A Grid-Matrix Based on Industry Needs to Evaluate Automation in Security Operations Centre (SOC)

1st Kamal Zidan
University of Gloucestershire
Cheltenham, United Kingdom
Kzidan1@glos.ac.uk

2nd Abu Alam
University of Gloucestershire
Cheltenham, United Kingdom
Aalam@glos.ac.uk

3rd Qublai Ali Mirza
University of Gloucestershire
Cheltenham, United Kingdom
Qalimirza@glos.ac.uk

***Abstract*—Security Operations Centre (SOC) is a unit used for events detection and responding to incidents associated with cyber security threats via monitoring, detecting, examining and reporting on anomalies. Well-known, unknown and new activities are part of SOC tasks that organisations looking to have in their security environment. The key purpose of SOC is to be able to analyse a large set of data and correlate other categories of events. Some network monitoring software solutions produce huge number of false positives due to the lack of accurate prediction processes. Manual processes can provide hackers with the advantage of having more time to accomplish their malicious activities. Thus, SOC analysts are required to apply automated mechanisms to help them in detecting threats. This paper presents a Grid-Matrix that contains different parameters to be considered when evaluating automation and machine learning (ML) models within SOC. An automation model using machine learning algorithms is presented to several cyber security specialists in industry. Based on their feedback the Grid-Matrix is created to compare and evaluate different automation solutions. Thus the obtained results of this work is the Grid-Matrix that highlights the essential parameters that need to be considered when applying automation solutions into SOC.**

***Index Terms*—SOC, Automation, Grid-Matrix**

I. Introduction

SOC is an entity/body with several components that have features and abilities to monitor the network and provide protective measures [3]. SOC can be referred to an organisational unit that is responsible for threat detection and risk mitigation. To enhance a firm security aspect, SOC combines processes, technologies and people (security analysts) via complex structure to prevent potential threats. SOC has always faced various challenges such as: lack of skilled analysts, complexity of technology and inadequate level of threat detection automation process [12].

Organisations operate their SOC by relying on tools that have the ability to automatically collect large set of events in real time environment and analyse them based on predefined rules [15]. The produced events are classified differently based on their type to prepare an effective response to each of them. Predefined rules and signatures are usually implemented to describe threats classifications and events. The set signatures are mainly used to deal with a huge number of alerts such as decreasing the number of false negatives which are genuine attacks that are categorized as normal alerts. In contrast the number of false positives is rising which are events that classified as threats events, but they are not. In fact, SOC analysts do not have the ability to react on all of the generated events as the number of tickets can be extremely overwhelming [16]. Therefore, this paper presents a Grid-Matrix with set of predefined parameters to evaluate the efficiency of an automation model or processes within SOC.

II. Related Works

SOC represents the combinations of people, processes and technologies (PPT). Governance and compliance are also being used and added to PPT as PPTGC to manage the whole security aspects of firms. Both PPT and PPTGC frameworks can be followed by SOC to manage an organisation real-time security environment [9]. Various functions and duties are blended to depict SOC as the main immune centre of an organisation [2]. There is a tiered approach that is followed when dealing with cyber security events [5]. This approach can be either of analysing incidents or escalate them to experienced analysts for more in-depth investigation [9].

Kim and Kwon [16] added that analysts are often able to respond into up to 29% of the detected tickets where 40% of these tickets can be recognised as false positives. Establishing successful data classifications models can be difficult due different reasons. For instance, a huge set of data including security events are required to train such models. The required time for training and amendments might be needed when a new threat occurs. This makes it hard to act on events in real time scenarios. Any types of responses delays expose SOC to fail in implementing effective defensive measures. Efforts have been set now and before in order to implement efficient threat detection approaches based on artificial intelligence and machine learning which would help in mitigating the number of noisy events including false positives [6]. Neural network models such as naive bayes, decision tree and Support vector machine (SVM) algorithms can be used for threats classifications [16].

To provide a secure cyber environment, SOC usually depends on set of systems. These tools are designed with the goal of collecting, analysing and visualising information in

an understanding way for analysts to investigate incidents effectively. Security information event management (SIEM), Intrusion detection systems (IDS), Intrusion prevention systems (IPS), Next generation firewalls (NGFW), Endpoint detection and response (EDR) and Threat intelligence platforms (TIP) are some of the tools that are part of the entire SOC as Kiiveri [11] stated.

SOC tools operate by collecting logs and data generated from several systems sources. Records and logs are produced from security products such as IPS or antivirus software. Also logs that are coming from operating systems and applications. Collecting logs by gathering data from sources then store it in a centralised location plus the ability to construct log correlation amongst various events are the main functions that SOC is able to provide. It offers continuous access to previous information and present the gathered data in readable reporting format. Hence, the deployment of Artificial Intelligence and machine learning in SOC solutions are required now more than ever to enhance the detection techniques and improve automation to respond to security incidents more effectively [13].

A sufficient effective model cannot be established without highlighting both threat classification and model learning [7]. Responding to new attacks such as zero-day threats is part of the learning process that is required to build valuable classification prototype for SIEM. A successful defence system is associated with the learning time and updates. It is vital to consider the time that is required for threat classification and learning. In threat classification, the expectations are to quickly detect and identify threats that are produced by assets. If not, then the targeted systems will be exposed to vulnerabilities. In some cases, threat classification cannot be applied into environments that include devices with law performance processors. Hence, it is important to apply models that have capabilities of quick classification [16].

Fig 1 below depicts the categorisation of some of AI correlation frameworks based on event knowledge which also described as the state of art according to [8]. The stated models included rule-based, semantic, graphical and ML as part of used labels in ML approaches. A rule-based model is usually associated with normal relationships amongst events. In fact, it relies on knowledge repository that comprises specific rules that assist in matching events characteristics. It can be summarised as a description of knowledge based on rules to evaluate and combine security events. Semantics frameworks are different where particular conditions are used based on specific language syntax. Semantics rules help in distinguishing correlation between input and output data. For example, an event can be recognised based on set of characters that represent a particular word and formal grammar in existing language. Thus, the knowledge description based on language syntax and semantics is the definition of semantic based technique [8].

Sopan et al. [1] have investigated alerts with SOC analysts

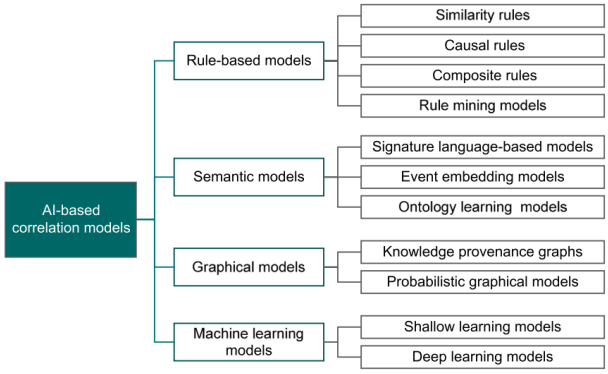

Fig. 1. Artificial Intelligence Correlation Frameworks [8]

from cyber security organisation. The analysts use cloud platform to monitor alerts that are triggered from various systems based on indicator of compromise (IOC) approach that is created by cyber security specialists. The web platform allows analysts to review raw data of alerts plus request more in-depth details of an alert to distinguish if it's real or false when needed to. Based on the outcome of an investigation of such alert, then it can be categorised as threat or false positive.

The model is built using the approach of categorising alerts as genuine or false. The aim of the model is to offer SOC analysts with alerts prediction approach using ML that adopt similar features to an analyst mind model. Also, to spread confidence amongst SOC analysts to use the model. Another aim is to validate the model and receive corrections from stakeholders to enhance the prototype performance. The identified alerts worked as training data for the founded model [1]. Fig 2 illustrates the structure of the model. The workflow begins with a system to detect signature-based alerts from various endpoints then deliver them to analysts. In the proposed model, alerts are being sent through ML technique that specify the reality of an alert. The alerts then marked with prediction labels and provided to analysts for further investigation. Combining raw data of alerts, prediction labels and analysts' investigations, an overview of the model performance is then presented to shareholders [1].

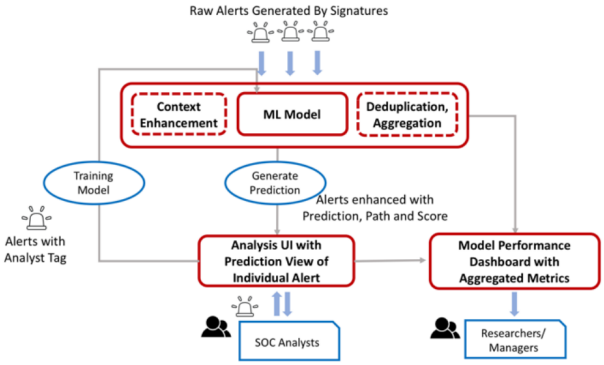

Fig. 2. Machine Learning Model [1]

Ndichu et al. [14] developed an approach that automate threat alerts and highlighted the issue of imbalance in appliances alert data. Neighbourhood Cleaning Rule (NCR) is used firstly to identify false positives. Support Vector Machine Synthetic Minority Oversampling Technique (SVMSMOTE) also applied to produce true alerts for training objectives. Then the alerts are classified via the adoption of Decision Tree (DT) and Random Forest (RF). Up to 8 systems were utilised to generate the alert data to present the model ability of reducing the demand of manual analysis. Fig 3 below depicts the delivered approach for detection of critical alerts from imbalanced multi-appliance threat alert logs.

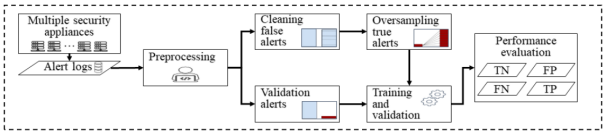

Fig. 3. Critical Alerts Detection Approach [14]

Accordingly, the amount of security alerts has decreased significantly, but Ndichu et al. [14] added that different approaches can be used for future studies to enhance precision metrics such as; probability tuning and mixture algorithms. They added that an appropriate labelling of data can improve the process of decreasing the amount of false negatives and false positives which also lead to an enhancement of threat detection performance [14].

AI defensive measures provide better performance of detecting cyber risks. Mathew [4] added that the future of cyber security defence is ML which is part of AI. It is important to enhance information systems by learning from data without the need to use precise programming approach. Implementing algorithms to extract data and search for patterns are the mathematical methods that ML is normally based on. There are several ML algorithms that are commonly used such as association rules, Bayesian algorithms and decisions trees. However, cyber security solutions are more focused on ML algorithms nowadays due to the ability in clustering practices to provide a clear picture of the probability of attacks.

III. Methodology

A. Overview

The author conducted literature review on previous studies. Also, we developed automation model then it is presented to 10 participants from cyber security to software development fields. The reason behind that is to gain feedback and to evaluate the model based on specialists' opinions. Based on the outcome of interviews a Grid-Matrix is created to evaluate different models solutions.

B. Participants

Table I below presents the roles and interviews methods used to evaluate our automation model where coding approach of P1-P10 is applied.

TABLE I
Participants of Model Feedback

Participant ID	Role	Interview Method
P1	Cyber Security Consultant	MS Teams
P2	Cyber Security Consultant	MS Teams
P3	Software Developer	Google Meet
P4	Software Sales	Google Meet
P5	Software Product Leader	Google Meet
P6	Cyber Security Consultant	MS Teams
P7	Penetration Tester	MS Teams
P8	Information Security Analyst	MS Teams
P9	Software Engineer Analyst	MS Teams
P10	IT Analyst	In Person

C. Ethics

The researcher makes sure direct identifiers of respondents are removed from any saved files on personal devices to protect individuals in case a breach takes a place. As any method of gathering and collecting data, interviews are exposed to different ethical concerns that the researcher must be aware of. The most essential ethical aspect when conducting the selected research is to protect respondents' confidentiality. In the occurrence of confidentiality breach, there are unwanted consequences that can impact on participants themselves as the researcher as well. Reputation damage, employability loss or even criminal liability can be the result of such a disclosure of information that respondents can be affected by. Also, participants were able to stop responding to questions if they had privacy and confidentiality concerns [10]. Participants were given the choice to turn their camera on/off. The recordings were saved and only accessed by the researcher using password protected one drive account.

IV. Grid-Matrix

Based on our findings we created a Grid-matrix that can be used to evaluate an automation model based on its performance and set parameters plus comparing it with more than one solution. Refer to Fig 4 for the Matrix. Organisations can evaluate the efficiency of threat detection automation based on the following set of parameters or adding other features if required.

Detection Methods: either signature based, anomaly based or ML based.

Data Sources: include network traffic, endpoints data, logs or users' behaviours.

Detection Accuracy: such as true/false positive and true/false negative.

Response Time: time to detect and time to respond.

Scalability: dataset size handling and number of devices involved.

Costs: operations and investments costs.

Integration: compatibility with other current systems.

Reporting & Alerting: tools and mechanisms for reports and alerts.

User Friendliness: the required training and ease of use.

Customization: the ability to apply and tailor it to particular threats.

Criteria							
Detection Methods	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Signature Based	10						
Anomaly Based	10						
ML Based	10						
Data Sources	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Network Traffic	9						
Endpoints Data	9						
Logs	9						
Users Behaviours	9						
Detection Accuracy	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
TP	8						
FP	8						
TN	8						
FN	8						
Response Time	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Time to Detect	7						
Time to Respond	7						
Scalability	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Dataset Size Handling	6						
Number of Devices Involved	6						
Costs	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Initial Investment	5						
Ongoing Operations	5						
Integration	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Compatibility with Current Systems	4						
Reporting & Alerting	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Reporting Instruments	3						
Alerting Methods	3						
User Friendliness	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Required Training	2						
Ease of Use	2						
Customization	**Scale**	**Solution I**	**Scale Score**	**Solution II**	**Scale Score**	**Solution III**	**Scale Score**
Particular Threats Applying Ability	1						
Total Score		**Solution I**		**Solution II**		**Solution III**	

Fig. 4. Grid-Matrix

Each parameter or criteria is assigned a specific scale based on its value to the business. For example, detection methods can be assigned 10 as a scale where customization might be assigned 8. Thus, due to the assigned value we can gather that detection methods criteria is more important than customization. However, these values can be set based on organisations requirements.

Solutions ratings can be assigned numerical values based on their performance that is aligned with each criterion to discover how well a solution is performed. As well, the scale score for each criterion is calculated by multiplying the scale **(S)** for each criterion by the rating **(R)** of how well a solution is performed based on that specific criterion. Overall, the total score of how well a solution is performed is extracted from adding up all the weighted scores for each criterion. Accordingly, an equation can be written as follow:

$$\text{Scale Score (SS)} = S \times R \tag{1}$$

$$\text{Total Score (TS)} = \sum_{i=1}^{n} \text{SR}_i \tag{2}$$

Where **SRi** is equal to weighted score for criterion **i**. Refer to below example for more explanation:

For instance, if a response time criterion is given **7** as a scale and a solution is performed **6** for this specific criterion. Then the scale score would **42** as follow:

$$7 \times 6 = 42$$

.

However, the total score of how well a solution is performed would be adding **42** to all other scale scores.

The selection of parameters of the Grid-Matrix is essential for the construction and evaluation of automated solutions to optimise performance and accuracy. This method includes systematically exploring a predefined set of parameter combinations. This allows for comprehensive evaluation across multiple dimensions. Weights are assigned to different parameters to reflect their relative importance based on an organisation needs to influence a model's behavior. By carefully defining these weights, SOC team can prioritise key aspects of an automation solution system. For example speed, precision and robustness ultimately lead to a more effective and tailored automated solution. This approach ensures that the solution is finely tuned to meet specific objectives and operational requirements of a particular organisation.

V. Conclusion

Based on feedback from participants, a Grid-Matrix is created to assess the effectiveness of such an applied automation solution. Nonetheless, with only few amendments such a matrix can be applied for different other solutions. Thus, the focus was more on automation and ML in saving time and reducing the work that can be done on analysing logs. SOC plays essential role in mitigating cyber attacks. Hence, research that target SOC and their challenges is always required to implement, enhance, improve and develop any existing functions.

A. Limitations

First of all, sample size is one of the limits of this study as we only conducted interviews with small number of participants. This can have an impact on the generalisability of our findings. Also, a bias can occur which could influence on honesty and accuracy of responses. Accordingly, it is essential to understand that findings of this research may only be applied to a particular group and might not be generalised to other settings or contexts.

B. Future Work

For future direction, the research can be expanded to enhance and publish our automation solution based on machine learning approach. Collaborative research can also be conducted between researchers and institutions or organisations to address the complexity of SOC. Considering this approach will help researchers in expanding the scope and the influence of future studies. Overall, the Grid-Matrix can also be tested from an industrial point of view then a feedback can be gained in terms of the efficiency of such a matrix.

REFERENCES

[1] A. Sopan, M. Berninger, M. Mulakaluri. and R. Katakam, Building a machine learning model for the soc, by the input from the soc, and analyzing it for the soc, In 2018 IEEE Symposium on Visualization for Cyber Security (VizSec), 2018, pp. 1–8.

[2] A. M. Majid and Z. A. K. Ariffi, Success factors for cyber security operation center (soc) establishment, EAI, 2019.

[3] A. S. Alharbi, A qualitative study on security operations centers in saudi arabia: challenges and research directions, J. Theor. Appl. Inf.Technol, issue. 98, vol. 24, 2020.

[4] A. Mathew, Artificial intelligence for offence and defense-the future of cybersecurity, Educational Research, vol. 3, 2021, pp. 159-163.

[5] C. Zhong, T. Lin, P. Liu, J. Yen and K. Chen, A cyber security data triage operation retrieval system, Computers Security, vol. 76, 2018, pp. 12–31.

[6] C. Crowley and J. Pescatore, J, Common and best practices for security operations centers: Results of the 2019 soc survey, SANS, Bethesda, MD, USA, Tech. Rep, 2019, pp. 1–24.

[7] C. Engel, S. Mencke, R. Heum¨uller, R. Hormann, H. Aedtner and F. Ortmeier, Customizable operation center for smart security management, Procedia CIRP, 54th CIRP CMS 2021 - Towards Digitalized Manufacturing 4.0, vol. 104, 2021, pp. 1930-1935.

[8] D. Levshun and I. Kotenko, A survey on artificial intelligence techniques for security event correlation: models, challenges, and opportunities, Artificial Intelligence Review, 2023, pp. 1–44.

[9] D. Shahjee and N. Ware, Integrated network and security operation center: A systematic analysis, IEEE Access, vol. 10, 2022, pp. 27881–27898.

[10] E. Singer and M. P. Couper, Ethical considerations in internet surveys 1, Social and Behavioral Research and the Internet, 2018, PP. 133–162.

[11] K. Kiiveri, Automation in cyber security, Turku University of Applied Sciences, 2021, pp. 1-31

[12] M. Vielberth, F. B¨ohm, I. Fichtinger and G. Pernul, Security operations center: A systematic study and open challenges, IEEE Access, vol. 8, 2020, pp. 227756–227779.

[13] M. Hristov, M. Nenova, G. Iliev and D. Avresky, Integration of splunk enterprise siem for ddos attack detection in iot, In 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA), pp. 1-5.

[14] S. Ndichu, T. Ban, T. Takahashi and D. Inoue, A machine learning approach to detection of critical alerts from imbalanced multi-appliance threat alert logs, In 2021 IEEE International Conference on Big Data (Big Data), 2021, pp. 2119-2127.

[15] S. A. Shatnawi, B. Al-Duwairi, M. M. Almazari, S. M. Alshakhatreh, N. A. Khader and A. A. Abdullah, Adaptable plug and play security operations center leveraging a novel programmable pluginbased intrusion detection and prevention system, arXiv preprint arXiv:2204.04576, 2022.

[16] Y.-J. Kim and Y.-H. Kwon, Threat classification model for security information event management focusing on model efficiency, Computers Security, vol. 120, 2022, pp. 102789.