 09:56:01	6360	123.0.6312.88_...	GoogleUpdate...	"C:\Program F...
Apr 4 2024 09:56:03	1092	setup.exe	123.0.6312.88_...	"C:\Program F...

Processes 151 | Network Action 22 | Terminal History 16 | Browser History 20 | Results: 10

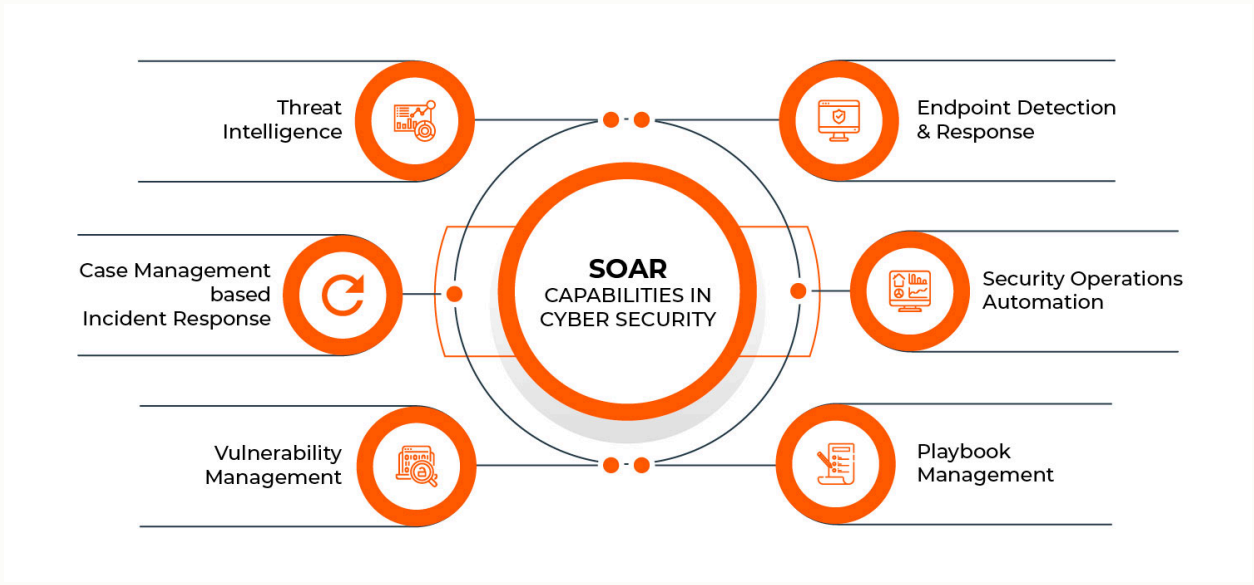
EVENT TIME	DESTINATION DOMAIN/IP ADDRESS
Apr 4 2024 09:54:58	52.142.223.178
Apr 4 2024 09:55:27	142.250.190.131
Apr 4 2024 09:56:23	52.111.236.26
Apr 4 2024 09:56:27	172.31.17.132
Apr 4 2024 09:56:35	142.250.190.131

Processes 151 | Network Action 22 | Terminal History 16 | Browser History 20 | Results: 10

EVENT TIME	COMMAND LINE
Apr 4 2024 09:58:56	whoami
Apr 4 2024 09:59:02	whoami /groups
Apr 4 2024 09:59:28	cd C:\Windows\System32\config
Apr 4 2024 09:59:44	Get-Content .\SavedConfigHash.txt
Apr 4 2024 09:59:59	cd C:\Users\LetsDefend\AppData\Roaming\Microsoft\Windows\PowerShell\PSReadLine\

SOAR (Security Orchestration Automation and Response)

SOAR stands for Security Orchestration Automation and Response. It enables security products and tools in an environment to work together, streamlining the tasks of SOC team members. For example, it will automatically search VirusTotal for the source IP of a SIEM alert, reducing the workload of the SOC analyst.



Centralization (A single platform for everything you need)

It allows you to use different security tools in your environment (sandbox, log management, 3rd party tools, etc.) by providing an all-in-one software. These tools are integrated into the SOAR solution and can be used on the same platform.

1. **Playbooks**

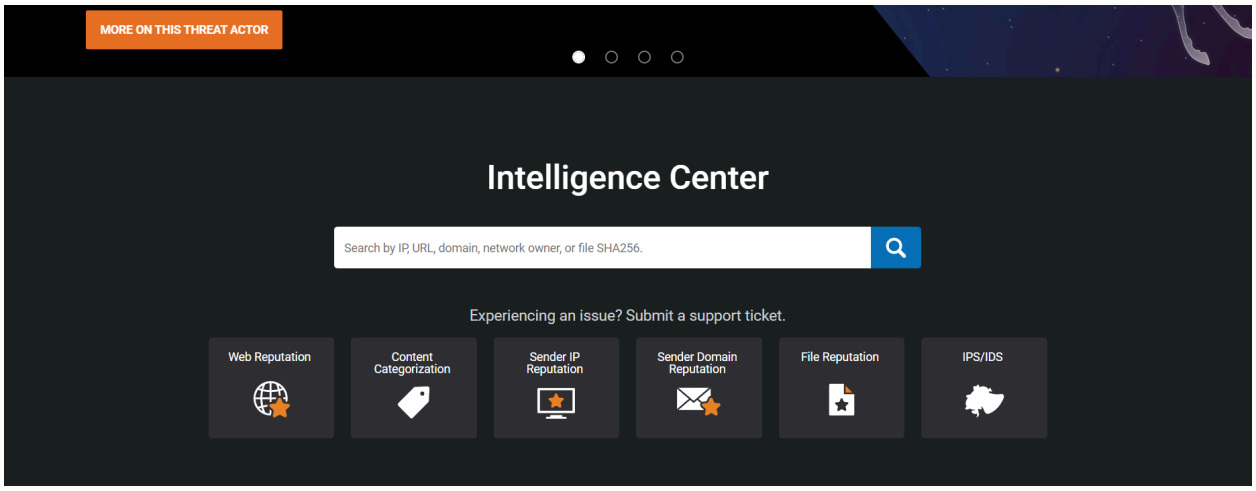
You can easily investigate SIEM alerts using playbooks created for different scenarios within SOAR. Even if you don't know or remember all the procedures, you can perform an analysis by following the steps outlined in the playbooks

2. **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.

The data here consists of artifacts from previous malicious activity. It could be the hash of malware or the IP address of a command and control center. As a SOC analyst, you need to search threat intelligence feeds to determine if a hash file at hand has ever been used in a malicious scenario in the past.

Here are some free and popular sources you can use:
1.https://talosintelligence.com/
2. https://www.virustotal.com



What is the data source of the "e1def6e8ab4b5bcb650037df234e2973" hash on the threat intel page?