**IMP Notes from Docuements Read**

**Docuement 1 - A systematic method for measuring the performance of Cyber security Operations Analyst**

This study article focus on performance of SOC Analyst based on their key functions Each of the function has associated KPIs.

# **Traditional model:-**

Traditional performance evaluation matrics involved to find out number of incidents processed by an analyst at the end of their shift to assess their performance.

# **Key Functions of Soc Anayst:-**

Monitoring and Threat Detection

Resonse and Reporting

Baseline and Vulnerability Function

Intelligence Function

Plolices and signatures management functions

# **Delphi Method -Input to collect opinion from SOC experts:-**

To establish the New model author used combination of Delphi Method and SOC-AMM Method

1. Delphi Method - used to collect opinion among soc experts

Questions considering while taking input for the survey are ‘who’ (attacker/malicious person), ‘what’ (indicators of compromise/actions done), ‘where’ (from what IP address), ‘when’ (timestamp), ‘why’ (the risk), ‘how’ (method of detection) and provide recommendations on the actions taken to address the identified incident.

# **SOC-AMM method :-**

The SOC-AAM contains two special KPIs (the quality of analysis and the quality of incident report) that must be scored by only a SOC manager or the technical lead, as part of the evaluation process.

The steps for evaluating analysts’ performance are outlined below:

• Step 1: The evaluator enters the total number of analysts in the team into the SOC-AAM tool. This will calculate the maximum team score for the quality of analysis and the quality of their

report. (Note: Each analyst can achieve only a maximum score of 7 for the quality of their analysis and 7 for the quality of their report, based on the seven indicators as stated earlier; the

overall team score is, therefore 7, multiplied by the number of analysts for each of the two functions);

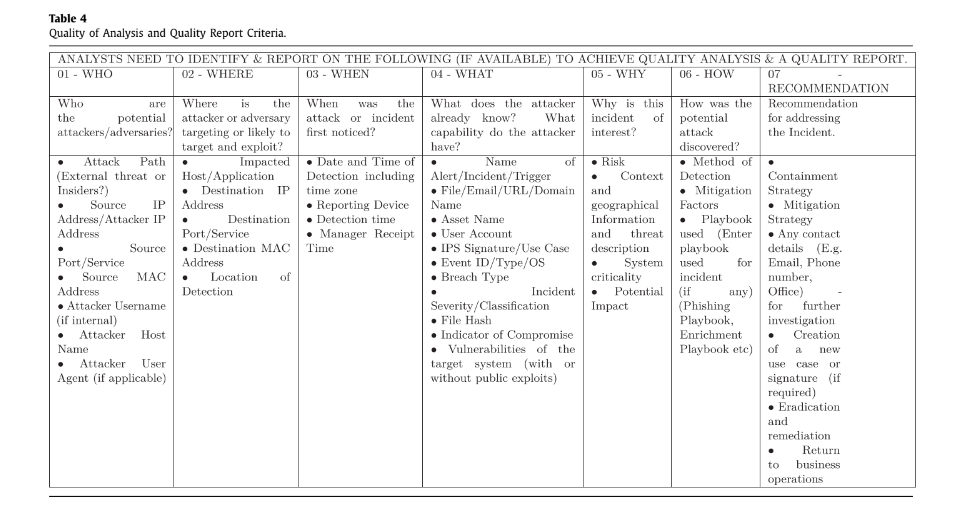
• Step 2: If an analyst has written a report over the assessment period, the SOC manager or the technical lead must review the report and assign a score between 1 and 7 for the quality of

report. The manager would also assign a score for the quality of analysis as explained above

Step 3: The evaluator must enter the scores for the remaining functions. Once the evaluator has entered all the scores, the SOC-AAM tool will automatically calculate an analyst’s overall

performance score

• Step 4: To allow a comparative assessment of an analyst’s performance against their peers, the team’s total scores for each function must be entered for the period.



**Docuement 2 -**

**Docuement 3 - SANS Institute Common Best Practices for SOC , SOC survey result**

Aim of the survey was to investigate the current barriers in effectiveness of SOC performance and define some common and best practices, provide defendable metrics that can be used to justify SOC resources to management,

# **Identified Barriers in Implemention of SOC:-**

* barriers to excellence: lack of skilled staff (58%) followed by absence of effective orchestration and automation (50%)
* assets are monitored by the SOC (and which are not) is typically based on resource constraints. Because organizations cannot defend everything, it is interesting to see when organizations choose to leave assets exposed or less protected.Leaving smart systems unprotected is common practice
* SOCs struggle to monitor and track current assets. Having an accurate inventory of all endpoints and users in a network can be a challenge.
* SOC team depedends upon CMDB database to be more accurate . It seens that its rarely updated
* Increased user of IaaS in SOC createdblind spots for traditional network scanning approaches,
* Little alignment of SOC team with IT operation team.
* Hiring skilled SOC Analayst
* Unplanned outage in cloud based SOC service .
* Used of AI technology in SOC , somewhere how its contributing to increase frequent false positives, requiring high levels of involvement by knowledgeable and skilled analysts.

# **Some of the improvements suggested are :--**

* Define the outsourcing strategy if needed for SOC
* Define the architecture for your soc
* Address the data protection laws
* Articulate services to the business.
* Build use cases.
* Retain staff through training and growth.
* Use external managed security service providers (MSSPs) strategically to bolster weakness.
* Closely coordinate with NOC/IT.
* Check your technology. If you’re dissatisfied in a technology or category where most other respondents are satisfied, you’re either using the technology incorrectly, or your technology selection methods have led you to choose the wrong product.
* If you’re a tool vendor or developer and are looking for a less crowded area of the market, seek ways to help your customers develop remediation.
* Have a way to verify the integrity of your data, or to recover data if it is lost from any sort of incident, including ransomware.
* Indefiy the weak area and found out about how to improve your SOC performance. Improve measurement methodology for “incident avoidability” and “losses prevented vs. losses accrued. Work to further automate data collection and metric calculations.

# **Article defines key SOC capabilities**

1. **Outsourced Capabilities**

To minimise the cost some of the functionality of soc can be outsourced.The most commonly outsourced actions continue to be pen testing (and its permutations of red-teaming and purple-teaming), digital forensics and threat

intelligence.

1. **Incident Handling**

Investigate the root cause of the issue and conduct the preliminary containment actions

1. **Knowledge Management**

Used to document process-related knowledge across the team and support both repeatability of operations and the ability to quickly bring on new analysts.Depending on the size of the organization. Large SOC uses JIRA,ServiceNow,BMC Remedy

1. **MSSP**

Develop your system for capturing tribal lore into documented internal guidance for new

and seasoned staff.

# **Identification Of Tools/Technology**

**Detection Tools - Network based and Host based detection tools**

earlier, when asset inventory accuracy levels are low, network-based tools are more effective

host-based tools that depend on agents being present on every endpoint.

**Log management Tools-** SIEM tools use to collect the event logs

**Protection Tools -** use Data Lost prevention technique

# **SOC Matrix**

Most people rely on the SIEM to merge event data with other security-related data. SIEM-

based correlation of event data is one source of SOC metrics, but respondents report low levels of satisfaction with the area of the technology.it can be easily count the items logged, and this is where most people stop with this metrics.

That a quantity-based metric such as the “number of incidents handled” is the most common response is not at all surprising: It’s easy to count; it’s easy to extract this data in an automated fashion; and it’s an easy way to proclaim

almost all organizations are increasing their ability to provide accurate time-based metrics. SIEM and log data are useful to identify the volume of events over time spans of months.

**Docuement 4 - CyOps1.1\_Chp01.pdf**

Nothing more important than rest documents

**Docuement 5 - Security Operatiion Center Case Study**

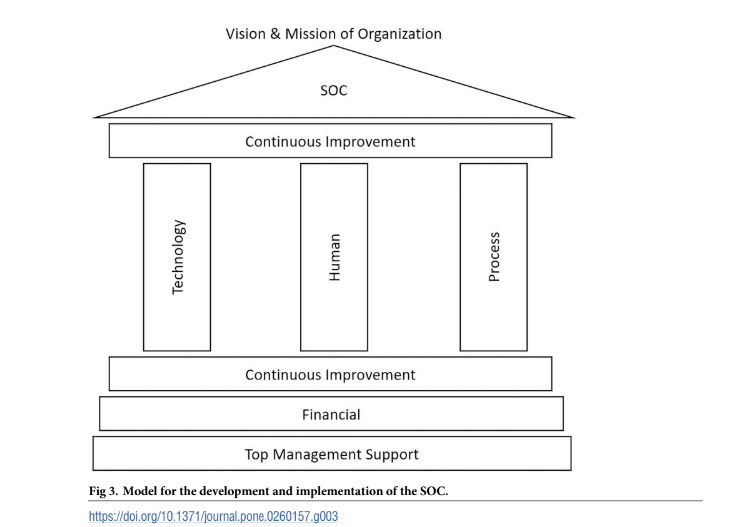
Not so much information to note down as it has basic which is covered by other articles

**Docuement 6 - Model for the successful development and implementation of the SOC**

This document tells about a successful model that can be use to establish the SOC team in the organization. It also tell us about the survey that happen and results into the critifcal factors for the any SOC team .

critical factors in terms of the human ,Technology and and Process for successfully SOC .Along with that as secondary factors - factors, with top management support, financial, and continuous improvement. Relevant organizations or agencies can use the model to develop and implement SOCs, formulate policies and guidelines, strengthen human models, and enhance cyber security.

# **SOC Model**



## **Top Management Support**

It Has hughes mean value all among the others and support the critical components of SOC .Top management support is crucial in governance, where it can set clear directions, set priorities, and formulate longterm strategies for SOC implementation.

The top management support is located at the lowest base because this factor is

described as the source of authority for the organization. Thus, the development and implementation of SOC can be supported through the direction and mandate from top management.

Upon approval from the top management, financial allocation can be utilised to support

the success of the SOC.

## **Finacial**

Financial factor is also considered because it plays a crucial role in ensuring that all other factors can be implemented. The development and implementation of SOC is closely linked to the financial ability of the organization.

## **Continuous Improvement**

Continuous improvement is considered vital because this factor ensures that the current SOC remains relevant over time.

It ensures that the SOC is up-to-date with recent trends in cyberattacks and technology. It is placed above and below the main components (human, process, and technology) to highlight that they are continually improving to ensure that the SOC remains relevant to the recent cyber security development.

## **Technology**

In the success of SOC is due to the process and technology factors, as according to survey result . It encourages the organization to be equipped with the latest and appropriate technology to protect security postures.

Thus, with proper tools and technologies, skillful employees can effectively understand the organization’s technical environment and solve incidents.

Automation in current operation is required to improve the operation efficiency.

Use of the technologies in SOC are needed for (1) monitoring and log collection, (2) analysis, (3) incident management and response, (4) forensic, (5) cyber threat intelligence, and (6) fundamental cybersecurity operational management.

1. **Human**

It will be consider as the least significant in human-process-technology factors in supporting the success of SOC. Hence, the human factor is placed in the center

between the technology and process. In the absence of a human factor, the SOC structure (roof) remains strong as the support comes from technology and process.

SOC personnel must outsmart malicious attackers, determine suspicious activities, and solve cyber incidents when they occur.highly qualified employees in cyber security,

especially in log analysis.

Outlines the need to have a positive attitude and natural curiosity among the SOC’s employees to keep them informed about the new cyberattacks trend as it continues to evolve. four factors that influence one’s competence: skills, empowerment, creativity, and growth.

Knowledge that required by the employees to ensure the implementation of the SOC is well function and operated (1) security monitoring, (2) incident handling, (3) forensics, (4) threat intelligence, (5) coding and development (6) risk management, (7) malware analysis (8) penetration test and vulnerability management, and (9) network communication.It also focus on Training on above mentioned points

1. **Process**

Its a most crucial factor in success of SOC.focus on the need for established procedures and their documentation. The procedures must also be tallied with the existing functions in the SOC.

Helps to to determine the actions and responsibilities of the members in the SOC.importance of establishing fully defined processes between the components in the SOC to ensure consistent and continuous operations. Process factors always depend on the functions, services, and technologies used to establish the SOC.

**Docuement 7 -**

**Docuement 8 - Security Operations Center: Ultimate SOC Quick Start Guide**

# **What is SOC**

This team analyzes and monitors the organization’s security systems. The SOC’s mission is to protect the company from security breaches by identifying, analyzing, and reacting to cybersecurity threats. SOC teams are composed of management, security analysts, and sometimes, security engineers. The SOC works with the company’s development and IT operations teams.

It ensure an appropriate organizational response when incidents do occur. SOC teams isolate unusualactivity on servers, databases, networks, endpoints, applications, etc., identify security threats, investigate them, and react to security incidents as they occur.

# **Two core responsibilities**

* **Maintaining security monitoring tools** – The team must maintain and update tools regularly.
* **Investigate suspicious activities** – The SOC team should investigate suspicious and malicious activity within the networks and systems. Generally, your SIEM or analytics software will issue alerts which the team then analyzes and examines, triages, and discovers the extent of the threat.

# **Core Functions**

Alert triage – The SOC collects and correlates log data, and provides tools that allow analysts to review it and detect relevant security events.

Alert prioritization – SOC analysts leverage their knowledge of the business environment and the threat landscape to prioritize alerts and decide which events represent real security incidents.

Remediation and recovery – Once an incident is discovered, SOC personnel are responsible for mitigating the threat, cleaning affected systems, and recovering them to their normal working condition.

Postmortem and reporting – An important function of the SOC is to document the organization’s response to an incident, perform additional forensic analysis to ensure that the threat has been fully contained, and learn from the incident to improve the SOC’s processes.

Control and Digital Forensics — enforcing compliance, penetration testing, vulnerability testing

Monitoring and Risk Management – capturing events from logs and security systems, identifying incidents, respond

Network and System Administration – administering security systems and processes such as identity and access management

# **Benifits of SOC:-**

Incident response – SOCs operate around the clock to detect and respond to incidents.

Threat intelligence and rapid analysis – SOCs use threat intelligence feeds and security tools to quickly identify threats and fully understand incidents, in order to enable appropriate response.

Reduce cybersecurity costs – Although a SOC represents a major expense, in the long run, it prevents the costs of ad hoc security measures and the damage caused by security breaches.

Reduce the complexity of investigations – SOC teams can streamline their investigative efforts. The SOC can coordinate data and information from sources, such as network activity, security events, endpoint activity, threat intelligence, and authorization.

# **Question to be consider when built SOC:-**

* **Availability and hours** – Will you staff your SOC 8×5 or 24×7?
* **Format**– Will you have a standalone SOC or an integrated SOC and NOC?
* **Organization**– Do you plan to control everything in house, or will you use an MSSP?
* **Priorities and capabilities** – Is security the core concern, or is compliance a key issue? Is monitoring the main priority, or will you need capabilities such as ethical hacking or penetration testing? Will you make extensive use of the cloud?
* **Environment** – Are you using a single on-premises environment or a hybrid environment?

# **Steps for Set up SOC-**

* **Ensure everyone understands what the SOC does tion.**
* **Provide infrastructure for your SOC –**
* **Find the right people –**
* **Have an incident response plan ready** – An incident response team should create a specific and detailed action plan. The team can also create a repeatable plan that can be used over time and adapt to different threat scenarios. Business, PR, and legal teams may also be involved if needed. The team should adhere to predefined response protocols so they can build on their experience.
* **Defend**– A key responsibility of the SOC is to protect the perimeter with a dedicated team focused on detecting threats.

**Docuement 9 - Security Operations and Incident Management Knowledge Area Issue 1.0**

# **What is SOIM**

The Security Operations and Incident Management domain includes many topics. From a

technical standpoint, SOIM requires the ability to observe the activity of an Information Sys-

tem or network, by collecting traces that are representative of this activity. It then requires

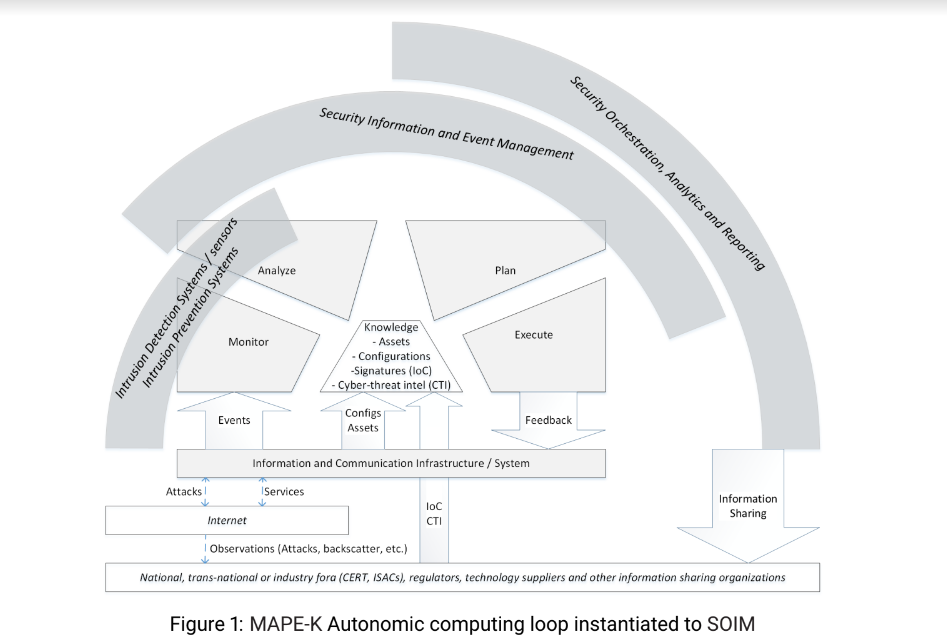
the ability to analyse these traces in real time, or almost real time, to detect malicious events

included in these traces, and to send out alerts related to these events.

an attack is detected, it must be reported and analysed on a SIEM platform, to assess the impact of the attack and to determine the potential remedial actions that can be applied to block the attack or mitigate its effects.

From an operational standpoint, SOIM is very much a process, and the definition of this process requires strong management. It relies on people to perform many of the tasks, from configuring the detectors to analysing the alerts to deciding on remediations. Therefore,skilled analysts are one of the cornerstones of Security Operations and Incident Management. Another key aspect is planning, as all the tools and personnel must be in place before anything can happen.

# **Architecture of SOIM**

****

# **Components that carry out SOIM Workflows**

1. **Intrusion Detection Systems (IDS)-** covering monitoring and detection
2. **Security Information and Event Management (SIEM)**
3. **Security Orchestration, Analytics and Reporting (SOAR)**

# **Intrusion Detection Systems (IDS)**

Most important is to monitor the IT system which is covered by IDSEC. Data sources of Monotring as follows 1) Network Packets 2) Network Infrastructure 3) Web server logs 4) System and Kernal Logs 5) Files and Docuements

Full packet capture concept is being implemented using libpcap library and the tcpdump and wireshark applications. Netflow [76, 36] is a widely used network monitoring tool used for detecting and visualising security incidents in networks [88, 84]. In brief, this protocol records counters of packet headers flowing through router network interfaces.

# **Security Information and Event Management (SIEM)**

It should be considered a decision support system and as such, covers the Analyse and Plan activities. From a Plan perspective, the SIEM platform aims to define the set of actions that can be performed to block an attack or mitigate its effects.

The first objective of a SIEM platform is to collect and centralise information coming from

multiple sensors into a single environment.

Secondly, the SIEM must be able to interpret the information provided by the sensors in a

coherent manner.

# **SOAR**

# **Incident Management**

Defined in the 3 catagory

* Prepare

**Estalblish the policies and proedures and operational Capabilities**

Policies must include formalised response plans that provide a roadmap for implementing the incident response capability, based on risk assessment methods.

* Handle

**Commnicate , Analyse and Mitigate**

the investigation must assess what exactly was compromised, and what was not, as well as the time the compromise occurred.

Mitigation is related to the deployment of emergency measures that can contain the incident and limit its impact. Mitigation must first limit the damage that is brought to systems,

* Follow-up

**Return to normal operations and Indentify and Implement lession learn**

verify that the full extent of the compromise has been realised and to clean up the system.

Another important aspect of post-incident activities is to measure the performance of the

team and the procedures, in order to improve them.

Communication is also an important aspect of follow-up. Lessons learned from incidents

should impact incident training, to ensure that responders are up to date with attacker methods

.

**Docuement 10 - IEEE Security Operations Center: A Systematic Study and Open Challenges**

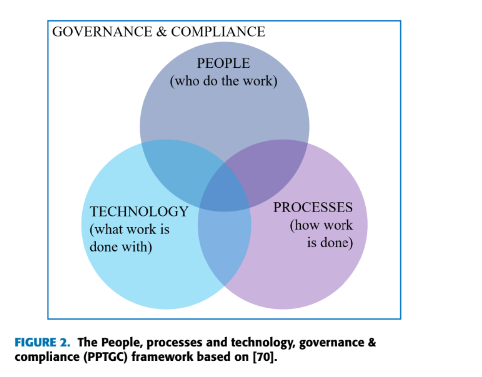
Security Operations Centers (SOCs) can provide an over- arching solution for detecting and mitigating an attack if implemented correctly.

# **Definition of the SOC**

A SOC is an organizational unit operating at the heart of all security operations. It is usually not seen as a single entity or system but rather as a complex structure to man- age and enhance an organization’s overall security posture. Its function is to detect, analyze, and respond to cyberse- curity threats and incidents employing people, processes, and technology

The Security Operations Center (SOC) represents an organizational aspect of an enterprise’s security strategy. It combines processes, technologies, and people to manage and enhance an organization’s overall security posture. This goal can usually not be accomplished by a single entity or system but rather by a complex structure. It creates situational aware- ness, mitigates the exposed risks, and helps to fulfill regula- tory requirements. Additionally, a SOC provides governance and compliance as a framework in which people operate and to which processes and technologies are tailored.

# **SOC Framework - People ,Process and Technology**



# **Types of SOC :-**

SOCs can either be structured as centralized, distributed, or decentralized entities on a high and abstract level. centralized architecture describes the approach where all the data is sent from different locations or subsidiaries to one central SOC for further processing .A distributed SOC, on the other hand, resembles one single system operating across several subsidiaries.Decentralized soc system, a combination of the two system designs mentioned above

# **SOC Archtecture :-**

1. **SOCBOX**

One of the first architecture models for SOCs is the SOCBox proposed by Bidou

SOCBox defines a SOC as composed of five main modules: event generators, event collectors, message databases, analy- sis engines, and reaction management software.

SOCBox primarily focuses on data collection

and incident management but fails to include digital forensics and reactive capabilities to prevent attacks. Moreover,the proposed architecture describes a centralized system with numerous single points of failure. Due to the complexityof modern IT landscapes and technological developments,distributed architectures are often deemed to be more appropriate .

1. **Distributed SOC (DSOC)**

The DSOC architecture lays the basis for the distributed Grid SOC (GSOC) architecture for critical infrastructures, which again is developed by the research teams starting the work on the original SOCBox.

# Factors that contribute towards choice of the SOC archhitectue among SOCBOX or DSOC are

* Company strategy
* Industry sector
* Size
* Cost
* Time
* Regulations
* Privacy
* Availability
* Management support
* Integration
* Data loss concerns
* Expertise:

# **SOC Team Architecture :-**

* **Tier 1 (Triage Specialist) Tier 1 Anayst**

responsible for collecting raw data as well as reviewing alarms and alerts.If occurring problems cannot be solved at this level, they are escalated to tier 2 analysts**.**

* **Tier 2 (Incident Responder)**

review the more critical security incidents escalated by triage specialists and do a more in-depth assessment using threat intelligence

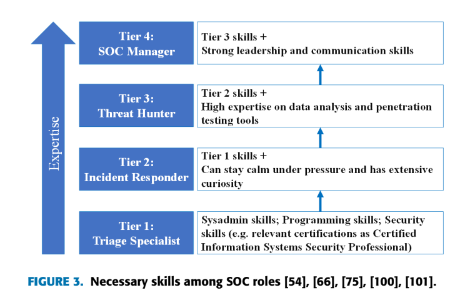
* **Tier 3 (Threat Hunter):**

Tier 3 analysts are the most experienced workforce in a SOC. They handle major incidents escalated to them from the incident responders. They also perform or at least supervise vulnerability assessments and penetration tests to identify possible attack vectors.to proactively identify possible threats, security gaps, and vulnerabilities that might be unknown.

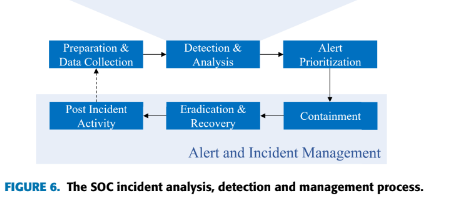
* **SOC Manager:**

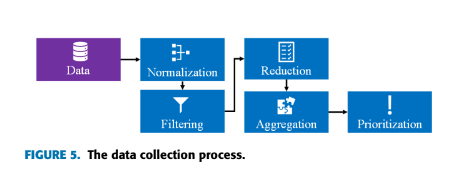
SOC managers supervise the security operations team. They provide technical guidance if needed, but most mportantly, they are in charge of adequately managing the team.

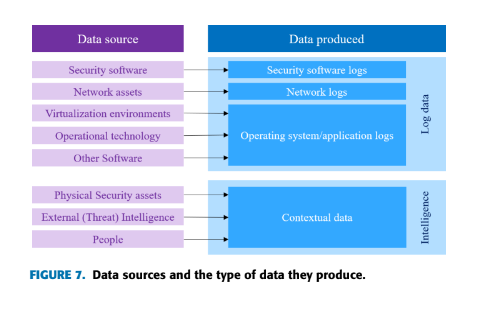
# **Skills needed for SOC -**

****

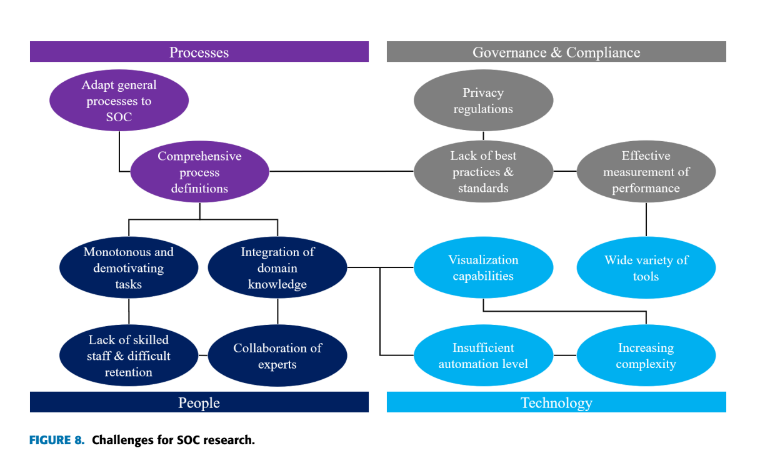
# **SOC Process**

****

****

****

# **SOC Challenges**

****

**Increased volumes of security alerts** – The growing number of security alerts requires a significant amount of an analyst’s time. Analysts may tend to tasks from the mundane to the urgent when determining the accuracy of alerts. They could miss alerts as a result, which highlights the need for alert prioritization.

**Management of many security tools** – As various security suites are being used by SOCs and CSIRTs, it is hard to efficiently monitor all the data generated from multiple data points and sources.

**Skills shortage** – Short staffing or lack of qualified individuals is an issue.

**Docuement 11 - SOC Digital Poster Guide to Secuirty Operations**

This document tells about the SOC tema functions , Tools that are being used in SOC . WHat are the key data that being collected ,Model and Matrics for Security Operations.

# **SOC Core Functions**

SOC Core Functions are as follows :-

1. **Collection**

This step involves recording security relevant events (any useful and observable but not necessarily malicious activity) in the environment. Recording all events such as web traffic, logins and more is required for spotting anomalous activity that may be used to identify attacks in progress.

1. **Detection Triage**

identify, as accurately as possible (without missing anything or generating false positives), all observed events that may indicate a potential attack. This happens two main ways, reactively and proactively.

1. **Triage**

All alerts on the events of interest, which are generated as part of above stages are will be moved for triage. In this stage, SOC analysts must sort through all the potentially malicious

activity that has been generated by the detection function and determine the order of importance in which to assess each alert.

Important factors which needs to be considered are how far the attack may have already progressed, the criticality of the system being attacked, the privilege of the account that may be compromised, and/or whether it appears to be a unique or targeted attack.

1. **Investigation**

Once an alert is selected from triage queue, SOC analysts investigate the alert in more detail to verify if something bad is truly going on.They will use their technical knowledge to investigate and identify the if its true positive or False Postive alert.

1. **Incident Response**

The outputs of an incident response function should be both the remediation of the incident and lessons learned on how to prevent that type of issue in the future.

# **SOC Tools**

The analyst core toolset consists of:

* **SIEM**

The SIEM’s main job is to faithfully receive all logs and parse them correctly into the fields of interest, potentially enriching and correlating the information in the process. Afterward, the parsed fields are indexed into a database of some sort for quick retrieval. It is this data you can then quickly search through, alert on, or make visualizations and reports with.

* **Threat Intelligence Platform**

Another key SOC tool is the Threat Intelligence Platform (TIP). In every SOC

there must be a master list of all the known-bad domains, hashes, IP addresses,

etc., that should be matched against all network and endpoint events. In many

cases, the TIP is where this information is stored, and the TIP serves as the

"source of truth" for IOCs to match against.

* **Incident Management System**

Analysts use the IMS to triage alerts as well as work through active incidents. To

do this as effectively as possible, integrations with your TIP and SOAR platform

can help make additional information lookup and correlation quick and painless.

Once the incidents are investigated, remediated, and closed, the analysts close

the associated ticket. In doing so, one key item that should not be ignored is

the categorization of the incident for metrics purposes.

# **Classification of Data Types**

Collected information can be broken down into two main camps network security monitoring data and endpoint monitoring dataThis data is collected from all points through the network and much of it is centralized to a SIEM for convenient searching, visualization, anomaly hunting and reporting.

# **Network Traffic Data Capturing**

**Flow Record capture : -**

These are high level of network security monitoring logs, describing mainly OSI layer 3 and 4 (TCP/IP) details as well as timing details.Used by SOC and NOC team.

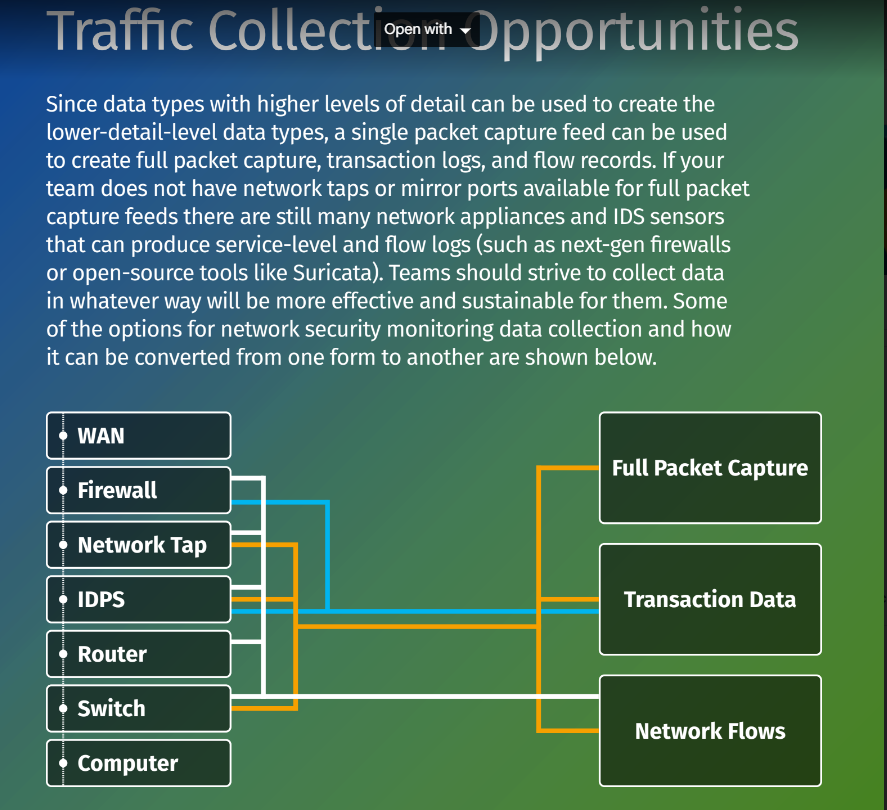
Drawback - not consist to prove if its potential attack

**Transaction Data capture**

Transaction data (also often referred to as network service logs) takes flow log-level data and extends it all the way to OSI layer 7, the application layer.This type of data is produced by tools that look at the full packet and do a true analysis of the protocols in use and the details of the information. This analysis provides information on TLS certificates, HTTP transactions, and more, and is much more useful for identifying attacks

**Full Packet capture**

In these cases, full packet capture provides every single byte sent over the wire and can be used by security teams to get to the ground truth of what happened in an investigation.There are two large common issues with full packet capture – encryption and the size of the data., retention periods for packet capture will typically be significantly shorter than for transaction and flow logs.



# **End Point Data Collections**

# Provides detail on the processes, logins, services, and other key info about what is happening on devices. This data, typically in the form of text logs, is generated by operating systems, applications, and security agents present on the device and is most often collected by log agents and centralized to a SIEM.

The other sources of information are Windows logs, Unix/Linux logs,Cloud Logs,IaaS,PaaS,SaaS logs

# **Three Levels of Threat Intelligence**

Strategic Level

• Consumers: Executives and policymakers

• Looks wide at threat landscape, drives investments, policy, risk

Operational Level

• Consumers: Senior responders, managers

• Goals and trends, campaign tracking, adversary capabilities, attribution data

Tactical Level

• Consumers: SOC analysts, threat intelligence analysts, incident responders

• IOC level: IPs/domains, host artifacts + analysis

• The most common type for analyst-level usage

# **Model for Threat Intelligence**

Every organization and individual should consider their threat model details

as a first step in building out their defense. Part of building a threat model involves answering questions like the following:

1. What are you protecting?

2. Who are you protecting it from?

3. How likely is it you will need to protect it?

4. How bad are the consequences if you fail?

5. How much trouble are you willing to go

through to prevent these consequences?

# **Attack Tree**

Attack trees are a method of visualizing the details of your threat model and how attackers might approach achieving their goals in your environment.It will help for exercise in brainstorming paths attackers may follow and reveals key evidence collection points to help improve your defensive posture.

# **Why Threat Heating is Important**

Threat is a key piece of daily operations and is the other key piece of the “detection” function as previously described. While any SOC will have a large library of known attacks and signatures to identify the attacks, it is guaranteed that there are plenty of unknown pieces of malware and attack methods out there as well for which no signature exists. Therefore, threat-hunting is a necessary activity for all SOC teams, regardless of size or experience.

# **How SOC can be succeed**

success in the SOC relies on effectiveness in both day-to-day operational tasks as well as continuous improvement. KPIs should be developed and used for SOC daily operational items

to know that security tools and processes are operating as expected.

# **SOC Tools**

Here are some SOC team favorites across various categories:

Incident Management Systems

• TheHive

• FIR

Network Security Monitoring

• IDS, network metadata

‒ Suricata: IDS, network metadata, and PCAP capable

‒ EVEbox: Alert triage

‒ Snort

‒ Zeek

• Full Packet Capture

‒ Moloch

‒ Google Stenographer

‒ Netsniff-ng

• Distributions

‒ Security Onion

‒ RockNSM

Endpoint monitoring / HIDS

• NXLog Community Edition: logging agent

• OSQuery

• OSSEC: HIDS

• Sysmon

• Wazuh: HIDS

Incident Response

• Kansa

• Velociraptor

Malware Sandbox and Malware Analysis

• Cuckoo Sandbox

• REMnux: malware analysis tools Linux distro

Threat Intelligence Platforms

• MISP

• OpenCTI

Purple Team Testing and Reporting

• Vectr

SIEM / Log Management

• Elastic Stack

‒ Elastalert: Alerting Engine

Security Orchestration Automation and Response

• NSA Walkoff

• Shuffle

• IBM Node-Red: generalized automation / orchestration framework