TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Giorgi Sharia IVSB177777

COMPARATIVE ANALYSIS OF ENTERPRISE SECURITY INFORMATION AND EVENT MANAGEMENT(SIEM) SOLUTIONS, CASE OF CYBERS

Bachelor's Thesis

Supervisor: Toomas Lepikult
PhD

Co-Supervisor: Tiit Erm
MSc

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Giorgi Sharia IVSB177777

TURVATEABE JA -SÜNDMUSTE HALDUSLAHENDUSTE (SIEM) VÕRDLEV ANALÜÜS ETTEVÕTTE CYBERS NÄITEL

Bakalaureusetöö

Juhendaja: Toomas Lepikult
PhD

Kaasjuhendaja: Tiit Erm
MSc

Tallinn 2020

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature, and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Sharia Giorgi

18.05.2020

Abstract

Security Information and Event Management systems play a vital role in the modern-day cybersecurity landscape. As the world of Information Technologies became more and more diverse, it was impossible for security specialists to manually track and interpret hundreds of different log sources and patterns as well as analyze an enormous amount of data for possible indication of compromise. The primary purpose of SIEM systems is handling log and event data from heterogeneous data sources, detecting, classifying, prioritizing, and mitigating cyber-attacks at the early stage of the cyber kill chain. Due to high demands from the enterprise market, the number of solutions exist, each with different approach to tackle the same objectives.

This thesis analyses and defines requirement criteria, from an enterprise standpoint, for SIEM solution, discusses feature set and architecture behind solution for each product.

After head-to-head assessment of each solution mapped to requirement criteria, combined with feature set evaluation, work is summarized in the definition of the overall market leader for enterprise solutions.

Work is performed based on the needs of Cyber Security company CYBERS, which provides full cybersecurity services to other businesses.

Annotatsioon

Turvateabe ja -sündmuste halduslahenduste (SIEM) võrdlev analüüs ettevõtte CYBERS näitel

Turvainfo ja -sündmuste haldamise süsteemil on tänapäeval küberturbe maastikul oluline roll. Infotehnoloogia valdkond mitmekesistub väga kiiresti ning seetõttu on turbespetsialistidel äärmiselt raske analüüsida käsitsi sadu logifaile võimalike rünnete tuvastamiseks.
SIEM-süsteemi esmane ülesanne on erinevate andmeallikate sündmuslogide ning andmete käsitlemine ning võimalike rünnete avastamine, klassifitseerimine, prioritiseerimine ning võimalike tagajärgede leevendamine ründe varajases faasis. Kõrge nõudluse tõttu on turul arvukalt vastavat tarkvara, mis erinevaid lähenemisviise kasutades probleemi lahendada püüavad.
Lõputöös analüüsitakse ja defineeritakse nõudeid ja kriteeriume SIEM-lahendusele ettevõtte aspektist. Samuti tuuakse välja erinevate lahenduste võimalused ning arhitektuurid.
Pärast iga üksiklahenduste hindamist nõuetele ja kriteeriumite le vastamise aspektist leitakse antud ettevõtte jaoks optimaalne lahendus.
Töö baseerub küberturbega tegeleva ettevõtte CYBERS vajadustel, mis pakub teistele ettevõtetele küberturbe täislahendusi.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti nelikümmend seitse leheküljel, kaheksa peatükki, kuus joonist, kaks tabelit.

List of abbreviations and terms

IT	Information Technology
IDS	Intrusion Detection System
SIEM	Security Information and Event Management
TI	Threat Intelligence
SOAR	Security Orchestration, Automation and Response
IOC	Indicator of Compromise
LMS	Log Management System
SIM	Security Information Management
SEM	Security Event Management
AI	Artificial Intelligence
ML	Machine Learning
UEBA	User Entity Behaviour Analytics
SOC	Security Operations Centre
IPS	Intrusion Prevention System
AV	Anti-Virus
SaaS	Security as a Service
UBA	User Behaviour Analytics
SOCaaS	Security Operations Centre as a Service
EPS	Events Per Second
FPM	Flows Per Minute
IOPS	Input/Output Operations per Second
RAM	Random Access Memory
CPU	Central Processing Unit
TB	TeraByte
GB	GigaByte
KB	KiloByte

Table of contents

List of figures

List of tables

1 Introduction

The world that we live in is changing and re-shaping with the highest tempo in history. The most prominent role in this has fallen to technological advancement that we have seen in the last four decades. Technological development changed every aspect of our day-to-day life. We learn, communicate, get news, share stories, manage and run businesses, and even govern countries using Information Technology (IT). Such ubiquitous involvement of Information Technology in our life has attracted cyber-criminals since the early steps of IT.

As IT systems are getting more and more complex and interconnected, managing them is getting harder. Cybercriminals have followed the advancement in technology, and cyber-attacks have grown exponentially in complexity. Utilizing perimeter defense techniques such as Firewalls and Intrusion Detection Systems (IDS) are no longer enough for ensuring the security of business. As a number of Information Technology services grew, as well as their variety in choice, it became impossible for cybersecurity specialists to monitor and track their activity one by one to ensure the security of the business. This is where the primary purpose of the Security Information and Event Management (SIEM) system comes in. SIEM systems aim to reduce the complexity of managing IT systems with the main target falling on their security. SIEM is a centralized system for application log, event, and network flow processing. It simplifies the task of a security specialist to visualize the big picture of the whole system within the business. Platform correlates data from different sources, enriches it with the information from different security field systems and platforms such as Threat Intelligence (TI), and even reduces the need for human involvement when used advantages of Security Orchestration Automation and Response (SOAR) platform.

This chapter provides an overview of Security Information and Event Management systems, describes the current situation on the market and upcoming development focus areas for SIEM. Next, it analyzes the background of the study, introducing works that

have been done around a similar topic. Lastly, the chapter defines research goals and pinpoints the expected outcomes of the work.

1.1 Background of the study

Logs hold a crucial role in the lifecycle of Information Technology systems. They provide real-time as well as historical information regarding systems state, health, recorded processes, and behavior. The importance of logs for security purposes is invaluable. As there is no single event that is recorded for security incidents within the system, regular log entries, their correlation within single and across multiple platforms are the basis for detection, identification, and investigation of an issue. For example, a single successful authentication event on its own cannot indicate suspicious behavior. However, hundreds of failure events followed by success is a high alert for a trial-and-error type of attack such as Brute Force or Dictionary Attacks. As IT systems got more integrated and complex, manually analyzing and correlating logs became impossible. The cybersecurity market demanded a solution, and Log Management Systems (LMS) emerged. LMS is a centralized platform for log collection from different sources into a single location. Based on the LMS platform, initially, two distinct systems were introduced: Security Information Management (SIM) and Security Event Management (SEM). SIEM combines the two systems mentioned above within a single platform for integrated functionality of historical and real-time analysis, cross-platform correlation, and standard compliance. Apart from log events, SIEMs utilize network packets for threat hunting, compromise detection, and health analysis. Each of the network packets can be inferred as a single event or combined into flows. In combination with SIEM's correlation capability, this further enhances the centralized picture of enterprise seen by SIEM and increases its capability in detection. Network packets independently can indicate at security threats such as Data Exfiltration; paired with system log events, confidence, and the level of security measure is increased. For example, when medium level suspicious activity is observed from a specific host, and additionally there is communication with bad reputation IP, this could indicate Command and Control and raise the priority and severity of the incident to be investigated by the security team.

According to M-Trends 2020[1], threat research study by FireEye, cybersecurity hardware, software, and service provider company, median dwell time[1] globally was 56 days for the period of one year between October 1, 2018, and September 30, 2019, a significant improvement compared to previous years 78-day median. Generally, the trend of improvement in business security is observed. Single reasoning behind it cannot be put. However, overall awareness from the society, businesses understanding the value of security and investing more money into security solutions and employee skillset, vendors of security solutions using advantages of emerging technologies, and improving products day-by-day has led to a positive trend.

Nowadays need for a centralized platform for security monitoring, event analysis, and correlation is highest than ever. Based on M-Trends 2020[1], during last year, more than five hundred new malware families have been observed. Situation brings an urge within the cybersecurity surface for functionality enhancement and overall improvement of security products. Due to demand from the market, dozens of vendors have tackled a challenge for developing SIEM. These companies range from ones that have well established their place on cybersecurity market such as McAfee and IBM, to ones that are at the early stage of the development but have shown promise or demonstrated quality in different field of Information Technology such as Elastic. Regardless of the numerous solutions and differences in feature-set, there is a significant portion of the functionality that all of them share. It can be inferred as baseline criteria that make the solution a Security Information and Event Management platform. Generalized list of requirements of functionality of SIEM are:

- Data collection and aggregation from various source systems and applications
- Data normalization, correlation and analysis with rule or behavior-based approach
- Storage and Retention for real-time and historical data
- Functionality for assuring compliance with regulations and standards
- Visualization for real-time and historical data (dashboards, graphs)

[1] Is calculated as a number of days an attacker present in a victim network before they are detected [1]

- Alert generation and prioritization based on the severity of the incident

Even within shared components, the approach to solution differs on a vendor basis. Architecture behind each functionality of SIEM varies as well as a set of capabilities. More advanced products utilize and integrate advantages of the Security Orchestration Automation and Response platform to existing SIEM solution. Standalone SIEM solution is not capable of automatic responses to the incident. For example, when a high priority incident is detected on a host, SIEM cannot isolate the machine from the network to prevent the spread of cyber-attack; however, with capabilities of the SOAR platform, this can be achieved. Another trend in the SIEM market is the use of Artificial Intelligence (AI) and Machine Learning (ML). ML models are used for behavior analysis, most commonly in User Entity Behavior Analytics (UEBA), to determine a deviate from normal behavior.

One of the most crucial aspects of a SIEM solution is integration with other cybersecurity applications and platforms. Ability to enrich observed data with the information such as geolocation of external IP, its reputation, involvement in previously observed activities is crucial. Having Threat Intelligence feeds within SIEM solution eases the work of Cyber Security Analysts to investigate, classify, prioritize, and mitigate the issue.

Considering all aforementioned capabilities, in combination with a variety of solution vendors, creates an overhead for an enterprise to determine the best product overall and specifically for their needs. Although there exist some works with general recommendations or somewhat detailed comparison of solutions, none of them analyze SIEM solutions with a detailed comparison of architecture behind each solution and functionality, licensing and costs, and deep dive in feature set.

1.2 Acknowledgment of Previous Work

Throughout the years' number of works have been done in regards to Security Information and Event Management platforms. Due to the high number of minor works concerning SIEM, it is impossible to acknowledge them all, however most valuable and tightly connected to the comparative analysis of SIEM solutions are discussed.

Annually Gartner [2], research and advisory company, publishes Magic Quadrant [3] for SIEM solutions. The document briefly describes the overall situation in the market, analyzes demands, and future trends. Gartner provides with a brief overview of functionalities for each solution discussed and places them in the Magic Quadrant for overall visualization classifying them into four categories: Leaders, Challengers, Visionaries and Niche Players. It shortly outlines the benefits and drawbacks of each SIEM product from the vendor.

Figure 1: Gartner Magic Quadrant 2020 [3]

Forrester [4], a research company in the field of Information Technology, works on the Forrester Wave report, which is buyers guide for various fields of technology. Last Forrester Wave in regard to SIEM solutions - Security Analytics Platforms Q3[5], which is a more general security analytics market overview rather than specific to

SIEM, was published in September of 2018 and already can be considered as dated. In report brief overview of solutions is provided with a concise definition of pros and cons for each solution.

In 2019 comparative analysis of proprietary and open-source SIEM tools has been done by Nika Ptskialadze as a diploma thesis at Tallinn University of Technology. Paper mostly focuses on a comparison of open-source and proprietary solutions, briefly lists the respective functionalities of products, and performs practical analysis on single representatives from each side of the approach.[6]

Solutions Review provides with annual study Security Information and Event Management Buyer's Guide. Document very briefly introduces market overview, lists down three critical features for a solution, and defines questions to be kept in mind while examining vendor products for best fit to a business. Unfortunately, the document provides a generalized examination of solutions without describing architecture behind, full feature set and their importance, key points such as scalability and stress handling, as well as licensing.[7]

1.3 Problem statement and research goals

Due to a wide variety of SIEM products determining the best solution is a complicated task. The work is based on the needs of determining suitable SIEM solution for Cyber Security company CYBERS [8] as a part of building a new Security Operations Center (SOC) as one of the tasks assigned to the author during the employment period at the company. Due to the needs of continuous support and updates for solutions, as well as demand on best quality and performance, only enterprise SIEM solutions were examined. Research goals of the work are as follows:

- Definition of comparison criteria for SIEM product evaluation
- Detailed overview of architecture behind each solution
- Qualitative analysis based on a feature set

- Measurement of hardware needs and performance

Licensing and pricing of a solution is one of the most significant contributors when making a decision. Usually, distinct prices are determined per case after a long process of negotiations between companies. Due to the high sensitivity of data and agreement with vendors, pricing offered to CYBERS will not be covered, however licensing terms provided by the companies for each solution will be discussed.

As an outcome, work will provide an overall best solution considering the needs of the existing market, demands of CYBERS in particular, and envisioning future trends. It will define evaluation criteria and identify the benefits and drawbacks of each discussed product in detail, establishing a benchmark for future comparison.

1.4 Thesis outline

This thesis is written in English and is forty-seven pages long, including eight chapters, six figures, and two tables.

2 Market Overview and Requirement Definition

SIEM market is driven by demands, with vendors tackling requirements set by the customers and problems introduced in the security field within their solutions. These requirements are dependent on cyberspace and are in direct connection to technology evolvement. IT advancements, with all the benefits, introduce new attack vectors and weak points to the modern technology landscape. Security products such as SIEM should follow cybersecurity posture introduced with technology advancement near real-time, to help enterprises detect and mitigate new threats.

This chapter focuses on the current market overview for Security Information and Event Management solutions, briefly describes the situation in the near past, and defines future trends and focus points for SIEM solutions.

2.1 Market Overview

Data has been one of the most valuable assets in the modern world. According to Cost of Data Breach report, a study conducted by Ponemon Institute and IBM based on more than 500 companies that experienced data breach between July 2018 and April 2019, the average total cost of a data breach was $3.92M with data breach lifecycle[1] being 279 days, an increase of 13 days on average compared to the previous year's numbers. Malicious attacks were the most common and costly source for data breaches. Patterns amongst the companies that experienced data breach show that third-party involvement, IT complexity, and extensive cloud migration as the most costly environmental factors. The study finds that companies with Incident Response teams and extensively tested plans in place saw $1.23M less cost damage on average, underlining the importance of cybersecurity within the business.[9]
Most defense techniques tend to focus on perimeter defense enforcement and the pre-exploit period. Solutions such as Intrusion Prevention System (IPS), Firewall, and Anti-

[1] Time to identify and contain the breach.

Virus (AV) mainly target the first four stages within the cyber kill chain, namely being Reconnaissance, Weaponization, Delivery, and Exploitation. [10] Defensive measures listed above have limitations in scope in terms of visibility, which ranges from endpoints to perimeter. SIEM solutions can have great value in detecting and identifying post-exploit actions bringing dwell time and breach lifecycle numbers down, and increasing enterprise security posture. Security Information and Event Management systems have contextual information at hand provided by full visibility of the IT infrastructure of the organization. Visibility is the key to these types of solutions as they can correlate data across platforms to detect possible indicators of compromise.

SIEM has been in high demand on the market. Vendors provide various deployment options, with different demands on-each from the customers. Initially, on-premise solutions were adopted, but as the complexity of the solution grew, so did the level needed to deploy, administer, and use the solution. Based on this market shift towards cloud and hybrid solutions as well as Security as a Service (SaaS) offerings.

Cloud migration has been one of the primary focuses of solution vendors. With time more and more businesses are looking into migrating their IT infrastructure to the cloud to avoid the complexity of setup and maintenance. Monitoring cloud infrastructure differentiates from traditional approaches. Although solution vendors have adapted cloud monitoring in their products, it is a continuous task as more and more services are migrated, providing the need for monitoring with different approaches.[9]

Users have been referred to as the weakest link in organizations' security posture, and security is as strong as its weakest link. In the past years, overall security awareness has grown within society. SIEM solutions have also tackled the problem with the utilization of technology advancement in terms of Machine Learning and applied User Behavior Analytics (UBA) within the solutions. The primary purpose of UBA is to look into deviations from normal behavior for anomaly detection with the use of historical analytics as well as peer activity comparison.
One more trend that advanced SIEM solutions have adopted is automation. SIEM products are no replacement for security specialists; they are used to increase their efficiency and ease their work. SOAR capabilities within the SIEM platform enables quicker and more efficient incident response and alarm triage.

Capabilities of both SIEM and UBA platforms are expected to grow and develop by the time.[11]

Integration with Threat Intelligence (TI) feeds is a great advantage in higher visibility and information about threats, adversaries, and threat actors. Advanced SIEM solutions provide direct integrations with TI feeds for product capability enhancement with TI solution vendors such as ThreatQuotient [12] and Recorded Future [13] or in-house developed appliances such as Threat Intelligence Exchange for McAfee and X-Force for IBM.

Figure 2 provides a visualization of Next-Gen SIEM architecture.

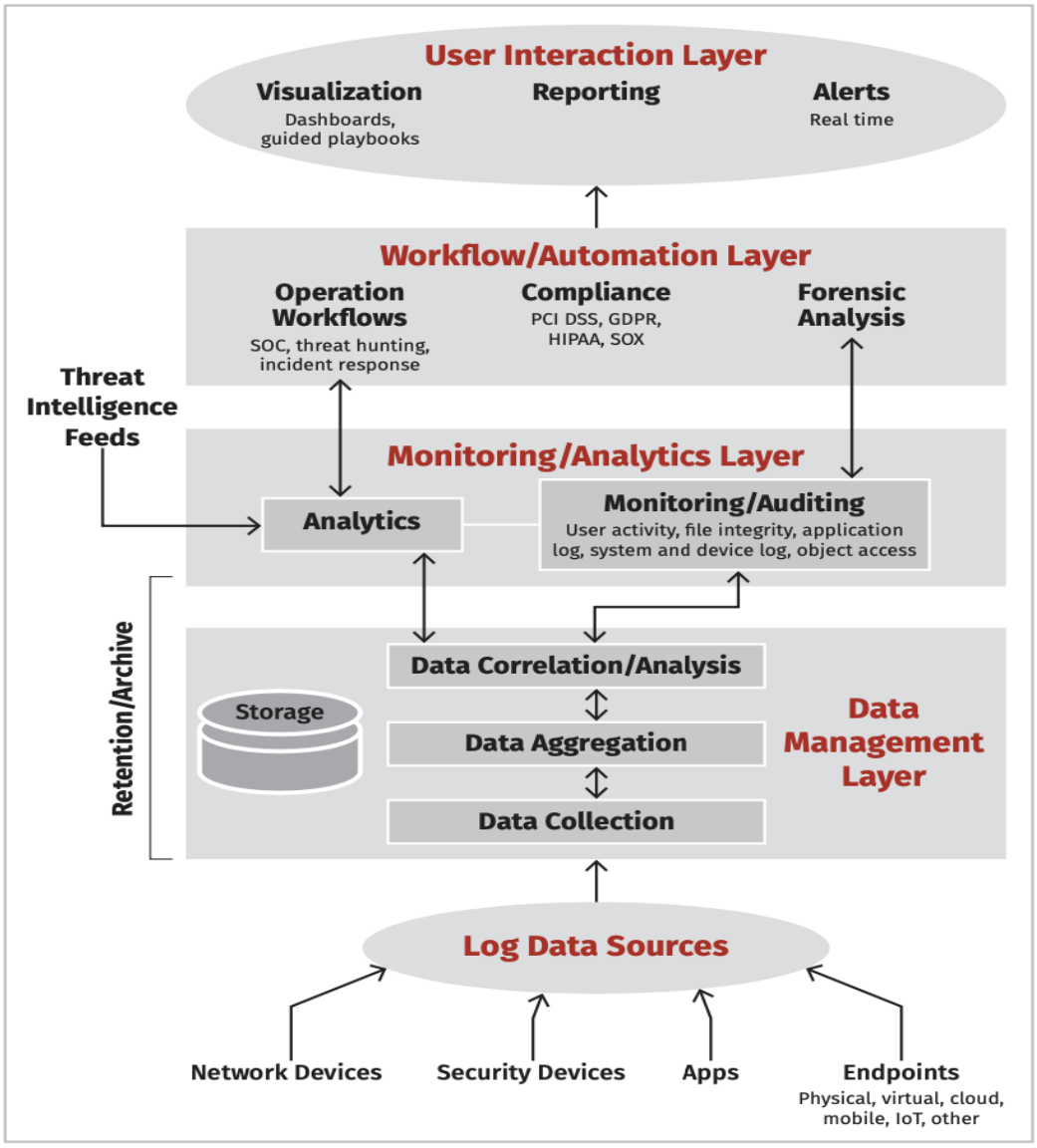

Figure 2 Next-Gen SIEM Architecture [11]

2.2 Requirement Definition

The defining requirements of the SIEM solution can be split up into two contexts. First market-driven requirements and second CYBERS specific needs.

Requirement definition used during the evaluation is based on the research performed by Hassan Mokalled, Rosario Catelli, Valentina Casola, identified in paper "The Applicability of SIEM solution: Requirements and Evaluation". Authors have identified and classified requirements for enterprise SIEM solution and divided them into five sections and three types. Definition is summarized in figure below.

Section	Type	Requirement
Platform	**Mandatory**	1. *Log Management System capability* 2. *Supporting an extended set of log sources* 3. *Customization of parsers/connectors* 4. *Method for retrieving events/flows/logs* 5. *Specification of the method for retrieving events/flows/logs* 6. *Hierarchical and modular/scalable architecture* 7. *Time-zones management* 8. *Platform computing capacity* 9. *Platform storage capacity* 10. *Installation model* 11. *High Availability/caching options* 12. *Availability of both default and customizable correlation rules* 13. *Dashboard features: ability to quickly prioritize response and analysis.* 14. *Customizable and compliance reports* 15. *Alerting capabilities* 16. *Technical documentation and online help* 17. *Ability of Monitoring the platform*
	Nice to have	18. *Multi-tenant capabilities (views)* 19. *Anonymization of logs*
Operations	**Mandatory**	1. *Role-based access control* 2. *Accounting: log events done by operators*

	Nice to have	3. *Customizable time-zones for the GUI*
Integration	**Mandatory**	1. *Active Directory integration for administrative management*
	Nice to have	2. *Integration with asset management tools* 3. *Case Management and trouble-ticketing activities tracking* 4. *Trouble ticketing module* 5. *Integration with vulnerability management tools*
Advanced features	**Nice to have**	1. *Threat Intelligence analysis tools support* 2. *Support for forensics analysis activities* 3. *Analytics support* 4. *Automatic response capabilities*
Licensing and support	**Mandatory**	1. *Specification of the preferred License type* 2. *Specification of the project Roadmap* 3. *Delayed license activation* 4. *Technical assistance support and professional services*
	Nice to have	5. *Technical assistance support and professional services* 6. *Training provided*

Table 1 Enterprise SIEM Requirements [14]

These requirements have been acknowledged and mapped to the needs and vision of CYBERS which in result has been applied as evaluation criteria during this work.

As a company that provides cybersecurity services to other businesses, the quality of our services at CYBERS is essential. With a client-oriented mindset, we demand the best solution on the market with advanced features and the possibility of integration since we utilize a wide range of security products, including vulnerability management and threat intelligence.

From general requirements, we target High Availability (HA) deployment options with priority. Each second, when the solution is experiencing issues or is entirely down, results in high risk and cost for enterprise as no visibility of security posture is available. Multi-

tenancy is optional but highly beneficial demand. As we provide security services to a broad range of business sizes, not all of them can afford dedicated solutions for their needs. Thus platform that can support multiple separated customers within a single environment gets an advantage from our perspective.

As an optional feature, we look into possibility from SIEM solution to match incidents against MITRE ATT&CK [19] framework, which is a joint knowledge base for adversary tactics and techniques providing common ground for investigation across multiple platforms and security products, easing up work of security analysts.

Based on the data observed in the past and estimation for future growth at CYBERS, we have defined technical requirements for SIEM solution:

- Handle up to 5,000 events per second
- Handle up to 2,000 Gb of incoming log data with 24 hours
- Retention policy of at least six weeks
- Retention policy for hot buckets of one month

As we are providing 24/7 Security Operations Centre as a Service (SOCaaS), support from vendors side at any point in time might be needed and will be treated as one of the requirement criteria when examining solutions.

Due to the requirements defined above, the scope limitations of this paper and targets of CYBERS in particular, only three enterprise solutions will be discussed in this document provided by IBM, Splunk, and McAfee.

3 Qualitative Analysis

Although the general flow of data and feature set might be similar across different solutions, which is caused by the nature of problems that solutions address, underlaying architecture is different. Understanding the structure behind the product provides greater visibility to a solution and points out the pros and cons of each approach.

This chapter focuses on analyzing architecture behind each solution examined and their feature set, pointing out benefits and drawbacks for each of them.

3.1 McAfee ESM

McAfee is one of the most prominent vendors on the cybersecurity market, producing many different security solutions for, including and not limited to, endpoint security, network security, database and server security, security analytics, and cloud security. McAfee's SIEM solution, formally known as McAfee Enterprise Security Manager or McAfee ESM, is one of the most advanced solutions on the market. Having products in different aspects of business security has resulted in ease of integration and communication between these products. For ESM, integration with McAfee products such as Threat Intelligence Exchange for file and certificate reputation within the environment, Global Threat Intelligence for global threat sensors, Network Security Manager as Intrusion Prevention System and a possibility for action automation within the integrated systems has resulted in cutting edge advancement for SIEM as a solution on integration part. However, evaluation of these products and their pricing is outside of the scope of this paper. Solution overview is based on version 11 of the product.

McAfee ESM architecture utilizes several appliances within the solution divided on the bases of functionality. Some of the appliances are optional and can be integrated within the different components, depending on the deployment option of the product. Others are core parts of the product and are required.

Components of ESM solution and their respective roles are described below.

1. ESM – Enterprise Security Manager is a core component providing a central console to the infrastructure. It utilizes online-database and provides a central configuration point to other components of the SIEM solution. It provides a web interface that acts as a gateway for using a product by security specialists, also providing storage for hot, normalized and aggregated data, which is used for views and dashboards in SIEM.

   ESM, which is Linux based component, can be deployed as a separate appliance on a dedicated server or a virtual machine (VM); or included in a combined

solution integrating Enterprise Log Manager (ELM) and Event Receiver (ERC) components. [20]

2. ERC – Event Receiver is a required component of the solution. Sole purpose landing on log collection and parsing. ERC communicates with third-party and McAfee products and applications to collect data using standard protocols i.e., rsyslog. It also normalizes and aggregates the data to forward it to ESM for use, as well as compresses the data and sends it to ELM for long term storage. Optionally it can perform local correlation of the data on a predefined correlation rule basis. ERC can be deployed separately on a dedicated machine, VM, or combined in a single unit with ESM and ELM.[20][21]

3. ELM – Enterprise Log Manager is a highly recommended component of McAfee ESM, focusing on long term storage of the data with the primary purpose of addressing compliance requirements. It does not have timing restrictions for data storage; retention policy can be configured and put in place. Data received by ERC is compressed first and then sent ELM for storage. The default compression ratio is 14:1, with options to reconfigure it and set to 17:1 and 20:1 ratio. It needs to be considered that an increased level of compression results in higher utilization of hardware, which may result in decreased performance for data processing. The data is digitally signed by ELM for proof of integrity, resulting in verification from the point of data collection. One of the drawbacks of the solution is storing the data without encryption. However, data is stored in none human-readable format.[20][22]

4. ELS - Enterprise Log Search is an optional component of the solution. ELS focuses on short term storage of uncompressed raw data that has been indexed for quicker search results. Technology is based on Elastic Search, a product developed by Elastic NV. [20][23]

5. ACE – Advanced Correlation Engine provides near real-time and historical event correlation. It utilizes both rule-based and risk-based approach for threat event scoring. Rule-based logic is a traditional way with preconfigured rules for correlating events and requires constant updates for signatures and is limited to the detection of known threat patterns. The risk-based approach utilizes reference

lists for high priority assets within the enterprise, tracking all associated activity and building risk score on real-time data on indexed fields such as source and destination IP and filename. ACE complements ERC's capability for event correlation with the possibility of a dedicated resource for the task, resulting in processing a higher volume of data and providing rule-less correlation additionally. It can supplement ERC in terms of correlation or completely take over the task. One of the more significant advantages of ACE is a historical correlation. When a new zero-day attack is explored, ACE has the capability to playback historical events to determine if an organization was exploited with this vulnerability in the past. Real-time correlation and historical correlation cannot run simultaneously. To tackle the issue two instances of ACE need to be deployed, one for historical and one for real-time correlation. [20][24]

6. ADM – Application Data Monitor is an optional aspect of McAfee ESM. It is a deep network packet inspection tool operating on the rule basis, matching them against monitored traffic as well as anomaly basis such as communication outside working hours and unusual protocol in use. It can investigate and retrieve data from packets such as source and destination addresses, protocol, file name, and type. There are limitations to ADM operation from encryption perspective; it can only apply deep inspection to unencrypted protocol traffic such as HTTP and FTP. [45]

7. DEM – Database Event Monitor, is an optional appliance targeting database activity from a security perspective. It performs event normalization and correlation, analysis, and reporting. It supports Windows, Unix/Linux, Mainframe, and AS400 operating systems and can infer data from major databases such as MySQL, PostgreSQL, Microsoft SQL Server, Oracle, and DB2. Currently, the DEM appliance has been discontinued by the vendor and functionality integrated in the McAfee Datacentre Security Suite product.[20][25]

Figure 2 illustrates the general overview of McAfee ESM organization and data flow.

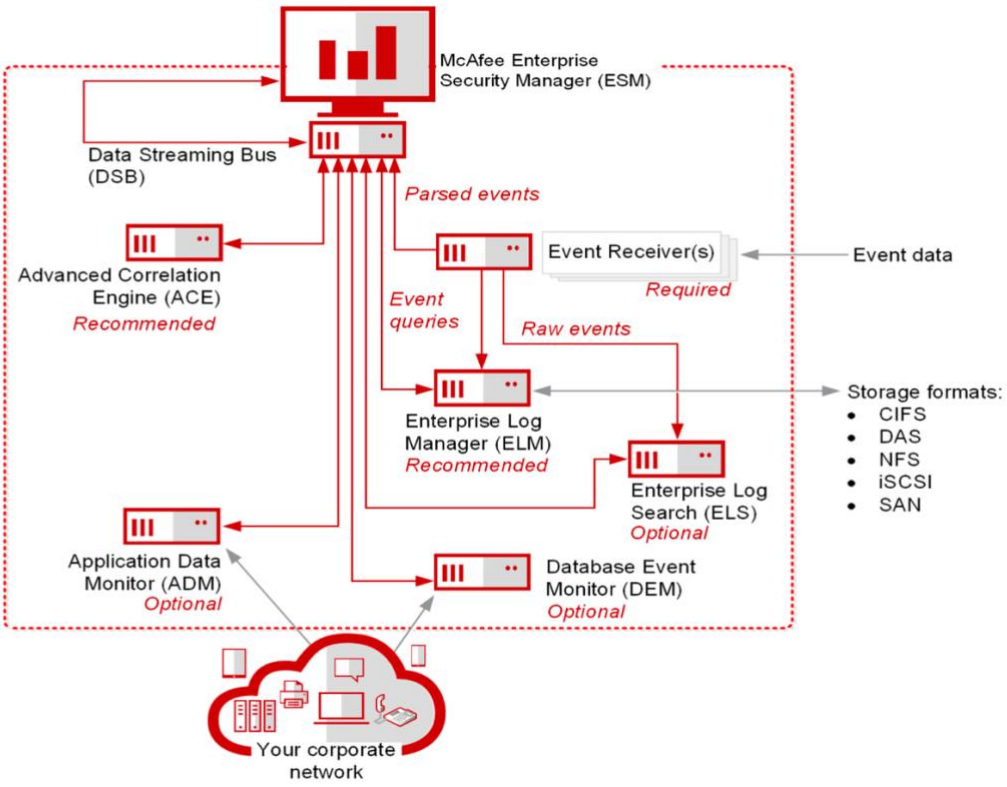

Figure 3: McAfee ESM [20]

With the version 11 of the software Kafka based data bus was introduced into the architecture. In previous releases, appliances were directly communicating with ESM introducing multiple single points of failure. Kafka data bus has the capability of storing the data for seventy-two hours, thus in case of any appliance outage, providing the possibility to re-ingest the data to the appliance. Initially, data is picked up by ERC and published to the data bus. Afterward, it is ingested to ELS for short term storage as well as ELM for long-term storage for compliance and forensics investigations. Ingestion of data to ELS and ELM can happen simultaneously. Next, data is transferred to Event Correlator for real-time in-memory analytics and pushes correlated data back to the data bus. Moreover, data can be shared with additional tool Advanced Analytics for User Entity Behaviour Analytics capabilities, which are based on Apache Spark, and processed data is ingested back to the data bus.

Figure 3 provides an overview of data flow with the utilization of Kafka-based Data Bus within McAfee ESM.

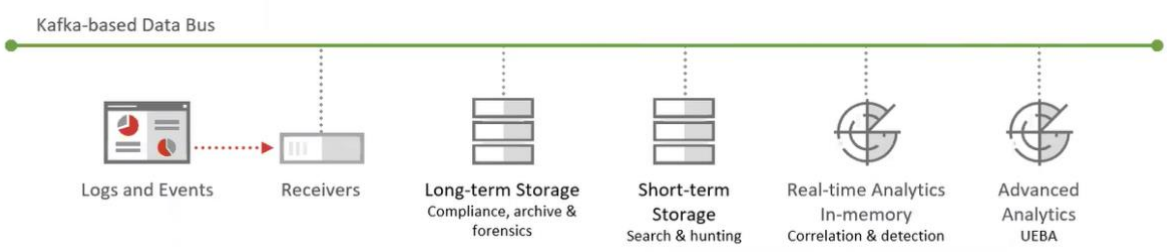

Figure 4: Kafka-based data flow

One of the main advantages of McAfee ESM is its database, formally known as EDB. Its development began back in 1979 with the sole purpose of addressing the needs of the SIEM and log processing market. With N-Tree sorting as underlaying technology, EDB addresses and fulfills all of the requirements dictated by the market, such as insertion of vast amounts of data in real-time, modification of stored data, and complicated queries on the data. With targets built into the underlying design of the solution, EDB gains overall advantage compared to other database systems approaches such as relational databases and flat file storage.[26]

McAfee provides content packs to enhance the capabilities of the SIEM solution. Content packs address specific use cases from a security or compliance perspective. They include correlation rules, reports, and pre-built dashboards and come with no additional cost to a customer. With version 11.3 of the product, the Mitre ATT&CK content pack was released. One of the most important add-ons is the User Entity Behaviour Analytics.[27][20]

User Entity Behaviour Analytics or shortly UEBA is an Artificial Intelligence-driven behavior analysis tool. Monitoring behavior analysis helps to detect credential compromise at an early stage, prohibiting attackers from lateral movement, privilege escalation, or data exfiltration before any damage is done, as well as preventing users from intentional or accidental malicious activities. McAfee UEBA content pack utilizes a rule-based approach, i.e., three failed login attempts within 5-minute window indicates on potential Brute-Force attack, as well as activity-based analysis, i.e., activity during

unusual hours for the account or unusual location of event originating source, and combination of two based on correlating of several events. Out of the box content pack addresses six security use cases, namely being Brute-Force Attack, Data Exfiltration, Account Compromise, Traffic Pattern Anomalies, Unusual Login Activities, Insider Account Misuse. In terms of addressing security surface for UEBA, McAfee's solution is quite limited; this has been pointed out by Gartner 2020 report, as well as acknowledged by McAfee. As an additional solution, the vendor offers integrations to third-party UEBA solutions based on Security Innovation Alliance. McAfee has teamed with and provided direct integration with dedicated UEBA products vendors such as Interset, Exabeam, Fortscale, and many more.[27][20]

To achieve high availability within McAfee SIEM configuration separately for appliances of product needs to be put in place. McAfee supports the HA option only with physical appliances. For ESM and ELM, redundancy configuration has to be put in place primary and standby state approach for each component. For ERC, HA options need to be set up with the primary receiver required to have three or more Network Interface Cards.[20] The solution does not support multi-tenancy out of the box. However, it can be achieved by logically separating appliances within architecture on a tenant basis.

Security Innovation Alliance or SIA is McAfee's ecosystem for partnership with other vendors easing direct integration with their products. For McAfee ESM, there are around a hundred and thirty partners, the majority of which provide direct integration with the solution. Some of the partner vendor products are Splunk Phantom, Demisto Enterprise, and Proofpoint Email Protection.[20]

3.2 IBM QRadar SIEM

IBM is one of the oldest and most respected companies within the Information Technology industry. Being around since the early 1900s, IBM has enhanced the world of IT and its development with products such as FORTRAN for scientific programming and Structured Query Language or SQL, which is a huge part of modern days relational database management systems (RDBMS). The technology giant has influenced the market of security as well.[28]

IBM QRadar is a family of products that are powered by IBM proprietary Security Intelligence Operating System – SIOS. The product list contains QRadar Vulnerability Manager for network scanning and vulnerability detection, QRadar Advisor with Watson, QRadar User Behaviour Analytics, QRadar Risk Manager, QRadar SIEM, and many more. Having a shared basis for different products results in ease of integration, scalability, as well as simplicity by delivering multiple functions and products within the common user experience. QRadar SIEM is based on componential division with each component of a solution built with a modular approach, where a specific module is responsible for specific functionality. Solution overview is based on a 7.3 version of the product. The architecture of the solution is described below.

1) QRadar Console - is a central part of the solution providing a user interface, asset information, dashboards, reports, offenses[1] as well as administrative functions. In a distributed solution environment, the console is used to manage other components of SIEM. In all-in-one scenario console is responsible for collecting, processing, and storing the data. It is utilizing PostgreSQL for storing offense, asset, and identity information; it acts as a master database with optional copies deployed on Event Processors (EP) for backup and automatic restoration. Console receives data from EP. First incoming data passes through Overflow Filter that ensures that incoming data stream meets licensing restrictions. If the number of events or flows coming in exceeds licensing terms, they are stored in Overflow Buffer. Usually, in the QRadar environment, overflow buffer has 5GB capacity, and stored data gets processed as incoming Events Per Second (EPS) and Flows Per Minute (FPM) numbers drop below the licensing threshold. If the buffer is full incoming events are dropped, and the specific event is generated for the administrator. Next events that have been marked for further investigation or generated offense are passed to the Magistrate component. It correlates events across event processors. Magistrate instructs Ariel Proxy Server, which is part of the console, to gather information from Ariel Query

[1] Offense – QRadar refers to security incidents as offenses

Servers residing in Event Processors about all events and flows that triggered the creation of an offense. Anomaly Detection Engine (ADE) is also part of the console; it searches the accumulator module on Event Processor for possible anomalies. ADE uses three types of rules:

- Threshold rule – examines numeric range such as large outbound data transfer
- Anomaly – change in behavior when compared to longer time frame i.e., new service activity
- Behaviour – difference from the same time during the previous day or week i.e., backup process issues

Lastly, Vulnerability Information Server is responsible for maintaining an asset database. [29][30][31]

2) EP– Event Processor is a mandatory part of the solution. It contains an engine for both event and flow processing, but the flow processor can be deployed as a separate appliance. EP processes events collected from Event Collector, Flow Collector, or other event processor components within the environment. Each event processor uses local storage based on Ariel database to store event and flow data with assurance for tamper-proof using hashing; optionally, storage can be delegated to Data Node. By default, stored data is not encrypted. However, it is possible to offboard storage with transparent to QRadar encryption, as an alternative specific data can be obfuscated with the use of regular expressions. Data can be selectively indexed for searching and reporting requirements. At the entry of data, overflow filter enforces EPS and FPM rates, similarly to console. Afterward, Custom Rule Engine tests data against enabled rules in QRadar Console, in case of a match, an offense is created, and predefined action within the rule is executed. Multiple events can be correlated into a single offense, and on the contrary, a single event can be part of multiple offenses. If a new identity or host is detected from incoming data, the Host Profiler sends information to Vulnerability Information Server on the console for storage. Each event processor within the environment uses Accumulator to accumulate events every minute,

hour, or day. They create time-series statistical metadata that is used for improved performance of dashboards, reporting, and searches. [29][30][31]

3) EC - Event Collector is used to continuously collect events and normalize from remote and local data sources and forward them to the event processor. Forwarding can be scheduled as well. First, similarly to other QRadar components Overflow Filter module enforces licensing restrictions, with an overflow buffer size of 5 GB. EC performs source auto-detection with the Traffic Analysis module. Each incoming event is matched against Device Support Modules to resolve a log source automatically. Device Support Module can be implemented within the EP and Console as well. Finally, event Coalescing Filter bundles together identical events that were observed with 10-second intervals to save system usage and storage before forwarding events to EP. [29][30][31]

4) FC – Flow Collector or QFlow targets network flows for collecting. It supports NetFlow, jFlow, and sFlow out of the box as well as can gather data from the network interface directly. Flows are a combination of internet packets that have the same source and destination IP addresses, source and destination ports, and protocol. QFlow is not a packet capture tool; for sessions of flows that exceed one minute, it creates a record at the end of each minute with updated information regarding metrics. First, after flows are received, licensing terms are enforced. Flow collector utilizes Application Detection module, which matches flows to application layer based on several approaches:

    - User-defined – User can insert specific definitions for statically identifying and matching flow to application
    - State-based decoders – determines application by analyzing payload and flow behavior
    - Signature matching – string matching in the payload, supports custom signatures as well
    - Port-based matching – i.e., port 443 identified as HTTPS

There are two more optional components within SIEM architecture: QRadar Data Node and QRadar App Host. The data node provides storage and processing capacity to QRadar deployments. App Host is a dedicated managed host that provides with CPU resources and memory for running apps. Extensional applications such as User Behaviour Analytics are resource-heavy; thus, the possibility of separating them from the console is beneficial. When QRadar deployment resources are heavily utilized, Data Node and App Host highly contribute to the scalability of the solution by simply embedding them to existing architecture. [29][30][31]

Figure 4 provides visualization of architecture for QRadar SIEM (Flow Processor is augmented within Event processor).

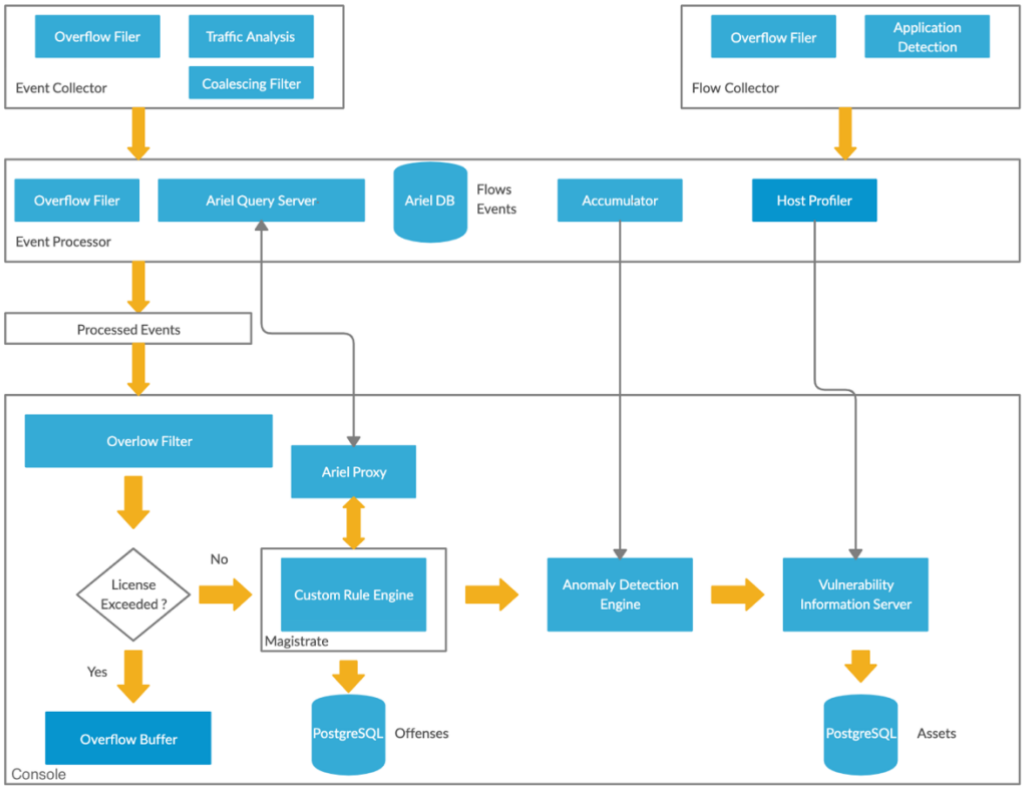

Figure 5: QRadar Architecture

In QRadar, data is stored in retention buckets with filtering applied to incoming events and flows. Retention buckets can be manually defined are being processed from top to bottom with default bucket at the end of the list. Starting from QRadar version 7.2, incoming data is stored for as long as possible no matter retention policy when placed in

default bucket. Custom retention buckets can be defined to force retention policy actions. [32]

From the Integration perspective, QRadar SIEM is easily integrated with other products developed by IBM as well as partner companies and software developed by third parties. QRadar also has RESTful API available, which provides an excellent advantage for the integration part. Requests can be made to endpoints, where each endpoint is dedicated to performing a specific function. [33]
IBM Security App Exchange is a platform where extensions and additional applications are available such as content packs for mapping offenses to MITTRE ATT&CK framework. QRadar User Behaviour Analytics (UBA) is a separate application available on the IBM marketplace that can be easily integrated within the SIEM solution. It comes with no additional cost when QRadar SIEM is purchased. It analyses behavior data comparing it to regular baseline activity as well as peer actions, triggering offenses, and generating risk scores for individuals. By default, only three rules are enabled: Unauthorized Access, Dormant Account Used, New Account Use Detected, with many more available out of the box. Each triggering rule has a value assigned to it, which contributes to the risk score of identity. QRadar analyses access and account traffic, application and endpoint logs, and network traffic for user and identity information enrichment. From 3.6 version of software support for multitenancy was introduced in UBA.[34]

IBM solution supports Hight Availability (HA) deployment options for both physical and virtual appliances with primary and secondary host approach combined into a cluster, where a secondary host is in the standby state and in case of primary host failure takes over the functionality of deployment.[35]
QRadar SIEM has capabilities to host multiple tenants in a single deployment. Domains are created for each tenant associating data sources to them and isolating tenant environments from each-other. For each tenant domain, specific rules can be introduced as well as retention policies and retention buckets.[36]

IBM SIEM licensing is based on incoming data rates. Licenses are separately purchased and enforced for EPS and FPM. Enforcement occurs on each stage of the pipeline in architecture as a single component can be receiving data from many others i.e., Event

Processor receiving data from multiple Event collectors and Console gathering information from multiple EPs, respectively.[37]
IBM provides exceptional documentation for each aspect of the product, which is a great advantage to understand the solution, deploy, and administer it.

3.3 Splunk Enterprise Security

Splunk Enterprise is a big data processing tool for gathering, parsing, indexing, analyzing, and visualizing the data. It utilizes apps and add-ons to expand the capabilities of the core product to meet specific needs. Applications contain knowledge-objects, configurations, pre-configured inputs, views, and dashboards. Splunk offers three premium applications that target the Security Information and Event Management platform capabilities. Splunk Enterprise Security is a core application for SIEM needs, Splunk User Behaviour Analytics enhances platform with machine learning models to detect anomalies within the behavior, and Splunk Phantom introduces orchestration and automation capabilities to the solution. As these premium products are built on top of the core part of the solution, underlaying architecture remains the same. Analysis is based on version 8 of the product.[38] The main components of Splunk are:

1) Forwarder - is a lightweight data shipper consuming data from a data source or another forwarder and passing it through to forwarder or more commonly to indexer. It breaks incoming stream into 64 KB chunks annotating each with metadata information about the host, source, character encoding, and target index. Splunk utilizes three types of forwarders:

    - Universal Forwarder
    - Light Forwarder
    - Heavy Forwarder

    Universal forwarders' sole purpose is data gathering and forwarding to the next destination in the pipeline. It has the lightest footprint on system resources and can run on various operating systems as well as in virtual and containerized environments. It cannot search or index data, and has no notion of events, it simply parses incoming stream and passes the data through to the next stage. Heavy

Forwarder, on the other hand, utilizes some functionalities of indexer, thus being able to filter, transform, route, and even index incoming data. Light Forwarder sits in between of the two, but Splunk has deprecated it with version 6.0. All forwarders support load balancing out of the box. They can send the data to the indexer or cluster of indexers changing specific destinations. Load balancing is achieved by time; in other words, how frequently forwarder switches the destination, the default value is 30 seconds, or by volume, how much data is sent to an indexer before switching. When a combination of both terms is used, a decision is made with whichever occurs earlier in point of time. Forwarder ensures safe delivery of traffic before switching, acknowledgment of data received can be configured as well. In the case of destination outage, forwarders utilize configurable buffer for incoming stream storage.[39][40]

2) Indexer – is responsible for transforming incoming data into events, processing, and storing in an index. Indexes in Splunk use buckets for storing data with bucket types being hot – read and write possibility, warm – read-only, cold, and thawed or restored from the archive. Bucket type change occurs automatically when the lifetime of the bucket has ended, or the maximum capacity has been reached. Once data is added to the index, tamper-proof assurance is put in place. Indexes use flat-file storage, and custom retention policy can be defined per index. In naming first and last timestamp of events is used for optimizing and achieving high-speed queries with time interval series and search deciding whether or not it should look into the bucket for a possible match. Indexers can be combined into clusters, where one indexer acts as a master node to manage the cluster, to achieve high availability automatic failover feature with data replication amongst them or ease of management. Splunk utilizes the anonymization of sensitive data such as credit card numbers based on user-defined rules.[42]

3) Search Head – is a core component in Splunk Enterprise architecture, providing a visual web interface to interact with solution and management capabilities to govern other appliances in architecture. Search heads can be combined into a cluster to achieve high availability with a minimum of 3 search heads in clusters as a requirement. They distribute search queries to indexers and consolidate results provided by each of them. Search heads utilize Splunk Processing Language (SPL), which, unlike typical search commands, can perform actions on

search results such as enrichment i.e., GeoIP lookup and calculation of statistical data. SPL is the main source of correlation of data in Splunk. With the addition of applications to core deployment, pre-defined correlation searches are added. Correlation searches look for patterns amongst distributed data sources; they can adjust risk scores and perform response actions.[41]

Figure 6 provides visualization for the general architecture of Splunk Enterprise.

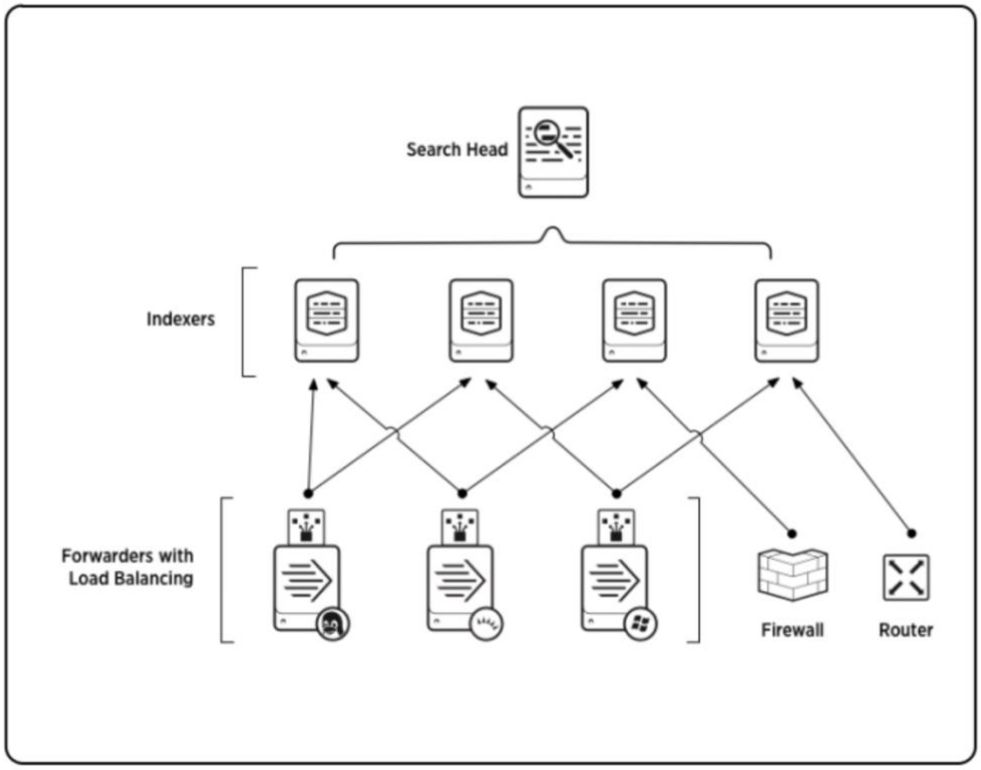

Figure 6: Splunk Enterprise Architecture [42]

Splunk Enterprise licensing is based on the volume of raw data indexed during a single day, summary indexes, internal logs and are not considered in calculations. In case the incoming amount exceeds licensing, terms warning is generated, and if subsequently five warnings are accumulated in 30 days, license violation is triggered.

Splunk Enterprise Security (ES) is a premium app that adds security mindset to the core component of the solution. SIEM solution approach from Splunk's perspective is analytics-driven. It ships with pre-configured correlation searches for malicious activity detection, which can be applied to real-time incoming data as well as scheduled to scan

matching patterns on historical events. When a match is found, notable events are generated. Enterprise Security includes dashboards and views for working with notable events, directing the investigation process, and easing the work of security analysts. Additional add-on license has to be purchased to utilize Splunk ES with the same amount of data as for Splunk Enterprise.[43]

Splunk Enterprise support for distributed environment setup and HA out of the box can be considered as a great advantage. Multi-tenancy within the solution is also supported. Additionally, User Behaviour Analytics add-on can be integrated into the platform; however, the license for it needs to be purchased separately.

Splunk provides with REST API interface, providing the capability to access, delete, create, and update resources to integrate the platform with third-party solutions manually. SplunkBase is a marketplace for apps and add-ons provided third-party sources as well as from the vendor itself. One of the notable apps is MITRE ATTACK for ES for mapping notable events and rules to corresponding techniques and tactics.

4 Hardware Requirements

This chapter points out the hardware requirements needed for each solution discussed. Metrics are based on the needs of CYBERS defined in chapter two of this paper. For calculation of hardware needs, manuals, and guides for solution deployment have been used. During the assessment, consulting has been conducted with each vendor of the solution.

Hardware requirements are summarized in Table 1.

Table 2 Hardware Requirements

	McAfee ESM	**IBM QRadar**	**Splunk ES**
HA requirements	N/A	Minimum Number of Nodes – 2 with an all-in-one appliance Link speed between nodes 1Gbps	Minimum Number of Nodes – 4 (Master Node, Search Head and two Indexers)
CPU Cores Per Node	ESM: 12 ACE: 8 ELM: 8	Minimum number:16 Recommended: 24	Master Node: 12 Search Head: 16 Indexer: 16
RAM per Node in GB	ESM: 32 ACE:16 ELM: 16	Minimum number:32 Recommended:48	Master Node: 12 Search Head: 12 Indexer: 32
Storage IOPS	3.6 TB N/A	5.6 TB 1200 IOPS	5.6TB 1200 IOPS

For hardware requirement analysis, only virtual appliance options where considered, thus HA for McAfee is not applicable. Additionally, only mandatory components for each solution were targeted.

5 Comparison Summary

This chapter provides with comparison summary where each product has been taken to head-to-head analysis based on key aspects of SIEM solution. These aspects were defined on the ground basis of comparison criteria identified in chapter 2 of this paper.

5.1 Gathering Data

Data gathering is one of the key aspects for SIEM solution, being able to retrieve information from various data sources easily aligns with the principal target of the platform to have clear visibility of IT infrastructure. Possibility to gather data using a variety of network protocols ensures that any kind of data source can ingest data to the SIEM platform. However, having dedicated data shippers eases setup and administration process, as well as optimizes collection. All three products provide with endpoint agents, but the IBM agent can be deployed only to the Windows operating system. In contrast, McAfee and Splunk solution can be set up on Linux machines as well, with Splunk universal forwarder having native capabilities to support a wide variety of Unix based systems out of the box.

5.2 Customization and support

All three vendors have demonstrated high quality of solutions with strong core capabilities. No matter the strength of the solution, to meet the needs of a specific environment, customization of a solution is needed. Products have strong capabilities in terms of customizability; within them, custom dashboards and views can be created, as well as specific alerts and actions defined. They support the definition of custom parsing rules in case log source data is not suitable for built-in ones.

SIEM tools are very complicated and challenging to implement and administer, thus help from vendors is crucial. The first key point in terms of support falls on to documentation. In these terms, IBM has demonstrated exceptional quality in terms of visibility of product architecture and feature set as well as guides and instructions for implementation. McAfee has remained strong, whereas Splunk demonstrated less visibility within architecture. All three of them provide with support person when a license is purchased, additionally having support pages, webinars, and certifications to raise knowledge and skills of customers.

5.3 Licensing

Although licensing has no role in functional capabilities for the SIEM platform, it is undeniably one of the critical aspects to consider when deciding on a solution vendor.

Licensing terms offered by Splunk have preferences from the client's perspective. As billing is done on the basis of the amount of data processed during the day, it eliminates licensing overflow during incoming data peaks. Data distribution is not uniformly spread during the monitoring period; rather, it is more densely populated in certain aspects such as working hours. Licensing offered by McAfee and IBM is based on EPS rates; thus, peak case scenarios might exceed license numbers, whereas low activity period numbers will fall way below them. It needs to be considered that in the case of Splunk, the additional fee needs to be paid for add-on Enterprise Security to get SIEM capabilities. Thus, although Splunk’s approach might seem preferable, it might result in overall higher price compared to IBM and McAfee.

5.4 User Behaviour Analytics

User Entity Behaviour Analytics has become one of the critical advantages of SIEM solutions compared to traditional defense products. Possibility to analyze behavior data with historical and peer analytics as basis unveils threats and indications of compromise that would not have been visible otherwise.

Both McAfee and IBM provide with UEBA solutions free of charge when core product is purchased, whereas Splunk UBA requires additional add-on purchase. From an effectiveness perspective, McAfee falls short to the peer's solutions with the possibility

to utilize only a certain number of use-cases. On the other hand, the solution offered by Splunk and IBM is more mature by nature. Overall based on two factors mentioned above, the IBM offering can be considered as preferable.

5.5 Integration

There is no one single product that can tackle all the challenges within cybersecurity space; thus, integration with other tools and solutions is essential.

All three products have shown excellent capabilities and maturity in terms of integration. They support REST API making custom integrations easier as well as have dedicated marketplaces for third-party software integrations. However, Splunk still falls short, coming from the analytics market, as both McAfee and IBM are huge players in the cybersecurity market, they have developed various products targeting different aspects of the field. Direct integrations with their essential products, such as Threat Intelligence solutions, provide an excellent advantage for the SIEM products as well.

5.6 High Availability and Multi-Tenancy

Assurance of failover proof is one of the critical aspects of any Information Technology service or solution. IBM and Splunk product, with their distributed solution architecture, supports high availability out of the box for both virtual and physical deployment options. In contrast, McAfee handles the problem only with a physical deployment option restricting customers with the option to use virtualization when HA is in demand.

Multi-tenancy cannot be considered as must-have functionality, as most of the customers of SIEM products target dedicated single business use. In this particular case, in terms of CYBERS, functionality was overlooked as an optional but highly preferable option. IBM supports multi-tenancy out of the box, whereas in Splunk and McAfee, it can be achieved with complex configuration and separation put in place, giving an edge of advantage to IBM.

5.7 Storage Options

Storage architecture for SIEM solutions is a crucial aspect as they perform advanced processing on vast amounts of data, generate reports, and feed dashboards. In terms of storage, a solution advantage can be given to McAfee with its dedicated database optimized for the product. Nevertheless, both IBM and Spunk utilize optimization and indexing of the data to achieve high rates in storage and search functionalities.

6 Conclusion

Based on the detailed overview of Security Information and Event Management solutions, deep dive into their architecture, feature set, and licensing terms decision has been made within CYBERS. As a result of the conducted research, the company has decided to favor the IBM solution as it exceptionally meets SIEM platform requirements and CYBERS' specific needs. QRadar SIEM has been rolled out into a production environment with multi-tenancy and high availability features included in the deployment. Currently solution hosts several customers and provides vision to their security posture and assurance of protection of cyber threats and actors.

7 Summary

Aim of this work has been to analyze Security Information and Event Management solutions for the enterprise market, identify key features and capabilities of modern SIEM solution, define comparison criteria and perform a comparative analysis of selected products. Research has been conducted based on the needs of cybersecurity company CYBERS, and as a result, the selected product, IBM QRadar SIEM has been implemented within the company for use in a production environment.

Paper provides an overview of the situation in cybersecurity and SIEM market. As a result of this work, the core capabilities of SIEM solutions have been identified, defining comparison criteria when product assessment is conducted. Detailed overview of solutions provided by McAfee, IBM, and Splunk listing their fundamental capabilities and mapping them to their architecture to define how they are achieved is discussed. Solutions from the vendors mentioned above were taken into head-to-head comparison to identify the most suitable one for the needs of the current market and CYBERS in particular.

During the work on research, the author has analyzed official documentation for solutions provided by vendors, got acquainted with researches of security professionals, and market research reports as well as conducted consultations with McAfee, IBM, and Splunk.

Work aids security specialists and organizations in making decisions for a suitable solution for their business requirements. It guides through the evaluation process and provides in-depth information regarding solutions discussed, defining the basis for future comparison and evaluation.

8 Further Development

Security Information and Event Management platforms are evolving and developing constantly. This work has targeted core components of solutions, which mainly are not subject of change in the field of Information Technology. Nevertheless, in case major modifications in any of the solutions discussed comparison shall be re-evaluated. On a contrary, in this research not only specifics to a particular solution were discussed, but general requirements for SIEM as a platform identified easing future comparisons.

Due to the specific needs of CYBERS, our vision and experience only three products were examined during the work. In case of need, additional products from different security vendors should be examined. As a ground basis, comparison criteria defined in this work can be used.

Due to difficulties caused by pandemic in the entire world, author was unable to perform detailed practical analysis as was initially planned when work outline was defined. Although general practical assessment has been performed on solutions discussed using MITRE CALDERA tool, author decided not to include results in this paper, as it provided no substantial ground for differentiation between products. Performing detailed practical analysis, with the measurement of hardware utilization, detection timing of particular imitated attacks can be considered as a target to further development of this paper.

References

[1] M-Trends 2020 – FireEye https://content.fireeye.com/m-trends/rpt-m-trends-2020

[2] Gartner - https://www.gartner.com/en/about retrieved 25.04.2020

[3] SIEM Magic Quadrant 2020 – Gartner

[4] https://go.forrester.com/ - retrieved 25.04.2020

[5] The Forrester Wave™: Security Analytics Platforms, Q3 2018

[6] Nika Ptskialadze - "Comparative Analysis of Open-Source and Proprietary Security Information and Event Management Tools" 2019, Tallinn University of Technology.

[7] Solutions Review – Security Information and Event Management Buyer's Guide 2020

[8] CYBERS - https://cybers.eu/about-us/ retrieved 17.04.2020

[9] IBM Security - Cost of Data Breach Report 2019

[10] Cyber Kill Chain - https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html retrieved 17.04.2020

[11] SANS Institute - An Evaluator's Guide to NextGen SIEM December 2018

[12] ThreatQuotient - https://www.threatq.com/threat-intelligence-management-2/ retrieved 20.04.2020

[13] Recorded Future - https://www.recordedfuture.com/about/ retrieved 20.04.2020

[14] Hassan Mokalled, Rosario Catelli, Valentina Casola – "The Applicability of SIEM solution: Requirements and Evaluation", 2019, 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises

[15] Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot – "The Operational Role of Security Information and Event Management Systems", Hewlett-Packard Laboratories, 2014

[16] Oskars Podzins, Andrejs Romanovs – “Why is SIEM Irreplaceable in Secure IT Environment”, 2019, Open Conference of Electrical, Electronic and Information Sciences

[17] Marcello Cinque, Domenico Cotroneo, Antonio Pecchia – “Challenges and Directions in Security Information and Event Management”, 2018, IEEE International Symposium on Software Reliability Engineering Workshops

[18] Ferda Özdemir Sönmez, Banu Günel – “Evaluation of Security Information and Event Management Systems for Custom Security Visualization Generation”, 2018, International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism

[19] MITRE ATT&CK - https://attack.mitre.org/ retrieved 25.04.2020

[20] McAfee Enterprise Security Manager – Product Guide 11.3

[21] McAfee Event Receiver - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-F2806AF0-D729-48AB-8411-A89136188294.html retrieved 12.04.2020

[22] McAfee Enterprise Log Manager - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-EF96D160-8CB5-4740-9556-1DB7157EB319.html retrieved 13.04.2020

[23] McAfee Enterprise Log Search - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-EA6EBE09-FD6F-44F6-9A98-35D6C0C913CD.html retrieved 12.04.2020

[24] McAfee Advanced Correlation Engine - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-598930C9-3227-4412-B1E3-987052D7474A.html retrieved 12.04.2020

[25] McAfee Database Event Monitor - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-A6601AD2-5CE3-49A1-A43C-2A921B150D71.html retrieve 12.04.2020

[26] Security Information and Event Management Unique McAfee data management technology – White Paper

[27] User and Entity Behaviour Analytics for McAfee Enterprise Security Manager - White Paper

[28] IBM about - https://www.ibm.com/ibm/history/ibm100/us/en/icons/ retrieved 26.04.2020

[29] IBM QRadar Version 7.3.3 Architecture and Deployment Guide

[30] IBM Security QRadar Version 7.3.3 Administration Guide

[31] IBM Security QRadar Version 7.3.2 User Guide

[32] QRadar SIEM Ariel retention policy - https://www.ibm.com/support/pages/qradar-event-and-flow-retention-ariel-retention-qradar-720-and-later retrieved 25.04.2020

[33] IBM Security QRadar Version 7.3.1 API Guide

[34] IBM QRadar User Behaviour Analytics (UBA) app Version 3.6.0 User Guide

[35] IBM Security QRadar SIEM Version 7.3.2 High Availability Guide

[36] QRadar SIEM multi-tenancy - https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.3/com.ibm.qradar.doc/c_qradar_adm_tenant_mgmt_overview.html retrieved 26.04.2020

[37] QRadar SIEM license management - https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/c_qradar_adm_license_mgmt.html retrieved 26.04.2020

[38] Splunk Enterprise Overview 8.0.3

[39] Splunk Universal Forwarder Manual 8.0.3

[40] Splunk Enterprise Forwarding Data 8.0.3

[41] Splunk Enterprise Search Manual 8.0.3

[42] Splunk Enterprise Managing Indexers and Clusters of Indexers 8.0.3

[43] Administer Splunk Enterprise Security 6.1.1

[44] Mitre Caldera - https://caldera.readthedocs.io/en/latest/ retrieved 20.04.2020

[45] McAfee Application Data Monitor - https://docs.mcafee.com/bundle/enterprise-security-manager-10.2.0-product-guide-unmanaged/page/GUID-7C3C5F6D-2DAE-4985-B7D7-62C5217D9D0A.html retrieved 12.04.2020

[46] ResearchFox - Security Information and Event Management (SIEM) Market - Outlook (2015-19)

[47] NIST – “Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations”, 2011