

Diploma in Infocomm Security Management (DISM)



Security Policy and Incident Management

ASSIGNMENT 1

Module Name: Security Policy and Incident Management

Module Code: ST2610

Class: DISM/FT/Class: DISM/FT/2A/23

Student Name and ID: Urias Francis Paul John Bato (p2123222)
Shushant Shashwat (p2123602)
Marcus Wong Yu Xuan (p2123392)
Muhammad Amirul Adeeb bin Rizal (p2107095)

Table of Contents

1. Executive Summary.....	3
2. SIEM Products Evaluation and Assessment	4
2.1 Splunk Enterprise	4
2.2 IBM	9
2.3 RSA NetWitness	17
2.4 McAfee	23
3. SIEM Product Recommendation	31
3.1 Recommendation.....	31
3.2 Indicators of Compromise.....	32
3.3 Rules implemented to detect a possible compromise	33
3.4 The Government Recommendations	35
3.4.1 Who are The Cyber Security Agency of Singapore	35
3.4.2 What is a Singapore Common Criteria Scheme?	36
3.4.3 The Benefits of Singapore Common Criteria Scheme?	36
3.4.4 Which products are being listed?	37
4. Conclusion.....	37
5. Appendix	38
6. References	40

1. Executive Summary

Security Information and Event Management (SIEM) products are an integral part of any organisation; they help to provide a platform for detection, analysis, and incident response to allow for real-time analysis of alerts and logs generated by applications and network hardware. SIEM products also help to facilitate the work of administrators and enable quick monitoring of whole organisations. Due to the high demand for SIEM products, there are many to choose from for an organisation. However, since there are so many SIEM products on the market, it may be difficult to decide which SIEM tool is the best for an organisation because of factors like organisation size and budget.

Therefore, this report will be identifying 4 different SIEM tools – Splunk, IBM, RSA NetWitness, and McAfee and evaluating them based on 5 criteria – Design, Architecture, Main Functionalities, Strengths, and Weaknesses; possibly adding other information that sets them apart from its competitors. After evaluating the products, we recommend using Splunk as we believe it is the most suitable for Skrull Pte Ltd. Finally, based on Splunk's features, we will implement 2 rules to put in place to detect compromise based on 2 vulnerabilities that HP Networked Printers may have.

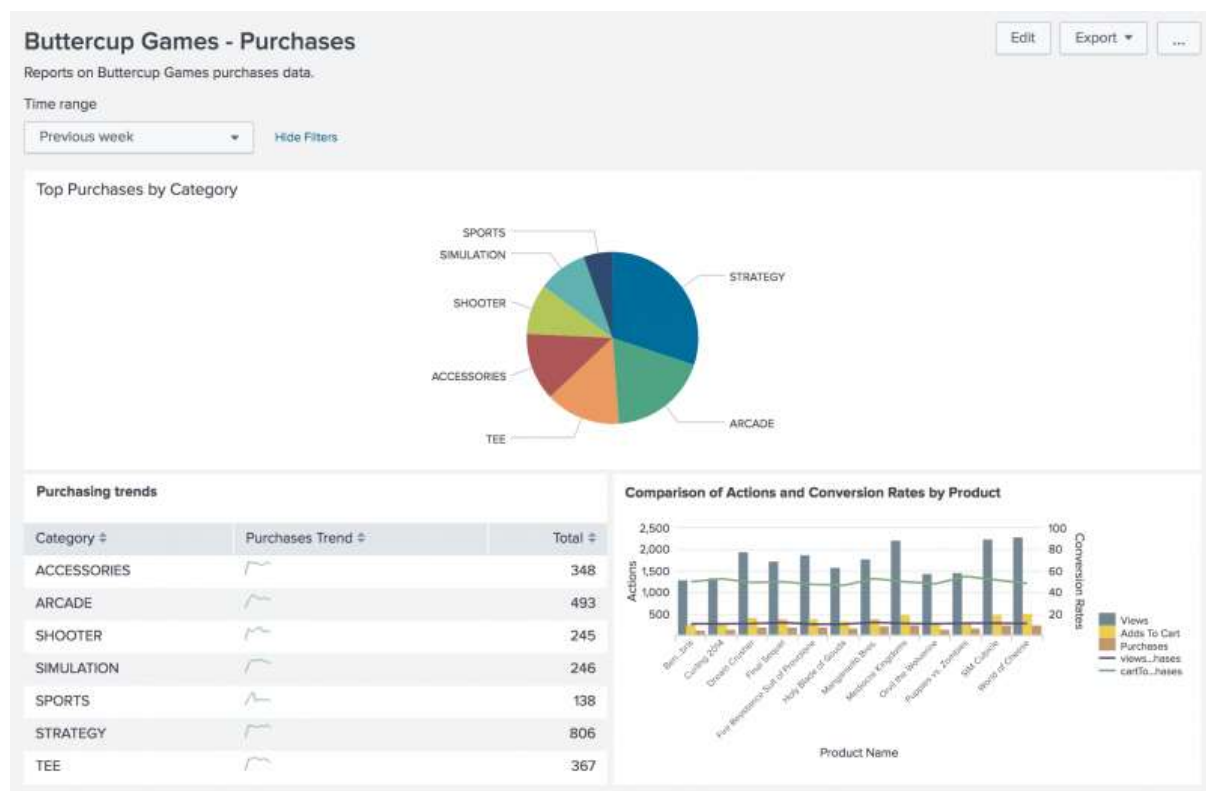
2. SIEM Products Evaluation and Assessment

2.1 Splunk Enterprise

The first SIEM product we will be evaluating is Splunk Enterprise Security, a component of the Splunk Enterprise platform. Splunk Enterprise Security is a data-centric, modern SIEM solution that helps to protect businesses and mitigate risks through full breadth visibility of data. The organisation Splunk Inc. was founded in October 2003, making it 19 years old in 2022.

Design

Splunk Enterprise Security utilizes its various functions and features to perform analysis and visualisation of large data. For analysis, data is captured from security devices to identify and address both known and unknown threats. For visualisation, data is presented in a pictorial or graphical format, such as charts and graphs. In terms of Splunk's user interface (UI), it is very intuitive and user-friendly.

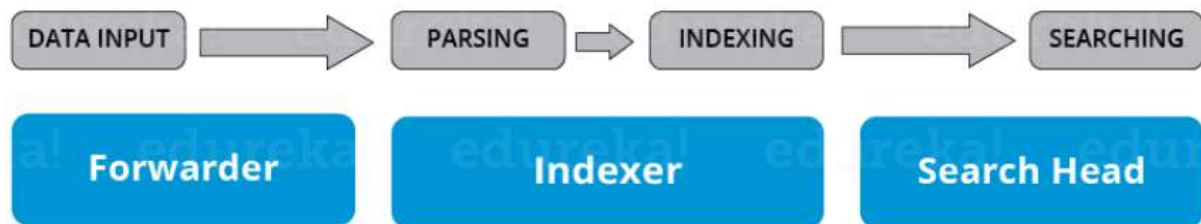


Having a very modern design, Splunk Enterprise is designed to be scalable to the business that it is used in. Splunk can dynamically change where it is deployed - be it locally on premise, cloud, or in a hybrid of both; depending on the growth of the business. Due to this, Splunk Enterprise Security can be used for organisations of all sizes; from Small and Medium-sized Enterprises (SMEs) to Multinational Corporations (MNCs). Being compatible with both Windows and Unix/Linux systems, Splunk is easily integrated into third-party applications from many vendors; some examples include Cisco and Amazon Web Services.

Architecture

Splunk Enterprise supports both Windows and Unix/Linux systems and can be run on a single server if the organisation is small and has no need for multiple servers. However, to run a single server effectively, the following minimum system requirements are needed: CPU Cores – 8 Physical or 16 vCPUs, CPU architecture – x86 (64bit), Network speed – 10Gb/s, Storage – 1TB.

On the other hand, for larger organisations, using multiple servers may be more beneficial for speed and efficiency. When using multiple servers, tasks can be distributed between them as different components. The three main components in Splunk are Forwarders, Indexers, and Search Heads.



Forwarders are the components used for data input, typically for collecting logs; Splunk uses a proprietary tool called Splunk Forwarder which consumes very less CPU (~1-2%), can be scaled up to tens of thousands of remote systems easily, and collect terabytes of data with minimal impact on performance.

Indexers are the components used for parsing and indexing; helping to store the data coming from the forwarder. Splunk transforms all incoming data into events and stores it in indexes to perform search operations efficiently. The indexing processes are as follows: separating the data stream into individual, searchable events, creating or identifying timestamps, extracting fields such as host, source, and source, as well as performing user-defined actions on the incoming data. Splunk uses a proprietary tool called the Splunk Indexer, which provides additional benefits like data replication which means that Splunk keeps multiple copies of indexed data.

Search Heads are the components used for searching and interacting with Splunk. They provide a graphical user interface to users for performing various operations such as searching. A search head performs only searching while a search peer performs both searching and indexing.

In conclusion, the architecture of Splunk Enterprise for large organisations is made up of multiple servers made up of forwarders, indexers, and search heads.

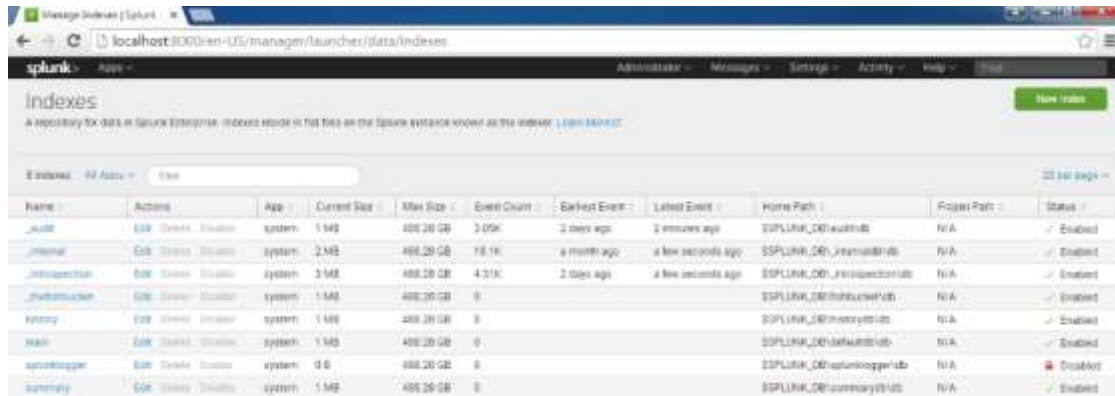
One optional component of the Splunk architecture is storage. Splunk can be configured to store data in the local storage of Splunk, in the file server within the network, in a remote system, or even cloud services like Amazon Web Services (AWS). For storing data in cloud services, Splunk provides a proprietary tool called Splunk Cloud Platform, which allows for Splunk's cloud services

Main Functionalities

Splunk Enterprise collects data from any source, including metrics, logs, clickstreams, sensors, stream network traffic, web servers, custom applications, containers, social media, and cloud services. Using this data, Splunk Enterprise can perform 6 functions: indexing, searching, alerting, data visualisation, reporting, and data modelling.

Indexing

The first function is indexing, which is Splunk's main log management feature, allowing other features like searching to work. When data is collected, Splunk Enterprise processes and indexes it. A Splunk Enterprise index contains a variety of files; split into two main categories: the compressed raw data, and the indexes that point to the raw data with some metadata files. These indexes facilitate flexible searching and fast data retrieval, eventually being archived.



The screenshot shows the 'Indexes' page in the Splunk web interface. It features a table with columns for Name, Actions, App, Current Size, Max Size, Event Count, Earliest Event, Latest Event, Home Path, Folder Path, and Status. The table lists several indexes including _audit, _internal, _introspection, _shrinkbuffer, _summary, _telemetry, _trunk, and _trunklog. Each row has a 'Status' column with a green checkmark and the word 'Enabled'.

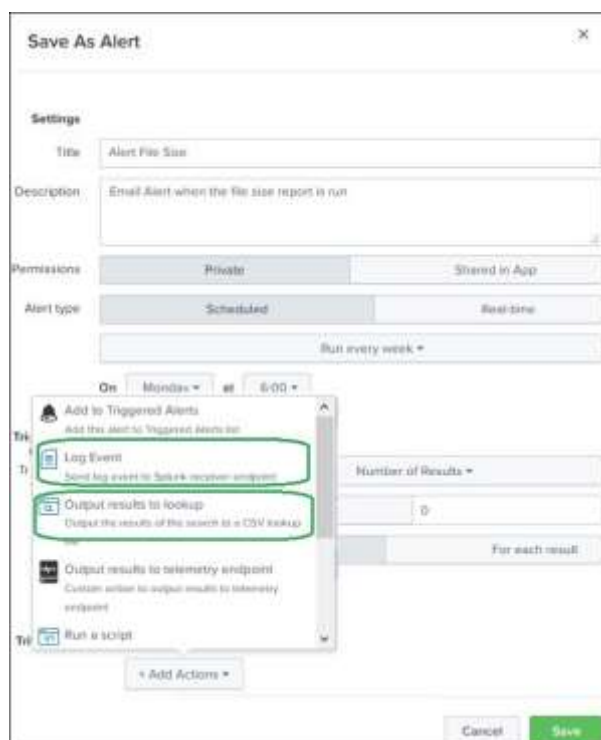
Name	Actions	App	Current Size	Max Size	Event Count	Earliest Event	Latest Event	Home Path	Folder Path	Status
_audit	Enable	system	1 MB	488.28 GB	3.05K	2 days ago	2 minutes ago	\$SPLUNK_DB/audit	N/A	Enabled
_internal	Enable	system	2 MB	488.28 GB	18.1K	a month ago	a few seconds ago	\$SPLUNK_DB/_internal	N/A	Enabled
_introspection	Enable	system	3 MB	488.28 GB	4.31K	2 days ago	a few seconds ago	\$SPLUNK_DB/_introspection	N/A	Enabled
_shrinkbuffer	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_shrinkbuffer	N/A	Enabled
_summary	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_summary	N/A	Enabled
_telemetry	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_telemetry	N/A	Enabled
_trunk	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_trunk	N/A	Enabled
_trunklog	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_trunklog	N/A	Enabled
_trunklog	Enable	system	1 MB	488.28 GB	0			\$SPLUNK_DB/_trunklog	N/A	Enabled

Searching

The second function is searching, which is the primary way users are able to navigate data in Splunk Enterprise through the help of indexes. Searches can also be used for other features like being saved to reports or used to power dashboard panels.

Alerting

The third function is alerting, which sends an alert to an administrator whenever past or present searches meet certain conditions that are defined by the configurations of the alert. Alerts can even be configured to perform various actions after being triggered like sending information to an email or running a script.



The screenshot shows the 'Save As Alert' configuration window. It includes fields for Title, Description, Permissions, Alert type, and a schedule. The 'Alert type' is set to 'Scheduled' with a frequency of 'Run every week'. The 'On' field is set to 'Monday' at '6:00'. The 'Triggers' section is expanded, showing a list of actions: 'Add to Triggered Alerts', 'Log Event', 'Output results to lookup', 'Output results to telemetry endpoint', and 'Run a script'. The 'Log Event' and 'Output results to lookup' actions are highlighted with green boxes. The 'Number of Results' is set to '10'. The 'For each result' checkbox is checked. The 'Save' button is green and visible at the bottom right.

Save As Alert

Settings

Title: Alert File Size

Description: Email Alert when the file size reports is run

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Run every week

On: Monday at 6:00

Triggers

- Add to Triggered Alerts
- Log Event
- Output results to lookup
- Output results to telemetry endpoint
- Run a script

Number of Results: 10

For each result

Cancel Save

Data visualisation

The fourth function is data visualisation, which gives voice to data; presenting them in a format that is easier to read. Splunk Enterprise provides many ways of data visualisation. The first way is through dashboards. Dashboards are customisable displays that integrate charts, reports, and reusable panels; allowing it to be edited for different audiences and use cases.



The second way is through pivot tables. Pivots provide a visualisation of data via methods like charts and graphs, which can be useful when looking and analysing entire organisations or departments. Using the pivot editor tool, we can create pivot tables, which we can add to the dashboard or save to a report.

Reporting

The fifth function is reporting, which allows user save pivots and searches as reports; they can also be added to the dashboard as a panel. Reports can be generated on a schedule or manually, as well as trigger alerts. Reports are stored in Splunk Enterprise by default.

Data modelling

The sixth function is data modelling, which encode specialised domain knowledge about sets of indexed data, enabling users of the Pivot Editor to create reports and dashboards without designing the searches that generate them.

Strengths

Overall, Splunk has multiple strengths; some supported by user reviews. After using Splunk, organisations have 82% reduced downtime, 70% lower risk of data breach, IP theft, and fraud, and 50% faster time to market for new apps. Many user reviews have highlighted the effectiveness of performing searches to find certain items. Users have also expressed the ease of security analysis of the machine logs collected. Overall, the strength of Splunk enterprise lies in its ability to do powerful searching and analysis while maintaining its ease of use because of its intuitive UI. In the 2022 Gartner Magic Quadrant, Splunk was named a “Leader” in SIEM products. Another strength is Splunk’s scalability that can be adjusted according to the business plan.

Weaknesses

Although Splunk has many strengths, it also has some drawbacks. One such drawback is the steep learning curve of Splunk expressed by users. For example, Splunk's dashboard is not as simple to use for beginners as compared to dashboards in other SIEM products. Another example that although Splunk's search queries are powerful, users need to learn Search Processing Language (SPL) to be used effectively. Another weakness that Splunk may have is that for large data volumes, Splunk can prove to be very expensive.

Others

As mentioned at the start of the Splunk overview, Splunk is a 19-year-old well-established organisation in the information security field, making it a trustworthy and reliable source to provide security. Splunk Enterprise Security has been named a "Leader" in SIEM products in the Gartner Magic Quadrant for 9 years in a row in 2022. In terms of market share, Splunk has the largest percentage at 30.25% of the SIEM market share according to the 2021 Gartner Market Share Report. Splunk has also received several accolades throughout the years; some of the most recent ones include Gold in the 2022 Silicon Data Awards in Cybersecurity, 2022 SD Times 100 in Security, 2022 CRN Big Data 100, 2022 CRN Security 100, a five-star rating on CRN's 2022 Partner Program Guide, and 2021 Fortune World's Most Admired Companies. In conclusion, due to Splunk's reputation with the cybersecurity industry and its users, it is a very reliable product that many organisations use as their first choice.

2.2 IBM

Design

IBM Security, formerly Internet Security System, is an information security provider founded in 1994 which was then later acquired by IBM in 2006 for a total of \$1.93 billion. IBM Security provides software services that focus on precautionary security solutions for businesses. IBM's new flagship security model QRadar, was originally developed by Q1 and then later acquired by IBM in 2011 and was designed to identify and analyse threats earlier in the attack cycle for the business to provide extra time to respond using advanced analytics and machine learning to detect suspicious events. IBM then further improved the system to as quoted by IBM "more intelligently secure their organization by applying analytics to connect information from major security domains and forming security dashboards for their organizations."



IBMs QRadar offers one of the most complete SIEM solutions and is targeted towards Linux Users and is designed specifically for Red Hat Enterprise Linux. QRadar is also designed for larger organizations and consists of a well-grounded platform used to build a corporate-wide threat detection and response system. It contains extensive blueprints and templates for simpler use cases. QRadar has a large deployment base and an extensive set of service providers that can help organizations procure, run, tune and monitor their deployments. QRadar is also designed to work with other IBM tools such as Watson AI. QRadar is made to reduce incident impact by responding to threats quickly due to insights into logs, events, and data flow. QRadar allows you to consolidate network flow data and low events from numerous devices, apps, and endpoints across your network.

QRadar also allows extensibility which includes the option to add extra services like the Security Intelligence Platform which builds around the QRadar SIEM and includes extra components such as Vulnerability Manager and Network Insights, which contextualizes event data with VM data and provide application visibility from network flows. QRadar is available as A hardware virtual appliance and software package based on the needs of the customer. QRadar is offered as on-premises hardware, software, or in the cloud. Smaller customers can offload all the deployment and

maintenance to an IBM cloud-based solution, while larger firms can choose either an on-premises or adopt a hybrid approach cto collecting data from local and cloud-based applications.

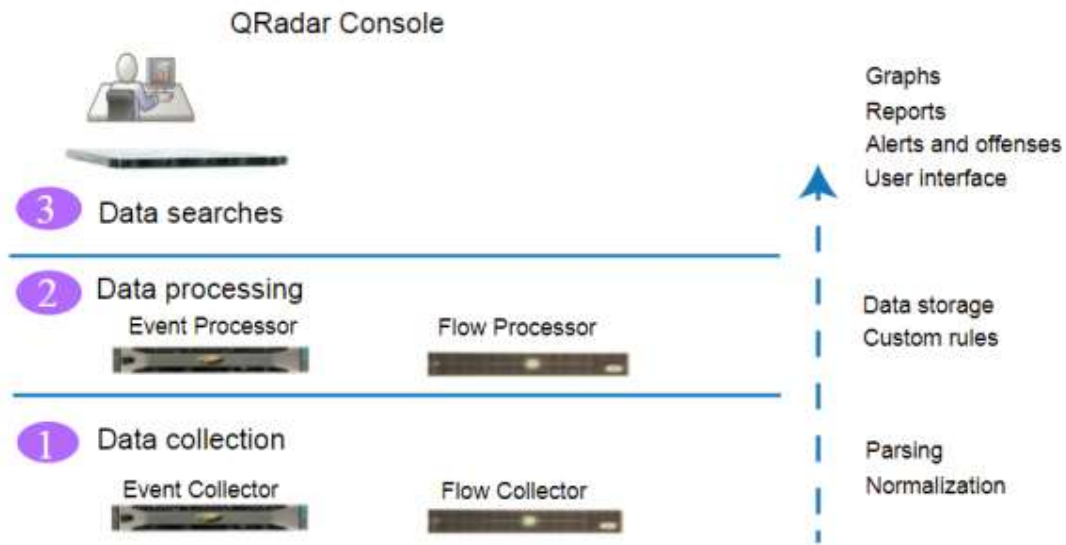


QRadar makes its service as simple to use as possible with the help of its All-In-One System which merges all of its services into one simple and effective Graphical User Interface (GUI) which manages and controls every service. All-In-One appliances can be used to collect the data directly from your network or you can use collectors such as QRadar Event Collectors or QFlow collectors to collect event or flow data.

Architecture

QRadar is a modular architecture that provides real-time visibility of your IT infrastructure, which you can use for threat detection and prioritization. QRadar security consists of three layers and applies to any QRadar deployment structure regardless of its size and complexity.

First is data collection where either QRadar's All-In-One Appliance or QRadar's QEvent Collectors and QFlow Collectors collect all of the activity flows and actions before the data are translated or normalized before passing it to the next layer. Translating and normalising the data is to make sure that the data is in an organised and usable format. The core functionality of QRadar SIEM is focused on data and flow collection. Event data represents events that occur at a point in time in the user's environments such as user logins, email, VPN connections, firewall denies, proxy connections, and any other events that you might want to log. Flow records is derived from receiving network activity information between two active hosts on a network. QRadar translates raw data into useful and proper information such as IP addresses, ports, bytes, packet counts, and other details into flow records which constitutes a session between two hosts. Full packet capture is available with QRadar Incident Forensics Component.



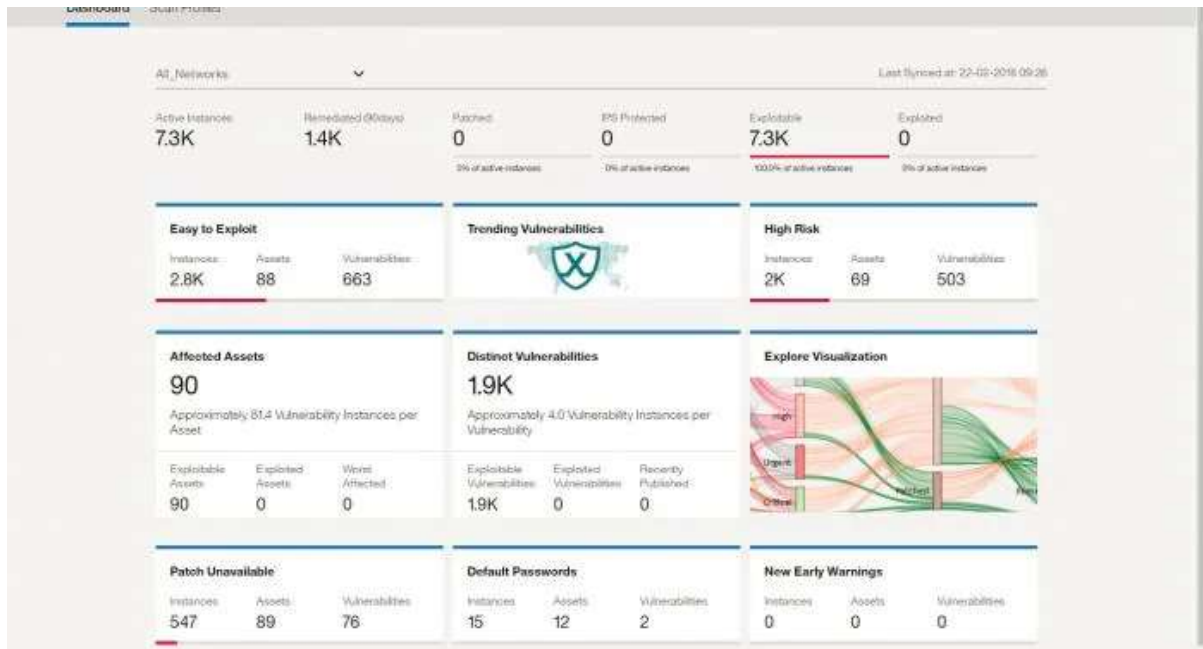
The second step is data processing. This is where event data and flow data passes through the Custom Rules Engine which creates offense and alerts before the data is written to storage.

The All-In-One appliance can process event and data flows without the need of additional Event and Flow Processors. Extra features for this step are also offered such as QRadar Risk Manager, QRadar Vulnerability Manager, QRadar Incident Forensics can vastly increase the capabilities of the system to collect and process different types of data to offer more functions.

QRadar's Risk Manager checks the configurations of your network infrastructure and computationally generates a map of your network topology. This will be vastly useful in that the data generated by the Risk Manager would be able to simulate the situations of your network and reduce the potential risks and damages the network could suffer from by simply changing a few configurations and rules in the network.

QRadar's Vulnerability Manager will also scan your network to receive information about the vulnerabilities of your network. This information can be used to find other possible security flaws in the network. QRadar's Vulnerability Manager can also be used to manage Vulnerability Data that is shared from other scanners such as Nessus and Rapid7.

QRadar's Incident Forensics can be run to carry out extensive forensic investigations and replay full network sessions.



In the third step, data collected by QRadar is accessible to users for various utilisations such as analysis, reporting and alerts. Users will be given the ability to search and manage security admin tasks from the QRadar Console.

In an All-In-One appliance, all of the data will be collected, processed and stored in the appliance.

In distributed environments, QRadar Console does not exercise event and flow processing, or storage. The QRadar console would be used for a User Interface for Data searches, reports, alerts and investigations.

One of QRadar's most attractive architectural designs is to be able to be deployed onto a single All-In-One appliance which offers users a simplified and centralised system where they can control and manage all of their services from just one easy system. However, this appliance is mainly designed for middle-sized companies and larger-sized companies can opt for a more advanced and larger deployment by incorporating other QRadar components, such as Flow Processors, Event Collectors and Data nodes.

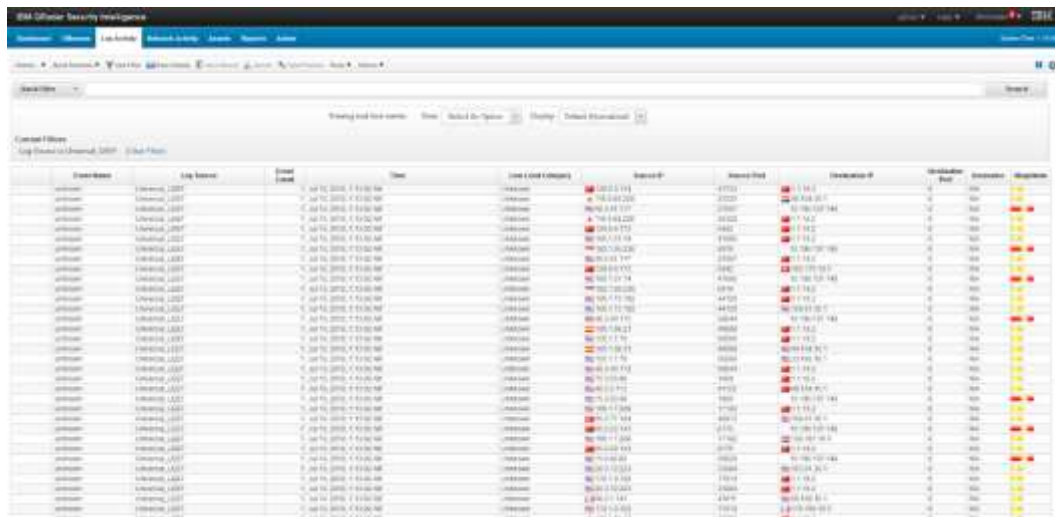
To host an All-In-One appliance, you can simply purchase the QRadar 3105 All-In-One appliance to collect, process and monitor the event and flow data. This system is suitable for medium-sized companies with less than 1000 employees. This appliance is able to process up to 5000 events per second and 200,000 flows per second. The All-In-One appliance also provides a web application where you can search, monitor and respond to security threats. Simply getting a QRadar 3105 will solve all of the extra worries and difficulties as it comes in an all-in-one package to save time and resources.

The specifications of the QRadar 3105 All-In-One appliance is stated as follows

- CPU : 2 x E5-2620 V4 2.1 GHz 8C 20MB 2133 MHz 85W
- Network Management Transceivers : 2 x 10 GbE Short Range SFP+
- Memory : 64 GB 2400 MHz DDR4 RDIMM
- Storage : 10 x 2.5 inch 1 TB 7.2 K rpm, 5.6 TB to store event and flow data

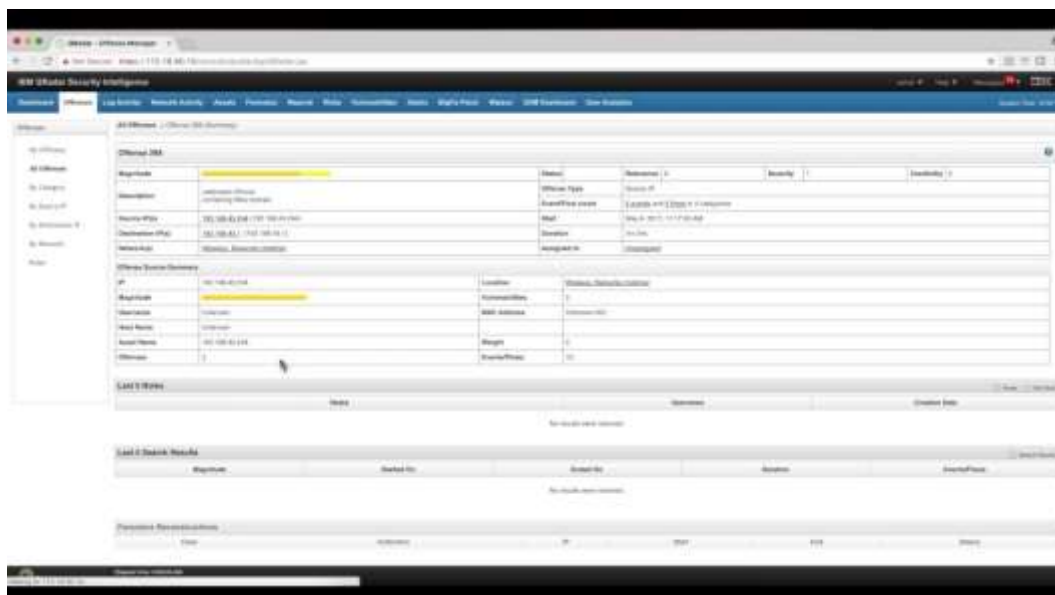
Main Functionalities

The main functionalities of QRadar include generating advanced alerts based on impact and severity. QRadar intelligently generates alerts and logs that are top of its class to allow the rest of the SIEM to more effectively operate and investigate the causes and scopes of possible attacks. From these logs, QRadar will be able to connect the entire chain of events and will start an investigation to detect the root cause and scope of the attack. They will also allow businesses to gain deeper visibility in user behaviour, endpoint activity, network traffic, and more. All of these features would be merged together into one platform for ease of use and can be managed from just one single computer.



The screenshot displays the QRadar console interface. At the top, there are navigation tabs for 'Overview', 'Alerts', 'Incidents', 'Reports', and 'Tools'. Below these, a 'Search' bar is visible. The main area shows a table of events with columns for 'Event Name', 'Log Source', 'Event Time', 'Event ID', 'Event Category', 'Severity', 'Impact', 'Classification', 'Status', and 'Assignments'. The table contains multiple rows of event data, including details like 'Log Source: 10.10.10.1', 'Event Time: 2018-10-10 10:10:10', and 'Severity: High'.

QRadar is used to mainly perform analysis of the log data and network flows in real-time so that malicious activities can be identified and stopped as soon as possible. QRadar targets a lack of actionable real-time security intelligence indicators, minimal endpoint visibility, no detection of abnormal activity. IBMs QRadar uses artificial intelligence to provide simple but effective risk assessments. SIEM offers a diverse system with countless functionalities for users to properly defend their systems and networks. QRadar's platform can be deployed in multiple forms such as an appliance, a virtual appliance, or an Infrastructure as a Service (IAAS) to become well-suited to various IT environments. QRadar's innovative prevention-focused approach and its ability to chain and link events together is unique and like no other SIEM.



The screenshot displays the QRadar console interface, showing a detailed view of an event. The top navigation bar includes 'Overview', 'Alerts', 'Incidents', 'Reports', and 'Tools'. The main area is divided into several sections: 'Event Details', 'Event Timeline', 'Event Analysis', and 'Event Summary'. The 'Event Details' section shows the event name, log source, event time, event ID, event category, severity, impact, classification, status, and assignments. The 'Event Timeline' section shows a list of related events. The 'Event Analysis' section shows a list of related events. The 'Event Summary' section shows a list of related events.

QRadar can collect logs from various different third party log sources such as syslog from the operating system, applications, firewalls, IPS/ SNMP, SOAP, JDBC for data from database tables and views.

Gain Comprehensive and centralised visibility

Traditional on-premises IT, cloud based and operational technology environments will need some oversight to properly protect, detect, and maintain. QRadars allows organisations to gain comprehensive and centralised visibility into protected environments by collecting and translating both log and flow data.

QRadar accomplishes this by having more than 450 pre-built Device Support Modules (DSM). This process is as easy as merely directing logs to QRadars. QRadars will then computationally find more information from the log and direct it to the correct DSM to normalise and translate the log into data. QRadars allows customers various choices of customisation options such as additional integrations of applications and also a DSM editor to enable users to define how they want to parse logs from their custom applications. QRadars can also help users to identify and classify assets on the network based on the services and applications that are necessary to the users.

Another major selling point of QRadars is its centralized data system which allows all of its activities to be linked together to generate reports on potential threats and risks that may lead to severe consequences.

Detect anomalous network, user, and application activity

As attackers become more creative and intelligent in their approaches, new forms of attacks are created nearly every day thus traditional known threat detection is no longer enough to fend off and against these attacks. Organisations must be given the ability to detect slight changes in the network, user or system behaviour. This may be hints to unknown threats. QRadars contains multiple kinds of anomaly detection to detect changes that may lead to unknown threats. QRadars also offers the ability to monitor and analyse Layer 7 application traffic to more effectively detect anomalies.

By using the QRadars Network Insights, organisations can now gain a more in-depth view of which systems communicate with one another. This correlation of information can help security analysts to expose unique activity that may be attempts of attacks. QRadars also offers the feature of allowing security analysts to modify and add rules to further help detect anomalies.

Automation of intelligence to effectively detect threats

QRadar is designed to automatically examine and link activity across all of its data sources which includes events, logs and user activity to find and prevent potential risks and problems.

QRadar involves hundreds of pre-built security use cases, for anomaly detection algorithms, rules, and correlation policies to discover threats. Everything in QRadars is automatic and this increases the users' ease of use to reduce errors and potential missed points. Prioritisation of threats and vulnerabilities is also automatic, and this will greatly ease the users' work as they now know which threats and risks are more important to target first. Thus, security analysts will now be able to more

effectively respond to all of their threats and vulnerabilities by dealing with the more important ones first.

Easily scale with changing needs

Another one of QRadar's largest selling points is its flexibility, scalable and massive number of customisation options to support organisations of all sizes and their needs and requirements. Due to QRadar's intelligent architectural design, QRadar is able to accommodate companies and organisations of all sizes where small companies can simply get the All-In-One appliance to begin with and slowly expand as their demands increase. All of its solutions are also being offered in various different options from hardware to software and even in the form of virtual appliances.

QRadar also offers ease of worry in where it offers high availability and disaster recovery protection when needed to ensure continuous operations. QRadar's disaster recovery solutions can forward live data, such as flows and events from the primary system to another in a separate facility.

Better manage compliance with pre-built content, rules, and reports

QRadar offers transparency, accountability and measurability which are some critical points for an organisation's success in meeting regulatory mandates and compliance. QRadar offers hundreds of pre-made reports and rules templates to help ease the jobs of organisations. QRadar also allows for the grouping of business functions to further help teams report on activities,

QRadar has the experience and resources required for organisations to convey their risk and regulatory exposures.

Strengths

You can add integrated modules to your QRadar platforms such as Risk Manager, Vulnerability Manager, and Incident Forensics which give QRadar an option to expand its services to suit your needs and a variety of customizations. You can scale QRadar to meet your log and flow connection, and analysis needs. These customization options provide QRadar with an edge over other SIEMs who are much more stubborn.

QRadar collects, possesses, aggregates and stores network data in real time. QRadar offers a one-of-a-kind set of functions that can help the user manage their logs easily and efficiently. (application, compliance, network overview, risk, system, and threat monitoring). QRadar uses that data to manage network security by providing real-time information and monitoring, alerts and offences, and responses to network threats. IBM's integration of its Watson AI also greatly improves and increases the performance of QRadar and its ability to link and chain events that may lead to potential malicious attacks.

QRadar offers complete visibility for the cloud and traditional environments which allows you to gain a centralized insight into the network events and data flow as it can be difficult to get insight across multiple security environments.

QRadar also offers real-time threat detection with its out-of-the-box analytics which investigates the network flows and logs to detect threats and prioritizes general alerts and forces the attacks into a kill chain.

QRadar also gives great security and reporting capabilities that can identify URLs and IP addresses that are associated with malicious activity and also a report builder wizard for security teams to create custom reports.

Another capability of QRadars is its ability to integrate with other third-party applications. QRadars can provide an API platform that can be used to build even more robust extensions to further elevate the performance and uses of QRadars.

QRadar is also definitely trustable as it is developed by tech giant IBM.

Weaknesses

Firstly, one big weakness of QRadars is in the price of the solution. QRadars mainly caters to larger companies with a significant number of systems and computers, thus a smaller business with little amounts of systems and computers would find this solution and SIEM a large price to pay for.

Another limitation of QRadars is that it is only operatable in RHEL or Red Hat Enterprise Linux, which makes it very limiting and only Linux-trained employees would be able to operate and maintain the SIEM in the system. Thus, Windows-based systems that are looking to get the QRadars would have to make significant changes to their systems to incorporate QRadars into their business. Getting a Virtual Machine or just changing your whole Operating System for the QRadars Manager would be inevitable and hiring employees experienced in Linux would be necessary.

QRadar also has a bad reputation in terms of customer experience, as IBM has a lack of employees dealing with this field. However, IBM has started to hire much more employees to deal specifically with customer support.

2.3 RSA NetWitness

The next SIEM product we will be evaluating is RSA's NetWitness platform. Ron Rivest, Adi Shamir, and Leonard Adleman established RSA in 1982, which bears their initials. They are also credited with creating the RSA public key cryptography method. RSA acquired NetWitness in 2011 and combined it with the RSA enVision SIEM in a combined security message. RSA has a main office in Bedford, Massachusetts, regional headquarters in Bracknell, United Kingdom, and Singapore, as well as many other overseas locations.

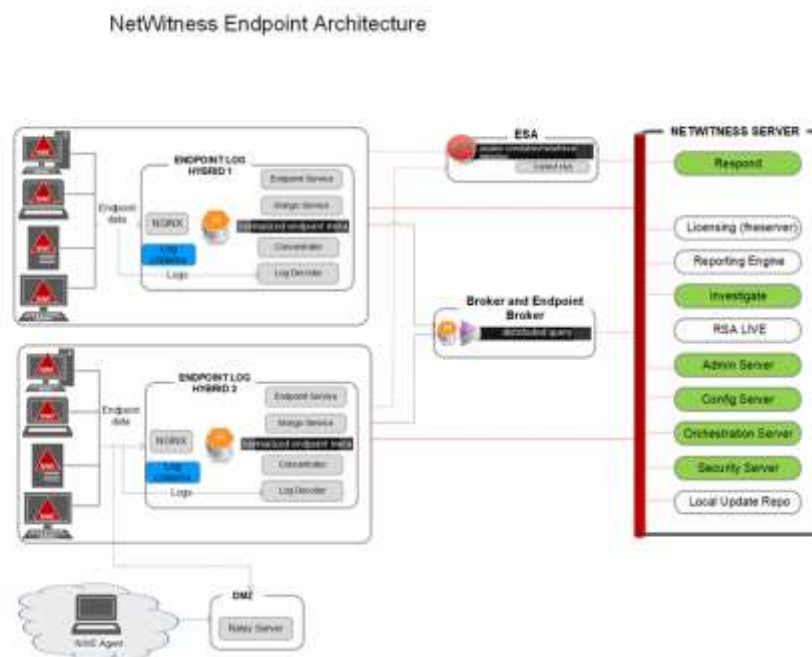
Design

To help security teams operate more effectively and efficiently, the RSA NetWitness platform makes use of cutting-edge technology. To assist analysts in identifying and resolving both known and undiscovered threats, it makes use of behavioural analysis, data science approaches, and threat intelligence. Additionally, it orchestrates and automates the entire incident response lifecycle using machine learning. By prioritizing the incidents fast, correlating incidents over time, and providing deeper insights, it exposes the full scope of an attack.

As the core of the security operations centre (SOC), the RSA NetWitness Platform combines advanced SIEM and XDR technologies that provide exceptional visibility, analytics, and automated response capabilities. With real-time data science and machine learning analytics, it can spot new, specific, and undiscovered threats, which it can subsequently log down. These logs can be used to try and replicate the occurrence so that security teams can dissect it. This leads to security teams understanding the full scope of an attack, allowing them to be more efficient and effective at detection and response. Security teams are better able to detect and respond to attacks because of having a complete picture of the attack's scope. From the smallest to the largest of companies, these features may scale.

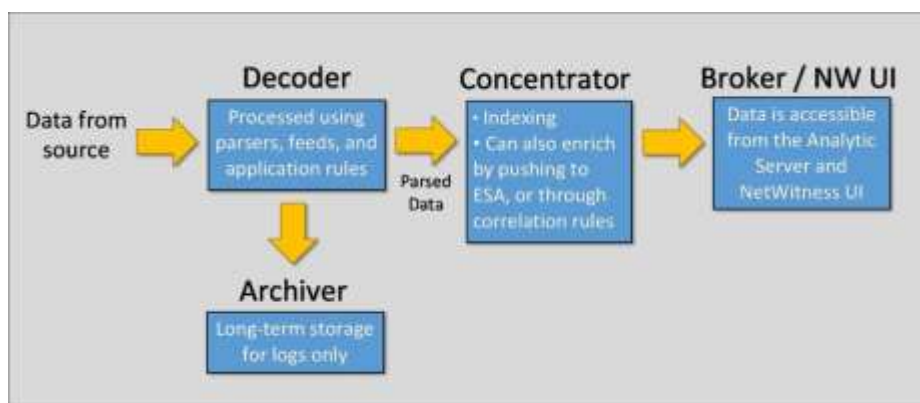
RSA NetWitness Protection is also highly integrable into third-party software, with over a thousand other modern applications from vendors such as Cisco, Amazon Web Services, and Dell EMC, and is compatible with both Windows and Unix/Linux systems.

Architecture



RSA NetWitness Platform is a distributed and modular system that allows for highly flexible deployment architectures that scale with the organization's needs. The System Architecture is composed of these major building blocks: Endpoint Log Hybrid, Decoder, Concentrator, Archiver, Broker, Event Stream Analysis (ESA), and the NetWitness Server. These components work together to detect any potential threats in the network and respond quickly and efficiently. We will elaborate further on how some of these components work together.

Firstly, data from a source, such as a network, is sent into the Decoder. NetWitness collects two types of data: packet data (network packets) and log data. Packet data is collected by the network decoder while log data is collected by the log decoder. These decoders process raw data that is parsed and enriched through parsers, feeds, and application rules. The logs are then sent to the Archiver for long-term storage. The parsed data from the decoder is sent to the Concentrator, which indexes the data for fast retrieval. There is an option to enrich it to the ESA. Lastly, the data is brought to the broker where we are allowed to view this data from the NetWitness User Interface, providing full visibility into what is being generated on the network.



RSA NetWitness can also be deployed to the cloud. The NetWitness Cloud SIEM is a service that was announced last year on May 26, 2021. It provides the same features as the original NetWitness SIEM but in cloud form. Users will find it simpler to utilize all of NetWitness' capabilities as a result of not needing the IT resources necessary for setting up, scaling, deploying, upgrading, and managing the product in a data centre.

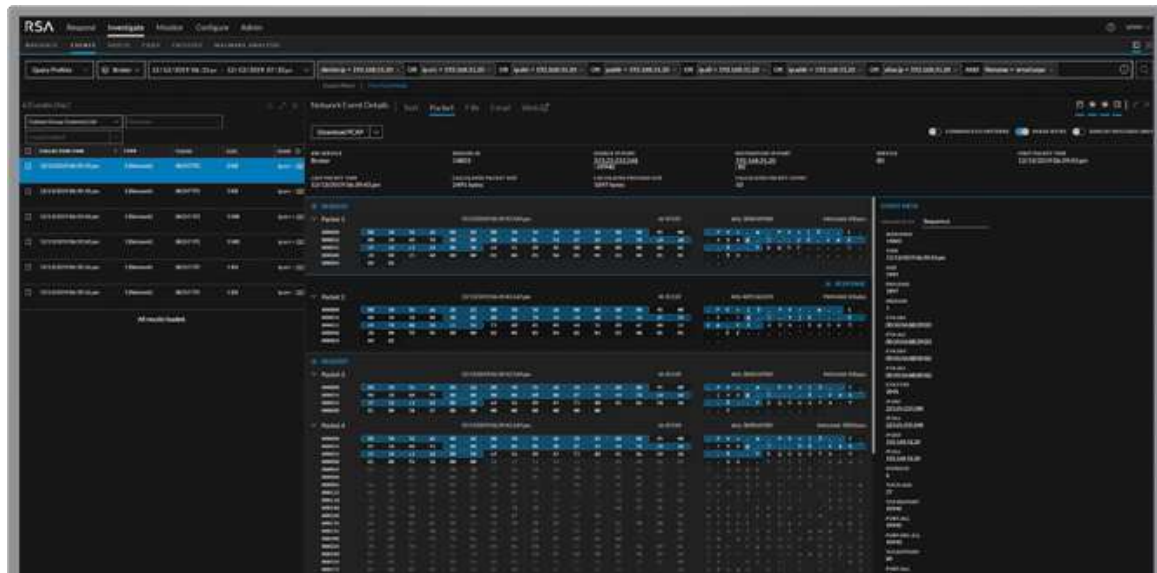
RSA NetWitness provides many functionalities that can help a company's system. It supports a wide range of data types such as File and directories, logged network events from network logging systems, data from Windows systems and other metric data from other applications. Using this data, NetWitness is able to perform 5 main features: log monitoring and management, threat detection, endpoint detection and response, User and Entity Behaviour Analytics (UEBA) and security orchestration, automation and response.

[illegible]

The first feature is log monitoring and management, which is done through the RSA NetWitness Logs. NetWitness Logs delivers real-time insight into log data across an organization's whole IT system, simplifying threat detection, minimizing dwell time, and assisting with compliance. It allows for centralized log management, log monitoring for logs produced by public clouds, and the detection of suspicious activity that avoids detection by security solutions that rely on signatures. Utilizing parsing and indexing technology that is already present in the service, it does this. While the log data is being gathered, it dynamically enriches and parses it, producing metadata that helps boost the alerting and analysis process. NetWitness Logs collects logs from over 350 different event

sources and enables log monitoring for public clouds like AWS and Azure, as well as SaaS services like Office 365. It also reads security information from a variety of protocols such as Syslog, SFTP, SCP, FTPS, and others.

Threat detection



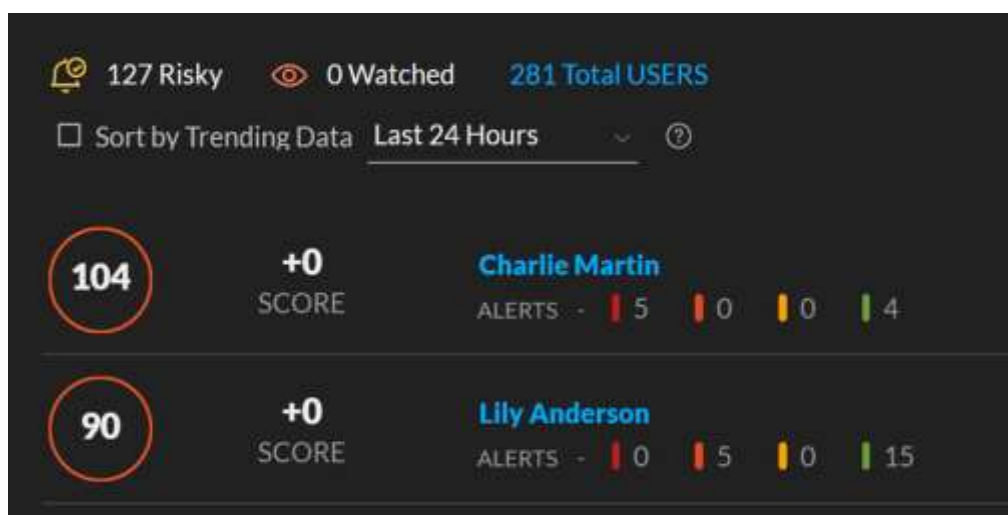
The second feature is threat detection using NetWitness Network. To enhance network threat identification and speed up threat response, NetWitness Network provides complete, real-time insight into a company's entire IT infrastructure. It does this by having full-packet capture. Users can identify and keep an eye on new, targeted, and undiscovered threats as they move around the network. Additionally, it combines deep inspection of hundreds of protocols with the ability to recreate whole network sessions to produce a potent and comprehensive toolkit for forensic investigations. NetWitness Network also includes native decryption functionality, so encrypted communication is not an issue, and it can interact with third parties to give extra decryption assistance.

Endpoint detection and response

FILE NAME	RISK SCORE	FIRST SEEN TIME	ON HOSTS	REPUTATION	SIZE	SIGNATURE
powershell.exe	100	12/30/2019 05:55:41 pm	1	Known Good	116.8 KB	microsoft
cmd.exe	100	12/30/2019 05:36:34 pm	2	Known Good	116.8 KB	microsoft
concatV.exe	36	12/30/2019 05:55:41 pm	1	Known Good	116.8 KB	microsoft
powershell.exe	36	12/30/2019 05:55:41 pm	1	Known Good	116.8 KB	microsoft
powershell.exe	31	12/30/2019 05:55:41 pm	1	Known Good	116.8 KB	microsoft
cmd.exe	31	12/30/2019 05:36:34 pm	1	Known Good	116.8 KB	microsoft
powershell.exe	31	12/30/2019 05:36:34 pm	1	Known Good	116.8 KB	microsoft
java.exe	31	12/30/2019 05:36:34 pm	1	Known Good	116.8 KB	microsoft
X64GameDevTab.exe	0	12/30/2019 05:59:14 pm	1	Known Good	31.5 KB	microsoft
mscman.dll	0	12/30/2019 05:59:14 pm	1	Known Good	124.0 KB	microsoft
xmldat.dll	0	12/30/2019 05:59:14 pm	1	Known Good	10.0 KB	microsoft
msasn1.dll	0	12/30/2019 05:59:14 pm	1	Known Good	81.0 KB	microsoft

The third feature is endpoint detection and response with NetWitness Endpoint. It keeps track of everything that happens on and off the network across all of the user's endpoints. This gives a thorough understanding of their security status and gives priority to alarms when a problem arises. Additionally, NetWitness Endpoint significantly minimizes dwell time by quickly identifying incoming non-malware attacks. As a result, security teams are able to function more effectively since they have access to the most vital information for determining the scope of an attack and carrying out efficient forensic investigations. It functions by offering continuous endpoint monitoring, giving full insight into all activities, executables, events, and behaviours on all endpoints used by a company, including servers, desktop computers, laptops, and virtual machines. Because it uses a lightweight endpoint agent, it collects entire endpoint inventories and profiles in minutes with no impact on user productivity. It also delivers real-time insights, actionable responses, and information ingestion from both Windows logs and endpoint core activities. NetWitness Endpoint is also scalable, with a single, tamper-proof agent that readily expands from hundreds to thousands of endpoints. The NetWitness Endpoint database is used for all data storage and processing, ensuring data integrity and substantially reducing endpoint impact.

User and Entity Behaviour Analytics (UEBA)



The fourth feature is User and Entity Behaviour Analytics (UEBA), which is done using NetWitness Detect AI. NetWitness Detect AI is a cloud-native SaaS product that identifies unknown threats using sophisticated behaviour analytics and machine learning. It uses network, endpoint, and log data recorded by the NetWitness Platform to establish a baseline of an organization's behaviour and IT usage to detect variations that suggest suspicious behaviour and sophisticated attacks. NetWitness Detect AI employs unsupervised machine learning, which allows it to quickly and correctly identify behaviours that may indicate an attack. Unsupervised machine learning eliminates the need to create rules, customize metadata, and continually tune underlying data models.

Security orchestration, automation and response

The fifth feature is security orchestration, automation and response, which is done using NetWitness Orchestrator. NetWitness Orchestrator delivers full security orchestration and automation to increase the productivity and efficacy of a security operations centre. It is also backed up by hundreds of predefined and configurable playbooks, allowing teams to cooperate and expedite incident response. NetWitness Orchestrator gathers, standardizes, and prioritizes alerts using

holistic incident management to expedite a security operation centre (SOC) team's response effort. It enables the collecting, querying, and enrichment of artifacts and indicators, including users, systems, IPs, and more, by leveraging vast data sources. It documents the incident management lifecycle automatically and in a well-organized manner.

Strengths and Advantages

Overall, RSA NetWitness Platform has many strengths. The first of which would be its deployment. Companies can build functional stacks by mixing multiple software, hardware, and virtual appliances, allowing for flexible deployments and horizontal scalability. Next, it is a solution that is ideally suited to advanced threat defence use cases because of multistage analytics, which includes RSA NetWitness Platform's large range of additional, natively integrated solutions for ubiquitous view and analytics across endpoints and networks. A multistage analytics engine with intriguing unsupervised modelling capabilities spanning endpoints, networks, and people is another feature of the RSA NetWitness Platform. Another strength of the RSA NetWitness Platform is its robust feature set for forensics and threat hunting, with ubiquitous access to forensics artifacts throughout the entire RSA technology stack. As mentioned earlier, it is easy to deploy, because RSA provides RSA Live, which can be accessed straight from the NetWitness Platform console and allows access to all RSA NetWitness Platform content. RSA offers a large global network of channel partners and service providers who provide local support for the NetWitness Program, including integration, management, and operations, making troubleshooting and obtaining information about the NetWitness Platform very simple. Some of these strengths are supported by many user reviews, with one user stating, "It has easy installation and deployment, the scalability of deployment is very good and effective technical support." and another user stating, "It is cost-effective, has great local support and easily integrates with other network devices."

Weaknesses and Limitations

While RSA NetWitness Platform has its strengths in deployment, it also has some weaknesses and limitations compared to other SIEM products. The first being its product strategy with security orchestration, automation, and response (SOAR). RSA's NetWitness SOAR strategy is based on Original Equipment Manufacturer (OEM) relationships in a dynamic market. So clients need to validate that RSA's SOAR partner fits their requirements, hence they need to take an extra step. The next weakness is that its UEBA capabilities offer fewer models than some of its competitors. RSA NetWitness Platform is also not offered as a Software as a Service (SaaS) solution from vendors, while some of RSA's partners do. Therefore, companies that want a vendor-delivered SaaS SIEM may find limitations in the product. Lastly, according to many user reviews, RSA NetWitness is more complex and harder to use compared to other SIEM products. One user stated, "It requires in-depth training to be able to understand the capabilities of the solution fully. The learning curve is steep." another user stated, "Difficult to learn and use initially, the Dashboards could have been a bit more pleasing to see and there is a lot of features and it's a bit overwhelming to use."

2.4 McAfee

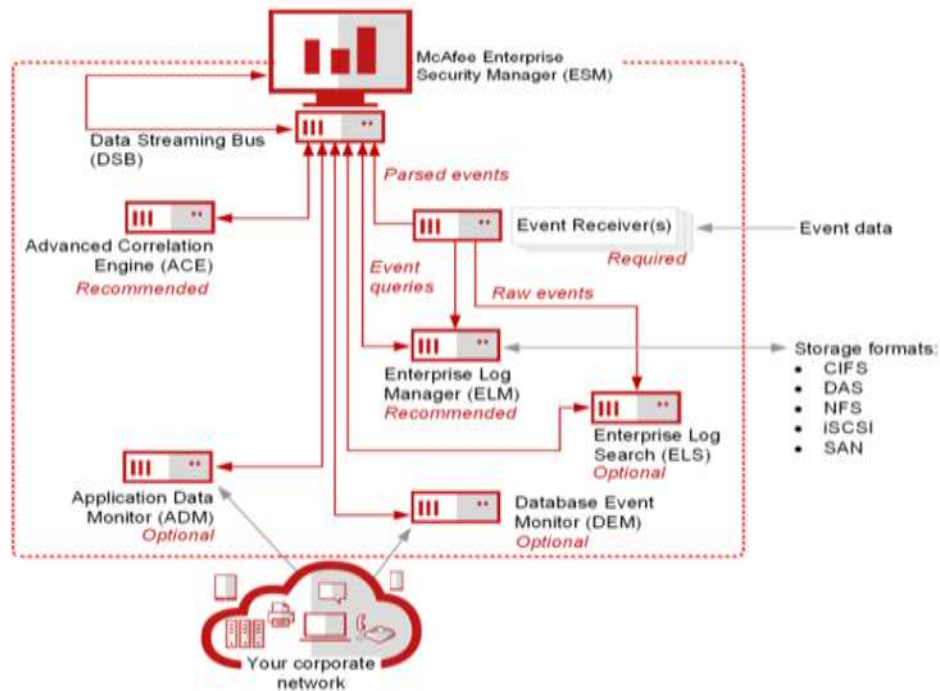


McAfee was founded in 1987 as McAfee Associates, named for its founder, John McAfee, who left the company in 1994. It was founded by McAfee's former CEO, Jim Warren, and was founded by John McAfee, who left the company in 1994. John McAfee left security software company McAfee in 1994, and the company was acquired by Intel in 2010 for \$7.68 billion. John McAfee rose to prominence in the 1980s when he founded McAfee Associates, a software company that made its name selling McAfee Associates commercial computer security software. In late 2011, the company acquired privately owned NitroSecurity, a developer of high-performance SIEM solutions that protects critical information and infrastructure.

Design

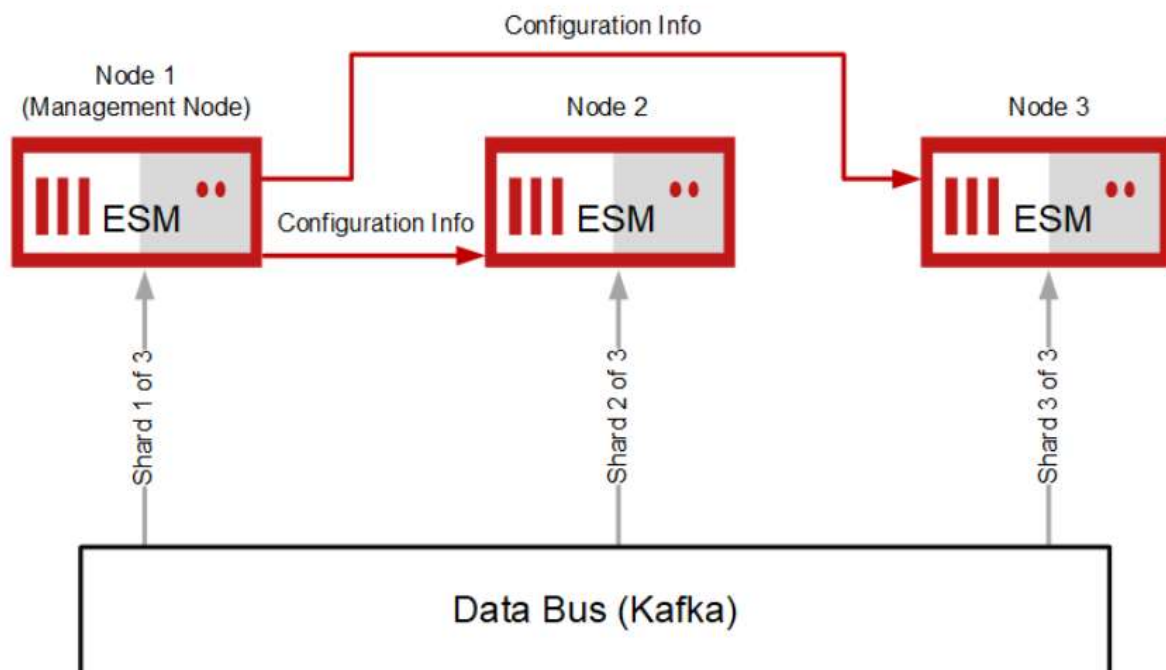
The Enterprise Security Manager (ESM), which is offered in two different formats—one as a cloud service called ESM Cloud and the other as a regular on-premises ESM which are a fundamental component of McAfee's SIEM solutions. On November 9, 2021, the company made the most recent ESM version 11.5.2 available. To improve the functionality of McAfee EMS, users can add a variety of components. However, it is advised or necessary to install some required/recommended components.

Advanced Correlation Engine (ACE), Event Receiver (ERC), and Enterprise Log Manager (ELM) are some of these components. ESM also includes Global Threat Intelligence (GTI). To improve the functionality of McAfee® ESM, we can also add more optional components in addition to those listed above. McAfee® Database Event Monitor (DEM), McAfee® Enterprise Log Search (ELS), and McAfee® Application Data Monitor (ADM) are the three optional parts in total. For instance, we can include ADM to watch over and track database transactions to spot shady activity.



While third-party programs can be used with McAfee® ESM, they can compromise system security and leave it vulnerable to flaws and instability. In order to ensure SIEM security and stability, McAfee advises against making changes to the system and running it outside of the graphical user interface (GUI).

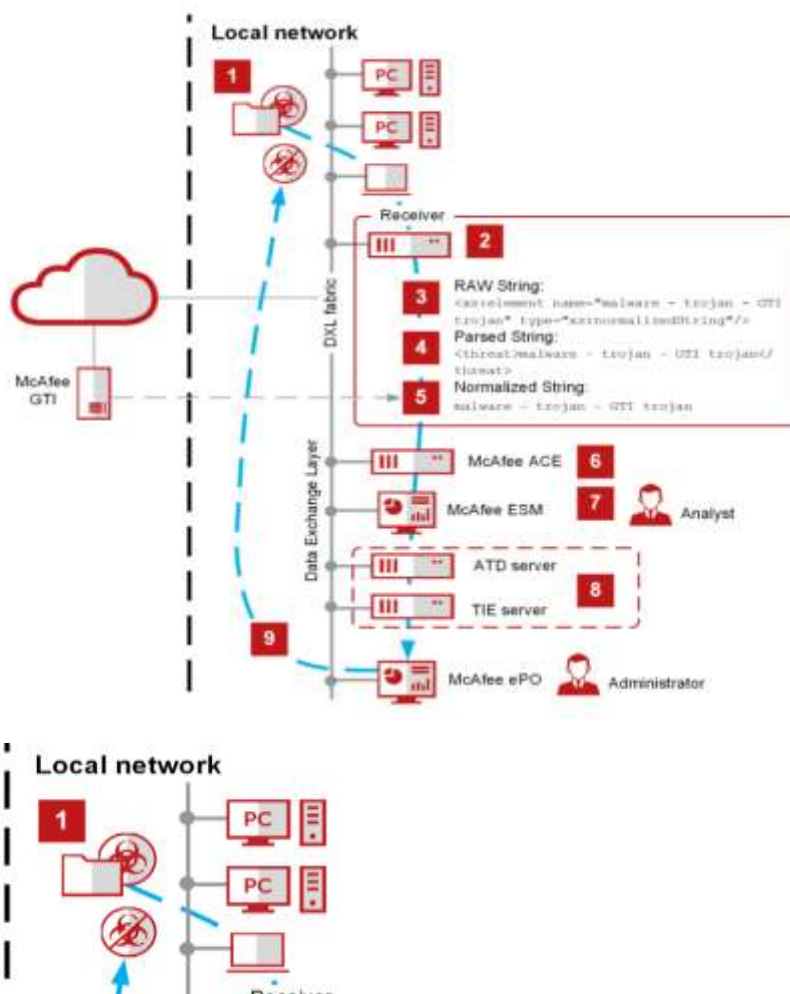
Nevertheless, McAfee® ESM can connect with software from manufacturers including Cisco, Intel, Dell, and Microsoft. A guide with instructions for configuring third-party software's data resources is also available from McAfee. Reviews of McAfee ESM, however, suggest that consulting services are necessary in order to integrate all Intel products. As a result, not all third-party software that can be integrated with McAfee® ESM is covered in this article.



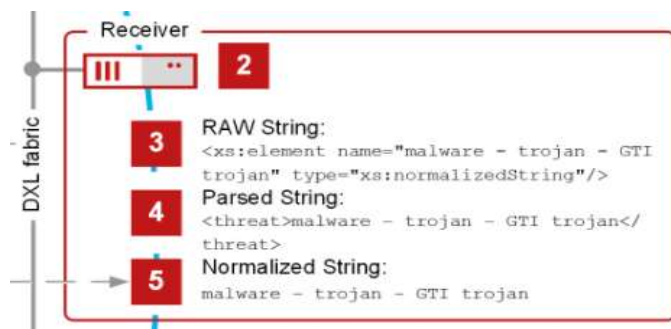
Users can form ESM clusters to maximize scaling by integrating numerous ESM devices into their architecture. In any clustered environment, one node acts as a management node that performs the management functions for the cluster.

By utilizing the processing capacity of numerous ESM appliances to handle event data, this boosts system throughput rates (more events per second). Each ESM appliance holds a fraction of the event data when scaled. The three-node ESM scaled cluster in the diagram below demonstrates that each ESM node holds a third of the data. Each ESM node conducts a query upon execution on the data it contains. A single set of results from each node is shown.

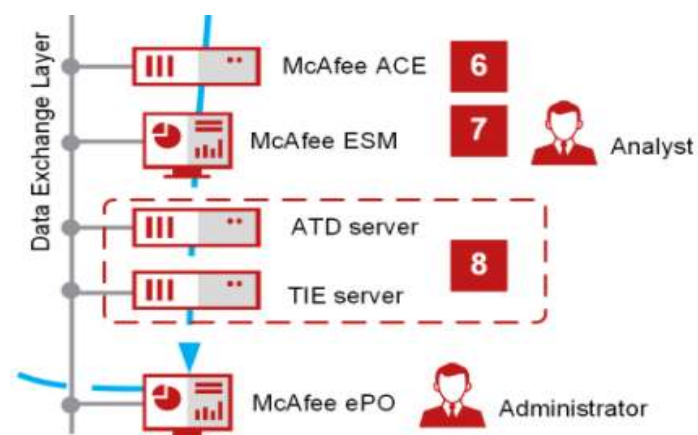
Architecture



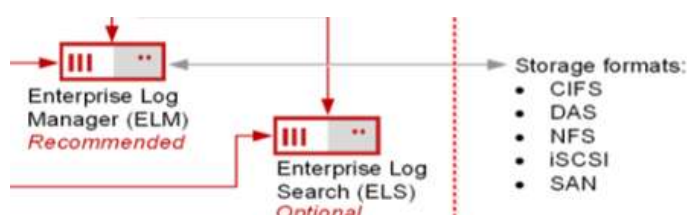
Real-time insight into all activity on your systems, networks, databases, and applications is provided by McAfee® ESM. Performance, actionable intelligence, and solution integration are delivered at the rate and scale required by security organizations.



McAfee® ERC gathers raw data and events from security devices, systems, networks, databases, and applications the minute a threat enters an organization's system. These data and events are then parsed into components and relationships depending on specific syntax rules established by the user. ERC then normalises the collected values to a common scale and uses them to identify known threats.



Next, McAfee® ACE will correlate patterns in the information to find potential security concerns. Dashboards, alarms, watchlists, cases, and reports can then be used by analysts to track and identify the threats. Finally, they can use McAfee ePolicy Orchestrator to immediately and automatically respond to the threat after identifying it using McAfee® Data Exchange Layer (DXL), McAfee® Advanced Threat Defense, and McAfee® Threat Intelligence Exchange (TIE).



The gathered data is saved, managed, accessed, and reported on the log file manager McAfee® ELM, which is required to offer log file management features by security standard. However, users have the option to store data on McAfee® ESM using a Direct-attached storage (DAS), Storage Area Network (SAN), or Small Computer System Interface (iSCSI) device.

McAfee® ELS, which is based on Elasticsearch and works with files created by McAfee® ACE or McAfee® ELM, can search the stored data. Additionally, it keeps uncompressed log data for predetermined amounts of time. Users can add up to six retention policies in terms of years, quarters, or months, and they can choose how long they want to keep the data for.

Both Windows and Linux are supported by McAfee® ESM, and it can run on a single server with Hyper-V VM, Linux KVM, and other supported Virtual Machines (VMs).

The minimum requirement for VM requires:

- Processor -- 8 core 64-bit, Dual Core2/Nehalem or higher, or AMD Dual Athlon64/Dual Opteron64 or higher
- RAM -- 16GB or more
- Disk space -- 500 GB or more
- VMware ESXi 5.0 or later

The minimum requirement for system requires:

- P4-class Intel (not Celeron) or later (Mobile/Xeon/Core2/Core i3/5/7) or AMD/AMD2 class or later (Turion 64/Athlon64/Opteron64/A4/6/8)
- 16GB RAM

The McAfee® ESM Cloud format can be used to deploy the ESM in the cloud. It supports Microsoft Azure, Oracle Cloud Infrastructure, and Amazon Web Services. Once installed, McAfee® ESM keeps track of and generates reports on cloud servers and other security infrastructure that is compatible with the cloud environment.

Main Functionalities

Hardware appliances, virtual devices, and the McAfee® ESM application make up McAfee SIEM. You need McAfee ERC, ELM, and ESM. There are 6 additional components that the user can add to improve the performance of McAfee® ESM, for a total of 10 components, including: McAfee® Enterprise Security Manager (ESM) device

The McAfee ESM device has features for log analysis, SIEM, and network analysis and is available as a hardware component or as software installed on a virtual machine (VM).

McAfee® Event Receiver (ERC)

It gathers third-party logs, events, and flow data for correlation and analysis by an ESM device. It is available as a hardware component or VM software installation.



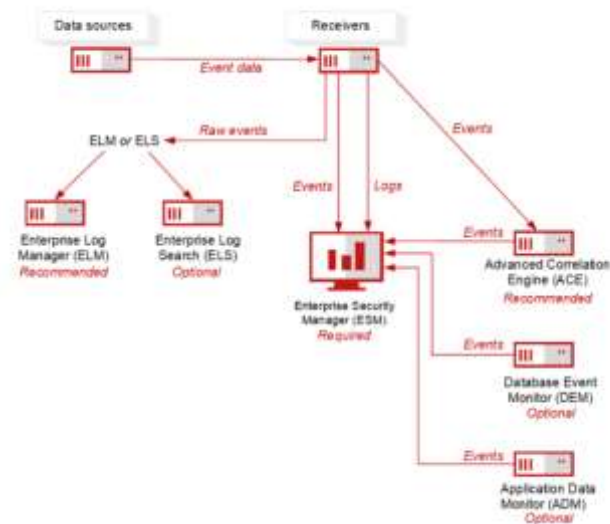
McAfee® Enterprise Log Manager (ELM)

It offers compliance log management features and is available as a hardware component or as a VM installation. Requires a McAfee ESM device and ERC. ELM is an example of a "cool" storage. It compresses for storage effectiveness and hashes for forensic integrity (in a small 2U package). Only very seldom may it be searched. And it ought to be the record storage that permits complete log retention.

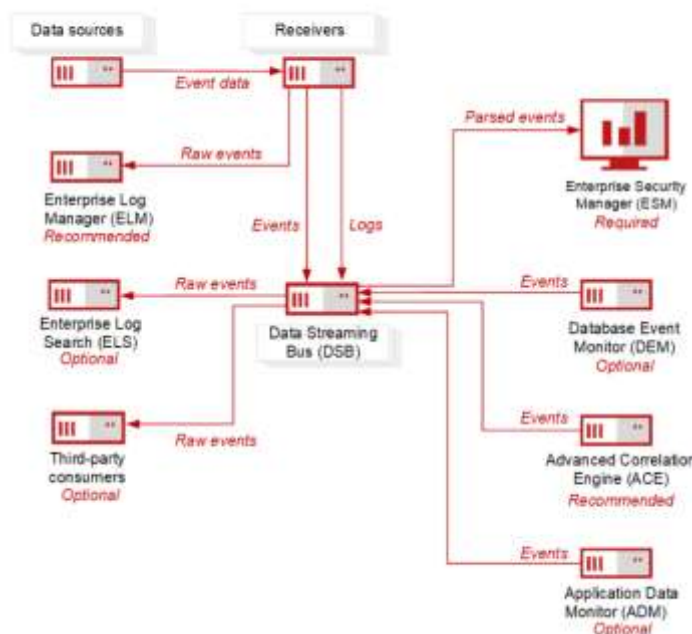
Data Streaming Bus

Utilize the data streaming bus to integrate data quickly and easily with McAfee Behavioural Analytics and other third-party products. Delivered in VM device form. Distributed ESM and Data Sharing features must be enabled for use.

System diagram without a Data Streaming Bus



System diagram with a Data Streaming Bus



McAfee Enterprise Log Search (ELS)

A hardware component that gathers, indexes, and saves every event to produce a verifiable audit trail of activity. The use of indexes in McAfee ELS allows it to search events more quickly than McAfee Enterprise Log Manager. ELS is comparable to a quick raw log search. Users can look for events in any section of the log using this feature (especially those that are not parsed). It enables McAfee ESM to

quickly filter out data that is "less important". This increases the efficiency, performance, and storage time of McAfee ESM. Because this data is not compressed, ELS often saves less data than the entire retention requirements (3-6 months, depending on EPS). High EPS situations soon reach the high Terabyte level.

McAfee Receiver/ELM (ELMERC)

ERC and ELM are included in a VM software installation or are available as hardware components.

McAfee® Advanced Correlation Engine (McAfee® ACE)

It is available to deploy McAfee RSC and Enterprise correlation as a hardware component or as a virtual machine software installation. These tools can identify and evaluate threat events in real-time or in the past using both rule-based and risk-based logic.

McAfee Application Data Monitor

A hardware or virtual machine component that records full session details of all violations and monitors more than 500 known applications across the entire layer stack.

McAfee Database Event Monitor (DEM)

A hardware that, for most database platforms, automates the gathering, management, analysis, visualization, and reporting of database access.

McAfee Direct Attached Storage (DAS)

A hardware device that adds more storage capacity to the ESM, ELM, or ELS.

Strengths and Advantages

McAfee is rated 4.4 out of a possible 5 stars on the Gartner website. There are 424 reviews total for McAfee, the majority of which are positive and rate McAfee® ESM from three to five stars. In terms of overall ratings, McAfee is tied with IBM and 0.1 stars better than Splunk. Users who have used McAfee are willing to recommend it 77% of the time, compared to 84% for Splunk and 87% for Rapid7.

In conclusion, users appreciate McAfee® ESM's capabilities, scalability, and real-time monitoring. Most users find McAfee® ESM to be very safe and practical, and it has assisted them in stopping numerous malware and intrusions, giving their businesses security and peace of mind. Since McAfee® ESM is not just for desktops, one user's company uses it to monitor its entire network and hasn't experienced any security problems since setting it up. One user who gave the product a two-star review stated, "Rules and detections worked well, but it was difficult to come up with new ones. The console was slow and unwieldy ". Thus, it is clear that McAfee® SIEM ESM can offer good security and can satisfy customer demands.

Weaknesses and Limitations

The flaws in McAfee® SIEM ESM were exposed after reading numerous online reviews. Users must invest a lot of time learning the ins and outs of the system because, among other things, the GUI is difficult to use and the UX and UI are subpar.

Even a customer who gave a review with a 4-star rating stated, "Although it asks the user to set a password and complete other initial setups, the UI isn't excellent and doesn't truly explain what it is. It was chosen by my organization because of its excellent capabilities."

Additionally, bad customer service is the problem that receives the worst reviews. Customer support has been known to close tickets without informing customers and before problems were resolved.

The "Emotional Footprint" or user experience of various SIEM products was also surveyed by ManageEngine. McAfee fell behind Splunk and IBM in all categories and failed to place in the top 5. In conclusion, McAfee® ESM offers solid performance and security. The company will, however, be more well-liked by customers if it can enhance its user interface.

3. SIEM Product Recommendation

3.1 Recommendation

After assessing and evaluating the four different SIEM products, we want to recommend a SIEM product that is suitable to use for Skrull Pte Ltd.; to do this, we can use five criteria to compare the SIEM products to determine which is the best option. The five criteria are scalability, integrations, User Interface (UI), cost, and reputation. From the five criteria, we have determined that Splunk is the best product for Skrull,

The first criteria is scalability, which is the ability to adapt to the size and growth of the organisation. A scalable SIEM product means that it works well for both SMEs and MNCs. For Splunk Enterprise, its design allows it to be scalable because of its ability to be deployed in many ways; on-site, on cloud, a hybrid of both, on a single instance, and as a distributed deployment.

The second criteria is integrations, which is the ability to pull in data from other enterprise applications, like antivirus software, login data, security auditing software, and more; saving not only time but also provides a holistic picture of the environment. For Splunk Enterprise, its design makes it very easily integrated with other third-party applications from many vendors, making it rank highly in integrations.

The third criteria is UI, which is an important factor to consider when using the product because it determines the speed and the ease of use of the product. For Splunk Enterprise, its UI is one of its stronger features as compared to other SIEM products in the market. Although the search and dashboard features may take some time to learn, its overall menu is easy to navigate and find certain sections, making Splunk's UI one of the most intuitive in the market.

The fourth criteria is cost, which is a very important factor to consider especially for an SME like Skrull. Being an SME, budget is a concern because they may not be able to afford the full product if it is too costly. For Splunk Enterprise, although one of its weaknesses is its high cost for large data volumes, the cost can be significantly reduced by using the idea of Security As A Service (SAAS), where security is not necessarily a product, instead it is offered as a service by third party vendors. In the case of Splunk Enterprise, it offers a Managed Security Service Provider (MSSP) called Splunk MSSP where it provides Splunk's features as a service instead of a whole product, drastically dropping the high cost of Splunk, which is beneficial for SMEs like Skrull.

The fifth criteria is reputation, which is important when deciding on a product because reputation represents the reliability and overall user satisfaction of the product. Organisations are more likely to use a product with a good reputation than a bad reputation. Reputation: For Splunk Enterprise, its reputation is second to none. Splunk has 19 years of experience, making it one of the oldest organisations for SIEM. Having the largest market share of 30.25% in the SIEM Gartner Market Share Report in 2021, it is used by a big percentage of organisations. Furthermore, Splunk has been granted multiple prestigious awards throughout the years, making it a reliable and successful company

Table 1. Rating products on criteria out of 5 stars

	Splunk Enterprise	IBM	RSA NetWitness	McAfee
Scalability	****	*****	****	*****
Integrations	*****	****	****	****
User Interface	****	****	***	***
Cost	****	**	****	****
Reputation	*****	****	***	****

Splunk would be deployed on site, as Skrull is a SME, which means that there is currently no need for any remote systems and cloud services. Since Splunk will be deployed on site, the forwarding and analysis of data will be easier and faster because there will be no transmission time between the processes. Furthermore, being fully on-site will reduce the overall cost of deployment long term, to ensure that Splunk Enterprise can meet the budget needs of Skrull.

The company has 200 HP Networked printers, which run firmware that has built-in support for Splunk Enterprise's data forwarding. Being a smaller organisation, a single instance of Splunk is enough to monitor and manage the logs of the printers within Skrull. For the storage of logs, there should not only be a storage within the Splunk server, but there should also be a file server that archives logs for longer than the Splunk server for future referencing.

3.2 Indicators of Compromise

Our team has performed research on two potential vulnerabilities that exist for our HP networked printers in order to detect signs of compromise.

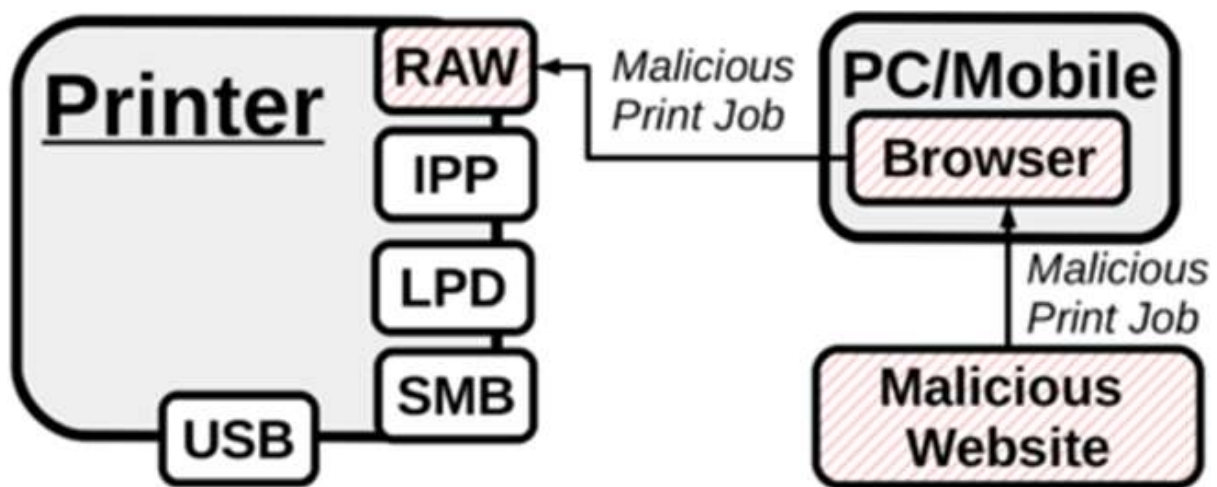
CVE-2021-3438

SentinelLabs first discovered the CVE-2021-3438 vulnerability in the first quarter of 2021, which is a 16-year-old bug. When experts were setting up a brand-new HP printer, they saw that a 2005 printer drive with the name SSPOORT.SYS was raising an alarm from the software Process Hacker. With a CVSS Score of 8.8, this high severity vulnerability was rated as having a very large list of affected HP and Samsung printer models totalling over 380. This vulnerability allows an unprivileged user to get access to a system account and run code in kernel mode by exploiting a printer's kernel driver, also known as a Privilege Escalation attack. This can be exploited to circumvent security technologies, possibly allowing attackers to install programs, access, alter, encrypt, or delete data, or establish new accounts with full user privileges.

We will employ a series of searches to identify potential attacks that might exploit this vulnerability in order to stop Privilege Escalation attempts. Searches on the Spoolsv.exe child processes, Windows accessibility binary alterations, registry keys utilized for privilege escalation, and atypical processes on endpoint are among the particular searches that are advised for us to do. If any suspicious behaviour is detected, additional investigation may be conducted by conducting searches on an endpoint's authentication logs, processes running on a host, registry actions, and web traffic to and from a host.

CVE-2021-39238

The National Institute of Standards and Technology (NIST) originally disclosed the CVE-2021-39238 vulnerability on February 11th, 2021. Over 150 different HP printer types are affected by the vulnerability, including a large number of HP Enterprise LaserJet, LaserJet Managed, Enterprise PageWide, and PageWide Managed models. With a CVSS score of 9.3, the vulnerability falls into the Critical severity category. Due to this flaw, printers might be remotely targeted with buffer overflows without requiring physical access to the device. Furthermore, CVE-2021-39238 is wormable, meaning an attacker might initially take advantage of a single networked printer before developing a self-propagating worm to infect other networked devices. A Cross Site Printing (XSP) attack, in which the attacker establishes a phishing site that sends a malicious payload to the target printer when someone on the network views the site, might be used to exploit a printer vulnerability.



We will search for malicious print jobs that are transmitted into Splunk Enterprise from our printer logs to detect a possible breach in our networked printers using this vulnerability. The Name and Size, Username, and Timestamp of the print job event are all important fields to check for here. This information might be combined with other data, such as data from a Network Intrusion Detection System (NIDS), to acquire further important information, such as the attacker's IP address. We will go through the specific rules that may be utilized to detect a possible breach in our HP networked printers in further detail.

3.3 Rules implemented to detect a possible compromise

We intend to set up alerting rules in Splunk Enterprise to alert an administrator if there is a possible breach in our HP networked printers. If necessary, the alerts can be customized to execute custom-written scripts. Splunk Enterprise enables us to construct alerts with precise trigger conditions and post-alert actions, which we will use to build effective rules.

Save As Alert

×

Enable Actions

List in Triggered Alerts

Triggered Alerts is available in the activity menu.

Send Email

Email must be configured in System Settings > Alert Email Settings. [Learn More](#)

Comma separated list of email addresses. [Show CC and BCC](#)

To

cosmo@example.com

Priority

Normal

Subject

Real Time Alert: \$name\$

The email subject and message can include tokens that insert text based on the results of the search. [Learn More](#)

Message

There were \$job.resultCount\$ errors.

Include

Link to Alert

Link to Results

Search String

Inline Table

Trigger Condition

Attach CSV

Trigger Time

Attach PDF

Run a Script

Action Options

When triggered events

Once

For each result

Cancel

Back

Save

CVE-2021-3438

We mentioned the possibility of a Privilege Escalation attack in the preceding section owing to the vulnerability triggered by CVE-2021-3438. We propose enabling Splunk Alerts to activate under the following criteria to identify any potential attacks:

- Any Modifications to registry keys that can be used to elevate privileges
- Any unusual user making modifications to a windows accessibility

If this alert is triggered, an administrator should get a high-priority email since an immediate response is critical when dealing with this issue due to how quickly attackers may work once they have an account with sufficient credentials.

CVE-2021-39238

Cross Site Printing is a potential attack vector for CVE-2021-39238, as we stated in the preceding section (XSP). To identify a potential attack, we recommend configuring Splunk Alerts to trigger under the following conditions:

- An unusual printing time is found
- Unknown and undefined usernames or job names
- An unusual small print job is conducted

For this use case, it is also critical that the logs stored in the local storage of the HP networked printers are configured to be automatically cleared after they have been sent to our Splunk Indexer for indexing and storing in the fileserver, so that if a printer is compromised, the attacker does not have access to previous log files, reducing the possibility of them forging the data in the log file to appear as a genuine print job.

If this warning is triggered, an administrator should get a high-priority email, as this vulnerability is important, and action should be done quickly if a breach occurs. A script can be built to automatically disconnect the vulnerable printer from the network, preventing a worm from spreading to other printers in the event of a real assault.

3.4 The Government Recommendations

Due to growing awareness of the dangers and threats that governments, corporations, and people face, the global cyber landscape has undergone significant change recently. As a strong reminder that cybersecurity must be taken seriously, ransomware attacks, data breaches, and other cyber incidents have made headlines. At the same time, people are eager to take advantage of the opportunities that the rapid advancements in digitalization and innovation present.

Every day, new technological products hit the market. Customers are given the assurance that the product has been objectively found to be more cyber secure and has adopted a Security by-Design approach throughout the product life cycle thanks to the government recommendations. The Cyber Security Agency of Singapore is an example of a company that performs this assessment.

3.4.1 Who are The Cyber Security Agency of Singapore



The Cyber Security Agency of Singapore (CSA) is a government agency responsible for the protection of Singapore's critical infrastructure against cyber-attacks. The CSA's mission is to safeguard national interests through the detection, investigation, and prevention of cyber-related threats.



The Cybersecurity Certification Centre (CCC), which is a part of CSA, is responsible for evaluating and certifying cybersecurity products. The CSA Cybersecurity Certification Centre runs the following programs to give customers the security assurance that their products have undergone objective inspection and testing to ensure that they are securely created, implemented, and suitable for reducing the risks associated with the identified security threats. The Singapore Common Criteria

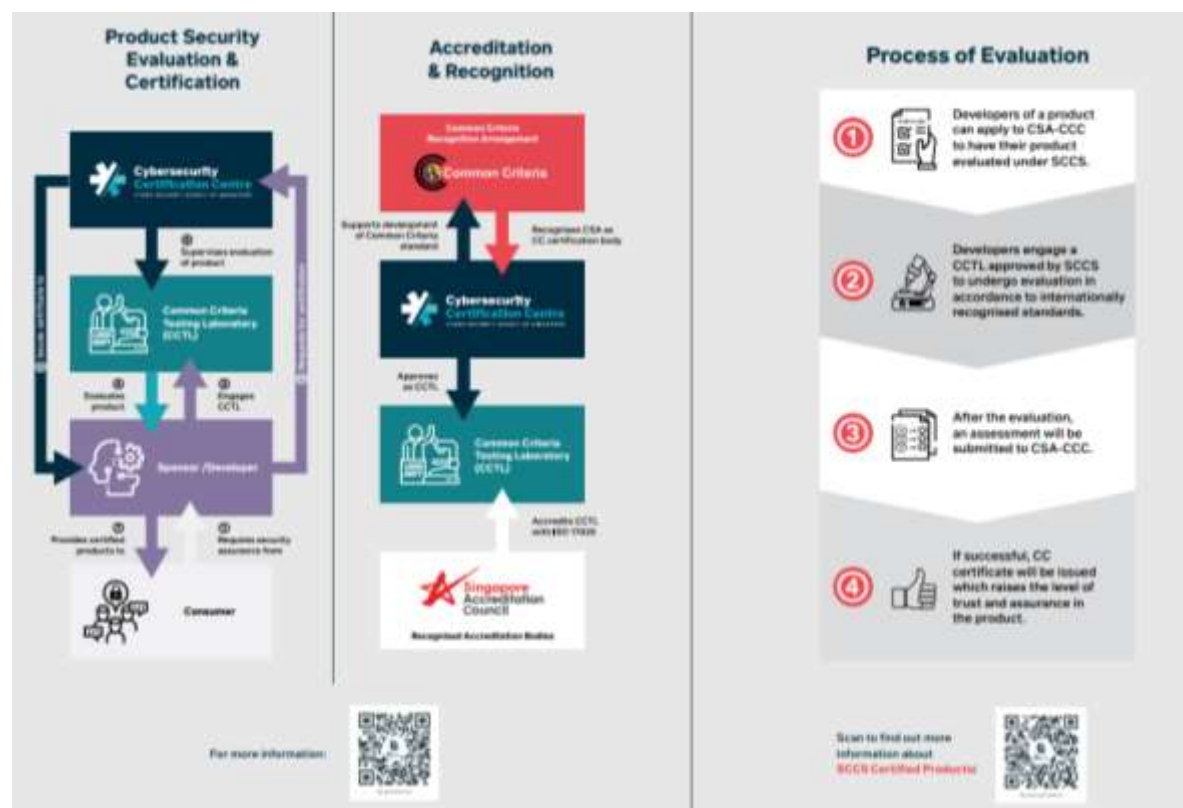
Scheme (SCCS), one of the programs, is for the certification of commercial IT products aimed at the global market.

3.4.2 What is a Singapore Common Criteria Scheme?



Singapore is recognized as a CC Certificate Authorising Nation as of January 2019. CC, also known as ISO/IEC 15408, is a widely accepted technical standard for assessing IT security. The Common Criteria Recognition Arrangement (CCRA), which allows CC certificates issued by an authorized nation to be mutually recognized across all member nations, has been signed by more than 30 countries as of this writing.

Singapore supports the CCRA's goals of increasing the accessibility of IT products that have been rigorously and consistently rated, removing the burden of redundant testing, and enhancing the effectiveness and efficiency of evaluations.



3.4.3 The Benefits of Singapore Common Criteria Scheme?

For Users:

- Better protect their digital assets and services
- Ensure that a product's security assessment is conducted consistently, objectively, and in accordance with international standards

For developers:

- Comply regulatory requirements
- Obtain market access without having to deal with redundant evaluations
- Create more secure products to stand out from the competition

3.4.4 Which products are being listed?

List of certified products can be accessed via the Common Criteria Portal (<https://www.commoncriteriaportal.org>).

Splunk Enterprise 8.1

It is listed at the common portal list. It has PKG_TLS_V1.1 & PP_APP_V1.3 for the Protection Profile.

IBM Security Access Manager for Enterprise Single Sign-On Version 8.2

It is listed at the common portal list. It has EAL3+, ALC_FLR.1 for the Assurance Level.

4. Conclusion

In conclusion, after doing research and evaluating 4 different SIEM products on the market based on their Design, Architecture, Main Functionalities, Strengths, Weaknesses, and Other factors, we decided that the most suitable SIEM product for the company Skrull Pte Ltd. with 200 HP Printers is Splunk Enterprise. We have also researched 2 indicators of compromise of the printers, as well as implemented rules to detect the compromise using Splunk's functions and features. Using this report, we hope that Skrull can make an informed decision on which SIEM product they want to use.

5. Appendix

Splunk Enterprise

Student Name/ID	Evaluation Item	Description	Reference/Comments
Francis/2123222	Design	-	-
Francis/2123222	Architecture	-	-
Francis/2123222	Functionalities	-	-
Francis/2123222	Strengths	-	-
Francis/2123222	Weaknesses	-	-
Francis/2123222	Others	-	-

IBM

Student Name/ID	Evaluation Item	Description	Reference/Comments
Marcus/2123392	Design	-	-
Marcus/2123392	Architecture	-	-
Marcus/2123392	Functionalities	-	-
Marcus/2123392	Strengths	-	-
Marcus/2123392	Weaknesses	-	-

RSA NetWitness

Student Name/ID	Evaluation Item	Description	Reference/Comments
Shushant/2123602	Design	-	-
Shushant/2123602	Architecture	-	-
Shushant/2123602	Functionalities	-	-
Shushant/2123602	Strengths	-	-
Shushant/2123602	Weaknesses	-	-

McAfee

Student Name/ID	Evaluation Item	Description	Reference/Comments
Adeeb/2107095	Design	-	-
Adeeb/2107095	Architecture	-	-
Adeeb/2107095	Functionalities	-	-
Adeeb/2107095	Strengths	-	-
Adeeb/2107095	Weaknesses	-	-

Overall Completion of Report and Proposed Solution

Student Name/ID	Evaluation Item	Description	Reference/Comments
Marcus/2123392	Executive Summary	-	-
Francis/2123222 Everyone discussed on the criteria to put and decide on the best product.	Recommendation of SIEM product	Splunk Enterprise	-
Shushant/2123602	Indicator of Compromise 1	-	-
Marcus/2123392	Indicator of Compromise 2	-	-
Marcus/2123392 Shushant/2123602	Rules implemented to detect compromise	-	-
Adeeb/2107095	The Government Recommendations	CSA is an organisation which does this assessment	
Francis/2123222	Conclusion	-	-
Shushant/2123602	Overall Formatting	-	-

6. References

Ecommerce subscription platform (2022) Recharge Payments. Available at: <https://rechargepayments.com/subscriptions/> (Accessed: November 21, 2022).

Fortra (2022) Evaluating security information and event management: Eight criteria for choosing the Right Siem Solution, Evaluating Security Information and Event Management: Eight Criteria for Choosing the Right SIEM Solution | Core Security. Available at: <https://www.coresecurity.com/blog/evaluating-security-information-and-event-management-eight-criteria-choosing-right-siem> (Accessed: November 24, 2022).

HP (2018) HP FutureSmart Printer Integration for Splunk® Security Information Event Management Solution. Available at: <http://h10032.www1.hp.com/ctg/Manual/c06181681.pdf> (Accessed: 2022).

Inc, G. (2022). RSA NetWitness Platform XDR Reviews, Ratings & Features 2022 | Gartner Peer Insights. [online] Gartner. Available at: <https://www.gartner.com/reviews/market/security-information-event-management/vendor/dell-technologies-rsa/product/netwitness-platform-xdr> [Accessed 23 Nov. 2022].

NetWitness.com (2022). NetWitness Platform – See Everything, Fear Nothing. [online] Available at: <https://www.netwitness.com/> [Accessed 23 Nov. 2022].

RSA Link (2022). NetWitness Platform Online Documentation. [online] Available at: <https://community.netwitness.com/t5/netwitness-platform-online/tkb-p/netwitness-online-documentation> [Accessed 23 Nov. 2022].

RSA Link. (2018). RSA NetWitness Logs & Network 11.0 Guides (All-in-One PDF). [online] Available at: <https://community.netwitness.com/t5/netwitness-platform-online/rsa-netwitness-logs-network-11-0-guides-all-in-one-pdf/ta-p/554728> [Accessed 23 Nov. 2022].

Splunk (2022) 2022 gartner Magic Quadrant for Siem: Splunk named a leader for the 9th consecutive yearSp, Splunk. Available at: https://www.splunk.com/en_us/blog/security/2022-gartner-magic-quadrant-for-siem-splunk-named-a-leader-for-the-9th-consecutive-year.html#:~:text=Moreover%2C%20the%20recently%20released%20Gartner,for%20making%20this%20recognition%20possible. (Accessed: November 20, 2022).

Splunk (2022) About data models, About data models - Splunk Documentation. Available at: <https://docs.splunk.com/Documentation/Splunk/9.0.2/Knowledge/Aboutdatamodels> (Accessed: November 20, 2022).

Spunk (2022) Awards, Splunk. Available at: https://www.splunk.com/en_us/about-splunk/awards.html (Accessed: November 20, 2022).

Splunk (2022) Hardware and software requirements, Hardware and Software Requirements - Splunk Documentation. Available at: <https://docs.splunk.com/Documentation/DSP/1.3.1/Admin/Compatibility> (Accessed: November 19, 2022).

Splunk (2022) Indexes, indexers, and indexer clusters, Indexes, indexers, and indexer clusters - Splunk Documentation. Available at: <https://docs.splunk.com/Documentation/Splunk/9.0.2/Indexer/Aboutindexesandindexers> (Accessed: November 20, 2022).

Splunk (2020) Paying it forward: Recharge positions itself for rapid growth with Google Cloud and Splunk. Available at: https://www.splunk.com/en_us/pdfs/partners/partner-briefs/recharge-google-cloud-and-splunk.pdf (Accessed: November 21, 2022).

Splunk (2022) Scaling your splunk enterprise deployment, Splunk Lantern. Splunk. Available at: https://lantern.splunk.com/Splunk_Platform/Product_Tips/Enterprise/Scaling_your_Splunk_Enterprise_deployment (Accessed: November 16, 2022).

Splunk (2022) Splunk enterprise product features, Splunk. Available at: https://www.splunk.com/en_us/products/splunk-enterprise-features.html (Accessed: November 20, 2022).

Splunk (2022) Splunk Enterprise Security product brief, Splunk Enterprise Security Product Brief. Available at: <https://www.splunk.com/pdfs/product-briefs/splunk-enterprise-security.pdf> (Accessed: November 16, 2022).

Splunk (2022) Splunk enterprise. Available at: <https://www.splunk.com/pdfs/product-briefs/splunk-enterprise.pdf> (Accessed: November 19, 2022).

Splunk (2022) Why customers choose Splunk, Splunk. Available at: https://www.splunk.com/en_us/about-us/why-splunk.html (Accessed: November 20, 2022).

Taylor, D. (2022) Splunk tutorial for beginners: What is splunk tool? how to use?, Guru99. Available at: <https://www.guru99.com/splunk-tutorial.html#:~:text=Disadvantages%20of%20using%20Splunk,-Some%20disadvantages%20of&text=Splunk%20can%20prove%20expensive%20for,time%20to%20learn%20this%20tool>. (Accessed: November 20, 2022).

tutorialspoint (2022) Splunk - schedules and alerts, Tutorials Point. Available at: https://www.tutorialspoint.com/splunk/splunk_schedules_and_alerts.htm#:~:text=Splunk%20alerts%20are%20actions%20which,to%20a%20lookup%20file%2C%20etc. (Accessed: November 20, 2022).

Vardhan (2021) Splunk Architecture: Forwarder, Indexer & Search head tutorial, Edureka. Available at: <https://www.edureka.co/blog/splunk-architecture/> (Accessed: November 16, 2022).

www.peerspot.com. (2022). NetWitness Platform Reviews, Competitors and Pricing. [online] Available at: <https://www.peerspot.com/products/netwitness-platform-reviews> [Accessed 23 Nov. 2022].

Cyber Security Agency. (2022). CSA | Singapore Common Criteria Scheme. [online] Available at: <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/about-cc> [Accessed 23 Nov. 2022].

Cyber Security Agency. (n.d.). Cybersecurity Certification Centre. [online] Available at: <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/cybersecurity-certification-centre> [Accessed 23 Nov. 2022].

Cyber Security Agency. (n.d.). CSA / Our Organisation. [online] Available at: <https://www.csa.gov.sg/who-we-are/our-organisation>.

Cyber Security Agency. (n.d.). CSA | Singapore Common Criteria Scheme - Product List. [online] Available at: <https://www.csa.gov.sg/Programmes/certification-and-labelling-schemes/csa-common-criteria/product-list> [Accessed 23 Nov. 2022].

www.commoncriteriaportal.org. (n.d.). Certified Products : New CC Portal. [online] Available at: <https://www.commoncriteriaportal.org/products/#> [Accessed 23 Nov. 2022].

Commoncriteriaportal.org. (2017). [online] Available at: https://www.commoncriteriaportal.org/products/certified_products.csv [Accessed 23 Nov. 2022].

Docs.mcafee.com. 2021. [online] Available at: <https://docs.mcafee.com/bundle/enterprise-security-manager-11.2.x-installation-guide/page/GUID-6D03A7BA-5FCA-4879-885A-BAC46F5A8137.html> [Accessed 23 Nov. 2022].

Docs.mcafee.com. 2021. [online] Available at: <https://docs.mcafee.com/bundle/enterprise-security-manager-11.3.x-product-guide/page/GUID-88473528-B9BD-4799-B3A7-BC7A8C22B55D.html> [Accessed 8 December 2021]. Docs.mcafee.com. 2021. [online] Available at: <https://docs.mcafee.com/bundle/enterprise-security-manager-11.3.x-product-guide/page/GUID-CC250175-1B53-427E-BDC1-F3119856059E.html> [Accessed 23 Nov. 2022].

Docs.mcafee.com. 2021. [online] Available at: <https://docs.mcafee.com/bundle/enterprise-security-manager-11.2.x-installation-guide/page/GUID-EB0C611C-B5B4-405F-BFDC-ED8C88A9A491.html> [Accessed 23 Nov. 2022].

Download.manageengine.com. 2021. [online] Available at: <https://download.manageengine.com/log-management/log360-2019-siem-customer-experience-report.pdf> [Accessed 23 Nov. 2022].

Trust Radius. 2021. McAfee Enterprise Security Manager Reviews. [online] Available at: <https://www.trustradius.com/products/mcafee-enterprise-security-manager/reviews?o=recent> [Accessed 23 Nov. 2022].

Gartner. 2021. McAfee Reviews. [online] Available at: <https://www.gartner.com/reviews/market/security-information-event-management/vendor/trellix/product/trellix-security-manager> [Accessed 23 Nov. 2022].

Kc.mcafee.com. 2021. Supported platforms for Enterprise Security Manager. [online] Available at: <https://kc.mcafee.com/corporate/index?page=content&id=KB82516> [Accessed 23 Nov. 2022].

expertinsights.com. (2022). McAfee Enterprise Security Manager (ESM) Reviews and Pricing | Expert Insights. [online] Available at: <https://expertinsights.com/reviews/mcafee-enterprise-security-manager-esm> [Accessed 23 Nov. 2022].

McAfee Enterprise Security Manager Reviews & product details - G2 (2022). Available at: <https://www.g2.com/products/mcafee-enterprise-security-manager/reviews> [Accessed 23 Nov. 2022].

www.youtube.com. (2022). McAfee ESM Knowledge Transfer Session. [online] Available at: https://www.youtube.com/watch?v=1Cnb7wjVbnc&ab_channel=CyberSecurityLearning [Accessed 23 Nov. 2022].

SIEM Foundation. (2022). [online] Available at: <https://www.mcafee.com/enterprise/en-us/assets/data-sheets/ds-siem-solutions-from-mcafee.pdf>. [Accessed 23 Nov. 2022].

Palmer, T. and McAfee (2018). Intelligent, Actionable, and Integrated Security Information and Event Management (SIEM) Senior IT Validation Analyst; and Alex Arcilla, IT Validation Analyst ESG Lab Validation. [online] Available at: <https://www.esg->

[global.com/hubfs/images/LabReports/McAfeeEnterpriseSecurityManagerMay2018/ESG-Lab-Validation-McAfee-Enterprise-Security-Manager-May-2018.pdf](https://www.mcafee.com/hubfs/images/LabReports/McAfeeEnterpriseSecurityManagerMay2018/ESG-Lab-Validation-McAfee-Enterprise-Security-Manager-May-2018.pdf) [Accessed 23 Nov. 2022].