Security Operations Centre
Using Open Source Tools

Synopsis Report submitted in partial fulfillment
of the requirement for the degree of
B. E.(Computer Engineering)

Submitted By

Kedar Walavalkar 20102A0039

Kunal Walavalkar 20102A0038

Yash Jagdale 20102A0005

Sanchit Gharge 20102A0047

Under the Guidance of
Prof. Amit Nerurkar
Department of Computer Engineering

VIT | Vidyalankar Institute of Technology
ACCREDITED A+ BY NAAC
(An Autonomous Institute Affiliated to University of Mumbai)

Vidyalankar Institute of Technology
Wadala(E), Mumbai 400 037

University of Mumbai

2023-24

CERTIFICATE OF APPROVAL

For

Project Synopsis

This is to Certify that

Kedar Walavalkar 20102A0039

Kunal Walavalkar 20102A0038

Yash Jagdale 20102A0005

Sanchit Gharge 20102A0047

Have successfully carried out Project Synopsis work entitled

“Security Operations Centre Using Open Source Tools”

in partial fulfillment of degree course in
Computer Engineering
As laid down by University of Mumbai during the academic year
2023-24

Under the Guidance of
Prof. Amit Nerurkar

Signature of Guide

Head of Department

Examiner 1

Examiner 2

Principal

Declaration

We declare that this written submission represents our ideas in our own words and where others' ideas or words have been included, we have adequately cited and referenced the original sources. We also declare that we have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in our submission. We understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Name of student	Roll No.	Signature
1. Kedar Walavalkar	20102A0039	
2. Kunal Walavalkar	20102A0038	
3. Yash Jagdale	20102A0005	
4. Sanchit Gharge	20102A0047	

Date: 30-10-2023

Acknowledgements

This Project wouldn't have been possible without the support, assistance, and guidance of a number of people whom we would like to express our gratitude to. First, we would like to convey our gratitude and regards to our mentor **Prof. Amit Nerurkar** for guiding us with his constructive and valuable feedback and for his time and efforts. It was a great privilege to work and study under his guidance.

We would like to extend our heartfelt thanks to our Head of Department, **Prof. Sachin Bojewar** for overseeing this initiative which will in turn provide every Vidyalankar student a distinctive competitive edge over others.

We appreciate everyone who spared time from their busy schedules and participated in the survey. Lastly, we are extremely grateful to all those who have contributed and shared their useful insights throughout the entire process and helped us acquire the right direction during this research project.

Table of Contents

Abstract

The focal point for an organization's security operations is a security operations centre (SOC). A SOC, which is also known as an information security operations centre (ISOC), is a centralised location where information security specialists use technologies to create and maintain the security architecture that continuously monitors, detects, examines, and responds to cybersecurity incidents. The security team, made up of security analysts and engineers, keeps an eye on everything that happens on servers, databases, networks, apps, endpoint devices, websites, and other systems in order to identify potential security threats and stop them as swiftly as possible. They also keep an eye on pertinent outside sources (like threat lists) that can have an impact on the organization's security posture. In addition to identifying threats, a SOC must also analyse them, look into their origins, report on any vulnerabilities found, and make plans on how to avoid future occurrences of the same kind. In other words, they are addressing security issues as they arise and are constantly looking for methods to strengthen the organization's security posture.

Introduction

Based on recent studies, the number of security breaches has seen an increase of 11%. This number has increased by a total of 65% over the previous five years. The number of actual occurrences is likely significantly larger.

The global cyber security landscape has seen increased threats in recent years. Through the pandemic, cyber criminals took advantage of misaligned networks as businesses moved to remote work environments. In 2020, malware attacks increased 358% compared to 2019.

From here, cyber attacks globally increased by 125% through 2021, and increasing volumes of cyber attacks continued to threaten businesses and individuals in 2022.

Russia's invasion of Ukraine has had a massive impact on the cyber threat landscape. Since the start of the war, Russian-based phishing attacks against email addresses of European and US-based businesses have increased 8-fold. Nearly 3.6 million Russian internet users have also experienced breaches in the first quarter of 2022, an 11% increase quarter-on-quarter

Example: Hardware giant MSI confirms cyberattack**.** The threat group claimed to have taken 1.5TB of data and issued a ransom demand of $4 million.

The increasing frequency and complexity of cybercrimes have made it crucial for organizations to have a Security Operations Center (SOC) to deal with them effectively. Some reasons why a SOC is important in dealing with increasing cybercrimes:

- 24/7 Monitoring: Cyber-attacks can occur at any time, and a SOC provides continuous monitoring of an organization's network, systems, and applications. By identifying and responding to security incidents in real-time, a SOC can mitigate the impact of an attack and reduce the time it takes to detect and respond to a threat.

- Threat Intelligence: A SOC is equipped with advanced security tools and technologies that allow it to gather and analyze threat intelligence. This helps identify patterns and trends that can inform security strategies and prevent future attacks.

- Incident Response: A SOC is responsible for managing security incidents and responding to cyber-attacks. SOC analysts use incident response procedures to contain and remediate security incidents quickly and effectively.

- Forensic Investigation: A SOC has access to forensic tools and technologies that allow it to investigate the root cause of a security incident. This helps organizations understand the extent of the damage caused by an attack and implement measures to prevent it from happening again.
- Compliance: Many organizations are subject to regulatory requirements that mandate the implementation of specific security controls and monitoring of security-related events. A SOC can

help organizations meet these compliance requirements by monitoring and reporting on security incidents.

- Proactive Approach: A SOC takes a proactive approach to security, by identifying and addressing potential vulnerabilities before they can be exploited by cybercriminals. This helps organizations stay ahead of emerging threats and prevent cyber-attacks from occurring in the first place.

Aim and Objectives:

Project Aims:

1. Understanding SOC: Gain a deep understanding of SOC functions and importance in cybersecurity.
2. Hands-on Experience: Acquire practical experience with industry tools and techniques used in SOC operations.
3. Fundamental Procedures: Learn core procedures for incident handling and threat detection.
4. Open Source SOC: Explore open-source SOC solutions and their integration possibilities.
5. Enhance Security Posture: Improve skills to swiftly identify and respond to security threats.

Project Objectives:

1. Research and Tools: Study SOC fundamentals and identify essential tools.
2. Tool Proficiency: Get proficient in specific SOC tools and explore open-source alternatives.
3. Incident Handling: Develop and practice incident response procedures.
4. Vulnerability Assessment: Learn to assess and manage vulnerabilities.
5. Threat Intelligence: Integrate threat intelligence for proactive monitoring.
6. Continuous Improvement: Plan for ongoing SOC enhancements.
7. Documentation: Create reports on incidents, vulnerabilities, and knowledge gained.

Literature Survey

Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy (2015)
- Onwubiko C.
In this paper, they focus on 4 vital aspects as in Collection, Analysis, Monitoring,and Response. Whereas they state a CSOC strategy should be driven by the business requirements of the organisation, and should be organisation focused and user-centred. Specifically, this means, the capability of a CSOC will vary from one organisation to the other; and in accordance to the organisation's business needs and requirements. For instance, if one organisation's business needs are driven by the ability to respond and defend nation state sponsored attacks, then the capabilities they should have in their CSOC service will be certainly different to another organization whose business requirements and needs are focused on mitigating internal privileged user misuse.

Cybersecurity Alert Prioritization in a Critical High Power Grid With Latent Spaces
-JUAN RAMÓN FEIJOO-MARTÍNEZ 1, ALICIA GUERRERO-CURIESES 2, FRANCISCO GIMENO-BLANES.
The safety of telecommunication networks associated with high-power electric grid networks is crucial. In this work, deep learning techniques such as Autoencoders or Multiple Correspondence Analysis are used to analyze and prioritize high-severity events in power communication networks. Categorical data types such as addresses or anomaly descriptions are used in anomaly and intrusion detection. The analysis allows for the quantification and statistical description of high-severity events, with 5-10% of alerts prioritized for handling by managers. Probability clouds of alerts have been shown to configure explicit manifolds in latent spaces, enabling more efficient analysis and visualization of data. Overall, the results offer a homogeneous framework for implementing anomaly detection prioritization in power communication networks.

Model for successful development and implementation of Cyber Security Operations Centre (SOC)

-Maziana Abd Majid, Khairul Akram Zainol Ariffin
Based on the descriptive analysis of the success factor of SOC, it was found that the top management support factor had the highest mean value (M = 4.888, SD = 0.316). This is supported by the fact that 88.9% of the respondents strongly agreed that this factor was the most influential factor in the development and implementation of SOC. Top management support is crucial in governance, where it can set clear directions, set priorities, and formulate long-term strategies for SOC implementation.

It is based on the critical factors of SOC, namely human, process, and technology, with support from external factors such as top management support, financial, and continuous improvement. For future work, it is suggested that the study conducts a combination of qualitative and quantitative methods to enhance the validity of the data.

"Success Factors for Cyber Security Operation Center (SOC) Establishment"

-M. Abd Majid and K. A. Zainol Ariffi

The research paper provides a comprehensive framework for establishing a successful Security Operations Center (SOC). The authors conducted a literature review and analyzed case studies of successful SOC implementations to identify the critical success factors for SOC establishment.

The paper provides valuable insights into the critical success factors and succession indicators that organizations need to consider when establishing and monitoring the performance of their SOC, some of them are top management commitment, skilled personnel, effective processes and procedures, advanced technologies, continuous monitoring and improvement, and a strong security culture. And in terms of assessing the performance of their SOC factors include incident response effectiveness, threat detection capabilities, mean time to detect (MTTD), and mean time to respond (MTTR).

"Formalizing and Integrating User Knowledge into Security Analytics"

- Fabian Böhm, Manfred Vielberth, and Günther Pernul

explores the importance of integrating user knowledge into the incident detection lifecycle in cybersecurity. They discuss the challenges associated with detecting and responding to cybersecurity incidents. They explain that traditional security analytics systems often rely on static rules and signatures, which can be ineffective against advanced and evolving threats. They suggest that incorporating user knowledge into the incident detection lifecycle can improve the accuracy and efficiency of security analytics. The paper then provides a framework for formalizing and integrating user knowledge into the incident detection lifecycle. The framework consists of several stages, including knowledge acquisition, formalization, integration, and validation. The authors explain that this framework can help organizations capture and use the knowledge of users, such as security analysts, to enhance the effectiveness of security analytics.

Problem Statement

As organizations face an increasing number of sophisticated cyber attacks, it has become imperative to establish a robust Security Operations Center (SOC) to identify, analyze, and respond to security threats. However, the effectiveness of SOC operations depends on several factors, including the skills and experience of SOC analysts, the quality of tools and technologies deployed, the level of automation, and the availability of relevant data sources. Moreover, the lack of standardization in SOC processes and procedures can lead to inefficiencies and gaps in coverage, resulting in increased risk to the organization. Therefore, there is a need to improve the efficiency and effectiveness of SOC operations by developing standardized processes, improving the quality of tools and technologies, and investing in training and development of SOC analysts.

Scope:

This project aims to provide a comprehensive understanding of SOC operations, including its core components, industry-relevant tools, and fundamental procedures. It will focus on developing hands-on experience and proficiency with tools commonly used in SOC environments and explore the concept of open source SOC solutions. The project's primary objective is to enhance the ability to swiftly identify, respond to, and prevent security threats, thereby strengthening an organization's security posture.
Also it holds particular significance for smaller organizations with limited budgets. Industry-relevant tools and open-source SOC solutions offer cost-effective means to establish and maintain robust cybersecurity practices. These organizations can leverage open-source tools and techniques to build and operate a SOC without the high licensing fees associated with proprietary solutions. This approach not only helps in cost control but also enables smaller organizations to proactively monitor and respond to security threats. The project's emphasis on open-source tools and methodologies can empower such organizations to enhance their security posture efficiently, aligning with their financial constraints while ensuring data protection and business continuity.

Proposed System

- OPNsense IPS/IDS - A network intrusion detection and prevention system that monitors network traffic and generates alerts when suspicious activity is detected.
- Elastic-Search - A distributed, RESTful search and analytics engine designed to store, search, and analyze large volumes of data quickly and in real-time.
- Kibana - A data visualization and exploration platform that provides real-time analytics and visualization of data stored in Elastic-Search.
- TheHive - A security incident response platform that centralizes and streamlines the management of security incidents and investigations.
- Cortex - An open-source security orchestration, automation, and response platform that enables analysts to automate the analysis of observables and streamline incident response.
- MISP - A threat intelligence platform that enables the sharing, storage, and correlation of threat intelligence data among organizations and security professionals.
- Second Model

  Splunk :Splunk is one of the leading SIEM solutions in the market that provides the ability to collect, analyze and correlate the network and machine logs in real-time. In this room, we will explore the basics of Splunk and its functionalities and how it provides better visibility of network activities and help in speeding up the detection.

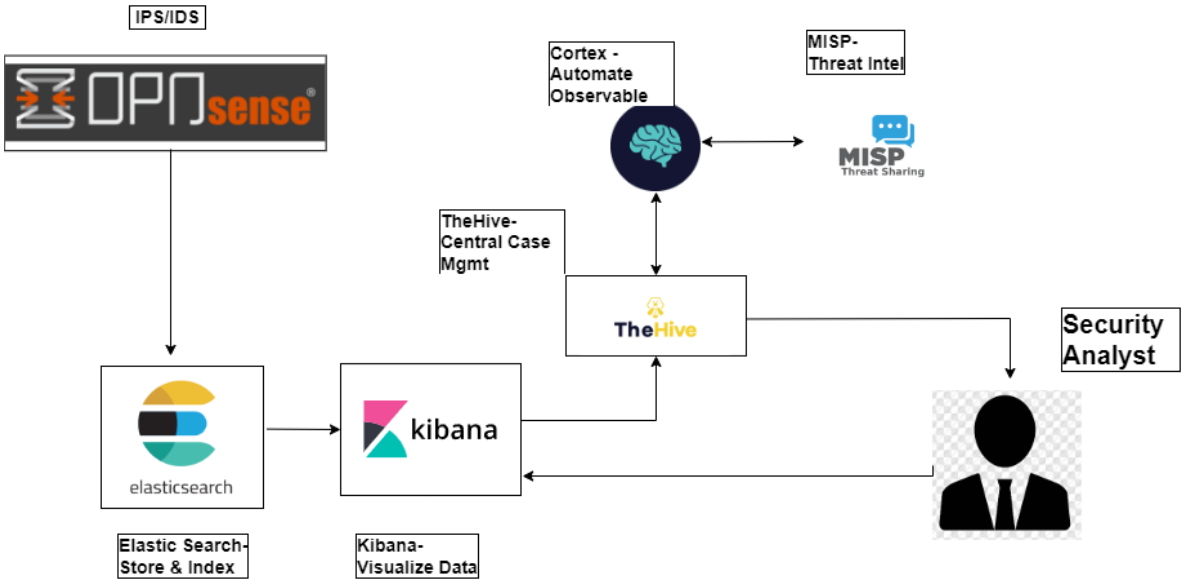
  Splunk Forwarder:Splunk Forwarder is a lightweight agent installed on the endpoint intended to be monitored, and its main task is to collect the data and send it to the Splunk instance. It does not affect the endpoint's performance as it takes very few resources to process.

  Splunk Indexer: Splunk Indexer plays the main role in processing the data it receives from forwarders. It takes the data, normalizes it into field-value pairs, determines the datatype of the data, and stores them as events. Processed data is easy to search and analyze.

  Search Head: Splunk Search Head is the place within the Search & Reporting App where users can search the indexed logs as shown below. When the user searches for a term or uses

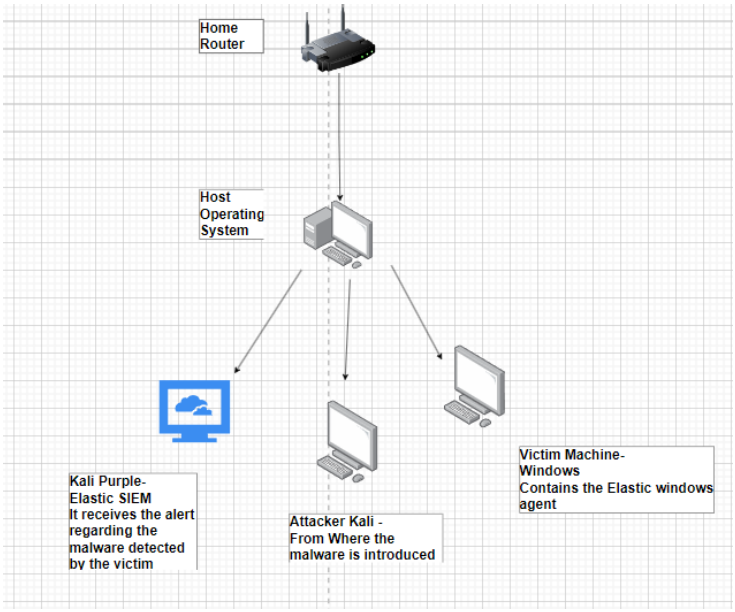
a Search language known as Splunk Search Processing Language, the request is sent to the indexer and the relevant events are returned in the form of field-value pairs.

Methodology

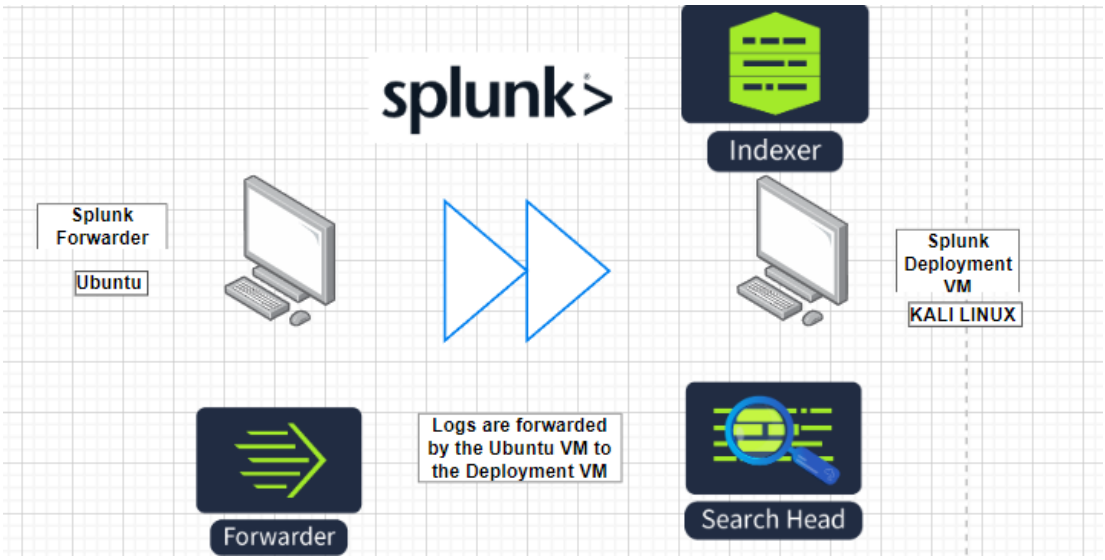


Analysis:

Process Model: Elastic SIEM (First Model)



Splunk SIEM (Second Model):



Feasibility Study:

1. Technical Feasibility:

Resource Availability: Resources for this project, including computers, open-source tools, and training materials, are readily available and affordable.

Technical Expertise: The project team possesses basic technical skills and can acquire additional knowledge through open-source materials.

2. Economic Feasibility:

Budget: The project is cost-effective as it primarily relies on open-source tools and free learning resources, making it feasible for organizations with limited budgets.

Benefit Analysis: The benefits include improved cybersecurity capabilities and a more secure operational environment, which can justify the project's costs.

3. Operational Feasibility:

Integration with Current Operations: The project seamlessly integrates with the organization's existing security practices and does not disrupt daily operations.

Disruption: Minimal disruption is expected as the project is designed for flexible and self-paced learning.

4. Legal and Regulatory Feasibility:

Compliance: The project emphasizes compliance with data protection regulations and security best practices, making it legally and regulatorily sound.

5. Schedule Feasibility:

Timeline: The project timeline is reasonable, allowing participants to complete the training and practice sessions effectively.

6. Risk Analysis:

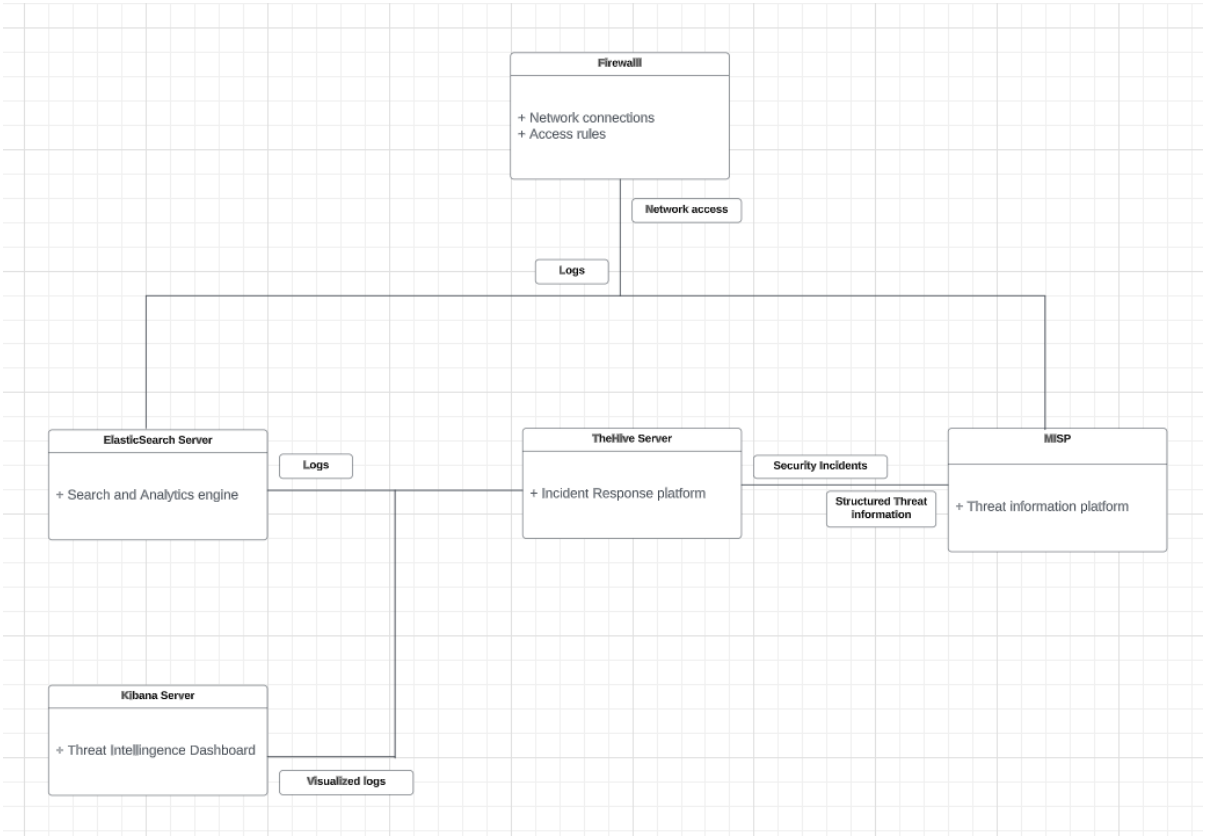
Risk Assessment: Potential risks, such as resource constraints, are minimal due to the project's emphasis on open-source tools and low-cost training materials. Participants can mitigate risks through effective planning.

Cost Analysis:

The project incurs no direct costs, it is achieved through the exclusive use of open-source tools and self-paced learning, which eliminates the need for expensive licenses or instructors. Minimal administrative expenses cover essential project management functions. This cost-free approach makes the project highly accessible to individuals and organizations with limited budgets. Its value lies in the acquisition of crucial SOC operation skills and knowledge, with practical, real-world applicability. We gain the ability to effectively monitor, detect, and respond to security threats, making it a valuable endeavor for those seeking cybersecurity careers and organizations aiming to enhance their security measures. The flexibility of self-paced learning further enhances its utility.

Design:

Data Flow Diagram:



Hardware and Software Requirements:

Hardware Requirements:

- Personal computer.
- WiFi router.

Software Requirements:

- Virtual Box.
- Kali Virtual Machine iso image.
- Windows Virtual Machine iso image.
- Ubuntu Virtual Machine iso image.
- ElasticSearch.
- Kibana.
- Elastic Agent.
- Splunk Enterprise.
- Splunk Forwarder.

References:

1. Security Operations Center: A Systematic Study and Open Challenges - MANFRED VIELBERTH , FABIAN BÖHM , INES FICHTINGER , AND GÜNTHER PERNUL , (Member, IEEE) Chair of Information Systems, University of Regensburg, 93053 Regensburg, Germany
2. Cybersecurity Alert Prioritization in a Critical High Power Grid With Latent Spaces JUAN RAMÓN FEIJOO-MARTÍNEZ 1 , ALICIA GUERRERO-CURIESES 2 , FRANCISCO GIMENO-BLANES 3,4, MARIO CASTRO-FERNÁNDEZ1 , AND JOSÉ LUIS ROJO-ÁLVAREZ 2,4, (Senior Member, IEEE) 1Red Eléctrica de España, Alcobendas, 28109 Madrid, Spain 2Department of Signal Theory and Communications, Telematics and Computing Systems, Rey Juan Carlos University, Fuenlabrada, 28943 Madrid, Spain 3D!lemmaLab Ldt Startup, Fuenlabrada, 28943 Madrid, Spain 4Departamento de Ingeniería de Comunicaciones, Universidad Miguel Hernández de Elche, 03202 Elche, Spain
3. Success Factors for Cyber Security Operation Center (SOC) Establishment M. Abd Majid1 , K. A. Zainol Ariffi2
4. A Review on the Role of Modern SOC in Cybersecurity Operations I Putu Elba Duta Nugraha Department of Electrical Engineering, Udayana University, Jimbaran, Badung Regency 80361, Indonesia
5. Security Operations Centers for Information Security, Incident Management, Natalia Miloslavskaya, National Research Nuclear University MEPhI (Moscow Engineering Physics Institute), Moscow, Russia
6. Onwubiko, C. (2015). Cyber security operations centre: Security monitoring for protecting business and supporting cyber defense strategy. 2015 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA).
7. Model for successful development and implementation of Cyber Security Operations Centre (SOC) by Maziana Abd Majid, Khairul Akram Zainol Ariffin.
8. Feng, C., Wu, S., & Liu, N. (2017). A user-centric machine learning framework for cyber security operations center. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI).
9. Schinagl, S., Schoon, K., & Paans, R. (2015). A Framework for Designing a Security Operations Centre (SOC). 2015 48th Hawaii International Conference on System Sciences.
10. Formalizing and Integrating User Knowledge into Security Analytics - Fabian Böhm · Manfred Vielberth · Günther Pernu