IOSR Journal of Engineering (IOSRJEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 56-62

Specialization In Security Operation Center (Soc) For Iot, Cyber Security & Big Data

Gargi Kulkarni[1], Mr. Harish Chandar[2]
[1](Cyber Security Analyst L1, India TechInternational),
[2](Director, India Tech International)

Abstract: *The explosive growth of internet and data generation since the past decade has really thrown the Administrators in a big nightmare as far as maintaining and managing them is concerned .This again leads to several solutions that must be easily adaptable, scalable and robust. Security Operation Centers (SOC) are the first step towards the untangling of this riddle and making the job of administrators easy to track, monitor and maintain the overall network infrastructure remotely from a single location.*
It is therefore imperative to surmise the concept, implementation and future trends of the SOC. The cost and complexity of managing such an immense setup can be prohibitive. Therefore corporates the world over are depending upon such SOCs that are taken care by third party setups that in turn can be in any part of the world.

I. Introduction

The next generation in security is (SOC) security operation center.To realize the need of system security, data related security and cyber related security & to protect our data from attackers, SOC needs to be implemented.

Information Security:

The protection of any kind of information and other related information systems from untoward and illegal access with the help of confidentiality, integrity and availability (CIA) of information is called information security. In simple way information security is protecting our information and handling risk management with control and balance for protection and unauthorized access.

Fig 1: Triad of Information Security

To protect valuable and important data from exploitation, 3 main concepts as indicated above are listed below-
Confidentiality: controlling who gets to read information
Integrity: only administrator or authorized person can use the change information and programs.
Availability:to be aware that only users who are legally allowed, to have continued access.
Cyber and its related security
Cyber and its related security is the technique of detection, defending and protection technologies.
It also helps in protection of all kinds of computing devices and data from unauthorized access.
It militates against vulnerabilities and malicious attacks delivered via the Internet by cyber criminals.

Cyber security provides the following security

- **Network security** secures a computer network from intruders (hacker), and opportunistic malware.
- **Application security** focuses sharply on the upkeep of software programs and devices devoid of threats and begins in the initial stages when designing is done.
- **Information security** protects the correctness and secret nature of data when it is being stored in storage and also whiles it is freely flowing around.

- **Security while in Operation** covers the methods one uses for taking care of data as an asset. It also determines the required level of accessibility of any user when they are using a network and the steps that allows one keep data at a certain place.
- **Disaster recovery and business continuity** defines an organizations response to cyber security incidence. Disaster recovery is the simple method of helping corporates to get back their original operations as like before. Business continuity sometimes is used by organizations to go ahead when they don't really have any fall back option.
- **End-user education**- educates the end user about good security practices. The aim here is to educate users about the perils of clandestine usage and practices when they are using computers and internet.

Difference between IS & CS

Figure 2: IS and CS differences

ICT- this is an amalgamation of IS & CS. CS is subset of IS.
Information security – allows one to keep the data as confidential as possible while maintaining its correctness and availability.
Cyber security- is an action against actual attacks and involves identifying, monitoring & detecting an erratic behavior in the system.

(SOC-) SECURITY OPERATION CENTER

The basic concepts involve detection, prevention & protection.

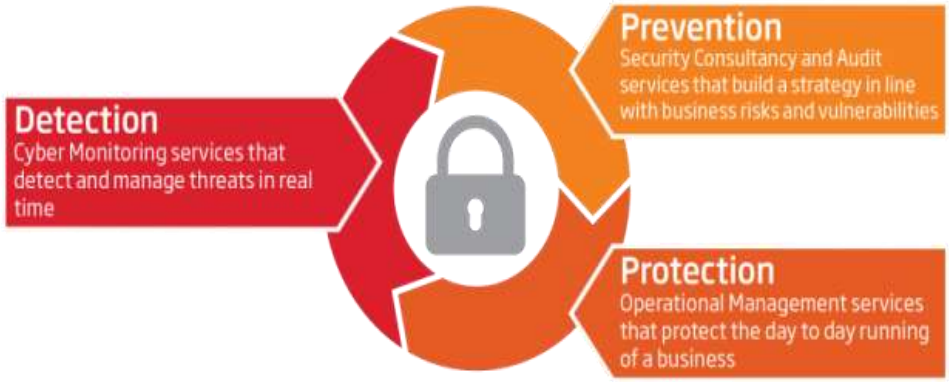

Figure 3: SOC basic concepts

http://bizsecure-apac.com- image

A security operations center (SOC) may be thought of as a set of people who work together depending upon the time zone required and as per the requirements of a local government rules and regulations.
Because of security threats, malicious attacks both have been growing exponentially as per a study done on this topic.

II. Literature Review

Need of the SOC-:

Recently cyber attackers hit several organization and banking systems & exposed about 4 billion records which were supposed to be confidential. The more accurate method to combat is with the help of SOC. SOC can be described as a cyber-clearing house manned by security professionals who leverage technology to monitor an organizations infrastructure and thus prevent attacks

Any SOC is supposed to do following

1. **Proactive detection** -: to detect new, unknown threats, malicious network and system activity
2. **Threat awareness** to adjust defenses before the threat hits.
3. **Vulnerability management -:**allows one to take action on a weakness sometime much before they can happen.
4. **Awareness of the assets being used-:** to be clear about threats that can destroy the assets running the network.
5. **Log management-:** to give one authority to do forensics during incident breach.

SOC Working

A quick snap shot of a SOC looks like.

Figure 4: A typical SOC Room

https://www.checksumis.com

Intoday's industry now a day new Attacks, Malwares, Trojans horses, phishing, spoofing, worms and virus occur regularly and to protect ,detect and cure one uses SOC in almost every area. To avoid attackers' criminal intentions we have to protect our information with the help of a SIEM tool.

Effectively SOC can be broken into the **following components**.

Figure 5:- SOC Components

SOC Components

- **Log collection -:** record of system activities are collected as logs & analyze at the SOC.

- **Reporting-:** Critical reports are collected across the infrastructure and deposited the SOC.
- **Research & Development-:** Since all kind of data accumulation take space at the SOC, It's easy to do research & development for more insight.
- **Threat Intelligence** -: with so much of information flowing through SOC, analyzing threats in advance becomes possible.
- **Knowledge Base-**: Since every systems data and other critical information is deposited in SOC, It becomes massive knowledge base for all future purposes.
- **Ticketing**-: Costumers complaints are handled as per incidence in the form of ticket. Tickets are them assigned to service representative.
- **SIEM-:** all incidence and events are constantly monitored to predict any kind of potential risk.
- **Aggregation/correlation-:** Since massive amount of data are centralized in SOC, it's become easy for aggregation and correlation using algorithms

SOC key features

- **24 hours monitoring:** allows to better safeguard the data and other critical assets always, nonstop.
- **Early Warning:**This allows one to get an insight in advance before there can a catastrophic issue that can disrupt the system.
- **Security assessment**: checks the security of information system. It allows the actual evaluation of the systems containing the pieces of information they protect, by remote intervention or in field intervention through activities like Network and System Discovery, Vulnerability Assessment, Penetration Test, Web Application Test.

Working of SIEM

The key concept behind SOC is SIEM which monitors and creates notifications.

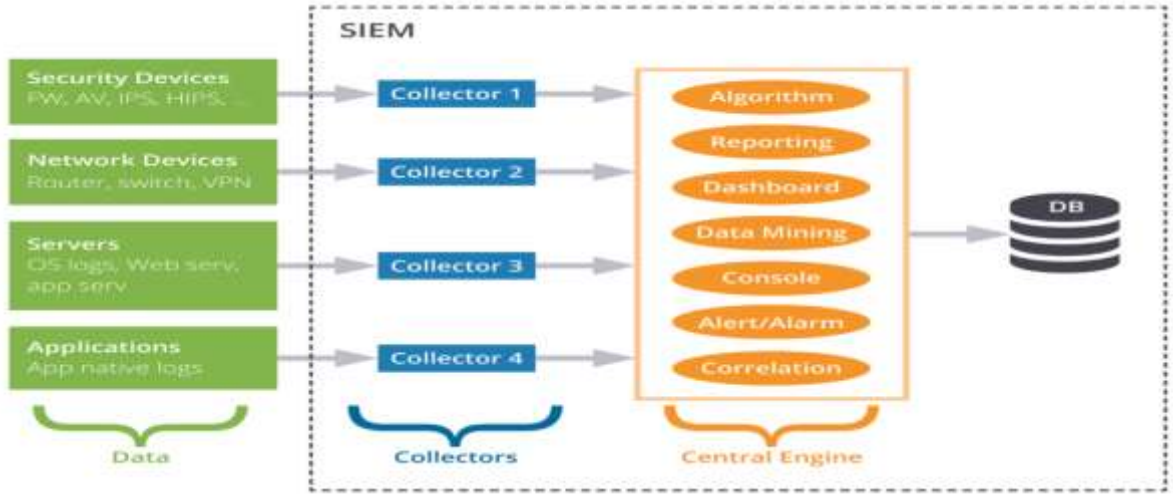

Figure 6: SIEM and its working

The SIEM essentially is all about event monitoring and notification. The heart of SIEM is logs.Logs are stored in small encrypted format which have some kind of security algorithms such as MD5, IDS, IPS, DES, RSA, BLOWFISH, TWOFISH and AES which helps us to read information

Generallythere are collectors and center engine which together collect data from devices, servers and application.

SIEM tools advantages.

- Allows one to optimize Time and Money while using other party tools.
- Detect issues and problems immediately, they day they erupt.

SIEM can further fortify the safety by using:-

- Firewalls and antivirus detection
- Cyber threats intelligence
- Vulnerability and penetration tests
- Website assessment

- Data base scanners
- Systems that checks for illegal entry
- Log management systems
- Governance and compliance system

III. Research design

Case Study Of Mauritius Traffic Police Department

The SOC is generally implemented after careful research and design. A typical case study here would be a traffic police department in the island of Mauritius. Typically, in the country of Mauritius the traffic police & the city police are generally responsible for the safety and security of the citizen. Throughout the island there are 300 security cameras, connected to the smart traffic poles which in-turn creates a giant network. All data is usually sent to several servers situated on the cloud (internet). A remote monitoring office (RMO) is used in the capital city of Port-Louis.

The SOC at this location is monitoring entire situation 24/7. A special series of monitor are set up to track every single incident. Since the Database or Data warehouse at each location is connected to the SOC, It creates massive amount of data, which I otherwise

Big Data. This data are monitored to SOC and check it with SIEM tool.

The SOC of the traffic police receives data from traffic signal poles, these poles are **IOT** based since sensors are set up at every sets. Any emergencies comes on the road CCTV, grader & sensors are monitor and report it directly **Cyber security** or the protection of the network and devices situated at the Port- Louis facility is one of the main concerns of the SOC support department.

Sample image of implementation of SOC in above CASE STUDY

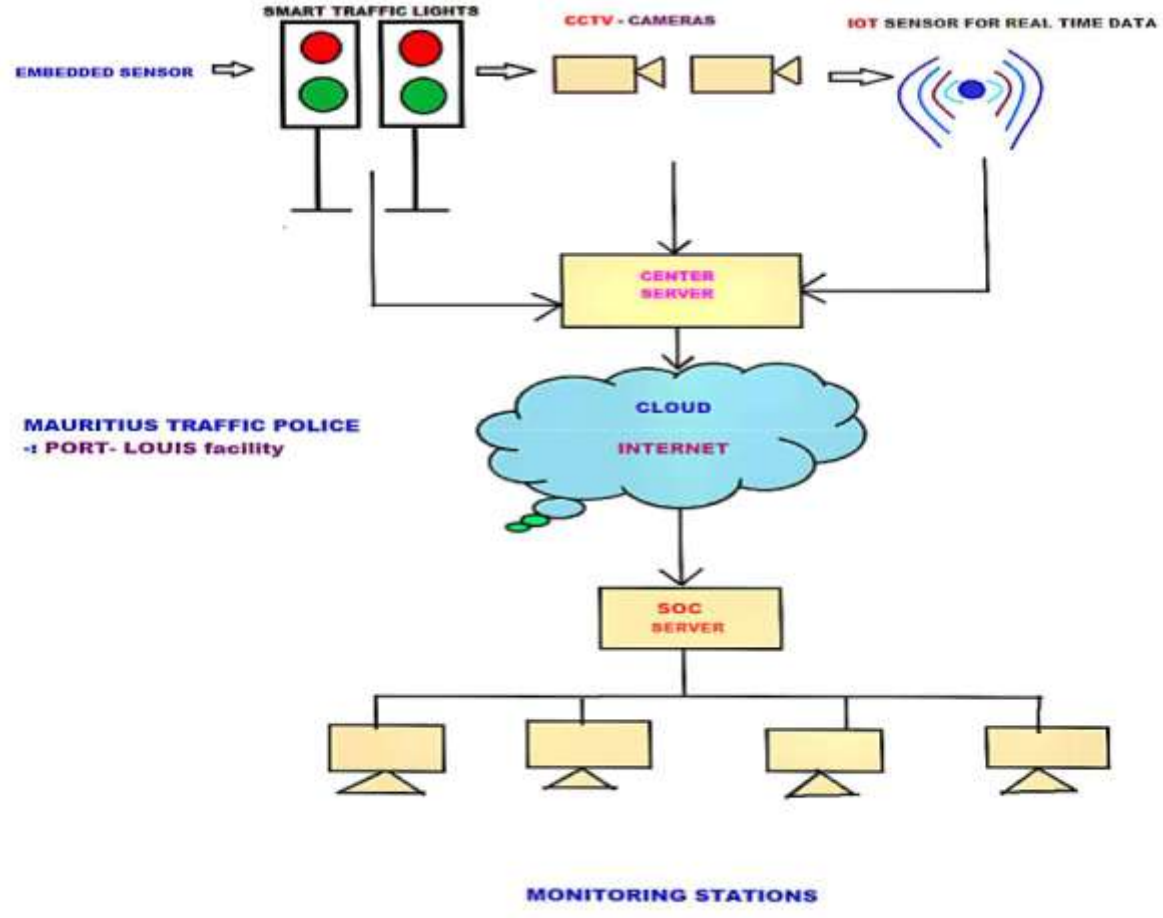

Figure 7: Mauritius Police SOC situated in capital city of Port Louis

IV. Implementation

The Implementation landscape of SOC is again much customized. The onus is on the client side requirements. Different clients or vendors have varied use cases of SOC, which may or may not match with each other.
The security operations centers need to use a new approach to detecting emerging attacks which will mature over time as landscape changes. Years ago, a SOC was primarily based on rules. Currently one can write their own customized rules and use them accordingly.
Organizations will need to consider some main factors while thinking of using an SOC:-

- Check how much level of security is required;
- Check how much threats are looming ahead;
- Understand the kind of technology required ;
- Select an operating technique or model;
- Createmarkers that enhancesthe performance.

SOC for IOT, Cyber security and Big data.
The threat to information has been increasing exponentially as more and more of new technologies come into play such as Big Data, IOT etc.
The rate at which new malwares grow is really alarming, so much so that more than 100 Corer malwares were detected till about 2015.
It is therefore very important to identify the weaknesses in these environments before the cyber criminals make their move.
The extent of intelligence for threats will need to cover the entire spectrum of attacks and typically the organizations need to keep alert and watchful.

Next Generation Soc And Its Use In Iot

Next-generation Security Information and Event Management (SIEM) solutions are created keeping in mind the different advanced use cases and also has many tools integrated .Specifically, User Entity Behavioral Analytics (UEBA) technology makes it possible to detect insider threats, perform more sophisticated threat hunting, prevent data exfiltration and mitigate IOT threats, even when traditional security tools don't raise a single alert.

One good example of this type of security system is the one developed by the company ExabeamInc... It has created a platform that is based on the UEBA technology mentioned above and helps in plenty of automated threat's that can come from insiders.

Cyber Security And Soc

The good part about SOC is that it works continuouslyand also manages known and existing threats while actively trying to recognize emerging types of risks and threats. They adopt two approaches of trying to meet the needs of the customer and at the same time also be well within the risk level tolerated. One requires human analysis more apart from firewalls etc. to fully prevent any kind of risks.Additionally the SOC must keep up with the latest threat intelligence and use this information to optimize internal detection and all kinds of defense mechanisms.

Building the Next Generation SOC
Security Operations Centers will need to undergo in-depth transformation in order to implement Prescriptive Security Analytics.
This transformation will require: The central use of Big Data Analytics, Machine Learning and threat models in the toolset of Prescriptive SOC's.

BIG DATA AND SOC
By using Big Data Analytics and supercomputing systems, it possible to enhance and optimize the systems.

Data visualization

Security analysts and Threat analysts are presented with a graphical perspective that deeply enhances the brain's capacity to identify the underlying and relevant data. Timely access to full and aggregated context data, speeds, augments the accuracy of the event qualification thus reducing dramatically both false positives and negatives. Dashboards show the Key parameters for users to understand the situation.

V. Technology

- In the current situation, SOCs are implemented as per the current and existing hardware and software platforms available.
- While this is not a blanket rule, it leaves space around for several more innovations and foresight in its adaptation.

Motivation for Using Next-Generation SOC Tooling

- **Next-generation SIEM**—assists to lessen alertness fatigue while letting analysts focus on the alerts that is important .The latest crop of analytics when combined with the range of security data, allows new generation of SIEMs to seek problems that no individual security tool can make out that easily.
- **NTA**—easy to implement, great at detecting abnormal network behaviors. Useful when the SOC has access to the traffic under investigation and is interested in investigating lateral movement by attackers already inside the perimeter.
- **UEBA**—uses machine learning and data science techniques to detect malicious insiders, or bypass of security controls. Makes it much easier to identify account compromise, whether by outside attackers or insiders.
- **EDR**—provides a strong defense against compromise of workstations or servers, helps manage the mobile workforce. Provides the data needed to carry out historic investigations and track root causes.

Emerging Trends

There are several new trends that are currently being thought of and implemented:

- GSOC or Global SOC --- where the distribution of systems and data are over the entire world.
- GNOC or Global Network OC ----- where the focus in entirely on the network infrastructure and its monitoring.

FINAL THOUGHTS

SOCs really are solutions to the problems that plagued the monitoring and incident fraternity.
Large Data Servers and Networks that are fanned all over the globe pose a big technological challenge as far as tracking them and optimizing them are concerned.
IOT security, Cyber Security and Big Data are definitely the key technologies to be integrated in the fabric of an SOC and by doing this we are able to lift the burdens of administrators across the globe, so that they have a single point of access and control.
My humble submission here is that SOCS as on today are not really used by everybody; maybe due to their scale and cost, so perhaps one solution will be to make the scale and cost factors affordable and the technology aspect also less intimidating

References

[1]. http://indiatechint.com/
[2]. Security Operations Center – CCIE book (Joseph Muniz ,Gary McIntyre,Nadhem, AlFardan)
[3]. https://www.alienvault.com/solutions/siem-log-management
[4]. http://google.com- image
[5]. https://www.nap.edu/
[6]. http://bizsecure-apac.com- image
[7]. https://usa.kaspersky.com
[8]. https://www.forbes.com
[9]. https://www.lewan.com/blog
[10]. https://www.alienvault.com
[11]. https://atos.net.com
[12]. https://www.exabeam.com