International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

A Review on the Role of Modern SOC in Cybersecurity Operations

I Putu Elba Duta Nugraha
Department of Electrical Engineering, Udayana University, Jimbaran, Badung Regency 80361, Indonesia

ABSTRACT: This paper will examine the position and mission of today's Security Operation Center (SOC), as well as the numerous tools available to those interested in pursuing a career in cybersecurity operations. Defending against today's threats necessitates a method that is formalized, organized, and disciplined. Professionals in a Security Operations Center (SOC) are commonly used by businesses. SOCs provide a wide variety of services, from monitoring and control to comprehensive threat solutions and hosted security, all of which can be tailored to suit the needs of individual customers.

KEYWORDS: Cybersecurity, Security Operation Center

INTRODUCTION

Cyber-attacks are expected to cost companies more than $5 trillion a year by 2024. Protected information such as personally identifiable information (PII), protected health information (PHI), and personal security information (PSI) is often compromised. When this knowledge, including trade secrets, is stolen, a company's competitive advantage may be lost. Customers also lose faith in the company's ability to protect their personal information. Governments have also been the target of cyber-attacks.
Defending against today's threats necessitates a method that is formalized, organized, and disciplined. Professionals in a Security Operations Center (SOC) are commonly used by businesses.

THE MODERN SECURITY OPERATION CENTER

SOCs provide a wide variety of services, from monitoring and control to comprehensive threat solutions and hosted security, all of which can be tailored to suit the needs of individual customers. SOCs can be fully in-house, owned and run by a company, or they can be outsourced to security vendors.

A. Elements of a SOC

People, processes, and technology are the major components of a SOC, as shown in Figure 1.

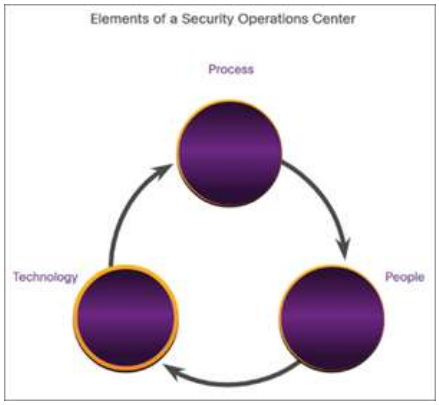

Fig. 1 – Elements of a Security Operations Center.

B. People in the SOC

In a SOC, job functions are rapidly changing. SOCs have traditionally assigned job positions to tiers based on the level of experience and duties needed by each. Jobs in the first tier are more entry-level, while jobs in the third tier need comprehensive knowledge.

- Tier 1 Alert Analyst – often known as Cybersecurity Analysts or CyberOps Associates, track incoming notifications, verify that a true incident has occurred, and, if appropriate, forward tickets to Tier 2.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

- Tier 2 Incident Responder – these experts are in charge of conducting in-depth investigations into incidents and recommending remediation or intervention.
- Tier 3 Threat Hunter – these experts have advanced knowledge of network, endpoint, threat intelligence, and malware reverse engineering. They are experts at tracing malware's processes to assess its effect and how to delete it. They're also heavily involved in the search for new threats and the deployment of threat detection software. Threat hunters look for cyber threats that haven't been identified yet but are present in the network.
- SOC Manager – this individual is in charge of the SOC's resources and acts as a point of contact with the larger company or client.

Figure 2 (courtesy of the SANS Institute) graphically depicts how these functions communicate with one another.

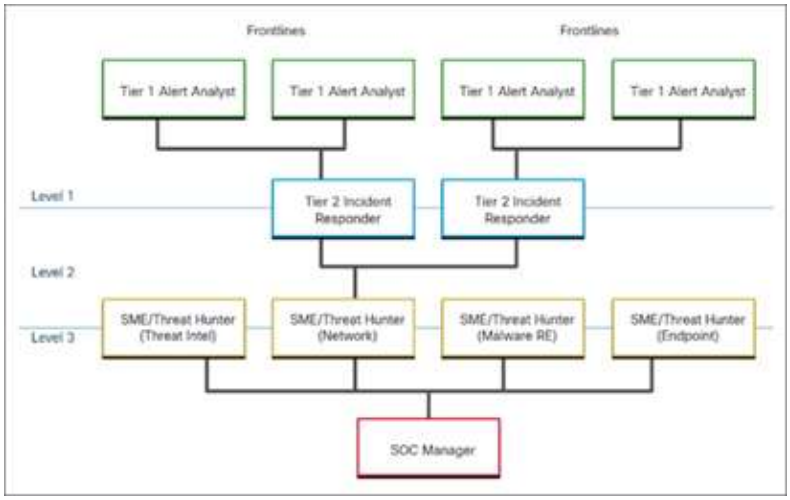

Fig. 2 – Interaction between roles in a SOC.

C. Process in the SOC

A typical day for a Cybersecurity Analyst starts with checking security alert queues. When assigning alerts to a list for an analyst to investigate, a ticketing system is commonly used. Since the software that produces alerts may cause false alarms, a Cybersecurity Analyst's role can include confirming that an alert reflects a genuine security incident. When the incident has been verified, it may be forwarded to investigators or other security officials for action. If not, the message may be ignored as a false alarm.

If a ticket cannot be handled by the Cybersecurity Analyst, the ticket will be forwarded to a Tier 2 Incident Responder for further review and remediation. If the Incident Responder is unable to resolve the ticket, it will be forwarded to Tier 3 staff who have extensive expertise and threat hunting experience. The roles of the people in a Security Operations Center are depicted in Figure 3.

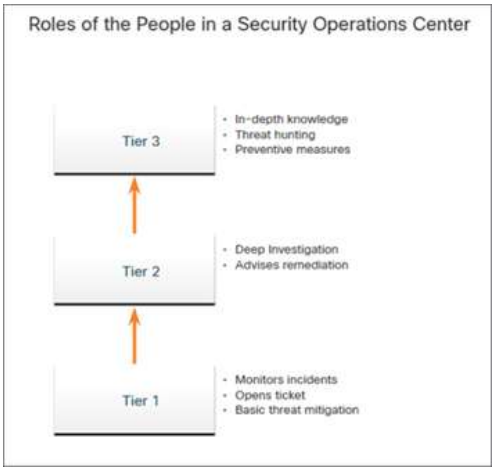

Fig. 3 – Roles of the people in a SOC.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

D. Technologies in the SOC: SIEM

A Security Operations Center (SOC), as shown in Figure 4, needs a security information and event management system (SIEM) or its equivalent. SIEM decodes the data produced by firewalls, network appliances, intrusion detection systems, and other devices.

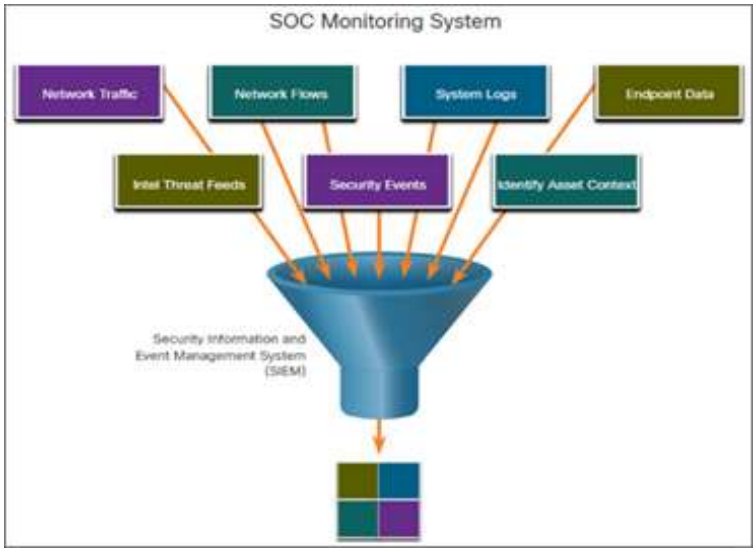

Fig. 4 – SOC monitoring system.

SIEM systems are used for data collection and filtering, threat detection and classification, and threat analysis and investigation. SIEM systems can also help enforce preventative measures and resolve potential risks by managing resources. One or more of the following technologies are used in SOCs:

- Event collection, correlation, and analysis
- Security monitoring
- Security control
- Log management
- Vulnerability assessment
- Vulnerability tracking
- Threat intelligence

E. Technologies in the SOC: SOAR

SIEM and SOAR (security orchestration, automation, and response) are often combined because their capabilities complement each other.Both technologies are used by large security operations (SecOps) teams to improve their SOC. By the end of 2020, 15 percent of organisations with a security team of more than five people are expected to use SOAR.

In the same way that SIEMs aggregate, compare, and interpret alerts, SOAR platforms do the same. SOAR technology, on the other hand, takes it a step further by combining threat intelligence and automating incident investigation and response workflows based on playbooks generated by the security team.

SOAR security platforms as shown in the Figure 5:

- Gather alarm data from each component of the system.
- Provide tools that enable cases to be researched, assessed, and investigated.
- Emphasize integration as a means of automating complex incident response workflows that enable more rapid response and adaptive defense strategies.
- Include pre-defined playbooks that enable automatic response to specific threats. Playbooks can be initiated automatically based on predefined rules or may be triggered by security personnel.

SOAR focuses on SOC process automation and integration tools. It automates many manual procedures, such as security alert investigation, requiring only human involvement when necessary. This frees up security staff to focus on more urgent issues such

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

as high-level investigation and threat mitigation. SOC processes and work functions will be reshaped as advanced SOAR platforms become more widely adopted.

In order to conservatively catch as many potential vulnerabilities as possible, SIEM systems must generate more alerts than most SecOps teams will possibly investigate. Many of these alerts would be processed automatically by SOAR, allowing security staff to concentrate on more complicated and potentially damaging exploits.

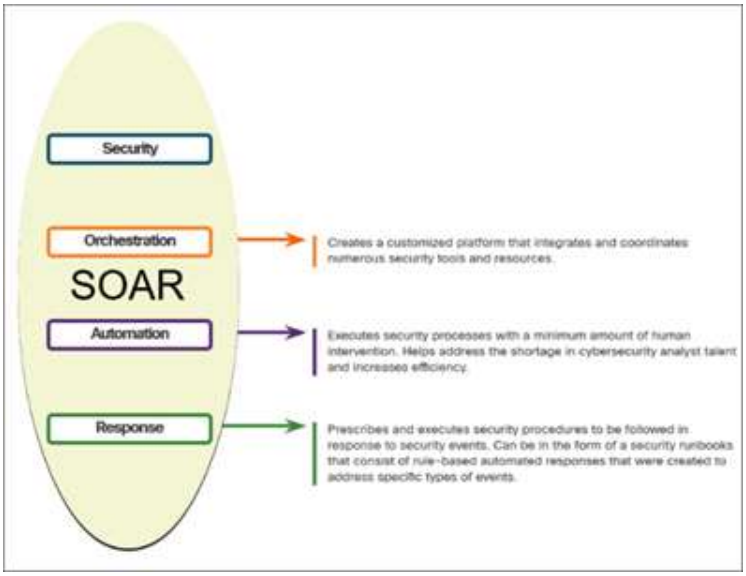

Fig. 5 – SOAR platforms.

F. SOC Metrics

A security operations center (SOC) is essential to an organization's security. Whether the SOC is internal to an organization, or providing services to several organizations, it's important to know how well it's working so that the staff, procedures, and technology that make up the SOC can be improved.

To assess various aspects of SOC efficiency, several metrics, or key performance indicators (KPIs), can be invented. Five metrics, however, are widely used as SOC metrics. Due to the diversity of cybersecurity threats, metrics that describe overall success often do not paint an accurate image of SOC activity. The following are some of the most common metrics collected by SOC managers:

- Dwell Time – the length of time that threat actors have access to a network before they are detected, and their access is stopped.
- Mean Time to Detect (MTTD) – the average time that it takes for the SOC personnel to identify valid security incidents have occurred in the network.
- Mean Time to Respond (MTTR) – the average time that it takes to stop and remediate a security incident.
- Mean Time to Contain (MTTC) – the time required to stop the incident from causing further damage to systems or data.
- Time to Control – the time required to stop the spread of malware in the network.

G. Enterprise and Managed Security

The company would benefit from introducing an enterprise-level SOC for medium and wide networks. The SOC can be used as a full-fledged in-house solution. Many larger organizations, on the other hand, would outsource some or all of their SOC activities to a security solutions provider.

The security solutions company has a team of professionals who assist in the prompt and effective resolution of incidents, as well as a wide range of incident response, preparedness, and management capabilities.

H. Security vs. Availability

Most business networks must be available at all times. Network availability must be maintained for the organization's goals to be met, according to security staff.

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

Network downtime is tolerable to a certain extent in each company or industry. The tolerance is normally determined by weighing the cost of downtime against the cost of avoiding downtime. It might be appropriate to have a router as a single point of failure in a small retail company with only one venue, for example. If, on the other hand, online sales account for a significant portion of the company's revenue, the owner can decide to provide redundancy to ensure that a connection is still available.
As shown in Table 1, preferred uptime is often calculated in the amount of down minutes per year. A "five nines" uptime, for example, ensures that the network is operational 99.999 percent of the time or for no more than 5 minutes per year. A year of "four nines" will be 53 minutes of downtime.

Table 1 - The number of down minutes in a year.

Availability %	*Downtime*
99.8%	17.52 hours
99.9% ("three nines")	8.76 hours
99.99% (" four nines")	52.56 minutes
99.999% ("five nines")	5.256 minutes
99.9999% ("six nines")	31.56 seconds
99.99999% ("seven nines")	3.16 seconds

Security, on the other hand, cannot be so strict that it interferes with employee needs or business functions. There is often a trade-off between ensuring good security and allowing for successful business operations.

BECOMING AN ANALYST

A. Certifications

Several organizations offer cybersecurity certifications that are applicable to employment in security operations centers (SOC):

- Cisco Certified CyberOps Associate
  The Cisco Certified CyberOps Associate certification is a good place to start if you want to learn how to work with a security operations center. It can be an important component of a career in the exciting and rapidly expanding field of cybersecurity operations.
- CompTIA Cybersecurity Analyst Certification
  The CompTIA Cybersecurity Analyst (CySA+) certification is an IT professional certification that is vendor-neutral. It certifies expertise and skills in configuring and using threat detection software, performing data analysis, and interpreting the findings to identify vulnerabilities, hazards, and risks to an enterprise. The ability to secure and protect applications and systems within an enterprise is the ultimate objective.
- (ISC)² Information Security Certifications
  (ISC)² is a non-profit organization based in the United States that provides the CISSP certification. They also deliver a variety of other cybersecurity certifications for different specialties.
- Global Information Assurance Certification (GIAC)
  GIAC is one of the oldest security certification organizations, having been established in 1999. It offers certifications in seven different categories.

B. Further Education

- Degrees
  A technical degree or bachelor's degree in computer science, electrical engineering, information technology, or information security should be seriously considered by those interested in a career in cybersecurity. Security-related specialized tracks and certifications are available at several educational institutions.
- Python Programming
  For anyone interested in a career in cybersecurity, computer programming is a must-have skill. Python may be the first language to learn if you've never programmed before. Python is an object-oriented, open-source programming language

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

that is often used by cybersecurity experts. For Linux-based systems and software-defined networking (SDN), it's also a common programming language.

- Linux Skills
  In SOCs and other networking and security environments, Linux is commonly used. As you learn to build a career in cybersecurity, Linux skills are a valuable addition to your skill set.

C. Sources of Career Information

Information technology jobs are advertised on a range of platforms and smartphone apps. Each platform caters to a particular group of job seekers and offers a variety of resources for candidates to find their ideal job. Many websites function as job aggregators. Job aggregators collect listings from multiple job boards and company career sites and view them in one place.

- Indeed.com
  Billed as the world's most famous job site, receives over 180 million unique visitors each month from more than 50 countries. Indeed.com is truly a global job site. It assists businesses of all sizes in hiring the best candidates and provides job seekers with the best opportunities.
- CareerBuilder.com
  Many big and prominent businesses use CareerBuilder. As a result, this website attracts candidates who have a higher level of education and qualifications. Employers who post jobs on CareerBuilder are more likely to receive applicants with college degrees, advanced qualifications, and industry certifications.
- USAJobs.gov
  On the USAJobs website, the US federal government posts any job vacancies.
- Glassdoor
  Salary statistics for various job types, businesses, and locations can be found on the website glassdoor.com. To see wages and qualifications for current job openings, search for "cyber security analyst."
- LinkedIn
  LinkedIn is a professional network of over 630 million members in over 150 countries, with the aim of assisting people in becoming more efficient and prosperous. LinkedIn is also a great place to look for job openings and career statistics.

D. Getting Experience

- Internships
  Internships are a great way to get started in the cybersecurity sector. Internships may often lead to full-time job offers. Even a temporary internship, though, will provide you with valuable insight into the inner workings of a cybersecurity firm. Internship connections will also serve as a valuable resource as you progress in your career. Look up the best websites for network security internships on the internet.
- Scholarships and Awards
  Organizations such as Cisco and INFOSEC have launched scholarship and awards programs to help close the security skills gap by providing money to students who meet qualification criteria. Look on the internet to see what resources are actually available.
- Temporary Agencies
  A temporary agency can be a good place to start if you're having trouble finding your first job. Most temporary agencies will assist you in polishing your resume and making suggestions for additional skills you will need to acquire in order to appeal to prospective employers. For the first 90 days, many companies use temporary agencies to fill work vacancies. The company can then offer to purchase the contract from the temporary agency, transferring the employee to a full-time, permanent position if the employee is a good fit.
- Your First Job
  If you have no prior experience in cybersecurity, you should look for a company that will prepare you for a job close to that of a Tier 1 Analyst. Working for a call center or a customer service desk might be the first step toward acquiring the experience you need to advance in your career. When it comes to your first career, how long do you stay? Before leaving an organization, you should usually go through the entire evaluation cycle. That is, you want to make it past the 18-month

International Journal of Current Science Research and Review
ISSN: 2581-8341
Volume 04 Issue 05 May 2021
DOI: 10.47191/ijcsrr/V4-i5-13, Impact Factor: 5.825
IJCSRR @ 2021
www.ijcsrr.org

mark. In most cases, potential employers may want to know whether you have met or surpassed expectations in your current or previous positions.

CONCLUSIONS

People, procedures, and innovations are all important components of the SOC. Job roles are changing at a rapid pace, with tiers dependent on skills and experience. A Tier 1 Alert Analyst, a Tier 2 Incident Responder, a Tier 3 Threat Hunter, and a SOC Manager are among these positions. A Tier 1 Analyst is responsible for monitoring events, opening tickets, and performing simple threat mitigation.

SIEM systems are used for data collection and filtering, threat detection and classification, and threat analysis and investigation. SIEM and SOAR are sometimes used in conjunction. SOAR is a sibling of SIEM. SOAR takes it a step further by combining threat intelligence and automating incident investigation and response workflows using playbooks created by the security team. Various aspects of SOC performance are measured using Key Performance Indicators (KPI). Dwell Time, Meant Time to Detect (MTTD), Mean Time to Respond (MTTR), Mean Time to Contain (MTTC), and Time to Control are all common metrics. There must be a compromise between network security and availability. Security must not be so strict that it obstructs staff or business operations.

Different organizations offer a range of cybersecurity certifications that are applicable to careers in SOCs. Cisco Certified CyberOps Associate, CompTIA Cybersecurity Analyst Certification, $(ISC)^2$ Information Security Certifications, Global Information Assurance Certification (GIAC), and others are some of the certifications available. Indeed.com, CareerBuilder.com, USAJobs.gov, Glassdoor, and LinkedIn are examples of job sites. Internships and temporary agencies are other options for gaining experience and starting your career. Programming skills in Linux and Python can also help you stand out in the job market.

REFERENCES

1. Cisco Networking Academy. (2021). CyberOps Associate 1.0 Modules 2, Fighters in the War Againts Cybercrime.
2. Bidou, Renaud. (2005). Security Operation Center Concepts & Implementation.
3. Majid, M. & Ariffi, K. (2019). Success Factors for Cyber Security Operation Center (SOC) Establishment. 10.4108/eai.18-7-2019.2287841.
4. Arimatsu, T. & Yano, Y. & Takahashi, Y.. (2018). Security operations center (SOC) and security monitoring services to fight complexity and spread of cyber threats. NEC Technical Journal. 12. 34-37.
5. Agyepong, Enoch & CHERDANTSEVA, YULIA & Reinecke, Philipp & Burnap, Pete. (2020). Cyber Security Operations Centre Concepts and Implementation. 10.4018/978-1-7998-3149-5.ch006.
6. Miloslavskaya, Natalia. (2016). Security Operations Centers for Information Security Incident Management. 10.1109/FiCloud.2016.26.
7. Cadena, Alyssa & Gualoto, Franklin & Fuertes, Walter & Tello Oquendo, Luis & Andrade, Roberto & Tapia Leon, Freddy & Torres, Jenny. (2020). Metrics and Indicators of Information Security Incident Management: A Systematic Mapping Study. 10.1007/978-981-13-9155-2_40.
8. Miloslavskaya, Natalia & Tolstoy, Alexander. (2019). New SIEM System for the Internet of Things. 10.1007/978-3-030-16184-2_31.
9. El Arass, Mohammed & Souissi, Nissrine. (2019). Smart SIEM: From Big Data logs and events to Smart Data alerts. 8. 3186-3191.
10. Vielberth, Manfred & Böhm, Fabian & Fichtinger, Ines & Pernul, Günther. (2020). Security Operations Center: A Systematic Study and Open Challenges. IEEE Access. PP. 10.1109/ACCESS.2020.3045514.

Cite this Article: I Putu Elba Duta Nugraha 2021). A Review on the Role of Modern SOC in Cybersecurity Operations. International Journal of Current Science Research and Review, 4(5), 408-414