Integrated Threat Management: A SIEMSolution with Autoblocking Capabilities for Proactive Cybersecurity

Nanda Kumar[1], Giridhar K R[2], K Aditya Arvind[3], Hruthik Nayak B S[4], Dr.Pallavi G B[5]
Computer Science and Engineering, BMS College of Engineering, Bangalore

Abstract:- In recent years, the surge in cybersecurity risks targeting industrial control systems (ICS) has underscored the need for robust detection and response measures. Integrating Security Information and Event Management (SIEM) systems with Intrusion Detection Systems (IDS) has become a popular strategy, offering comprehensive defense capabilities. Our proposed study focuses on exploring active and passive cyber threats and how SIEM and IDS solutions can effectively counter them. We envision evolving SIEM and IDS systems to provide extensive visibility, enabling proactive threat mitigation and streamlined incident response processes to reduce costs and response times. Additionally, our study aims to identify challenges in current SIEM and IDS implementations and propose enhanced solutions to address these limitations. This includes bolstering the capabilities of SIEM and IDS systems to adapt to and mitigate evolving cyber threats effectively.

1.INTRODUCTION

In the ever-evolving landscape of cybersecurity, organizations face an incessant barrage of threats ranging from sophisticated intrusions to subtle, insidious attacks. To fortify against these challenges, Intrusion Detection Systems (IDS) emerge as indispensable guardians, tirelessly monitoring network activities for anomalous patterns and potential security breaches [9]. IDS serves as a vigilant sentinel, employing advanced algorithms and rule-based analyses to detect malicious behavior, unauthorized access, and emerging threats. With the capacity to distinguish between normal and suspicious activities, IDS plays a pivotal role in proactive threat management, offering real- time alerts and insights crucial for safeguarding digital assets and ensuring the integrity of organizational infrastructures [13]. This introduction sets the stage for a comprehensive exploration of how IDS, within the context of an integrated threat management system, becomes a linchpin in the defence against cyber adversaries, contributing to the resilience and security posture of modern enterprises. Or smart devices. Examples of current cybersecurity incidents affecting IT and ICT are [2]: Ransom ware attacks malware having impact on the utility’s ability to conduct business and operations; phishing campaigns directed to executives, executive assistants, SCADA engineers, IT administrators or other privileged users; business email compromise incidents, including account takeover or impersonation of executives; data leakage and thefts; social engineering to gather sensitive information from personnel.

According to a recent report from NIST [3], cybersecurity solutions in industrial control systems should provide real-time behavioral anomaly detection, enable faster incident management and allow for intelligent visualization of the network and all its interconnected nodes. Security Information and Event Management (SIEM) systems consider the aforementioned capabilities as built-in features.

In general, SIEMs have the capacity to collect, aggregate, store, and correlate events generated by a managed infrastructure [4]. They constitute the central platform of modern security operations centers as they gather events from multiple sensors (intrusion detection systems, anti-virus, firewalls, etc.), correlate these events, and deliver synthetic views of the alerts for threat handling and security reporting [5,6]. Besides these key capacities, there are many differences between the existing systems that normally reflect the different positions of SIEMs in the market.

Several companies have developed SIEM software products in order to detect network attacks and anomalies in an IT system infrastructure. Among them, we can find classical IT companies (e.g., HP, IBM, Intel, McAfee), others with more visionary options (e.g., AT&T Cybersecurity/ SIEMs), and promising tools to be taken into consideration in aSIEM context (e.g., Splunk). In this paper, we review the most widely used security information and event management tools (commercial and open source) aiming at identifying their maincharacteristics, benefits, and limitations to detect and react against current attack scenarios. We provide an in-depth analysis of the features and capabilities of current SIEMs and focus on their limitations in order to propose potential enhancements to be integrated into current SIEM platforms

2. LITERATURE SURVEY

2. Related WORK

2.1 Types of attacks

Cyber threats manifest in a spectrum of techniques, distinguishing between active assaults, where adversaries strive to breach system defences, and passive manoeuvres, focused on extracting information without resource disruption [8]. In active attacks, intruders not only attempt unauthorized access but also manipulate and introduce data within the system. Noteworthy active attack types encompass distributed Denial of Service (DOS), session replay, and masquerade, exemplified by the likes of viruses, worms, and Trojans. Conversely, passive attacks, such as tapping, encryption, and scanning, discreetly aim to acquire information sans system interference. The origin of attacks can be traced to both insiders with authorized access and outsiders engaged in illicit use of systems. Insider attacks involve malicious actions by authorized personnel, whereas outsider attacks, typified by spoofing, spam, and spin, stem from unauthorized external sources [16]. Given this nuanced threat landscape, the incorporation of diverse intrusion detection systems becomes imperative. The subsequent section delves into the intricate components of IDS, elucidates their integration for active and passive attack detection and prevention, and explores the multifaceted applications of various agent types.

Intrusion Responses

Passive IDS: A passive IDS logs the attack and may also raise an alert to notify someone. Most IDS are passive by default. The notification can come in many forms, including an email, a text message, a pop-up window, or a notification on a central monitor.

Active IDS: An active IDS logs and notifies personnel just as a passive IDS do, but it can also change the environment to thwart or block the attack. For example, it can modify access control lists on firewalls to block offending traffic, close processes on a system thatwere caused by the attack, or divert the attack to a safe environment, such as a honeynet or honeypot [17].

Active Intrusion Detection System Design

An Intrusion detection system is designed for detecting both well-known and unknown intrusion behaviours. The system is composed of Intrusion detection system (IDS), management centre and intrusion detection centre.

If any suspected activities are discovered, the corresponding responses of IDS are sent to intrusion detection center for further analyzing. Management has the ability to service agents. The active node can get the desired services from the Management centre according to its needs and environment. It also allows the IDC to update the detection model [19].

Step 1: The node manager creates the mobile agent according to the user configuration and system environment.

Step 2: The designed mobile agent is sent to the management center. The mobile agent negotiates with the management center to get the specific service.

Step 3: The management center which is responsible for providing services can dispatch the appropriate mobile agents to the client according to the information carried by the previous user's mobile agent.

Step 4: When the mobile agent arrives at the client host and reside into the node manager, they begin to perform the assigned tasks or services. Besides, they can communicate with the predefined protocol [17].

In a distributed system, intelligent agents play a crucial role, acting as autonomous entities with the ability to interact and collaborate to achieve specific objectives.

There are three main types of agents in distributed systems:

Agents

Intelligent agent is defined as physical entities (hardware in real world) or virtual entities (software, program) autonomous, able to act in their environment to change it and communicate with other agents. There are three types of agents on distributed systems [20]:

1. Cognitive Agents:
   These agents are characterized by advanced reasoning, processing, learning, perception, and control capabilities. They can solve complex problems through communication with other agents and by leveraging their knowledge databases.
   Role: Cognitive agents contribute to sophisticated decision-making and problem-solving within the distributed system.

2. Reactive Agents:
   Reactive agents are designed to act quickly, particularly suited for solving simple problems that do not require intricate reasoning.
   Role: Reactive agents are efficient in rapid response scenarios, addressing straightforward tasks within the distributed system.

3. Hybrid Agents:
   Hybrid agents combine functionalities of both cognitive and reactive agents, offering a balanced approach that suits a variety of scenarios.
   Role: Hybrid agents provide a flexible and adaptive solution by integrating aspects of advanced reasoning and swift response.

Inter-Agent Communication:

Agents within the architecture communicate through two primary types of information exchange: control flow and data flow.

Control Flow:

Control flow involves exchanges between the core agent, local agents, and probe agents. It encompasses instructionsand rules to modify agent behaviour, such as enabling or disabling local agents, sending configuration files, and adding new rules based on intrusion analysis.

Example: The core agent may instruct local agents to reject connections from a machine detected during an intrusion analysis.

Data Flow:

Data flow facilitates access to data maintained by informational agents and includes exchanges of data, log files, and accounting files between local agents, probe agents, and the core agent.

Example: Local agents share information with the core agent, enabling the system to analyses and respond to security events effectively [20].

2.2 SIEM Solutions

Security Information and Event Management (SIEM) systems have been developed in response to help administrators to design security policies and manage events from different sources. Generally, a simple SIEM iscomposed of separate blocks (e.g., source device, log collection, parsing normalization, rule engine, log storage, event monitoring) that can work independently from each other, but without them all working together, the SIEM will not function properly [3]. Figure 1 depicts the basic components of a regular SIEM solution.

SIEM platforms provide real time analysis of security events generated by network devices and applications. In addition, even though the new generation of SIEMs provide response abilities to automate the process of selecting and deploying countermeasures, current response systems select and deploy security measures without performing a comprehensive impact analysis of attacks and response scenarios.

2.3. SIEM Features and Capabilities

Fundamentally, all SIEMs have the capacity to collect, store, and correlate events generated by a managed infrastructure [4]. Besides these key capacities, there are many differences between existing systems that normally reflect the different positions of SIEMs in the market. This section provides a list of features to be considered in the analysis of SIEM solutions. Based on our experience with different commercial SIEMs and contrasting the identified information related to the usage of commercial and open- source SIEMs from the literature, In

[4] the authors have summarized this analysis and assesses each SIEM feature as low/basic (poorly implemented or not implemented at all), average (partly

implemented), or high/advanced (fully implemented) for the most promising SIEM solutions described in Table 1.

Correlation rules: The success of detecting an event by a SIEM relies on the power of the correlation rules. While most SIEMs possess basic correlation rules, few of them have robust search capabilities and support search processing languages to write complex searches that can be used on the SIEM's data.

Data sources: One of the key features of a SIEM system is the capacity for collecting events from multiple and diverse data sources in the managed infrastructure. Most SIEMs support several types of data sources natively, including both the supported sensors, and the supported data types (e.g., threat intelligence). For other solutions such a feature could be supported by additional components integrated to the SIEM. This feature evaluates the natively supported data sources and the possibility for a SIEM to automatically customize them.

Real time processing: This feature considers the ability of a SIEM to handle real-time data under constant change. It evaluates the real-time controls, monitoring, and pipelining capabilities deployed by the tool in preventing or reacting to cybersecurity incidents, as well as the performance computation capabilities that SIEMs have to analyse millions of events in real time. All the studied SIEMs have advanced real time processing capabilities.

Data volume: Analysing large volumes of data coming from different sources is important to gain more insights from the collected events and to have a better monitoring. However, keeping large volumes of collected data in a live SIEM system is often costly and impractical. This feature evaluates the possibility of current systems to support large volumesof data for correlation, indexing and storage operations.

Visualization: One of the key factors that hinder the analysis of security events is the lack of support for proper data visualization methods and the little support provided for interactive exploration of the collected data. It is therefore important to understand the capabilities of the analysed systemsin terms of creation of new data visualization methods and custom dashboards.

Data analytics: More recent versions of leading SIEMs support extensive integration with application and user-based anomaly detectors. These capabilities include the analysis of the behaviour of employees, third-party contractors, and other collaborators of the organization. For this, the SIEM must comprise the management of user/application profiles and the use of machine learning techniques for detecting misbehaviour.

Performance: This feature evaluates the performance of a SIEMsolution in terms of computational capacity, data storage capabilities (e.g., read/write), rule correlation processing (e.g., high performance correlation engine), as well as datasearch, index, and monitoring.

Forensics: In addition to logging capabilities, some SIEMs (e.g., ArcSight, LogRhythm) offer built-in network forensic capabilities that include full session packetcaptures from network connections considered as malicious aiming at converting packet data into documents, web pages, voice over IP, and other recognizable files. Some other products (e.g., QRadar, Splunk) are able to save individual packets of interest when prompted by a security analyst, but do not automatically save network sessions of interest [15], and the rest of studied solutions have no built-in network forensic capabilities.

Complexity: SIEMs are known for being difficult to deploy and manage. However, it is important to understand if the analysed system can be installed for testing with low or moderate effort. From the eight studied SIEMs, ArcSight is the tool with the highest complexity for deployment and management, whereas LogRhythm and Splunk are seen as easy and friendly tools to install, deploy, and use.

Scalability: This feature considers the ability for a SIEM deployment to grow not only in terms of hardware, but also in terms of the number of security events collected at the edge of the SIEM infrastructure. The new digital transformation leads to more sensors and more devices (e.g., servers, agents, nodes) connected to the same network.

Risk analysis: Recent versions of leading SIEM systems (e.g., QRadar, LogRhythm, Splunk) include features for doing risk analysis on the assets of the managed infrastructure. This feature evaluates if the SIEM natively supports risk analysis or if it can be integrated with external appliances for that purpose.

Storage: Considering that SIEMs generally store information for no more than 90 days, this feature evaluates the length at which current SIEM technologies keep data stored in their systems for further processing and forensics operations.

Price: This feature evaluates the licensing method associated to the SIEM solution (e.g., enterprise, free, beta, premium) and the limits in the number of users, queries, index volumes, alerts, correlations, reports, dashboards, and automated remedial actions. Most of the studied solutions are very expensive, except for LogRhythm, USM, and SolarWinds, with more reasonable costs and the possibility to use open-source solutions with more limited capabilities.

Resilience: Resilience or fault tolerance is an important feature of any critical monitoring system. It is important to understand what the fault tolerancecapabilities of existing SIEMs are, for example, if the correlation engine supports fault tolerance; the way disaster recovery and replication are supported on the event storage; if the connectors support high availability features.

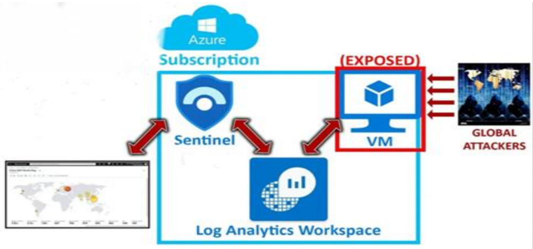

Fig1. Workflow of SIEM , ref [2]

4.MOTIVATION

In an era dominated by rapidly evolving cybersecurity threats, the motivation behind this research lies in the critical need for robust and adaptive defense mechanisms. The incessant barrage of sophisticated intrusions, ransomware attacks, and intricate social engineering tactics poses unprecedented challenges to organizational security. Motivated by the imperative to fortify against these threats, this study delves into the realm of Intrusion Detection Systems (IDS) and Security Information and Event Management (SIEM) tools. By comprehensively examining their capabilities, limitations, and potential enhancements, the research aims to contribute valuable insights to the evolving landscape of cybersecurity.

5. PROBLEM DOMAIN

The. problem domain of cybersecurity within industrial control systems (ICS) encompasses a multifaceted landscape of evolving threats, including active and passive attacks orchestrated by nation-states and cybercriminals. These threats pose significant risks to critical infrastructure, such as utilities and manufacturing facilities, with potential consequences ranging from operational disruptions to compromised safety and integrity. As organizations increasingly rely on interconnected digital systems, the complexity and scale of cyber threats continue to escalate, highlighting the urgent need for robust security measures. Within this domain, challenges persist in effectively detecting and mitigating diverse cyber threats, necessitating innovative solutions that can adapt to evolving attack vectors and provide comprehensive protection for industrial assets andprocesses.

6. PROBLEM DEFINITION

The problem at hand involves addressing the escalating cybersecurity risks faced by industrial control systems (ICS). These systems are increasingly targeted by sophisticated attacks from nation-states and cybercriminals, posing significant threats to critical infrastructure and operational continuity. The challenge lies in effectively detecting and mitigating these diverse cyber threats within ICS environments, necessitating the development of advanced security solutions that can adapt to evolving attack vectors, provide real-time threat intelligence, and ensure the resilience of industrial assets and processes against malicious activities.

7. STATEMENT

The statement encapsulates the pressing need to address escalating cybersecurity risks within industrial control systems (ICS), necessitating the development of advanced security solutions capable of detecting and mitigating sophisticated attacks from nation-states and cybercriminals to safeguard critical infrastructure and ensure operational continuity.

8. INNOVATIVE CONTENT

Integration of Security Information and Event Management (SIEM) Systems: The proposed work aims to explore the integration of SIEM systems within industrial control systems (ICS) to enhance cybersecurity capabilities. By leveraging SIEM's capabilities for real-time event correlation, anomaly detection, and threat intelligence aggregation, the research seeks to provide comprehensive visibility into ICS networks and facilitate proactive threat mitigation strategies. This integration represents an innovative approach to bolstering the resilience of critical infrastructure against evolving cyber threats.

Advanced Intrusion Detection Systems (IDS): The researchexplores advancements in IDS technology, particularly their application within industrial control systems to enhance threat detection capabilities. By leveraging advanced algorithms andrule-based analyses, the study aims to develop IDS solutions capable of identifying anomalous behavior and potential security breaches in real-time. This innovative approach to intrusion detection within ICS environments seeks to bolstercyber resilience by providing early detection and response to emerging threats, thereby minimizing the impact of cyber-attacks on critical infrastructure.

9.PROBLEM FORMULATION

The problem of enhancing cybersecurity within industrial control systems (ICS) can be captured through a comprehensive design methodology that incorporates several key stages:
Identification of Threat Landscape: The first stage involves analyzing the evolving threat landscape facing industrial control systems, considering factors such as the typesof attacks, their origins, and potential impact on criticalinfrastructure. This stage justifies the capture by providing a foundational understanding of the cybersecurity challenges confronting ICS environments.

Requirements Analysis: The next stage focuses on eliciting and prioritizing the requirements for an effective cybersecurity solution tailored to industrial control systems. This involves considering factors suchas real-time threat detection, scalability, interoperability with existing systems, and usability by security operators. Justification for this stage lies in ensuring that the proposed solution addresses the specific needs and constraints of ICS environments.

Model Development: Following requirements analysis, the model development stage involves creating a mathematical model or algorithmic framework that captures the interactions between various components of the cybersecurity solution. This model may include elements such as intrusion detection algorithms, event correlation mechanisms, threat intelligence feeds, and response strategies. Justification for this stage lies in providing a systematic representation of the proposed solution's functionality and logic.

Integration and Testing: The final stage focuses on integrating the components of the cybersecurity solution into a cohesive system and rigorously testing its efficacy in simulated and real-world environments. This involves validating the model against known cyber threats, evaluating its performance metrics (e.g., detection accuracy, false positive rate), and refining the solution based on feedback from testing. Justification for this stage lies in ensuring that the proposed solution is robust, reliable, and capable of effectively mitigating cyber threats within industrialcontrol systems.

In totality, this design methodology provides a structured approach to addressing the problem of enhancing cybersecurity within industrial control systems, capturing the complexities of the threat landscape, requirements of the system, functional aspects through modeling, and validation through integration and testing.

10.LIMITATIONS OF CURRENT SIEMS

Even though the new generation of SIEMs provides powerful features in terms of correlation, storage, visualization, and performance, as well as the ability to automate the reaction process by selecting and deploying countermeasures [8,9], current response systems are very limited and countermeasures are selected and deployed without performing a comprehensive impact analysis of attacks and response scenarios [10].

11.PROPOSED SOLUTION

The proposed "Integrated Threat Management" system incorporates a robust Intrusion Detection System (IDS).

Integration with Intrusion Detection System (IDS):
Seamlessly integrate the Active Blocking Module with the Intrusion Detection System (IDS) for a cohesive defence mechanism.
Active Blocking Module: The Active Blocking Module is responsible for actively preventing and neutralizing detected threats in real-time.It employs predefined countermeasures and responses to disrupt and mitigate the impact of potential intrusions.

Enhanced Visualization Analysis:
Display a visual representation of security events on a global or regional map, using colour gradients to indicate the intensity of incidents in specific geographic areas.

12.DESIGN SPECIFICATION

Components of the System:

1. Log Data Analytics:
Log Data Analytics serves as the eyes and ears of our system, collecting and scrutinizing vast amounts of log data generated across our network. This component is responsible for extracting valuable insights, patterns, and anomalies from the log entries.

2. Sentinel with APIs:
Sentinel, fortified with APIs (Application Programming Interfaces), acts as a central nervous system, connecting and coordinating various elements of our cybersecurity infrastructure. It serves as a communication hub, facilitating seamless interaction between different components.

3. Intrusion Detection System (IDS):
The IDS is our digital watchdog, constantly monitoring network activities for signs of malicious behaviour. It complements the insights derived from Log Data Analytics by focusing specifically on detecting and thwarting potential threats.

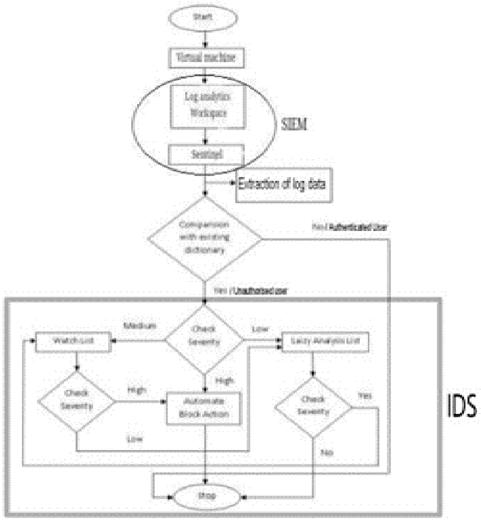

Fig2. Design specification of proposed system

13.CONCLUSIONS

In the dynamic realm of cybersecurity, the Integrated Threat Management System (ITMS) stands as a digital fortress, shielding our online presence from a spectrum of potential threats. Imagine it as a vigilant guardian equipped with advanced capabilities to detect and neutralize cyber adversaries. What sets ITMS apart is its proactive nature – it doesn't merely detect threats; it learns,adapts, and actively prevents them. Like a digital superhero, it leverages past experiences to anticipate and thwart evolving cyber tactics. When a threat is identified, it doesn't hesitate to deploy countermeasures, ensuring our digital assets remain secure Computer-wide and widely available online shopping. The purpose of the development is to provide a fun and inviting shopping experience controlled by a virtual reality Tablet.

REFERENCES

[1] González-Granadillo, G.; González-Zarzosa, S.; Diaz,R. Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors 2021, 21, 4759. https://doi.org/10.3390/s21144759

[2] WaterISAC. 15 Cybersecurity Fundamentals for Water and Wastewater Utilities. Best Practices to reduce Exploitable Weaknesses and Attacks. Available online: https://www.waterisac.org/system/files/articles/15%20 Cyberse curity%20Fundamentals %20%28WaterISAC%29.pdf (accessed on 14 December 2020).

[3] CyberX. NIST Recommendations for IoT & ICS Security. An Executive Summary. White Paper. Available online: https://cyberx-labs.com/resources/nist-recommendations-for- iot-ics- security/ (accessed on 10 November 2020).

[4] Miller, D.; Harris, S.; Harper, A.; Van Dyke, S.; Blask,C. Security Information and Event Management (SIEM) Implementation; Mc Graw Hill: New York, NY, USA, 2010. [Google Scholar]

[5] Granadillo, G.G.; El-Barbori, M.; Debar, H. New types of Alert Correlation for Security Information and Event Management Systems. In Proceedings of the 8th International Conference on New Technologies, Mobility and Security, NTMS, Larnaca, Cyprus, 21– 23 November 2016. [Google Scholar]

[6] Bryant, B.D.; Saiedian, H. Improving SIEM alertmetadata aggregation with a novel kill-chain based classification model. Comput. Secur. 2020, 94. [Google Scholar] [CrossRef]

[7] Nicolett, M.; Kavanagh, K.M. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online: http://docplayer.net/2407833- Magic- quadrant-for-security-information-and-event-management.html (accessed on 10 November 2020).

[8] Nicolett, M.; Kavanagh, K.M. Magic Quadrant for Security Information and Event Management, Gartner Technical Report.Availableonline:https://www.novell.com/docrep/documents/yuufbom4u2/gartner_magic_quadrant_siem_report_may2011.pdf (accessed on 12 November 2020).

[9] Nicolett, M.; Kavanagh, K.M. Magic Quadrant for Security Information and Event Management, Gartner Technical Report.Available online: https://www.bankinfosecurity.com/whitepapers/2012-gartner- magic-quadrant-for-siem-w-602 (accessed on 12 November2020).

[10] Nicolett, M.; Kavanagh, K.M. Magic Quadrant for Security Information and Event Management, Gartner Technical Report.Available online:https://www.gartner.com/en/documents/2477018/magic- quadrant-for-security-information-and-event-manage (accessedon 25 November 2020).

[11] Nicolett, M.; Kavanagh, K.M.; Rochford, O. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online: https://www.bwdigitronik.ch/ application /files/5814/5450/756 5/www.gartner.com.com.pdf (accessed on 25 November 2020).

[12] Kavanagh, K.M.; Rochford, O. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online: https://www.gartner.com/en/documents/3097022/magic-quadrant-for-security-information-and-event-manage (accessedon 10 November 2020).

[13] Kavanagh, K.M.; Rochford, O.; Bussa, T. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online: https://securelink.net/wp-content/uploads/sites/7/2016- Magic- Quadrant-for-SIEM.pdf (accessed on 10 November 2020).

[14] Kavanagh, K.M.; Bussa, T. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online: https://www.gartner.com/en/documents/3834683/magic-quadrant-for-security-information-and-event-manage (accessedon 12 November 2020).

[15] Kavanagh, K.M.; Sadowski, T.B.G. Magic Quadrant for Security Information and Event Management, Gartner Technical Report. Available online:

https://virtualizationandstorage. files.wordpress.com/2018/03/ magic-quadrant-for-security-information-and-event-3-dec- 2018.pdf (accessed on 10 November 2020).

[16] A survey on Intrusion Detection System (IDS) and Internal Intrusion Detection and protection system (IIDPS) Published