EDPACS THE EDP AUDIT, CONTROL, AND SECURITY NEWSLETTER

THE STATE OF INFORMATION SECURITY LAW: A FOCUS ON THE KEY LEGAL TRENDS

Thomas J. Smedinghoff

EXECUTIVE SUMMARY

IN THIS ISSUE

EDPACS

The EDP Audit, Control, and Security Newsletter

ISSN: 0736-6981 (Print) 1936-1009 (Online) Journal homepage: www.tandfonline.com/journals/uedp20

SOC Analyst Performance Metrics: Towards an optimal performance model

Samir Achraf Chamkar, Yassine Maleh & Noreddine Gherabi

To cite this article: Samir Achraf Chamkar, Yassine Maleh & Noreddine Gherabi (2023) SOC Analyst Performance Metrics: Towards an optimal performance model, EDPACS, 68:3, 16-29, DOI: 10.1080/07366981.2023.2259046

To link to this article: https://doi.org/10.1080/07366981.2023.2259046

Published online: 20 Sep 2023.

SOC ANALYST PERFORMANCE METRICS: TOWARDS AN OPTIMAL PERFORMANCE MODEL

SAMIR ACHRAF CHAMKAR, YASSINE MALEH AND NOREDDINE GHERABI

Abstract. Security Operation Center represents nowadays an indispensable component of the socio-technical system by supporting businesses to protect their security and ensure the confidentiality, integrity, and availability against cyberthreats and security attacks.The Security Operation Center provides various service levels and capabilities that need to be continuously assessed and tracked to ensure improvement of the main success factor of the SOC, which include technologies, processes, and SOC analysts. SOC analysts' performance evaluation remains problematic due to the choice of the performance metrics and their inadequacy with the SOC socio-technical system. While we have some quantitative and qualitative measures to assess the performance of a SOC analyst, SOC capabilities, and SOC maturity levels, this evaluation is based on root cause analysis and independent evaluation of SOC elements, which is unrealistic, given the complex and evolving nature of SOC systems. However, the baselines of the performance metrics are the SOC challenges announced by the SOC analysts and their ability to face, reduce, and overcome them to provide and maintain a high detection rate of malicious and abnormal behaviors. We provide a comprehensive overview of the challenges faced by SOC analysts based on our previous study, and we provide a deep analysis of the challenges and the interconnexion of those challenges. Furthermore, we present the quantitative performance metrics and their weaknesses to assess the performance of the SOC analysts due to the SOC socio-technical system nature. Our study will enable SOC managers, analysts, and decision-makers to have clear visibility and details on the quantitative performance metrics and will provide a baseline for a new performance metrics model.

INTRODUCTION

A Security Operation Center (SOC) can be defined as a centralized facility covering personnel, processes, and technology dedicated to monitoring, detecting, and responding to cybersecurity threats and incidents within an organization. Its primary purpose is to ensure the confidentiality, integrity, and availability of an organization's data and systems, while also helping businesses to maintain cyber situational awareness, address compliance issues, and threat management (Mansfield-Devine, 2016).

Security Operation Centers (SOCs) can be categorized into several types based on their primary function, scope, and the organizations they serve, and businesses are adopting the services provided by the SOC depending on the available resources, goals, and targeted implementation. Meanwhile, organizations that cannot afford to invest in an SOC rely on third-party service providers or a Managed Security Service Provider (MSSP) to deliver SOC services (Miloslavskaya, 2016).

The SOC serves as a vigilant guardian, functioning as both a proactive and reactive defense mechanism against the ever-evolving landscape of cyber threats, and its continuous performance evaluation and improvement efforts are indispensable for staying ahead of cyber threats, ensuring regulatory compliance, and safeguarding the organization's overall stability and resilience in the face of an ever-changing cybersecurity landscape (Chamkar et al., 2022).

Researchers and cybersecurity experts remain deeply engaged in the ongoing evaluation and improvement of SOC operations due to the role it plays to protect the company's business, which explains the number of articles in the literature to afford SOC metrics and models to asses the performance.

However, the SOC performance metrics need to be continually measured as anything that is not measured cannot be improved. A large portion of the SOC-related research are paying attention to technology and processes with little attention to the SOC analysts as the human factor inside the socio-technical system (Zimmermann & Renaud, 2019).

A literature review revealed a lack of adequate performance metrics for assessing the SOC and the SOC analyst's performances for the continued measurement of the delivered security service for continuous improvement. What can't be measured can't be improved (Sundaramurthy et al., 2014).

This review seeks to shed light on the challenges and the performance metrics in detail, presenting the challenge-performance metric relationship as well as the weaknesses of the actual metrics in use.

We believe that a better understanding of the challenges faced by the analyst will provide a useful insight that SOC managers and stakeholders can use to devise intervention strategies that can improve the performance of analysts. Such understanding may also be of interest to system designers and ergonomist who typically take into consideration multiple humans and environmental factors during system design.

The remainder of this article is structured as follows: we provide an overview of the components of a security operation center and how those components work together. In the second section, we provide a reminder of the SOC challenges from our quantitative and qualitative study conducted with security experts. In the third section, we provide a deep analysis of the SOC challenges followed by the mapping challenge-performance metric and a deep analysis of the metrics in use. In the last section, we provide the criteria and success factors of the performance metrics and the target model in our future work.

BACKGROUND

Setting up and operating a SOC is an expensive adventure, and businesses continually estimate their return on security investment and how to ameliorate the overall performance and quality of the security service delivered by the SOC entity (Agyepong et al., 2020a).

Setting up and operating a Security Operations Center (SOC) is a complex and resource-intensive endeavor that demands a significant financial commitment from businesses.

This venture involves not only substantial financial investments but also the allocation of human resources, advanced technology deployments, and ongoing operational expenses. The goal behind this costly journey lies in the paramount importance of securing an organization's digital assets and sensitive data in today's digital landscape, where cyber threats are continuously evolving (Maleh et al., 2021).

When it comes to assessing the performance of the SOC analysts, the SOC managers and decision-makers rely on the dashboard feeds from the onboarded technologies such as the Security Information and Event Management, Firewalls, antivirus, Intrusion Detection and Prevention Systems (Zimmerman, 2014). Unfortunately, technical-centric approaches often overlook crucial aspects by concentrating solely on the technical dimension. These studies tend to neglect the vital human factors that play a pivotal role in achieving a satisfactory level of monitoring, detection, reporting, and incident response through established playbooks. Additionally, they fail to address the ongoing maintenance of deployed security controls and the decision-making process for distinguishing malicious from non-malicious activities. Ultimately, the potential courses of action based on available resources and their performance become the determining factors when cybercriminals launch their attacks. (Maleh et al., 2020).

Therefore, maintaining a high standard of operational effectiveness and performance is the main SOC analyst's responsibility as a poor operational performance will hinder the overall efficiency of a SOC (Agyepong et al., 2020a). It becomes clear that it is very important to understand the performance metrics for SOC assessment alongside the SOC challenges faced by the human factor, which impact their performance and therefore the whole performance of the SOC. How can we measure the performance of SOC analysts, what are the priorities for these performance metrics, and what constitutes the challenge of mapping actions to these metrics in order to construct a comprehensive performance metric model?

A literature review reveals a lack of pertinent metrics for assessing SOC analysts due to the complexity and interdependent nature of the SOC while taking into account the whole socio-technical system. The present lack of such a review makes this article important by reviewing the challenge-metric mapping and presenting the weaknesses of the actual quantitative-based metrics in use.

Our findings will offer a transparent understanding of the metrics in use, their alignment with challenges, identification of weaknesses, assessment of potential influencing factors on these metrics, and considerations for future efforts in developing a universal performance metric model.

RESEARCH METHODOLOGY

Our research involves evaluating the performance of the SOC and the SOC analysts using several metrics that encompass various aspects of the SOC. Our research methodology consists of several phases. In the first phase, we present the outcome of the first conducted study, which consists of a quantitative and qualitative study using survey-based questionnaires and interviews with 45 participants who are currently working in several internal SOCs and SOC service providers in their various roles and levels of experience to make a holistic view of the challenges from narrative overview.

In the second part, we deeply discuss the challenges announced by the SOC analysts and present the mapping logic of the challenge performance metric.

In the third phase, we present the weaknesses of quantitative and qualitative performance metrics due to the nature of the SOC socio-technical system and propose improvements on the currently used metrics.

In the meantime, we try to answer the following questions:

- What are the most faced challenges by the security analysts from analyst's narrative view?
- What are the performance metrics in use and how are they mapped to the SOC challenges to assess the SOC analyst's performance?
- What are the weaknesses of the performance metrics in use?
- What are the factors impacting the quantitative metrics?
- How can we improve the accuracy of the current performance metrics?

DEEP ANALYSIS OF THE SOC CHALLENGES

In this section, we performed an in-depth analysis of challenges reported by SOC analysts in our survey-based study and interviews with SOC security experts. We will prioritize the top four challenges identified in our research and combine our findings with insights from the literature review to provide a comprehensive understanding of these challenges. This analysis will aid in mapping these challenges to existing SOC assessment models.

Lack of Automation and Orchestration

Automation and orchestration become widely used inside SOC to harmonize processess and technologies and the implementation of low-level security actions as the building blocks to reduce human intervention in repetitive security operations and invest time on more valuable and complex tasks.

Automation inside the SOC is referred to as the security orchestration, automation and response, and it is considered as effort multiplier for SOC analysts. However, the level of integration of the SOAR depends on the SOC maturity and the challenges related to the deployment and integration such as (Najwa et al., 2022):

- Logging level provided by the onboarded technologies.
- Number of events gathered.
- Complexity of patterns and whether the task could be automated and, if so, to what level of automation.
- Integration level of the SOAR with the different technologies using the API calls and permission provided to the SOAR under the permission strategy.

- Automation skills of the dedicated profile alongside the SOC analysts for automating tasks to ensure consistency of some incident handling and responses, reducing information bias and using higher-fidelity data sources.
- Knowledge of network security, including threat intelligence and the technical infrastructure to support SOC automation tools, for instance.
- Another problem is that few people want to work in a SOC where they will be bombarded with thousands of false positives per day.
- Unfortunately, there are still major technical limitations that prevent automation from becoming a reality.
- Automation performance assessment could not be performed independently because every organization will have a unique environment and edge conditions that change the name of the game.

Lack of Visibility into the IT Security Infrastructure

SOC needs to achieve and maintain clear visibility over the network, and any blind spot can increase the probability of a successful breach and reduce SOC effectiveness. The absence of data and logs from any location means that the SOC ensures no monitoring at that point, and on the other hand, the SOC may get flooded with data logs from different log sources using Syslog, agents, and API system call if there is no prior value-driven approach to decide whether the logs need to be collected, processed, used, and stored (Hausken, 2020).

The most frequent questions, in this case, are what log data should be used and gathered by the SOC and whether the logs are meeting all the requirements for the use cases, visibility, and future investigation. Figure 1 shows the log source and event check list.

Several challenges are faced to achieve a good visibility and coverage of the monitored system among which:

- Lack of understanding the mission performed by the monitored system;
- Clarity and visibility of logs produced by the log source;
- Availability of fields of interest for correlation or forensics purposes;
- Layered and hybrid environments

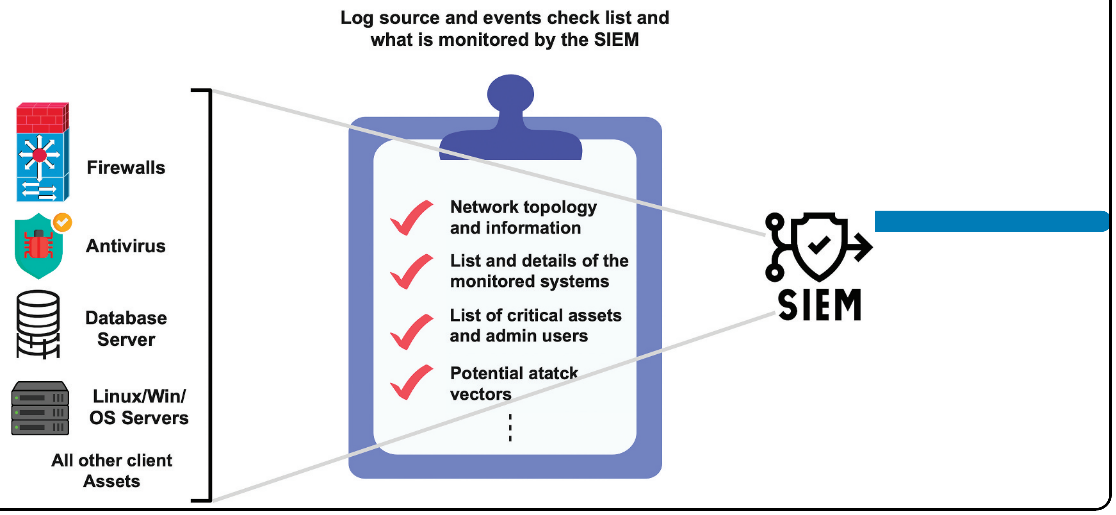
Number of Generated and False Positives

False-positive remains a significant challenge for SOC analysts and the whole SOC capabilities for any monitored system, as shown in Figure 2. It consumes analysts' time dealing with false security incidents and occasionally responding to the real attacks in the worst cases, which impacts both the SOC capabilities and the experience of the SOC analysts, which could leave them vulnerable to severe attacks within the noise (van Os, 2018).

Security incidents fired by the security solutions can fall into one of the following categories:

- True positives: A real and correct detection of malicious activity.

Figure 1. *Event log collection on the technical.*

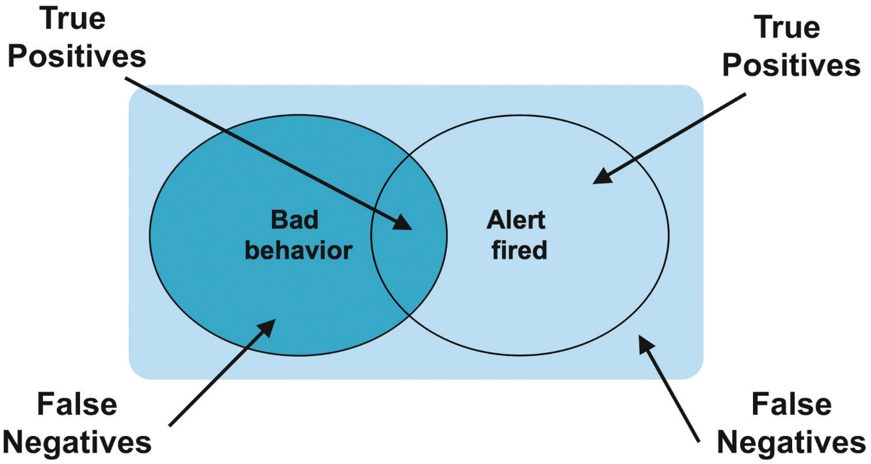

Log source and events check list and
what is monitored by the SIEM
Firewalls
Antivirus
Database Server
Linux/Win/ OS Servers
All other client Assets
Network topology and information
List and details of the monitored systems
List of critical assets and admin users
Potential atatck vectors
SIEM

- True negatives: The activity is benign, and no alert has been generated.
- False positives: A fake detection, the system alerts when a benign activity occurred
- False negatives: A real attack without being detected by the security measures.

Lack of Processes and Playbooks

One of the greatest challenges for today's IT professionals is planning and preparing for the unexpected, especially in response to a security incident. Cybercriminals try to target the weakest links in the security chain, starting with human

Figure 2. *False positives.*



errors and skills shortage to follow events from inception to resolution. Playbooks serve as a development factor toward sharpening the incident response plan, processes and procedures to detect, investigate, eradicate, and recover from a cyber incident and ensure the mapping, coordination, and communication with the stockholders.

Without playbooks, analysts tend to revert to their gut—which might be effective for the individual, but it leaves the entire team at the mercy of the knowledge that exists within that analyst's mind. SOCs that suffer from high turnover rates risk not only the loss of analysts but also the loss of their undocumented expertise. In addition, Moore said that without a playbook, "your work product will vary in effort and quality, and new associates will take longer to acclimate without a playbook."

PERFORMANCE METRICS

Several methods are used to assess the performance and the capabilities of the SOC analysts in socio-technical system and the overall performances of the SOC (Yassine et al., 2017). However, the SOC managers, analysts, and research community are suggesting a lack of adequate metrics to assess SOC analysts and provide clear performance metrics. To this end, Agyepong et al. (2020b) grouped existing assessment methods into quantitative and qualitative metrics. While quantitative metrics provide concrete measures and less open to interpretation, the qualitative metrics uses non-numerical and interpretive approach. We grouped the quantitative metrics that are mostly time-based and used by SOC managers while they provide concrete measures to perform SOC performance assessment. During the analysis of quantitative metrics, we revealed various overlapping such as the Mean Time to Respond, Mean Time to Recovery, and Mean Time to Contain, and sometimes, we have different naming convention. In this part we provide a detailed study of the most announced quantitative metrics during the incident lifecycle starting with the Mean Time to Detect till the overall cost of the incident.

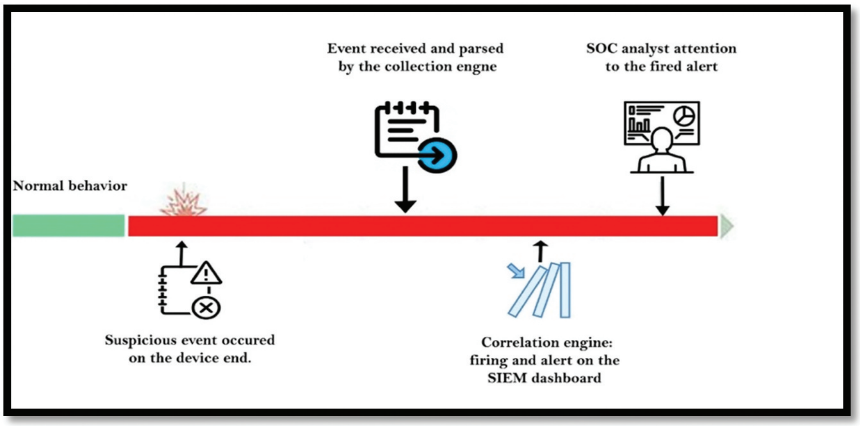
Mean Time to Detect

The Mean Time to Detect is defined as the average amount of time needed to detect a security incident. This metric is used to track and measure the performance metric for the SOC analysts in their different roles and also to evaluate the whole detection capabilities of the SOC as a service. The Figure 3 bellow describes the time between the logging of the suspicious events and the generation of the incident on the monitored dashboard passed by the collection and correlation phases.

Mean Time to Acknowledge (MTTA)

MTTA (Mean Time to Acknowledge) quantifies the time elapsed from when a system generates an alert on the SIEM or monitored dashboard to the point at which a member of the SOC Team initiates an investigation and begins addressing the issue. Its primary

Figure 3. *Mean time to detect.*


Event received and parsed by the collection engne
SOC analyst attention to the fired alert
Normal behavior
Suspicious event occured on the device end.
Correlation engine: firing and alert on the SIEM dashboard

emphasis is on the duration required to recognize and commence problem resolution. This metric is useful for tracking your team's responsiveness and your alert system's effectiveness. Figure 4 shows MTTA metrics. This metric is useful in tracking incident response's effectiveness and alert fatigue, and it's calculated by adding up the time between alert and acknowledgement, then divide by the number of incidents. This metric can be used for single analyst or for the whole SOC Team.

Mean time to respond (MTTR)

Mean time to respond is defined as the average time it takes for incident responders to prepare, identify, contain, eradicate, recover (Casey et al., 2010), and post-incident activity after it has been identified and to return a system to operational condition, as show in Figure 5. It provides insight into how quickly the SOC analyst or the incident response team are responding to the detected security incident and returning to the normal behavior of the impacted systems. MTTR can also refer to other indicators that are similar but not identical such as

- Mean Time to Repair is the average time from starting maintenance work to restoring the system and verifying its performance.
- Mean Time to Recover is the average time from failure to full recovery.
- Mean Time to Resolve is the average time for an incident to be resolved completely, including detecting the problem, correcting the consequences, and taking measures to prevent the event from recurring.

Mean time to Contain (MTTC)

The Mean Time to Contain brings together the time to detect alongside the time to acknowledge and to respond to security incidents. This metric focuses on how long the whole incident response process takes from the detection to the point when the risk contained

Figure 4. *Mean time to acknowledge.*

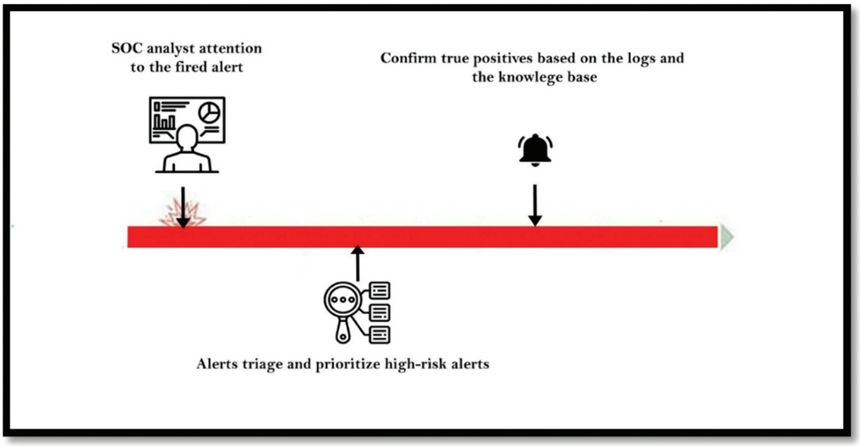
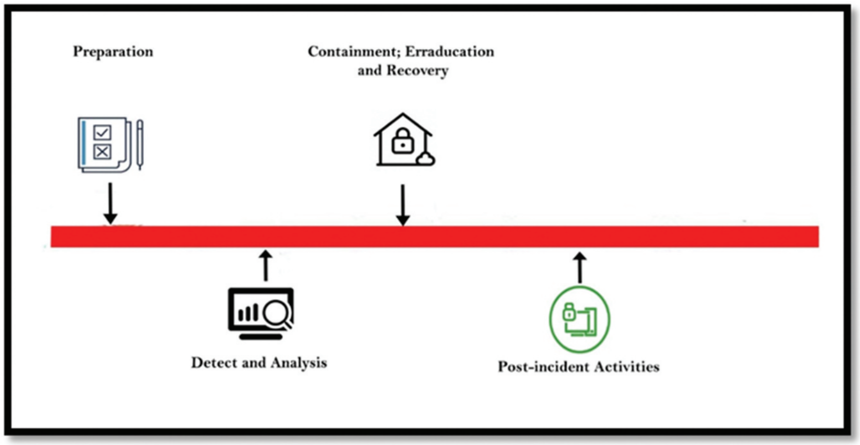

SOC analyst attention to the fired alert
Confirm true positives based on the logs and the knowlege base
Alerts triage and prioritize high-risk alerts

Figure 5. *Mean time to respond.*



and the threat left and effectively prevent a cybercriminal from doing more harm.

MTTC gives a holistic look at how your team works together. If the MTTC is high, then you want to start drilling down into which area - detection, acknowledgment, or recovery - is the weakest link.

Cost of an Incident

Fully detect and resolve an incident, then translating that time into combined salary costs of staff involved.

This metric excludes major incidents that require third parties getting involved. This metric is important while it shows how much incidents cost and having a roadmap for faster incident detection and response will likely show a number those trends down over time.

Alongside the quantitative metrics we have other qualitative metrics used to assess the performances of the SOC analysts such as:

- Competency and the experience of the analysts which might be approved using simulated exercises on a test environment to assess the experience of the analyst.
- Quality of reporting.
- Cyber security Certifications.

DEPENDENCIES OF THE CHALLENGE-PERFORMANCE METRIC

The quantitative performance metrics are based on the challenges faced by the SOC analysts and how they are performing to reduce the time to correctly handle the security incident.

But digging deeper into the challenges revealed that studying SOC analyst's performance metrics during the incident lifecycle independently is unrealistic, given the complex and evolving nature of SOC systems (Agyepong et al., 2020b).

The Figure 6 bellow describes an overview of the interdependent nature of the challenges and the performance metrics inside the SOC socio-technical:

Table 1 bellow describes the SOC's factors and properties impacting performance metrics.

DISCUSSION

The field of Security SOC (Security Operations Center) has emerged as a dynamic and continuously evolving domain of research and practice within the broader realm of cybersecurity. The challenges and the performance metrics become one of the main research topics when it comes to Security Operation Center analysis and improvement. This increase on the research related to challenges and SOC performance metrics is giving more visibility on the real challenges faced by the analysts and provide the security expert with valuable learning resource for assessment and continuous improvement, because anything that is not

Figure 6. ***Interdependent nature of the challenges and performance metrics inside the SOC***

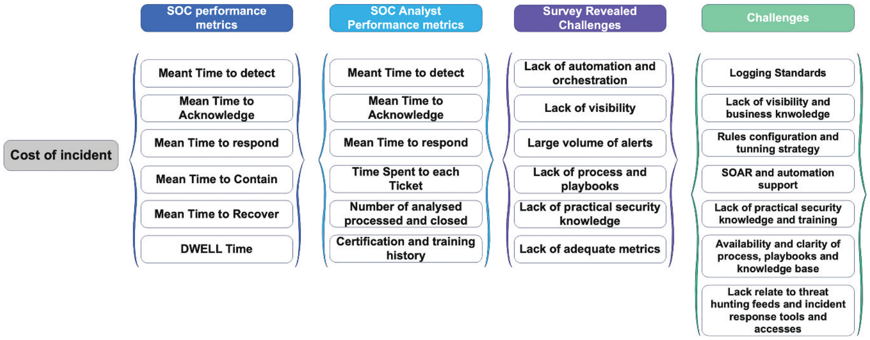

SOC performance metrics
SOC Analyst Performance metrics
Survey Revealed Challenges
Challenges
Cost of incident
Meant Time to detect
Mean Time to Acknowledge
Mean Time to respond
Mean Time to Contain
Mean Time to Recover
DWELL Time
Meant Time to detect
Mean Time to Acknowledge
Mean Time to respond
Time Spent to each Ticket
Number of analysed processed and closed
Certification and training history
Lack of automation and orchestration
Lack of visibility
Large volume of alerts
Lack of process and playbooks
Lack of practical security knowledge
Lack of adequate metrics
Logging Standards
Lack of visibility and business knwoledge
Rules configuration and tunning strategy
SOAR and automation support
Lack of practical security knowledge and training
Availability and clarity of process, playbooks and knowledge base
Lack relate to threat hunting feeds and incident response tools and accesses

Table 1: ***Incident Response Performance Metrics and Factors***

Mean Time To Detect	Mean Time To Acknowledge	Time To Respond or to contain
Incident complexity	Incident complexity	Incident complexity
Incident severity	Incident severity	Incident severity
Incident details on the monitoring platform	Incident details on the monitoring platform	Incident details on the monitoring platform
Availability of the artifacts and the applied logging on the log source	Availability of the artifacts and the applied logging on the log source	Availability of the artifacts and the applied logging on the log source
Experience of the Analyst and practical security knowledge.	Experience of the Analyst	Experience of the Analyst
SIEM Plataform configuration such as: rules, architecture, permissions…	SIEM Plataform configuration such as: rules, architecture, permissions…	SIEM Plataform configuration such as: rules, architecture, permissions…
Threat actors feeds and resources	Threat actors feeds and resources	Threat actors feeds and resources
Number of false and true positives	Existing processes and playbooks	Existing processes and playbooks
		Access permissions on the remote system: Real time access to the remote or compromised assets or the need of collaboration with the asset manager.
		Automation maturity: SOAR and EDR in place
		Tunning on the detection rule

measured cannot be managed. When it comes to measuring the analyst’s performance, literature review suggests that various metrics exist for doing this. However, some authors argue about their completeness and objectivity and make a case for the need for further research in this area. Almost all the existing performance tends to focus on analysts’ reaction time or the frequency at which a particular analyst task is carried out in numerical terms as they are more likely to provide relevant performance indicator and can be used by the analyst for self-assessment to establish how well they are contributing to the team’s objectives.

However, many aspects of SOC analyst work and challenges are not considered to give a holistic picture of their performance and contribution in the SOC. In fact, those metrics do not provide enough information to differentiate two or more analysts raising the same indicators timely based indicators MTTD, MTTR if all the aspects work, and challenges are not taken into account.

But rather, we argue that a good metric should have features that make such distinctions, considering multiple factors to help SOC managers and analysts to get holistic view. In our proposal model, we tried to provide some of the factors impacting each timely based performance metrics for SOC analysts and by identifying and considering those factors on the metrics we can make the assessment more accurate using realistic model.

For example, to perform assessment of SOC analyst using MTTD we need to make sure we are having the same factors impacting the metric such as:

- Incident severity.
- Incident complexity.
- Available documentation and incident response playbooks.
- Number of incidents raised by the SIEM platform during the shift.

- Number of tasks assigned to the analyst during the detection or the response time.

Having the same or close criteria provides more accurate results on the SOC analyst performance regarding a timely based metric of choice and can provide clear visibility to the SOC managers on how the SOC analysts are reacting to security incidents.

Given that a SOC is unique to its organization, we need to design an universal set of metrics that take into account all the factors impacting the metrics to have the ability to differentiate the level of contribution of two SOC analysts based on two security operation centers.

CONCLUSION

This paper suggests that more research is needed to provide a full understanding of the organizational and environmental factors that impact the analyst's assessment and the need of an universal model for assessing the SOC and SOC analysts performance. Therefore, our future work continues to target the factors derived from the analysts works that impact the assessment.

This paper analyzes the challenges and performance metrics used to assess the performance of security analysts based on our prior research and a thorough examination of the factors affecting these metrics from a practical perspective. In this study, we concentrated on the most commonly encountered challenges and the most relevant time-based performance metrics, including MTTD (Mean Time to Detect), MTTR (Mean Time to Respond), MTTC (Mean Time to Contain), and the Cost of Incidents, as these are deemed most suitable and widely used by SOC (Security Operations Center) managers and decision-makers. We presented the weaknesses of time-based metrics and their dependencies on various aspects of work and challenges within SOC analysis routines, which can lead to assessments that are inaccurate and sometimes irrelevant. Conversely, we provided specific factors and criteria that must be considered to enhance assessment accuracy and facilitate the distinction and evaluation of two SOC analysts, whether they work within the same SOC or in different SOCs. Our paper suggests that several factors should be taken into account when evaluating SOC and SOC analysts to provide a comprehensive understanding of the work performed by a SOC analyst

DISCLOSURE STATEMENT

No potential conflict of interest was reported by the author(s).

ORCID

Yassine Maleh http://orcid.org/0000-0003-4704-5364

REFERENCES

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020a). Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of*

Cyber Security Technology, *4*(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178

Agyepong, E., Cherdantseva, Y., Reinecke, P., & Burnap, P. (2020b). Challenges and performance metrics for security operations center analysts: A systematic review. *Journal of Cyber Security Technology*, *4*(3), 125–152. https://doi.org/10.1080/23742917.2019.1698178

Casey, E., Daywalt, C., & Johnston, A. (2010). Intrusion investigation. In *Handbook of digital forensics and investigation* (pp. 135–206). Elsevier Academic Press. https://doi.org/10.1016/B978-0-12-374267-4.00004-5

Chamkar, S. A., Maleh, Y., & Gherabi, N. (2022). The human factor capabilities in SEcurity Operation Center (SOC). *EDPACS*, *66*(1), 1–14. https://doi.org/10.1080/07366981.2021.1977026

Hausken, K. (2020). Cyber resilience in firms, organizations and societies. *Internet of Things*, *11*, 100204. https://doi.org/10.1016/J.IOT.2020.100204

Maleh, Y., Sahid, A., & Belaissaoui, M. (2020). A maturity framework for cybersecurity governance in organizations. *EDPACS*, *63*(6), 1–22. https://doi.org/10.1080/07366981.2020.1815354

Maleh, Y., Sahid, A., & Belaissaoui, M. (2021). A maturity framework for cybersecurity governance in organizations. *EDPACS*, *64*(2), 1–22. https://doi.org/10.1080/07366981.2020.1815354

Mansfield-Devine, S. (2016). Creating security operations centres that work. *Network Security*, *2016*(5), 15–18. https://doi.org/10.1016/S1353-4858(16)30049-6

Miloslavskaya, N. (2016). Security operations centers for information security incident management. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)* (pp. 131–136). https://doi.org/10.1109/FiCloud.2016.26

Najwa, E., Bertrand, R., Yassine, M., Fernandes, G., Abdeen, M., & Souad, S. (2022). Lean 4.0 tools and technologies to improve companies' maturity level: The COVID-19 context. *Procedia Computer Science*, *196*, 207–216. https://doi.org/10.1016/j.procs.2021.12.007

Sundaramurthy, S. C., Case, J., Truong, T., Zomlot, L., & Hoffmann, M. (2014). A tale of three security operation centers. *Proceedings of the 2014 ACM Workshop on Security Information Workers* (pp. 43–50). https://doi.org/10.1145/2663887.2663904

van Os, R. (2018). *SOC-CMM: Measuring capability maturity in Security Operations Centers*. University of TwenteAccessed 09 July 2023 https://essay.utwente.nl/92859/

Yassine, M., Sahid, A., & Ezzati, A. (2017). A capability maturity framework for IT security governance in organizations. *13th International Symposium on Information Assurance and Security (IAS 17)*.

Zimmerman, C. (2014). *Cybersecurity operations center*. The MITRE Corporation.

Zimmermann, V., & Renaud, K. (2019). Moving from a "Human-as-problem" to a "Human-as-solution" cybersecurity mindset. *International Journal of Human-Computer Studies*, *131*, 169–187. https://doi.org/10.1016/j.ijhcs.2019.05.005

Samir Achraf Chamkar *is now a Ph.D. student at Sultan Moulay Slimane University. He has worked in the cybersecurity industry for many years. Passionate about protecting information systems and facing cyber-attacks. He worked for many well-known Cybersecurity companies in Morocco, such as Dataprotect and Omnidata. His goals include the continuous improvement of the Security Operation Centers' performances and capabilities.*

Yassine Maleh*, is an associate professor of cybersecurity and IT governance at Sultan Moulay Slimane University, Morocco. He is the founding chair of IEEE Consultant Network Morocco and founding president of the African Research Center of Information Technology & Cybersecurity. He is a senior member of IEEE and a member of the International Association of Engineers IAENG and The Machine Intelligence Research Labs. Dr Maleh has made contributions in the fields of information security and privacy, Internet of things security, wireless and constrained networks security. His research interests include information security and privacy, Internet of things, net-works security, information system, and IT governance. He has published over 80 papers (book chapters, international journals, and conferences/work-shops), 14 edited books, and 3 authored books. He is the editor-in-chief of the International Journal of Information Security and Privacy, and the International Journal of Smart Security Technologies (IJSST). He serves as an associate editor for IEEE Access (2019 Impact Factor 4.098), the International Journal of Digital Crime and Forensics (IJDCF), and the International Journal of Information Security and Privacy (IJISP). He is a series editor of Advances in Cybersecurity Management, by CRC Taylor & Francis. He was also a guest editor of a special issue on Recent Advances on Cyber Security and Privacy for Cloud-of-Things of the International Journal of Digital Crime and Forensics (IJDCF), Volume 10, Issue 3, July–September 2019. He has served and continues to serve on executive and technical program committees and as a reviewer of numerous international conferences and journals such as Elsevier Ad Hoc Networks, IEEE Network Magazine, IEEE Sensor Journal, ICT Express, and Springer Cluster Computing. He was the Publicity chair of BCCA 2019 and the General Chair of the MLBDACP 19 symposium and ICI2C'21 Conference.*

Noreddine Gherabiis *a professor of computer science with industrial andacademic experience. He holds a doctorate degree in computer science From Hassan 1st University, Morocco, In 2013. He worked as a professor of computer science at Mohamed BenAbdellah University and since 2015 has worked as a research professor at Sultan Moulay Slimane University, Morocco.*