

SOC Fundamentals (Let's Defend Course)

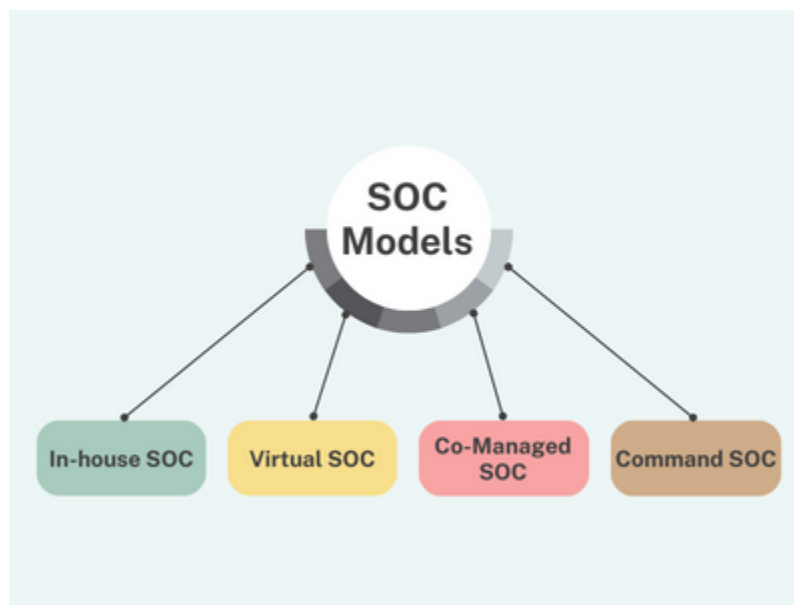
What is a SOC?

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 SOC's 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.

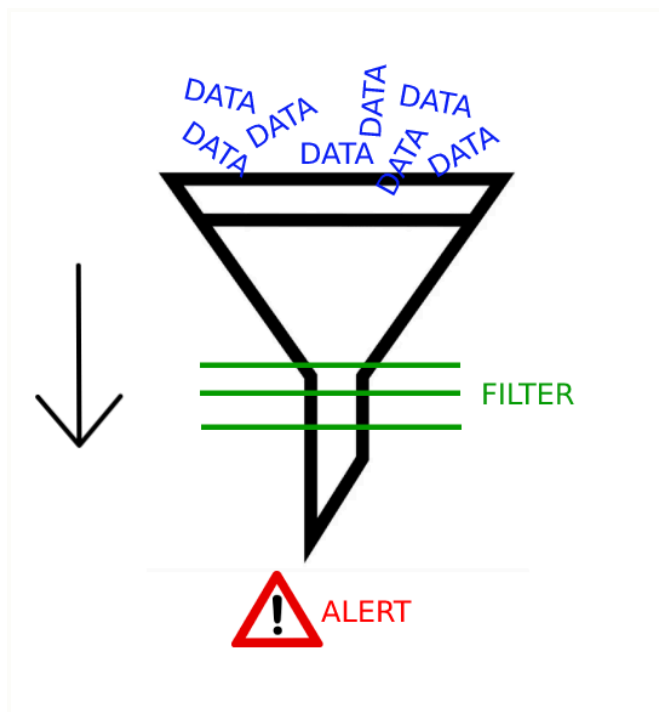
SOC Manager	A SOC manager takes on management responsibilities such as budgeting, strategizing, managing staff, and coordinating operations. They deal with operational rather than technical issues.
-------------	---

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.

MAIN CHANNEL		INVESTIGATION CHANNEL		CLOSED ALERTS		
SEVERITY	DATE	RULE NAME		EVENTID	TYPE	ACTION
▼ High	Sept. 5, 2021, 12:43 p.m.	★ SOC153 - Suspicious Powershell Script Executed		101	Malware	🔍+
▼ High	Sept. 4, 2021, 8:08 p.m.	SOC155 - Suspicious SSH Login		104	Unauthorized Access	🔍+
▼ Medium	Sept. 4, 2021, 3:07 p.m.	SOC157 - Suspicious WAR File		107	Malware	🔍+
▼ Medium	Sept. 4, 2021, 2:30 p.m.	SOC154 - Service Configuration File Changed by Non Admin User		102	Generic	🔍+

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.

MAIN CHANNEL

INVESTIGATION CHANNEL

CLOSED ALERTS

SEVERITY	DATE	RULE NAME	EVENTID	TYPE	ACTION
<div>▼</div> High	Sept. 5, 2021, 11:33 a.m.	SOC128 - Malicious File Upload Attempt	106	Malware	» ✓
<div>▼</div> Medium	Dec. 1, 2020, 5:50 a.m.	SOC102 - Proxy - Suspicious URL Detected	32	Proxy	» ✓
<div><div>EventID:</div><div>32</div></div> <div><div>Event Time:</div><div>Dec. 1, 2020, 5:50 a.m.</div></div> <div><div>Rule:</div><div>SOC102 - Proxy - Suspicious URL Detected</div></div> <div><div>Level:</div><div>Security Analyst</div></div> <div><div>Source Address</div><div>172.148.17.14</div></div> <div><div>Source</div><div>MikeComputer</div></div> <div><div>Hostname</div><div></div></div> <div><div>Destination</div><div>172.217.17.174</div></div> <div><div>Address</div><div></div></div> <div><div>Destination</div><div>encrypted-tbn0.gstatic.com</div></div> <div><div>Hostname</div><div></div></div> <div><div>Username</div><div>Mike01</div></div> <div><div>Request URL</div><div>https://encrypted-tbn0.gstatic.com/images?q=tbn:ANd9GcSjESkzn2LUxELhnqZZWBbmGwtbqfFsaemB9w8usqp=CAU</div></div> <div><div>User Agent</div><div>Mozilla/5.0 (iPhone; CPU iPhone OS 13_4_1 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/13.1 Mobile/15E148 Safari/604.1</div></div> <div><div>Device Action</div><div>Blocked</div></div>					
<div>▼</div> Medium	Oct. 19, 2020, 9:54 p.m.	SOC105 - Requested T.I. URL address	20	ThreatIntel	» ✓

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.

MAIN CHANNEL

SEVERITY

DATE

▼

Medium

Mar, 07, 2023 11:33 AM

▼

Medium

Jan, 01, 2023 11:33 AM

▼

Medium

Dec, 27, 2022 11:33 AM

▼

High

Nov, 21, 2022 11:33 AM

▼

High

Nov, 08, 2022 11:33 AM

▼

Critical

Oct, 06, 2022 11:33 AM

▼

High

Jun, 21, 2023, 01:51 PM

▼

High

May, 29, 2023, 01:01 PM

▼

High

Sep, 30, 2022, 07:19 AM

SOC210 - Possible Brute Force Detected on VPN

SOC202 - FakeGPT Malicious Chrome Extension

★ SOC175 - PowerShell Found in Requested URL - Possible CVE-2022-41082 Exploitation

Filter Alert

Critical

Persistence

Security Analyst

Filter

Clear Filter

EVENTID

TYPE

ACTION

234

Brute Force

+

214

Exchange

+

212

Data Leakage

+

201

Unauthorized Access

+

197

Web Attack

+

2023-29357

Web Attack

+

189

Web Attack

+

162

Brute Force

+

153

Data Leakage

+

125

Web Attack

+

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.

DATE	TYPE		SRC ADDRESS	SRC PORT	DEST. ADDRESS	DEST. PORT	RAW
<div>Columns</div> <div>X Dest. Address</div>	<div>Operator</div> <div>▼ contains</div>	<div>Value</div> <div>▼ letsdefend.io</div>	.186	47847	172.16.20.3	25	
Mar, 21, 2021, 12:06 PM	Exchange	189.162.189.159	49371	172.16.20.3	25		
Sep, 22, 2020, 03:02 PM	Exchange	172.82.128.241	48173	172.16.20.3	25		
Oct, 11, 2020, 09:51 PM	Exchange	176.88.147.251	55212	172.16.20.3	25		
Oct, 11, 2020, 09:52 PM	Exchange	176.88.147.251	55212	172.16.20.3	25		
Oct, 11, 2020, 09:53 PM	Exchange	176.88.147.251	55212	172.16.20.3	25		
Feb, 07, 2021, 04:23 AM	Exchange	172.16.17.82	49582	172.16.20.3	25		
Mar, 22, 2021, 09:23 PM	Proxy	172.16.17.49	55662	91.189.114.8	80		
Feb, 14, 2021, 03:00 AM	Exchange	27.128.173.81	37658	172.16.20.3	25		

Example :

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

Destination Port contains "52567"
All Time
🔍

✓ 1 events (before Aug, 11, 2022, 04:57 AM)
< 1 >

< Hide Fields
INTERESTING FIELDS
type
source_address
source_port
destination_address
destination_port
raw_log

Event
[Aug, 11, 2022, 07:57 AM] source_address=8.8.8.8 source_port=53 destination_address=172.16.17.81 destination_port=52567 raw_log: {Standard Respon...

Field	Value
type	DNS
source_address	8.8.8.8
source_port	53
destination_address	172.16.17.81
destination_port	52567
time	Aug, 11, 2022, 07:57 AM
Raw Log	
Standard Response A	3.134.39.220

1 row selected

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

The screenshot shows a network log viewer interface. At the top, a search bar contains the text "Raw Log contains 'github.com/apache/flink/compare'". Below the search bar, it indicates "1 events (before Dec, 19, 2020, 06:15 AM)". The main area displays a single event with the following details:

Field	Value
type	Proxy
source_address	172.16.17.54
source_port	54211
destination_address	140.82.121.3
destination_port	443
time	Dec, 19, 2020, 09:15 AM
Raw Log	
Request URL	https://github.com/apache/flink/compare

On the left side, there is a sidebar with "INTERESTING FIELDS" and a list of fields: type, source_address, source_port, destination_address, destination_port, and raw_log. At the bottom, it says "1 row selected".

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\PSRead Line\			

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

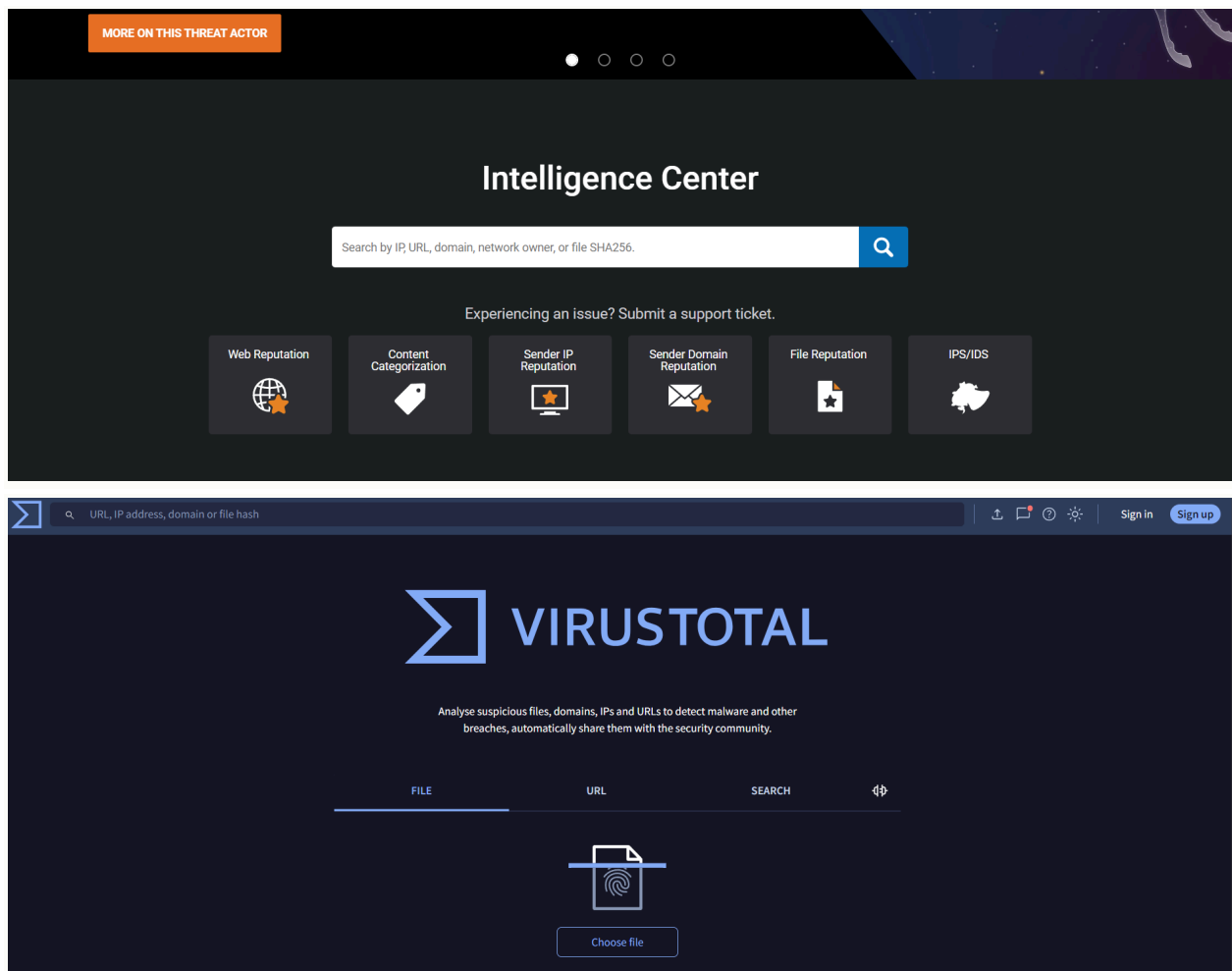
A SOC team should be immediately aware of the latest threats and take the necessary precautions. To meet this need, threat intelligence feeds are created. As a SOC analyst, you can use these feeds to guide your investigations.

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?

52631
URL

2616
IP

359
Hash

535
Domain

Select Filters...Clear

Free text search

e1def6e8ab4b5bcb65

Date range

Select Date

Search by data type

Select

Search by data

Search

Search by tag

Search

Search

Minimize ^

DATE	DATA TYPE	DATA	TAG	DATA SOURCE
Oct, 11, 2020, 09:24 PM	Hash	e1def6e8ab4b5bcb650037df234e2973	malware	AbuseCH