applied sciences

MDPI

Article

Enhancing Cloud Security—Proactive Threat Monitoring and Detection Using a SIEM-Based Approach

Emmanuel Tuyishime *, Titus C. Balan, Petru A. Cotfas, Daniel T. Cotfas and Alexandre Rekeraho

Electronics and Computers Department, Transilvania University of Brasov, 500036 Brasov, Romania
* Correspondence: emmanuel.tuyishime@unitbv.ro

Abstract: With the escalating frequency of cybersecurity threats in public cloud computing environments, there is a pressing need for robust security measures to safeguard sensitive data and applications. This research addresses growing security concerns in the cloud by proposing an innovative security information and event management system (SIEM) that offers automated visibility of cloud resources. Our implementation includes a virtual network comprising virtual machines, load balancers, Microsoft Defender for Cloud, and an application gateway that functions as a web application firewall (WAF). This WAF scans incoming Internet traffic and provides centralized protection against common exploits and vulnerabilities, securing web applications within the cloud environment. We deployed the SIEM system to automate visibility and incident response for cloud resources. By harnessing the power of this employed SIEM, the developed system can continuously monitor, detect security incidents, and proactively mitigate potential security threats. Microsoft Defender for Cloud consistently assesses the configuration of cloud resources against industry standards, regulations, and benchmarks to ensure compliance requirements are met. Our findings highlight the practicality and effectiveness of deploying such solutions to safeguard cloud resources, offering valuable insights to organizations and security professionals seeking sustainable and resilient security measures in the cloud computing environment.

Keywords: cloud security; SIEM system; security threats; Microsoft Sentinel; compliance

check for updates

Citation: 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. *Appl. Sci.* **2023**, *13*, 12359. https://doi.org/10.3390/app132212359

Academic Editor: Mohamed Amine Ferrag, Leandros Maglaras and Helge Janicke

Received: 13 October 2023
Revised: 7 November 2023
Accepted: 8 November 2023
Published: 15 November 2023

1. Introduction

The rapid adoption of public cloud services has prompted organizations to migrate their valuable data from on-premises servers to cloud data centers. Recent reports [1] indicate that a significant portion of global businesses, approximately 70%, currently conduct their daily activities in the cloud, with Microsoft Azure, Amazon Web Service (AWS), and Google Cloud Platform (GCP) emerging as the top three cloud service providers (CSPs) [2]. These providers offer a range of services based on the primary cloud services model, namely Infrastructure as a Service (IaaS), Software as a Service (SaaS), and Platform as a Service (PaaS). While cloud services offer various benefits, ensuring the security of cloud resources remains a critical concern due to the prevalence of cloud data breaches [3,4].

Over the past decade, security has consistently emerged as a prominent challenge in the cloud landscape, as highlighted in a series of cloud state reports published by Flexera [2]. Key security issues include data security, confidentiality, and integrity [5]. Industry experts have highlighted [6] cloud platform misconfiguration, sensitive data leakage, insecure interfaces/APIs, and unauthorized access as the primary cloud attack vectors. The latter raises a significant question of who bears the responsibility for configuring and safeguarding cloud resources? In traditional settings, organizations assume full responsibility for securing on-premises systems. However, in the realm of public cloud environments, this responsibility is shared between cloud service providers (CSPs) and their customers. According to this model, cloud customers must ensure that they uphold security, governance, and compliance measures “in the cloud”, while the CSPs are accountable for the security "of the cloud" (physical and infrastructure security) [7]. Table 1 demonstrates the overall structure of the shared responsibility model, which highlights the potential variability in the distribution of responsibilities between CSPs and their customers, contingent on the type of cloud service model employed [8]. However, the exact responsibilities of each party can vary depending on the specific CSP, and each CSP has its own standard security control. It is important for cloud customers to understand the shared responsibility model of their CSP and to take appropriate steps to secure their own data and applications in the cloud.

Table 1. Division of responsibility between CSP and customer, adapted from [8].

Responsibility	On-Premises	IaaS	PaaS	SaaS
User access	✔	✔	✔	✔
Data	✔	✔	✔	✔
Application	✔	✔	✔	➚
Runtime Environment	✔	✔	➚	➚
Middleware	✔	✔	➚	➚
Operating System	✔	✔	➚	➚
Virtualization	✔	➚	➚	➚
Servers	✔	➚	➚	➚
Storage	✔	➚	➚	➚
Networking	✔	➚	➚	➚

Note: The checkmarks ✔ denote the responsibilities retained by the cloud customer, whilst the arrows ➚ are indicative of the responsibilities transferred to the CSP.

Likewise, as organizations continue to migrate their data in the cloud environment, they still must comply with data and technologies regulations like General Data Protection and Regulations (GDPR), Health Insurance Portability and Accountability Act (HIPPA), and Payment Card Industry Data Security Standards (PCI-DSS) [9]. Those regulations enforce the implementation of policies and practices to protect Personal Identifiable Information (PII) and other standards depending on the organization's service type [10]. Compliance is not synonymous with security; however, it is one of the security processes. Complying with such regulations can help organizations pass IT security audits or any other audit relevant to a particular standardization. Failing to comply can cause an organization to pay high amounts of fines and can cause reputation damage.

Irrespective of the type of cloud service deployment, there are responsibilities that the cloud customers always retain. Those include ensuring the security of their data, accounts, endpoints protection, and access management. Thus, the above-explained model shows that the data proprietor (the entity that stores data in the cloud) has the responsibility for implementing proper configurations to protect its data and control who can access those data. Furthermore, the EU's GDPR data privacy legislation, which went into effect on 25 May 2018, explains that the responsibilities of securing personal data are on the data owner's shoulders, not the CSP's [11]. They must also ensure that the cloud providers with whom they collaborate support appropriate security and compliance safeguards. In other words, organizations still own their data and identities even in the public cloud. Hence, they are ultimately responsible for their security and all other components found under their control.

Moreover, various reports and guidelines published by organizations and agencies such as ENISA, the European Union Agency for Cybersecurity [12], and the US National Institute of Standards and Technology (NIST) [13] emphasize that cloud security is a shared responsibility between the involved parties (cloud actors). Each party should understand their roles and obligations and establish clear and transparent contracts and service level agreements that specify the security objectives, controls, and metrics. The NIST Cloud Computing Reference Architecture [13] outlines the five main cloud actors, comprising (1) the cloud consumer—a person or an entity that uses cloud services or resources from a cloud provider; (2) the cloud provider—an entity that provides cloud services or resources to cloud consumers; (3) the cloud auditor—the entity that conducts independent assessments of the cloud services or resources, such as security, performance, and compliance; (4) the cloud broker—the entity that intermediates between cloud consumers and cloud providers; and (5) the cloud carrier—the entity that transports data between cloud consumers and cloud providers, such as by providing network connectivity or bandwidth. While we acknowledge the significance of all cloud actors, comprehending their responsibilities and developing policies and procedures for their respective aspects of cloud security, this study particularly emphasizes the responsibilities of cloud consumers.

NIST has recently introduced a Cybersecurity Framework 2.0 (public draft) as an updated version of its predecessor, aiming to align with the continually evolving cybersecurity landscape and assist organizations in more efficiently managing cybersecurity risks. The framework outlines six core functions to achieve cybersecurity outcomes. These encompass the following [14]: (1) Govern—establish and monitor the organization's cybersecurity risk management strategy, expectations, and policy. (2) Identify—help determine the current cybersecurity risk to the organization. (3) Protect—use safeguards to prevent or reduce cybersecurity risk. (4) Detect—find and analyze possible cybersecurity attacks and compromises. (5) Respond—take action regarding a detected cybersecurity incident. (6) Recover—restore assets and operations that were impacted by a cybersecurity incident.

One of the tools that can be leveraged to achieve some of these security outcomes is the SIEM system. SIEM stands for security information and event management. SIEM systems collect, aggregate, and analyze data from various sources, such as logs, events, alerts, and incidents, and provide security teams with a centralized view of an organization's security posture, enabling security teams to identify, investigate, and remediate potential security incidents more effectively.

The traditional deployment method for SIEM systems is self-managed on-premises. This mandates that organizations conduct a thorough assessment of the magnitude of the log and event data they produce, as well as the necessary system resources for their efficient management. Following the surge in cloud computing adoption, most major SIEM vendors now offer a cloud-based version of their products. This gives organizations the option to deploy SIEM solutions either on-premises or in the cloud.

However, cloud-based SIEM solutions that were originally designed for traditional IT environments may not be well suited to cloud environments. This is because cloud infrastructures have unique characteristics and requirements that may not align with the capabilities and configurations of traditional SIEM systems. For example, cloud environments are dynamic, scalable, heterogeneous, distributed, and multi-tenant, which makes it difficult to collect and analyze data from various sources and locations. Cloud environments also have specific data types and formats that are not supported by traditional SIEM solutions.

Some of the major cloud service providers have proactively anticipated these challenges and have recently started to introduce cloud-native SIEM solutions. Examples include Chronical SIEM for Google Cloud [15] and Microsoft Sentinel for Microsoft Azure [16]. These cloud-native SIEM solutions are purpose-built for the cloud environment from the start, utilizing microservice architectures and incorporating cloud-specific analysis methods and detection capabilities.

These cloud-native solutions are deemed essential. However, it is still the responsibility of cloud consumers to take the necessary steps to integrate SIEM solutions into their cloud environment. Considering the persistent and widespread risk of encountering threats and malicious activities in any cloud computing infrastructure, establishing a cloud-native centralized system for monitoring, detecting, and responding to security threats is critically important.

Therefore, as a part of our contribution, we present an architectural deployment framework that integrates a cloud-native SIEM solution within a public cloud environment. We propose and demonstrate in an empirical way a security design for internet-exposed infrastructure elements that need to reside behind a web application firewall (WAF), but also describe the steps for setting up a cloud-based Security Operation Center (SOC) leveraging cloud-native solutions. Beyond threat monitoring and detection, the framework encompasses a module for compliance assessment. This component evaluates compliance with pertinent industry standards and regulatory requirements, ensuring that the deployed cloud infrastructure aligns with the necessary criteria for compliance.

The rest of this paper is structured as follows: Section 2 provides a comprehensive review of the related works in the field, emphasizes the research gap, and sets the stage for our contribution. Section 3 presents the method, materials, and steps employed to design the proposed architecture. Section 4 discusses the results obtained from the deployed system, demonstrating the effectiveness and limitations of the proposed model. Finally, in Section 5, we provide the concluding remarks and future direction.

2. Related Works

This section aims to provide an overview of the existing research and literature pertinent to the subject of our study and highlights the contribution of our research.

In the realm of cloud security, several established frameworks serve as pivotal guides for organizations aiming to fortify their cloud environments. These frameworks and several other guidelines from states or federal agencies offer structured approaches and best practices to mitigate risks and ensure the integrity, confidentiality, and availability of data and services in cloud infrastructures.

Among the notable [17,18] frameworks are the NIST Cybersecurity Framework, which provides a comprehensive set of guidelines for managing and reducing cybersecurity risks, while the NIST Special Publication (SP800-144) provides guidelines on security and privacy in public cloud computing. It covers the security and privacy challenges and considerations for organizations that outsource data, applications, and infrastructure to a public cloud environment. Similarly, the Center for Internet Security (CIS) Controls provides a prioritized and actionable framework to help organizations enhance their cybersecurity posture and defend against cyber threats. Also, both ENISA and the Cybersecurity and Infrastructure Security Agency (CISA) have released extensive guidelines specifically tailored to address the unique challenges and requirements of cloud security. ENISA provides valuable insights into cloud security best practices and risk management strategies within the European context, while CISA offers comprehensive resources for safeguarding critical infrastructure and enhancing cybersecurity resilience in the United States.

In addition, the Cloud Security Alliance (CSA) provides a suite of resources and frameworks tailored specifically to cloud security. Their frameworks, such as the Cloud Controls Matrix (CCM) and the Security Guidance for Critical Areas of Focus in Cloud Computing, are instrumental in establishing robust cloud security strategies. Likewise, COBIT 5, a globally recognized framework for the governance and management of enterprise IT, was extended to COBIT 5 for cloud computing to provide practical guidance for enterprises using or considering using cloud computing. The framework highlights cloud computing challenges, governance and management in the cloud, cloud assurance reviews, and cloud risk assessment.

Furthermore, ISO/IEC2701 [19], an extension of the ISO/IEC 27001 standard [20], focuses specifically on information security controls for cloud services. It provides additional guidelines and controls to address the unique challenges and requirements of cloud computing environments. Moreover, the major CSPs (Azure, AWS, Google) developed well-architected frameworks that provide tailored recommendations and specific guidance for securing cloud environments within their respective platforms.

Table 2 presents an overview of implementation strategies and recommendations tailored for incident management and compliance, specifically aligned with the Microsoft Well-Architected Framework in accordance with Microsoft Azure as the cloud environment utilized in this study.

Table 2. Microsoft Azure Well-Architected Framework compliance and incident management controls.

Frameworks	Compliance Controls	Incident Management Controls
Microsoft Azure Well-Architected Framework [21]	• Compliance review: - Improve secure score in Microsoft Defender for Cloud; - Use an industry standard benchmark to evaluate your organization's current security posture; - Perform regular internal and external compliance audits, including regulatory compliance attestations; - Review the policy requirements.	• Logs and alerts: - Configure central security log management; - Enable audit logging for Azure resources; - Collect security logs from operating systems; - Configure security log storage retention; - Enable alerts for anomalous activities. • Review and remediation: - Processes for handling incidents and post-incident activities, such as lessons learned and evidence retention. - Remediate the common risks identified by Microsoft Defender for Cloud. - Track remediation progress with secure score and comparison against historical results. - Address alerts and take action with remediation steps. • Use a combination of native services to obtain a full view: Azure Monitor, Microsoft Defender for cloud, and Microsoft Sentinel.

Several other studies have been carried out on this subject matter, Jakub et al. [22] highlighted the critical nature of security in cloud environments and the difficulty of maintaining a comprehensive view of the safety of individual resources in large cloud computing systems. To address this challenge, the authors propose the utilization of SIEM technology for central monitoring and maintaining awareness of security threats. The paper analyses the technical requirements, logic, and legal framework of SIEM in the context of the Czech Republic and proposes a framework for utilizing SIEM in cloud computing environments. López et al. [23] conducted a comprehensive review of the status and prospects of SIEM technology. The study highlights that SIEM technology is constantly evolving and facing new requirements and demands from users, such as compatibility with cutting-edge technologies (e.g., blockchain, cloud, containers), adherence to international standards and regulations (e.g., GDPR), and improvements in detection engines and response mechanisms. It also proposes a new framework termed SIEM-SC (security compliance), which integrates blockchain, encryption, and containers to enhance the security and compliance of SIEM systems. The authors claim that their framework is compatible with GDPR and can improve the performance, scalability, and reliability of SIEM technology. In [24], Adriano et al. proposed a low-cost serverless SIEM solution that utilizes cloud services to store and correlate security events. The authors highlight the advantages of SIEMs in detecting and responding to security incidents but also acknowledge the high cost and maintenance requirements associated with traditional SIEMs. The study addresses these issues by investigating techniques to index, compress, and store events in a cost-efficient and safe way for a long time. The proposed solution leverages a serverless platform, like Amazon Lambda, to streamline the management of SIEMs and charge the customer only for the event processing time.

The study presented in [25] proposes a SIEM architecture that can be deployed to a cloud-based security service platform for analyzing and recognizing intelligent cyber threats based on virtualization technologies. The authors argue that the traditional SIEM paradigm can be shifted to cloud-based security services, leveraging the scalability, flexibility, and cost-effectiveness of cloud computing technologies. The authors claim that the proposed architecture can help improve the accuracy and efficiency of cyber threat detection and response by leveraging the advanced analytics and machine learning capabilities of virtualization technologies. Ghallab et al. [26] provide an overview of the integrity and security problems in distributed cloud computing environments, while Kanwal et al. [27] highlight the potential issues that are being investigated and are preventing organizations from migrating traditional IT environments to cloud computing. Alam et al. [28] address the challenge of processing large amounts of data in real time for identifying security issues, especially when hardware infrastructure is limited. The authors propose a solution for optimizing SIEM throughput on the cloud using parallelization, which can help managed security service providers (MSSPs) to process large amounts of data efficiently and identify security issues quickly.

In [29], Garg et al. presented a study on analytical approaches to understanding the overall structure and developments in cloud computing but also discussed the concept of cloud computing security issues in terms of vulnerabilities, threats, and attacks. Rady et al. [30] focused on integrity and confidentiality in cloud-outsourced data. They offered a top-level view of various cryptographic algorithms primarily based on different systems inside the outsourced database security and query authentication. In addition, they proposed a structure that could help in achieving the confidentiality and integrity of query outcomes of the outsourced database. Attou et al. [31] provide valuable insights into leveraging machine learning for intrusion detection in the cloud computing environment. The authors propose an intrusion detection system model leveraging Deep Learning (DL) algorithms, specifically, the Radial Basis Function Neural Network (RBFNN) and Random Forest (RF). Their approach demonstrates improved accuracy and a substantial increase in the Matthews Correlation Coefficient (MCC). According to the authors, integrating this proposed IDS model into cloud environments has the potential to offer cloud providers enhanced security measures, such as minimizing unauthorized access and the risk of data breaches.

PADRES, a tool designed for privacy, data regulation, and security, was created in [32] to assist companies in evaluating their compliance with GDPR. The emphasis of the software is the analysis of web applications, which results in a GDPR classification and a report with recommendations for improvement. In addition, the software also has a component that searches for vulnerabilities by integrating open-source scanning tools. However, PADRES did not directly focus on privacy concerns, and the responsibility of designing the inputs still falls on the developer as the compliance assessment questions are answered manually. Georgiou [33] reviewed and analyzed the existing cloud threats and focused on those that do not apply to traditional systems. They also examined CSPs' security requirements by taking Europe's e-health system as a case study.

The reviewed studies emphasize the significance of security in the cloud and highlight SIEM technology as a promising approach to tackling the complex security challenges posed by the dynamic and complex nature of cloud networks. Furthermore, a substantial portion of the reviewed studies predominantly concentrate on exploring security challenges related to Software as a Service (SaaS) models, while relatively fewer studies address security issues specific to Infrastructure as a Service (IaaS) models. While data confidentiality has rightly received considerable attention in the literature, it is crucial to recognize that safeguarding data confidentiality alone is inadequate for upholding the fundamental principles of the CIA triad, which encompasses confidentiality, integrity, and availability. It is undeniable that data confidentiality is a critical aspect of security, yet it is equally crucial to ensure the integrity and availability of cloud-based systems and services. Maintaining data integrity guarantees that data remain accurate, unaltered, and trustworthy throughout their lifecycle, while availability focuses on ensuring uninterrupted access to cloud resources and services. Moreover, the reviewed works have predominantly focused on security aspects; however, it is also important to recognize the significance of compliance as an integral part of an organization's overall security strategy. Ensuring compliance entails verifying that cloud resources adhere to industry standards and regulatory requirements. Neglecting compliance requirements can lead to severe consequences, including financial penalties, loss of customer trust, and damage to the organization's reputation.

Considering that cloud environments pose new security challenges and risks, this study adds to the existing literature by implementing a cloud-based SOC leveraging cloud-native solutions to manage incidents and compliance in cloud infrastructure, emphasizing the role of the cloud consumer in protecting the cloud ecosystem in accordance with the shared responsibility model.

3. Materials and Methods

This section outlines the approach taken to conduct our study and the resources used in the process. It provides insight into the experimental design, security event collection procedures, and employed techniques.

The first step in the SIEM's functional process typically involves the data collection phase. At this stage, the SIEM system gathers data from various sources, such as logs, events, and other security-related information from across the network and information systems. These data are then aggregated and normalized to create a standardized dataset that can be further analyzed for security insights and alerts. Before the data collection phase, it is crucial to have a solid infrastructure in place. To obtain this infrastructure, we successfully deployed a virtual network (Vnet) within the Microsoft Azure public cloud environment. This virtual network establishes the foundation infrastructure to support the SIEM system.

A virtual network in a cloud environment is an abstraction of a physical network. It is a logically isolated section of the cloud provider's network infrastructure and allows one to define their own IP address ranges, subnets, security groups, etc. [34]. It still exists physically in the sense that it relies on the underlying hardware and internet connections of the cloud service provider to transmit data and signals. Hence, in the subsequent sections, when we refer to a virtual network or virtual machines (VMs), we are referring to the way these resources are abstracted and provisioned, not that they do not physically exist. The implemented Vnet consisted of three network subnets, facilitating the deployment of diverse Azure cloud resources such as VMs, firewalls, and gateways. For illustrative purposes, this study employed Microsoft Azure as a public cloud environment and adopts the Azure Well-Architected Framework recommendations for deploying solutions on a cloud-based infrastructure.

Through the subsequent subsections, we provide in-depth insights into the deployed cloud instances, highlighting their roles, functionalities, and contributions to the overall functionality and security of the implemented virtual network. We also provide a detailed account of how we integrated other solutions into this deployed infrastructure. Figure 1 depicts the overall deployment architectural model.

3.1. Virtual Network Design

As depicted in Figure 2, the deployed virtual network (Vnet) comprises three subnets. The first subnet, referred to as the front subnet (subnet1), is publicly accessible and Internet-facing. It includes an application gateway serving as both a web application firewall (WAF) and a public load balancer. The application gateway directs incoming traffic to the second subnet (subnet3), which consists of two VMs functioning as web servers and one VM serving as a logic server. The third subnet, referred to as the back subnet (subnet3), accommodates two VMs operating as storage servers. To balance the loads between subnet2 and subnet3, an internal load balancer is employed.

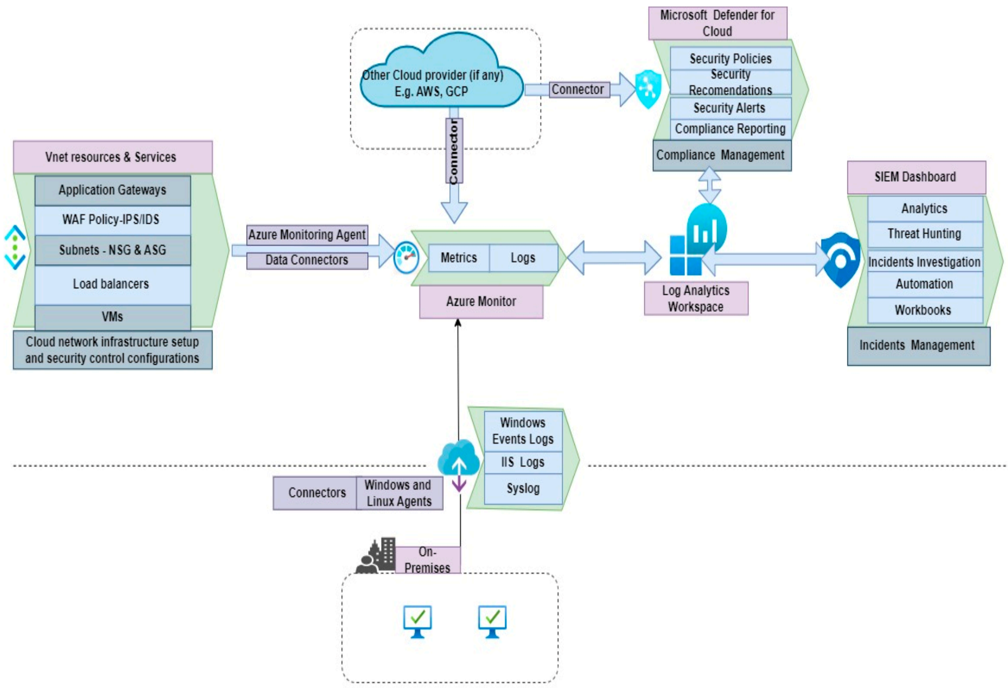


Figure 1. Overall deployment architecture model.

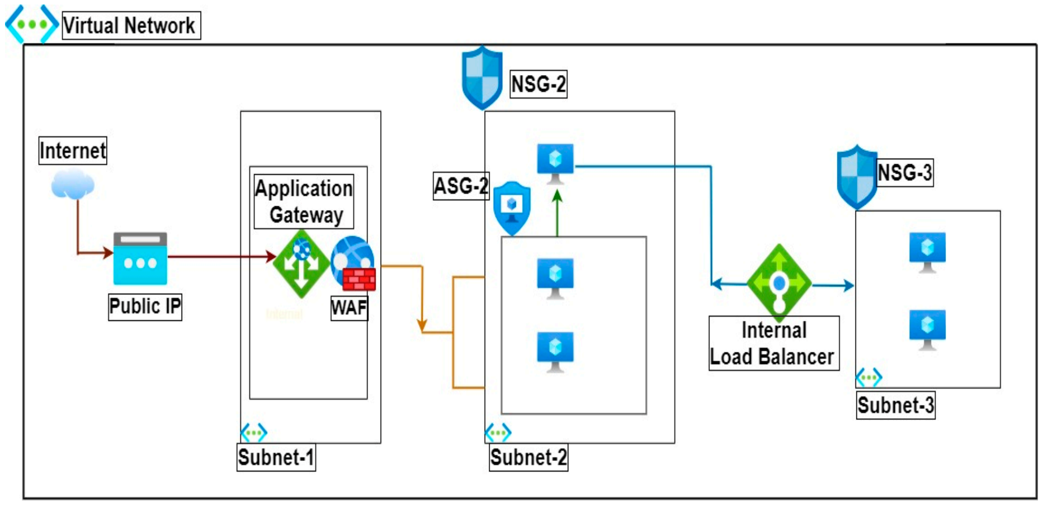
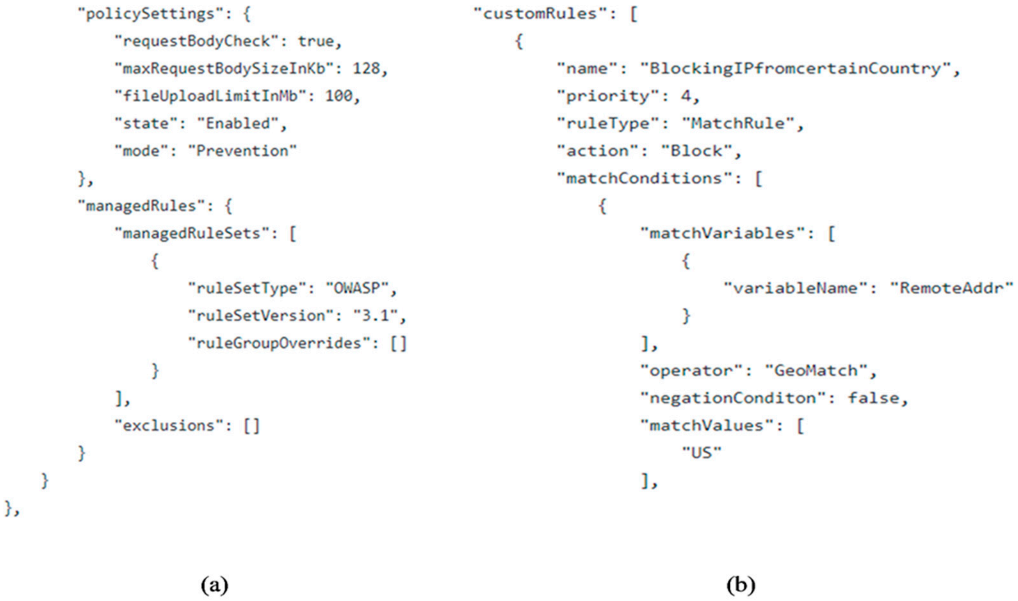


Figure 2. Logical virtual network design.

3.1.1. Application Gateway/Web Application Firewall

An Azure instance that serves as a public web traffic load balancer and as a WAF to protect against web application vulnerabilities. It supports TLS/SSL traffic encryption between users and an application gateway and between application servers and an application gateway [35]. In this experiment, the application gateway serves as a gateway to the web servers running in the back-end pool. The servers are accessible using the public IP address of an application gateway, and a listener routes requests to a back-end pool of servers following a configured HTTP rule.

The WAF component examines incoming requests before they reach the listener and employs the Open Web Application Security Project (OWASP) core rules to detect potential threats [27]. The OWASP defines a collection of rules known as the core rule set, which covers common security threats such as remote file inclusion, HTTP request smuggling, cross-site scripting (XSS), SQL injection, command injection, HTTP response splitting, and various types of bots and scanners. The Azure WAF currently supports four core rule sets: CRS 3.2, 3.1, 3.0, and 2.2.9. In our experiment, we utilized CRS 3.1. By default, the WAF policy consists of managed rules, but it is also possible to incorporate customized rules, for example, to restrict remote access to a cloud infrastructure based on geo-location. Additionally, the WAF policy can operate in either detection or prevention mode. A snippet of the policy settings and rules is depicted in Figure 3.



```
        "policySettings": {
            "requestBodyCheck": true,
            "maxRequestBodySizeInKb": 128,
            "fileUploadLimitInMb": 100,
            "state": "Enabled",
            "mode": "Prevention"
        },
        "managedRules": {
            "managedRuleSets": [
                {
                    "ruleSetType": "OWASP",
                    "ruleSetVersion": "3.1",
                    "ruleGroupOverrides": []
                }
            ],
            "exclusions": []
        }
    }
},
```

(a)

```
"customRules": [
    {
        "name": "BlockingIPfromcertainCountry",
        "priority": 4,
        "ruleType": "MatchRule",
        "action": "Block",
        "matchConditions": [
            {
                "matchVariables": [
                    {
                        "variableName": "RemoteAddr"
                    }
                ],
                "operator": "GeoMatch",
                "negationConditon": false,
                "matchValues": [
                    "US"
                ],
```

(b)

Figure 3. OWASP policy settings (**a**) and rule creation (**b**).

3.1.2. Network Security Group (NSG)

The NSG filters network traffic in and out of Azure resources within Azure Vnet [36]. The security rules allow or deny inbound or outbound network traffic from various Azure resources. The NSG can be associated with either a subnet or a Network Interface Card (NIC) of a particular VM. The evaluation of rules is performed according to the priority associated with them. In addition, rules creation requires specifying the direction (inbound or outbound), source/destination (IP addresses, service tags, application security group), protocol (could be UDP, TCP, or any), port or port ranges (HTTP-80, SSH-22, RDP-3389, etc.), and action (allow or deny). The NSG has preconfigured rules that can be overridden by creating augmented rules with higher priority than the default ones. In this experiment, we created two NSGs assigned to subnet2 and subnet3. The flow record in Azure Vnet enables an NSG to be stateful. It implies that if one specifies an outbound security rule for any address through a specific port, one does not need to set an inbound security rule for the response to the outbound traffic.

3.1.3. Application Security Group (ASG)

In Azure Vnet, an ASG enables the grouping of virtual machines and the configuration of network security policies based on that group [37]. This approach offers a more streamlined alternative to traditional explicit IP-address-based configurations and multiple rule sets, which can become complex to manage. An ASG is assigned to a NIC for effective implementation. As illustrated in Figure 1, our implementation involves utilizing an ASG to consolidate and manage two web server VMs, simplifying network security policy management.

3.1.4. Internal Load Balancing

In this study, we utilize an internal load balancer to distribute incoming flows from its front end to the back-end pool servers located in subnet3. This load distribution is performed based on the rules configured for the load balancer, ensuring efficient resource utilization and optimal performance.

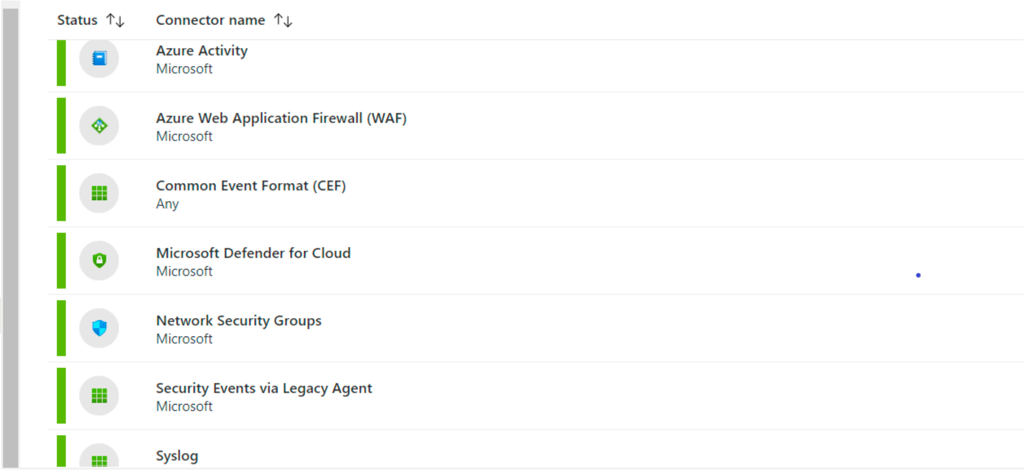
3.2. Microsoft Sentinel and Log Analytics Deployment

Microsoft Sentinel is "a scalable, cloud-native, security information and event management (SIEM) and Security Orchestration Automation and Response (SOAR) solution" [29]. It collects data from all sources, including users, servers, and applications, in both cloud-based and on-premises devices [16]. It has built-in connectors to make it easier to integrate popular security solutions. Microsoft Sentinel can support open standard formats such as Common Events Format (CEF) and Syslog.

An Azure Log Analytics workspace is "a logical storage unit in Azure where all log data generated by Azure Monitor from various sources are stored" [38]. It uses the Kusto Query Language (KQL) version to speedily fetch, consolidate, and analyze all data collected into Azure Monitoring Logs. To meet the objectives of this study, we deployed a Microsoft Sentinel instance with a log analytics workspace. To ingest data in our environment, we connected the VMs created in the previous section to the workspace using an Azure Monitor Agent (AMA). The AMA collects monitoring data from Azure virtual machines' guest operating systems and sends them to Azure Monitor (log analytics workspace) [39]. Microsoft Defender for Cloud is connected to our workspace to check industry and regulatory compliance status. Figure 4 depicts a selection of the data connectors that were utilized. In addition, to have more data ingested in our log analytics, we installed a log analytic agent—an operation management suite (OMS) on on-premises machines that collects data and sends them to a log analytics workspace in Azure. The agent configurations are adjusted to meet the nature of events that one wishes to gather and their severity. Figure 5 showcases the flow for data logging and processes.

For a user to detect a threat in their cloud environment, they need to be notified when suspicious activity occurs. In this regard, Microsoft Sentinel uses analytics rules to correlate alerts into incidents [40]. These rules automatically search the environment for any suspicious activity and can be used either as-is or customized to fit the need of the organization. A playbook is set to automatically be executed if an alert is generated by Sentinel analytics rules. With the help of Microsoft solution, we ingested pre-recorded data [41] to enable several artifacts to simulate real-world scenarios. From that, we created a rule to detect malicious phishing activity from the real-world experience available in [42].

Furthermore, Microsoft Sentinel workbooks offer a wide range of usage options. Starting from visual data representation to complex graphing and resource investigation maps, Sentinel has different types of workbooks. In this experiment, we focused on the Investigation Insight, Identity and Access, Data Collection, and Health Monitoring workbooks.



Status ↑↓	Connector name ↑↓
	Azure Activity Microsoft
	Azure Web Application Firewall (WAF) Microsoft
	Common Event Format (CEF) Any
	Microsoft Defender for Cloud Microsoft
	Network Security Groups Microsoft
	Security Events via Legacy Agent Microsoft
	Syslog

Figure 4. Employed data connectors.

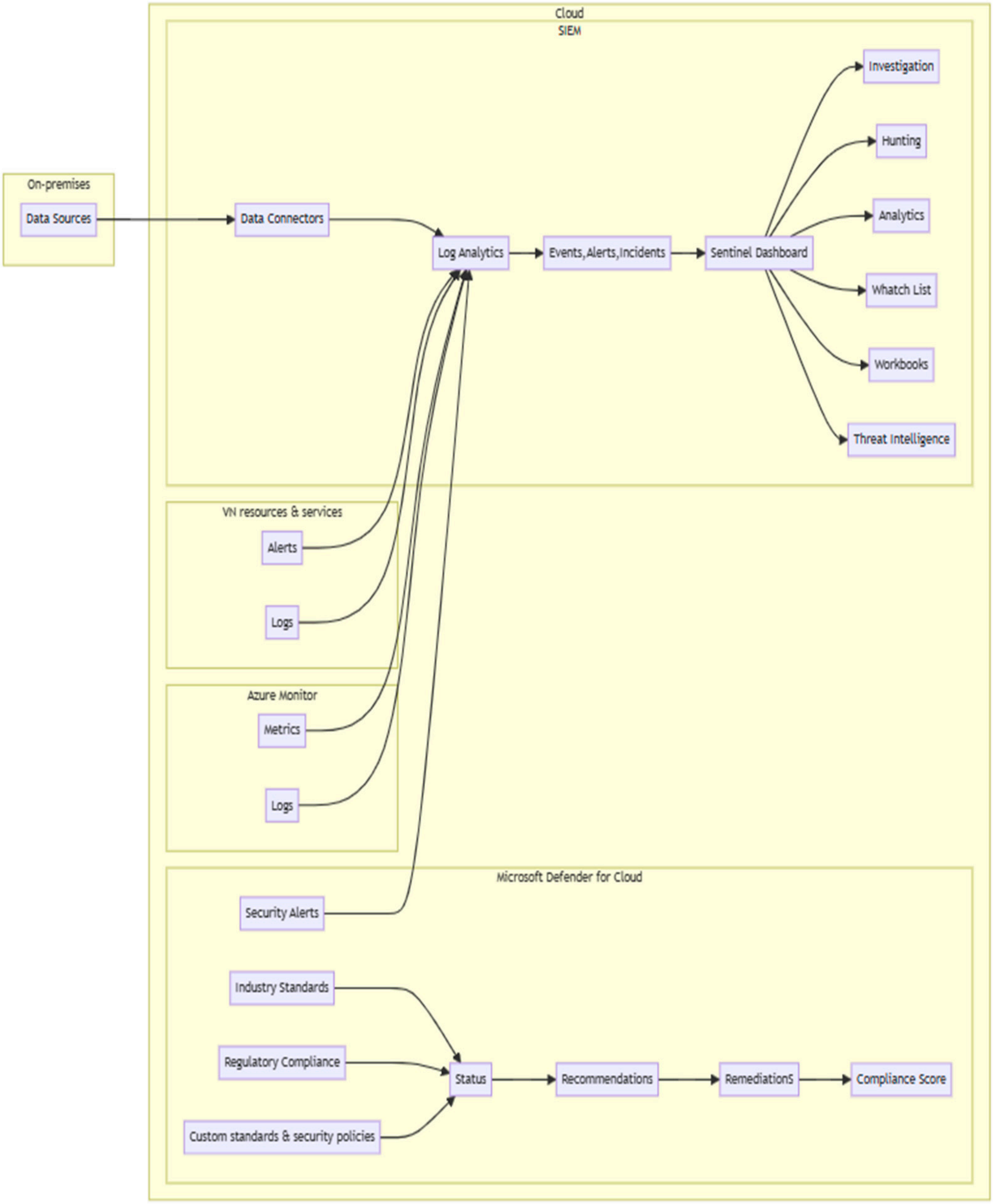


Figure 5. Data logging and processes flow.

3.3. Microsoft Defender for Cloud

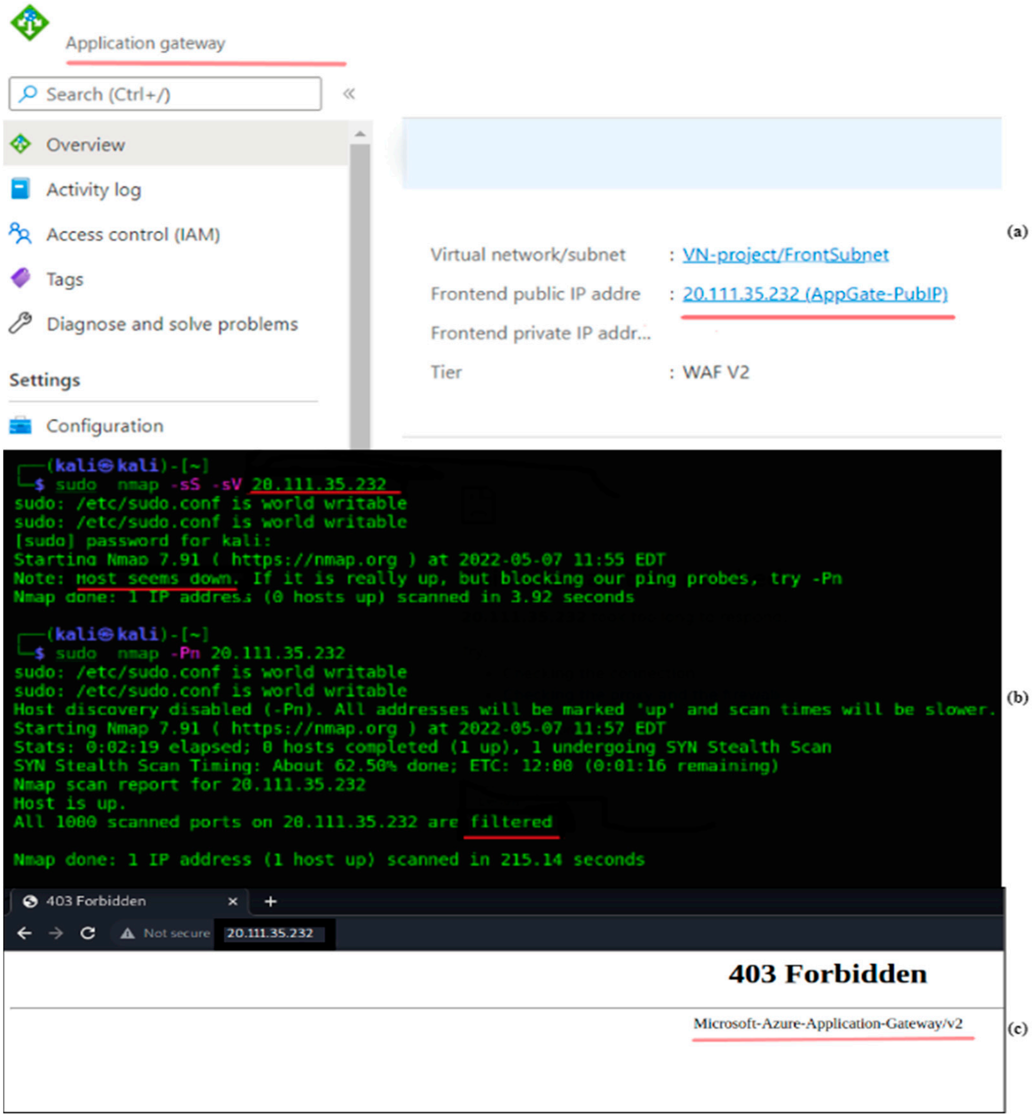
Microsoft Defender for Cloud is linked to Sentinel to check industry and regulatory compliance status. Microsoft Defender for Cloud has an integrated regulatory compliance dashboard that assesses cloud instances configurations by comparing them with the industry standards, regulations, and benchmarks needed to meet compliance requirements. With a focus on cloud-centric security, the Azure Security Benchmark expands on controls developed by the Center for Internet Security (CIS) and the National Institute of Standards and Technology (NIST) [43]. A permanent link to the deployment configurations repository is available in [44].

4. Results and Discussions

4.1. Virtual Network Security Control

In this section, we present the key aspects of the results obtained from our study, providing insights into the effectiveness and performance of the implemented solutions. In addition to presenting the results, this section discusses the encountered challenges and limitations as well as recommendations.

To begin with, we conducted configuration validation by setting up Internet Information Services (IISs) on the virtual machines in the back-end pool. These VMs hosted a publicly accessible web page, accessible through the front IP address (public IP) of the application gateway. To validate the feasibility of the employed security configurations, we performed a Network Mapper (Nmap) scan, examining the running services, versions, and open ports. However, the scan yielded failed results as the ports were filtered, representing one of the port states recognized by Nmap [45]. The Nmap tool can be used for both legitimate and malicious purposes. It is not an intrusion attack by itself, but it can help attackers find ways to intrude into a network. The filtered status signifies that the Nmap probes were unable to determine the status of the ports due to the preventive measures implemented by the WAF, effectively blocking their access. Moreover, we attempted to access the servers from a restricted region using a browser connected through a virtual private network (VPN). It resulted in a denied access, demonstrating the effectiveness of the custom rule in place to prevent specific remote access. In Figure 6, a segment of the Nmap scan results and denied remote access are depicted.



Virtual network/subnet : VN-project/FrontSubnet
Frontend public IP addre : 20.111.35.232 (AppGate-PubIP)
Frontend private IP addr...
Tier : WAF V2

```
┌──(kali㉿kali)-[~]
└─$ sudo  nmap -sS -sV 20.111.35.232
sudo: /etc/sudo.conf is world writable
sudo: /etc/sudo.conf is world writable
[sudo] password for kali:
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-07 11:55 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.92 seconds

┌──(kali㉿kali)-[~]
└─$ sudo  nmap -Pn 20.111.35.232
sudo: /etc/sudo.conf is world writable
sudo: /etc/sudo.conf is world writable
Host discovery disabled (-Pn). All addresses will be marked 'up' and scan times will be slower.
Starting Nmap 7.91 ( https://nmap.org ) at 2022-05-07 11:57 EDT
Stats: 0:02:19 elapsed; 0 hosts completed (1 up), 1 undergoing SYN Stealth Scan
SYN Stealth Scan Timing: About 62.50% done; ETC: 12:00 (0:01:16 remaining)
Nmap scan report for 20.111.35.232
Host is up.
All 1000 scanned ports on 20.111.35.232 are filtered

Nmap done: 1 IP address (1 host up) scanned in 215.14 seconds
```

403 Forbidden ×
Not secure 20.111.35.232

403 Forbidden

Microsoft-Azure-Application-Gateway/v2

Figure 6. (**a**) Application gateway configuration, (**b**) Nmap scan, (**c**) forbidden remote access.

The main objective was to establish secure measures within the virtual network to protect against unauthorized access to the storage server (subnet3), which may house critical data. Through the implementation of access control rules in NSG and ASG, respectively, we aimed to ensure that only authorized traffic is allowed to reach the storage server, effectively mitigating the risk of unauthorized individuals gaining access to the sensitive data. The results demonstrate the effectiveness of the network security group and application security group in managing and securing network access.

4.2. SIEM Solution

The employed SIEM system analytics allow a security analyst to identify recurring incidents and uncommon trends that would otherwise go un-noticed. The incident page is the entry point for an analyst to consume security incidents (tickets) in Sentinel, and Figure 7 illustrates the deployed SIEM incident status page.

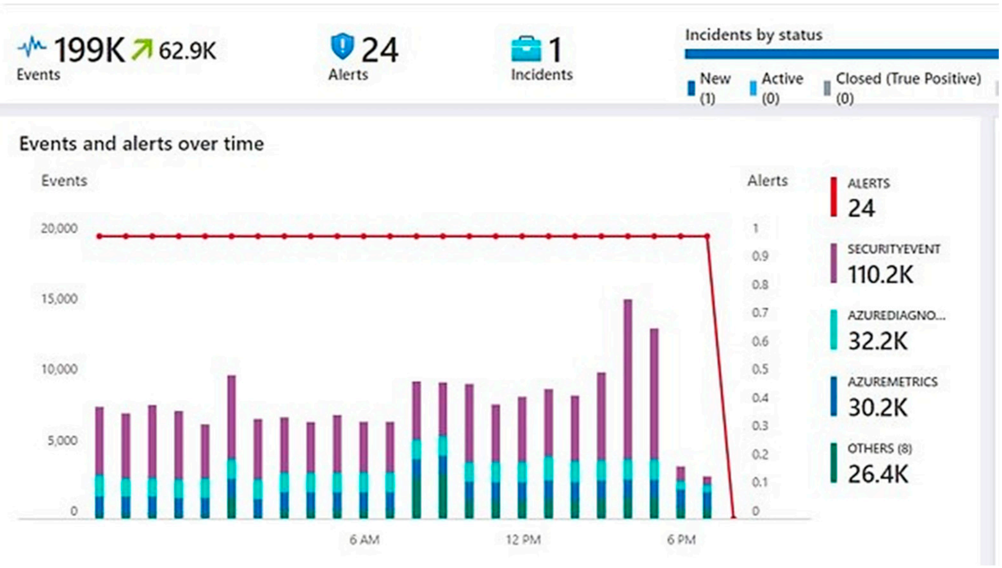


Figure 7. SIEM incident status page.

This page offers visibility into all entities involved in an alert and presents a user-friendly interface (UI) for investigating the detections, allowing analysts to swiftly grasp the scope of a breach. The investigation graph showcased in Figure 8 enables the correlation of relevant data with the associated entities, facilitating a deeper understanding and determination of the potential security threat's root cause. The Timeline tab facilitates analysts to scrutinize the chronological sequence of alerts within an incident, thereby enabling them to reconstruct the sequence of attack activities with precision and depth. Meanwhile, in the Entities tab, analysts can explore all the entities mapped as per the defined alert rule. It offers a comprehensive overview of the diverse objects implicated in the incident, ranging from users and devices to addresses and files, among others.

Working with Microsoft Sentinel workbooks provides quantified graphical data representation and allows for the creation of interactive reports that can enhance security analysts' ability to see beneath the surface of what is going on in the cloud. Figure 9 presents data collection and health monitoring, identity and access, and threats intelligence in the log analytics workspace workbooks. The dashboard and visual representations are very useful in the world of security operations to show trends and anomalies in day-to-day security events. Without such analytics capabilities in place, the ability of security analysts would be limited in scope and effectiveness.

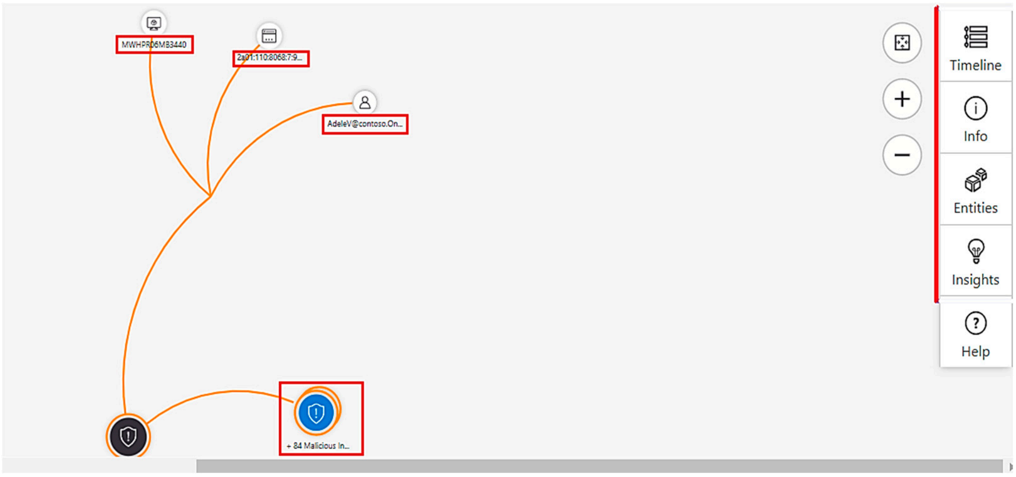
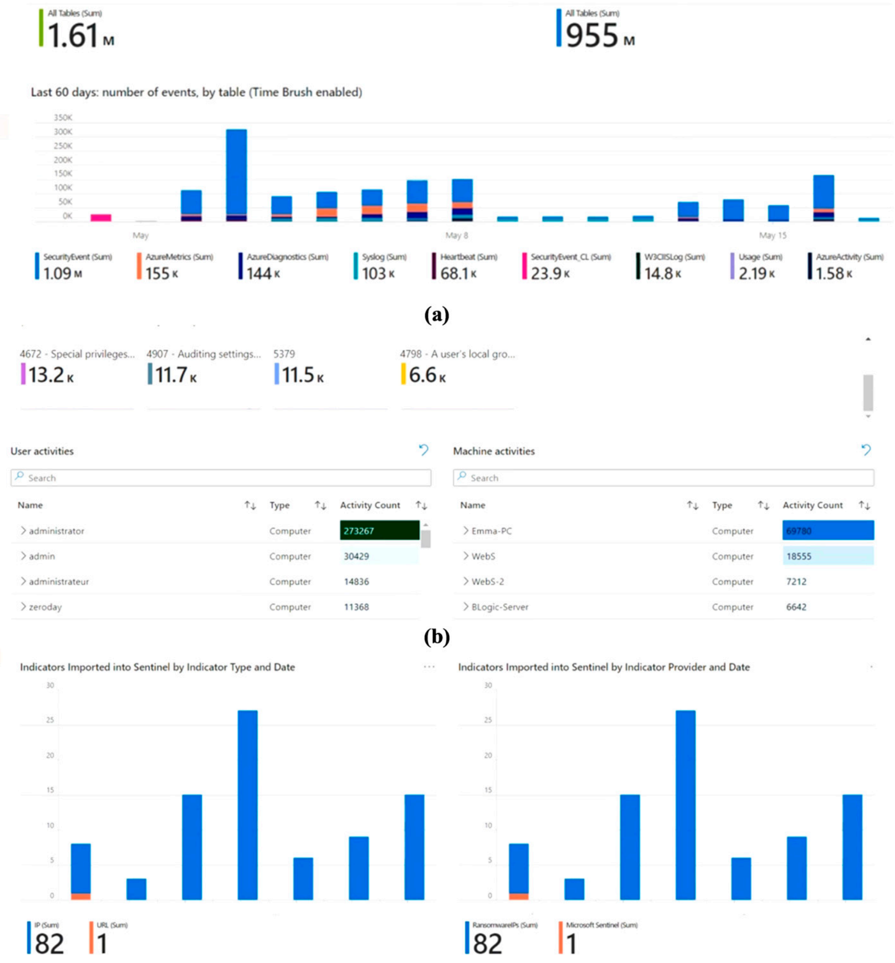


Figure 8. Investigation graph.


All Tables (Sum)
1.61 M
All Tables (Sum)
955 M
Last 60 days: number of events, by table (Time Brush enabled)
350K
300K
250K
200K
150K
100K
50K
0K
May
May 8
May 15
SecurityEvent (Sum) 1.09 M
AzureMetrics (Sum) 155 K
AzureDiagnostics (Sum) 144 K
Syslog (Sum) 103 K
Heartbeat (Sum) 68.1 K
SecurityEvent_CL (Sum) 23.9 K
W3CIISLog (Sum) 14.8 K
Usage (Sum) 2.19 K
AzureActivity (Sum) 1.58 K
4672 - Special privileges... 13.2 K
4907 - Auditing settings... 11.7 K
5379 11.5 K
4798 - A user's local gro... 6.6 K
User activities
Machine activities
Search
Indicators Imported into Sentinel by Indicator Type and Date
Indicators Imported into Sentinel by Indicator Provider and Date
30
25
20
15
10
5
0
IP (Sum) 82
URL (Sum) 1
RansomwareIPs (Sum) 82
Microsoft Sentinel (Sum) 1

(a)

User activities

Name	Type	Activity Count
administrator	Computer	273267
admin	Computer	30429
administrateur	Computer	14836
zeroday	Computer	11368

Machine activities

Name	Type	Activity Count
Emma-PC	Computer	69780
WebS	Computer	18555
WebS-2	Computer	7212
BLogic-Server	Computer	6642

(b)

(c)

Figure 9. Performance of data collection and health monitoring (**a**), identity and access (**b**), threats intelligence (**c**)—Log analytics workspace workbooks.

The analysis of the Data Health and Monitoring workbook revealed valuable insights into critical metrics, such as ingestion size, latency, logs per source, and the identification of data collection anomalies. Figure 9a demonstrates how events were categorized into tables based on activated log types, including security events, Syslog, Azure metrics, Azure diagnostics, and more. The workbook helps ensure seamless and uninterrupted data ingestion into the log analytics workspace. Moreover, the Identity and Access workbook (Figure 9b) provided a comprehensive view of users and connected device activities within the Azure Active Directory. It enabled the analysis of identity and access events, including sign-in events, audit events, and risky users. The visualizations and metrics presented in this workbook proved instrumental in understanding user behaviors and identifying potential security issues.

Additionally, the Threat Intelligence workbook (Figure 9c) played a vital role in the identification and response to threats. By leveraging indicators of compromise (IOCs) such as IP addresses, domains, URLs, and email addresses, it facilitated threat hunting across cloud workloads. The workbook's analysis capabilities allow a deeper understanding of observed threats, including their associated threat groups, targeted assets, tactics, techniques, and procedures (TTPs).

4.3. Compliance Assessment

The compliance solution continuously evaluates a user's cloud environment to identify risk factors based on the controls and best practices in the standards they have applied to their subscriptions. In that line, the status of all chosen standards and regulations is displayed on the regulatory compliance dashboard. This evaluation helps the compliance analyst to continue acting on the security recommendations and improve the compliance posture by reducing the risk factors. Compliance assessment offers several benefits within the cloud environment. Firstly, users have the flexibility to choose from a wide range of supported standards and benchmarks, including Azure Security Benchmark, NIST SP 800-53, HIPAA/HITRUST, PCI-DSS, SOC TSP, and more, ensuring alignment with industry-specific requirements. Additionally, users can customize the set of standards and benchmarks to focus on their specific compliance needs. Moreover, users can set up alerts to promptly detect changes in compliance status and export compliance data either as a continuous stream or as weekly snapshots. Lastly, the compliance assessment module provides actionable recommendations for investigating and remediating compliance issues, empowering users to maintain and enhance their compliance posture.

4.4. Challenges, Limitations, and Recommendations

While our system demonstrated promising results, it is essential to acknowledge the limitations encountered during the experiment. Firstly, we strategically deployed cloud resources within our budgetary limits, allowing us to initiate the implementation of solutions while considering further scalability enhancement. To ensure comprehensive evaluation, future research should aim to incorporate large-scale deployments that align more closely with organizational-level scenarios, ensuring a greater relevance and applicability of findings. Secondly, we must emphasize that our study primarily focused on exploring a cloud-native SIEM solution. Nevertheless, it is worth acknowledging the availability of various third-party SIEM solutions that offer promising opportunities for effective integration within the cloud environment, broadening the range of options for potential users. Exploring these alternative solutions can provide valuable insights and expand the scope of research in this domain.

Thirdly, while it is feasible to integrate data sourced from third-party cloud service providers (CSPs) to evaluate pertinent compliance scores, this could be a daunting task for organizations that adopted multi-cloud environments—signifying entities that have implemented two or more distinct CSPs. As of the time of composition, the sole third-party CSPs supported in Sentinel are AWS and GCP. Furthermore, it was apparent that for large-scale deployments, the mismanagement of cloud resources could potentially result in inflated charges, which may prove burdensome to organizations. In this light, it is significant to have proficient individuals who can govern cloud expenditure to circumvent unnecessary expenses. As there are various security tools, a comprehensive assessment may be required to judge which one best fits organizational demand. It is equally important to leverage the inherent features of cloud computing, such as rapid elasticity, which allows cloud resources to be shrunk and/or grown to accommodate organizational needs. Likewise, with the metered services characteristic of cloud computing systems, customers can monitor and regulate the utilization of provisioned resources in real time, thereby providing transparency between the CSPs and the customers.

Nevertheless, we maintain that the advantages of implementing a SIEM system outweigh the associated challenges. Integrating such a system within a cloud environment enables the automation of security controls, reducing risks and mitigating the impact on cloud resources. Once the requisite configurations are in place, the system alleviates the burden on security professionals, who are typically accountable for cybersecurity incidents. This can promote a more resilient security framework and enhance an organization's overall security posture in the cloud environment.

5. Conclusions

This paper has presented and demonstrated an empirical security design for Internet-exposed infrastructure elements that require a web application firewall, as well as the initial steps for establishing a cloud-based Security Operation Center. The proposed design can serve as a model for small enterprises that manage their own cloud infrastructure and incident response without relying on externally managed security service providers. The paper has also emphasized the shared responsibility between the cloud service provider and the cloud consumer, as well as the limitations of the design. One of the benefits of using a commercial cloud-native solution like Microsoft Sentinel is that it can integrate different cloud or on-premises infrastructure elements under a single system. Although challenges persist, particularly in the public cloud, continued exploration and refinement of SIEM solutions would contribute to strengthening overall security measures and fostering the secure and resilient operation of cloud-based infrastructure. By applying log minimization techniques, the efficiency and cost of a cloud SIEM solution can be significantly improved, as the consumption cost depends on the amount of log data ingested. However, log minimization and event investigation require advanced cybersecurity skills, so cloud consumers should consider their level of expertise before deciding to handle security by themselves. In future work, we plan to extend the implementation with an identity access management component and apply the SIEM solution to a distributed Industrial IoT infrastructure scenario.

Author Contributions: Conceptualization, E.T. and T.C.B.; methodology, E.T. and T.C.B.; software, E.T.; validation, T.C.B.; investigation, E.T. and A.R.; supervision, T.C.B.; writing—original draft preparation, E.T.; writing—review and editing, P.A.C. and D.T.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available in [44].

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Cloud Security and Technology Maturity Survey | CSA. 2 March 2022. Available online: https://cloudsecurityalliance.org/artifacts/cloud-security-and-technology-maturity-survey (accessed on 11 May 2023).
2. Luxner, T. Cloud Computing Stats: Flexera 2023 State of the Cloud Report. Flexera Blog, 5 April 2023. Available online: https://www.flexera.com/blog/cloud/cloud-computing-trends-flexera-2023-state-of-the-cloud-report/ (accessed on 15 May 2023).
3. Kolevski, D.; Michael, K.; Abbas, R.; Freeman, M. Cloud Data Breach Disclosures: The Consumer and their Personally Identifiable Information (PII)? In Proceedings of the 2021 IEEE Conference on Norbert Wiener in the 21st Century, Chennai, India, 22–25 July 2021; pp. 1–9. [CrossRef]

4. Chen, D.; Chowdhury, M.; Latif, S. Data Breaches in Corporate Setting. In Proceedings of the 2021 International Conference on Electrical, Computer, Communications and Mechatronics Engineering (ICECCME), Mauritius, Mauritius, 7–8 October 2021. [CrossRef]
5. Bennasar, H.; Essaaidi, M.; Bendahmane, A.; Ben-Othman, J. A Systematic Literature Review of Cloud Computing Cybersecurity. *Adv. Dyn. Syst. Appl.* **2021**, *16*, 1883–1919. Available online: https://www.ripublication.com/Volume/adsav16n2.htm (accessed on 12 April 2023).
6. Shackleford, D. SANS 2022 Cloud Security Survey | SANS Institute. 15 March 2022. Available online: https://www.sans.org/white-papers/sans-2022-cloud-security-survey/ (accessed on 17 May 2023).
7. CloudPassage. Shared Responsibility Model Explained. Cloud Security Alliance, 26 August 2020. Available online: https://cloudsecurityalliance.org/blog/2020/08/26/shared-responsibility-model-explained/ (accessed on 17 May 2023).
8. Umesh Singh, K.; Sharma, A. Cloud Computing Security Framework Based on Shared Responsibility Models. In *Cyber-Physical, IoT, and Autonomous Systems in Industry 4.0*; CRC Press: Boca Raton, FL, USA, 2021; pp. 39–55. [CrossRef]
9. PCI Security Standards Council. PCI DSS Quick Reference Guide Understanding the Payment Card Industry Data Security Standard Version 3.2.1. 2018. Available online: https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf (accessed on 9 October 2023).
10. Yimam, D.; Fernandez, E.B. A survey of compliance issues in cloud computing. *J. Internet Serv. Appl.* **2016**, *7*, 5. [CrossRef]
11. Shah, A.; Banakar, V.; Shastri, S.; Wasserman, M.; Chidambaram, V. Analyzing the Impact of {GDPR} on Storage Systems. In Proceedings of the 11th USENIX Workshop on Hot Topics in Storage and File Systems (HotStorage 19), Renton, WA, USA, 8–9 July 2019.
12. ENISA. *Cybersecurity is a Shared Responsibility: 2018 European Cyber Security Month Kicks Off*; ENISA: Athens, Greece, 2018.
13. Liu, F.; Tong, J.; Mao, J.; Bohn, R.; Messina, J.; Badger, L.; Leaf, D. *NIST Cloud Computing Reference Architecture. Recommendations of the National Institute of Standards and Technology*; Special Publication 500-292; NIST: Gaithersburg, MD, USA, 2011. [CrossRef]
14. NIST. *Public Draft: The NIST Cybersecurity Framework 2.0*; NIST: Gaithersburg, MD, USA, 2023. [CrossRef]
15. Chronicle. Chronicle | Suite | Overview. Available online: https://chronicle.security/platform (accessed on 5 November 2023).
16. What is Microsoft Sentinel? 14 March 2023. Available online: https://docs.microsoft.com/en-us/azure/sentinel/overview (accessed on 13 May 2023).
17. Chauhan, M.; Shiaeles, S. An Analysis of Cloud Security Frameworks, Problems and Proposed Solutions. *Network* **2023**, *3*, 422–450. [CrossRef]
18. Bailey, E.; Becker, J. A Comparison of IT Governance and Control Frameworks in Cloud Computing. 2014. Available online: https://core.ac.uk/download/pdf/301361909.pdf (accessed on 5 November 2023).
19. ISO. ISO/IEC 27017:2015. 2015. Available online: https://www.iso.org/standard/43757.html (accessed on 9 November 2023).
20. ISO. ISO/IEC 27001 Standard—Information Security Management Systems. ISO, October 2022. Available online: https://www.iso.org/standard/27001 (accessed on 9 November 2023).
21. Microsoft. Azure Well-Architected Framework—Azure Well-Architected Framework. 28 March 2023. Available online: https://learn.microsoft.com/en-us/azure/well-architected/ (accessed on 30 October 2023).
22. Pavlik, J.; Komarek, A.; Sobeslav, V. Security information and event management in the cloud computing infrastructure. In Proceedings of the 2014 IEEE 15th International Symposium on Computational Intelligence and Informatics (CINTI), Budapest, Hungary, 19–21 November 2014; pp. 209–214. [CrossRef]
23. Lopez Velásquez, J.M.; Martínez Monterrubio, S.M.; Sánchez Crespo, L.E.; Garcia Rosado, D. Systematic review of SIEM technology: SIEM-SC birth. *Int. J. Inf. Secur.* **2023**, *22*, 691–711. [CrossRef]
24. Serckumecka, A.; Medeiros, I.; Bessani, A. Low-Cost Serverless SIEM in the Cloud. In Proceedings of the 2019 38th Symposium on Reliable Distributed Systems (SRDS), Lyon, France, 1–4 October 2019; pp. 381–3811. [CrossRef]
25. Lee, J.-H.; Kim, Y.S.; Kim, J.H.; Kim, I.K. Toward the SIEM architecture for cloud-based security services. In Proceedings of the 2017 IEEE Conference on Communications and Network Security (CNS), Las Vegas, NV, USA, 9–11 October 2017. [CrossRef]
26. Ghallab, A.; Saif, M.H.; Mohsen, A. Data Integrity and Security in Distributed Cloud Computing—A Review. In Proceedings of the International Conference on Recent Trends in Machine Learning, IoT, Smart Cities and Applications, Hyderabad, India, 29–30 March 2020; Springer: Singapore, 2020; pp. 767–784.
27. Kanwal, I.; Shafi, H.; Memon, S.; Shah, M.H. Cloud Computing Security Challenges: A Review. In *Cybersecurity, Privacy and Freedom Protection in the Connected World*; Springer: Cham, Switzerland, 2021; pp. 459–469. [CrossRef]
28. Alam, M.; Ihsan, A.; Khan, M.A.; Javaid, Q.; Khan, A.; Manzoor, J.; Akhundzada, A.; Khan, M.K.; Farooq, S. Correction: Optimizing SIEM Throughput on the Cloud Using Parallelization. *PLoS ONE* **2017**, *12*, e0171581. [CrossRef]
29. Garg, D.; Sidhu, J.; Rani, S. Improved TOPSIS: A multi-criteria decision making for research productivity in cloud security. *Comput. Stand. Interfaces* **2019**, *65*, 61–78. [CrossRef]
30. Rady, M.; Abdelkader, T.; Ismail, R. Integrity and Confidentiality in Cloud Outsourced Data. *Ain Shams Eng. J.* **2019**, *10*, 275–285. [CrossRef]
31. Attou, H.; Mohy-Eddine, M.; Guezzaz, A.; Benkirane, S.; Azrour, M.; Alabdultif, A.; Almusallam, N. Towards an Intelligent Intrusion Detection System to Detect Malicious Activities in Cloud Computing. *Appl. Sci.* **2023**, *13*, 9588. [CrossRef]
32. Pereira, F.; Crocker, P.; Leithardt, V.R. PADRES: Tool for PrivAcy, Data REgulation and Security. *SoftwareX* **2022**, *17*, 100895. [CrossRef]

33. Dimitra, G.A. Security Policies for Cloud Computing. Ph.D. Thesis, University of Piraeus, Piraeus, Greece, 2017.
34. Azure Virtual Network. January 2023. Available online: https://learn.microsoft.com/en-us/azure/virtual-network/virtual-networks-faq (accessed on 4 November 2023).
35. Orin-Thomas. Introduction to Azure Application Gateway—Training. Available online: https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-application-gateway (accessed on 17 May 2023).
36. Kumud, D. Azure Network Security Groups Overview. 16 March 2023. Available online: https://docs.microsoft.com/en-us/azure/virtual-network/network-security-groups-overview (accessed on 17 May 2023).
37. Kumud, D. Azure Application Security Groups Overview. 9 April 2023. Available online: https://docs.microsoft.com/en-us/azure/virtual-network/application-security-groups (accessed on 17 May 2023).
38. Overview of Log Analytics in Azure Monitor—Azure Monitor. 2 October 2022. Available online: https://docs.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-overview (accessed on 1 May 2023).
39. Azure Monitor Agent Overview—Azure Monitor. 3 May 2023. Available online: https://docs.microsoft.com/en-us/azure/azure-monitor/agents/azure-monitor-agent-overview? (accessed on 20 May 2023).
40. Detect Threats with Built-In Analytics Rules in Microsoft Sentinel. 22 June 2023. Available online: https://docs.microsoft.com/en-us/azure/sentinel/detect-threats-built-in (accessed on 28 June 2023).
41. About Microsoft Sentinel Content and Solutions. 22 June 2023. Available online: https://docs.microsoft.com/EN-US/azure/sentinel/sentinel-solutions (accessed on 30 June 2023).
42. Recent Phishing Attempts—My Experience and What to Look Out for. 20 December 2017. Available online: https://www.reddit.com/r/sysadmin/comments/7kyp0a/recent_phishing_attempts_my_experience_and_what/ (accessed on 17 June 2023).
43. Overview of the Microsoft Cloud Security Benchmark. 22 March 2023. Available online: https://learn.microsoft.com/en-us/security/benchmark/azure/overview (accessed on 13 May 2023).
44. Tuyishime, E.T. Deploying Microsoft Sentinel SIEM in Azure Virtual Networks | Microsoft Azure. 17 March 2023. Available online: https://github.com/Emmanuelt48/Azure-Virtual-Networks-with-SIEM.git (accessed on 5 November 2023).
45. Calderon, P.; Lyon, G. *Nmap 6: Network Exploration and Security Auditing Cookbook*; Packt Publishing Ltd.: Birmingham, UK, 2012; ISBN 9781849517485.

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.