IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 8, Issue 4, Aug - Sep, 2020
ISSN: 2320 – 8791 (Impact Factor: 2.317)
www.ijreat.org

BUILDING AN EFFECTIVE SECURITY OPERATION CENTER

[1]Sulaiman Muhail Abdullah Al Khatri, [2]Basant Kumar

[1]Master Information Technology (Cyber Security), Deptt of Computer Sc, Modern College of Business and Science, Muscat, Sultanate of Oman, Muscat, Sultanate of Oman, Modern College of Business and Science, basant.info@gmail.com, basant@mcbs.edu.om

[2]Master Information Technology (Cyber Security), Deptt of Computer Sc, Modern College of Business and Science, Muscat, Sultanate of Oman, Muscat, Sultanate of Oman, Modern College of Business and Science

Abstract— The aim of the Security Operation Center(SOC) is to protect the personal data, intellectual property, brand protection and business system of the organizations. The research relies on the inclusion criteria which is supported through secondary data collection sources. Interpretation of the data is made through content analysis. Building a successful SOC is authoritative for organizations everything for the purpose of equality. Characterizing the strategies and systems that helps to administer individuals that are a part of this group must be a progressing procedure to more likely serve the group and organization overall. The management of roles and responsibilities is valuable in this regard, the control room must consists of advanced equipment for fulfilling the requirements of tasks properly. The risk of leaking personal data, business documents and intellectual property affects the credibility of the organization as well as brand integrity. The tactics of data security must contain data classification, permissions management, access management, identity management, security analytics and threat detection. Response solution are needed from the organizations for valuing the investment and challenges that are faced in the processes. Designing of frameworks requires policy practicing in effective manner from people, suppliers, partners, technology and products to accept the change in practices.

.

Keywords— ***Security Operation Center; Cybersecurity; Intellectual Property,; Organization; Technology***

I. INTRODUCTION

The term Security Operation Center (SOC) is defined as a program which helps to brought together the capacities occur inside the organization. This organization aid in controlling and managing the individuals. Furthermore, provide technology to proceeds with monitoring and improve the posture of security to predict, prevent, investigation and responding or retorting of the cybersecurity (Tafazzoli & Garakani, 2016). Furthermore, Information Technology (IT) is found to be the foundation of SOC. It incorporates with the IT system, inside the organization including devices, networks, information and appliances. SOC is the term which is found associated with each occasion in the organization. The fundamental objective of SOC is to ensure the organization intellectual property, business structure and system, brand integrity and individual information. SOC is having authentic and well-known understanding about the cybersecurity work process and tools. The group of SOC should pay consideration over the latest upgrade's settings, steps towards recognizing the cybercrime and its danger (Tafazzoli & Garakani, 2016). SOC team should pay focus to make a move on attacking or on the individuals who misuse organization Information Technology infrastructure. This can be done by means of refreshing firewall polices, whitelisting, patching, fixing system weakness and securing the SOC applications.

A. *Problem Statement*

SOC is comprising of many purposes and capacities. The work process occur in SOC must be line up with all the process arrangements, technologies and individuals for yielding remarkable outcomes (Kwon, et.al., 2018). Furthermore, it is found that majority of SOC's are assembling or stacking on single function of SOC because of numerous motives and aims. Variation occur in SOC due to services provided by different organizations. Different organization provide different applications and resources in result variation occur.

B. *Objectives of the study*

The objectives of the study are as follows:

1. To prevent, analyze, detect and respond to cybersecurity, as well as to identify the functions for improving the security posture considered under the consideration of SOC.

2. To protect the security operations for different organizations in terms of personal data, intellectual property, and brand integrity and business system.
3. To state the roles and responsibilities for informing technological requirement for SOC.
4. To identify threat intelligence and challenges for reaching an effective or good maturity level in SOC.

II. LITRATURE REVIEW

A. Efficient SOCs use security automation

By means of utilizing exceptionally talented security experts together with security automation, organizations can examine greater security occasions, distinguish more episodes and ensure against them more adequately (Cantatore, & Crawford-Spencer, 2018).

B. Use of effective technology

It is found that the capacities of SOC are reliant on its innovation abilities. Furthermore, innovation should gather and total information, forestall dangers, and react as they happen. A group that is outfitted with instruments and information sources that lessen bogus positives to a base can amplify the time investigators spend examining genuine security occurrences (García-Peñalvo, & Durán-Escudero, 2017).

C. Be up to date with current threat intelligence

Risk information from inside the organization related to data from outer sources gives understanding into vulnerabilities and dangers to the SOC team. Outer digital knowledge incorporates signature refreshes, news channels, reports, alarms, and briefs of risk. SOC staff can use SOC observing instruments that give incorporated risk insight (Cantatore, & Crawford-Spencer, 2018).

D. People and responsibilities

Organizations regularly share authoritative obligations across backups, between accomplice organizations, and specialty units. The organization's security approach norms ought to be utilized to characterize duties corresponding to assignments and responsibility for a reaction. An organization can likewise characterize the job of every specialty unit or organization corresponding to the SOC (Shackelford, 2016).

SOC that characterized, assessed and adaptable is recommended for all the advance occurring enterprises to viably screen existing and developing dangers. It is found that 82 percent of SOCs are neglecting to meet these criteria and falling underneath the ideal level of development (García-Peñalvo, & Durán-Escudero, 2017). Furthermore, SOC are exceeding expectations by adopting a fair strategy to cybersecurity that tempers the favorable individuals, procedures and innovations, just as accurately use automation, investigation, continuous checking, and half breed staffing models to build up a develop and repeatable digital barrier program (Cantatore, & Crawford-Spencer, 2018).

E. SOC maturity decreases with hunt-only projects

According to Sjelin & White (2017), the usage of dash groups for the process of finding any doubtful dangers has become a significant pattern in the security business. Furthermore, all those organizations that pursuit groups to their current constant checking capacities expanded their development levels, programs that concentrated exclusively on pursuit groups had an incompatible impact (Shackelford, 2016).

F. Complete automation is an unrealistic objectives or goal

Lack of security highlight worries for security tasks, creation of basic automation part for any effective SOC. For finding dangers despite everything require human analyzation and appraisals for risks need human thinking and perceptive. Furthermore, making it basic that organizations find synchronization among staffing and automation (Spiekermann, & Korunovska, 2017).

G. Focus and goals are more important priority than size of organization

It is stated by Sillaber, et.al., (2018), there is no connection between the size of business and development of its defense against cyber security. Organizations that utilizes security as a serious differentiator, for advertise administration, or to make arrangement with their industry are better indicators of develop SOCs.

H. The functions for improving the security posture for SOC

A SOC is a hierarchical structure that persistently monitor and investigates the security methodology of an organization. The point of the SOC group is to distinguish, break down and respond to cybersecurity dangers utilizing a solid arrangement of procedures and innovation arrangements (García-Peñalvo, & Durán-Escudero, 2017). The SOC staff by and large incorporates administrators, security examiners, and architects who cooperate with authoritative reaction groups to address security issues rapidly. A SOC tracks and investigates movement on servers, endpoints, systems, applications, databases, sites and other innovation frameworks (Cantatore, & Crawford-Spencer, 2018). Its generations give a basic layer of examination expected to search out any unpredictable

movement that could recommend a security episode. While innovation frameworks, for example, IPS or firewalls can forestall essential assaults, human skill is expected to react to genuine incidents (Rogers, & Marres, 2016).
Security information and event management (SIEM) is found to be an answer that engages SOC experts by gathering security information from over the attempt, distinguishing occasions that have security importance and carrying them to the consideration of the SOC team (Eastwood, Klerkx, & Nettle, 2017). Nambisan, (2017), stated that, a cutting edge SIEM places all the important data before security authorities to assist them with distinguishing and relieve occurrences quicker. The SOC team provide guarantee that conceivable security incidents are precisely recognized, guarded against, analyzed explored and made known.

III. Basic Responsibilities of a SOC Team

The responsibilities that the team of SOC is responsible to entertain within any organization are as follows:

A. Implement and manage all tools regarding to the security.

According to Salter, (2018), a SOC group should have innovative items that give knowledge into the organization's security condition. The SOC needs to designate a talented security group that can choose and use the fitting apparatuses for an occupation. The group must assess the proposals requests (RFPs) from sellers, coordination necessities, create arrangement preliminaries and samples (Eastwood, Klerkx, & Nettle, 2017). Basic or fundamental security apparatuses incorporate firewalls, interruption identification, innovation, danger and helplessness the board devices (Salter, 2018). Information trouble anticipation devices, separating advancements, traffic review arrangements, detailing innovation and information examination stages. The SOC may likewise approach undertaking measurable devices that help incident reaction examinations (Barnard-Wills, 2017).

B. Investigate suspicious activities, detection and prevention.

Skopik, Settanni, & Fiedler, (2016), encountered that, with the help of security checking apparatuses, the SOC team investigates all the doubtful program inside IT and its systems. They do this by accepting and investigating alarms from the SIEM, which may contain indications of reduced and related danger insight. Organizations will most likely be unable to overall prevent dangers from entering their system, SOC should correspond and approve cautions. SOC staff can contextualize these occasions inside the system condition of the business and arrange reaction exercises with key staff continuously (Sundaramurthy, et.al. 2016).

C. Reduce downtime

Asghar, Hu, & Zeadally, (2019), found that the organizations need to guarantee their system run with insignificant or occurring no downtime. It was once conceivable to close a mail server tainted by a risk for clean-up. In the present condition the business can't continue down of basic framework, for example, email. The SOC can proactively tell the fitting business partners about genuine security events. Risks are assuaged before security events arrive at key business framework, and on the off chance that they do arrive at basic frameworks, repetition must be set up to guarantee of the business continuity (Sun, et.al. 2018).

D. Security Strategy

SOCs in a perfect world capacity as shared assistance places that offer some incentive to business partners and assist them with meeting their plans. SOCs are useful relations that bring together activities completed by various divisions (Asghar, Hu, & Zeadally, 2019).

E. Audit and compliances

According to Parker, & Brown, (2018), skilled or efficient access to risk data, character and access control information is fundamental for consistence. Organizations utilizes existing documentation to make new documentation for a review. This procedure is inclined to blunders.

IV. Security Operations Centre Roles and Responsibilities in terms of personal data, intellectual property, and brand integrity and business system.

A. Security Analyst

The reaction of security analyst commonly happens in three phases which are found to be risk identification, danger examination and opportune reaction. Security investigators should guarantee that the right organizing is set up and that staff can actualize strategies and approaches (Nese, 2018).

B. Security Engineer/ Architect

They are the individuals who make a security design and work with engineers to guarantee that this engineering is masterpiece and will set example in the advancement cycle. A security designer might be a product or equipment master who considers security angles when structuring data frameworks. They create instruments and arrangements that permit organizations to forestall and react successfully to assaults.

They record methodology and conventions (Mavroeidis, Vishi, & Jøsang, 2018).

C. *SOC manager*

The SOC administrator regulates the program of the SOC group, including hiring, preparing, and the evaluating staff. Many responsibilities incorporate with the creating process, executing emergency correspondence plans, they make consistence reports, review procedure, measure SOC execution measurements, and report on security activities to business innovators (Skopik, Settanni, & Fiedler, 2016).

D. *CISO*

It characterizes the security tasks of the organization. They speak with the executives about security issues and supervise consistence assignments (Mavroeidis, Vishi, & Jøsang, 2018).

V. The Three-Level SOC Analyst Hierarchy

Tier 1 Support Security Analyst: it gets and investigates alerts day by day surveys the latest SIEM cautions to see their urgency and importance. Tier 2 Support Security Analyst: Skopik, Settanni, & Fiedler, (2016), addressed that, genuine security occurrences. Assesses occurrences distinguished by level 1 experts. Completes inside and out danger knowledge examination to discover the culprit, the sort of assault, and the information or frameworks affected. Makes and executes a technique for control and recuperation. Tier 3 Security Analyst: Powerlessness assessments and entrance tests to survey the strength of the organization and to segregate zones of shortcoming that need consideration. Audits alarms, risk insight, and information security (Mavroeidis, Vishi, & Jøsang, 2018).

A. *Response Manager*

According to Nese, (2018), manages and organizes activities during disengagement, investigation, and control of an incident. They additionally impart any exceptional basics of high seriousness incidents to both interior and outer partners.

B. *Threat intelligence and challenges for reaching an effective or good maturity level in SOC.*

There are number of challenges faced by the team of security operation including exhausted environment, short-staffed and regular base consideration increasing from higher administration. By means of best practices security operations can provide all the elements which an organization require for the purpose of protection (Kokulu, et.al. 2019). This offers SOC team to work in improved and well environment. The use of security automation and analysts give the organization opportunity to encounter more security incidents, events and get preventions from all threats. SOC abilities are highly dependent upon its technology modification (Tounsi, & Rais, 2018). The information to encounter threat attain from the internal sources of the organization which is co-related to data or information gathered from the external sources gives understanding about the vulnerabilities, susceptibilities and dangers to the SOC team. For attain the knowledge of threats SOC team can use checking devices which are completely incorporated for this purpose (Sillaber, et.al. 2018).
Organization frequently using or mutualizing all the responsibilities across backups with the organization. The security arrangement of organization and principles must be utilized to characterize duties corresponding to errands and responsibility for a reaction (Kokulu, et.al. 2019). Miter ATT&CK provide open information which is based on the strategies and procedures dependent on genuine perceptions related to the cyberattacks. In appearance they are in lattices form that are organized by means of attack stages, from beginning framework access to information crime or machine control (Madzibane, 2018). There are lattices for basic work area stages Linux, macOS and Windows just as portable stages (*More information*: https://attack.mitre.org/matrices/enterprise/). Utilizing ATT&CK for this individual reflection will assist you with progressing in the realm of cybersecurity. Miter ATT&CK represents antagonistic strategies, methods, and normal information (Siegel, & Dorner, 2017). For the accomplishment of goals, the attackers would use multiple tactics, as it is found to be more progressive and effective. It also provides less possibility to disclosure (Sillaber, et.al. 2018).

VI. Research Methodology

A. *Research Design*

A research conducted by Savela, (2018), presented that the design of the research has the most prominent value in the process of investigating a research topic. In addition, the design of the research can support the nature of selected subject by means of employing information in the appropriate context. In this regard, it is mandatory for the researcher to select the research design accordingly. Generally, there are many types of research design including exploratory, descriptive and explanatory are used in different types of research to fulfil the requirements of the study. In exploratory research design preference is given to meet the requirements of research topic (Queirós, Faria, & Almeida, 2017). In addition, it relies on secondary data and outcomes are not supported with the primary findings. This affects the authenticity of the research design. However, the aim and objectives of the study does not require any sort of primary data, as the goal is to explain and state improvements in SOC therefore, the research design is most suitable for fulfilling the research needs in the context. According to Rahman, (2017), exploratory research design is keen to collect primary data as well as secondary data while, it depends on the nature of the study and requirements of the subject. Meanwhile, there is no such requirement for the study therefore, the influence of primary data us not admired in the research. In addition, this is not influencing the outcomes of the research. The main weakness of the research design is it avoids the involvement of social science phenomenon and real cases (Flick, 2018). This was the main and fundamental reason for not selecting exploratory research design for the topic, as it requires consideration over the challenges faced by the organizations regarding SOC.

B. Research Approach

Mackey, & Bryfonski, (2018), stated that research approach can be classified in three categories, this includes quantitative research approach, qualitative research approach and mixed method research approach. In this research, elements of qualitative research approach are employed. According to DeCuir-Gunby, & Schutz, (2018), subjective data is incorporated through qualitative research approach, it allows the researcher to focus on the secondary sources and past publication studies. The information collected through this approach is considered as secondary, however, the outcomes are obtained through evaluation of primary and secondary data. While, theoretical approach is preferred in this study for managing the authenticity of information collected, however, the element of reliability in terms of primary data is opted in the investigation. According to Bengtsson, (2016), authentic information is obtained by a researcher by means of quantitative approach. In addition, quantitative approach focuses on the information corresponding to the nature of primary sources and numeric data for the verification of hypothesis designed. The research is highly admired due to effective and accurate results; however, it is not suitable for the phenomenon of cybersecurity and comparing the trends of SOC in recent times. It is stated by DeCuir-Gunby, & Schutz, (2018), quantitative approach is not suitable for conducting research on social, business and medical science subjects. For accomplishing both the factors i.e. authenticity and reliability researchers consider mixed method research approach. The approach is flexible for approaching objective and subjective information in terms of collecting and analyzing the information. However, the approach contains complex mechanism and it is considered as a time-consuming process therefore, it is not used in the current study. In this regard, for protecting the personal data, intellectual property, brand integrity and business system of the organization qualitative research approach is employed.

C. Method(s) and Tool(s) of Data Collection

According to Reilly, & Jones III, (2017), it is a worldwide accepted concept and belief that data is collected through two types of methods that are known as primary and secondary methods of data collection. In real mean, data that is collected as firsthand is primary data and data that is already used in the existing studies is secondary data. The process by which data is collected are known as data collection tools, however, there are different sources and tools for collecting both types of data. For instance, primary data is collected through survey questionnaire, experiments and interviews, while, secondary data is collected through using the existing studies, peer-reviews, e-books, newspaper, commercial reports, articles and previous publications relevant to the topic of research (Mackey, & Bryfonski, 2018). The selection of the data collection tool depends on the needs of topic; however, it was mentioned earlier that the research topic requires to focus on the inclusion criteria that can be obtained through the assistance of secondary data sources. Therefore, in this presented research qualitative research approach is used with descriptive research design and interpretivism philosophy for collecting and analyzing secondary data. Specifically, the secondary tools used in the study are reports, e-books, previous publications, websites and articles.

D. Method(s) of Data Analysis

Pham, (2018), stated that there are several methods used by the researchers for data analysis. However, preference to the method of data analysis is given based on researchers experience and method of data collection. Mainly, the methods of data analysis are categorized in the form of qualitative and quantitative methods. The integration of quantitative method is required for analyzing the information to meet the objectives and hypothesis of the study. However, it is one of the well-known process to measure the subjectivity and objectivity of the research through analyzing the numeric data. The techniques used in this data analysis method are software, this includes e-views, SPSS, Stata, excel or forms of regression. In addition, it follows inferential, coding and inferential & descriptive statistics for analyzing the primary information collected by the researcher (Savela, 2018).
However, the method of analyzing information is really time consuming and difficult to address by the researcher. Secondly, it prefers analysis of primary and secondary data. In this regard, the method of data analysis suitable for this research study is qualitative method. There are two method two analyze information in qualitative data analysis, this includes content and thematic analysis (Pham, 2018). In this presented study, there are no themes designed, on the other side it is essential to analyze information for ensuring that the objectives are accomplished. Therefore, content analysis method is selected for analyzing the secondary information collected. Interpretation of the collected data from various sources is made based on relevant sources that answered the research questions.

E. Ethical Considerations and/or Limitations

In every research, there are several issues regarding ethical consideration are faced and handled by the researchers. However, the effectiveness of the results obtained from a research are based on the actions taken by the researcher for entertaining ethical consideration. The key limitation for this research study was time, initially it was difficult to systematically handle the project for collecting and organizing the data. However, schedules were made later for completing specific parts of the project and handling the process of data collection. To avoid the issue of limited results, attention was given to authentic and reliable sources. Mainly, attention was given to variety of literature gathered for fulfilling each objective. There is no primary data or statistical information used in the evaluation which is considered as a limitation for accurate outcomes.

VII. Findings and Results

The term confidentiality is defined and understood from the literature review as the procedure by which individual control and finds a serviceable bound. Integrity is characterized as the assurance that information and tasks both are changed particularly in a predefined and affirmed way. Availability is the affirmation that endorsed customers have proceeded with access to information and resources. All the additional information on assurance issues and checking the outcomes of an unpremeditated audit of business security authorities is given in the two area appendixes. The prerequisites may be focused on separately in various applications. The analysis of the content states that the approaches to distinguish, investigate, react and forestall cybersecurity dangers depends on the earth of SOC. It is educated that cautious arranging is required for considering and structuring the design of physical security in the activities focal point of organizations. Be that as it may, the structuring ought to be founded on the utilitarian abilities of the operational prerequisites and must be agreeable to guarantee each issue is tended to.

Similarly, the content analysis of the studies selected presents that the control and effectiveness of the SOC territories is relied upon to comprise the administrator's workplaces and war room in each situation. Interestingly with the mechanical necessities, the elements of security stance can be improved through individuals and procedures of the organization. In the light of the literature review it is comprehended that the structure inside which any of the organization give its activity to address its prerequisites or issues with the end goal of data security are named as security strategy. A security technique is a succinct articulation, by those which are at risk for system, information regards or qualities, confirmation commitments, and positioned obligation. It is informed by the content evaluation that the administration of jobs and duties is significant right now, control room must comprise of cutting-edge hardware for satisfying the necessities of assignments appropriately. On the other side, the review of literature estimates that may shield people from doing unapproved things can't shield them from doing things that their movement limits qualify them for do. Right now, expect or anticipate infringement of trust instead of basically fix the mischief that results. One must depend essentially upon human consideration regarding what others in an affiliation are doing. Indeed, even an in-reality sound structure with taught and mindful organization and customers cannot be freed from each possible defenselessness

SOC gathering should have inventive things that give information into the affiliation's security condition. The SOC needs to assign a gifted security bunch that can pick and utilize the fitting mechanical assemblies for an occupation. Analysis of the content expresses that the state of information ought to be checked and approved by methods for basic technique for honesty interlined with the elements of SOC for the specific organization. The danger of releasing individual information, business reports and protected innovation influences the believability of the organization just as brand respectability. The strategies of information security must contain information arrangement, consents the board, get to the executives, personality the board, security investigation and danger location. Literature review presented the notion that essential or key security devices join firewalls, interference ID, development, peril and vulnerability the board tools. Data inconvenience expectation tools, isolating headways, traffic audit game plans, specifying advancement and data assessment stages. The SOC may in like manner approach undertaking quantifiable tools that help occurrence response assessments. It is informed by the analysis of the content that malevolent demonstrations are considered as one of the best risks to the brand protection which is caused because of human mistake. Data is moved to the programmers from the finish of client or client tools, access of the client is devastated by the programmer in the wake of sharing the data. In the light of the literature review, assistance of security checking contraptions, the SOC bunch examines all the farfetched program inside IT and its frameworks. They do this by tolerating and exploring cautions from the SIEM, which may contain signs of decreased and related threat knowledge. Organizations will no doubt be not able to generally be speaking keep threats from entering their framework, SOC ought to relate and affirm alerts. SOC staff can contextualize these events inside the framework state of the business, and mastermind response practices with key staff consistently

It is informed by the analysis of the content that the inclination of the activities is underestimate if the exhibition of the staff isn't sufficient. Reaction arrangement are required from the organizations for esteeming the venture and difficulties that are looked in the procedures. It is the duty of the security activity group to comprehend the earth of cybersecurity and stress on the profile organization to catch and present the centrality of cybersecurity. Esteeming the point of convergence of SOC builds the operational productivity of the group and lessens issues in the game plan.

On the other side, the review of literature states that the response of security investigator usually occurs in three stages which are hazard distinguishing proof, peril assessment and advantageous response. Security agents should ensure that the privilege getting sorted out is set up and that staff can complete techniques and approaches. The content analysis of the studies selected presents that the administration of jobs and obligation requires examination for the apparatuses and exercises which expands security the board position. The systems of the security framework require apparatuses alongside the mindful colleagues. Be that as it may, the principal obligation of any SOC group is to keep up cloud foundation which is conceivable through the log examination and SIEM apparatuses. Ramifications of tasks must be tended to by the security observing group to state and manage genuine ramifications. It is comprehended from the review that potential suspicious exercises that can influence the activities of the frameworks and systems must be routed to give alarms. A security architect may be an item or hardware ace who gives explicit thought to security edges while organizing information systems. They make instrument and game plans that grant relationship to hinder and respond effectively to ambushes. They record philosophy and shows. It is informed by the analysis of the content that administration of the apparatuses is the duty of the security engineer, it is basic to refresh the framework and create practice stage for the architects. Be that as it may, security engineers are likewise liable for growing right mechanical assets, conventions and methodology. On the opposite side, the literature survey educated that the SOC director controls the program of the SOC gathering, including enlisting, getting ready, and the assessing staff. Numerous duties join with the making procedure, executing crisis correspondence plans, they make consistence reports, survey strategy, measure SOC execution estimations, and report on security exercises to business trend-setters.

Various difficulties looked by the group of security activity including depleted condition, short-staffed and normal base thought expanding from higher organization. By methods for best practices security tasks can give all the components which an organization require with the end goal of assurance. The content analysis of the studies selected presents that Miter ATT&CK is equipped for managing utilization of risk knowledge, it uses to respond with the watched action of aggressors by gathering information from the security activity focus. The safeguards structure high need cautions for settling the episodes involving decoding. Mix of high hazard movement expresses the likelihood of making sure about the digital guard condition, it guarantees strategical arrangement of dangers. Right now, imminent and strategies of aggressors are mapped to consider by methods for the Miter ATT&CK systems. On the opposite side, the literature review stated that the standard language of Miter ATT&CK is utilized right now sorting out and choosing the methods. Exact and point by point infiltration plans are utilized to educate displaying for this present reality assailants. The data to experience risk accomplish from the inward wellsprings of the organization which is co-identified with information or data accumulated from the outside sources gives understanding about the vulnerabilities, susceptibilities and risks to the SOC gathering. For achieve the information on dangers SOC group can utilize checking tools which are totally consolidated for this reason. It is informed by the analysis of the content that the procedure keeps up consistency in the exercises to guarantee believability in testing results. Red team entrance testing is another approach to adapt up to the dangers and difficulties to SOC. An agenda is should have been planned by each organization for assessing the everyday errands and really testing the scientific categorization of dangers. The literature educated that organization much of the time utilizing or mutualizing all the obligations across reinforcements with the organization accomplice. The security plan of organization and standards must be used to describe obligations relating to tasks and duty regarding a response. Miter ATT&CK give open data which depends on the systems and strategies reliant on authentic recognitions identified with the cyberattacks. In appearance they are in cross sections structure that are sorted out by methods for assault stages, from starting system access to data wrongdoing or machine control. The content analysis of the studies selected presents that the SOC and blue team includes ground-breaking use case to effectively and quickly evaluate the manifestations of assault. BAS offers mechanization and operationalize reaction to the product stages structured through Miter ATT&CK system. It uncovered issues and vulnerabilities at run time for testing the creation condition.

VIII. Conclusions

The term Security activity focus is characterized as a framework or organization which serves to unite the limits happen inside the organization. It consolidates with the IT framework, inside the organization including tools, systems, data and machines. The aim of the study is to protect the personal data, intellectual property, brand integrity and business system of the organizations. The research relied on the inclusion criteria which is supported through secondary data collection sources.

The security activities for each state and region can be ensured ordinarily through securing accessibility, policies and privacy of data resources. The normal condition of dangers distinguished from the exploration influencing the brand protectionincorporates; human mistake, malware, unintended exchange blunders, security blunders, cyberattacks, insider dangers and traded off equipment. By and large, there are different norms and approaches intended for managing such issues, for example, the gauges of ISO 27001 contains viable procedure to experience elements of data security the executives. Organizations can structure their own models like; resource the board, get to control, business progression, consistence, interchanges security, cryptography, episode reaction, HR security, physical and natural security, operational security and provider connections for dealing with the capacities and activities productively.

The most significant preferred position of SOC is that it centers on the area event of security by methods for determined examination and seeing of the data. Examining and breaking down the activity of organization by methods for frameworks or systems, servers, endpoints and database. Data about each moment or second enables the security activity to focus to experience all the cautious occurrences with the source, day, time, date and sort of assault. SOC can helps in recognizing would be or each conceivable assault by methods for learning component which is causing assault and what is its source with its data structure. Organizations that are having SOC can without much of a stretch experience any defects in their IT structures.

REFERENCES

[1] Almeshekah, M. H., & Spafford, E. H. (2016). Cyber security deception. In *Cyber deception* (pp. 23-50). Springer, Cham.

[2] Ariffin, T. A. B. M. T., & binti Shahidan, S. (2018). Cyber Defense Competition and Information Security: The Red Teaming Exercise Implementation to Resolve Skills and Techniques with Cyber Range Concept. POLITEKNIK JAMBI, INDONESIA 16 OCTOBER 2018, 24.

[3] Asghar, M. R., Hu, Q., & Zeadally, S. (2019). Cybersecurity in industrial control systems: Issues, technologies, and challenges. *Computer Networks*, *165*, 106946.

[4] Aung, W. P., Lwin, H. H., & Lin, K. K. (2020, February). Developing and Analysis of Cyber Security Models for Security Operation Center in Myanmar. In 2020 IEEE Conference on Computer Applications (ICCA) (pp. 1-6). IEEE.

[5] Barnard-Wills, D. (2017). The technology foresight activities of European Union data protection authorities. *Technological Forecasting and Social Change*, *116*, 142-150.

[6] Bengtsson, M. (2016). How to plan and perform a qualitative study using content analysis. *NursingPlus Open*, *2*, 8-14.

[7] Cantatore, F., & Crawford-Spencer, E. (2018). Effective Intellectual Property Management for Small to Medium Businesses and Social Enterprises: IP branding, licenses, trademarks, copyrights, patents and contractual arrangements. Brown Walker Press.

[8] Crowley, C. (2017). Future SOC: SANS 2017 Security Operations Center Survey. *SANS Institute InfoSec Reading Room*.

[9] DeCuir-Gunby, J. T., & Schutz, P. A. (2018). Critical Race Mixed Methodology: Designing a Research Study Combining Critical Race Theory and Mixed Methods Research. In *Understanding Critical Race Research Methods and Methodologies* (pp. 166-179). Routledge.

[10] Eastwood, C., Klerkx, L., & Nettle, R. (2017). Dynamics and distribution of public and private research and extension roles for technological innovation and diffusion: Case studies of the implementation and adaptation of precision farming technologies. *Journal of Rural Studies*, *49*, 1-12.

[11] Flick, U. (2018). Designing qualitative research. Sage.

[12] García-Peñalvo, F. J., & Durán-Escudero, J. (2017, July). Interaction design principles in WYRED platform. In *International Conference on Learning and Collaboration Technologies* (pp. 371-381). Springer, Cham.

[13] Greenwood, D. A., Gee, P. M., Fatkin, K. J., & Peeples, M. (2017). A systematic review of reviews evaluating technology-enabled diabetes self-management education and support. *Journal of diabetes science and technology*, *11*(5), 1015-1027.

[14] Gupta, N., Traore, I., & de Quinan, P. M. F. (2019, December). Automated Event Prioritization for Security Operation Center using Deep Learning. In 2019 IEEE International Conference on Big Data (Big Data) (pp. 5864-5872). IEEE.

[15] HÁMORNIK, B. P., & KRASZNAY, C. (2017). Prerequisites of virtual teamwork in security operations centers: knowledge, skills, abilities and other characteristics. *Academic and Applied Research in Military and Public Management Science*, *16*(3), 73-92.

[16] Hámornik, B. P., & Krasznay, C. (2017, July). A team-level perspective of human factors in cyber security: security operations centers. In *International Conference on Applied Human Factors and Ergonomics* (pp. 224-236). Springer, Cham.

[17] Han, J. W., Hoe, O. J., Wing, J. S., & Brohi, S. N. (2017, December). A conceptual security approach with awareness strategy and implementation policy to eliminate ransomware. In Proceedings of the 2017 International Conference on Computer Science and Artificial Intelligence (pp. 222-226).

[18] Hull, J. L. (2017). Analyst burnout in the cyber security operation center-CSOC: A phenomenological study (Doctoral dissertation, Colorado Technical University).

[19] Jahankhani, H., Carlile, A., Emm, D., Hosseinian-Far, A., Brown, G., Sexton, G., & Jamal, A. (Eds.). (2017). Global Security, Safety and Sustainability: The Security Challenges of the Connected World: 11th International Conference, ICGS3 2017, London, UK, January 18-20, 2017, Proceedings (Vol. 630). Springer.

[20] Jansen, C. (2017). Stabilizing the Industrial System: Managed Security Services' Contribution to Cyber-Peace. IFAC-PapersOnLine, 50(1), 5155-5160.

[21] Kokulu, F. B., Soneji, A., Bao, T., Shoshitaishvili, Y., Zhao, Z., Doupé, A., & Ahn, G. J. (2019, November). Matched and Mismatched SOCs: A Qualitative Study on Security Operations Center Issues. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security* (pp. 1955-1970).

[22] Kwon, T., Song, J. S., Choi, S., Lee, Y., & Park, J. (2018, August). VISNU: A novel visualization methodology of security events optimized for a centralized SOC. In 2018 13th Asia Joint Conference on Information Security (AsiaJCIS) (pp. 1-7). IEEE.

[23] Le, N. T., & Hoang, D. B. (2017). Capability maturity model and metrics framework for cyber cloud security. Scalable Computing.

[24] Mackey, A., & Bryfonski, L. (2018). Mixed methodology. In *The Palgrave Handbook of Applied Linguistics Research Methodology* (pp. 103-121). Palgrave Macmillan, London.

[25] Madzibane, S. S. (2018). Development of a Systems Front End Research Framework to inform strategic planning of projects in transnet SOC Ltd (Doctoral dissertation).

[26] Marx, G. T. (2016). Windows into the soul: Surveillance and society in an age of high technology. University of Chicago Press.

[27] Mason, A. (2018). Protection of Intellectual Property of the Plant Continuity through IT/OT Cyber Security Measures and Governance into Industrial Automation & Control Systems (Doctoral dissertation, The George Washington University).

[28] Matsumura, N., & Tago, A. (2019). Negative surprise in UN Security Council authorization: Do the UK and French vetoes influence the

general public's support of US military action?. Journal of Peace Research, 56(3), 395-409.

[29] Mavroeidis, V., Vishi, K., & Jøsang, A. (2018, August). A framework for data-driven physical security and insider threat detection. In *2018 IEEE/ACM International Conference on Advances in Social Networks Analysis and Mining (ASONAM)* (pp. 1108-1115). IEEE.

[30] McLean, L. (2019). U.S. Patent Application No. 15/809,273.

[31] Miloslavskaya, N. (2016, August). Security operations centers for information security incident management. In 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud) (pp. 131-136). IEEE.

[32] Moss, M. (2016). The Advantages and disadvantages of mixed methodology research. *Demand Media. Retrieved on*, *20*(04), 2015.

[33] Nambisan, S. (2017). Digital entrepreneurship: Toward a digital technology perspective of entrepreneurship. *Entrepreneurship Theory and Practice*, *41*(6), 1029-1055.

[34] Nese, A. (2018). Improving Security Posture by Learning from Intrusions (Master's thesis, NTNU).

[35] Onwubiko, C., & Ouazzane, K. (2019, June). Cyber Onboarding is 'Broken'. In 2019 International Conference on Cyber Security and Protection of Digital Services (Cyber Security) (pp. 1-13). IEEE.

[36] Parker, A., & Brown, I. (2018, August). Skills Requirements for Cyber Security Professionals: A Content Analysis of Job Descriptions in South Africa. In *International Information Security Conference* (pp. 176-192). Springer, Cham.

[37] Pham, L. T. M. (2018). Qualitative Approach to Research A Review Of Advantages and Disadvantages Of Three Paradigms: Positivism, Interpretivism And Critical Inquiry. *University of Adelaide*.

[38] Policy, I. P. A., Tagging, P., & Policy, Q. A. (2018). Associate Lab Directorate (ALD) Area Burden Costs. *Policy*, *9*, 10.

[39] Policy, I. P. A., Tagging, P., & Policy, Q. A. (2018). Financial Management System (FMS) User Access Control. *Policy*, *3*, 29.

[40] Queirós, A., Faria, D., & Almeida, F. (2017). Strengths and limitations of qualitative and quantitative research methods. *European Journal of Education Studies*.

[41] Rahman, M. S. (2017). The Advantages and Disadvantages of Using Qualitative and Quantitative Approaches and Methods in Language" Testing and Assessment" Research: A Literature Review. *Journal of Education and Learning*, *6*(1), 102-112.

[42] Reilly, T. M., & Jones III, R. (2017). Mixed methodology in family business research: Past accomplishments and perspectives for the future. *Journal of Family Business Strategy*, *8*(3), 185-195.

[43] Rittinghouse, J. W., & Ransome, J. F. (2016). Cloud computing: implementation, management, and security. CRC press.

[44] Rogers, R., & Marres, N. (2016). Landscaping climate change: A mapping technique for understanding science and technology debates on the World Wide Web. *Public Understanding of Scien*