Cyber Security Briefing: Countering Cyber Threats

NCI Post Graduate Diploma Cyber Security
Semester 1

Author: Jonathon Taaffe

Title: Cyber Security Briefing: Countering Cyber Threats
Author: Jonathon Taaffe

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this publication, the author assumes no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

Warning and Disclaimer
The information is provided on an “as is” basis. The author shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this publication. The opinions expressed in this publication belong to the author.

Trademark Acknowledgments
All terms mentioned in this publication that are known to be trademarks or service marks have been appropriately capitalised. The author cannot attest to the accuracy of this information. Use of a term in this publication should not be regarded as affecting the validity of any trademark or service mark.

Contents

Executive Summary

This *Cyber Security Briefing: Countering Cyber Threats* report is a detailed analysis of the requirement for a Security Monitoring (SOC) solution.

This report presents detailed intelligence outlining the current Global Cyber Security Threat Landscape, Internal Cyber Security Threats, the clients current Security Monitoring Controls and demonstrates the necessity for a comprehensive Security Monitoring (SOC) solution at the client to better manage exposure to Internal and External Cyber Threats.

Cyber Security Threats – Global

In Accenture's 2018 State of Cyber Resilience report [1], CISO's responded

- **33%** of their organisation is not protected by their Cyber Security program.
- **83%** agree new technologies and solutions are essential to securing the organization.
- **71%** commented cyber attacks are still a "bit of a black box; we don't know how they are going to affect our organization."

Threat Actors (cyber criminals) have demonstrated a voracious ability to innovate at velocity appearing to stay n^2 steps ahead of defences. Cyber-attacks are now recognised as the primary risk for businesses and organisations.

> *"The risks to business, privacy and related data grow by the day — so much so that cybersecurity is outranking some of the more traditional business risks and concerns,"*
> SonicWall CEO Bill Conner [2]

Forbes Cyber Security Year on Year 2018-2019 Threat predictions[3] clearly confirms there is no sign of cyber-attacks declining, quite the opposite

+ **14%** Zero-day Attacks
+ **15%** Phishing Attacks
+ **151%** Malware Attacks
+ **226%** Ransomware Attacks
+ **430%** Encryption-based Attacks

As cyber threats continue to evolve, becoming more complex and sophisticated, they are proving difficult to detect. The CYFIRMA Cyber Security Threat forecast for 2019 [4] highlights existing cyber threats including:

- Social Engineering Attacks
- Crypto Mining Malware
- Banking Trojans
- Ransomware Attacks

But also includes new cyber-attack vectors namely:

- AI Machine Learning Botnet Attacks
- Internet of Things Cyber Threats
- Supply Chain Malware Attacks
- Exploitation of GDPR Procedures

These cyber-threats are 'real'; cyber-attacks have already occurred using these existing and new attack vectors. As new technology is developed, new attack opportunities are discovered.

[1] Accenture (2018) *2018 State of Cyber Resilience* https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf [Accessed 26th April 2019].

[2] Help Net Security (2018) *Cyber attacks becoming No. 1 business risk* https://www.helpnetsecurity.com/2018/03/07/cyber-attacks-business-risk/ [Accessed 26th April 2019].

[3] Forbes (2018) *Real-Time Cyber Threat Intelligence Is More Critical Than Ever* https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/ [Accessed 26th April 2019].

[4] CYFIRMA (2018) *CYFIRMA's Cyber Threat and Risk Prediction Report for 2019* https://www.cyfirma.com/insights/cyfirmas-cyber-threat-and-risk-prediction-report-for-2019/ [Accessed 26th April 2019].

In addition to CYFIRMA Cyber Security Threat forecast, US Cyber Security Magazine reports the following additional risks to take note of for 2019 [5]

- Insecure Application User Interface (API)
- Cloud Abuse
- Single Factor Passwords
- Shadow IT Systems (software used in organizations not supported by IT)

CYFIRMA and US Cyber Security Magazine threat lists above clearly demonstrate there is no single line of defence and no 100% secure platform. To ensure Cyber Security protection, businesses must continually evaluate and optimise security solutions and policies, utilise real-time cyber threat intelligence and develop an integrated, defence-in-depth Cyber Security model.

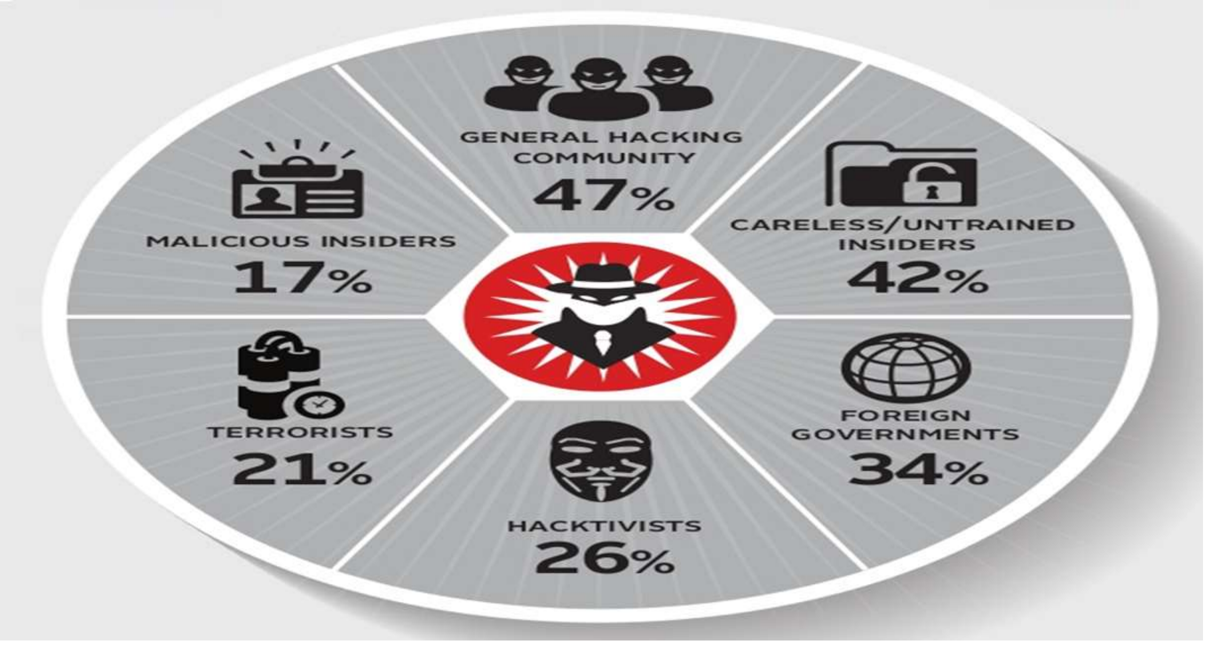


Image 1: Security Threat Sources [6]

[5] United States Cyber Security Magazine (2018) *Top 10 Cybersecurity Risks For 2019* https://www.uscybersecurity.net/risks-2019/ [Accessed 27th April 2019].

[6] Week 8 – Security Fundamentals (2019) *Security Threat Sources Slide 53* https://moodle.ncirl.ie/mod/resource/view.php?id=52586 [Accessed 27th April 2019].

Cyber Security Threats – Internal

So far, I have highlighted global threats which can impact any company or organisation. One area that must be incorporated and, that the client can enforce security controls on, are internal cyber threats.

The Identity Theft Resource Center® (ITRC) reported a 44.7% [7] increase in data breaches for 2017 in the US alone. This increase is primarily due to businesses and organisations becoming more transparent regarding data breach reporting. The ITRC Data Breach list, which tracks 5 industry sectors, reported total number of breaches per sector as follows:

55.0% Business Sector

23.7% Medical/Healthcare Industry

8.5% Banking/Credit/Financial Sector

8% Educational Sector

4.7% Government/Military Sector

ITRC data breach tracking over a 12-year period shows overall declines in the Banking/Credit/Financial, Educational and Government/Military Sectors but increases in the Business and Medical/Healthcare Industry

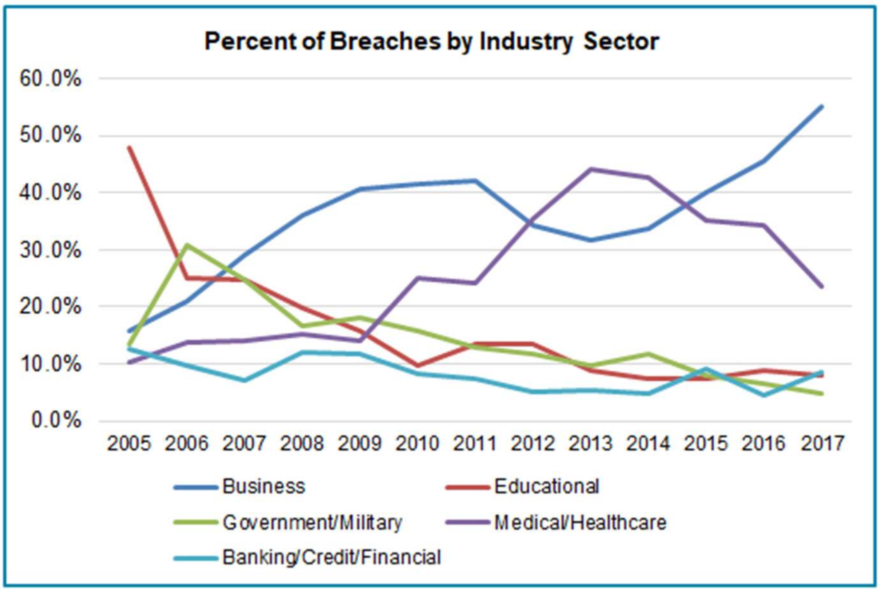


Figure 1. ITRC Percent of Breaches by Industry Sector [7]

ITRC also gives a breakdown of the data breaches by attack types including

- Hacking (including phishing, ransomware, malware and skimming)
- Unauthorized Access
- Insider Theft
- Data on the move
- Accidental Exposure

[7] Identity Theft Resource Center (2018) *2017 Annual Data Breach Year-End Review* https://www.idtheftcenter.org/2017-data-breaches/ [Accessed 29th April 2019].

- Employee error/negligence/improper disposal/loss

As represented by the ITRC data, hacking is and remains the highest attack type with 59.4% of overall breaches.

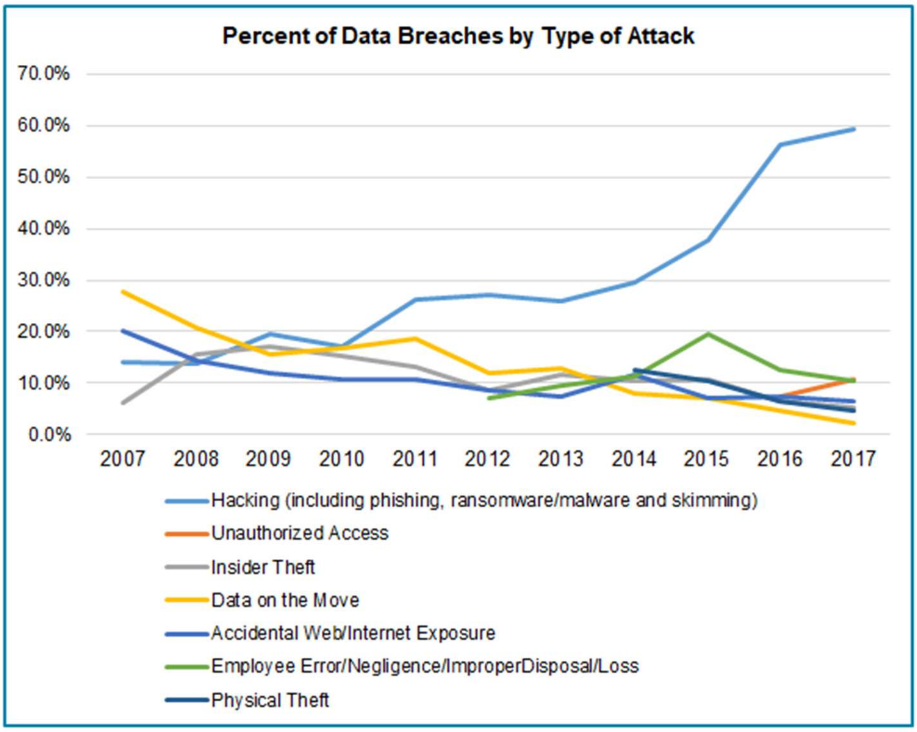


Figure 2. ITRC Percent of Data Breaches by Type of Attack [7]

A breakdown of the hacking category reveals:

21.4% Phishing Attacks

12.4% Ransomware/Malware Attacks

11% Unauthorized Access Attacks

Preventing unlawful access to company data is paramount. Data breaches not only cause financial losses for businesses, reputational damage is also inflicted. Implementing innovative data security strategies is vital but a thorough understanding of the most significant data threats is required.

You can't protect what you can't see! [8]

Phoenix NAP collaborated with 31 Cyber Security Industry Exports [9] and posted an in-depth analysis on business data security predictions for 2019. This analysis is far reaching and ranges from Inadequate Cyber Hygiene to Personal Identifiable Information loss to Crypto-Jacking.

This analysis re-emphasises the focus on internal cyber threats, which is an area the client can and must control.

[8] CSO Online (2018) *You can't protect what you can't see* https://www.csoonline.com/article/3256211/you-cant-protect-what-you-cant-see.html [Accessed 30th April 2019].

[9] Phoenix NAP (2018) *2019 Cybersecurity Trends: 31 Experts on Current Issues* https://phoenixnap.com/blog/cybersecurity-experts-threats-trends [Accessed 30th April 2019].

Summary analysis of Phoenix NAP’s Cyber Security Trends in the context of the client

#	Prediction	Category	Contributor	Risk[1]	Control[2]
1	Privileged Account Abuse	Accounts	Csaba Krasznay	H	Yes
11	Weak Passwords	Accounts	Ori Eisen	H	Yes
29	Advanced Persistent AI Threats	AI	Matt Corney	L	No
25	AI and Automation Development	AI	Harrison Brady	L	No
3	Machine Learning Hacking	AI	Monica Eaton-Cardone	L	No
20	Blockchain Attacks	Blockchain	Monika Goldberg	L	No
27	Crypto-Jacking	Blockchain	Kashif Yaqoob	L	No
14	New Technologies/New Attacks	Blockchain	David Kosmayer	M	No
10	Incorrect Cloud Data Security	Cloud	Timothy Platt	H	Partial
30	Incorrect Cloud Permissions	Cloud	Pete Markowsky	H	Partial
21	Endpoint Security	Endpoints	Rob Juncker	M	Partial
24	Outdated Equipment	Equipment	Amy O	L	Yes
31	IoT Device Attacks	IoT	George Tatar	L	No
17	Email Phishing Attacks	Phishing	Pieter Van Iperen	H	Partial
23	Email Phishing Attacks (Mailsploit)	Phishing	Eyal Benishti	H	Partial
26	Digital Technology Growth and PII	PII	Felicity Cooper	H	Partial
15	Smartphone and PII Data Loss	PII	Keith Moore	H	Partial
18	Malware Attacks	Malware	David Friend	H	Partial
5	Ransomware and zero-day attacks	Ransomware	Greg Scott	H	Partial
13	Sophisticated Ransomware	Ransomware	Ian Pratt	H	Partial
7	Inadequate Cyber Hygiene	Security Strategy	Nik Whitfield	H	Yes
2	Inadequate Security Strategies	Security Strategy	Dr. Salvatore Stolfo	H	Yes
22	Internal Cyber Attacks	Security Strategy	Larry Lunetta	H	Partial

[1] Risk: This is either a High, Medium or Low Risk

[2] Control: There is, there is not or there is a partial security control currently in place

Table 1. Summary of Phoenix NAP analysis on business data security predictions for 2019 [10]

[10] Phoenix NAP (2018) *2019 Cybersecurity Trends: 31 Experts on Current Issues* https://phoenixnap.com/blog/cybersecurity-experts-threats-trends [Accessed 30th April 2019].

Event Monitoring Controls

A computing event is

> *"…an action or occurrence recognised by software, often originating asynchronously from the external environment, that may be handled by the software."* [11]

Events range from Informational (user logon) to Critical (physical component failure) and are stored locally on IT assets. Critical security, hardware, operating system and application events are monitored, and critical events trigger alerts to the relevant IT support group:

- Security alerts to Security Operations Centre (SOC)
- Network alerts to Network Operations Centre (NOC)
- Server alerts to Server Operations Centre (SRVOC)
- Application alerts to Application Operations Centre (AOC)

The client's event monitoring solutions evolved over time and deployments were not centrally managed. The event monitoring solutions landscape consists of:

4 Disconnected Isolated Alert Platforms

- With separate Security, Network, Server and Application Alert Platforms

10 Separate Vendor/Device Alert Platforms

- Additional Separate Vendor Alert Platforms within Isolated Alert Platforms including: Separate Cisco, Checkpoint, HP, Dell, IBM, Microsoft, JBoss, etc. Alert Platforms

0 Single Central Events Database

0 Single Central Administrative 'Company-wide' Event Console

0% Internal Support Centre Event Correlation

0% Event Cross-Correlation between Support Centres

0% Informational, Error or Warning Event Monitoring

Image 2. Client Event Monitoring Controls Word Cloud

[11] Wikipedia.org (2019) *Event (computing)* https://en.wikipedia.org/wiki/Event_(computing) [Accessed 31st April 2019].

Event Monitoring Landscape

The image below is a graphical representation of the client's Event Monitoring Landscape[12]. The key takeaways are:

4 Disconnected Isolated Alert Platforms

0 Single Central Events Database

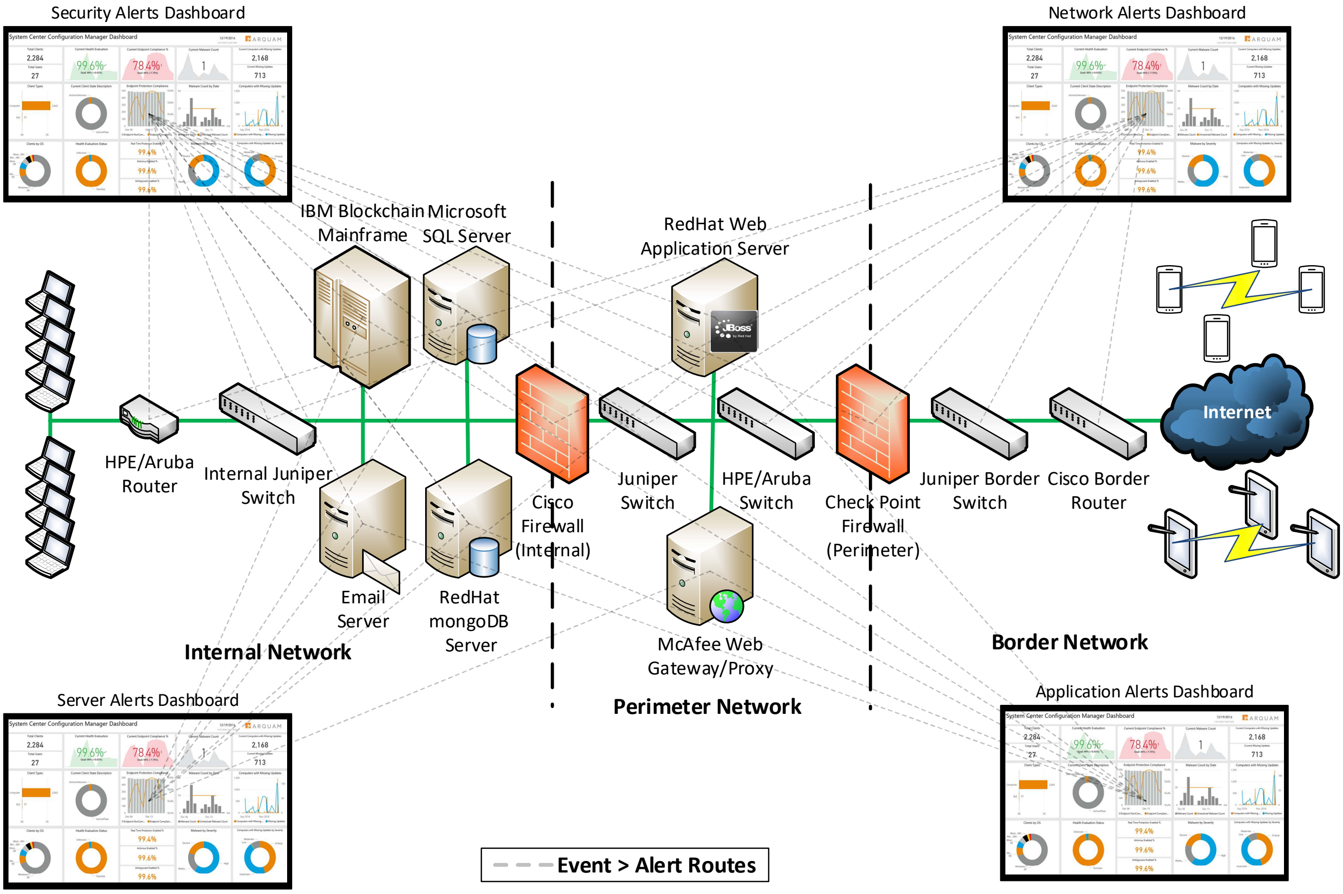


Image 3. Client Event Monitoring Landscape

[12] Taaffe, J. (2019) Client *Event Monitoring Landscape* [Created 31st April 2019].

Security Monitoring Controls Solution Requirements

In choosing a Security Controls Solution that ensures Cyber Security resilience, the following key features [13] must be integral to the chosen solution

Priority	Weight	Details
1	25.00	Advanced Security Incident Management with Automated Real Time Cyber Threat Remediation
2	15.00	Real Time Cyber Threat Visibility
3	15.00	Advanced Security Event Alerting and Compliance Reporting
4	10.00	Centralised Collection, Aggregation and Normalisation (CAN) of Security Event Data
5	10.00	Correlation and Orchestration of Security Event Data
6	10.00	Real Time Cyber Threat Intelligence (Feed)
7	5.00	Scalable with Minimal Network Latency
8	5.00	Security Data Management and Retention
9	5.00	Advanced Forensic Analysis Support

Table 2. Key Security Controls Solution Features [13]

Additional considerations that also need to be factored into the solution include

Priority	Weight	Details
1	30.00	Cost
2	25.00	Centralised Administrative Console
3	25.00	Vendor Support
4	10.00	Vendor and Device Independence
5	10.00	Agent and Agentless Log Shipping

Table 3. Key Security Controls Solution Considerations [13]

[13] Info-Tech Research (2019) *Select and Implement a SIEM Solution* https://www.infotech.com/research/ss/select-and-implement-a-siem-solution [Accessed 31st April 2019].

Security Monitoring Controls Proposal

Deploy a Security Information and Event Management (SIEM) system into which all security, network, server and application events are routed, stored, analysed, correlated and actioned either manually or automatically.

A Security Information and Event Management (SIEM) system combines Security Information Management (SIM) which stores, analyses and reports on event data, and Security Event Management (SEM) which enables real-time monitoring and alert notification.

A SIEM System monitors threats, provides real time security alerts and facilitates policy and regulation compliance.

Security Information and Event Management (SIEM) Benefits [14]

Primary Function: Detect, identify, alert and remediate security events.

Increase Efficiency: Collate multiple network connected device event logs enabling Security Operations Centre to rapidly identify and manage security events. Improved information management reducing irrelevant data analysis.

Visibility: Provision of 'real-time' activity across networks improving event analysis and response.

Security Breach Prevention: Security event detection prior to breach potentially preventing damage.

Impact Reduction: Instantaneous security event detection significantly reducing impact. Early detection preventing a breach ensures no financial or reputation loss.

Expenditure

- **Reduction:** Minimise capital expenditure and deployment costs with SIEM trend reporting.
- **Focused:** identify and prioritise capacity related issues to inform capital investment.

Enhanced Reporting and Analysis

- **Comprehensive**: network activity reporting providing detailed analysis for Security Operations, IT Management, Finance, Human Resources and IT Operations.
- **Assets:** Network connected asset identification and utilisation.
- **Identity and Access Management (IAM):** Unauthorised and unusual authentication and access reporting.
- **Compliance [15] :** Enhanced reporting and analysis supports regulatory compliance, for example:
    - Cyber Security Compliance
    - GDPR Data Protection Compliance
    - Trading Regulations Compliance
    - Sarbanes-Oxley Compliance
    - Payment Card Industry Data Security Standard (PCI DSS) Compliance

[14] Computer Weekly (2019) *Security information and event management (SIEM) systems streamline compliance* https://www.computerweekly.com/tip/Security-information-and-event-management-SIEM-systems-streamline-compliance [Accessed 1st April 2019].

[15] Tech Target (2018) *SIEM benefits include efficient incident response, compliance* https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products [Accessed 1st April 2019].

SIEM Use Cases

In choosing a SIEM solution fit for the client SIEM Use Cases need to be defined, identified and documented. Use cases will determine the SIEM features required which will then assist with vendor choice. There are 2 types of defined Use Cases:

1. High-level SIEM Use Case Definition
2. Specific SIEM Function Use Case Definition (Starter Use)

High-level SIEM Use Case Definition [16]

The following Use Case definitions describe high-level requirements for deploying a SIEM:

- **Threat Management:** for security-conscious organisations whose protection of data and/or intellectual property from internal or external threats is paramount.
- **Compliance Management:** for compliance focussed organisations pursuing regulatory and industry compliance.
- **Management of Security Events:** for large scale globally dispersed security event management.
- **SME Deployment:** SME's who require a streamlined SIEM with fewer advanced features while still ensuring effective security oversight.
- **Risk Management:** where an organisation requires data protection security controls and alignment with compliance obligations, while also providing risk visibility.

SIEM Functional Use Case Definition (Starter Use) [17]

The following Function Specific or SIEM Starter Use Cases focus on identifying the specific functions of a SIEM an organisation requires:

Use Case	Description
1	Authentication Event Mapping and Account Compromise Detection
2	System Compromise Detection
3	Vulnerability Detection
4	Exfiltration and Suspicious Network Connectivity
5	Application Attack Detection
6	Cloud Security Monitoring
7	Threat Intelligence and Threat Detection

Table 4. SIEM Function Use Case Definition (Starter Use) [17]

[16] Log Rhythm (2015) *Select and Implement a SIEM Solution (Slide 23)* https://logrhythm.com/pdfs/3rd-party-review/lr-info-tech-select-and-implement-a-siem-solution-2015-full-report-3rd-party-review.pdf [Accessed 1st April 2019].

[17] Anton Chuvakin, Gartner (2018) 2018 Popular SIEM Starter Use Cases https://blogs.gartner.com/anton-chuvakin/2018/07/20/2018-popular-siem-starter-use-cases/ [Accessed 1st April 2019].

SIEM Client Use Cases

From the analysis, the client's high-level Use Case is for a **SME SIEM Deployment**. This will provide a streamlined SIEM, keeping costs low, while providing effective security oversight.

Regarding the specific SIEM functions required, focus should be **Threat, Compromise, Vulnerability Detection wit Compliance Reporting**.

SIEM Vendor Analysis

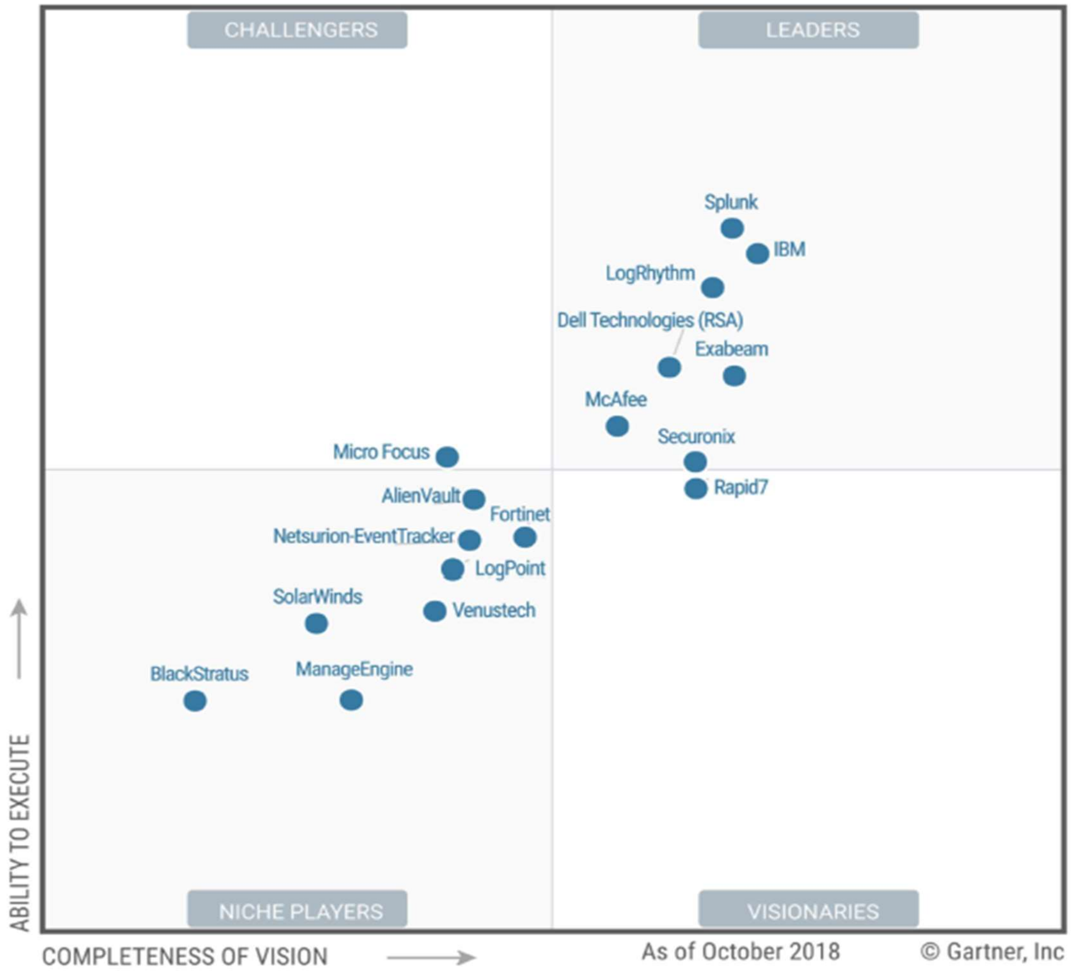
In December 2018, Gartner complete a comprehensive analysis of the Security Information and Event Management market and provided a detailed report on the solutions provided by the SIEM industry leaders.

Gartner's detailed analysis can be accessed at:

Source: https://www.gartner.com/doc/3894573/magic-quadrant-security-information-event

Download: https://logrhythm.com/gartner-magic-quadrant-siem-report-2018/

Gartner produced a Magic Quadrant for Security Information and Event Management (SIEM) [18] which provides a summarised view of their extensive analysis into the Security Information and Event Management market as follows



Source: Gartner (December 2018)

Figure 3. Gartner Magic Quadrant for Security Information and Event Management (SIEM) [18]

[18] Gartner (2018) *Magic Quadrant for Security Information and Event Management (SIEM) ID G00348811* https://www.gartner.com/doc/3894573/magic-quadrant-security-information-event (document source) https://logrhythm.com/gartner-magic-quadrant-siem-report-2018/ (download source) [Accessed 2nd April 2019].

SIEM Feature Analysis

Applying Gartner's extensive market research to the client's Solution Requirements (page 10), High-level Use Case and Specific SIEM Functions Required (page 13), vendor analysis is focussed on the following vendors:

- LogRhythm
- McAfee
- Solarwinds
- IBM
- Event Tracker
- Splunk

Summary of Vendor to Feature to Client Requirements Analysis is as follows [19]

	Vendors					
Feature	LogRhythm	McAfee	Solarwinds	IBM	Event Tracker	Splunk
Advanced Security Incident Management with Automated Real Time Cyber Threat Remediation	****	***	***	**	***	***
Real Time Cyber Threat Visibility	***	****	***	***	**	**
Advanced Security Event Alerting and Compliance Reporting	****	***	***	***	**	**
Centralised Collection, Aggregation and Normalisation (CAN) of Security Event Data	****	***	**	***	**	**
Correlation and Orchestration of Security Event Data	****	****	***	**	***	***
Real Time Cyber Threat Intelligence (Feed)	****	****	**	**	***	**
Scalable with Minimal Network Latency	****	****	***	**	**	***
Security Data Management and Retention	***	****	***	**	**	**
Advanced Forensic Analysis Support	****	**	***	***	***	**
Overall Result	****	***	***	***	**	**

****	Best in Class
***	Good
**	Adequate

Table 5. Vendor to Feature to Client Requirements Analysis [20]

[19] Info-Tech Research (2019) *SIEM Solutions Comparison Tool* http://siemcomparison.com/ [Accessed 2nd April 2019].

[20] Taaffe, J. (2019) Detailed analysis of Vendor to Feature to Client requirements analysis [Created 3rd April 2019].

SIEM Additional Considerations

In addition to the Vendor to Feature to Client Requirements Analysis on the previous page, I have also analysed Vendor to Additional Considerations (page 10) to the Client's requirements.

The additional Considerations for the client's solution included:

Priority	Weight	Details
1	30.00	Cost
2	25.00	Centralised Administrative Console
3	25.00	Vendor Support
4	10.00	Vendor and Device Independence
5	10.00	Agent and Agentless Log Shipping

Table 3. Key Security Controls Solution Considerations [21]

Summary of Vendor to Additional Considerations to Client Requirements Analysis is as follows [22]

	Vendors					
Consideration	**LogRhythm**	**McAfee**	**Solarwinds**	**IBM**	**Event Tracker**	**Splunk**
Cost	****	**	****	**	****	**
Centralised Administrative Console	****	****	***	***	***	***
Vendor Support	***	***	***	****	***	***
Vendor and Device Independence	****	***	**	****	**	***
Agent and Agentless Log Shipping	****	***	**	****	**	***
Overall Result	****	***	***	***	***	**

****	Best in Class
***	Good
**	Adequate

Table 6. Vendor to Additional Considerations to Client Requirements Analysis [23]

[21] Taaffe, J. (2019) *Table 3. Table 3. Key Security Controls Solution Considerations* https://www.infotech.com/research/ss/select-and-implement-a-siem-solution [Accessed 3rd April 2019].

[22] Info-Tech Research Group (2019) *SIEM Solutions Comparison Tool* http://siemcomparison.com/ [Accessed 3rd April 2019].

[23] Taaffe, J. (2019) *Table 6. Vendor to Additional Considerations to Client Requirements Analysis* [Created 3rd April 2019].

SIEM Vendor Selection

Combining the Client’s Security Monitoring Controls Solution Requirements (Page 10) and the Client’s SIEM specific Use Case (SME Deployment) with a focus on Threat, Compromise and Vulnerability Detection (Page 12) and Gartner’s market analysis including Vendor Strengths and Cautions (page 15), the following 3 vendors were chosen:

LogRhythm The Security Intelligence Company [24]   McAfee Together is power. [25]   solarwinds [26]

Vendor	Solution Name	Solution URL
LogRhythm	NextGen SIEM Platform	https://logrhythm.com/solutions/security/siem/
McAfee	Enterprise Security Manager	https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html
Solarwinds	Log & Event Manager	https://www.solarwinds.com/log-event-manager-software

Table 7. Chosen Vendor, Solution Name and Solution URL [27]

[24] LogRhythm (2019) *LogRhythm Official Logo* https://logrhythm.com/about/branding-guidelines/ [Accessed 4th April 2019].
[25] McAfee (2019) *McAfee Official Logo* https://www.mcafee.com/enterprise/en-us/mcafee-brand.html [Accessed 4th April 2019].
[26] Solarwinds (2019) *Solarwinds Official Logo* https://www.solarwinds.com/ [Accessed 4th April 2019].
[27] Taaffe, J. (2109) *Table 7. Chosen Vendor, Solution Name and Solution URL* [Created 4th April 2019].

SPAM Costs to the Client

Applying a real-world scenario where SIEM can have an immediate beneficial impact to is regarding SPAM. In my Q1 2019 *Cyber Security Briefing: The Threat of SPAM* [28] I presented analysis of the volume, the impact and the cost of SPAM to the client.

The following excerpts highlight the impact SPAM has at the client

Productivity Impact

- 3 SPAM Emails per Employee per Day @ 90 seconds to address each SPAM email
- **500 Total Hours Lost Company-wide per year**

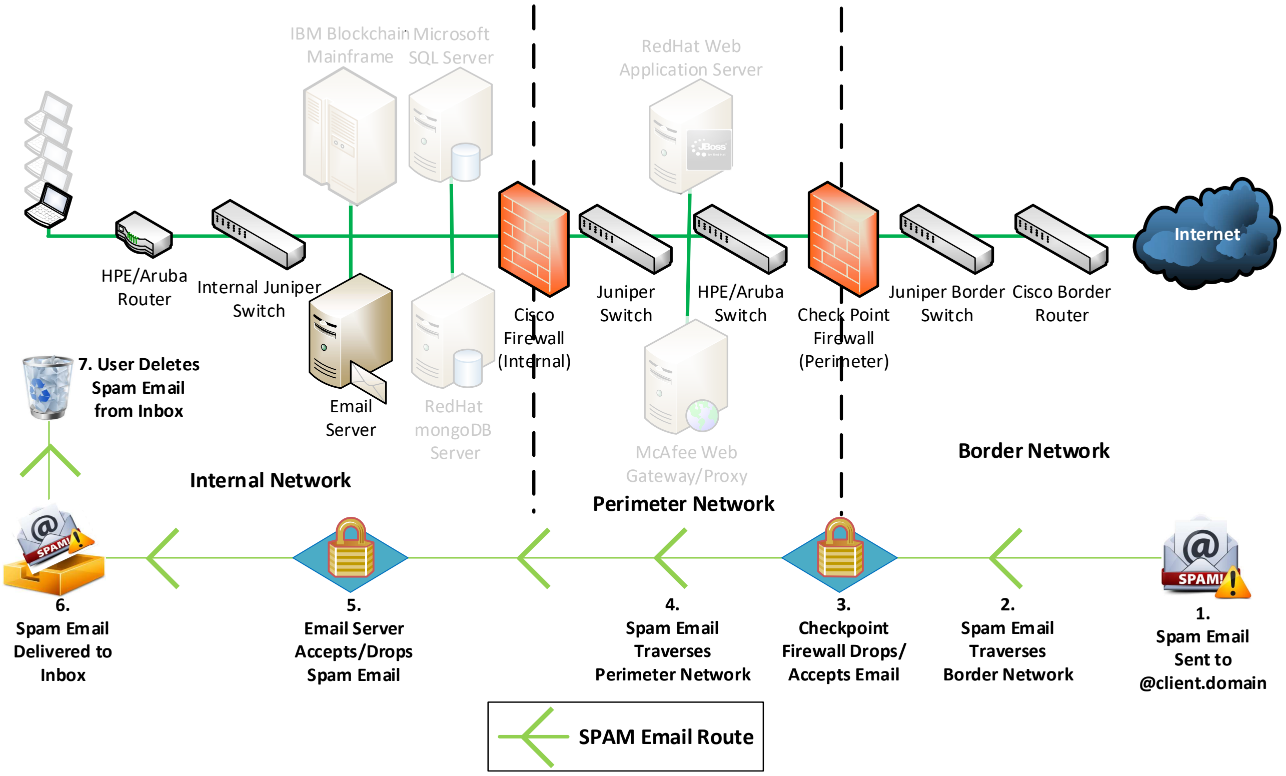
Cost Impact

- €12,500 Productivity Loss + €18,500 IT Storage Costs
- **€21,000 Total Annual Cost of SPAM**

[28] Taaffe, J. (2019) *Cyber Security Briefing: The Threat of SPAM* [Created Q1 2019].

SPAM Email Route through Clients Network

The following diagram [29] shows the route a SPAM email which evades our first-line defences will take from the Internet (on the right) through to a client's inbox:


IBM Blockchain Mainframe
Microsoft SQL Server
RedHat Web Application Server
HPE/Aruba Router
Internal Juniper Switch
Email Server
RedHat mongoDB Server
Cisco Firewall (Internal)
Juniper Switch
HPE/Aruba Switch
McAfee Web Gateway/Proxy
Check Point Firewall (Perimeter)
Juniper Border Switch
Cisco Border Router
Internet
7. User Deletes Spam Email from Inbox
Internal Network
Perimeter Network
Border Network
6. Spam Email Delivered to Inbox
5. Email Server Accepts/Drops Spam Email
4. Spam Email Traverses Perimeter Network
3. Checkpoint Firewall Drops/ Accepts Email
2. Spam Email Traverses Border Network
1. Spam Email Sent to @client.domain
SPAM
SPAM Email Route

Process Flow

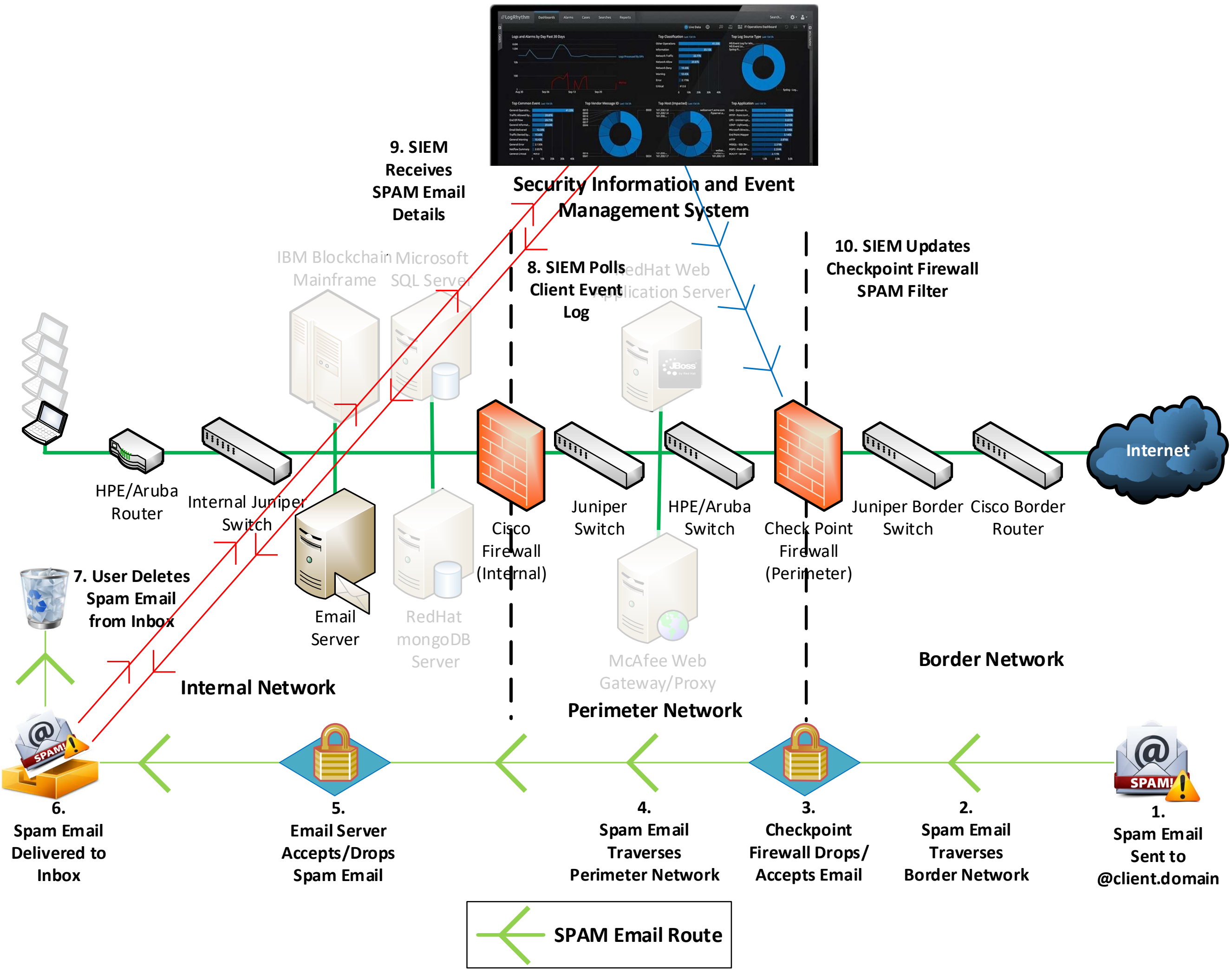
1. Spam Email Sent from Threat Actor or BotNet to a @client.domain email address
2. Spam Email Traverses Client Border Network enroute to Checkpoint Firewall
3. Checkpoint Firewall will apply SPAM filters to the Email and will either Drop or Accept the Email
4. If the Checkpoint Firewall does not identify the email as SPAM accepts it, the Spam Email will traverse the client's Perimeter Network
5. The Spam email will be routed to the client's Email Server and will also apply SPAM filters and will either Drop or Accept the Email
6. If the Spam Email avoids both SPAM filters it will be delivered to an employee Inbox
7. The user the reviews the email, determines its SPAM and deletes the Spam Email

Once the SPAM email is delivered, the inbox owner spends approx. 30 seconds addressing the spam email and then deletes the SPAM email. That is the end of the SPAM email delivery process and no further action is taken.

[29] Taaffe, J. (2019) *SPAM Email Route through Clients Network* [Created Q1 2019].

Using SIEM to Address SPAM

With a fully operational and tuned SIEM solution, the SPAM email delivery process does not end at SPAM email deletion. Further automated actions, without user interaction and invisible to the user, are taken by the SIEM solution as follows [30]:


9. SIEM Receives SPAM Email Details
Security Information and Event Management System
IBM Blockchain Mainframe
Microsoft SQL Server
8. SIEM Polls Client Event Log
RedHat Web Application Server
10. SIEM Updates Checkpoint Firewall SPAM Filter
HPE/Aruba Router
Internal Juniper Switch
Cisco Firewall (Internal)
Juniper Switch
HPE/Aruba Switch
Check Point Firewall (Perimeter)
Juniper Border Switch
Cisco Border Router
Internet
7. User Deletes Spam Email from Inbox
Email Server
RedHat mongoDB Server
McAfee Web Gateway/Proxy
Internal Network
Perimeter Network
Border Network
SPAM
6. Spam Email Delivered to Inbox
5. Email Server Accepts/Drops Spam Email
4. Spam Email Traverses Perimeter Network
3. Checkpoint Firewall Drops/ Accepts Email
2. Spam Email Traverses Border Network
1. Spam Email Sent to @client.domain
SPAM Email Route

Process Flow

1-6. Same steps as previous example

7. The user reviews the email, determines its SPAM and deletes the Spam Email
8. SIEM System Polls/Queries the Client Event Log
9. Client Event Log reports SPAM email deleted by user and includes the SPAM Email Details
10. SIEM automatically updates the Checkpoint Firewall SPAM Filter with the SPAM Email Details

Result: All further SPAM emails with that signature sent to the client will never be delivered again.

This example demonstrates SIEM's automated Centralised Collection, Aggregation and Normalisation (CAN) of Event Data capability and demonstrates its Event Correlation and Orchestration ability.

[30] Taaffe, J. (2019) SIEM Auto Updating Checkpoint Firewall SPAM Filters [Created 5th April 2019].

Conclusion

This *Cyber Security Briefing: Countering Cyber Threats* report is to support a budget request. Below is a summary of the key point of this report.

Cyber Security Threats – Global (page 3)

Forbes Cyber Security Year on Year 2018-2019 Threat predictions[31] clearly confirms there is no sign of cyber-attacks declining, quite the opposite

+ **14%** Zero-day Attacks
+ **15%** Phishing Attacks
+ **151%** Malware Attacks
+ **226%** Ransomware Attacks
+ **430%** Encryption-based Attacks

Client Event Monitoring Controls (page 8)

4 Disconnected Isolated Alert Platforms

10 Separate Vendor/Device Alert Platforms

0 Single Central Events Database

0 Single Central Administrative 'Company-wide' Event Console

0% Internal Support Centre Event Correlation

0% Event Cross-Correlation between Support Centres

0% Informational, Error or Warning Event Monitoring

Security Monitoring Controls Proposal (page 11)

Deploy a Security Information and Event Management (SIEM) system into which all security, network, server and application events are routed, stored, analysed, correlated and actioned either manually or automatically.

Security Information and Event Management Benefits (page 12)

Primary Function: Detect, identify, alert and remediate security events.

+ Increase Efficiency
+ Visibility
+ Security Breach Prevention
+ Impact Reduction
+ Expenditure Reduction
+ Enhanced Reporting and Analysis

[31] Forbes (2018) *Real-Time Cyber Threat Intelligence Is More Critical Than Ever* https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/ [Accessed 26th April 2019].

SIEM Client Use Cases (page 14)

From my analysis, the client's high-level Use Case is for a SME SIEM Deployment. This will provide a streamlined SIEM, keeping costs low, while providing effective security oversight.

Regarding the specific SIEM functions required, our focus should be Threat, Compromise, Vulnerability Detection wit Compliance Reporting.

SIEM Vendor Selection

Combining the client's Security Monitoring Controls Solution Requirements (Page 10) and the client's SIEM specific Use Case (SME Deployment) with a focus on Threat, Compromise and Vulnerability Detection (Page 12) and Gartner's market analysis including Vendor Strengths and Cautions (page 15), the following 3 vendors were chosen:

Vendor	Solution Name	Solution URL
LogRhythm	NextGen SIEM Platform	https://logrhythm.com/solutions/security/siem/
McAfee	Enterprise Security Manager	https://www.mcafee.com/enterprise/en-us/products/enterprise-security-manager.html
Solarwinds	Log & Event Manager	https://www.solarwinds.com/log-event-manager-software

Table 7. Chosen Vendor, Solution Name and Solution URL [32]

[32] Taaffe, J. (2019) *Table 7. Chosen Vendor, Solution Name and Solution URL* [Created 4th April 2019].

References

1	Accenture	(2018)	2018 State of Cyber Resilience	https://www.accenture.com/_acnmedia/PDF-76/Accenture-2018-state-of-cyber-resilience.pdf	[Accessed 26th April 2019].
2	Help Net Security	(2018)	Cyber-attacks becoming No. 1 business risk	https://www.helpnetsecurity.com/2018/03/07/cyber-attacks-business-risk/	[Accessed 26th April 2019].
3	Forbes	(2018)	Real-Time Cyber Threat Intelligence Is More Critical Than Ever	https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/	[Accessed 26th April 2019].
4	CYFIRMA	(2018)	CYFIRMA’s Cyber Threat and Risk Prediction Report for 2019	https://www.cyfirma.com/insights/cyfirmas-cyber-threat-and-risk-prediction-report-for-2019/	[Accessed 26th April 2019].
5	United States Cyber Security Magazine	(2018)	Top 10 Cybersecurity Risks For 2019	https://www.uscybersecurity.net/risks-2019/	[Accessed 27th April 2019].
6	Week 8 – Security Fundamentals	(2019)	Security Threat Sources Slide 53	https://moodle.ncirl.ie/mod/resource/view.php?id=52586	[Accessed 27th April 2019].
7	Identity Theft Resource Center	(2018)	2017 Annual Data Breach Year-End Review	https://www.idtheftcenter.org/2017-data-breaches/	[Accessed 29th April 2019].
8	CSO Online	(2018)	You can’t protect what you can’t see	https://www.csoonline.com/article/3256211/you-cant-protect-what-you-cant-see.html	[Accessed 30th April 2019].
9	Phoenix NAP	(2018)	2019 Cybersecurity Trends: 31 Experts on Current Issues	https://phoenixnap.com/blog/cybersecurity-experts-threats-trends	[Accessed 30th April 2019].
10	Phoenix NAP	(2018)	2019 Cybersecurity Trends: 31 Experts on Current Issues	https://phoenixnap.com/blog/cybersecurity-experts-threats-trends	[Accessed 30th April 2019].
11	Wikipedia.org	(2019)	Event (computing)	https://en.wikipedia.org/wiki/Event_(computing)	[Accessed 31st April 2019].
12	Taaffe, J.	(2019)	Client Event Monitoring Landscape		[Created 31st April 2019].
13	Info-Tech Research	(2019)	Select and Implement a SIEM Solution	https://www.infotech.com/research/ss/select-and-implement-a-siem-solution	[Accessed 31st April 2019].
14	Computer Weekly	(2019)	Security information and event management (SIEM) systems streamline compliance	https://www.computerweekly.com/tip/Security-information-and-event-management-SIEM-systems-streamline-compliance	[Accessed 1st April 2019].
15	Tech Target	(2018)	SIEM benefits include efficient incident response, compliance	https://searchsecurity.techtarget.com/feature/Three-enterprise-benefits-of-SIEM-products	[Accessed 1st April 2019].
16	Log Rhythm	(2015)	Select and Implement a SIEM Solution (Slide 23)	https://logrhythm.com/pdfs/3rd-party-review/lr-info-tech-select-and-implement-a-siem-solution-2015-full-report-3rd-party-review.pdf	[Accessed 1st April 2019].
17	Anton Chuvakin, Gartner	(2018)	2018 Popular SIEM Starter Use Cases	https://blogs.gartner.com/anton-chuvakin/2018/07/20/2018-popular-siem-starter-use-cases/	[Accessed 1st April 2019].
18	Gartner	(2018)	Magic Quadrant for Security Information and Event Management (SIEM) ID G00348811	https://www.gartner.com/doc/3894573/magic-quadrant-security-information-event	[Accessed 2nd April 2019].
19	Info-Tech Research	(2019)	SIEM Solutions Comparison Tool	http://siemcomparison.com/	[Accessed 2nd April 2019].
20	Taaffe, J.	(2019)	Detailed analysis of Vendor to Feature to Client requirements analysis		[Created 3rd April 2019].
21	Taaffe, J.	(2019)	Table 3. Table 3. Key Security Controls Solution Considerations	https://www.infotech.com/research/ss/select-and-implement-a-siem-solution	[Accessed 3rd April 2019].
22	Info-Tech Research Group	(2019)	SIEM Solutions Comparison Tool	http://siemcomparison.com/	[Accessed 3rd April 2019].
23	Taaffe, J.	(2019)	Table 6. Vendor to Additional Considerations to Client Requirements Analysis		[Created 3rd April 2019].
24	LogRhythm	(2019)	LogRhythm Official Logo	https://logrhythm.com/about/branding-guidelines/	[Accessed 4th April 2019].
25	McAfee	(2019)	McAfee Official Logo	https://www.mcafee.com/enterprise/en-us/mcafee-brand.html	[Accessed 4th April 2019].
26	Solarwinds	(2019)	Solarwinds Official Logo	https://www.solarwinds.com/	[Accessed 4th April 2019].
27	Taaffe, J.	(2019)	Table 7. Chosen Vendor, Solution Name and Solution URL		[Created 4th April 2019].
28	Taaffe, J.	(2019)	Cyber Security Briefing: The Threat of SPAM		[Created Q1 2019].
29	Taaffe, J.	(2019)	SPAM Email Route through Clients Network		[Created Q1 2019].
30	Taaffe, J.	(2019)	SIEM Auto Updating Checkpoint Firewall SPAM Filters		[Created 5th April 2019].
31	Forbes	(2018)	Real-Time Cyber Threat Intelligence Is More Critical Than Ever	https://www.forbes.com/sites/forbestechcouncil/2018/05/22/real-time-cyber-threat-intelligence-is-more-critical-than-ever/	[Accessed 26th April 2019].