SOC Analyst Learning Path BY P3NGU1N

SOC Fundamentals

what is soc?

Security Operations Center is a facility information security team

- monitors
- analyze

security of an organization

primary purpose of soc

- detect
- analyze
- respond of CYS incidents

using

- technology
- people
- processes

Types of SOC Models:

- depending on NEEDS and Budget
- In-House SOC:
- within an organization
- present at site
- costly
- time consuming
- company needs its own employees for SOC team

Virtual SOC:

- operates remotely
- not present on site
- cloud based solution
- cost effective no infrastructure and man power needed within organization

Co-Managed SOC:

- consists of internal SOC team and external MMSP (managed security service provider)SOC team
- organization can keep sensitive matters in house while outsource other
- less expensive than in house
- proper coordination between teams is required
- flexibility and scalability to organization

Command SOC:

- High level SOC Model
- multiple SOC teams at multiple locations, all coordinate
- in larger organizations which are spread across globally
- Each team is Dedicated to specific tasks
- In this case everything is double checked
- quite expensive

People, Process, and Technology

their coordination is a requirement of SOC

People

- highly skilled and trained people
- familiar with attack scenarios

- willing to conduct research

Processes

- security requirements
- standardizations to ensure nothing is left while conducting research

Technology

- tools
- how to improve tools using advanced technologies to make organizations SOC work better
- finding the product that best fits for ur team

SOC Roles

SOC Analyst

- monitors
- analyzes
- responds
- classifies alert, look for cause

Incident Responder

- performs threat detection
- initial assessment of security breach

Threat Hunter

- finds potential threats and vulnerabilities
- apply mitigations to improve security
- full understanding of security posture of organization
- knowledge of emerging threats

- eliminate threats which can damage organizations infrastructure

Security Engineer

- maintenance of SIEM solution and SOC products
- builds, manages ,maintains ,updates SOAR **Security Orchestration, Automation, and Response products**

SOC Manager

- management responsibilities
- budgeting
- managing
- coordination between teams
- reporting
- more operational tasks then technical
- technical stuff is more related to a SOC Anlayst

SOC Analyst and Their Responsibilities

- first person to responds to & investigate threats
- need to inspect what situation demands

skills & abilities

Operating Systems:

- understanding of normal and abnormal operations and processes happening
- both in linux and windows
- knowledge of normal working is important

Networking:

- In order to analyze malicious URLs and IPs to see where its tryna connect
- to be able to find a potential leak

Malware Analysis

- In order to understand the behavior of malicious software u might encounter
- to be able to determine C2 channel

SIEM and SOC Analyst Relationship

What is SIEM?

- security information and event management
- real time logging of events
- ultimate purpose of event logging is detect security incident
- we make rules for activities happening beyond threshold
- whatever happening will pass through that filter/rule
- if the rule is triggered alert will be generated

SIEM SOLUTIONS: IBM QRadar, FortiSIEM, SPLUNK

Relationship between SOC Analyst and SIEM

SIEM	SOC ANALYST
rules are triggered → which generates alerts	→alerts are monitored → analyzed to see if real or false alert

🎯 QUESTION:

When you close an alert, which channel(tab on the monitoring page) can you access it from?

ANSWER: closed alerts

Log Management:

- where there are alerts ,there will be logs
- what to look for, where to look for in logs
- how logs should be used effectively by SOC Analysts

what is log management

- all types of logs in one place
- type: web logs, OS logs, firewall, proxy, EDR

Purpose of Log Management:

- determine any communication with a particular address and to view details of that communication.
- to find c2 channels and servers
- if u find sus activity on 1 host
- there might be other hosts which are affected
- In logs you'll be able to find any other alerts from any other host communicating to the same c2 channel

🎯 QUESTION:

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

ANSWER: 172.16.17.54

🎯 QUESTION:

What is the type of log that has a destination port number of 52567 and a source IP address of 8.8.8.8?

ANSWER: dns

EDR - Endpoint Detection and Response

What is an EDR?

- Endpoint detection and response EDR
- Endpoint Threat Detection and response ETDR
- is a endpoint security solution

combines:

- continuous monitoring
- collection of endpoint data
- rule based automated response
- analysis capabilities

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

Analysis with EDR

list of edr are given you can also search from them

we can see details like:

- browser history
- command history
- process list
- network connections
- we can also do live investigations by connecting with it and containment

🎯 QUESTION:

What is the type of log that has a destination port number of 52567 and a source IP address of 8.8.8.8?

ANSWER: EricProd

🎯 QUESTION:

A "Ps1.hta" file was executed on a device with the hostname "Roberto". What is the complete CMD command?

ANSWER: C:/Windows/System32/mshta.exe C:/Users/roberto/Desktop/Ps1.hta

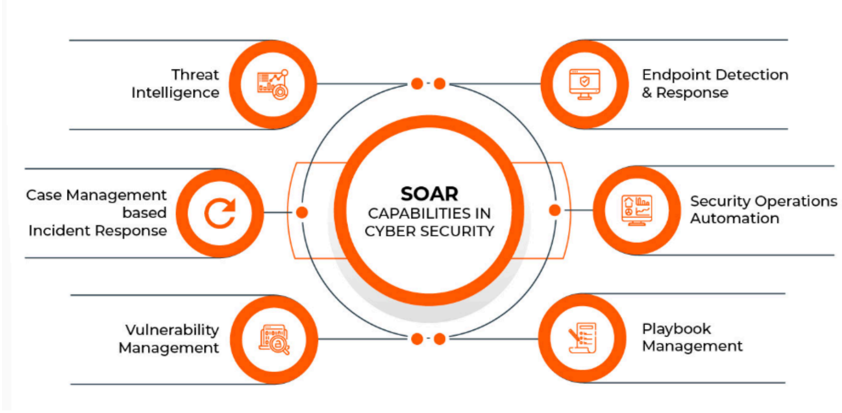
---

SOAR (Security Orchestration Automation & Response)

enables security products and tools in an environment to work together

Some SOAR products commonly used in the industry:

- Splunk Phantom
- IBM Resilient
- Logsign
- Demisto

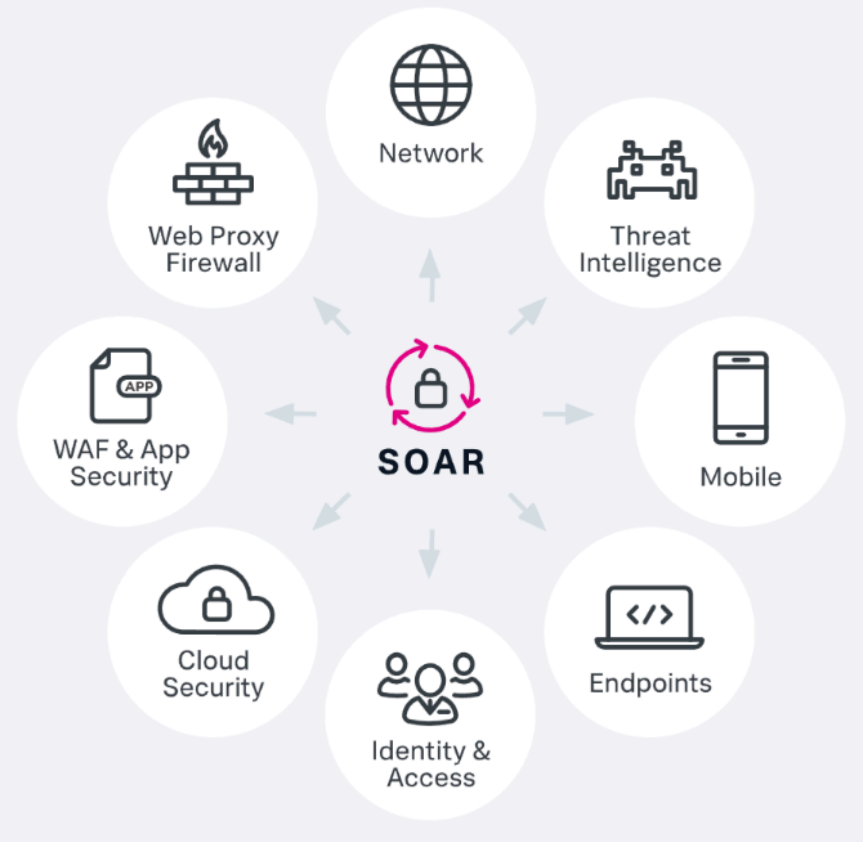

Threat Intelligence
Endpoint Detection & Response
Case Management based Incident Response
SOAR
CAPABILITIES IN CYBER SECURITY
Security Operations Automation
Vulnerability Management
Playbook Management

shows what can be achieved with SOAR solution

- SOAR automates processes
- saves time
- all in one software

how?

- ip address reputation control
- scanning file in sandbox
- hash query



all in one software

Threat Intelligence Feed

- SOC team should be immediately aware of the latest threats
- take the necessary precautions
- could be the hash of malware or the IP address of a command and control center
- 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:

- VirusTotal
- Talos Intelligence

If data you run through feeds does not show up

- if u find nothing suspicious about a file or ip

- doesn’t mean u should think its safe as a SOC Analyst

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.

🎯 QUESTION:

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

ANSWER: AbuseCH

Common Mistakes made by SOC Analysts

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

CYBER KILL CHAIN