Electrical Science & Engineering
https://ojs.bilpublishing.com/index.php/ese

ARTICLE

Cyber Security Professionals' Challenges: A Proposed Integrated Platform Solution

Mohammed Daffalla Elradi*   Khalid Abass Abdelmajeed   Mutaz Osman Abdulhaleem

Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan

ARTICLE INFO

Article history
Received: 16 June 2021
Accepted: 30 July 2021
Published Online: 09 August 2021

Keywords:
Cyber security
Threat
Intelligence
SOC
IR

ABSTRACT

As cyber threats and attacks are immensely increasing and broadly spreading catastrophically worldwide, cyber security professionals need to cope up with such a highly demanding environment. Security teams, such as Security operation Centre (SOC), Incident Response (IR) and Threat management teams are the people responsible for dealing with cyber security threats and attacks from detection to containment and preventing future incidents; which encompasses some significant challenges that might impose some limitations to the efficiency and effectiveness of activities cyber security professionals conduct, as these processes are time-consuming. In this paper we propose an integrated platform to help cyber security professionals to proactively manage cyber security threats and emerging incidents by providing an automated functionality that can optimize the workflow. The proposed security platform is supposed to diminish the average time taken by cyber security professionals to respond to cyber incidents with an average of 42%. This study can be used as a preliminary design for such an integrated platform.

1. Introduction

Cyber security threats and attacks have been rising scaringly in the last few years, as a result; the need for a sophisticated approach to collect and trace threat actors has become an essential prerequisite to investigate and counter threats and cyber security incidents [1]. Security Operations Centre (SOC) and Incident Response (IR) teams are required to keep well aligned with the rapidly-evolving cyber threats and attacks or they might find themselves at the verge of being catastrophically exploited.

As attackers tend to reuse similar tactics and almost the same resources across multiple attacks, threat hunting and sharing Cyber Threat Intelligence (CTI) can greatly be beneficial in investigating, mitigating and even defending cyber-attacks [2].

Threat intelligence (TI) can be referred to as a proof-based knowledge, it involves collecting mechanisms, evidences, indicators and actions to be taken for a robust and rapid incident response to form a preventive measure in advance [3]. Threat Intelligence greatly helps cyber security professionals to prevent cyber-attacks and precedingly identify those attacks, which as a result expands the visibility towards the highly-evolving threat landscape [4].

1.1 Indicators of Compromise

Indicators Of Compromise (IOCs) are forensic artifacts that are used to indicate that a system has been compromised or infected with a sort of malware [5]. IOCs are

**Corresponding Author:*
Mohammed Daffalla Elradi,
Communication Systems Engineering Department, University of Science and Technology, Khartoum, Sudan;
Email: mohd_daf_elradi@hotmail.com

DOI: https://doi.org/10.30564/ese.v3i2.3376

composed of a combination of Ips, URLs, domain names and virus signature. Collecting IOCs immensely helps to indicate with a high-level of precision if a system has been compromised or not and then these IOCs are deployed on security tools for the purpose of investigation [6].

There are miscellaneous types of compromise indicators upon which IOCs can be classified, which are: computed, behavioural and atomic indicator respectively [7]. They will be discussed briefly below.

1.1.1 Computed indicators

Mainly developed from materials involved in the incident, an example is the hash of a malicious file.

1.1.2 Behavioural indicators

They combine other indicators in order to create an overall profile of the targeted malicious behaviour. They adopt some behavioural indicators that are observed from individual or collective incident response action against attackers' activities. Such behavioural indicators are often referred to as attacker's tactics, techniques and procedures.

1.1.3 Atomic indicators

They are fragments of data that individually indicate suspicious activity. Fully-Qualified Domain Name (FQDN), IP address or email address is an example. However, atomic indicators need further investigation as they might not necessarily indicate an adversary activity.

1.2 Security Operation Centre (SOC) Team

SOC is primarily a group of security analysts who are required to detect, analyze, respond to, report on and prevent cyber security emerging incidents. Soc teams are likely to deal with data feeds from various sources like Intrusion Detection Systems (IDS), security audit logs and others. In case of emerging incident, there is a process of sorting, categorizing and prioritizing incoming events, which is referred to as triage. Soc team is segmented into tiers as will be described briefly below.

1.2.1 Tier 1 Security Analyst

Monitors alerts and their triage, runs vulnerability scans and escalate incidents to Tier 2 security analyst, known as Triage Specialist.

1.2.2 Tier 2 Security Analyst

Deals with the escalated incidents, influences threat intelligence IOCs, collects data for further investigation and conduct recovery attempts, known as Incident Responder.

1.2.3 Tier 3 Expert Security Analyst

Conducts penetration testing to identify system breaches, validates resilience and fix these vulnerabilities. Known as Threat Hunter.

1.2.4 Tier 4 SOC Manager

Supervises the SOC team activities, manages the escalation process, reviews incident reports and prepares Disaster Recovery (DR) plans.

1.3 Incident Response Team

Is a group of cyber security analysts, who are responsible for planning and responding to cyber threats and attacks, observing system vulnerabilities and developing incident response plan to mitigate the impacts imposed by a threat and remediate it as quickly as possible to keep systems running in an ordinary condition.

1.4 Threat Team

Responsible for proactively looking for and hunting cyber threats by recognizing their potential effect and also figuring out the behaviour adopted by threat actors, so it can facilitate the process of identifying a threat in their environment.

2. Literature Review

Many studies have been conducted regarding cyber security threats, attacks, incident response, mitigation procedures and how to defend cyber-attacks. Security Operation Centre (SOC) teams represent the first line of defence as they are anticipated to detect threats and escalate them to Incident response (IR) teams [8]. Although many researches highlighted SOC, many of them had lacked a thorough overview of the challenges that might face SOC teams as observed from [9,10].

In [11], a survey was conducted to highlight some major areas that SOC teams should focus on to increase the efficiency and effectiveness of security operations. SOC teams perform advanced forensic analysis on artifacts. However, the extent to which they can automate the process of analysis is limited [12].

A major concern for cyber security professionals is the increasingly complicated security environment, as organizations tend to implement cyber security technologies and services from different providers. That adds a considerable difficulty for teams to handle incidents within an acceptable time interval. Also, taking into consideration

DOI: https://doi.org/10.30564/ese.v3i2.3376

the massive volume of workload that cyber security professionals are confronted with leads to an overwhelm.

Cyber security threats need to speed in action to deal with, but this speed requires vision. This vision is complemented by real-time threat information sharing, which will not only provide a thorough vision for how to react to cyber threats but also anticipating approaches to overcome them [17].

SOC analysts form kind of familiarity with their constituency as well as relevant cyber threats, which in return brings them to a more sophisticated mastery over time. Also, staff attrition can be a mishap and affect the overall performance of SOCs. Hence, it should be diminished as possible.

3. Method

In this paper we intend to highlight the challenges that most of the cyber security professionals face in response to cyber threats and attacks. As they are inclined to extremely rapid response time due to the sensitivity of their environment which might lead to catastrophic impacts if not swiftly contained. Some of the challenges will be discussed below.

3.1 Cyber Security Professionals' Challenges

Cyber security professionals including SOC teams, IR teams and Threat teams are required to identify, analyze and react to cyber security threats using a reliable set of processes and solutions. Hence, there are many challenges that most cyber security professionals face, which are depicted in Figure 1 below.

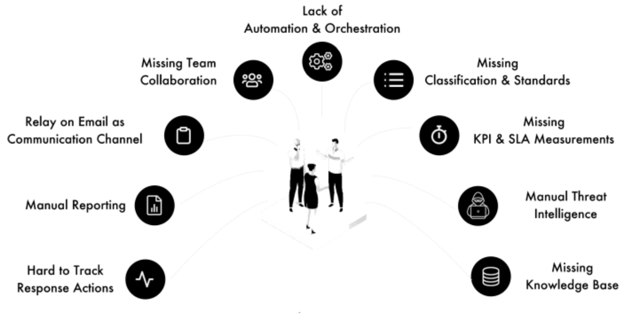
Lack of Automation & Orchestration
Missing Team Collaboration
Missing Classification & Standards
Relay on Email as Communication Channel
Missing KPI & SLA Measurements
Manual Reporting
Manual Threat Intelligence
Hard to Track Response Actions
Missing Knowledge Base

Figure 1. SOC team challenges.

As shown in Figure 1, the challenges that SOC teams confront, which will be discussed briefly as follows:

3.2 Lack of Automation & Orchestration

Cyber security professionals suffer from the difficulty of the process of reporting cases, escalating incidents, collecting IOCs, and imitating attacks. All the previously-mentioned processes are merely hard to conduct and yet time consuming, in an environment that requires rapid actions to be taking to tackle threats and counter cyber-attacks. So, the need for automating and providing a comprehensive platform that rhymes all these processes is crucial.

3.3 Missing Team Collaboration

Having a common workspace that can involve the departments responsible for maintaining cyber security and other departments within an organization or even subsidiaries and third-party entities really counts in keeping well-aligned with security measures.

3.4 Relying on Email as a Communication Channel

Most of cyber-attacks are launched using spamming and phishing emails. So, solely relying on emails as a communication channel between cyber security teams can have catastrophic impacts if it has not been seriously considered.

3.5 Manual Reporting

As it had been discussed above, conducting case reporting manually can be such a frustrating process, yet prone to errors and uncertainty and might even be ambiguous.

3.6 Hard to Track Response Actions

Here the ransomware process will communicate with encryption-key servers in order to retrieve the public key needed for data encryption.

3.7 Missing Classifications and Standards

Standards play a pivotal role in cyber security, as they tend to provide a reference point for every counter-measures that should be taken in response to cyber threats and attacks. Example of cyber security standards include but not limited to National Institute of Standards and Technology (NIST), SANS, International Organization for Standardization (ISO), Information Technology Infrastructure Library (ITIL), Information Systems Audit and Control Association (ISACA) …etc.

3.8 Missing KPI and SLA Measurements

Key Performance Indicator (KPI), Key Risk Indicator (KRI) used to indicate how risky an activity is, Key Change Indicator (KCI) used to understand the effectiveness of risk controls and actions taken to mitigate the impacts emerging from risks [8]. These metrics acknowledge strategic and operational improvements by providing analytical basis for decision making.

DOI: https://doi.org/10.30564/ese.v3i2.3376

Also, Service-Level Agreement (SLA) is a key factor in guarantee of high-quality services provided by entities involved in the process of maintaining a trustworthy cyber security environment.

3.9 Manual Threat Intelligence

Threat Intelligence is a mandatory factor in defending and pre-empting prospective cyber-attacks. Taking a step ahead and proactively anticipating attacker's targets and strategies would immensely afford a broad vision for preventing and mitigating future attacks and at the same time significantly strengthen security postures [13]. There are many sources available for obtaining threat intelligence ranging from observing one's own systems, public sources or through paid services [14]. Tracing threat intelligence manually would be time consuming and also imposes a burden of analysis for these collected threat intelligence data which is quite ineffective.

3.10 Missing Knowledge Base

Cyber security knowledge base fundamentally highlights the mandatory cyber security necessities needed for every business and also individually. It is also intended to match the detected security pattern and behaviour against a set of common incidents, threats and vulnerabilities to form a robust mitigation approach to confront the detected threat [15]. Not having the adequate knowledge base would result in more susceptible cyber environment.

Taking the previously-mentioned challenges into consideration and how much benefit that can be brought to a design approach for facilitating the work parameters for SOC teams will be such an accommodating contribution for a resilient cyber security environment.

The results of the proposed integrated solution that can be designed to overcome the barriers that confronts cyber security professionals will be discussed thoroughly in the next section.

4. Result

This section describes the proposed solution for bringing together the best methodologies that can incorporate faster detection, reduced response time, resilient threat intelligence, team collaboration, processes integration, automation and visualization to cyber security teams.

The solution aims at speeding up SOC operation and improving SOC team advancement by providing instant team collaboration platform, where it can be integrated with Security Information and Event Management (SIEM) software, that analyzes activities from miscellaneous resources within the organization and collects security artifacts from network infrastructure.

It also involves notifications for emerging threats, which are automatically triggered. The ability to assign tasks and track actions taken as required by providing a flexible workspace that can involve individuals within the same department, from other departments within the organization or can even include subsidiaries and third-parties while maintaining privileges by assigning roles to limit the contribution level of a participant in any processes. Figure 2 shows the workspace that the proposed security platform can provide.

Workflow process

The proposed platform encompasses a sequenced approach for managing security, which are mentioned in brief as follows:

- **Case**

Is the first level of workflow where a case can be initiated according to some predefined anomaly events.

- **Trigger**

Here, SOC analyst recognizes anomaly triggers.

- **Task**

Response actions are assigned to SOC team.

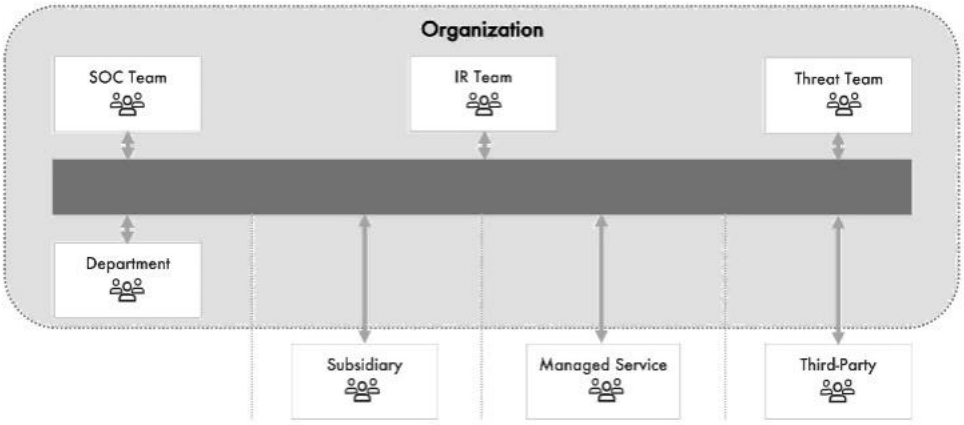

Figure 2. The workspace provided by the proposed platform.

DOI: https://doi.org/10.30564/ese.v3i2.3376

Considering the people, process and technology (PPT) framework, which refers to the methodology in which the balance between the three components of the framework drives action to achieve organizational efficiency [16]. The proposed platform effectively adopts the PPT framework to bridge the gap imposed by the challenges discussed earlier by providing a holistic view of performance boosting mechanisms that are mandatory for optimum detection, rapid response time, team collaboration, visualization and recommendations for future reference. Figure 3 below depicts the PPT framework insights.

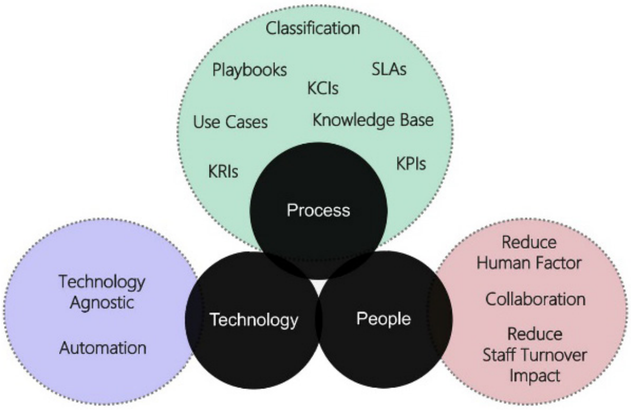

Figure 3. The PPT framework insights.

Our proposed platform will give the full capability to create, assign and fully manage cases and their triage as well as carrying out analytical processes by utilizing the automation technology of Security Orchestration, Automation and Response (SOAR), which allows the collection of data related to cyber threats and respond to cyber security incidents without human interaction.

Also a major contribution of our proposed model is the automation conducted in threat intelligence by automatically checking IOCs in threat intelligence service providers like Virus Total, SHODAN, ALIEN VAULT, Malwarebytes, TaLOS, PAYLOAD SECURITY, ... etc. The operation model is depicted in Figure 4.

5. Discussion

The proposed cyber security integrated platform in this paper is solely intended to facilitate the procedures conducted by SOC teams, starting from creating cases for emerging cyber threats, escalate incidents, responding to those incidents till containment. In addition to team collaboration and tasks assignation.

Having a security system with such capabilities will not only help cyber security professionals to rapidly handle emerging threats or incidents but will also provide a comprehensive cyber security control over an organization and automates some time-consuming procedures which yields to a highly optimized threat and incident management aptitudes and empowers workflow.

The proposed cyber security integrated platform is likely to diminish the time taken by cyber security professionals to detect, report, manage, escalate and mitigate a cyber threat or attack by an average of about 42% as illustrated in Figure 5.

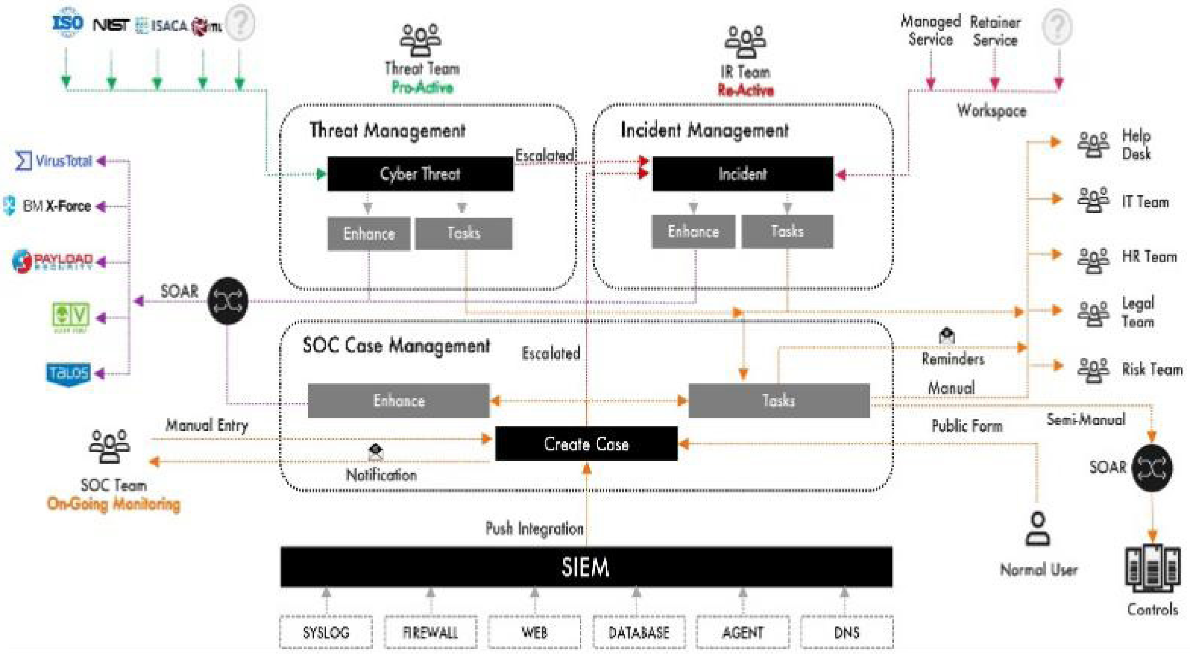

Figure 4. The proposed platform operation model.

DOI: https://doi.org/10.30564/ese.v3i2.3376

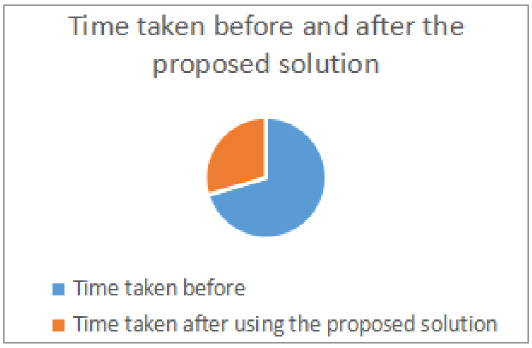

Figure 5. Time taken by cyber security professionals to respond to incidents before and after the proposed solution.

6. Conclusions

In this paper, a comprehensive cyber security platform was proposed to overcome some major challenges that cyber security professionals suffer from, taking into consideration the importance of time as a prominent factor in cyber security environment. Also the sense of automation that empowers cyber security professionals with a fully-rounded set of analytical and holistic view for better response actions.

The results of the proposed platform were quite rewarding as it would minimize the average time needed by cyber security teams to resolve the increasing numbers of cyber threats and attacks by about 42%, which significantly empowers cyber security professionals to keep with such a highly-demanding realm.

It is recommended to conduct further studies to some other challenges and barriers that might degrade or make cyber security teams lag behind. This paper can be considered as a preliminary design for an integrated solution.

References

[1] A. Niakanlahiji, L. Safarnejad, R. Harper and B. Chu, "IoCMiner: Automatic Extraction of Indicators of Compromise from Twitter," 2019 IEEE International Conference on Big Data (Big Data), 2019, pp. 4747-4754. DOI: 10.1109/BigData47090.2019.9006562.

[2] G. Husari, X. Niu, B. Chu and E. Al-Shaer, "Using entropy and mutual information to extract threat actions from cyber threat intelligence", 2018 IEEE International Conference on Intelligence and Security Informatics (ISI), pp. 1-6, Nov 2018.

[3] Definition: Threat intelligence, 2013, [online] Available: https://www.gartner.com/doc/2487216/definition-threat-intelligence.

[4] G. Husari, E. Al-Shaer, M. Ahmed, B. Chu, and X. Niu. 2017. TTPDrill: automatic and accurate extraction of threat actions from unstructured text of cti sources. In Proc. ACSAC 2017, pages 103-112.

[5] B. J. Kwon, V. Srinivas, A. Deshpande, and T. Dumitras. 2017. Catching worms, trojan horse and PUPs: un-supervised detection of silent delivery campagins. In Proc. NDSS 17.

[6] O Catakoglu, M. Balduzzi, and D. Balzarotti, "Automatic extraction of indicators of compromise for web applications," International World Wide Web Conference Committee (IW3C2), Montréal, Québec, Canada, 2016, pp. 1-11.

[7] J. Andress. (2015, May). Working with indicators of compromise. ISSA Journal. [Online]. Available: www.issa.org.

[8] 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.

[9] F. B. Kokulu, A. Soneji, T. Bao, Y. Shoshitaishvili, Z. Zhao, A. Doupé, and G.-J. Ahn, "Matched and mismatched SOCs," in Proc. ACM SIGSAC Conf. Comput. Commun. Secur., New York, NY, USA, Nov. 2019, pp.1955-1970.

[10] B. Hámornik and C. Krasznay, "A team-level perspective of human factors in cyber security: Security operations centers," in Advances in Human Factors in Cybersecurity, vol. 593 D. Nicholson, Ed. Cham, Switzerland: Springer, 2018, pp. 224-236.

[11] Chris Crowley, John Pescatore. Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey. SANS Institute Information Security Reading Room, July 2019.

[12] X. Liao, K. Yuan, X. Wang, Z. Li, L. Xing, and R. Beyah, "Acing the ioc game: toward automatic discovery and analysis of open-source cyber threat intelligence," in Proc. CCS 16, 2016, pp. 755-766.

[13] crowdstrike.com. 2021. What is Cyber Threat Intelligence? [Beginner's Guide]. [online] Available at: https://www.crowdstrike.com/cybersecurity-101/threat-intelligence.

[14] Z. Zhu and T. Dumitras, "ChainSmith: automatically learning the semantics of malicious campaigns by mining threat intelligence reports,"in Proc. EuroS&P 2018, 2018.

[15] IT Exchange. 2021. CyberSecurity Knowledge Bases: The Brain of Security Systems. [online] Available at: https://www.itexchangeweb.com/blog/cybersecurity-knowledge-bases-the-brain-of-security-systems.

[16] Smartsheet. 2021. Complete Guide to the PPT Framework | Smartsheet. [online] Available at: https://www.smartsheet.com/content/people-process-technology.

[17] World Economic Forum. 2021. 4 key challenges for cybersecurity leaders. [online] Available at: https://www.weforum.org/agenda/2020/01/four-key-challenges-for-cybersecurity-leaders.

DOI: https://doi.org/10.30564/ese.v3i2.3376