GROUP ASSIGNMENT

NAME (TP NUMBER)	**:**	Androjuniko (TP081988) Tung Jean San (TP082276) Koo Wai Kit (TP081761)
INTAKE CODE	**:**	APUMF2406CYS
MODULE TITLE	**:**	Security Operations Centre and Incident Response (072024-JUL)
MODULE LECTURER	**:**	Dr. Julia Binti Juremi
PROJECT TITLE	**:**	Assignment 1 Section A (Research)
DATE ASSIGNED	**:**	16 July 2024
DATE COMPLETED	**:**	12 August 2024

Table of Contents

List of Figures

List of Tables

1.0 Introduction

As organisations grow, expanding their digital operations and integrating with various systems, applications and devices become an integral part of their business development plan. Consequently, it is crucial to manage and defend their increasingly complex systems and its data against cybersecurity threats and risks. However, as organisations scale, the increased complexity of systems will also lead to an increase in computer log data, which can be overwhelming if organisations do not have a dedicated and sophisticated log management tool. The National Institute of Standards and Technology (NIST, 2006) recommends organisations to utilise a Security Information and Event Management (SIEM) system to address this log management issue. By aggregating and consolidating all computer-generated log data and presenting them in real-time, a SIEM system plays an integral role within a Security Operations Center (SOC).

Generally, SIEMs are designed to collect, aggregate, store and correlate events based on log data generated from its connected data sources (González-Granadillo, González-Zarzosa & Diaz, 2021). These data sources range include intrusion detection systems (IDS), intrusion protection systems (IPS), antivirus programs and firewalls. The data is then correlated to provide a consolidated view, assist in managing threats, and generate security reports. While the core functionalities are common across different SIEM solutions, there are notable variations among the various SIEM solutions available in the market.

In this paper, three SIEM solutions are analysed and evaluated which are Microsoft Sentinel, IBM Security QRadar and Wazuh. An in-depth analysis of the SIEM solutions is provided on their key differentiators, functionality and operations, embedded technology, usability, cost-effectiveness, performance analysis and integration capabilities.

The rest of the paper is structured as follows: Section 2 introduces and analyses the Microsoft Sentinel, IBM Security QRadar and Wazuh SIEM solutions. Section 3 compares these three SIEM solutions and discusses their differences. Section 4 provides a prediction on the future technology of SIEM solutions. Finally, Section 5 presents a conclusion of the paper.

2.0 SIEM Solution Overview and Evaluation

2.1 Microsoft Sentinel

Microsoft Sentinel, launched in 2019, is a cloud-based Security Information and Event Management (SIEM) solution that combines SIEM and Security Orchestration, Automation and Response (SOAR) capabilities in one platform (Microsoft, 2024). It offers comprehensive cyberthreat detection, investigation, response and proactive threat hunting features, as well as natively integrates with Microsoft Azure services.

As a SIEM, Microsoft Sentinel collects and aggregates data from all sources, such as users, applications, servers and devices running on-premise or in any cloud environment. It then works to translate these data into an intelligible form, enabling users to analyse it effectively and respond to any incidents detected.

2.1.1 Key Differentiators

Cloud-Native Architecture. As a cloud-based SIEM, Microsoft Sentinel is designed to modernise traditional Security Operation Centres (SOCs) by enabling their users to access its SIEM capabilities without the need for on-premise infrastructure and maintenance (Microsoft, 2024). This also allows for Microsoft Sentinel to leverage its cloud platform to offer high flexibility and scalability. The platform is immensely scalable to handle massive amounts of data and analytics. It is also elastic to ensure optimum utilization of resources based on the demand at a given time.

Content Hub. The Content Hub in Microsoft Sentinel is a central repository that allows users to access, manage and deploy security content (Microsoft, 2024; Krishna, 2021). Users can customise and deploy out-of-the-box (OOTB) contents and solutions according to their specific requirements. The Content Hub offers a library of pre-built content provided by Microsoft and its partners, some of which includes:

- Analytics Rules: Predefined rules to detect and alert suspicious activities
- Workbooks: Pre-configured dashboards and visualisations
- Hunting Queries: Custom queries for threat hunting
- Playbooks: Automated workflows for responding to security incidents and alerts

The Content Hub enables a centralised and streamlined management of security content, allowing for rapid deployment and customisation of pre-built content, as well as efficient maintenance of an organisation's security monitoring and response capabilities.

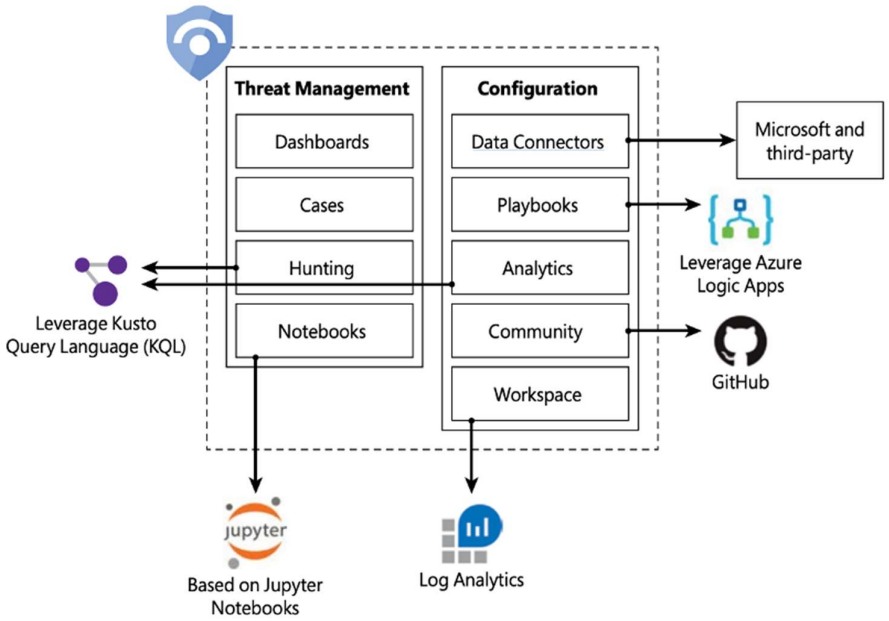
Integration with Microsoft Ecosystem. Microsoft Sentinel allows for seamless integration with the Microsoft ecosystem and products, which enhances its capabilities and provides a unified view, as well as a centralised security management and operation process. Some examples of integration with Microsoft solutions include the Microsoft 365 Defender, Azure Security Center, Azure Active Directory, Microsoft Defender for Cloud and Microsoft Graph Security API.

2.1.2 Functionality and Operations

Figure 1 below presents the major components of Microsoft Sentinel divided into two main categories, which is threat management and configuration. These components are further discussed below.

Figure 1.

The major components of Microsoft Sentinel.



Data Connectors. Data connectors are an essential component in Microsoft Sentinel that enables the integration of data sources into the SIEM (Microsoft, 2024). It supports a

wide range of connectors. This includes data sources from both Microsoft-native connectors and external non-Microsoft products, which can be connected via Syslog, Common Event Format (CEF) or REST APIs. Some examples of data sources supported by Microsoft Sentinel's data connectors are listed in Table 1 below (Diogenes, 2020).

Table 1.

Microsoft-native and external connectors supported by Microsoft Sentinel.

Supported Microsoft-native connectors	Supported external connectors
• Azure AD • Office 365 • Cloud App Security • Azure Activity Log • Azure AD Identity Protection • Azure Information Protection • Azure ATP • Azure Security Center • Domain Name Server • Microsoft Defender ATP • Microsoft Web Application Firewall • Windows Firewall • Windows Security Event	• Amazon Web Services (AWS) • Barracuda • Check Point • Palo Alto Networks • Fortinet • F5 • Symantec ICDX

For other data sources, logs can be collected as files using the Log Analytics custom log collection agent. After data is collected, the Advanced Security Information Model (ASIM) then normalises them into a consistent format (Microsoft, 2023). This allows for easier correlation and analysis across various data sources.

Playbooks. A playbook in Microsoft Sentinel is a set of automated response and remediation actions that can be executed as a routine (Microsoft, 2024). Playbooks can help to automate and orchestrate threat responses, integrate with both internal and external systems and can run automatically in response to alerts or incidents, as well as run manually when required. These playbooks are created using Azure Logic Apps, which helps to

automate and orchestrate tasks and workflows. This integration allows playbooks to leverage all the functions and features of Azure Logic Apps.

Analytics. Analytics in Microsoft Component is a core component that helps to detect, investigate and respond to security threats by analysing security data (Microsoft, 2024). The Content hub provides a library of pre-built analytics rules which are designed to detect threats and were created based on common threats and known attack vectors. Users can also choose to create custom analytics rules to address unique security requirements by using the analytics rule wizard function in Microsoft Sentinel. Analytics rules in Microsoft Sentinel uses the Kusto Query Language (KQL) to query and analyse data.

Community. The Microsoft Sentinel Community page at GitHub is a valuable resource for collaboration and sharing within the Microsoft Sentinel ecosystem (Diogenes, 2020). It serves as a platform where users can find, share, and collaborate on different Microsoft Sentinel components, and contains both official repositories and repositories contributed by community members. Examples of contributions include solutions, playbooks, workbooks, threat hunting queries, notebooks, analytic rules, and data connectors. This allows for efficient resource sharing, collaboration, customisation and provides opportunities to learn among Microsoft Sentinel users.

Workspace. A Log Analytics workspace is a central repository for collecting, analysing, and managing security data (Diogenes, 2020; Microsoft, 2024). It plays an important role in organising and optimising security operations. Users can monitor data using customised log tables as well as view workspace insights such as usage, performance, health, data ingestion, queries and change logs. Users can also design their Microsoft Sentinel workspace architecture depending on their requirements, such as creating a single or multiple workspaces based on any regulatory or compliance requirements. In addition, data access in the workspace is controlled by defining access controls using built-in or customised user roles.

Dashboards. Log Analytics dashboard provides data visualisation of the connected data sources, which allows users to find, correlate and share the operational data with their organisation (Microsoft, 2023). It provides a centralised view of the organisation's security posture, and helps to interpret complex data through graphical representation. Users can either use pre-built templates, or create and customise a graphical view of their log queries

using Log Analytics, then pin the graph to the dashboard. The dashboard also enables real-time data monitoring, data aggregation and interactive data exploration.

Cases. Microsoft Sentinel provides a comprehensive case management platform for handling security incidents by aggregating all relevant evidence such as alerts, entities, insights and logs, which are referred to as a "case" (Diogenes, 2020; Microsoft, 2023). Some key features provided by Microsoft Sentinel's case management system includes incident creation and tracking, standardisation and task management, audit and activity tools, incident timelines and entity examination. These features enhance the efficiency and effectiveness of SOC operations by providing a streamlined process and detailed insights.

Threat Hunting. Microsoft Sentinel offers a robust set of tools for proactive threat hunting by using powerful search and query capabilities across the organisation's data sources (Microsoft, 2024). These hunting queries, which are built in Kusto Query Language (KQL), aid in detecting anomalies that might otherwise not be captured by existing security applications or predefined analytics rules.

Notebooks. Jupyter notebooks enhance Microsoft Sentinel's capabilities by combining extensive programmability and library support for machine learning, visualisation and data analysis (Diogenes, 2020; Microsoft, 2024). It enables advanced analytics beyond Microsoft Sentinel's built-in features, custom visualisations such as unique timelines and process trees as well as integration of external data sources outside of Microsoft Sentinel. This allows security analysts to perform in-depth investigations and develop more sophisticated threat detection methods.

2.1.3 Embedded Technologies

Security Orchestration, Automation and Response (SOAR). As a platform that combines SIEM and SOAR capabilities, Microsoft Sentinel allows user to automate repetitive tasks related to incident enrichment, response and remediation (Microsoft, 2024). Playbooks can be utilised for advanced automation in handling incidents and alerts by running automated threat response to specific alerts or incidents. The SOAR functionalities enhance SOC efficiency by automating routine tasks and allowing SOC teams to focus on more complex threat investigations.

User and Entity Behaviour Analytics (UEBA). Microsoft Sentinel's UEBA feature enhances threat detection and investigation by leveraging behavioural analytics (Microsoft, 2024). It involves behavioural profiling which collects and analyses logs to build baseline profiles for entities. This profiling establishes a normal behaviour for each entity. By using machine learning algorithms, Microsoft Sentinel monitors ongoing activities and detects anomalies that deviate from the established baselines. Activities are scored based on their deviation from their normal behaviour, with higher scores indicating greater anomalies. The UEBA feature improves the efficiency of threat detection and investigation by automating the process, thus allowing SOC teams to focus on more complex and critical threats.

Kusto Query Language (KQL). KQL is the primary tool for analysing and manipulating data within Microsoft Sentinel (Microsoft, 2023). This includes data from external sources, data generated by Microsoft Sentinel such as alerts and incidents, as well as additional data such as threat intelligence feeds. KQL is used in Microsoft Sentinel for data visualisation, creating custom queries for threat detection, and analysing security events. KQL is also optimised for handling large datasets with high efficiency, which is important for SOCs where real-time analysis and quick response time is required. Hence, KQL can help users to uncover insights and respond to threats effectively.

2.1.4 Usability

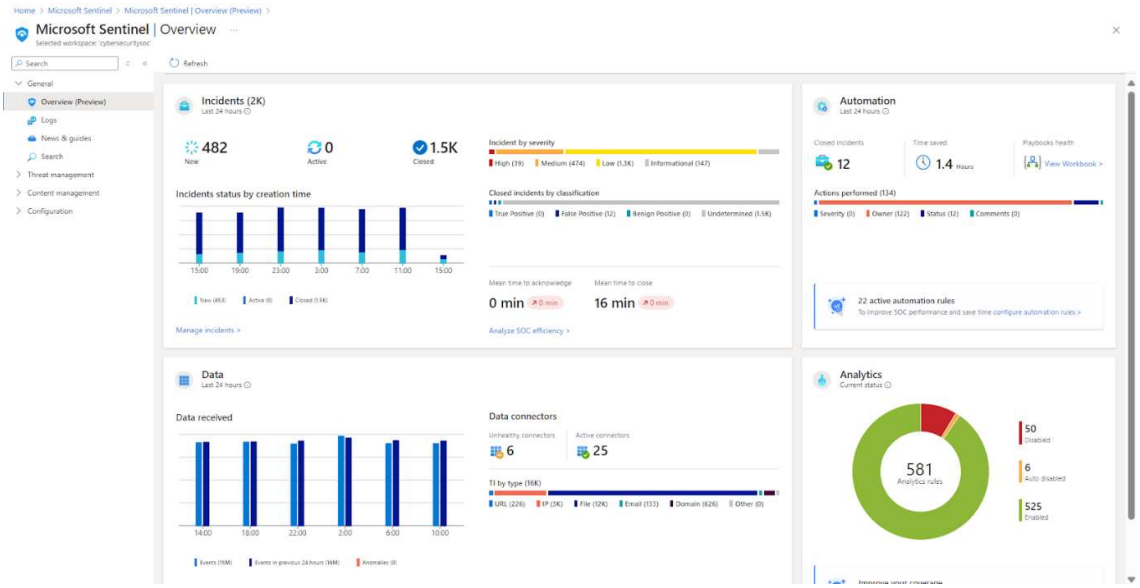
Ease of Deployment. As a cloud-native SIEM, Microsoft Sentinel was designed for easy setup management by users with basic IT knowledge (Cloud Direct, n.d.). In contrast, traditional on-premise SIEM solutions are more complex and require a high level of expertise to deploy. Hence, this helps reduce deployment costs and time. Organisations can quickly implement and customise Microsoft Sentinel without the need for hardware installation or manual maintenance, thanks to its scalable cloud resources. They can also utilise the prebuilt content from Microsoft Sentinel to reduce deployment time and effort. In a study conducted by Forrester (2023), the reduction in configuration and deployment time of the new connections was reduced by 93%.

Dashboards for Data Visualisation. The overview dashboard displayed in Figure X allows users to view, monitor and analyse activities across all connected data sources (Microsoft, 2024). Examples of information that can be viewed in the dashboard include incident data, automation data, analytics data, as well as the status of data records, data

collectors and threat intelligence. The instant data visualisation in the form of dashboards allow users to efficiently monitor the security data within the organisation in real-time and gain valuable insights of the security of the organisation. Additionally, organisations can also define roles and permissions to control who can access and view the information in the Overview dashboard.

Figure 2.

Overview dashboard in Microsoft Sentinel



User Experience. A study conducted by Forrester (2023) found that Microsoft Sentinel's user-friendly interface allows organisations to employ staff without requiring highly specialised expertise. The automation of complex processes enabled users with general IT knowledge to utilise the SIEM effectively in threat detection and response. Furthermore, Wafula (2021) shared that Microsoft Sentinel is designed with accessibility in mind in compliance with the Web Content Accessibility Guidelines (WCAG). In addition, it also provides responsive design, allowing for users to navigate the SIEM portal portably via mobile phones.

2.1.5 Cost-Effectiveness

Pricing Model. There are no upfront costs required when setting up Microsoft Sentinel (Microsoft, n.d.). Instead, Microsoft Sentinel's pricing is based on the amount of

data analysed and stored in Azure Monitor Log Analytics workspace. Two payment options are offered, which are the Pay-As-You-Go and Commitment Tiers.

Under the Pay-As-You-Go model, charges are incurred based on the amount of data ingested for security analysis and stored in the Azure Monitor Log Analytics workspace. The price under this model is charged at $5.59 per GB of data.

Users who opt for Commitment Tiers have to pay a fixed fee depending on the chosen tier, which allows for a more predictable cost. The tiers are offered at a discounted rate compared to the Pay-As-You-Go pricing, with a lower price per GB for every higher commitment tier. For instance, the 100 GB per day tier is charged at $3.85 per GB, while the 300 GB per day tier is charged at $3.47 per GB.

Cost Savings. A study conducted by Forrester (2023) examined the cost savings of Microsoft Sentinel and found the following benefits of implementing Microsoft Sentinel compared to traditional on-premise SIEM solutions:

- $5.1 million saved on the cost of operation from traditional on-premise SIEM expenses related to licensing, storage, and infrastructure
- $1.5 million saved through enhanced SOC team efficiency
- $1.1 million saved due to improved management efficiencies
- $618,300 saved from the reduced time needed to deploy and configure Microsoft Sentinel
- $2.8 million saved by mitigating and reducing the impacts of security breaches

Overall, Forrester (2023) concluded that organisations adopting Microsoft Sentinel saw a 44% reduction of total cost of ownership and a 234% return of investment.

2.1.6 Performance Analysis

Through 2022 to 2024, Microsoft Sentinel has been consistently acknowledged by Gartner as a Leader in the Gartner Magic Quadrant for SIEM (Lefferts, 2024). In addition, Forrester Research has also named Microsoft Azure as a Leader in the Forrester Wave report on SIEM solutions (Microsoft, 2020). These industry recognitions are a testament to the advanced performance capabilities, effectiveness and overall impact of Microsoft Sentinel on the SIEM landscape.

According to Cloud Direct (n.d.), modern cloud-native SIEM systems such as Microsoft Sentinel offers real-time threat detection with reduced bandwidth overhead and increased processing power as compared to traditional on-premise SEM systems. Logs are analysed immediately as soon as they are ingested into the SIEM. As Microsoft Sentinel operates on the cloud and automatically scales, the process of log collection does not impact its speed in querying and correlating data.

2.1.7 Integration Capabilities

Native Integration with Microsoft Products. As a Microsoft SIEM product, Microsoft Sentinel is tightly integrated with other Microsoft security solutions such as Microsoft 365 Defender and Microsoft Defender (Mudaliar, 2021). This integration offers a unified approach in managing risks across the entire digital environment from a single platform. It delivers a cohesive view of the organisation's security by allowing for sharing of incidents, schemas and alerts between Microsoft Sentinel and Microsoft 365 Defender.

In addition, Microsoft Sentinel also seamlessly integrates with other Microsoft Azure services, allowing organisations to fully leverage their existing cloud infrastructure (Rawat, 2024). Microsoft Sentinel is able to ingest data from Azure services such as Azure Security Center, Azure Active Directory, Azure Firewall, and Azure Virtual Machines. This integration enhances visibility and improves threat detection ability throughout the organisation's Azure environment.

Integration with Third-Party Solutions. Aside from Microsoft-native products, Microsoft Sentinel is also able to effectively integrate with a variety of other cloud platforms including Amazon Web Services (AWS) and Google Cloud, as well as other on-premise infrastructure, third-party security tools such as firewalls, intrusion detection systems, and other software as a service (SaaS) applications (Mudaliar, 2021). Users are able to leverage pre-built data connectors from the Content Hub to integrate with popular third-party solutions, thus simplifying the integration process (Microsoft, 2024).

For other less common systems, Microsoft Sentinel supports the ability to create custom connectors (Microsoft, 2024). The custom connectors are built using APIs provided by the data source and connected via Microsoft Sentinel's REST APIs. This allows for Microsoft Sentinel to integrate with third-party tools that do not have native support in Microsoft Sentinel, which can include integration with other custom or proprietary SIEM

systems and log aggregation tools. Thus, organisations are able to leverage Microsoft Sentinel's flexibility to tailor their security data collection based on their specific requirements and scenarios.

Cyber Threat Intelligence (CTI). CTI involves gathering and analysing information about current or potential cyber security threats (Microsoft, 2024). Threat indicators, also called Indicators of Compromise (IoC) or Indicators of Attack (IoA) are a common form of CTI in SIEM systems. These indicators include URLs, file hashes and IP addresses, and can help detect and respond to threats such as phishing and malware. In Microsoft Sentinel, organisations can integrate CTI by enabling data connectors to various threat intelligence platforms and feeds, manage them through logs and use analytics rules to generate alerts. Users can leverage threat indicators from Microsoft's threat intelligence by enabling the Microsoft Intelligence Analytics rule. Additionally, users can also connect to other threat intelligence feeds such as the Accenture Cyber Threat Intelligence, Cybersixgill Darkfeed, Cyware Threat Intelligence eXchange (CTIX) and ESET, IBM X-Force, and many more (Microsoft, 2024).

2.2 IBM Security QRadar SIEM

IBM Security QRadar SIEM is a powerful, and commercially available SIEM solution designed by IBM. It features cutting-edge threat detection and incident response capabilities, leveraging machine learning and behavioural analytics to pinpoint unusual activities (Šuškalo et al., 2023). Being a commercial product, QRadar SIEM operates on proprietary software and follows a licensing model, which allows IBM to restrict access to their source code. Šuškalo (2023) also states that QRadar SIEM is designed as a modular architecture, allowing it to provide visibility across the IT infrastructure. Additionally, the platform is also scalable to meet the varying demands of its end users.

2.2.1 Key Differentiators

IBM QRadar SIEM stands out for its advanced threat detection and incident response capabilities, utilising multiple layers of AI and automation to enhance threat prioritisation, alert enrichment, and incident correlation. These features enable QRadar SIEM to consolidate related alerts cohesively into a single, cohesive dashboard, thereby reducing unnecessary noise and helping security analysts save crucial time (IBM, n.d.). It can integrate well with IBM Security SOAR (Security Orchestration, Automation, and Response) to automate

incident response workflow, which helps to reduce the time in responding to threats and minimise the impact of security incidents.

In addition, QRadar SIEM excels in comprehensive log management, as it offers in-depth visibility into user, network, and application activities (IBM, n.d.). It compiles security-relevant data from multiple sources and contextualises this information to present a complete view of the security environment. Its advanced User Behaviour Analytics (UBA) enhances this visibility further by effectively identifying insider threats and unusual behaviour by performing detailed analysis of user activities (SelectHub, 2024).

Furthermore, QRadar SIEM offers robust compliance management capabilities, featuring a comprehensive set of reporting templates designed to assist organisations in meeting both operational and regulatory requirements (IBM, n.d.). These templates can streamline the process of adhering to various industry standards, making regulatory compliance more accessible and efficient. Lastly, integration is another key strength of QRadar SIEM. According to IBM (n.d.), the platform supports over 700 integrations and extensions provided by partners, which covers different aspects of cybersecurity, such as cloud security and endpoint security.

2.2.2 Functionality and Operations

IBM Security QRadar SIEM is designed to deliver robust and versatile functionality to meet the diverse needs of modern security environments. According to IBM (2019), this comprehensive platform unifies log management SIEM, vulnerability management, network analysis, threat intelligence, user behaviour analytics, and AI-driven investigations into a single system, all managed through one centralised interface (IBM, 2019).

The following subsections will delve into the specific operational aspects of QRadar SIEM, highlighting its core functionalities and how they contribute to a more secure and manageable IT infrastructure.

Data collection and integration. QRadar SIEM efficiently gathers logs and network flow data from a wide array of sources, which includes network devices, servers, applications, and cloud platforms. With support for over 450 pre-configured Device Support Modules (DSMs), it ensures seamless integration with various commercial technologies (IBM, 2019).

Data parsing and normalisation. After the data is collected, QRadar SIEM processes and standardises it into a uniform format (IBM, 2019). This involves recognising the type of log source and applying the relevant DSM to organize the data for analysis. This normalisation is essential for effective correlation and evaluation of security events.

Real-time threat detection and incident prioritisation. QRadar SIEM utilises near real-time automated security intelligence to identify and prioritise threats (IBM, n.d.). It employs advanced analytics and AI to correlate related security events into a single incident, and prioritises the incidents based on their severity and impact. This helps the security team to act quickly against emerging threats and focus their efforts on critical issues.

User Behaviour Analytics (UBA). QRadar SIEM features sophisticated User Behaviour Analytics (UBA) to detect insider threats and unusual activities (IBM, n.d.). By analysing user behaviour and identifying deviations from normal patterns, it can flag potential security concerns that might otherwise be overlooked.

Threat intelligence integration. QRadar SIEM integrates with various threat intelligence feeds, including IBM X-Force Threat Intelligence, which allows the system to stay updated with the latest threat data (IBM, 2019). This integration enhances its ability to recognise and respond to emerging and evolving threats.

Automated response. QRadar SIEM supports automation of routine tasks and integration with other security tools for efficient incident response. For example, its integration with IBM Security SOAR allows the automation of incident response workflows. This can reduce response times and lessen the impact of security incidents.

Compliance management. QRadar simplifies compliance management with extensive reports and rule templates designed to meet operational and regulatory needs (IBM, 2019). It also provides default setting compliance packages for multiple regulations like the General Data Protection Regulation (GDPR). The system's automated data handling and reporting features facilitate adherence to various industry standards.

Customisable dashboards and reports. The platform offers highly customisable dashboards and reporting options, allowing security teams to tailor the interface to their specific requirements (IBM, n.d.). Some customisations that can be made include adding, removing, and moving dashboard items.

2.2.3 Embedded Technologies

Components of QRadar SIEM. According to Šuškalo (2023), QRadar SIEM's architecture comprises several key components. Firstly, Event and Flow Processors are responsible for gathering raw data from sources such as network devices, applications, servers, and endpoints. This data is processed and stored in distributed Data Nodes, which ensure high availability and minimise latency. Event and Flow Collectors retrieve data from intermediary devices via SPAN (Switchport Analyzer) ports and forward it to the Processors. The QRadar Console serves as the main interface for managing and monitoring events, while the QRadar Risk and Vulnerability Manager assists in visualising network topology and identifying vulnerabilities and misconfigurations. The platform also includes an App Framework that supports the integration of third-party applications and extensions.

Comprehensive centralised visibility. QRadar SIEM provides centralised visibility by collecting, parsing, and normalizing log and flow data from across the enterprise (IBM, 2019). There are over 450 pre-built Device Support Modules (DSMs), and the platform integrates seamlessly with a range of commercial solutions, automatically detecting log sources and applying the correct DSM for rapid deployment. QRadar SIEM also features a DSM Editor with an easy-to-use GUI, allowing security teams to easily customise log parsing for unique applications. Additionally, the platform automatically identifies and classifies network assets by analysing network flow data, helping the organisation to establish a foundation of an accurate asset database. Once data is centralized, QRadar SIEM performs automated analysis to detect known threats, anomalies, and critical risks, offering thorough insight into enterprise-wide activities.

Automation of security intelligence for swift threat detection. QRadar SIEM automates security intelligence by analysing and correlating data from multiple sources, which include logs, events, and network flows, to detect both known and unknown threats (IBM, 2019). It comes with hundreds of pre-built use cases, correlation policies, and anomaly detection algorithms that help identify and prioritise security threats. When a threat is detected, related events are aggregated into single, prioritized alerts called "offenses". The system will automatically prioritise the offenses based on their threat level and the significance of the compromised assets. Each offense presents a complete chain of threat activity on a single screen, allowing security analysts to investigate, assign, or resolve incidents efficiently. The offenses will be updated in real-time when new related activities are

detected, giving analysts an up-to-date view of critical threats and reducing overall alert volume.

Detection of unusual network, user, and application behaviour. QRadar SIEM offers a range of advanced anomaly detection capabilities to identify unusual behaviour that could indicate an unknown threat (IBM, 2019). Its unique ability to monitor and analyse Layer 7 application traffic enhances its effectiveness in detecting anomalies that other SIEM solutions might overlook. There is an option to use QRadar Network Insights as part of the deployment, which allows organisations to track interactions between systems, applications, and data exchanges. This provides a deeper visibility into the network behaviour. By correlating these insights with other data sources, security analysts can detect suspicious activities such as compromised hosts or data exfiltration. QRadar SIEM also includes several anomaly detection rules by default and allows security teams to create custom rules and settings. Moreover, the security team is able to install more than 160 additional pre-built apps available in the IBM Security App Exchange to enhance their monitoring capabilities.

Seamlessly scale to meet evolving requirements. QRadar SIEM is designed with a modular architecture which consists of several components. These components are available as hardware, software, or virtual appliances, and can be deployed on-premises, in IaaS environments, or across hybrid setups (IBM, 2019). The solution supports scalability by allowing organisations to add high availability and disaster recovery features as needed. In addition, QRadar SIEM provides integrated failover and full-disk synchronisation to ensure continuous operation, eliminating the need for third-party fault management tools. Additionally, it offers disaster recovery capabilities by enabling the transfer of live data, such as events and flows, from a primary system to a secondary one at a different location for enhanced data protection and recovery.

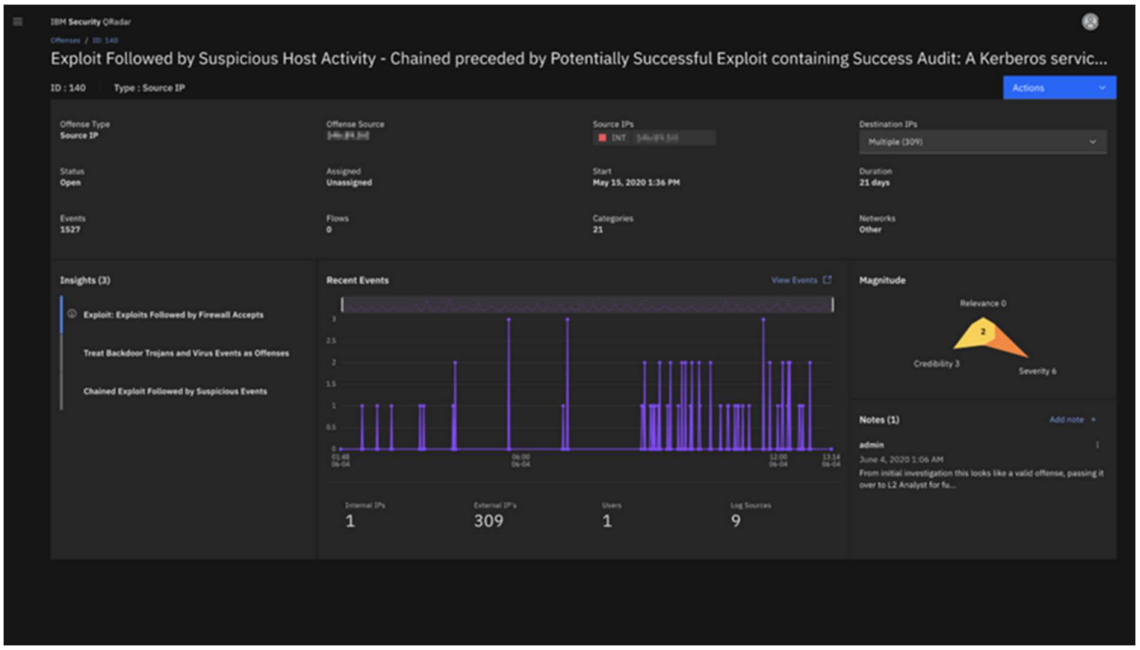
2.2.4 Usability

QRadar SIEM is known to have a steep learning curve, and its user interface may be too complex for smaller teams or beginners to use (Miguel, 2023). Miguel also states that users can customise the dashboard, but system knowledge is essential for optimal setup (2023). The dashboards and reports are highly customisable to fit diverse operational needs, in which they can be tailored to display the most relevant data, helping analysts focus on

critical information. An example of a report created by QRadar SIEM is illustrated in Figure 3 below.

Figure 3.

QRadar SIEM's detailed report on suspicious host activity.



Additionally, it supports over 700 integrations and extensions, enabling seamless interoperability with existing tools and providing a unified security view (IBM, n.d.). Its flexible deployment options cater to various organisational needs, and the platform is designed to scale with organisational needs without sacrificing performance.

To navigate the complexities of the platform, IBM provides extensive training and support to help users grasp the platform capabilities, which comes in the form of documentation, online courses, and community forums. These resources are beneficial in overcoming the usability challenges, enabling users to maximise the platform's potential.

2.2.5 Cost-Effectiveness

The cost-effectiveness of QRadar SIEM is influenced by several factors, including the size of the organisation, the complexity of its IT infrastructure, the specific use cases, and the chosen deployment model.

Pricing structure. QRadar SIEM provides adaptable pricing structures to fit various organisational requirements (IBM, n.d.):

1. **The Usage Model**: This model charges based on the volume of log events processed per second (EPS) and network communications per minute (FPM). It is particularly suitable for organisations that need to handle large volumes of data, as it aligns with their specific data management requirements.
2. **The Enterprise Model**: This model is based on the count of Managed Virtual Servers (MVS) utilized, which is determined based on the quantity of physical, virtual, and cloud servers within the environment. It offers the capacity to ingest unlimited log events and network behaviour, providing flexibility and scalability for large-scale deployments.
3. **The Licensing Model**: For on-premises deployments, QRadar SIEM offers both subscription and perpetual licensing options. In contrast, SaaS deployments are available solely through a subscription model, providing a range of choices to suit different organisational needs and preferences.

Flexible Deployment Options and Cost Transparency. The organisation can choose from different deployment options, including on-premises, cloud, and hybrid models. This flexibility allows organisations to choose the most cost-effective deployment strategy based on their infrastructure and budget. In addition, QRadar SIEM avoids hidden fees by not imposing limits on log and daily index volumes, providing organisations with clearer budgeting and reducing the likelihood of unexpected costs (IBM, n.d.).

Managed Services and Efficiency Gains. IBM X-Force Threat Management Services provide managed services for QRadar SIEM. This option combines advanced tools with skilled security analysts and threat hunters, offering a budget-friendly way to boost security without extensive in-house resources (IBM, n.d.). Furthermore, QRadar SIEM utilises AI and automation to lessen the manual workload for security analysts, resulting in significant cost savings by enhancing the efficiency of security operations and reducing time spent on routine tasks.

Integrations and Compliance Support. The 700 pre-built integrations provided allows seamless connection with existing security tools and data sources, which maximises the value of current investments and reduces the need for additional tools. Additionally, the

platform features comprehensive reporting templates to address various compliance needs, which helps in streamlining compliance management and contributing to further cost savings. Apart from the paid version, IBM also offers a completely free QRadar Community Edition, which is tailored for learning and experiencing QRadar's latest features. It includes a few features of the full version but is intended for smaller environments.

Cost Estimates and Financial Impact. A rough estimated price of an organisation with 3000 employees and 300 servers for the software version of QRadar SIEM will incur an estimated monthly cost in the range of USD 2680 to USD 3910 (IBM, n.d.). A Forrester Total Economic Impact study indicates that QRadar SIEM offers a 239% ROI, with total benefits amounting to $6.1 million over three years, compared to costs of $1.8 million (Forrester, 2023). The study also highlights a net present value (NPV) of $4.3 million, reflecting the substantial financial advantages of implementing QRadar SIEM. This study highlights the financial benefits of implementing QRadar SIEM as a security solution.

2.2.6 Performance Analysis

According to IBM (n.d.), QRadar SIEM is capable of handling high data volumes, with the ability to process thousands of events per second, ensuring efficient real-time log data processing. Additionally, it supports substantial rates of network flow data ingestion, measured in flows per minute, which is essential for effective network activity monitoring.

QRadar SIEM employs real-time, automated security intelligence to swiftly detect and prioritise threats, allowing security teams to respond promptly to new threats (IBM, 2019). Its correlation engine is capable of managing billions of events and flows, streamlining them into a smaller set of prioritised offenses based on their impact on the business. The platform uses AI and machine learning to prioritise incidents according to their severity and potential impact, helping analysts allocate their resources and time more effectively.

In addition, it has consistently received high recognition in industry benchmarks, such as being named a Leader in the Gartner Magic Quadrant for SIEM (IBM, 2019). The solution's integration with IBM Security SOAR automates incident response workflows, decreasing manual effort and facilitating faster remediation.

Test-case scenarios. Its performance can be observed from a research paper evaluating the performance of the QRadar system, where several test scenarios were conducted to assess its effectiveness in monitoring and detecting security events (Šuškalo, 2023). The experiments involved setting up a virtualised network environment with multiple virtual machines and a firewall, with a QRadar system installed to collect and analyse log data. The test scenarios included monitoring user activities, detecting brute-force attacks on remote access and Outlook Web Access services, scanning for vulnerabilities on the Apache web service, and identifying malicious attempts to access the network firewall.

The test results showed that QRadar SIEM successfully detected user login activities, password changes, and modifications to user accounts. It also effectively identified brute force attempts on the SSL VPN and attacks on the Outlook Web Access (OWA) service, generating appropriate chained violations. While the Apache web service scanner was detected, it did not trigger a violation due to its scanning nature. Lastly, QRadar SIEM flagged numerous unsuccessful SSH access attempts to the Fortigate firewall, producing multiple alerts for immediate investigation. These test scenarios confirm QRadar SIEM's proficiency in detecting and responding to various security events.

2.2.7 Integration Capabilities

Extensive Pre-Built Integrations and Partner Extensions. QRadar SIEM is highly regarded for its robust integration capabilities, which significantly enhance its functionality and cost-effectiveness. It comes equipped with over 700 pre-built integrations and partner extensions, enabling seamless integration with a wide array of security tools and data sources (IBM, 2019). These integrations include essential connections with cloud security providers like AWS, Google Cloud, and Microsoft Azure, as well as endpoint security solutions from companies such as Trend Micro and Palo Alto Networks (IBM, n.d.). Additionally, network security tools like Check Point and Cisco are integrated to provide comprehensive visibility into network traffic and potential threats.

Seamless Integration with IBM Security Products. Furthermore, QRadar SIEM integrates effortlessly with various IBM security products, creating a unified and cohesive security ecosystem. According to IBM (n.d.), the key integrations are IBM Security SOAR, which automates incident response workflows to facilitate and streamline the response to security incidents, and IBM X-Force Threat Intelligence, which enhances threat detection by

providing access to global threat intelligence. Moreover, the platform's support for open-source sigma rules allows the adoption of community-driven detection rules for identifying emerging threats. Apart from that, it can integrate well with a variety of compliance and reporting tools, making the generation of compliance reports more straightforward and efficient.

Custom Integration Capabilities via API Support. Additionally, QRadar provides extensive API support that allows organisations to extend the platform's capabilities through custom integrations (Miguel, 2023). This API support enables data ingestion from custom sources, ensuring comprehensive visibility across all relevant security data. The API allows for the creation of tailored workflows and automation scripts, increasing the flexibility and efficiency of security operations.

Additional Resources through IBM's App Exchange. Another key feature would be IBM's App Exchange, which serves as a marketplace for further integrations and extensions, providing organisations with additional resources to customise and enhance their QRadar deployments (IBM, 2019). QRadar SIEM's components are completely integrated, ensuring that it can scale effectively with organisational growth and evolving security needs.

2.3 Wazuh

Wazuh is an open-source SIEM solution which is able to detect threats, monitor file integrity, send incident response alerts, and manage compliance based on established standards. It was initially part of OSSEC (Open Source Security Event Correlator) which was a popular intrusion detection system in 2004, founded by Daniel Cid. OSSEC was synonymous with log analysis, maintaining file integrity, and compliance monitoring. Nonetheless, Wazuh's developers had a higher ambition to further improve on its functionality, scalability, and integration, which led to the founding of Wazuh in 2015.

Prior to its founding, Wazuh began as a project with the aim to enhance upon the basic OSSEC functionality by integrating with the ELK (Elasticsearch, Logstash, and Kibana) stack which made complex visualisation of data, real-time data processing, and more manageable security events possible. Over the years, Wazuh transformed into a robust SIEM solution with capabilities such as the detection of threats and vulnerability, real-time monitoring and alerts, as well as integration with cloud services such as AWS, Google Cloud, and Microsoft Azure. Today it is popular among SMEs and even large organisations across

different industries. It is the go-to choice for a cost-effective and flexible solution for SIEM-related requirements.

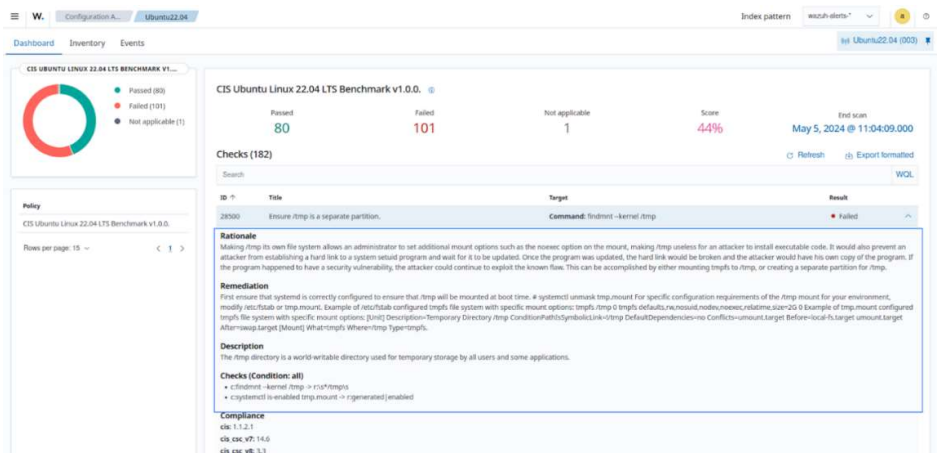
2.3.1 Key Differentiators

Configuration Assessment. In addition to system monitoring, Wazuh also keeps track of various configuration settings, ensuring that they are in accordance with the user's security standards. Periodic scans are also carried out to identify any misconfigurations or vulnerabilities that threat actors can exploit. On top of that, customisations are available, allowing maximum flexibility for users to use Wazuh according to the organisation's requirements (Wazuh, 2024).

IT Hygiene. Wazuh automates the up-to-date record of inventory of all endpoints that are under Wazuh's surveillance, such as installed applications, running processes, operating system information, and many more. This information allows users to effectively maintain and improve asset visibility and uphold IT hygiene. This can be further enhanced with other Wazuh's features such as vulnerability detection and malware detection to safeguard endpoints. Furthermore, the Server Configuration Assessment module from Wazuh scans the monitored devices on a regular basis based on the CIS (Center for Internet Security) benchmark to detect any misconfigurations or flaws. In the report generated from the SCA scan, users can get a general overview of how many devices that have passed or failed the scan, the overall score of the scan, as well as other indicators such as rationale, remediation steps, and the description that can be improved (Wazuh, 2024).

Figure 4.

CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0.



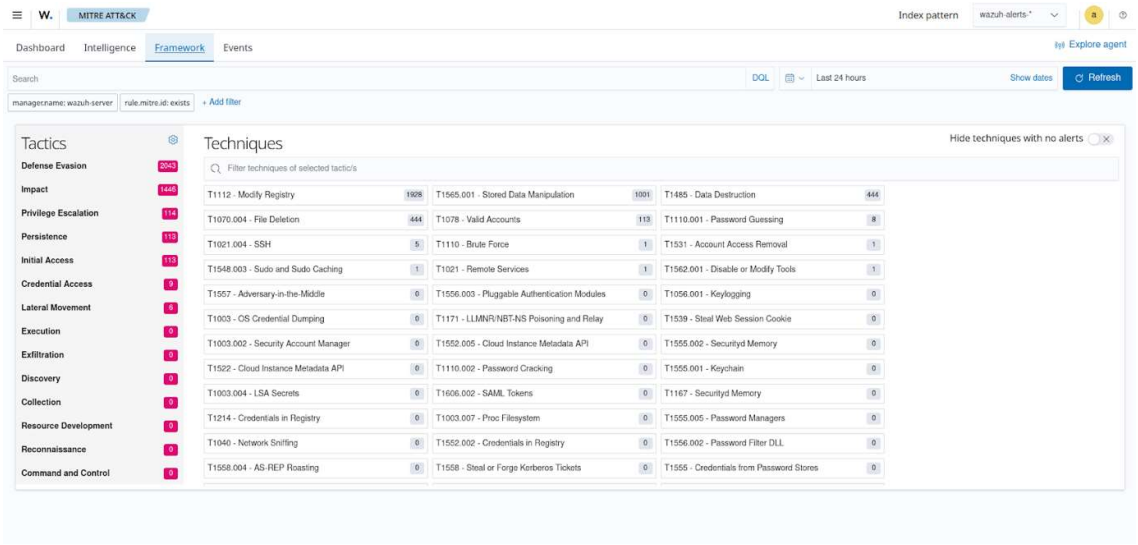
2.3.2 Functionality and Operations

Threat Hunting. Wazuh allows log retention, indexing, and the ability to query which can come in handy when investigating threats that have bypassed the security measures put in place. Additionally, the threat detection rules are based on the MITRE ATT&CK framework which helps in the identification of attack techniques that are known to be used by threat actors (Wazuh, 2024).

Wazuh's integration with the MITRE ATT&CK module assigns attack tactics, techniques, and procedures (TTPs) to generated events so that patterns in the threat actor's behaviour can be tracked. For instance, credential stuffing in MITRE ATT&CK's framework can be demonstrated by a suspicious login attempt. With this, users are equipped with the ability to analyse the number of such attacks and enforce the required security measures to minimise risks. The MITRE ATT&CK module along with the TTP mapping is shown on Wazuh's dashboard, as can be seen in Figure 5 below.

Figure 5.

MITRE ATT&CK's module on Wazuh's Dashboard.



File Integrity Monitoring (FIM). Wazuh constantly performs monitoring against the system files, recognising any content changes, permissions, as well as ownership that is essential to observe. Wazuh's documentation shows some general use cases where it can help with monitoring:

- **Real-time monitoring**: The “realtime” attribute from the FIM module allows continuous monitoring, which can also be set especially for selected directories.
- **Scheduled monitoring**: Using the “frequency” option, users can customise the schedule of file integrity monitoring in advance. The scan interval that comes in default is 12 hours and can be configured differently on every endpoint. In addition, the scans can be further customised through the use of “scan_time” and “scan_day” options which allow scanning outside of business hours.
- **Who-data monitoring**: Wazuh can obtain advanced insights after the monitoring thanks to the function of who-data. It takes advantage of auditing tools such as Microsoft Windows SACL to decide which information is important about any file changes that have been found. It summarises the data about when the change took place, what or who did the change, and what was changed, all of which are required to preserve integrity and accountability in the file structure.

Log Data Analysis. Wazuh’s log data analysis gathers, analyses, and keeps logs from various sources such as endpoints, devices connected to the network, and applications. Furthermore, logs can be sent by users to Wazuh’s server through syslog or third-party integrations. The following are the several commonly supported log sources by Wazuh:

- **Operating System Logs**: Wazuh collects several operating systems’ logs such as Linux, Windows, and MacOS. On Windows, the logs are collected through Windows’s event channel and event log format. On MacOS, Wazuh uses the Unified Logging System, or ULS, to gather the logs.
- **Syslog Events**: Logs are gathered from devices where syslog is enabled, which covers a wide range of sources including Linux or Unix-based systems and devices that have no support for agent installation.
- **Custom Logs**: Users can customise Wazuh so that it can collect and analyse logs from a series of applications and third-party security solutions such as VirusTotal and Windows Defender.

Rules and Decoders. Wazuh’s decoders play a role in converting the raw logs that are based on different formats into a combined and organised form so that effective processing by Wazuh can be made possible. In addition, users are given the choice to set custom decoders for analysing logs from chosen applications or network devices with

distinctive log formats. Through the use of decoders, Wazuh can interpret logs and present relevant information like timestamps, source IP addresses, usernames, and many more.

Wazuh's ruleset notifies about security events and anomalies from the gathered logs. The rules are based on specific conditions and alarms can be triggered when those conditions are met. Users can develop their own custom rules to suit their particular environment and security needs, on top of an extensive choice of pre-built rules on general security use cases.

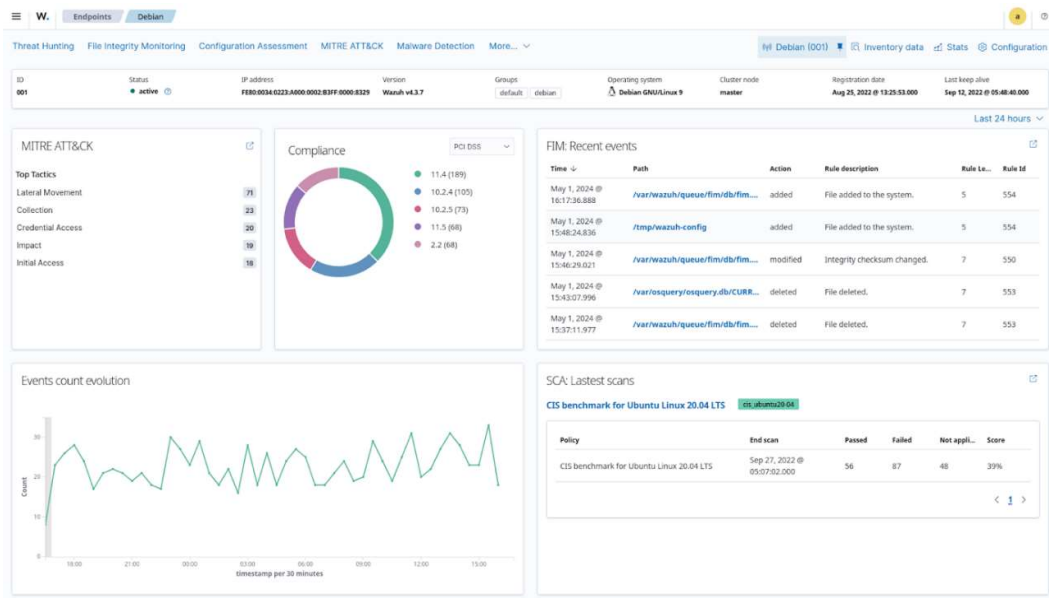
2.3.3 Embedded Technologies

Active Response. Wazuh's active response is based on particular triggers, which by default are configured on Wazuh's server. The triggers can be an SSH Brute Force Attack or a Malware Detection. Each response has been defined by the execution of a command, the location, the rule ID that causes the reaction to be carried out, as well as a timeout indicator as to how long the response should last. The reactions may range from the blocking of IP addresses, the disabling of a user's account, or the restart of a service. That being said, Wazuh also allows the user to create a unique active response option tailored to the user's environment based on various programming languages for more customisation.

2.3.4 Usability

Figure 6.

Debian endpoint dashboard



Wazuh's monitoring dashboard shows the general information that is expected from an SIEM tool, such as the overview of the monitored endpoint, the list of the common tactics that have been detected in the monitored environment, the different categories of compliance as well as the number of related issues, the File Integrity Monitoring, and the Security Configuration Assessment latest scans. Overall, this comprehensive view allows the user to manage and obtain up-to-date information about the latest security events which is essential in maintaining the security posture. That being said, it might be missing some other features that might enhance the use of the SIEM tool, such as User and Entity Behaviour Analytics (UEBA) which can identify some behaviours that are considered abnormal, and a customisation feature of the dashboard, since the default dashboard might require some users who are not familiar with SIEM tools to go through a learning process before getting used to it.

2.3.5 Cost-Effectiveness

Since Wazuh is open-source, it helps in reducing costs, particularly regarding licensing fees in comparison to commercial SIEM options (Manzoor et al., 2024). In addition, the open-source nature means that it has the advantage of an extensive community of contributors, which means that users of Wazuh will constantly receive regular improvements free of charge. Considering that Wazuh is fairly flexible in terms of deployment, Wazuh is able to scale relative to the requirements of the users which cuts operating costs even further. This makes it an appealing choice for users who are looking for an entry-level or budget-friendly SIEM solution, especially SMEs. Some might even say that the solution that it offers is actually above the free price tag that it has. However, there are also some drawbacks:

Increased costs. This may happen due to many reasons, some of which are:

- Customised development and scripting, which is the byproduct of Wazuh's flexible nature. When there are a lot of customisations involved, this may lead to the rising demand for labour costs and the need for specific skills.
- Scalability issue. Maintaining and ensuring the desired performance can be reached, especially in extensive environments, can be quite a challenge, which translates to increased costs related to the scaling and optimisation area. This may involve additional hardware, storage, and employees.

- Learning curve. Taking into account that Wazuh is both open-source and highly customisable, it requires a lot of resources and time to properly use and manage it (G2, n.d.), which leads to extra costs.

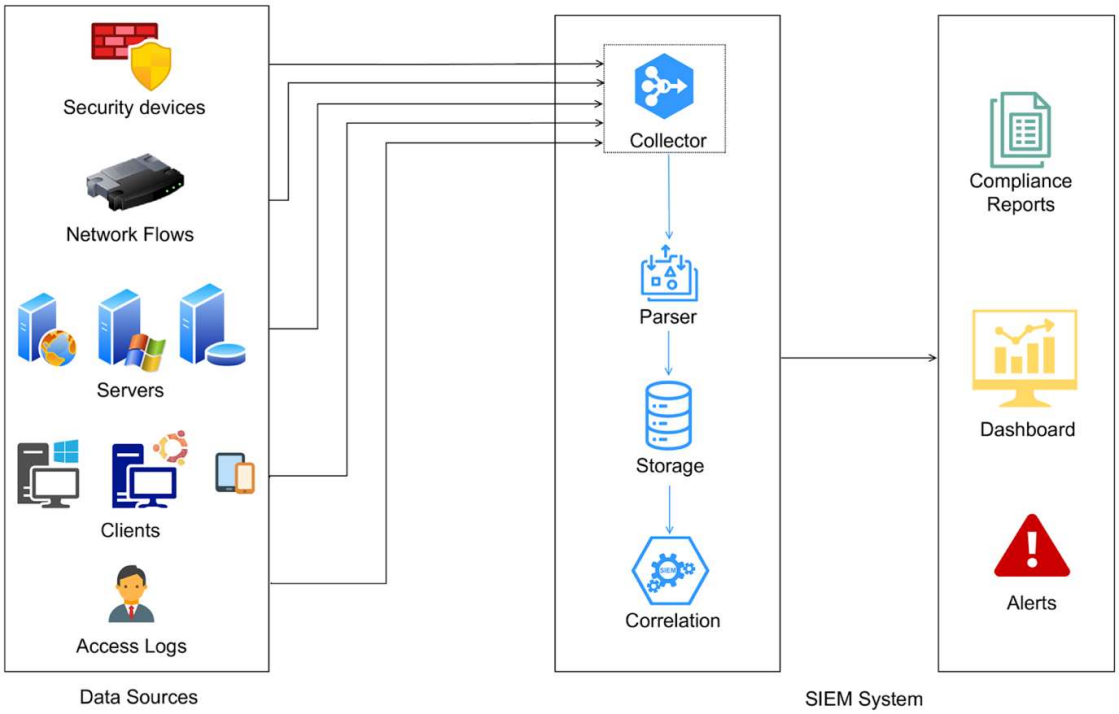
The lack of advanced features such as Machine Learning, Artificial Intelligence, integration with OSINT, and SOAR. This is also one of the recommended improvements produced by Manzoor et al. (2024), where some of the well-known commercialised SIEM solutions have those features integrated, such as Splunk. With the role of AI that is only ever-growing, it is hoped that AI can be used to include predictive capabilities for the analytics of user behaviour.

All in all, it is a critical step for the user to first identify the nature and size of the organisation, the budget, as well as the human resources that it has before finally choosing Wazuh as a SIEM solution. Careful considerations must be taken since all the extra resources needed from the aforementioned drawbacks might be more costly than the licensing fees when using other alternatives.

2.3.6 Performance Analysis

Figure 7.

SIEM workflow diagram



In order to analyse the performance of Wazuh, it is essential to understand the basic workflow of an SIEM as displayed in Figure 7. To put it simply, various data such as logs and others are collected from endpoints by the SIEM. Since a lot of them have different formats, they will go through the normalisation process under the parser stage. Normalisation changes all the different formats to a unified form so that it would be easier for the SIEM to process and presentable to the user for monitoring purposes. The correlation stage learns the obtained data and draws parallels between them and known security incidents through numerous statistical methodologies, rule-based reasoning, etc. (Manzoor et al., 2024). The findings are then reported to the user on the dashboard, or in the form of compliance reports or alerts.

There are many metrics to measure the capability of an SIEM's performance. This paper will focus on three areas, which are the Time to Detect (TTD), Active Response Reaction Time, and Event Per Second (EPS).

Time to Detect (TTD). Farrel et al. (2024), in the research of the active response test of Wazuh and its implementation with Telegram's API for alert forwarding, it was found that during the brute force attack simulation with pre-configured rules set in place, Wazuh successfully detected all attacks with no attacks going undetected, and mitigated them, ensuring that none breached the security measures. Even though there were variants among the Time to Detect, they were not deemed to be significant.

The same paper also underscored the ability of Wazuh to distinguish between users and threat actors. In a scenario where there were regular users without threat actors, Wazuh classified them as indications of non-brute force attacks.

Active Response Reaction Time. The same paper from Farrel et al. (2024) also emphasized the reaction time indicator, which is the amount of time taken by Active Response to act against the source IP that carried out the brute force attack. Using the formula of Active Response Reaction Time = time to response - time to detect, the team was able to quantify the reaction time based on the various scenarios provided in the paper.

It was found that the average time taken for the Active Response to respond after the detection of brute force attacks was 0.51 seconds, which clearly indicates the high efficiency and reliability of Wazuh in addressing threats promptly. Additionally, the shortest time discovered by the researchers was an astounding 0.00 seconds, meaning that there was an

immediate response after the identification of the attack. All in all, Wazuh was found to be fast, reliable, as well as having a 100% accuracy rate without any false positives being triggered in the controlled experiment.

Event Per Second (EPS). In the research conducted by Manzoor et al. (2024), it was decided that EPS was to be used for the performance evaluation. The events are sourced from a wide range of endpoints where the SIEM would parse through them and establish connections based on the parsed logs based on the predefined rules. It was discovered that when compared to other open-source SIEM solutions such as OSSIM, SIEMonster, and Elastic Security, Wazuh produced the highest number of EPS, and it was around 64% higher EPS than other SIEMs for pfsense, and more than 200% higher for Windows and Ubuntu.

The team of researchers also developed their unique methodology to measure the overall score to the tested SIEMs through the consideration of two important factors, which are the primary and the secondary features of each security solution. It was agreed that Wazuh was the best solution with the most efficient performance benchmark along with the essential security features that came with it. Therefore, if organisations, especially SMEs, are looking for an SIEM solution, it is recommended for Wazuh to be considered first.

That being said, the research also found some drawbacks with Wazuh. The first is that Wazuh did not come with threat intelligence capability built-in. Only Elastic Security and SIEMonster did. Secondly, even though open-source SIEM tools may seem powerful and fulfil the requirements of many SMEs, it is important to bear in mind that they are not on the same level as the commercialized SIEMs. Therefore, accounting for the important factors such as scalability, features, compliance, and long-term support, an organisation might want to start to consider moving to a commercial SIEM if open-source SIEMs are no longer capable of support.

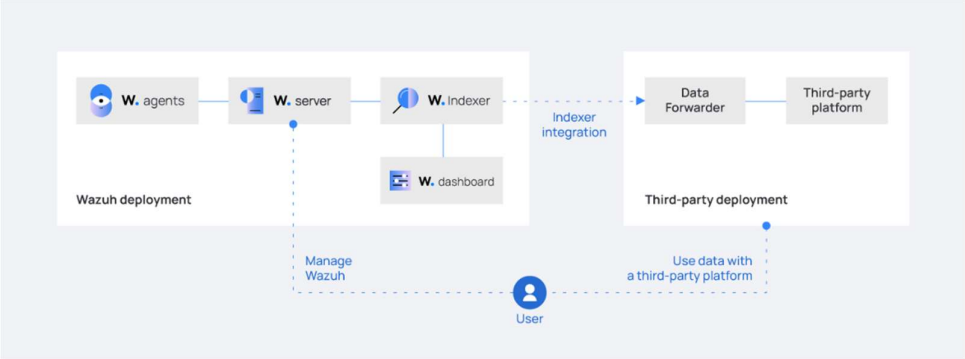
2.3.7 Integration Capabilities

Integration with third-party SIEM solutions. Wazuh allows for flexible compatibility and integration with third-party platforms such as Elastic, OpenSearch, and Splunk. There are two areas of integration, which are Indexer Integration and Server Integration.

Indexer Integration. The indexer integration works when the Wazuh agent analyses and indexes the security logs gathered from the monitored endpoints. It is then sent to the third-party platform in the index form. The Wazuh indexing integration has to have a Wazuh indexer run and forward the log using Logstash to other security solutions, which has to be installed either on a dedicated server or on the server where the third-party indexer is hosted.

Figure 8.

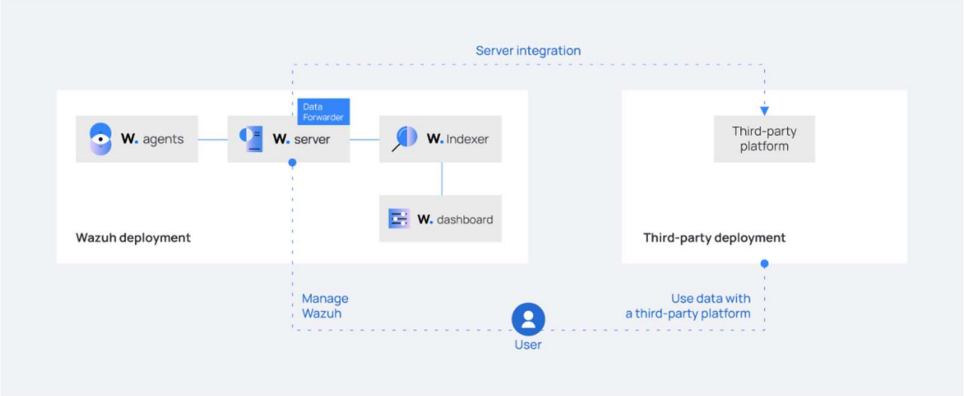
Wazuh indexer integration diagram.



Server Integration. Security data are collected by the Wazuh agent from the monitored endpoints, which are then analysed and used to generate alerts, which are stored locally, on the Wazuh dashboard by the Wazuh server. It is recommended that the users prioritise the server integration over the indexer integration when faced with resource limitations for hosting the indexers from both the third-party platform and Wazuh, since operating Wazuh at an extensive scale will generate a huge number of alerts.

Figure 9.

Wazuh server integration diagram.



Workload Protection. Wazuh offers protection to workloads in both cloud environments and on-site. It can be integrated with cloud platforms such as Google Cloud, AWS, Microsoft 365, and GitHub, among many others, to monitor services, VMs, and all activities happening on those platforms. Wazuh's centralised management of logs helps users comply with regulatory standards such as PCI DSS, GDPR, HIPAA, NIST 800-53, and TSC.

3. Comparison between Selected SIEM Solutions

3.1 Comparison Table

Table 2 below displays a comparison table of the three analysed SIEM solutions and their features.

Table 2.

Comparison between the selected SIEM solutions.

Components	Microsoft Sentinel	IBM Security QRadar SIEM	Wazuh
Deployment model	Cloud-native (SaaS)	On-premises, cloud, and hybrid	Open-source, on-premises, and cloud
Year launched	2019	2006	2015
Industry positioning (Gartner's Magic Quadrant for SIEM)	"Visionary" (2021), "Leader" (2022-2024)	"Leader" (2012-2024)	Not listed
Log management	Automated data ingestion and real-time analysis	Centralises log and flow data with over 450 pre-built Device Support Modules (DSMs) and features a	Collects and analyses logs from various sources. It supports logs from Linux, Windows, and MacOS, and allows

		GUI-based DSM Editor for custom log parsing	integration with third-party solutions for enhanced log management
User Interface	Pre-built content and intuitive dashboards	Has a steep learning curve and a complex interface, but offers highly customizable dashboards and extensive training resources	Provides a comprehensive monitoring dashboard but lacks advanced features like dashboard customization
AI and Machine Learning	Advanced AI and machine learning features	Advanced AI and machine learning features	Limited AI capabilities
UEBA	Built-in UEBA capabilities	Partial support, UBA only tracks end-user behaviour patterns but does not monitor non-user entities.	None
SOAR	Integrated SOAR capabilities through Azure Logic Apps and playbooks	Integrated SOAR capabilities through IBM Security SOAR	None, requires third-party integration
Scalability	Highly scalable due to its cloud-native architecture, supports auto-scaling with Azure	Scalable due to its modular architecture, with options to add high availability and disaster recovery features	Less scalable, within the constraints of the open-source architecture

Integration capabilities	Integrates seamlessly with Microsoft products like 365 Defender and Azure services, and also supports third-party platforms such as AWS, Google Cloud, and custom connectors.	Provides over 700 pre-built integrations, including major cloud providers and IBM's own security tools, with extensive API support for custom workflows.	Integrates with third-party SIEMs like Elastic and Splunk, offers cloud and on-site workload protection, and supports compliance with various regulatory standards.
Cost	No upfront cost required, flexible pay-as-you-go model or commitment tiers	Depends on data volume, server count, and licensing model, offering flexible options like usage-based, server-based, or subscription pricing.	Open-source and free to use. However, increased costs may be incurred when an organisation expands and requires more scalability and customisation.

3.2 How Different Technologies and Advancement in Technologies Help in Performance Optimization of Each SIEM Solution

3.2.1 Microsoft Sentinel

Technological Advancements. Microsoft Sentinel's cloud-native architecture and integration with Azure services provide significant performance optimization. Its scalable design and the use of Azure's auto-scaling capabilities, ensures that Sentinel can handle varying loads efficiently without needing manual intervention. Its advanced AI and machine learning capabilities enhance threat detection by analyzing large volumes of data in real time. These technologies allow Sentinel to identify patterns and anomalies quickly, leading to more accurate and faster threat responses.

Performance Optimization. The integration with Microsoft 365 Defender and Azure services streamlines data collection and analysis, as it leverages built-in data connectors for seamless integration. Its pay-as-you-go pricing model aligns costs with usage, reducing excess resource usage and maximizing financial returns. The built-in SOAR capabilities through Azure Logic Apps further automate incident response, which reduces manual efforts and accelerates remediation processes.

3.2.2 IBM Security QRadar SIEM

Technological Advancements. QRadar SIEM leverages a modular architecture that supports scalable deployments, including options for high availability and disaster recovery. Its extensive use of AI and machine learning enhances log and flow data analysis, enabling accurate detection of threats and anomalies. The platform provides over 450 pre-built Device Support Modules (DSMs), which promotes rapid deployment and efficient log management. The DSM Editor allows for customization of log parsing, optimizing data accuracy and relevance for more effective threat analysis.

Performance Optimization. QRadar SIEM offers numerous pre-built integrations and extensive API support, allowing it to seamlessly connect with a wide range of tools and data sources. This capability ensures comprehensive security visibility by efficiently aggregating and analyzing data from various environments. Additionally, the platform's scalability is enhanced by its flexible deployment options, which include on-premises, cloud, and hybrid models. This flexibility enables organisations to optimize performance according to their specific needs and infrastructure.

3.2.3 Wazuh

Technological Advancements. Wazuh's open-source architecture offers significant flexibility for customization and integration with various log sources and third-party tools. While its AI capabilities are not as advanced as Microsoft Sentinel and QRadar, its log management features provide extensive customization and scalability. Wazuh's compatibility with multiple operating systems and custom log sources ensures it can adapt to diverse organisational environments and requirements.

Performance Optimization. Wazuh excels in collecting and analyzing logs from a wide array of sources, while maintaining comprehensive visibility over the monitored

environment. Its integration with third-party SIEMs and compliance management tools supports a streamlined approach to data management and threat detection. However, its scalability can be limited by its open-source nature, which may require additional resources for large-scale deployments. The platform is cost-effective due to its free-to-use model, though costs may increase with higher customization and scalability needs.

4.0 Future Technology Predictions

As the complexity of cyber threats continue to increase, SIEM tools evolve alongside the advancements in technology to address these threats effectively. According to Pulyala (2023), traditional SIEM systems were only used to centralise, normalise and analyse event and log data across the organisation's digital environments. However, they lack the sophistication to detect alerts and do not provide high scalability as organisations grow and expand their digital systems and ecology. Next-generation SIEM systems emerged with the integration of AI and machine learning, with features such as UEBA and SOAR, enhancing the capabilities of a SIEM system in detecting and responding to cyber threats. The advancement of cloud computing has also led to the emergence of hybrid and cloud-based SIEM solutions. Microsoft Sentinel and IBM Security QRadar are examples of next generation SIEM systems that were studied in this paper.

4.1 Advanced AI and Machine Learning Capabilities

Pulyala (2023) predicts that the incorporation of AI and machine learning will continue to evolve and enhance the SIEM systems. A primary benefit of advanced machine learning is the reduction of false positives, which are activities incorrectly flagged as threats. Machine learning can help to address this issue as it develops a more accurate predictive algorithm to distinguish legitimate threats, thus reducing the amount of false positives. Additionally, Pulyala (2023) also believes that more SIEM systems will incorporate the use of Generative AI, such as Large Language Models (LLM), into SIEM systems. These chatbots can help to automate responses and provide guidance on investigation suspicious activities. Another prediction proposed by Pulyala (2023) is the integration of AI and machine learning into the training and skill development of security teams to utilise SIEM tools effectively. For instance, Splunk introduced the Splunk AI which helps new users learn the system quickly as well as assist veteran users to maximise the features offered by the

SIEM system. This addresses the issue of high learning curve when it comes to SIEM systems.

4.2 Open Source Intelligence (OSINT)

Another possible improvement for current SIEM systems is incorporating language processing to detect threats based on keywords that are commonly associated with threats, such as “DDoS”, “leak”, and “security breach” (González-Granadillo et al., 2021). This enables SIEM systems to categorise OSINT data as relevant or irrelevant. Additionally, details from OSINT sources, such as location and involved entities, can also be extracted to offer a more detailed threat profile. The inclusion of a prediction confidence of the classifier can help to reduce false alarms.

4.3 Improved GDPR Privacy Compliance

Menges et al. (2021) discusses a significant challenge faced by SIEM systems, which is the need to balance the functionality of SIEM systems with compliance to privacy regulations such as the General Data Protection Regulation (GDPR). SIEM systems that are dependent on processing personal data to accurately detect threats may face conflicts with GDPR’s privacy requirements. However, the inability to capture complete user data limits the effectiveness of the SIEM system’s correlating ability, resulting in a higher number of false positives and negatives. Hence, it is important for future SIEMs to comply with GDPR while also gathering sufficient data for accurate security threat detection and response. To address this issue, Menges et al. (2021) proposes a GDPR-compliant SIEM system through integrating anonymisation and pseudonymisation into SIEM systems while maintaining effective threat detection as well as preserving the ability to verify the integrity of the data.

5.0 Conclusion

In this report, we have evaluated and analysed three prominent Security Information and Event Management (SIEM) solutions: Microsoft Sentinel, IBM Security QRadar SIEM, and Wazuh. Each solution offers unique strengths and capabilities, catering to different organisational needs and preferences.

Microsoft Sentinel offers a cloud-native, scalable solution with advanced AI and machine learning for real-time threat detection. Its integration with Microsoft services and

flexible pricing model makes it suitable for organisations seeking modern, scalable SIEM capabilities.

IBM Security QRadar SIEM excels with its modular architecture, extensive integration options, and robust AI-driven analytics. Its flexibility and customizable features make it ideal for organisations with diverse needs and complex environments.

Wazuh provides a cost-effective, open-source solution with significant customization and integration flexibility. While its AI capabilities are less advanced, it supports comprehensive log management and compliance, making it a good choice for budget-conscious organisations.

Ultimately, the choice of a suitable SIEM system is dependent on the organisation's specific requirements, existing infrastructures and budget considerations.

In the future, we predict further incorporation of advance AI and machine learning capabilities to improve and enhances SIEM systems, such as improved machine learning-powered predictive algorithms to reduce false positives, the incorporation of Generative AI and the integration of AI and machine learning into training security teams on the usage of the SIEM systems. Furthermore, we also predict the use of OSINT with SIEM systems to detect and investigate security threats. Lastly, we identified the need for SIEM systems to improve their GDPR privacy compliance without compromising their threat detection effectiveness, which can be achieved through integrating anonymisation and pseudonymisation into SIEM systems.

6.0 References

Cloud Direct. (n.d.). *Microsoft Sentinel vs. traditional SIEMs.* Retrieved August 9, 2024, from https://www.clouddirect.net/learning-hub/microsoft-sentinel-vs-traditional-siems/

Diogenes, Y., DiCola, N., & Trull, J. (2020). *Microsoft Azure Sentinel: Planning and implementing Microsoft's cloud-native SIEM solution.* Pearson Education, Inc.

Farrel, F. I., Mardianto, I., Qamar, A. S. (2024). Implementation of Security Information & Event Management (SIEM) Wazuh with active response and telegram notification for mitigating brute force attacks on the GT-I2TI USAKTI information system. *Intelmatics*. https://doi.org/10.25105/itm.v4i1.18529

Forrester. (2023). *The total economic impact™ of IBM Security QRadar SIEM*. Retrieved August 10, 2024, from https://4719eaee91034be722d8-c86a406a93c55de2464febd03debd4f0.ssl.cf1.rackcdn.com/ar_Forrester_The_Total_Economic_Impact_Of_IBM_Security_QRadar_SIEM_1.PDF

Forrester. (2023). *The total economic impact of Microsoft Sentinel.* Retrieved August 9, 2024, from https://tei.forrester.com/go/microsoft/microsoft_sentinel/

G2. (n.d.). *Wazuh, the open-source security platform: Reviews, pros and cons*. Retrieved August 10, 2024, from https://www.g2.com/products/wazuh-the-open-source-security-platform/reviews?qs=pros-and-cons

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security information and event management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors 2021, 21*(4759). https://doi.org/10.3390/s21144759

IBM. (n.d.). *Advanced threat detection with IBM QRadar SIEM*. Retrieved August 10, 2024, from https://www.ibm.com/products/qradar-siem/advanced-threat-detection

IBM. (n.d.). *IBM QRadar 7.4.3 user guide*. Retrieved August 10, 2024, from https://www.ibm.com/docs/en/SS42VS_7.4/pdf/b_qradar_gs_guide.pdf

IBM. (n.d.). *IBM QRadar SIEM*. Retrieved August 10, 2024, from https://www.ibm.com/products/qradar-siem

IBM. (2019). *IBM QRadar SIEM solution brief*. Retrieved August 10, 2024, from https://www.ibm.com/downloads/cas/RLXJNX2G/name/0046039bf9005a8f.pdf

IBM. (n.d.). *Integrations for partners*. Retrieved August 10, 2024, from https://www.ibm.com/products/qradar-siem/integrations

IBM. (n.d.). *Pricing*. Retrieved August 10, 2024, from https://www.ibm.com/products/qradar-siem/pricing#priceestimator

IBM. (n.d.). *User behavior analytics with IBM QRadar SIEM*. Retrieved August 10, 2024, from https://www.ibm.com/products/qradar-siem/user-behavior-analytics#:~:text=IBM%20QRadar%20SIEM%20User%20Behavior,better%20detect%20threats%20to%20your

IBM. (n.d.). *Using IBM QRadar SIEM*. Retrieved August 10, 2024, from https://www.ibm.com/support/pages/using-ibm-qradar-siem-0

Krishna, P. (2021). *Introducing Microsoft Sentinel Content hub!* Retrieved July 31, 2024, from https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/introducing-microsoft-sentinel-content-hub/ba-p/2928102

Lefferts, R. (2024). *Microsoft is again named a Leader in the 2024 Gartner Magic Quadrant for Security Information and Evet Management.* Retrieved August 10, 2024 from https://www.microsoft.com/en-us/security/blog/2024/05/13/microsoft-is-again-named-a-leader-in-the-2024-gartner-magic-quadrant-for-security-information-and-event-management/

Manzoor, J., Waleed, A., Jamali, A. F., Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. *Plos One*. https://doi.org/10.1371/journal.pone.0301183

Maple Networks. (2021). *The operational and commercial benefits of Microsoft Sentinel.* Retrieved August 9, 2024, from https://info.maplenetworks.co.uk/the-operational-and-commercial-benefits-of-azure-sentinel

Menges, F., Latzo, T., Vielberth, M., Sobola, S., Pöhls, H. C., Taubmann, B., Köstler, J., Puchta, A., Freiling, F., Reiser, H. P., & Pernul, G. (2020). Towards GDPR-compliant

data processing in modern SIEM systems. *Computers & Security, 103*(2021). https://doi.org/10.1016/j.cose.2020.102165

Microsoft. (2024). *About Microsoft Sentinel content and solutions.* Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/sentinel-solutions.

Microsoft. (2024). *Advanced threat detection with user and entity behavior analytics (UEBA) in Microsoft Sentinel.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

Microsoft. (2024). *Automation in Microsoft Sentinel: Security orchestration, automation, and response (SOAR).* Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/automation/automation

Microsoft. (2020). *Azure Sentinel achieves a Leader placement in Forrester Wave with top ranking in Strategy.* Retrieved August 10, 2024 from https://www.microsoft.com/en-us/security/blog/2020/12/01/azure-sentinel-achieves-a-leader-placement-in-forrester-wave-with-top-ranking-in-strategy/

Microsoft. (2023). *Create and share dashboards of Log Analytics data.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/azure-monitor/visualize/tutorial-logs-dashboards

Microsoft. (2024). *Jupyter notebooks with Microsoft Sentinel hunting capabilities.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/notebooks

Microsoft. (2023). *Kusto Query Language in Microsoft Sentinel.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/kusto-overview

Microsoft. (2024). *Log Analytics workspace overview.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/azure-monitor/logs/log-analytics-workspace-overview

Microsoft. (2024). *Microsoft Sentinel data connectors.* Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/connect-data-sources

Microsoft. (n.d.). *Microsoft Sentinel documentation*. Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/

Microsoft. (n.d.). *Microsoft Sentinel pricing.* Retrieved August 9, 2024, from https://azure.microsoft.com/en-us/pricing/details/microsoft-sentinel/

Microsoft. (2023). *Normalisation and the Advanced Security Information Model (ASIM) (Public preview).* Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/normalization

Microsoft. (2024). *Threat detection in Microsoft Sentinel.* Retrieved July 31, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/threat-detection

Microsoft. (2024). *Threat hunting in Microsoft Sentinel.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/hunting

Microsoft. (2023). *Understand Microsoft Sentinel's incident investigation and case management capabilities.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/incident-investigation

Microsoft. (2024). *Visualise collected data on the overview page.* Retrieved August 9, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/get-visibility

Microsoft. (2024). *What is Microsoft Sentinel?* Retrieved July 31, 2024, from https://learn.microsoft.com/en-gb/azure/sentinel/overview

Microsoft. (2024). *Threat intelligence integration in Microsoft Sentinel.* Retrieved August 10, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/threat-intelligence-integration

Microsoft. (2024). *Threat detection in Microsoft Sentinel.* Retrieved August 10, 2024, from https://learn.microsoft.com/en-us/azure/sentinel/threat-detection#threat-intelligence

Miguel, P. G. (2023). *IBM Security QRadar SIEM in depth review*. The CTO Club. Retrieved August 10, 2024, from https://thectoclub.com/tools/ibm-security-qradar-siem-review/

Miguel, P. G. (2023). *IBM Security QRadar SIEM offers a detailed report on suspiscious host activity* [Infographic]. The CTO Club. Retrieved August 10, 2024 from https://thectoclub.com/tools/ibm-security-qradar-siem-review/

Mudaliar, Y. (2021). *Why Microsoft Sentinel should be your first choice for a SIEM.* Retrieved August 10, 2024, from https://atech.cloud/resources/why-should-azure-sentinel-be-your-first-choice-for-a-siem/

National Institute of Standards and Technology. (2006). *Special Publication 800-92: Guide to computer security log management*. Retrieved form https://csrc.nist.gov/pubs/sp/800/92/final

Pulyala, S. R. (2023). The future of SIEM in a machine learning-driven cybersecurity landscape. *Turkish Journal of Computer and Mathematics Education, 14*(03), 1309-1314.

Rawat, P. (2024). *Key components of Microsoft Sentinel.* Retrieved August 10, 2024, from https://www.infosectrain.com/blog/key-components-of-microsoft-sentinel/

SelectHub. (2024). *Microsoft Sentinel vs IBM QRadar*. Retrieved August 10, 2024, from https://www.selecthub.com/siem-tools/microsoft-sentinel-vs-ibm-qradar/

Šuškalo, D., Morić, Z., Redžepagić, J., & Regvart, D. (2023). Comparative analysis of IBM QRadar and Wazuh for security information and event management. In B. Katalinic (Ed.), *Proceedings of the 34th DAAAM International Symposium*. DAAAM International. https://doi.org/10.2507/34th.daaam.proceedings.014

Wafula, I. (2021). *Accessibility and usability for all in Azure Sentinel.* Retrieved August 9, 2024, from https://www.microsoft.com/en-us/security/blog/2021/07/07/accessibility-and-usability-for-all-in-azure-sentinel/

Wazuh. (2024). *CIS Ubuntu Linux 22.04 LTS Benchmark v1.0.0.* Retrieved August 9, 2024, from https://documentation.wazuh.com/current/getting-started/use-cases/it-hygiene.html

Wazuh. (2024). *Debian endpoint dashboard.* Retrieved August 9, 2024, from https://documentation.wazuh.com/current/getting-started/components/wazuh-dashboard.html

Wazuh. (n.d.). *File integrity monitoring use case*. Retrieved August 10, 2024, from https://documentation.wazuh.com/current/getting-started/use-cases/file-integrity.html

Wazuh. (n.d.). *Integrations guide*. Retrieved August 10, 2024, from https://documentation.wazuh.com/current/integrations-guide/index.

Wazuh. (n.d.). *IT hygiene use case*. Retrieved August 10, 2024, from https://documentation.wazuh.com/current/getting-started/use-cases/it-hygiene.html

Wazuh. (2024). *MITRE ATT&CK's module on Wazuh's dashboard*. Retrieved August 10, 2024, from https://documentation.wazuh.com/current/getting-started/use-cases/threat-hunting.html

Wazuh. (n.d.). *Platform overview*. Retrieved August 10, 2024, from https://wazuh.com/platform/overview/

Wazuh. (n.d.). *SIEM platform*. Retrieved August 10, 2024, from https://wazuh.com/platform/siem/

Wazuh. (n.d.). *Wazuh dashboard components*. Retrieved August 10, 2024, from https://documentation.wazuh.com/current/getting-started/components/wazuh-dashboard.html

Wazuh. (2024). *Wazuh indexer integration diagram.* Retrieved August 9, 2024, from https://documentation.wazuh.com/current/integrations-guide/index.html

Wazuh. (2024). *Wazuh server integration diagram*. Retrieved August 9, 2024, from https://documentation.wazuh.com/current/integrations-guide/index.html