Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6, 4319-4348
2024
Publisher: Learning Gate
DOI: 10.55214/25768484.v8i6.2933

Leveraging Microsoft sentinel and logic apps for automated cyber threat response

Vedran Dakić[1*], Zlatan Morić[2], Ana Kapulica[3], Damir Regvart[4]
[1,2,3,4]Algebra University, Croatia; vedran.dakic@algebra.hr (V.D.) zlatan.moric@algebra.hr (Z.M.) ana.kapulica@algebra.hr (A.K.) damir.regvart@algebra.hr (D.R.)

Abstract: An integrated approach to automated cyber threat response is explored in this paper, with Microsoft Sentinel's Security Information and Event Management (SIEM) capabilities being leveraged alongside Logic Apps' workflow automation within the Azure ecosystem. Efficient identification and automated mitigation of security incidents are enabled by a combination of AI-driven analytics and advanced threat-hunting capabilities, resulting in a substantial reduction of manual intervention and response times. The approach is demonstrated to contribute scientifically across three core areas: (1) a novel integration of Sentinel's SIEM with Logic Apps is proposed to streamline response workflows using automated playbooks; (2) the effectiveness of the system is assessed through multiple cyber threat scenarios, including automated account blocking and virtual machine isolation in response to identified threats; and (3) Sentinel's performance is evaluated relative to other SIEM solutions, such as Splunk and IBM QRadar, particularly in Azure-centric and hybrid environments. The potential of Microsoft Sentinel and Logic Apps to advance proactive cybersecurity defenses is underscored, while key limitations in scalability and cross-platform adaptability are also identified.

Keywords: *Automatic response, Cyber threats; Cybersecurity, Logic apps, Microsoft sentinel, Security solutions.*

1. Introduction

The ongoing challenges presented by the increasing sophistication and frequency of cyber threats are faced by organizations striving to maintain effective defenses. It has been observed that traditional manual threat response methods are no longer sufficient, leading to the conclusion that automated solutions are considered indispensable. The development of Microsoft Azure Sentinel, a cloud-native Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) platform, was undertaken specifically to address these needs in cloud computing environments. Advanced AI-driven analytics are leveraged by Sentinel, and seamless integration with the Microsoft ecosystem is provided, resulting in a robust tool for monitoring and responding to security incidents. Accompanying this, workflow automation across diverse applications and systems is enabled by Microsoft's Logic Apps, allowing for streamlined, scalable responses to identified threats.

The combined use of Microsoft Sentinel and Logic Apps for automated cybersecurity responses is explored in this paper, with a focus on the interaction of these technologies in the detection, management, and neutralization of cyber threats. The Kusto Query Language (KQL) is identified as a key component of this approach, with advanced threat-hunting and analytics capabilities being powered within Sentinel. Custom detection rules and automations are enabled, facilitating a rapid response. Furthermore, the application of Logic Apps as automated playbooks, which are tightly integrated with Sentinel, is evaluated in this research to enable

* Correspondence: vedran.dakic@algebra.hr

prompt and efficient responses to cyber incidents and to assess the effectiveness of these solutions for specific threat scenarios.

Three core contributions are made by the paper. (1) A novel integration of Sentinel's SIEM capabilities with Logic Apps is introduced and assessed to streamline cybersecurity automation, with automated responses to threats being directed by AI-driven analytics. The practical implications of this approach are examined through multiple cyber threat scenarios, with the system being showcased as capable of automating responses, including the blocking of compromised accounts and the isolation of affected virtual machines. (3) A comparative analysis of Sentinel against leading SIEM solutions such as Splunk and IBM QRadar is provided, with an evaluation of the advantages and limitations of each in various deployment contexts.

Following the introduction of these technologies, a review of related works is presented, followed by a description of the experimental setup and deployment processes. The threat scenarios and responses are detailed in the evaluation section, an analysis of the system's effectiveness is provided, and recommendations for future research are presented.

2. Related Works

The cloud-native SIEM platform Microsoft Azure Sentinel, linked with the Microsoft ecosystem, has drawn much interest. However, a thorough literature analysis reveals that many studies have compared the functionality, scalability, security, and integration of different cloud-based SIEMs. These studies frequently compare Microsoft Azure Sentinel to rivals like Google (Mountain View, CA, US) Cloud Platform (GCP) and Amazon (Seattle, WA, US) Web Services (AWS), providing information about which platform could best suit a given organization's functionality, security, and pricing needs.

In their 2020 comparison of cloud platforms, Wankhede et al. focused on the networking, security, database, and artificial intelligence (AI) capabilities of Amazon, Microsoft Azure, and Google Cloud. By integrating Azure Sentinel into its ecosystem and automating attack responses, Microsoft Azure gains a distinct advantage over other Azure services. Nevertheless, AWS and Google Cloud offer sophisticated machine learning (ML) and security services as competitive alternatives [1]. Similarly, Rajendran et al. (2023) compared Azure and AWS performance. They discovered that while AWS provides more comprehensive ML capabilities and easier deployment, Azure excels in critical metrics like download and inference times [2].

Muhammed and Ucuz (2020) compared the IoT cloud platforms offered by Microsoft Azure, AWS, and Google Cloud, emphasizing analytics and security features. All three platforms provide complete IoT solutions, but Azure jumped out due to its native AI integration with SIEM tools and more sophisticated analytics [3]. This bolsters the idea that users may benefit significantly from Azure Sentinel's integration capabilities regarding real-time data-driven threat analysis and mitigation.

In their 2020 study, Copeland and Jacobs concentrated on the network security capabilities of Microsoft Azure, demonstrating how Azure Sentinel uses artificial intelligence and machine learning to lower the false positive rate in alerts and increase the efficiency of the Security Operations Center (SOC) teams. Comparing Azure Sentinel to rivals still honing their automation skills, this AI integration is a crucial differentiation [4]. A comparison of the computational resources provided by AWS, Azure, and Google Cloud was carried out by Kelley et al. (2020). According to their analysis, Microsoft Azure is the go-to option for many computes intensive operations. Still, only some distinctions exist across the platforms, which shows how competitive these services are in the cloud SIEM market [5].

In comparison of cloud computing systems, Chauhan (2020) pointed out that while AWS, Google Cloud, and Azure all provide comparable services, Azure has an edge over the others

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

due to its scalability and range of services, which includes the integration of sophisticated SIEM solutions like Azure Sentinel. The report also mentioned Azure's improved automation capabilities with Logic Apps and security features [6]. In their assessment of AWS, Azure, and Google Cloud's performance in cloud computing environments, Kaushik et al. (2021) confirmed Azure's superior performance in threat detection scenarios, especially when processing vast amounts of data in real-time [7].

Azure's significance in IoT and cloud computing was underscored by K and Davis (2022). They pointed out that Azure's AI and ML capabilities greatly enhance the identification of security risks in real-time environments. This capability is essential to Azure Sentinel's potency as a cloud-native SIEM platform [8]. An early examination of Azure's deployment and administration capabilities was given by Copeland et al. (2015). These capabilities have since improved by adding AI-powered tools such as Sentinel, establishing Azure as a market leader for cloud SIEM solutions [9].

After thoroughly examining Azure's cloud infrastructure, including SIEM implementations, Alamsyah and Febrianto (2021) concluded that the platform's scalability and interaction with Logic Apps make it the best option for companies wishing to automate threat response [10]. Suryawan et al. (2020) supplied additional information regarding the intricacy of moving on-premises apps to Azure App Service – which facilitates the integration of Azure Sentinel for improved security monitoring [11].

In their cognitive research of AWS and Azure for web application deployment, Sharma et al. (2020) discovered that Azure's sophisticated security and AI technologies provided a more reliable defense against web-based threats. This trait is essential for SIEM implementations [12]. In their 2020 study, Pierleoni et al. looked at how IoT and cloud platforms like Azure and AWS integrated, and they found that Azure's cloud and IoT services offer a complete SIEM solution for tracking and controlling security threats in IoT environments [13].

Azure's IoT platform capabilities, which are tightly coupled with Azure Sentinel to offer seamless security across IoT devices and systems, were highlighted by Bansal (2020), bolstering Azure's standing in the cloud SIEM market [14]. Chilberto et al. (2020) discussed how building solutions in Azure differs from traditional on-premises development, focusing on the security benefits of Azure's integration with Azure Sentinel, which allows organizations to automate their security responses [16]. Tiutiunnyk and Rybachok (2021) highlighted the flexibility of Azure's architecture, which allows for scalable security solutions, including SIEM implementations, making it ideal for organizations with complex security needs [15]. In their comparative analysis of cloud providers, Tasnim et al. (2022) emphasized Azure's superior security capabilities, which make it an excellent option for businesses using SIEM systems [17].

When comparing Azure's MLOps capabilities to those of AWS and Google Cloud, Moutaouakal and Baïna (2023) discovered that Azure has a significant advantage in automating and improving security operations due to its incorporation of ML into its SIEM products, such as Azure Sentinel [18]. Lastly, Zibitsker and Lupersolsky (2020) concentrated on how businesses might evaluate and model cloud platforms to choose the best SIEM solution. They found that Azure is the best option for many companies trying to strengthen their security posture because of its flexibility and automation capabilities [19].

3. Microsoft Sentinel, Logic Apps, Kusto Query Language and Analytic Rules

This section will briefly overview advanced tools and technologies used for security monitoring, data querying, and workflow automation for security footprint management and reporting.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

3.1. Microsoft Sentinel

Microsoft Sentinel is a cloud-based SIEM system offering organizations advanced security analytics and threat intelligence essential in cybersecurity [20]. As with other SIEM solutions, it has evolved into a comprehensive system that offers extensive visibility, enabling the identification of high-risk areas and proactive mitigation strategies to minimize costs and incident response time [21]. Artificial intelligence and automation immediately identify potential dangers and take quick action, improving security measures' effectiveness. Sentinel can also use ML as a viable approach to reduce the false positive rate and enhance the productivity of SOC analysts [22]. Due to its scalability, smooth integration with diverse data sources, and extensive analytical capabilities, Microsoft Sentinel is a potent tool for complete and proactive cybersecurity management. Gartner Magic Quadrant for SIEM report indicates that Microsoft Sentinel is a leader in SIEM solutions.

Microsoft Azure Sentinel is crucial for contemporary cybersecurity because its cloud-native architecture enables scalability and adaptability. The system employs sophisticated artificial intelligence and machine learning techniques to identify potential dangers accurately and offers thorough surveillance across on-site, mixed, and multi-cloud settings. Sentinel streamlines incident response, effortlessly integrates with other security solutions, provides cost-effectiveness with a pay-as-you-go model, and improves proactive protection through continuous monitoring and threat hunting, greatly enhancing an organization's overall security stance.

3.2. Logic Apps

Microsoft Sentinel utilizes the Logic Apps solution to automate actions. Playbooks are Logic Apps that utilize the Microsoft Sentinel connector to initiate automated actions. These two components enable the Logic App to retrieve targeted data and perform actions like isolating virtual machines in Azure Active Directory or extracting JSON objects, as demonstrated in the project's practical portion. Logic Apps enable a seamless connection with any Azure application. Logic apps can be constructed using custom code or the designer console.

Obtaining security information from multiple sources inside the business environment is essential to produce alerts and events. This data can consist of log logs or threat intelligence data. The logs contain various security information related to the IT system, such as system logs, security devices, and identification data. Microsoft defines threat intelligence data as widely recognized information about threats and vulnerabilities gathered from external sources. An example of an external source is the TAXII service, a protocol used to convey cyber threat data over HTTPS.

3.3. Kusto Query Language

A substantial volume of data acquired from many sources must be sorted and presented visually. KQL is a linguistic tool used to analyze data, identify inconsistencies within the provided data, and perform additional functions. The query utilizes databases, tables, columns, and schema components organized in a hierarchical structure akin to SQL.

To illustrate the capabilities of KQL, consider the following query, which may monitor Office 365 activity logs and detect suspicious inbox rules containing keywords:

```
Let Keywords = dynamic(["helpdesk", " alert", " suspicious", "fake", "malicious", "phishing", "spam", "do not click", "do not open", "hijacked", "Fatal"]);
OfficeActivity
```

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

```
    | where OfficeWorkload =~ "Exchange"
    | where Operation =~ "New-InboxRule" and (ResultStatus =~ "True" or ResultStatus =~ "Succeeded")
    | where Parameters has "Deleted Items" or Parameters has "Junk Email" or Parameters has "DeleteMessage"
    | extend Events=todynamic(Parameters)
    | parse Events with * "SubjectContainsWords" SubjectContainsWords '}'*
    | parse Events with * "BodyContainsWords" BodyContainsWords '}'*
    | parse Events with * "SubjectOrBodyContainsWords" SubjectOrBodyContainsWords '}'*
    | where SubjectContainsWords has_any (Keywords) or BodyContainsWords has_any (Keywords) or SubjectOrBodyContainsWords has_any (Keywords)
    | extend ClientIPAddress = case( ClientIP has ".", tostring(split(ClientIP,":")[0]), ClientIP has "[", tostring(trim_start(@'[[]',tostring(split(ClientIP,"]")[0]))), ClientIP )
    | extend Keyword = iff(isnotempty(SubjectContainsWords), SubjectContainsWords, (iff(isnotempty(BodyContainsWords),BodyContainsWords,SubjectOrBodyContainsWords )))
    | extend RuleDetail = case(OfficeObjectId contains '/' , tostring(split(OfficeObjectId, '/')[-1]) , tostring(split(OfficeObjectId, '\\') [-1]))
    | summarize count(), StartTimeUtc = min(TimeGenerated), EndTimeUtc = max(TimeGenerated) by Operation, UserId, ClientIPAddress, ResultStatus, Keyword, OriginatingServer, OfficeObjectId, RuleDetail
    | extend AccountName = tostring(split(UserId, "@")[0]), AccountUPNSuffix = tostring(split(UserId, "@")[1])
    | extend OriginatingServerName = tostring(split(OriginatingServer, " ")[0])
```

Code 1: KQL Malicious Inbox Query [23]

The inquiry commences by generating a "Keywords" inventory. The keywords encompass terminology such as "helpdesk," "alert," "suspicious," "fake," "malicious," and others. Next, filters are applied to the "OfficeActivity_CL" database as it contains entries about developing new Inbox rules. Once the table has been filtered, it is crucial to filter the pertinent parameters further. This will narrow down the events by only selecting those that contain parameters mentioning "Deleted Items" or "Junk Email". These parameters show the actions related to moving emails to these folders. Extracting the parameter details and saving them as a dynamic object called "Events" is imperative to facilitate data manipulation.

Subsequently, the values are retrieved from the "SubjectContainsWords" field within the "Events" object, as well as from the "BodyContainsWords" and "SubjectOrBodyContainsWords" fields within the same object. Once the values have been obtained, the query verifies if any extracted words correspond to predetermined keywords from the initially defined "Keywords" list. Ultimately, the customer's IP address is ascertained using the available information. The "ClientIP_s" field accommodates many formats, including circumstances where the IP address is enclosed in parenthesis or includes port information. Subsequently, a novel "Keyword" field is introduced, derived from previous fields, with precedence given to "SubjectContainsWords", followed by "BodyContainsWords" if it is not devoid of content, and ultimately "SubjectOrBodyContainsWords" if the former options are vacant. A new field called "RuleDetails" is constructed by extracting additional information from the "OfficeObjectId_s" column. Ultimately, the outcomes are consolidated by tallying impressions, ascertaining the commencement and conclusion times, and categorizing them

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

based on several categories such as "Operation_s," "UserId__s," "ClientIPAddress," "ResultStatus_s," "Keyword," "OriginatingServer_s," "OfficeObjectId_s," and "RuleDetail." The fields produced by the "summarize" and "extend" operators for the "RuleDetail" in a specific query are primarily valuable for executing a query directly or for ad-hoc analysis. When implementing an analytics rule in Microsoft Sentinel, these fields will not be immediately relevant or utilized to generate an incident.

Inbox rules enable users to establish laws that autonomously regulate the arrival of emails. These rules can involve automatically relocating emails from one folder to another based on specific keywords or if they originate from a particular sender.

3.4. Analytic Rules

Microsoft Sentinel employs analytic rules, and pre-established or user-created logical expressions designed to identify and recognize patterns, anomalies, or occurrences associated with the gathered data. The analytic principles are derived from the query syntax of the Kusto Query Language. Utilizing the complete query makes establishing an analytics rule within Microsoft Sentinel feasible, enabling the generation of incidents and alerts. Figure 1 illustrates the process of creation of an analytical rule:

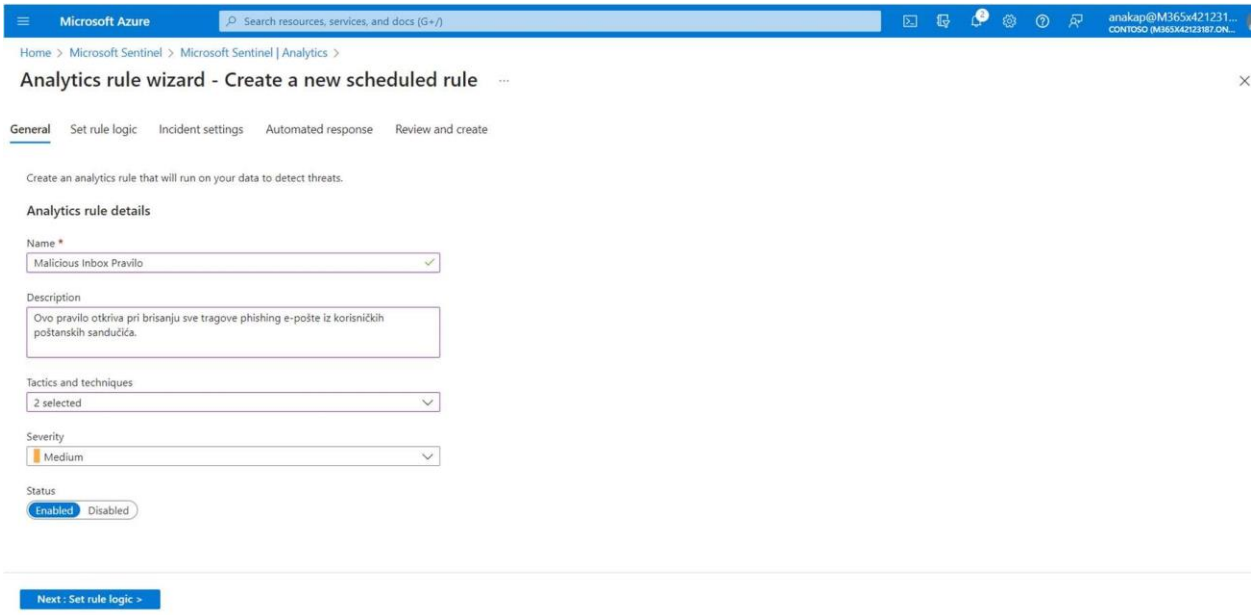

Figure 1.
Creating an analytic rule, "Malicious Inbox Rule."

Once the information about the rule, including its name, description, tactics, and strategies utilized, and the warning's importance, has been provided, the crucial step of including the Kusto Query Language query in the rule follows. This query, the backbone of the rule, can then be executed as a test without delay.

4. Comparative Analysis, AI/ML Integration, Ecosystem Consideration, Ethical And Privacy Consideration

Advanced threat detection and response capabilities are offered by Microsoft Azure Sentinel, which are enhanced by artificial intelligence (AI) and machine learning (ML). The real-time identification and mitigation of security threats are significantly enhanced by these

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

technologies. In a competitive market of cloud-based Security Information and Event Management (SIEM) solutions, distinct strengths and limitations are presented by each platform, including Splunk, IBM QRadar, and Google Chronicle. The evaluation of these SIEM solutions is guided by key criteria, which include scalability, compatibility within diverse ecosystem architectures, and the capacity for efficient management of complex, heterogeneous data sources.

The integration of AI/ML into SIEM platforms is reshaping the field of cybersecurity, with an amplified importance placed on the scrutiny of ethical and privacy considerations, particularly in relation to the handling of sensitive data. The reliance on AI/ML for the detection and response to security incidents is necessitated by the need for transparent, ethical frameworks that are aimed at mitigating risks associated with data privacy and bias in automated decision-making processes. In light of these implications, a comparative analysis of Azure Sentinel's functionality relative to other leading SIEM systems is conducted, with an emphasis placed on scalability, AI and ML integration, compatibility across ecosystem configurations, and ethical considerations that are critical to its implementation and deployment.

4.1. Comparative Analysis With Other Cloud SIEMs

Microsoft Azure Sentinel, a cloud-based SIEM and SOAR platform, leverages artificial intelligence (AI) and machine learning (ML) to deliver advanced security analytics and threat intelligence, positioning itself as a core component for comprehensive cybersecurity management in Azure-heavy environments. Sentinel's design seamlessly integrates with other Azure services and provides numerous built-in connectors that streamline integration with a variety of third-party tools and security information sources. With its robust threat-hunting capabilities powered by the Kusto Query Language (KQL), Sentinel facilitates detailed data analysis and detection of anomalies, allowing security teams to engage in complex threat hunting with high efficiency. Its scalability enables organizations to process substantial data volumes with low latency, supporting expansive monitoring in real time. Furthermore, Sentinel's pay-as-you-go pricing structure enables flexible expense management, billing users based on actual data ingestion, which is particularly advantageous for organizations with fluctuating data flows.

IBM QRadar on Cloud, part of IBM's extensive SIEM ecosystem, combines cloud and on-premises capabilities to offer detailed insights through centralized aggregation of logs, network flows, and event data. QRadar excels in behavioral analytics and anomaly detection, which are essential for identifying advanced threats and reducing false positives in complex environments. QRadar's extensive integration with a range of IT and security systems enhances its incident response capabilities, making it well-suited for enterprises with hybrid or multi-cloud infrastructures. QRadar also offers configurable dashboards and automated reporting, aiding compliance management by mapping detected threats to regulatory requirements, an essential feature for industries facing stringent compliance obligations. [24]

Splunk Cloud provides a high-performance, cloud-native SIEM that specializes in big data analytics and machine data visualization. It stands out for its real-time data ingestion and processing capabilities, which allow enterprises to efficiently search, analyze, and visualize large data volumes across diverse sources. Splunk's app ecosystem, combined with its advanced Search Processing Language (SPL), gives users exceptional flexibility to customize queries and automate analysis, supporting a high degree of customization that is advantageous for data-driven security event management. However, due to its data-volume-based pricing model, costs

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

may increase significantly with higher data ingestion rates, presenting a consideration for organizations with large or growing data needs. [25]

Google Chronicle, a cloud-native SIEM solution built on Google's infrastructure, prioritizes speed, scalability, and simplicity. Its architecture allows rapid data ingestion and processing at petabyte-scale with minimal latency, which is advantageous for organizations that require high-throughput analysis in real time. Chronicle's long-term data retention, which defaults to one year at a fixed rate, benefits organizations with extensive compliance and historical data analysis requirements. Although Chronicle's design emphasizes ease of use and cost transparency, its customization capabilities are somewhat limited compared to other SIEM solutions, which may pose constraints for enterprises needing highly tailored solutions.

Comparatively, Microsoft Sentinel is ideal for enterprises seeking deeply integrated, AI-enhanced security analytics within the Microsoft ecosystem. Its design simplifies implementation in Azure-centric environments, offering robust native integration with Microsoft Defender, Azure Active Directory, and other Azure services, creating a comprehensive security framework optimized for Azure-heavy infrastructures. IBM QRadar on Cloud is well-suited for companies that require advanced behavioral analytics and seamless integration across hybrid environments, as it supports both cloud and on-premises systems, enabling flexible deployment in mixed infrastructure setups. Splunk Cloud's capabilities in big data analysis, customization, and visualization make it the preferred choice for enterprises focused on extensive data analytics and high customization. Google Chronicle, with its unmatched scalability and ease of use, appeals to organizations needing rapid, scalable data processing within Google's infrastructure.

Table 1.
Comparison of cloud-based SIEM platforms: azure sentinel, IBM QRadar, Splunk cloud, and Google Chronicle.

Platform	Advantages	Disadvantages	Speed/Complexity Metrics
Microsoft azure sentinel	- Seamless integration with Azure ecosystem - AI/ML for advanced threat detection - Pay-as-you-go pricing	- Limited integration in multi-cloud environments - Steep learning curve for non-Azure users	- High scalability with real-time data processing - Complex KQL language requires expertise
IBM QRadar	- Robust threat detection with behavioral analytics - High integration with on-premise systems	- Expensive in high-volume deployments - Limited user interface customizability	- Rapid anomaly detection with optimized incident response
Splunk cloud	- Flexible, powerful search processing (SPL) - Extensive app ecosystem for customization	- Costs increase significantly with data volume - Steep learning curve for advanced features	- Fast real-time processing for large data sets - Complex queries can add latency in high volumes
Google chronicle	- High-speed data processing at	- Limited customization and	- High ingestion speed

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

	petabyte scale - - User-friendly with transparent pricing	integration outside Google services	- Fixed one-year data retention

Distinct features and strengths are offered by Microsoft Azure Sentinel, IBM QRadar, Splunk Cloud, and Google Chronicle within the realm of Security Information and Event Management (SIEM). Azure Sentinel is recognized for its seamless integration with Microsoft tools and AI/ML capabilities, which enable rapid threat detection and automated response workflows, as it is native to the Microsoft Azure ecosystem. Efficiency in threat hunting and scalability are recognized as factors that render it well-suited for Azure-based environments that handle extensive data volumes. The threat detection capabilities of Sentinel, utilizing Kusto Query Language (KQL), enable the crafting of detailed queries by security teams for the purpose of facilitating faster incident response. However, the complexity of KQL may require additional training for users who are not experts.

In contrast, it is noted that IBM QRadar excels in handling both cloud and on-premises environments, which positions it as a strong choice for hybrid infrastructures. The strength of QRadar is attributed to its behavioral analytics, which contributes to the improvement of anomaly detection accuracy, the reduction of false positive rates, and the enhancement of alert precision. The configurability of QRadar and the comprehensive dashboards provided are also beneficial for compliance management, which is considered a crucial feature for industries that are subject to stringent regulatory requirements.

The powerful data processing and customization abilities of Splunk Cloud are recognized, and extensive data analytics with real-time visibility across diverse data sources is supported. The Search Processing Language (SPL) of the platform is characterized by high levels of customization; however, it is acknowledged that this flexibility may introduce increased complexity, which could result in slower responses when faced with high data volumes. Furthermore, it has been observed that the data-volume-based pricing model of Splunk Cloud may lead to escalating costs for organizations with high ingestion needs, particularly when compared to the flat-rate pricing of Google Chronicle.

Google is leveraged by Google Chronicle to provide high-speed data ingestion and minimal latency, even at petabyte scales, thereby rendering it suitable for large-scale data analysis. The fixed-rate, one-year data retention policy is designed to enhance transparency in pricing and to support organizations with compliance or historical analysis needs. However, it has been observed that the customization options of Chronicle are more limited, which may potentially constrain enterprises that require tailored configurations for specialized threat scenarios.

Each SIEM platform is designed uniquely to meet distinct organizational requirements, tailored to specific infrastructure and operational needs. The seamless integration of Microsoft Azure Sentinel within the Azure environment is noted, with the Microsoft ecosystem being leveraged for a streamlined and efficient experience. Strong adaptability within hybrid configurations is offered by IBM QRadar, which makes it an attractive choice for organizations that are managing both on-premises and cloud-based resources. The distinguishing features of Splunk Cloud include powerful analytics and high customization capabilities, which are catered to enterprises that prioritize extensive data analysis and flexible configurations. High-throughput data management and operational simplicity are emphasized by Google Chronicle, rendering it ideal for large-scale environments that prioritize speed and ease of use. It has been observed that Azure Sentinel is optimal for organizations that are deeply embedded in Azure-native environments. However, it has been noted that enterprises operating across hybrid or

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

multi-cloud settings may find that the versatility of QRadar or the flexibility of Splunk Cloud is better suited to their diverse and complex needs.

4.2. Machine Learning And AI/ML Integration

Machine learning and artificial intelligence are essential elements of contemporary SIEM platforms, augmenting their capacity to identify, address, and alleviate security threats. Microsoft Sentinel, IBM QRadar, Splunk Cloud, and Google Chronicle all integrate AI/ML to enhance threat detection precision and diminish the incidence of false positives that encumber security analysts.

Microsoft Sentinel employs sophisticated AI algorithms for real-time threat intelligence and anomaly identification. Using Microsoft's comprehensive cloud infrastructure and data from Azure's security services, Sentinel can accurately identify suspicious activity. Machine learning models are trained on extensive datasets, enabling them to discern trends in network traffic, user behavior, and security records. These models are particularly effective in identifying insider threats, zero-day vulnerabilities, and advanced persistent threats (APTs), frequently neglected by conventional rule-based systems. Sentinel employs machine learning to prioritize warnings, guaranteeing that serious problems receive quick attention while less significant occurrences are managed automatically through playbooks integrated via Logic Apps [26].

IBM QRadar utilizes AI and machine learning to enhance its SIEM functionalities. QRadar's Watson AI technology is instrumental in the analysis of security issues. Watson aggregates security data from many sources, employs cognitive analytics, and delivers incident insights derived from historical data. Deep learning models are enhanced progressively, enabling QRadar to correlate various indications of compromise (IOCs) across network settings and facilitating the early detection of intricate, multi-stage attacks. This cognitive method aids in contextualizing security incidents, enabling security professionals to comprehend what transpired and the reasons and mechanisms behind them [27].

Splunk Cloud, recognized for its data analytics functionalities, incorporates machine learning via the Splunk Machine toolkit (MLTK). This tool set enables enterprises to develop bespoke machine-learning models for predicting security problems and detecting abnormalities in real-time. Splunk's AI-driven insights assist security teams in forecasting future assaults by examining historical threat trends, which is especially beneficial for identifying non-signature-based threats such as zero-day exploits. Splunk's anomaly detection models are adaptable, enabling enterprises to customize their detection systems according to their security needs and threat environments [28].

Machine learning provides two essential benefits on these platforms: scalability and adaptability. In contrast to conventional SIEM systems that depend on static rule-based engines, AI-driven SIEMs can adjust to emerging risks. Machine learning models can undergo continual training, enabling them to identify new attack vectors that may not align with established security protocols. This adaptability is essential as cyber threats grow increasingly sophisticated, frequently incorporating multi-stage operations that combine social engineering, malware, and data exfiltration [29].

Furthermore, AI and ML reduce the time necessary for danger identification and response. By automating everyday operations such as log analysis, alert triage, and incident correlation, AI allows security analysts to concentrate on more complex investigations, thus enhancing overall SOC efficiency. Research demonstrates that AI-driven SIEMs can decrease incident response durations by as much as 70%, making them essential for alleviating the effects of cyberattacks [30].

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

Nonetheless, integrating AI and ML poses obstacles, especially with model correctness and the necessity for high-quality training data. An ML model trained in incomplete or biased data may produce false positives or fail to identify authentic threats. Regularly updating AI/ML systems with precise threat intelligence is crucial for sustaining their effectiveness. Moreover, there are apprehensions regarding the ethical use of AI, especially with data processing and utilization in threat detection, necessitating further investigation.

Incorporating AI and machine learning in cloud-native SIEMs such as Microsoft Sentinel, IBM QRadar, Splunk Cloud, and Google Chronicle is revolutionizing cybersecurity. These platforms provide enhanced threat detection accuracy, expedited incident response times, and superior adaptability to emerging threats. As AI/ML technologies advance, their significance in SIEM platforms will become increasingly vital for sustaining strong cybersecurity measures in complex digital landscapes.

4.3. Ecosystem Considerations

The cybersecurity environment is crucial in assessing the efficacy of an SIEM platform. Microsoft Sentinel is intricately embedded inside the Microsoft Azure environment, providing specific advantages for enterprises that predominantly utilize Microsoft services. The seamless connection with Azure Active Directory, Microsoft Defender, and Office 365, along with other Azure-native services, establishes a unified security framework that can effortlessly expand across large companies. This seamless integration enables Sentinel to deliver comprehensive threat detection, encompassing identity management, device security, and network monitoring inside a unified ecosystem [31].

One of the prominent aspects of Sentinel is its inherent integration with Azure services, enabling real-time monitoring and threat detection across Azure workloads. This connection encompasses the Azure Monitor and Azure Security Center, offering comprehensive insights into system health and potential security vulnerabilities. The close integration with Azure services facilitates the swift deployment of automated playbooks using Logic Apps, optimizing responses to threats, including ransomware assaults, DDoS attempts, and insider threats. Organizations utilizing Azure's cloud services can fully leverage Sentinel's functionalities without investing in third-party security solutions [32].

Nonetheless, Sentinel's pronounced emphasis on Azure may provide a constraint for enterprises operating inside multi-cloud or hybrid cloud frameworks. Companies utilizing AWS or Google Cloud alongside Azure may perceive Sentinel's close integration as a double-edged sword. Although Sentinel may assimilate data from AWS and Google Cloud, its efficiency may not be as fluid as its operations unique to Azure. Platforms such as Splunk Cloud or IBM QRadar may provide greater flexibility. QRadar and Splunk Cloud are engineered to be more cloud-agnostic, offering enhanced support for enterprises with varied cloud infrastructures. QRadar provides extensive hybrid cloud compatibility, rendering it appropriate for organizations operating in both on-premises and cloud settings [33].

Splunk Cloud excels in multi-cloud scenarios owing to its highly customizable data ingestion functionalities. It can interact with several cloud providers, including AWS, Google Cloud, and Azure, and offer customizable dashboards for monitoring multi-cloud systems. The Splunk Phantom solution augments this capability by providing SOAR functions across many cloud platforms, facilitating real-time threat hunting and response in multi-cloud environments [34].

Conversely, AWS offers its proprietary security ecosystem, featuring services such as AWS GuardDuty, AWS Security Hub, and AWS CloudTrail. Although these services provide numerous features like Azure Sentinel, they are primarily intended for operation within the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

AWS ecosystem. AWS GuardDuty offers continuous threat detection by analyzing network traffic, account activity, and log data; however, its seamless interaction with other AWS services limits its flexibility in hybrid or multi-cloud setups [35].

Although Microsoft Sentinel performs exceptionally well in Azure-native environments owing to its extensive integration with Azure's service suite, there may be a better selection for enterprises operating in multi-cloud or hybrid infrastructures. In such instances, platforms such as IBM QRadar, Splunk Cloud, or Google Chronicle provide enhanced flexibility and compatibility with various cloud ecosystems. Every platform possesses distinct advantages, and the selection of an SIEM should be contingent upon the needs of the organization's cybersecurity framework.

4.4. Privacy Considerations

SIEM products like Microsoft Sentinel, QRadar, and Splunk Cloud provide comprehensive security monitoring functionalities; nevertheless, they can elicit privacy issues, particularly in cloud deployments. Cloud SIEMs are required to manage substantial quantities of sensitive information, rendering them susceptible to threats like illegal access and data breaches. Serckumecka et al. have shown that serverless SIEM methods can save expenses while heightening privacy threats due to restricted control over event storage periods [36]. Gunder emphasizes that QRadar's regulatory compliance capabilities require rigorous privacy measures [37]. Moreover, cloud-based SIEMs may unintentionally disclose data to other parties, as shown in Tuyishime et al.'s study on proactive threat detection with SIEM, underscoring the necessity for ongoing compliance monitoring in cloud settings [38]. Splunk Cloud's integration for DDoS detection exposes the same dangers, as data aggregation may introduce weaknesses, especially with IoT devices [39]. Pearson examined the mitigation of cloud privacy concerns by the integration of privacy into the design of SIEM tools [40].

SIEM tools guarantee transparency and accountability mandated by the GDPR and the NIS Directive. Singh et al. observed that cloud SIEMs must integrate privacy-preserving methodologies to comply with GDPR on data protection [41]. Furthermore, the NIS Directive underscores the necessity of real-time threat detection, rendering SIEMs essential for national infrastructure security [42].

4.5. Ethical Considerations in the Use of AI-Driven SIEM Systems

The integration of artificial intelligence (AI) and machine learning (ML) in Security Information and Event Management (SIEM) systems is associated with significant benefits to cybersecurity operations; however, critical ethical concerns are also introduced. The use of AI in SIEM systems such as Microsoft Azure Sentinel, IBM QRadar, Splunk Cloud, and Google Chronicle is associated with concerns related to privacy, transparency, and fairness, particularly given that sensitive data is handled, and semi-autonomous decisions are made by these systems.

The primary ethical concern identified is data privacy. Vast amounts of log data are aggregated and analyzed by SIEM systems, which often include personal and potentially sensitive information, such as user behavior patterns, location data, and access details. The essential nature of this data for threat detection is acknowledged; however, it is noted that a risk exists regarding the potential infringement on user privacy if the analysis is not managed properly. In regulated industries, such as finance and healthcare, the imposition of strict controls on data handling and storage by data privacy laws, including the GDPR and HIPAA, is considered especially critical. It is essential that robust data anonymization, encryption, and access control measures be implemented to mitigate the risks of privacy breaches.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

The potential for bias within AI-driven threat detection algorithms is identified as another ethical issue. If not carefully managed, biases can be introduced or perpetuated by the ML models utilized in SIEM systems, particularly when training occurs on imbalanced datasets that overrepresent certain behaviors or user groups. Disproportionate targeting or increased false positive rates for specific groups could be led to by such biases, raising concerns about fairness and discrimination. It is necessary for regular audits of AI models and careful selection of training data to be conducted to ensure that these algorithms operate equitably across diverse user populations.

Lastly, challenges related to accountability and transparency can be created by the opacity of AI models in SIEM systems. It has been observed that many AI-based SIEM tools function as "black boxes," which results in challenges for users in comprehending the processes through which specific decisions or alerts are generated. The ability of security teams to audit and explain system actions is complicated by this lack of transparency, which is particularly problematic in regulatory contexts where accountability is deemed critical. To address this, it is suggested that explainable AI techniques be implemented by developers of AI-driven SIEM systems, with the aim of providing interpretable insights into the decision-making process of these systems to facilitate trust and compliance.

5. Experimental Setup and Study Methodology

Because of the time constraint on one of the Azure subscriptions and the limited duration of the free trial licenses, it was required to operate in two separate Microsoft Azure tenants. The initial tenant, Microsoft's pre-configured evaluation environment, will be utilized for one of three automated threat response scenarios. In comparison, the second tenant will be utilized for the remaining two scenarios. The environmental topology used is shown in Figure 2:

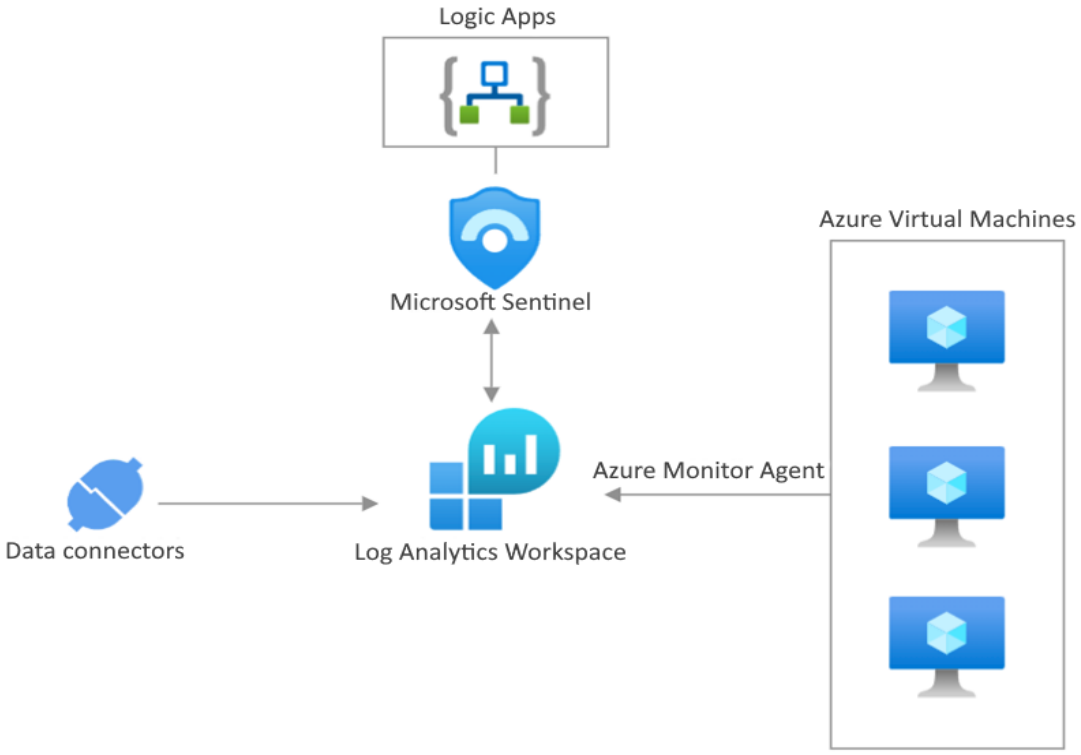

Figure 2.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

Azure environment topology used for evaluation.

The central repository of crucial data is the Log Analytics Workspace, which is now being established for Microsoft Sentinel. The Log Analytics Workspace can gather data from a wide range of sources. Data connectors or virtual machine agents play a crucial role in this process. To complete this task, utilizing the Microsoft Defender for Cloud connectors, which safeguards Azure subscriptions and the associated resources, was imperative.

Due to the absence of antivirus capabilities in Microsoft Defender for Cloud, it was imperative to utilize Microsoft Defender for Endpoint, which is situated as a constituent within the Microsoft 365 Defender Data connection. Microsoft Defender for Endpoint surveils internal device/server activities on Azure rather than examining external access methods like Microsoft Defender for Cloud. Subsequently, it was imperative to incorporate the Azure Activity Data Connector to provide comprehensive monitoring of all events in Azure, including events from Azure Resource Manager and information about the status of operations carried out. Additionally, an Azure Active Directory connector is necessary to facilitate monitoring user accounts within Azure Active Directory using Audit and Sign-in logs. As detailed in the third chapter, the TAXII connector has been implemented to retrieve external threat intelligence data. Microsoft Sentinel utilizes the Logic Apps connector, a critical component that facilitates data manipulation and events in many applications, to ensure comprehensive monitoring.

The Logic App must be granted the necessary permissions to execute specific actions within its resource group, such as automatically responding to threats. Also, Microsoft Sentinel must be permitted to execute playbooks within the exact location of the Logic App. The individual operating a specific Logic App must also possess the requisite permissions. The paper uses three virtual machines; however, only one was necessary to evaluate the last two scenarios of autonomous threat response. It was essential to set up onboarding to enable the Microsoft Defender for Endpoint service on the VMs. Additionally, security data was collected via the Azure Monitor agent and then forwarded to the Log Analytics Workspace.

In terms of data connectors used for this paper, here's the breakdown:

- Microsoft Defender for Cloud: Protects Azure subscriptions and resources; lacks antivirus capabilities.
- Microsoft Defender for Endpoint: This component monitors activities within Azure devices/servers and is part of the Microsoft 365 Defender data connector.
- Azure Activity Data Connector: Monitors subscription-level events like those from Azure Resource Manager and activity status.
- Azure Active Directory Connector: Provides Audit and Sign-in logs for monitoring user accounts.
- TAXII Connector: Accesses external threat intelligence data.
- Logic Apps Connector: This allows interaction with data and events in other applications. It requires proper permissions for execution.
- In terms of virtual machines, the following setup was used:
- Three virtual machines were used; one was sufficient to evaluate the last two automated threat response scenarios.
- Configured onboarding for Microsoft Defender for Endpoint service.
- Security data collection via Azure Monitor Agent, forwarded to Log Analytics Workspace.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

- To be able to do the sort of cyber threat evaluations in this paper, the following additional licenses and subscriptions are needed:
- Appropriate subscriptions and licenses are required for configuring automated threat response scenarios in Microsoft Sentinel.
- Two subscriptions assigned: Azure Pass – Sponsorship: Contoso (M365x42123187) - time-limited lab environment, and MVP Visual Studio Enterprise: TKLABS - renewable every month with limited rights.

The free trial duration varies by product, so time planning is essential when conducting these evaluations. Now that the evaluation setup has been described, the cyber threat scenarios used in this paper will be discussed.

6. Cyber Threat Scenarios

This section will define the cyber threat scenarios and analytical rules that meet them. Then, an evaluation of how these analytical rules work before defining automatic response rules to threats and the Logic App will be done.

6.1. Defining Cyber Threat Scenarios

In this article, three automated cyber threat response scenarios are presented. The first scenario helps SOC teams view and group warnings by location. If you try to log in to disabled accounts, alerts and incidents will be issued, and the location from which you attempted to connect will be identified as a reaction to the threat. The second scenario deactivates accounts if they log in from Microsoft Sentinel's blocklist of IP addresses. Famous Tor output nodes were used for IP addresses. Tor's IP address anonymization makes tracking users harder. Exit nodes are the last nodes before the user reaches the destination. Hence, they can be blocked. After the analytics rule detects the user login from the IP address on the watchlist, the account will be blocked and must be manually activated.

This reaction compromises the account, preventing the attack from escalating and causing more damage. Last, a single Azure-created and configured VM will be used. The preceding chapter showed the configuration. Eicar, a test malware, will be downloaded on this virtual system. The European Institute for PC Antivirus Research created Eicar to evaluate antivirus software without damaging the PC or network. The antivirus component should block downloading a file, but the user can specify an exemption for downloading a harmful file, which puts the entire network at risk. Therefore, it is essential to act quickly and separate the computer from the network after downloading a malicious file to analyze it. Analytical rules are created and analyzed for defined instances.

6.2. Creating and Analyzing Analytical Rules

For the first scenario, the analytical rule will use the KQL query in the Microsoft Sentinel Training Lab on GitHub [43].

After creating a scheduled analytics rule, where the mapped entity is an IP address and contains the previous query, the incident is shown in Figure 3:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

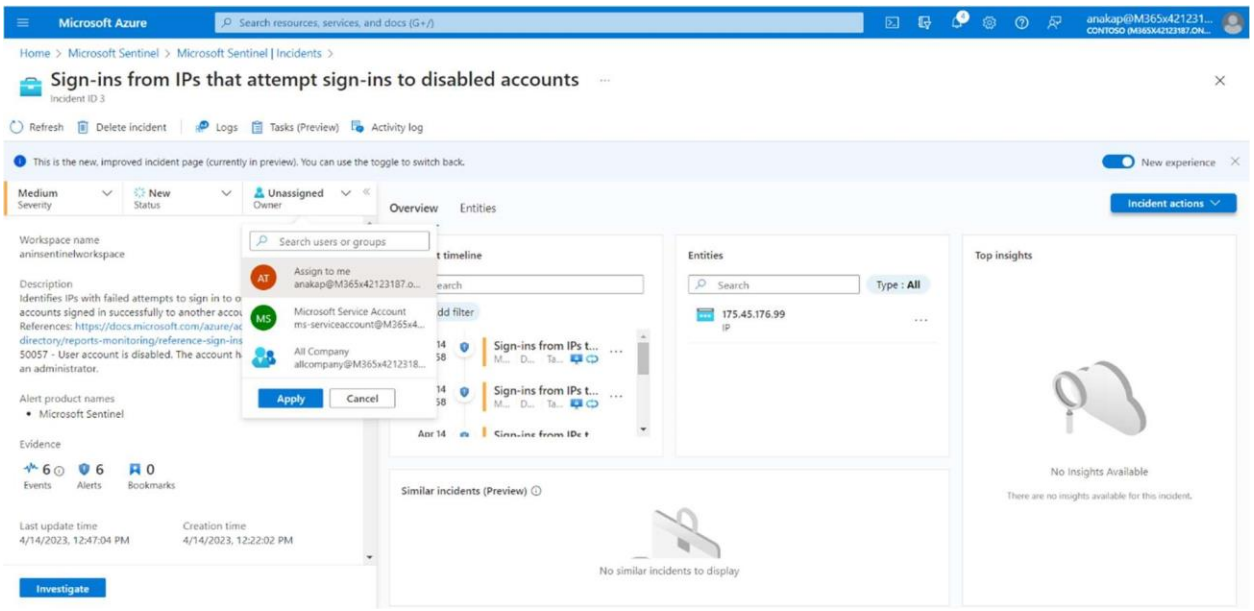

Figure 3.
Scenario 1 – Incident where a login attempt was made for a disabled user account.

The identified IP address (175.45.176.99), the location details of which will be known during the automatic threat response. Let's now extend that scenario by creating a watchlist by using a .csv file containing a list of all currently known Tor exit nodes, as is shown in Figure 4:

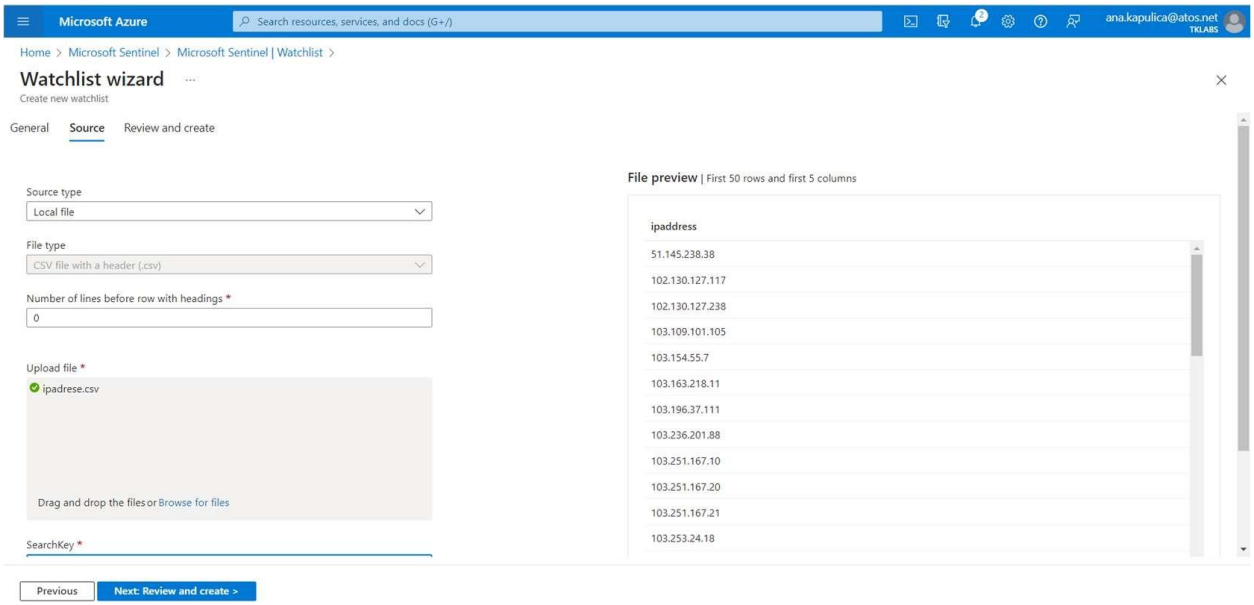

Figure 4.
Scenario 2 – Watchlist for Tor output nodes.

After this step, we'll create a KQL query which is going to use addresses from the watchlist and collate them with those from which the login attempt was made:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

```
Address Flight = (_GetWatchlist('IP address) | project address);
SigninLogs
| where IPAddress in (addresses);
```

Code 2: KQL query that correlates IP addresses from the watchlist with addresses from which login was attempted.

The query begins by defining a variable under the address name using the flight keyword. A variable is assigned as the result of a call to the function _GetWatchlist('IP address), which retrieves a watchlist containing IP addresses. „| The project address part only processes the IP address column from the watchlist (the only column in the .csv file). The "SigninLogs" table is prompted "| where IPAddress in (addresses)." This filter limits the results to include only records in which the "IPAddress" field matches one of the IP addresses in the "address" variable in the watchlist.

An evaluation account has been created, and login attempts will be made. Namely, in the TKLABS tenant, the "Security defaults" parameter is set to "Yes," which turns off login if Microsoft is not able to collect more information about the location or device from which the login was made, which happens if someone tries to log in from the Tor exit nodes. Otherwise, if this option were turned off, it would be possible to log in successfully, but because it is a tenant owned by another person, this option is not excluded. This did not prevent the automatic response to threats from being evaluated, and incidents were generated anyway because it records successful logins from specific IP addresses and all attempts. After a scheduled analytical rule is created and entities are mapped correctly, the whole incident can be seen in Sentinel UI, as shown in Figure 5:

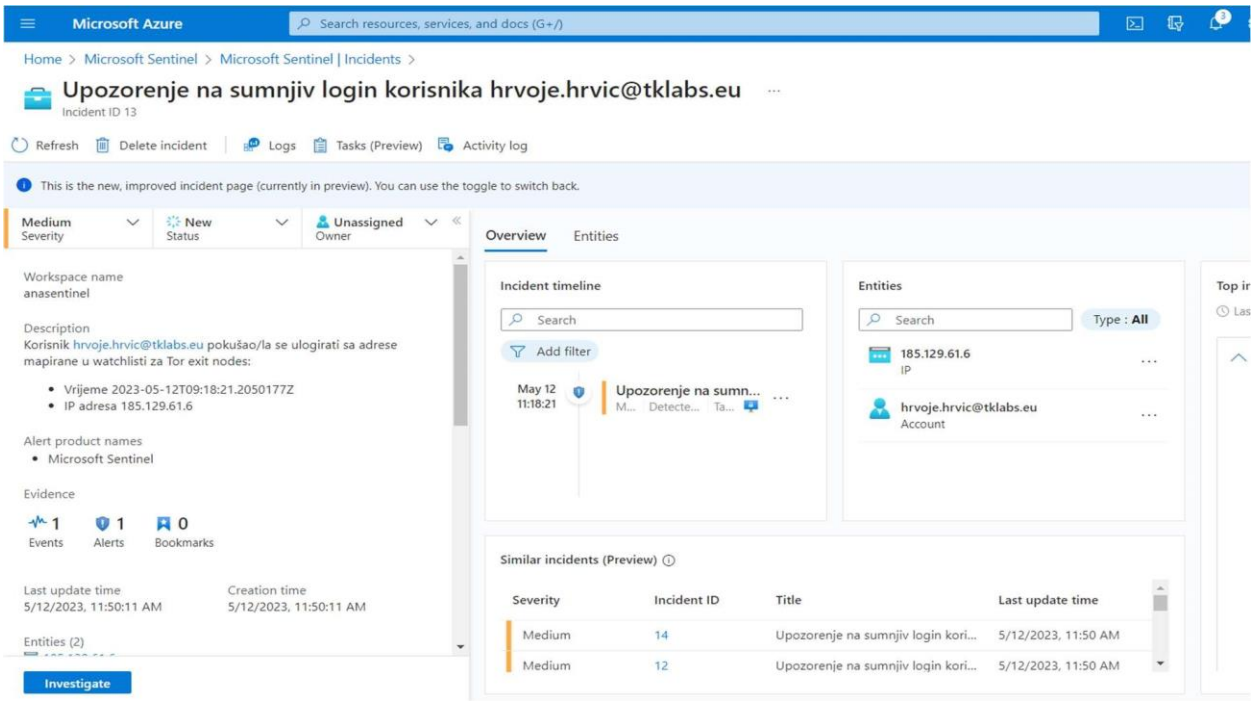

Figure 5.
Suspicious login to a user account incident

For the third scenario, Microsoft's predefined analytics policy for Microsoft Defender for Endpoint incidents was used, as shown in Figure 6:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

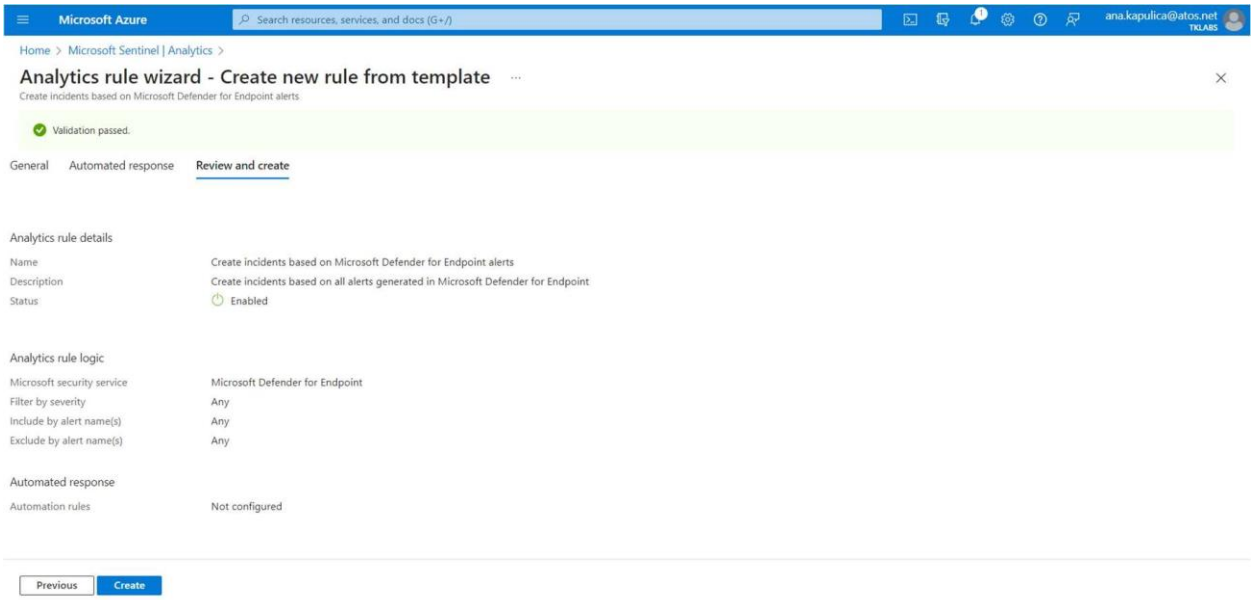

Figure 6.
An analytics rule that uses Microsoft Defender for the built-in endpoints rule.

When formulating rules for automated threat response, the scope of incidents triggering the threat response will be restricted. This analytics rule will display all events associated with Microsoft Defender for Endpoint in Microsoft Sentinel. However, we do not want automatic threat response to occur for incidents irrelevant to the specified scenario. During the evaluation, an effort was made to download the eicar file onto a virtual system. As mentioned earlier in the paper, despite the antivirus software's ability to prevent the download, it is still feasible to download it successfully by making an exception. Therefore, it is crucial to respond promptly to this threat. After downloading the file, an incident will occur. Incidents can either have "Malware" in the name or the name of the file that was downloaded, as shown in Figure 7:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

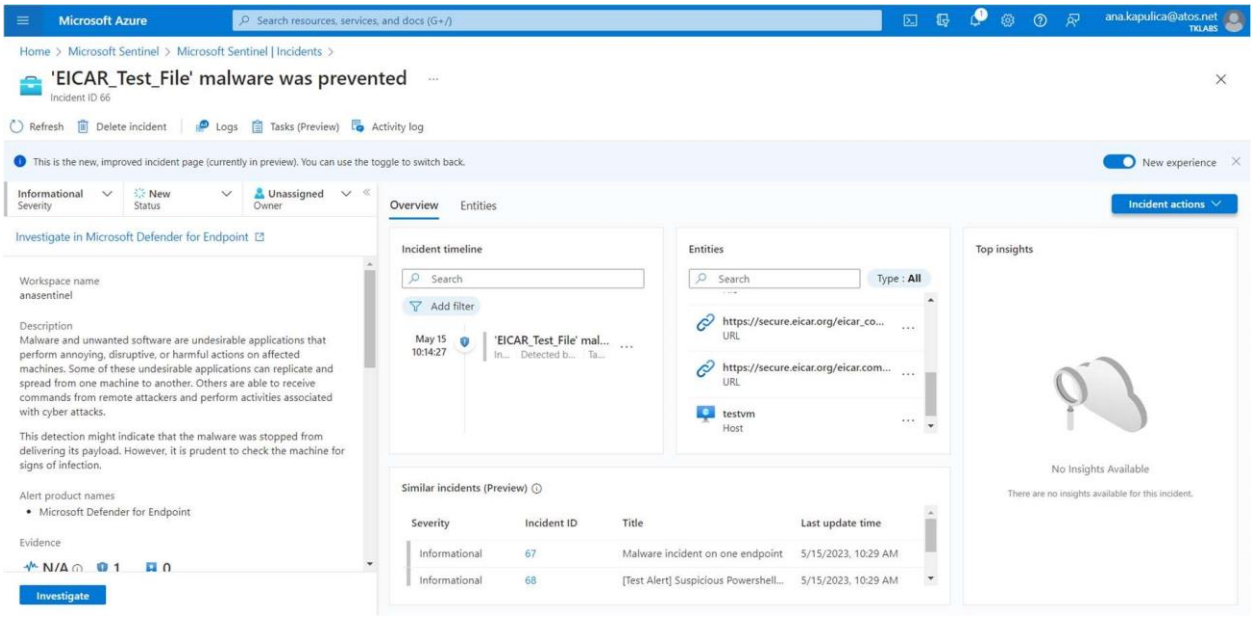

Figure 7.
Malware incident from scenario 3.

The mapped entities include the computer that may be infected, the downloaded file, the hash files, and the URLs from which the file was obtained. Depending on whether the incident occurred during the download or when the file was detected on the system, the URL may or may not be shown as an entity.

Let's now demonstrate how to establish an automated countermeasure for each scenario.

6.3. Logic App as an Automatic Threat Response

In the first scenario, an automated rule was established. This rule is triggered when the analytics rule is "Sign-ins from IPs that attempt sign-ins to disabled accounts," an alert is generated. Once the alert is triggered, it initiates an action that activates the script. This playbook includes a pre-existing Logic App. Therefore, the Logic App will be configured to make the management job more manageable. The result for this Logic App is shown in Figure 8.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

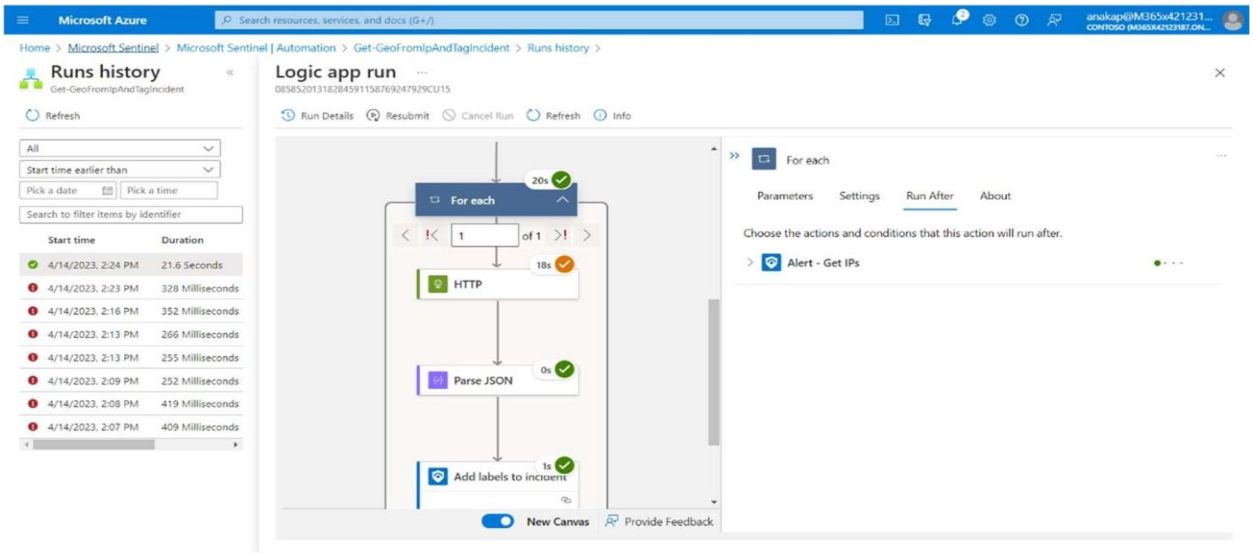

Figure 8.
The first part of the Logic App for scenario 1.

This Logic App starts automatically upon the occurrence of an alert. It begins by receiving an incident that is linked to the triggering alert. Subsequently, it comprehensively compiles all IP addresses related to the alert. The second part of our Logic App is shown in Figure 9:

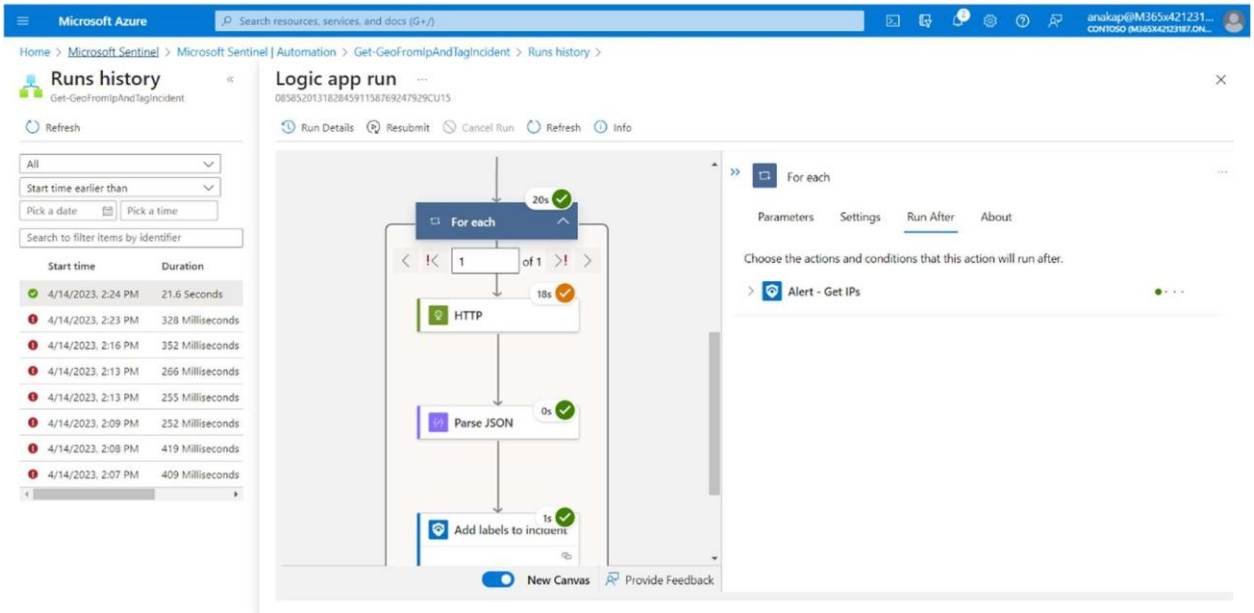

Figure 9.
The second part of our Logic App for Scenario 1.

The Logic App initiates a loop for each address upon receiving the IP addresses. It then sends an HTTP request to the ip-api.com page, extracting the IP address linked to the warning in the request. Subsequently, it retrieves a JSON record from the page, which includes precise details regarding the geographical coordinates of the IP address. This feature signifies the

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

incident's conclusion by providing a detailed record of the place. SOC staff can screen alerts and categorize them into groups selectively using this feature.

For the second scenario, it is necessary to define a Logic App according to the analytical rule it will use to respond to threats automatically. Subsequently, when an incident transpires according to this analytical rule, the prescribed activities are executed to initiate the playbook (Logic App). Ultimately, the incident's status will be updated from active to closed, and a comment will be added to the incident if the user is successfully disabled. The term "True Positive" refers to accurately identifying a threat, as opposed to an evaluation or rule that incorrectly finds "False Positive" occurrences. Logic App for this scenario is shown in Figure 10:

Figure 10.
Logic app for scenario 2.

This Logic App begins similarly to the Logic App in the initial scenario. When generating an incident linked to a preexisting analytics rule, a comprehensive list of all user accounts related to that incident is provided. Subsequently, the program enters a loop wherein it iterates through each user account in the list and turns it off. For the execution of this Logic App to occur, it is essential to map the entities accurately. Therefore, the complete name is associated with "UserPrincipalName" rather than "UserID," for instance.

The third scenario features an automation rule that operates similarly to the automation rule in the second scenario, albeit with some distinctions, as shown in Figure 11.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

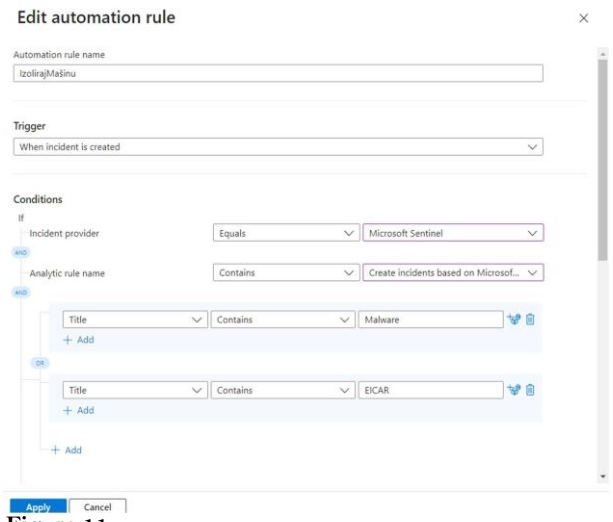

Figure 11.
Automation rule for Scenario 3.

The distinction lies in the requirement to choose "Microsoft Sentinel" as the incident supplier under the execution conditions and utilize the default analytics rule provided by Microsoft Defender for the Endpoint connector for Microsoft Sentinel. Additionally, it is crucial to monitor the title of the event produced. Specifically, if the title includes "Malware" or "EICAR," it indicates that the Eicar file will be downloaded.

Once the conditions have been defined, the next step is to initiate a script to isolate the virtual machine and update the incident status to close. In addition, he will append a remark to the occurrence, stating that it was imperative to segregate the virtual machine because of a nasty file. It was important to register an application capable of managing virtual machines, meaning that it possesses the authority to isolate the machine and establish a connection with the Logic App, which is shown in Figure 12:

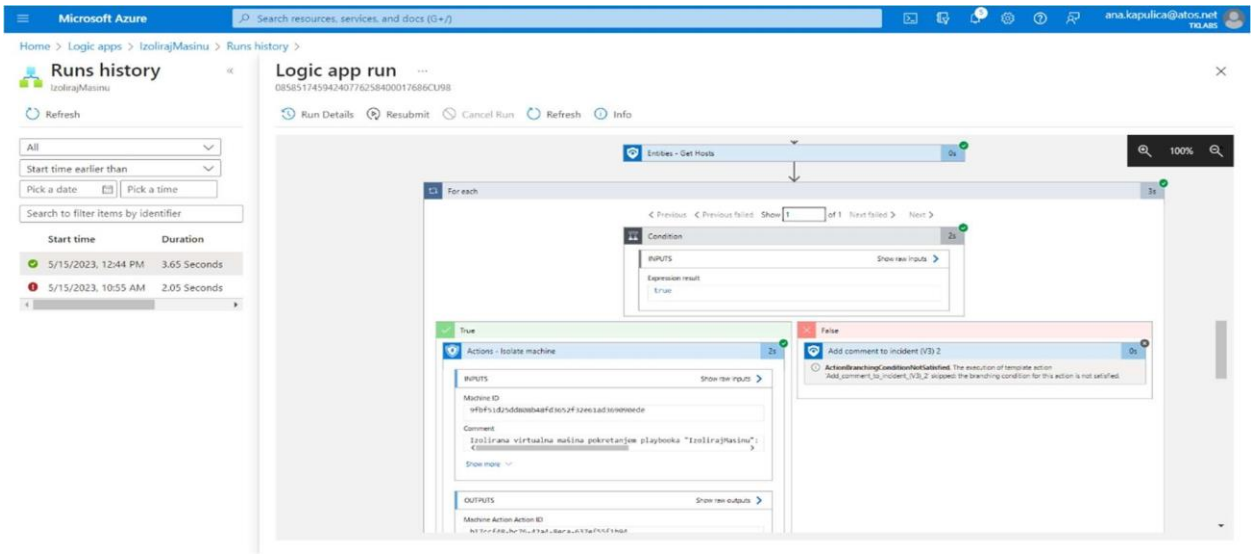

Figure 12.
Logic app for scenario 3.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

Once the application is registered and connected to the Logic App, the option to isolate the machine is available in the "True" statement, but only if the criterion "MDATPDeviceID" is not equal to zero. "MDATPDeviceID" is the specific identifier for a device in Microsoft Defender for Endpoint. Microsoft Defender for Endpoint allocates a unique identifier to every device. It is imperative to allocate the accurate "MDATPDeviceID" to isolate the relevant PC. If the requirement is not satisfied, a remark will be written regarding the incident, stating that it was not feasible to isolate the virtual machine.

The following section presents the outcomes of the automated reaction to dangers and evaluates the ultimate execution of the security resolution.

7. Future Work

This section will enable the automatic threat response configured in the previous chapter. The first step is to analyze the autoresponder results. The initial scenario is designed to provide an instructive reaction to the threat. The objective is to assign geographical locations to occurrences based on the IP address that generated the alert in Microsoft Sentinel. An analysis of the response to the threat in the initial scenario is shown in Figure 13:

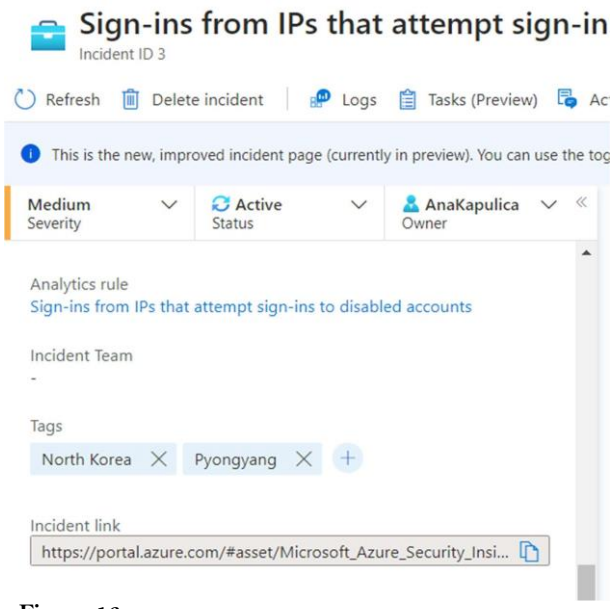

Figure 13.
Scenario 1 - Automatic threat response.

The outcome is an incident labeled with a location corresponding to the IP address. The IP address 175.45.176.99 is associated with the geographical location of Pyongyang, North Korea. By analyzing this IP address, an investigation can be done to determine the accounts it is linked to and consequently identify all compromised artifacts, specifically user accounts. An example is shown in Figure 14:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

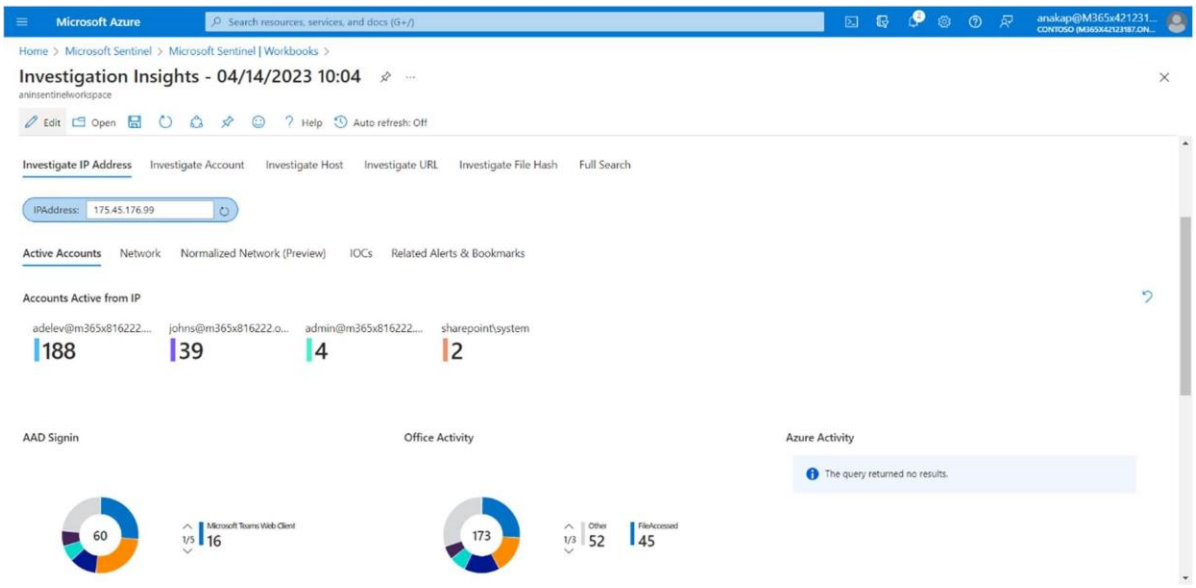

Figure 14.
Investigation Insights for Scenario 1.

Based on the evidence, it can be inferred that the assailant, hailing from North Korea, successfully infiltrated numerous user accounts, including one with administrative powers. Furthermore, the specific resources that were accessed can be observed. This level of visibility facilitates analysts in effectively seeing the extent of the harm incurred thus far and predicting the potential next move of the adversary. Knowing the attacker's location is crucial as it allows us to analyze and compare their tactics and techniques with those commonly observed in that area. Additionally, it helps us understand the potential motives behind the attack.

In the second case, the user's account must be deactivated automatically if they attempt to log in from IP addresses that are on the "blacklist" or watchlist due to security concerns. A test user account, hrvoje.hrvic@tklabs.eu, was utilized in this situation. Figure 15 shows the outcomes of the automated threat response:

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

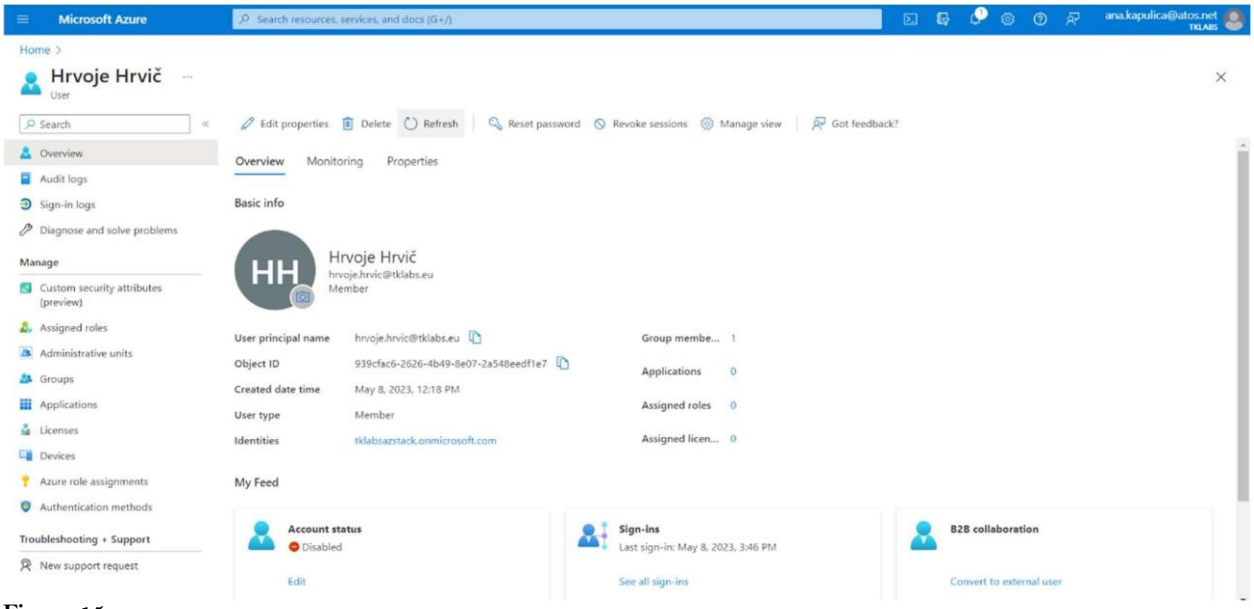

Figure 15.
Automated threat response for Scenario 2.

The user's account has been successfully deactivated. Also, when an incident is opened, it is visible that specific actions have been taken on that user account. In this case, the action is to deactivate the account, as shown in Figure 16:

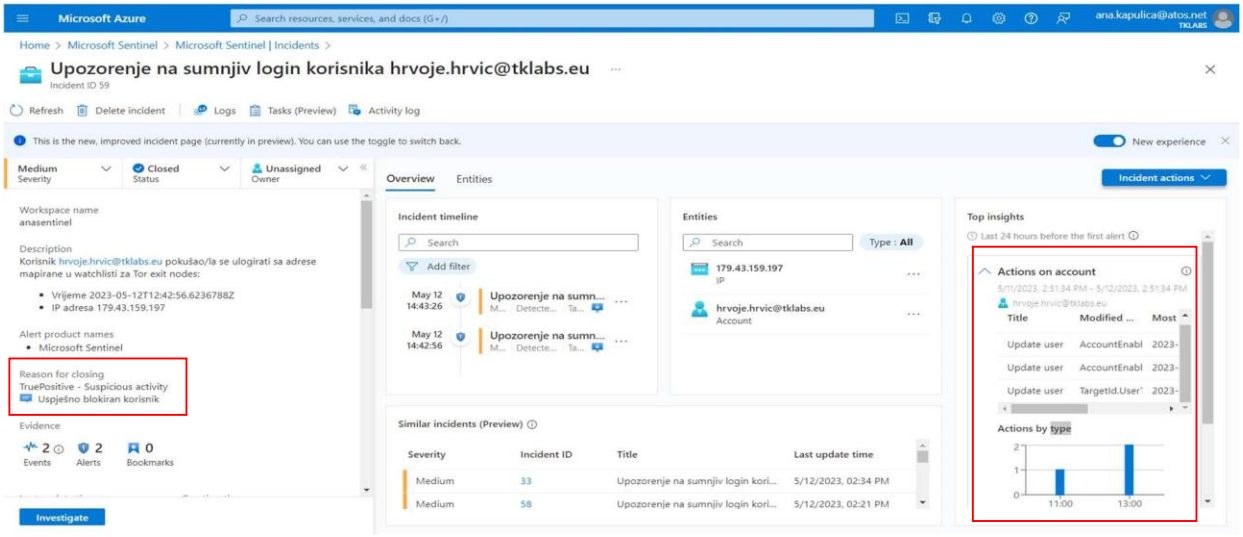

Figure 16.
Actions taken on the user account.

In the third and final scenario, the virtual machine must be disconnected from the network as a precaution in reaction to the threat. Suppose a potentially harmful file has been downloaded, regardless of whether Microsoft Defender previously blocked it. In that case, it is necessary to isolate the virtual machine to assess whether any additional harm has been

inflicted on the computer. Once the test Eicar file is downloaded, the machine is placed in isolation, as shown in Figure 17:

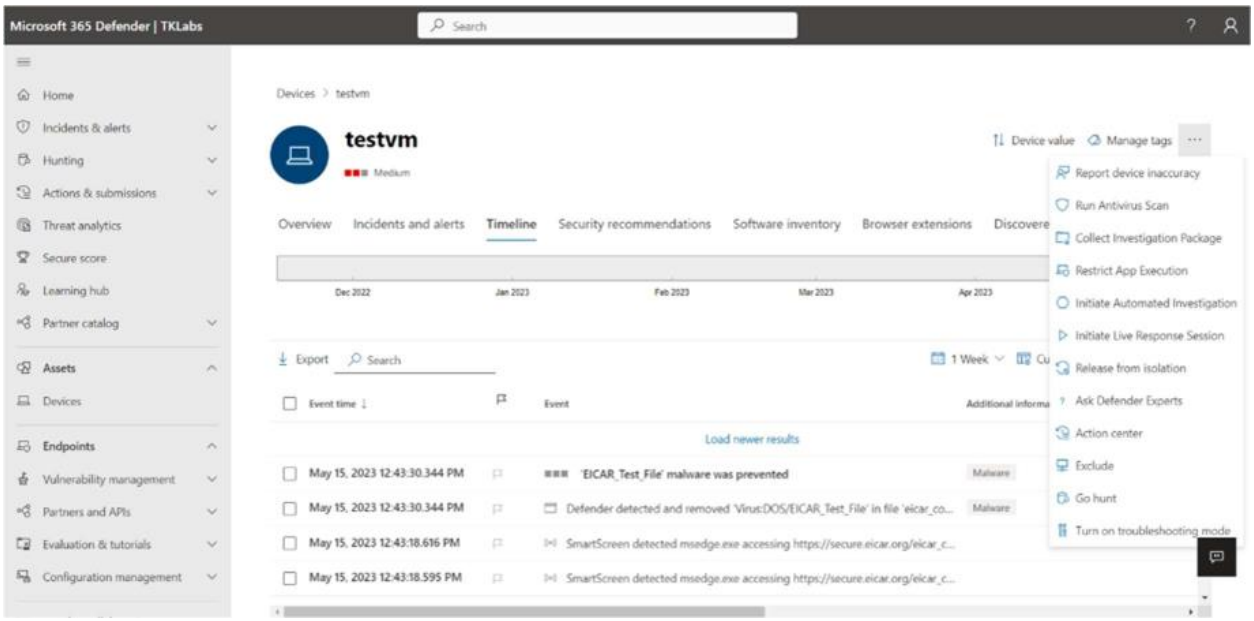

Figure 17.
Automatic Virtual Machine isolation for Scenario 3.

These three scenarios are just some of the simpler ones we used to research the usability of the options mentioned in this paper. Hundreds of scenarios for a larger, enterprise-size company might need automated responses involving various additional systems, files, or services. Protecting large-scale environments will make these tools even more helpful, as they're powerful and customizable to any scenario involving Azure and its objects.

8. Threat Response Analysis

To deploy Microsoft Sentinel and Logic Apps as a security solution, careful planning and thorough examination of the Microsoft documentation are necessary. Consequently, it is feasible to achieve a successful execution of the intended plan. Naturally, challenges were encountered during the implementation phase, and resolving these challenges necessitated further investigation. The results of all three implemented scenarios were successful. The implemented security solution would alleviate the burden on analysts who would otherwise need to investigate the location of IP addresses manually, manually deactivate user accounts, and correlate them with the list of prohibited IP addresses. Additionally, analysts would no longer need to manually isolate machines when a suspected "infected" virtual machine is detected. Therefore, we can deduce the following findings through analysis:

- Implementing this security solution enhances reaction efficiency and speed, resulting in a quicker and more efficient response to threats. Utilizing Logic Apps allows for automated activities, facilitating swift reaction to occurrences and substantially decreasing issue resolution time.
- Reducing Human Error—Manual investigation and danger response are susceptible to human fallibility. This security solution minimizes the danger of errors because normal

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

operations are automatically performed using logical flows, removing the need for manual interventions.

- Automation enhances analyst efficiency by enabling them to dedicate their time to more intricate work rather than repeated and mundane ones. As a result, there is a boost in productivity and team efficiency since resources are available for in-depth study and analysis of more sophisticated threats.

Using these automatic security response methodologies dramatically reduces analysts' time to respond to threats, decreasing the number of vulnerable areas that attacks can target. This increases efficiency and allows us to focus on delivering applications that businesses need to operate instead of wasting time manually fixing security issues.

9. Future Work

Future investigations on automating cyber threat responses utilizing Microsoft Sentinel and Logic Apps may pursue various intriguing avenues. One aspect to explore is adapting this automated response system to alternative cloud-based SIEM platforms, such as Google Chronicle and IBM QRadar. Research might evaluate the integration of Logic Apps inside these ecosystems and analyze the efficacy of such integrations, especially in environments dependent on diverse SIEM solutions.

Another area of interest is the ability to augment the system by integrating more sophisticated machine learning models. These models may be developed to enhance the precision of threat detection, especially for intricate and developing threats like zero-day vulnerabilities and advanced persistent threats. This would also diminish the prevalence of false positives, a critical concern in contemporary cybersecurity systems.

The efficacy of Microsoft Sentinel and Logic Apps in hybrid or multi-cloud settings represents a promising domain for investigation. As enterprises increasingly utilize platforms such as Microsoft Azure, AWS, and Google Cloud, it is essential to evaluate the efficacy of these tools in detecting and responding to threats across varied cloud infrastructures. This research may also formulate solutions for efficient threat detection and automated responses inside multi-cloud settings.

Subsequent studies could explore the potential for Microsoft Sentinel to enhance its integration with external threat intelligence platforms, thereby establishing a real-time, collaborative threat detection network. This strategy would improve the detection and alleviation of global dangers by utilizing collective intelligence and automated reactions.

Ethical and privacy concerns in automated cybersecurity responses represent a significant area for research. As AI and machine learning increasingly contribute to threat detection and mitigation, assessing their compliance with global data protection requirements such as GDPR is essential to uphold privacy while addressing cyber dangers.

Furthermore, the present emphasis on external threats might be broadened to investigate the optimization of Microsoft Sentinel and Logic Apps for detecting and responding to insider threats. This entails creating customized data analysis and reaction strategies to mitigate organizational risks, which typically necessitate a distinct approach compared to external cyberattacks.

Research may also focus on enhancing Logic App playbooks to manage more intricate situations within extensive organizational settings. This entails developing increasingly sophisticated automated solutions that may be tailored to address the specific security requirements of companies, especially those confronting complex, large-scale cyberattacks. Future research could enhance the conclusions of this study by investigating these areas, thereby contributing to more effective automated cybersecurity solutions.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

10. Conclusions

The integration of Microsoft Sentinel and Logic Apps is presented as a highly effective solution for automated cyber threat detection and response, with advanced AI and machine learning being leveraged to enhance security capabilities within the Azure ecosystem. The automation of threat identification and incident response results in a significant strengthening of an organization's security posture. This is achieved through real-time analytics, anomaly detection, and streamlined workflows that reduce the necessity for manual intervention. The advantages of these features in addressing sophisticated cyber threats, including malware, phishing, and unauthorized access attempts, are highlighted by their seamless integration with core Azure services such as Azure Active Directory and Microsoft Defender.

Three key contributions are underscored by the results from this study. (1) The novel integration of Sentinel's SIEM functionality with Logic Apps is presented as providing a streamlined and automated response system that enhances incident management capabilities; (2) The evaluation of various cyber threat scenarios is demonstrated to reveal the system's practical ability to automate response actions—such as account blocking and virtual machine isolation—thereby allowing for efficient threat containment; and (3) The comparative analysis with other prominent SIEM platforms, including Splunk and IBM QRadar, is highlighted to showcase Sentinel's specific advantages in Azure-centric environments while also identifying limitations in cross-platform adaptability.

Despite these benefits, challenges are present, particularly regarding the steep learning curve of the platform and its dependency on the Azure ecosystem. The complexity associated with the configuration of custom workflows, the utilization of Kusto Query Language, and the design of effective playbooks is recognized as requiring a considerable level of expertise. This may be perceived as an obstacle for smaller teams or organizations that possess limited cybersecurity resources. Furthermore, it has been observed that while Sentinel excels within Azure-based environments, its limited compatibility with multi-cloud or hybrid cloud setups may hinder its utility in more diverse infrastructures. In these scenarios, enhanced flexibility and adaptability may be offered by alternative SIEM platforms, such as Splunk or IBM QRadar.

It is suggested that valuable advancements in proactive cybersecurity solutions are represented by Microsoft Sentinel and Logic Apps, particularly for organizations that are heavily invested in the Azure environment. Future research may be directed towards the extension of these capabilities to additional cloud providers, the optimization of the system for multi-cloud applications, and the development of enhanced machine learning models aimed at further reducing false positives and improving detection accuracy. The ongoing evolution of automated cybersecurity defenses is expected to be contributed to by this line of research, with resilience against emerging threats in increasingly complex digital landscapes being enhanced.

References

[1] Wankhede, P.; Talati, M.; Chinchamalatpure, R. COMPARATIVE STUDY OF CLOUD PLATFORMS - MICROSOFT AZURE, GOOGLE CLOUD PLATFORM AND AMAZON EC2. jreas 2020, 05, 60–64. https://doi.org/10.46565/jreas.2020.v05i02.004.

[2] Rajendran, P.; Maloo, S.; Mitra, R.; Chanchal, A.; Aburukba, R. Comparison of Cloud-Computing Providers for Deployment of Object-Detection Deep Learning Models. Applied Sciences 2023, 13, 12577. https://doi.org/10.3390/app132312577.

Edelweiss Applied Science and Technology
ISSN: 2576-8484
Vol. 8, No. 6: 4319-4348, 2024
DOI: 10.55214/25768484.v8i6.2933

[3] Muhammed, A.S.; Ucuz, D. Comparison of the IoT Platform Vendors, Microsoft Azure, Amazon Web Services, and Google Cloud, from Users' Perspectives. 2020 8th International Symposium on Digital Forensics and Security (ISDFS) 2020. https://doi.org/10.1109/ISDFS49300.2020.9116254.
[4] Copeland, M.; Jacobs, M. Azure Network Security Configuration. Cyber Security on Azure 2020, 37–81. https://doi.org/10.1007/978-1-4842-6531-4_2.
[5] Kelley, R.; Antu, A.D.; Kumar, A.; Xie, B. Choosing the Right Compute Resources in the Cloud: An Analysis of the Compute Services Offered by Amazon, Microsoft and Google. 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC) 2020. https://doi.org/10.1109/CyberC49757.2020.00042.
[6] Chauhan, A. A Comparative Study of Cloud Computing Platforms. TURCOMAT 2020, 11, 821–826. https://doi.org/10.17762/turcomat.v11i1.13563.
[7] Kaushik, P.; Rao, A.M.; Singh, D.P.; Vashisht, S.; Gupta, S. Cloud Computing and Comparison Based on Service and Performance between Amazon AWS, Microsoft Azure, and Google Cloud. 2021 International Conference on Technological Advancements and Innovations (ICTAI) 2021. https://doi.org/10.1109/ICTAI53825.2021.9673425.
[8] K, S.; K, A.X.; Davis, D.; Jayapandian, N. Internet of Things and Cloud Computing Involvement Microsoft Azure Platform. 2022 International Conference on Edge Computing and Applications (ICECAA) 2022. https://doi.org/10.1109/ICECAA55415.2022.9936126.
[9] Soh, J.; Copeland, M.; Puca, A.; Harris, M. Microsoft Azure; Apress, 2020. http://doi.org/10.1007/978-1-4842-5958-0.
[10] Alamsyah, N; Febrianto, N.I. Analysis of The Utilization and Implementation of Cloud Computing Infrastrucutre Services on The Azure Microsoft Platform, Mantik, vol.5, no.1., pp 127.136,Apr 2021.
[11] Suryawan, R.B.; Ferdiana, R.; Widyawan The Comparison of Cloud Migration Effort on Platform as a Service. J. Phys.: Conf. Ser. 2020, 1577, 012056. https://doi.org/10.1088/1742-6596%2F1577%2F1%2F012056.
[12] Sharma, V.; Nigam, V.; Sharma, A.K. WITHDRAWN: Cognitive Analysis of Deploying Web Applications on Microsoft Windows Azure and Amazon Web Services in Global Scenario. Materials Today: Proceedings 2020. https://doi.org/10.1016/j.matpr.2020.10.126.
[13] Pierleoni, P.; Concetti, R.; Belli, A.; Palma, L. Amazon, Google and Microsoft Solutions for IoT: Architectures and a Performance Comparison. IEEE Access 2020, 8, 5455–5470. https://doi.org/10.1109/ACCESS.2019.2961511.
[14] Bansal, N. Microsoft Azure IoT Platform. Designing Internet of Things Solutions with Microsoft Azure 2020, 33–48. https://doi.org/10.1007/978-1-4842-6041-8_3.
[15] Tiutiunnyk, P.B.; Rybachok, N.A. Creating Web Application for Organizing Teamwork Online Using Microsoft Azure Cloud Services. Control syst. comput. 2021, 52–59. https://doi.org/10.15407/csc.2021.02.052.
[16] Chilberto, J.; Zaal, S.; Aroraa, G.; Price, E. Building Solutions in the Azure Cloud. Cloud Debugging and Profiling in Microsoft Azure 2020, 1–19. https://doi.org/10.1007/978-1-4842-5437-0_1.
[17] Tasnim, R.; Akter Mim, A.; Hasan Mim, S.; Jabiullah, Md.I. A Comparative Study on Three Selective Cloud Providers. IJCI 2022, 11, 167–178. https://doi.org/10.5121/ijci.2022.110413.
[18] Moutaouakal, W.E.; Baïna, K. Comparative Experimentation of MLOps Power on Microsoft Azure, Amazon Web Services, and Google Cloud Platform. 2023 IEEE 6th International Conference on Cloud Computing and Artificial Intelligence: Technologies and Applications (CloudTech) 2023, 1–8. https://doi.org/10.1109/CloudTech58737.2023.10366138.
[19] Zibitsker, B.; Lupersolsky, A. How to Apply Modeling to Compare Options and Select the Appropriate Cloud Platform. Companion of the ACM/SPEC International Conference on Performance Engineering 2020, 16–16. https://doi.org/10.1145/3375555.3384938.
[20] Tuyishime, E.; Balan, T.C.; Cotfas, P.A.; Cotfas, D.T.; Rekeraho, A. Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. Applied Sciences 2023, 13, 12359.
[21] 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.
[22] Feng, C.; Wu, S.; Liu, N. A User-Centric Machine Learning Framework for Cyber Security Operations Center. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI) 2017, 18 2, 173–175. https://doi.org/10.1109/ISI.2017.8004902.
[23] Module 3 - Analytics Rules. Available online: https://github.com/Azure/Azure-Sentinel/blob/master/Solutions/Training/Azure-Sentinel-Training-Lab/Modules/Module-3-Analytics-Rules.md (accessed on 01.10.2024.)
[24] Breiter, G.; Naik, V.K. A Framework for Controlling and Managing Hybrid Cloud Service Integration. 2013 IEEE International Conference on Cloud Engineering (IC2E) 2013, 217–224. https://doi.org/10.1109/IC2E.2013.48.
[25] De Tender, P.; Rendon, D.; Erskine, S. Azure Sentinel (Preview). Pro Azure Governance and Security 2019, 267–310. https://doi.org/10.1007/978-1-4842-4910-9_8.
[26] Ren, H.; Xu, B.; Wang, Y.; Yi, C.; Huang, C.; Kou, X.; Xing, T.; Yang, M.; Tong, J.; Zhang, Q. Time-Series Anomaly Detection Service at Microsoft. Proceedings of the 25th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining 2019. https://doi.org/10.1145/3292500.3330680.
[27] Watson, M.R.; Shirazi, N.; Marnerides, A.K.; Mauthe, A.; Hutchison, D. Malware Detection in Cloud Computing Infrastructures. IEEE Trans. Dependable and Secure Comput. 2016, 13, 192–205. https://doi.org/10.1109/TDSC.2015.2457918.

[28] Opara, E.; Wimmer, H.; Rebman, C.M. Auto-ML Cyber Security Data Analysis Using Google, Azure and IBM Cloud Platforms. 2022 International Conference on Electrical, Computer and Energy Technologies (ICECET) 2022, 38, 1–10. https://doi.org/10.1109/ICECET55527.2022.9872782.
[29] Xu, S.; Qian, Y.; Hu, R.Q. Data-Driven Network Intelligence for Anomaly Detection. IEEE Network 2019, 33, 88–95. https://doi.org/10.1109/MNET.2019.1800358.
[30] J, G.K.; S, G.; Rajendran, S.; Vimali, J.S.; Jabez, J.; Srininvasulu, S. Identification of Cyber Threats and Parsing of Data. 2021 5th International Conference on Trends in Electronics and Informatics (ICOEI) 2021, 4, 556–564. https://doi.org/10.1109/ICOEI51242.2021.9452925.
[31] De Tender, P.; Rendon, D.; Erskine, S. Azure Sentinel (Preview). Pro Azure Governance and Security 2019, 267–310. https://doi.org/10.1007/978-1-4842-4910-9_8.
[32] Copeland, M.; Jacobs, M. Azure Network Security Configuration. Cyber Security on Azure 2020, 37–81. https://doi.org/10.1007/978-1-4842-6531-4_2.
[33] Katzer, M. Managing Office 365. Securing Office 365 2018, 499–609. https://doi.org/10.1007/978-1-4842-4230-8_8.
[34] Pathak, P.; Rangasamy, K.; Selvaraj, T. Security Analytics and Benchmarking Log Aggregation in the Cloud. EAI Endorsed Transactions on Cloud Systems 2018, 3, 154464. https://doi.org/10.4108/eai.11-4-2018.154464.
[35] Bihari, V.; Kumar, A.; Sattar, A.M.; Mritunjay, K.R. Fortifying the Cloud: Unveiling the Next-Generation Security Model of AWS. IJIRMPS 2023, 11. https://doi.org/10.37082/ijirmps.v11.i3.230230.
[36] Hristov, M.; Nenova, M.; Iliev, G.; Avresky, D. Integration of Splunk Enterprise SIEM for DDoS Attack Detection in IoT. 2021 IEEE 20th International Symposium on Network Computing and Applications (NCA) 2021. https://doi.org/10.1109/nca53618.2021.9685977.
[37] Pearson, S. Taking Account of Privacy When Designing Cloud Computing Services. 2009 ICSE Workshop on Software Engineering Challenges of Cloud Computing 2009. https://doi.org/10.1109/CLOUD.2009.5071532.
[38] Singh, J.; Pasquier, T.; Bacon, J.; Ko, H.; Eyers, D. Twenty Security Considerations for Cloud-Supported Internet of Things. IEEE Internet Things J. 2016, 3, 269–284. https://doi.org/10.1109/JIOT.2015.2460333.
[39] 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.
[40] Serckumecka, A.; Medeiros, I.; Bessani, A. Low-Cost Serverless SIEM in the Cloud. 2019 38th Symposium on Reliable Distributed Systems (SRDS) 2019. https://doi.org/10.1109/SRDS47363.2019.00057.
[41] Gunder, A.M. Security Monitoring and Management Based on the Use of IBM QRadar SIEM System. MIS 2022, 2. https://doi.org/10.31673/2409-7292.2022.020614.
[42] Tuyishime, E.; Balan, T.C.; Cotfas, P.A.; Cotfas, D.T.; Rekeraho, A. Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach. Applied Sciences 2023, 13, 12359. https://doi.org/10.3390/app132212359.
[43] Sign-ins from IPs that attempt sign-ins to disabled accounts. Available online: https://github.com/Azure/Azure-Sentinel/blob/master/Detections/ASimAuthentication/imSigninAttemptsByIPviaDisabledAccounts.yaml (accessed on 01.10.2024.)