12-2017

Analyzing, Implementing and Monitoring Critical Security Controls: A Case Implemented in J & B Group

Hareesh Reddy Eemani
St. Cloud State University, heamani@stcloudstate.edu

Analyzing, Implementing and Monitoring Critical Security Controls:

A Case Implemented in J & B Group

by

Hareesh Reddy Eemani

A Starred Paper

Submitted to the Graduate Faculty of

St. Cloud State University

in Partial Fulfillment of the Requirements

for the Degree

Master of Science

in Information Assurance

December, 2017

Starred Paper Committee:
Susantha Herath, Chairperson
Jim Q. Chen
Ezzat Kirmani

Abstract

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function in organizations. Software companies and application vendors are unable to keep up with rapidly growing attacks and changing threat patters. The need for information security should be apparent and require substantial research, knowledge, and ability to design and implement an effective security program. Also, requires a great investment of time and resources. Many small and medium businesses may understand the importance of risk, but lack in grasping the severity of the problem and resources to identify it. A well analyzed and implemented information security program can reduce the damage caused by an attack by reducing the mean time to detect, contain and restore.

The purpose of this paper is to present a systematic approach to conduct analysis by gathering data, implementing and monitoring the critical security controls. An effective information security process ensuring strong security posture to defend against cyber-attacks with minimum resources and open source software is the key to this research as it reduces the cost to implement and maintain the security operations center.

The literature focuses on increasing cyber-attacks on organizations and how to prevent these attacks using technical countermeasures and non-technological side of information security. This research refers to CIS critical security controls (CSC) to classify data, systems and analyze risk using Qualitative and Quantitative data. Research data is collected from J & B Group Information technology team. Importance of security program is not only adopting best security processes and tools but also must be reviewed, updated and maintained on a regular basis. Continuous monitoring of security controls is driven with open source SIEM tool with minimum license and by establishing custom rules for generating offenses and alerts.

Acknowledgements

I would like to express my sincere gratitude to my supervisors as well as committee members Dr. Susantha Herath, Dr. Jim Q. Chen, and Dr. Ezzat Kirmani for providing their invaluable guidance, comments and suggestions throughout the course of the paper.

Table of Contents

Chapter Page

Chapter Page

Appendices

List of Tables

Table Page

List of Figures

Figure Page

Chapter I: Introduction

Introduction

The increasing sophistication of information security threats and the ever-growing body of regulation has made information security a critical function in organizations. Information security means protecting or securing information from an unauthorized access, use, disclosure, interference, alteration, or damage. To ensure effectiveness in the implementation of security may require more resources, controls, and maintenance. This chapter introduces the problem statement, significance of problem, objectives, and limitations of the research and definition of terms.

Problem Statement

Need for information security with the increase in latest cyber-attacks, security breaches and government regulations urged many organizations to adopt and implement security strategies on their existing information technology infrastructure. By fulfilling a growing need to provide open access to information resources, companies have reached a key juncture in cyber security. The IT Systems are increasingly sophisticated with more traffic and types of activity affecting their networks than ever before. Some of the many concerns for any organizations include theft of company information via external hackers and dissatisfied employees, website defacement, phishing attacks and types of malicious software block access to a computer so hackers can hold data for ransom and data loss due to natural events and incidents.

One of the key challenges organizations are facing today is a timely collection, collating and analysis of security events generated from a wide source of network systems and applications deployed in their environment. But, the organizations lack in finding the appropriate process for implementing and gaining visibility to security logs in one location for situational awareness. Subscribing to third-party tools and services to maintain security will have a significant increase in cost as well.

This paper provides a process to analyze, choose critical security controls to implement with minimum or no cost depending upon resource allocations and open source software and gain visibility over their environment, strengthens security and be self-sufficient to defend against dynamic attack patterns. While this research is not based on any known incident, it is certainly a plausible situation, and need for information security.

Nature and Significance of Problem

According to the Cisco's (2016) research, 90,000 victims are targeted to attack per day and 147 redirections servers per month. The gross income for ransomware per campaign is $34 million considering $300 average ransomware per record or file. New malware variants are added each year. From the research conducted by Symantec (2016) for the year 2015, 36% increase in the new malware for the year compared to 2014 and found a total of 431 million malware variants. Increasing cyber-attack over small, mid-sized and large organizations making them adapt to critical security controls which defends cyber-attacks. Many organizations lack resources and appropriate tools to monitor or prevent any security breaches. This paper helps the organizations as a starting step to adapt and implement appropriate security controls. The research is intended not only to support the premise that an information security program is necessary for any computing environment but also to offer practical advice on the implementation and monitoring of critical controls.

Objectives of the Research

This study will cover assessment of risk using CIS critical controls, the process of implementing and monitoring critical controls. The following are the sub-objectives the study has:

- Assessment of existing information security controls of an organization using CIS 20 critical controls and ISO/IEC 15504 process model.
- Using the results from above analyze and consider critical controls based on risk level, Maturity level to handle and capabilities of SIEM tool for implementation.
- Implementing the selected critical security controls using open source SIEM tool.
- Establish rules for monitoring the selected controls for creating offenses and alerts which is a reactive approach towards compromise.
- For the above, an automation plan is drafted which can be considered as scope for improvements in future.

It is not the idea or intent of this paper to promote any product or technology, only to offer suggestions and guidance who are seeking to maintain security and privacy as related to computer use.

The results of the assessment are compared with the standard implementation of CIS 20 critical controls. Analyzing quantitative and qualitative data will yield to consider the high risk and critical controls that need to be implemented and monitored. The critical controls only present a subset of technical controls, but the data breach can also happen due to non-technical controls that are in day-to-day operations. The assessment of critical controls and improvement plans to be considered a way of enhancing the security posture through implementation and monitoring of technical controls.

Limitations of the Research

The objective of this paper is to assist in implementing and monitoring security controls with minimum or no cost with open source software. Not all open source software or tools are fully functional as intended and few products require purchased licenses after a certain time to continue the services. This paper, however, uses the trial version of the software which may not have access to entire functionality and licenses. Due to the restrictions on EPS licenses over the open source SIEM software only two critical controls are implemented. The objective of the SIEM test evaluation was to inform any decision to take the project further into the next phase with a wider scope of data source collection and move from test to production. The research documented in this paper was limited to the test build and evaluation only.

Definition of Terms

To provide an understanding of the terms, phrases, and properties used in information security and to adhere to industry standards terminology below are the following terms and definitions taken from SANS Institute website (SANS Institute, 2017)

Availability: The need to ensure that the business purpose of the system can be met and that it is accessible to those who need to use it.

Authentication: The process of confirming the correctness of the claimed identity.

Authenticity: The validity and conformance of the original information.

Computer network: A collection of host computers together with the sub-network or Inter-network through which they can exchange data.

Confidentiality: The need to ensure that information is disclosed only to those who are authorized to view it.

Cost-benefit analysis: A comparison of the cost of implementing countermeasures with the value of the reduced risk.

Cryptography: The process of garbling a message in such a way that anyone who intercepts the message cannot understand it.

Data custodian: The entity currently using or manipulating the data, and therefore, temporarily taking responsibility for the data.

Data owner: The entity having responsibility and authority for the data.

Defense-in-depth: The approach of using multiple layers of security to guard against failure of a single security component.

Denial of service: The prevention of authorized access to a system resource or the delaying of system operations and functions.

Dictionary attack: An attack that tries all the phrases or words in a dictionary, trying to crack a password or key. A dictionary attack uses a predefined list of words compared to a brute force attack that tries all possible combinations.

Digital signature: A hash of a message that uniquely identifies the sender of the message and proves the message has not changed since transmission.

Disaster recovery plan (DRP): The process of recovery of IT systems in the event of a disruption or disaster.

Domain: (1) A sphere of knowledge, or a collection of facts about some program entities or (2) Network points or addresses, identified by a name. On the Internet, a domain consists of a set of network addresses. In the Internet's domain name system, a domain is a name with which name server records are associated that describe subdomain hosts. In Windows NT and Windows 2000, a domain is a collection of computers on a network that shares a common user database and security policy. A domain is administered as a unit with common rules and procedures by the domain administrator. The user needs only log in to the domain to gain access to the resources, which may be located on many different servers in the network.

Domain name: A domain name locates an organization or other entity on the Internet.

For example, the domain name "www.sans.org" locates an Internet address for "sans.org" at Internet point 199.0.0.2 and a host server named "www". The "org" part of the domain name reflects the purpose of the organization or entity (in this example, "organization") and is called the top-level domain name. The "sans" part of the domain name defines the organization or entity and together with the top-level is called the second-level domain name.

Domain name system (DNS): The way that Internet domain names are located and translated into Internet Protocol addresses. A domain name is a meaningful and easy to- remember "handle" for an Internet address.

Due diligence: The requirement that organizations must develop and deploy a protection plan to prevent fraud, abuse, and additional deploy a means to detect them if they occur.

Encryption: The Cryptographic transformation of data (called "plaintext") into a form (called "ciphertext") that conceals the data's original meaning to prevent it from being known or used.

Firewall: A network security device that ensures that all communications attempting to cross it meet an organization's security policy. Firewalls track and control communications, deciding whether to allow, reject or encrypt communications.

Hardening: The process of identifying and fixing vulnerabilities on a computer system.

Hijack attack: A form of active wiretapping in which the attacker seizes control of a previously established communication association.

Honeypot: Programs that simulate one or more network services that you designate on your computer's ports. A honeypot can be used to log access attempts to those ports including the attacker's keystrokes. This could give you advanced warning of a more concerted attack.

Incident: An adverse network event in an information system or network, or the threat of the occurrence of such an event.

Incident handling: An action plan for dealing with intrusions, cyber-theft, denial of service, fire, floods, and other security-related events. It is comprised of a six-step process: Preparation, Identification, Containment, Eradication, Recovery, and Lessons Learned.

Integrity: The need to ensure that information has not been changed accidentally or deliberately and that it is accurate and complete.

Internet: Multiple separate networks connected all together.

Intranet: A computer network, usually based on Internet technology, that an organization uses for its own internal purposes, and that is closed to outsiders.

Intrusion detection system (IDS): A security management system for computers and networks. An IDS gathers and analyzes information from various areas within a computer or a network to identify possible security breaches, which include both intrusions (attacks from outside the organization) and misuse (attacks from within the organization).

Least privilege: The principle of allowing users or applications the least amount of permissions necessary to perform their intended function.

NIST: The National Institute of Standards and Technology, a unit of the US Commerce Department. Formerly known as the National Bureau of Standards, NIST promotes and maintains measurement standards. It also has active programs for encouraging and assisting industry and science to develop and use these standards.

Network address translation (NAT): The translation of an Internet Protocol address used within one network to a different IP address known within another network. One network is designated the inside network and the other is the outside.

Penetration: Gaining unauthorized logical access to sensitive data by circumventing a system's protections.

Port: The endpoint of a communication stream, identified by a number. Only one process per machine can listen on the same port number.

Proxy: A server that acts as an intermediary between a workstation user and the Internet so that the enterprise can ensure security, administrative control, and caching service.

Registry: The Registry in Windows® operating systems in the central set of settings and information required to run the Windows computer.

Risk assessment: The process by which risks are identified and the impact of those risks determined.

Security policy: A set of rules and practices that specifies or regulates how and why a system or organization provides security services to protect sensitive and critical system resources.

SYN flood: A denial of service attack that sends a host more TCP SYN packets (request to synchronize sequence numbers, used when opening a connection) than the protocol implementation can handle.

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action, or event that could breach security and cause harm.

Trojan (a.k.a. Trojan Horse): A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Virtual private network (VPN): A restricted-use, logical (i.e., artificial or simulated) computer network that is constructed from the system resources of a relatively public, physical (i.e., real) network (such as the Internet), often by using encryption (located at hosts or gateways), and often by tunneling links of the virtual network across the real network.

Virus: A hidden, self-replicating section of computer software, usually malicious logic, that propagates by infecting, i.e., inserting a copy of itself into and becoming part of – another program.

Vulnerability: A flaw or weakness in a system’s design, implementation, or operation and management that could be exploited to violate the system’s security policy.

Worm: A computer program that can run independently, can propagate a complete working version of itself onto other hosts on a network, and may consume computer resources destructively.

Summary

This section discussed the importance of information security and provided problem statement with objectives and sub-objectives. Nature and significance of the problem are discussed using some references on recent cyber-attacks and threat analysis reports. There are no assumptions or hypothesis in this paper. Definitions of terms are provided in this chapter for user references. The next chapter will be literature review related to the problem and methodology.

Chapter II: Background and Literature Review

Introduction

This chapter deals with background, literature related to the problem, analyzing risk using CIS critical controls and ISO/ISE 15504 process. The strategy is a concept that has evolved from a military setting where it is best described as deciding what means to use, how to use it and how to apply it (Howard, 1979). This literature review determines the process of analysis, implementing and monitoring of critical security controls. Next step illustrates background and literature related to the problem, literature related in analyzing risk, a literature review on SIEMs and literature related to methodology.

Background Related to the Problem

Research has shown the tendency of companies not paying close attention to the importance of security as in the case of the Target security breach in 2014 (Ponemon Institute LLC, 2015). The issues in many cases were a lack of attention to detail and proper configuration of security controls (Vijayan, 2014). Cybersecurity awareness has been increasing from past years and tendencies of organizations to move towards visibility of what is happening in an around their cyber environment and develop monitoring techniques.

Literature Related to the Problem

Threats of all kinds continue to evolve, and today’s organizations find that the threat landscape changes and presents new challenges every day. Many organizations have learned over decades to defend themselves and respond better, moving from very basic level measures and immediate responses to sophisticated, robust and formal process.

Information is an asset, and having specific, relevant and correct information can make a massive difference to an organization’s efficiency. With the huge number of available technologies, it is possible for information to be collected, shared, sold, exchanged and distributed without notice to the owner (Varney, 1996). It is most important to ensure information security so that it becomes a natural phase in the daily activities of an organization. Organizations must define the threats and vulnerabilities to information resources to ensure the confidentiality, integrity, and availability thereof (Gollmann, 1999; Pfleeger, 1997; Sebastiaan, Solms, & Eloff, 2003).

Information security not only covers the information itself, but also the entire infrastructure that facilitates its use. It covers human factors; hardware, software related threats, vulnerabilities, physical security and each has its own characteristics. Given the number of organizational security breaches increasing daily, and the more accessible the information, the greater the hazards, it is inevitable that security will need to be tightened (Brown & Duguid, 2002).

Information security has been regularly considered to be a technological problem with a technological solution. That is simply untrue because information security is about managing risk (Whitman & Mattord, 2005) and managing risk is about discovering and measuring threats to information assets (Lampson, 2004) and taking actions to respond to those threats.

Increasing number of employees, systems and applications information becomes more difficult and consequently increases the vulnerabilities. Organizations make use of information security policies to determine the secure use of hardware and software. An information security policy is a combination of principles, regulations, methodologies, techniques, and tools

(Tryfonas, Kiountouzis, & Poulymenakou, 2001) written or established to protect the organization from cyber threats. These policies also help organizations to identify its information assets and define the corporate attitude to these information assets (Canavan, 2003).

After an increase of 36% between 2015 and 2016, the rate of ransomware infections seen has continued to increase. In the first and second quarters of 2017, there were 319,000 ransomware infections identified. The spike in infections was a large part due to the WannaCry and Petya outbreaks, which accounted for 28% of infections in May and 21 percent of infections in June (Symantec, 2017). The version of WannaCry, once installed on a computer, attempts to use the Eternal Blue exploit to spread to other computers on the local network. In addition, it would also attempt to spread itself across the internet by scanning random IP addresses to find other vulnerable computers This propagation mechanism explains how WannaCry heavily affected some organizations and how it managed to jump from one organization to another. Likewise, Petya, once infected, will began the encryption process. It first modifies the master boot record allowing it to hijack the normal loading process of the infected computer during the next system reboot.

Organizations need to be aware of the threat posed by this new breed of ransomware. While worm-type ransomware such as WannaCry and Petya has dominated the headlines this year, it is far from the only ransomware threat affecting businesses. The most prevalent for of ransomware continues to be the traditional crypto ransomware delivered through massive spam campaigns. Since most businesses receive a high volume of similar albeit legitimate emails from customers and suppliers, malicious emails could be inadvertently opened if they aren’t blocked by email security software.

Another threat which specifically affects organizations is targeted ransomware attacks, where the attackers select their target in advance and attempt to cause the maximum disruption possible in the hope of a big ransom payout. One of the key messages organizations should take from the wave of recent attacks is to avoid complacency. Simply patching against vulnerability doesn’t inoculate you against the threat of ransomware, since attackers may play the long game and attempt to encrypt all backups as well. Organizations need to adopt a multi-layered approach to security to best ensure that any point of failure is mitigated by other defensive practices. This should include the deployment of regularly updated firewalls as well as gateway anti-virus and an IDS/IPS system.

Most of the organizations obtain a false sense of security by investing in the latest tools. Although tools and technologies are an integral part of an organization’s information security plans, it is argued that they alone are not sufficient to address information security problems (Herath & Rao, 2009). “The CIS 20 Critical controls” present a prioritized list of technical controls that organizations can consider implementing and auditing to assess the implementation of information security measures.

Literature Related to Analyzing Risk

Identifying, quantifying, and mitigating risks to data and computers is the core for a risk management program. There are seven basic steps proposed by (Bragg, 2003):

- Identify the assets
- Assign value to the assets

- Identify the risks and threats
- Estimate the potential loss
- Estimate the possible frequency of the threat occurring
- Calculate the cost of the risk
- Recommend countermeasures or other remedial activities.

Asset identification is not only the hardware of software but also the amount of data stored and processed on that computer. The value of data routinely transcends the value of computers and infrastructure by many orders of magnitude (Berger, 2003).

Every asset has a value. The next step in performing a risk analysis is to determine what that value is for each asset. There are generally two approaches to asset valuation quantitative method and the qualitative method. The quantitative method functions by assigning a financial value to each asset, which is then compared to the cost and effectiveness of the counter-measure (Bragg, 2003). The qualitative system ranks threats and security measures relative to the system being analyzed, often using a scoring, or classification system (Bragg, 2003). For the purposes of descriptions and examples in this study, the qualitative method will be assumed. Having identified and valued the assets to be protected, threats to those assets must be examined. Any process or event that has the potential to harm an asset is considered a threat. Examples of threats include hackers, tornados, poor procedures, human error, and terrorists (Visintine, 2003).

Literature Related to SIEM

Security Information and Event Management (SIEM) solutions are systems capable of analyzing security event in real time and acts as a log storage, historical reporting, and behavioral analysis tool. They also act as correlation tool for vulnerability and threat data to offer insight into risk prediction and reporting for compliance purpose such as NERC CIP, HIPPA regulations.

SIEM can provide the security team a landscape view of their exposure to security threats through the consolidation of log data from different log sources, such as Anti-virus, Firewalls, proxy servers etc. Correlation and intelligence from the log data, alerting when certain event conditions are reached and one single pane of view to the dashboard that gives visibility to events that might have required management of multiple dashboards and reporting tools Mercer, 2013).

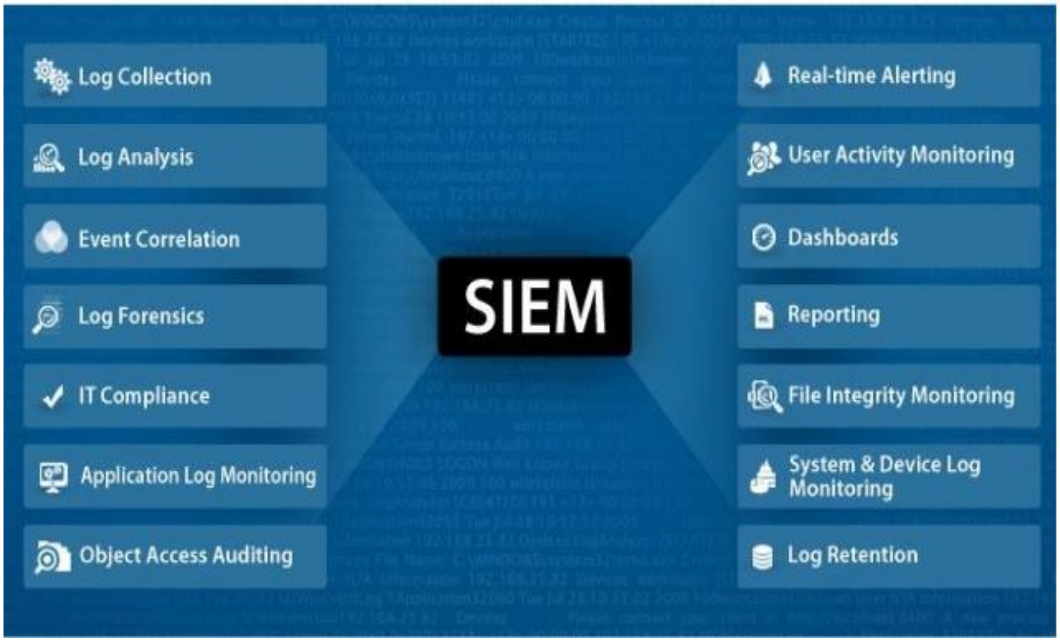


Figure 1. Features of SIEM (Security Information Event Management Tool).

Every security information event management (SIEM) system gives defenders a set of tools to combat malicious activity on a network. SIEM collect logs from standard security sources, enrich logs with supplemental data, correlate via finding the proverbial needles in the log haystacks, investigate logs follow up and fix, standard operating procedures, service level agreements, build white lists etc.

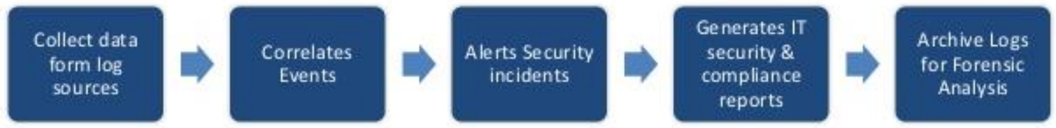

Collect data form log sources
Correlates Events
Alerts Security incidents
Generates IT security & compliance reports
Archive Logs for Forensic Analysis

Figure 2. Work Flow of SIEM (Security Information Event Management).

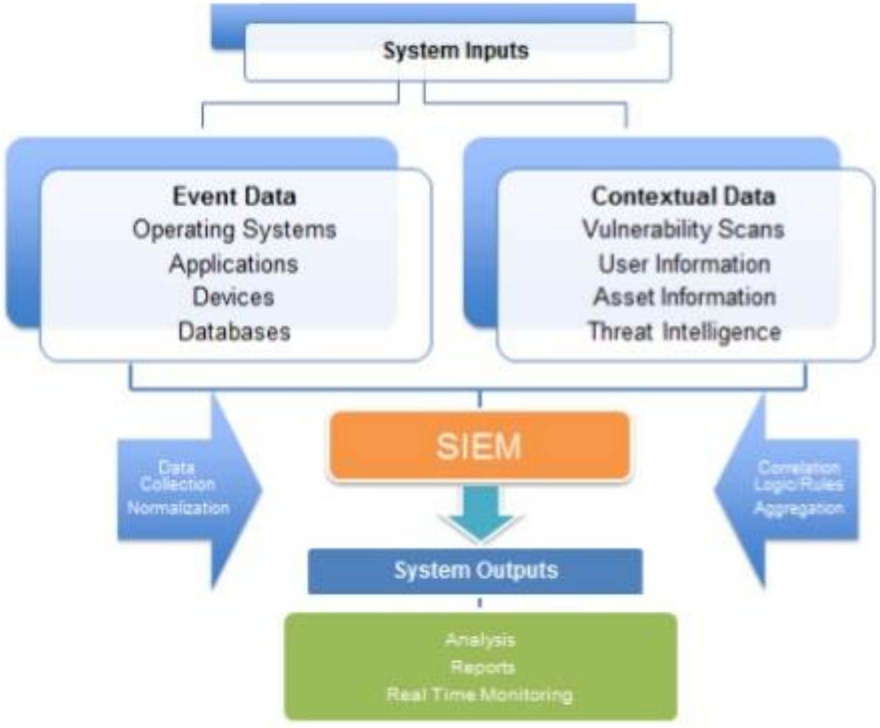


Figure 3. SIEM (Security Information Event Management) Architecture.

Literature Related to the Methodology

Information security strategies have been defined and classified in many ways. Studies have identified various strategies such as Prevention (Lampson, 2004; McDermott 2000), Detection (Henauer 2003; Stolfo 2004) and Response (Beauregard 2001; Cahill 2003).

Prevention aims to protect information assets prior to an attack by prohibiting unauthorized access, modification, destruction, or disclosure (Liu, Sullivan, & Ormaner, 2001). Detection is an operational-level strategy aimed at identifying specific security behavior (Hamill et al., 2005). Response takes appropriate corrective actions against identified attacks. The response to an attack can be divided into two phases. The reaction phase where the appropriate actions are taken against the attack and secondly the recovery phase, the situation is restored to its original state (Armstrong, Carter, Frazier, & Frazier, 2004; Hamill, Deckro, & Kloeber, 2005; Tirenin & Faatz 1999).

Considering prevention, detection, and response as key to adopting a measurement framework laid the path to take up CIS 20 critical controls with ISO/IEC 15504 specific rating criteria for evaluation. The CIS is a 501c3 nonprofit organization whose mission is to identify, develop, validate, promote and sustain best practices in cybersecurity. The controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions (International Organization for Standardization, 2015).

The advantages of CIS top 20 Security controls are:

1. Implementation of controls can reduce the potential impact of known high-risk attacks as well as attacks expected in future. This ensures to have a strong security fence around the company's IT environment.
2. The CIS controls to address the most important areas of concern and is comprehensive.

3. These controls are written in such a way that is easy to understand and implement. They are also approachable and can make common security requirements.
4. The controls were generated by experts in both federal government and private industry.
5. Leverage cyber offense to inform cyber defense, focusing on high payoff areas.
6. The security investments are focused to counter the highest risk threats and use of automation to enforce these controls could negate human errors.

Continuous monitoring programs facilitate ongoing awareness of threats, vulnerabilities, and information security to support organizational risk management decisions. The terms continuous and ongoing imply that organizations assess/analyze security controls and information security-related risks at a frequency sufficient to support organizational risk-based decisions. The results of continuous monitoring programs generate appropriate risk response actions by organizations. Continuous monitoring programs also allow organizations to maintain the security authorizations of information systems and common controls over time in highly dynamic environments of operation with changing mission/business needs, threats, vulnerabilities, and technologies. Having access to security-related information on a continuing basis through reports/dashboards gives organizational officials the capability to make more effective and timely risk management decisions, including ongoing security authorization decisions. Automation supports more frequent updates to security authorization packages, hardware/software/firmware inventories, and other system information. Effectiveness is further enhanced when continuous monitoring outputs are formatted to provide information that is specific, measurable, actionable, relevant, and timely. Continuous monitoring activities are scaled in accordance with the security categories of information systems (National Institute of Standards and Technology, 2013).

Summary

Once a security control has been implemented and monitored, it must be kept up to date with the latest Intel. As any changes to the systems are introduced, the controls must be re-evaluated to ensure that are appropriate and performing as required. This chapter offered the background, literature, and significance of implementing and continuous monitoring. The actual methodology adopted for this research is discussed in next chapter along with tools and techniques.

Chapter III: Methodology

Introduction

The effective information security program is made up of Identification, Evaluation, Remediation, Maintenance, and education areas. The primary step is to assess the existing capability level or organizational maturity level (Wysocki, 2004). The methodology used for this assessment can be repeatable to enhance the security measures. Data is gathered from J & B Group IT Department using CIS critical controls template. ISO 15504 model is adapted for assessment of collected data. Risk levels are analyzed from gathered data and critical controls are taken from the results of the analysis for implementing. Open source SIEM (Security Information and Event Management) tool is used in the implementation. Monitoring rules are established based on each critical control criteria for alerting and generating offenses.

Design of Study

A combination of research methods used in this paper while part of the research is based on the previous works of others (applied research) and some experimentation, experience and taught are used to verify or corroborate the findings (pure research).

Books, newsletters, and other media, printed and electronic were chosen and these sources were used throughout the study in all areas:

- Government websites including Federal Bureau of Investigation and the Department of Homeland Security.
- SANS Reading room was used as a source of material written by information security professionals on a wide range of areas.

The SANS Institute (n.d.) “. . . develops, maintains and makes available at no cost, the largest collection of research documents about various aspects of information security, and it operates the Internet’s early warning system–Internet Storm Center” (¶ 2). The Top 20 security controls are also promoted by SANS Institute.

The SANS (Sysadmin, Audit, Network, Security) Institute was established in 1989 as a cooperative research and education organization. Its programs now reach more than 165,000 security professionals, auditors, system administrators, network administrators, chief information security officers, and CIOs who share the lessons they are learning and jointly find solutions to the challenges they face (SANS Institute, n.d., Trend Micro, 2016).

Tools and Techniques

Security and good IT management go together, a well-managed network is more difficult to attack than a poorly managed one. To understand well about managing cybersecurity, here are some of the questions which needs to be answered.

- Do we know what is connected to networks and systems?
- Do we know what software is running on networks and computers?
- Do we manage who has access to sensitive information or who has elevated privileges?

To help to prioritize the efforts, CIS 20 controls recommends using a phased approach.

- Phase 1: Involves knowing what’s on the network and understanding cybersecurity baseline.
- Phase 2: Focuses on protecting security baseline through prevention and situational awareness.

- Phase 3: Helps organizations to prepare in advance for disruptive events.

There are 20 security controls constitute to 150 sub-controls. All these 150 sub-controls depending on the implementation status can be assessed at three different levels. The table below indicates the rating and suggested numeric score for each rating (Riffat, 2015).

Table 1

Sub-Control Rating Scheme

Rating Description	Numeric Score
	1
Partially Addressed	0.5
Not Addressed	0

Every sub-control is rated with Implementation Level Score, Maturity of IT to implement and handle this control and risk posed by not implementing this control in the organization. As per ISO/IEC 15504, there are six maturity levels that can be used to depict the status of each critical control. To make it simplified, these six maturity levels are further reclassified into three maturity levels as shown in Table 2. “1-Low maturity” indicates that controls are not implemented. “2-Medium Maturity” shows that the controls are partially implemented and “3-High Maturity” indicates that the controls are fully implemented and achieve their purpose.

Table 2

Maturity and Risk Schema

Maturity of IT to Implement this Control	Risk to the Organization
1-Low Maturity	1-Low Risk
2-Medium Maturity	2-Medium Risk
3-High Maturity	3-High Risk

To evaluate the maturity of each critical control the following formula is used to calculate the score. The score interpretation of score is provided in Table 3.

Formula: (Sum of Implementation Level Score of sub controls in each control/ Total number of sub-controls in each control) * 3.

Table 3

Interpretation of Score

Maturity Level	Numeric Score
Low	Between 0.00-0.99
Medium	Between 1.00-1.99
High	Between 2.00-3.00

The critical controls which are to be implemented are selected based on the Risk, Maturity to implement the control and the open source SIEM tool capabilities. Shortlisting the high-risk controls with the high maturity to implement and at the same time the open source SIEM tool carrying the required functionality is the evaluation criteria used to select the important critical controls out of the assessed 20 security controls.

CIS 20 security controls along with ISO/ISE 15504 framework, SIEM (Security Information and Event Management tool) IBM QRadar community version with 100 EPS licenses used for this research. Appendix C is used to identify the best SIEM tool QRadar by its capabilities and licensing.

ISO/IEC 15504 is the reference model for the maturity models consisting of capability levels against which data can be placed that were obtained during the assessment. This helps to give an overall determination of organization’s capabilities for implementing the critical controls. This model is considered as measurement framework.

ISO/IEC 15504 framework is little sophisticated and complex for evaluation and implementation. Changes have been made to this framework to make the evaluation simple and ease of understanding. Out of the 20 critical controls, only 17 are assessed based on business requirements.

Data Collection and Analysis

The primary method for research was through the web for identifying the latest security controls, open source software, and tools for deployment and monitoring. Secondarily, a structured Questionnaire/template is prepared with the identified security controls and three basic questions for each sub-control associated with the control. Thirdly, the collected data is analyzed to select the critical security control for implementation. Fourthly, open source software is selected and deployed in the environment. Lastly, the author's work experience in information security was used to develop rules with logic built in to correlate the data with the Intel of indicators of compromise, failed logins etc. Refer TO Appendix A for the template used for this research.

Critical Security Controls

Inventory of authorized and unauthorized devices. Actively manage (inventory, track, and correct) all hardware devices on the network so that only authorized devices are given access, and unauthorized and unmanaged devices are found and prevented from gaining access.

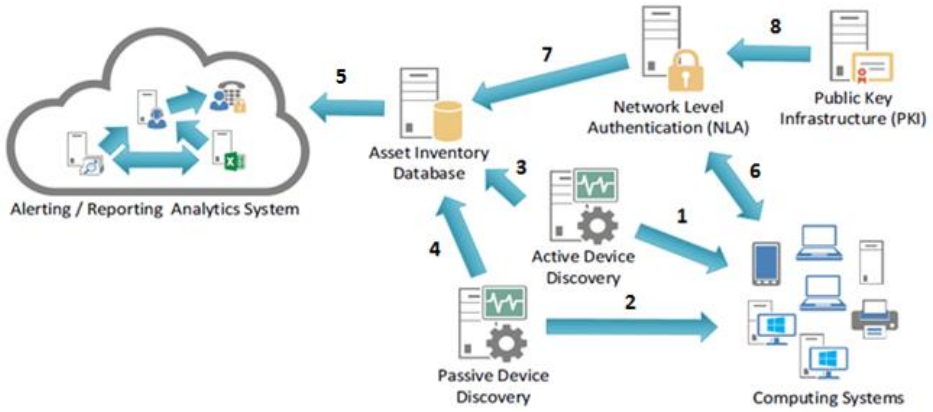

Alerting / Reporting Analytics System
5
Asset Inventory Database
7
Network Level Authentication (NLA)
8
Public Key Infrastructure (PKI)
3
4
Active Device Discovery
1
6
2
Passive Device Discovery
Computing Systems

Figure 4. System Entity Relationship Diagram of CSC.

- Step 1: Active device scanner scans network systems.
- Step 2: Passive device scanner captures system information.
- Steps 3 and 4: Active and passive devices report to the inventory database.
- Step 5: Inventory database initiates alert system and within this alert system notifies security defenders and security defenders monitor and update inventory database.
- Steps 6 and 7: Network-level authentication monitors, checks and provides updates on network traffic to asset inventory database.
- Steps 8: Utilize client certificates to validate and authenticate systems prior to connecting to the private network.

a.1. Deploy an automated asset inventory discovery tool and use it to build a preliminary inventory of systems connected to an organization’s public and private network(s). Both active tools that scan through IPv4 or IPv6 network address ranges and passive tools that identify hosts based on analyzing their traffic should be employed. Quick win*

The requirement is a one-time thing. It is to establish some baseline of asset inventory for the organization. This requirement underscores the fact that, without an accurate and precise understanding of assets under control, the rest of what your information security management system could be considered suspect. More than one discovery method should be used to maximize effectiveness.

Any tool(s) that are employed to detect devices on the network should include both active and passive techniques and have an ability to scan wired and wireless networks and able to monitor any cloud-based infrastructure or services.

While considering any tool and automation might include Asset life cycle management, Network scanning, Patch management, Endpoint monitoring, Vulnerability management (Malware, spyware) and configuration management integrations. It is important that these aspects to be considered when evaluating a tool as it could be a single module in bigger solution or must integrate with other solutions that are in use in the company.

The best way is to continuously monitor what devices are authorized and remove the devices from the network which are unauthorized.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No, Tool owned by J&B to complete this task.	Required	We have WUG, SCCM that may be able to address this issue. We may need external support to complete this.

Risk Level a.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

a.2 If the organization is dynamically assigning addresses using DHCP, then deploy dynamic host configuration protocol (DHCP) server logging, and use this information to improve the asset inventory and help detect unknown systems. Quick win*

DHCP services, it is a great way to passively detect new IP hosts in your enterprise and can be configured to generate logs which can be an easy source of discovery information. Automation of DHCP is recommended and backup of DHCP database and configuration.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes, this is enabled	Manual process today.		Yes, it could	Could we re-deploy a "soon-to-be-retired" server to act as a logging server? EMOPS, TW, VMXX?

Risk Level a.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

a.3 Ensure that all equipment acquisitions automatically update the inventory system as new, approved devices are connected to the network. Quick win*

Inventory system update is necessary whenever new equipment is added to the network. Automate the change control process. There is no baseline or standard for this section, enterprise would come up with a solution that is unique to their needs. If we have a data model representing assets would be helpful.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
We have a change control process for when new equipment is added to the network. This is not an automated process.	SCCM will detect all new servers and PCs	WUG can be configured to automatically scan network devices	Yes	WUG/SCCM

Risk Level a.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

a.4 Maintain an asset inventory of all systems connected to the network and the network devices themselves, recording at least the network addresses, machine name(s), purpose of each system, an asset owner responsible for each device, and the department associated with each device. The inventory should include every system that has an Internet protocol (IP) address on the network, including but not limited to desktops, laptops, servers, network equipment (routers, switches, firewalls, etc.), printers, storage area networks, Voice Over---IP telephones, multi---homed addresses, virtual addresses, etc. The asset inventory created must also include data on whether the device is a portable and/or personal device. Devices such as mobile phones, tablets, laptops, and other portable electronic devices that store or process data must be identified, regardless of whether they are attached to the organization's network. Visibility/attribution*

WUG and SCCM maintain IP address and machine names. Purpose, asset owner responsible for each device and the department associated with it. Asset identification model proposed by NIST would be the best start.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes - partially	WUG and SCCM maintain IP and device name. Owner and purpose is done manually.		No	We need to pay special attention to devices used by vendors for equipment access i.e. production stuff at Pipestone (eWon), printer, Neilson,

Risk Level a.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

a.5 Deploy network level authentication via 802.1x to limit and control which devices can be connected to the network. The 802.1x must be tied into the inventory data to determine authorized versus unauthorized systems. Configuration/hygiene*

The technology architecture published by TCG (Trusted computing group and adopted by NEA working group of the IETF) may suit for this requirement. The Asset inventory system needs to be integrated with the port-based NAC controls.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		We would need to purchase a NAC tool to implement	Yes	This was strongly recommended for network devices that do not authenticate through AD. In addition, a logging server should be used to maintain a history of device access.

Risk Level a.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

a.6 Use client certificates to validate and authenticate systems prior to connecting to the private network. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes, for certain applications	Public and private certs. For Exchange, Skype, and M3.	Desktop and User accounts do not have certificates	Yes	J&B IT doesn't understand how to further investigate this one.

Risk Level a.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	1

Overall CSC a Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
Low Maturity	Medium Risk

Overall Implementation level CSC a

Total Numeric score = **2**

Number of sub controls = **7**

Percentage implemented **= 28%**

Inventory of authorized and unauthorized software. Actively manage (inventory, track, and correct) all software on the network so that only authorized software is installed and can execute, and that unauthorized and unmanaged software is found and prevented from installation or execution.

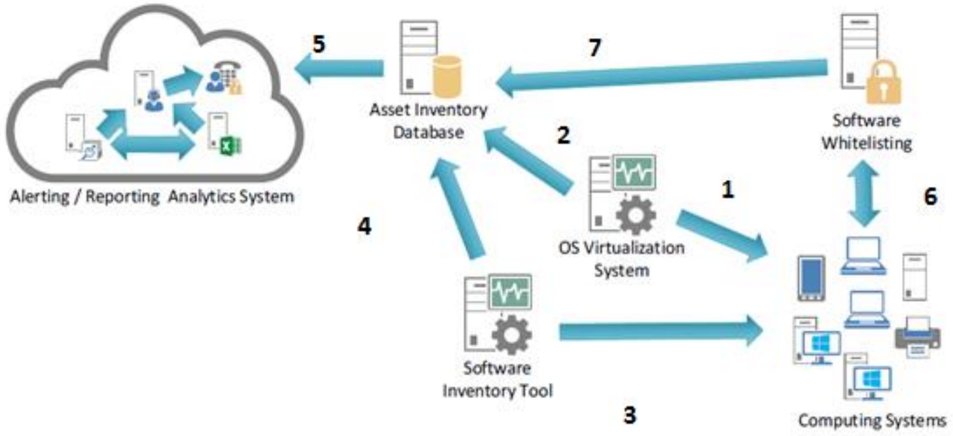


Figure 5. System Entity Relationship Diagram of CSC b.

- Steps 1 and 2: Used to isolate and run applications but not installed within a networked environment.
- Steps 3 and 4: Software inventory tool track the OS and applications running on the computing systems and integrated to hardware inventory database.
- Step 5: Inventory database compares to inventory baseline and initiates alerting system, alert system notifies security defenders and security defenders monitor, secure and update the inventory database.
- Steps 6 and 7: Software whitelisting tool monitors all systems on the network, checks and makes updated to the inventory database.

Attackers actively scan for vulnerable software, it is necessary for a company's cyber security program to know what software is installed and running on its network. If one system is compromised, through that system attackers will navigate entire company network and compromise other systems. CSC 2 identifies the software running on each detected device.

White list: Software that can be used in the company to be placed on the white list.

Black list: Software that is not allowed to be placed on the black list.

Gray list: Software that is used in the compiling or decompiling of software, penetration testing and scanning are some examples of software that should be classified as authorized high-risk software and should be placed on gray list. This software must be monitored and restricted to limited named users for security purposes.

b.1 Devise a list of authorized software and version that is required in the enterprise for each type of system, including servers, workstations, and laptops of various kinds and uses. This list should be monitored by file integrity checking tools to validate that the authorized software has not been modified. Quick win*

Identifying the assets and creating a list of software for each of those types. Here is a point of integration that stands to be automated. If it is not automated, then whenever you update your authorized software list, you also need to update your FIM (Forefront identity manager) tool. If this could be automated, then FIM tool should be capable of understanding when it comes across an asset (it will know what should/shouldn’t be installed).

Q: Perform regular scanning and generate alerts when unapproved software is installed on a computer.

+ This must be automated, scanning involves three steps:

a. Harvesting information from your computing devices.

b. Comparing the information, you’re harvested against your white list of authorized software.

c. Generating an alert when an unauthorized piece of software is discovered.

Q: A strict change control process should also be implemented to control any changes or installation of software to any systems on the network.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No	n/a		

Risk Level b.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

b.2 Deploy application whitelisting that allows systems to run software only if it is included on the whitelist and prevents execution of all other software on the system. The whitelist may be very extensive (as is available from commercial whitelist vendors), so that users are not inconvenienced when using common software. Or, for some special-purpose systems (which require only a small number of programs to achieve their needed business functionality), the whitelist may be quite narrow. Quick win*

This requirement depends on having the list of authorized software. OS vendors provide this type of support which is more advantageous if OS provided whitelisting capabilities.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No	n/a		

Risk Level b.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	2	2

b.3 Deploy software inventory tools throughout the organization covering each of the operating system types in use, including servers, workstations, and laptops. The

software inventory system should track the version of the underlying operating system as well as the applications installed on it. The software inventory systems must be tied into the hardware asset inventory so all devices and associated software is tracked from a single location. Visibility/attribution*

This requirement lends credence to the idea of an asset inventory tool being holistic, covering network and computing devices as well as software. The software inventory tool should inform your patch and vulnerability assessment process. The requirement describes two systems to cooperate so computing devices and software are tracked from a single location which is cooperation of the two inventory systems where one is dominant.

The software inventory tool should also monitor for unauthorized software installed on each machine.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	SCCM		Automated today

Risk Level b.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

b.4 Virtual machines and/or air-gapped systems should be used to isolate and run applications that are required for business operations but based on higher risk should not be installed within a networked environment. Advanced*

An organization needs to understand all their applications, what their needs are, risks they pose to business processes, and then potentially re-architect they system to accommodate virtualization or establish manual processes to deal with migrating information over an air gap.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Both virtual and air gapped, with no overlap of the network		n/a

Risk Level b.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Overall CSC b Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC b

Total Numeric score = **2**

Number of sub controls = **4**

Percentage implemented **= 50%**

Secure configurations for hardware and software. Establish, Implement, and actively manage (track, report on, correct) the security configuration of laptops, servers, and workstations using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

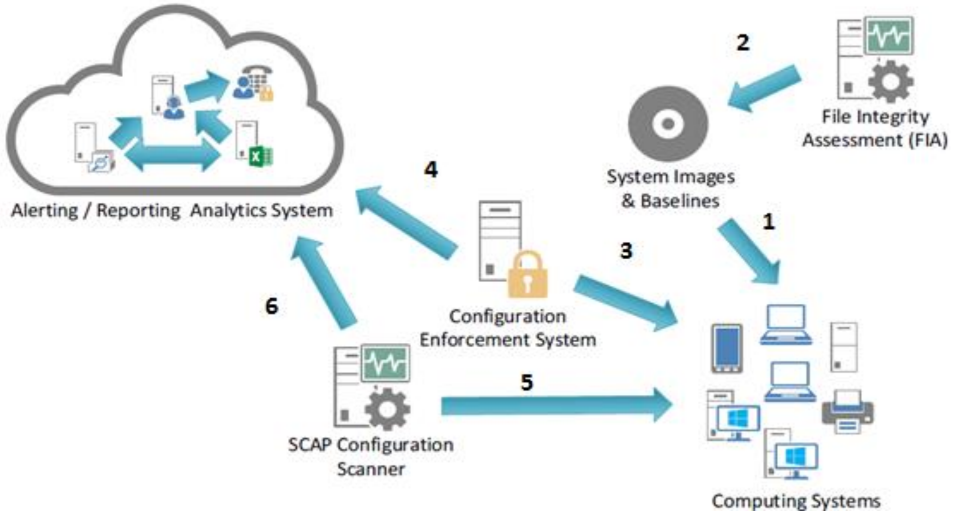

Alerting / Reporting Analytics System
File Integrity Assessment (FIA)
System Images & Baselines
Configuration Enforcement System
SCAP Configuration Scanner
Computing Systems
1
2
3
4
5
6

Figure 6. System Entity Relationship Diagram of CSC c.

- Step 1: Secure system images applied to computing systems.
- Step 2: File integrity assessment systems monitor critical system binaries and data sets.
- Steps 3 and 4: Configuration management system validates and checks system images and initiates to the alerting system.
- Steps 5 and 6: SCAP configuration scanner validates configurations and sends deviations to alerting system.

c.1 Establish standard secure configurations of operating systems and software applications. Standardized images should represent hardened versions of the underlying operating system and the applications installed on the system. These images should be validated and refreshed on a regular basis to update their security configuration considering recent vulnerabilities and attack vectors. Quick win*

The purpose of security settings is to harden the systems. This requirement pertaining to what hardening should entail, some recommended benchmarks could be provided on a per-industry basis. Secure system images are subject to updating along with all the production systems in operation. When production patch cycle is in process, the secure images should be updated as well.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	System build checklist and gold image standards		SCCM and scripted installs

Risk Level c.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

c.2 Follow strict configuration management, building a secure image that is used to build all new systems that are deployed in the enterprise. Any existing system that becomes compromised should be re-imaged with the secure build. Regular updates or exceptions to this image should be integrated into the organization's change management processes. Images should be created for workstations, servers, and other system types used by the organization. Quick win*

This is an obvious requirement and it is better to create, maintain and secure a master image used for the platforms. Re-images if compromised is straightforward requirement but it also must align with the IDS (Intrusion detection system) and response processes. Images for other system types include laptops and any system which can be imaged, that should be imaged.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	System build checklist and gold image standards		SCCM, VMware golden images, and scripts

Risk Level c.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

c.3 Store the master images on securely configured servers, validated with integrity checking tools capable of continuous inspection, and change management to ensure that only authorized changes to the images are possible. Alternatively, these master images can be stored in offline machines, air- gapped from the production network, with images copied via secure media to move them between the image storage servers and the production network. Quick win*

Securing the master images is not really a control as it is the decision based on risk. Risk pertaining to this requirement is low. Storing these images in offline machines would be the strategy for securing the master images more than it is a control requirement. If the images are stored offline, then physical access controls become the gate. If you need the physical access then automation and speed gets reduced.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		Integrity Check missing	Yes	Does VMware have the ability to check changes to images? Could SCCM be used to monitor changes to images

Risk Level c.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	1

d. 4 Perform all remote administration of servers, workstation, network devices, and similar equipment over secure channels. Protocols such as telnet, VNC, RDP, or others that do not actively support strong encryption should only be used if they are

performed over a secondary encryption channel, such as SSL, TLS or IPSEC.

Configuration/hygiene*

This requirement is how you manage your systems throughout the organization and choose secure protocols to implement. This could be a medium risk for the organization as the protocols such as telnet, RDP, VNC are considered vulnerable and prone to attacks.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		RDP internal is not secure, from external to J&B we use SSL	n/a	They could be automated with NAC to prevent running of vnc, rdp and telnet

Risk Level c.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

c.5 Use file integrity checking tools to ensure that critical system files (including sensitive system and application executable, libraries, and configurations) have not been altered. The reporting system should: can account for routine and expected changes; highlight and alert on unusual or unexpected alterations; show the history of configuration changes over time and identify who made the change (including the original logged-in account in the event of a user ID switch, such as with the su or sudo command). These integrity checks should identify suspicious system alterations such as: owner and permissions changes to files or directories; the use of alternate data streams which could be used to hide malicious activities; and the introduction of extra files into key system areas (which could indicate malicious payloads left by

attackers or additional files inappropriately added during batch distribution processes). Configuration/hygiene*

System integrity is more important, scanning must be done once a day for maintaining better security. This shall not affect to the business operations. There might be few exceptions for the time stamp on scanning based on the business needs. Reporting system is included as part of the integrity monitoring tool. This is referring to HIDS (Host intrusion detection system).

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Don't have technology in place to accomplish this	Yes

Risk Level c.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

c.6 Implement and test an automated configuration monitoring system that verifies all remotely testable secure configuration elements, and alerts when unauthorized changes occur. This includes detecting new listening ports, new administrative users, changes to group and local policy objects (where applicable), and new services running on a system. Whenever possible, use tools compliant with the Security Content Automation Protocol (SCAP) to streamline reporting and integration. Advanced*

This requirement is that we need to monitor the hardening settings mentioned in the previous points. This is termed as configuration assessment. If we are using a configuration assessment tool, it should be capable of ingesting SCAP benchmarks.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Don't have technology in place to accomplish this	

Risk Level c.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

c.7 Deploy system configuration management tools, such as Active Directory Group Policy Objects for Microsoft Windows systems or Puppet for UNIX systems that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals. They should be capable of triggering redeployment of configuration settings on a scheduled, manual, or event-driven basis. Configuration/hygiene*

It is best to check configuration setting in variety of ways, ensure that group policy objects themselves are correctly configured, systems governed by group policy objects are properly configured and the local security policy is appropriately configured.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Group policy		Yes

Risk Level c.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	3

Overall CSC c Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC c

- Total Numeric score = **4**
- Number of sub controls = **7**
- Percentage implemented **= 57%**

Continuous vulnerability assessment and remediation. Continuously acquire, assess, and act on new information to identify vulnerabilities, remediate, and minimize the window of opportunity for attackers.

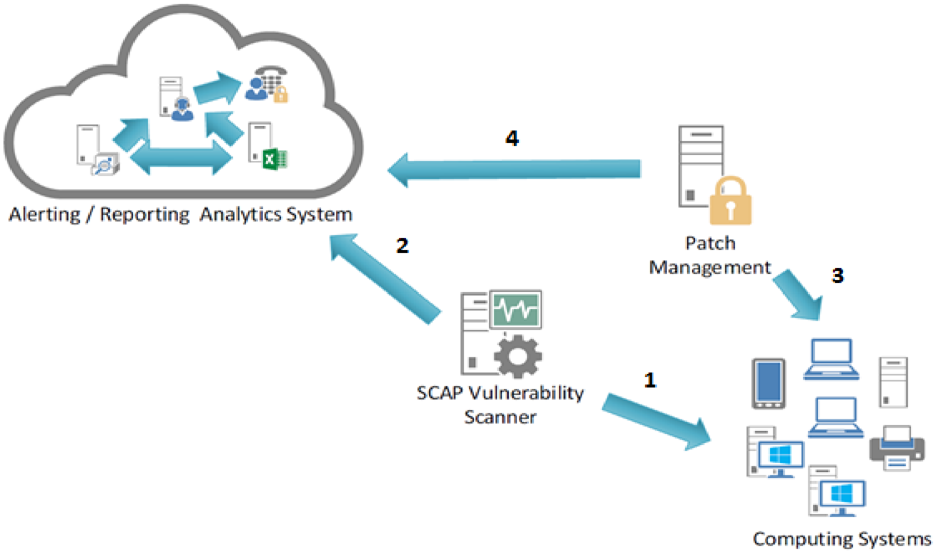

Alerting / Reporting Analytics System
4
2
Patch Management
3
SCAP Vulnerability Scanner
1
Computing Systems

Figure 7. System Entity Relationship Diagram of CSC d.

- Steps 1 and 2: Vulnerability scanner scan the computing systems and report the detected vulnerabilities to alerting/reporting system.
- Steps 3 and 4: A patch management system applies software updates to computing systems and initiates to the reporting system.

d.1 Run automated vulnerability scanning tools against all systems on the network on a weekly or more frequent basis and deliver prioritized lists of the most critical

vulnerabilities to each responsible system administrator along with risk scores that compare the effectiveness of system administrators and departments in reducing risk. Use a SCAP-validated vulnerability scanner that looks for both code---based vulnerabilities (such as those described by Common Vulnerabilities and Exposures entries) and configuration-based vulnerabilities (as enumerated by the Common Configuration Enumeration Project). Quick win*

Using SCAP validated scanners should enable you to take vulnerability scanning content for multiple sources as it is released. Daily scan is probably good for normal systems but for critical systems having real-time vulnerability detection enabled will match better.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, for malware and virus, No for patches and other vulnerabilities and configurations	Trend Micro, Juniper IDP, Iron Port	Don't have technology in place to accomplish this	Yes

Risk Level d.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	3

d.2 Correlate event logs with information from vulnerability scans to fulfill two goals. First, personnel should verify that the activity of the regular vulnerability scanning tools is itself logged. Second, personnel should be able to correlate attack detection events with prior vulnerability scanning results to determine whether the given exploit was used against a target known to be vulnerable. Quick win*

This requirement is focused on SIEM and audit-logger. This is an indication of the different ways these controls interact.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Don't have technology in place to accomplish this	Yes

Risk Level d.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

d.3 Perform vulnerability scanning in authenticated mode either with agents running locally on each end system to analyze the security configuration or with remote scanners that are given administrative rights on the system being tested. Use a dedicated account for authenticated vulnerability scans, which should not be used for any other administrative activities and should be tied to specific machines at specific IP addresses. Ensure that only authorized employees have access to the vulnerability management user interface and that roles are applied to each user. Quick win*

Using dedicated accounts will be easier to lock it down, correlate on what is doing the vulnerability scanning. We can consider Center for internet security or DISA sources for recommendations on other ways to lock down the account. It explicitly recognizes that the tools used to enforce technical security control are themselves subject to security control. Keep a list of authorized users for vulnerability management system and that list should be role-based. LDAP integration might work here.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Don't have technology in place to accomplish this	Yes

Risk Level d.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	1

d.4 Subscribe to vulnerability intelligence services to stay aware of emerging exposures, and use the information gained from this subscription to update the organization's vulnerability scanning activities on at least a monthly basis. Alternatively, ensure that the vulnerability scanning tools you use are regularly updated with all relevant important security vulnerabilities. Quick win*

Vendor is not the only source of vulnerability information. Depending upon the specific organization needs, it may be advantageous to source vulnerabilities from several locations to ensure maximum vulnerability coverage.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, not completely		There are other services that should be used could include: SANS Storm, US CERT, secunia	

Risk Level d.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	1

d.5 Deploy automated patch management tools and software update tools for operating system and software/applications on all systems for which such tools are available and safe. Patches should be applied to all systems, even systems that are properly air gapped. Visibility/attribution*

This requirement states that you need to ensure coverage for all classes of software in your asset inventory. If the systems are air gapped its vulnerabilities are not exploitable.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No	No focus has been put towards this one and the technology is there to accomplish for desktop/laptop		yes

Risk Level d.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	2	1

d.6 Monitor logs associated with any scanning activity and associated administrator accounts to ensure that this activity is limited to the timeframes of legitimate scans. Visibility/attribution*

This requirement is concerned with audit logging and more of a process. This audit logging has no much importance in this control.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No	Would need auditing in place to track usage of account performing scanning activities	No technology in place to complete	Yes

Risk Level d.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	1

d.7 Compare the results from back-to-back vulnerability scans to verify that vulnerabilities were addressed, either by patching, implementing a compensating control, or documenting and accepting a reasonable business risk. Such acceptance of business risks for existing vulnerabilities should be periodically reviewed to determine if newer compensating controls or subsequent patches can address vulnerabilities that

were previously accepted, or if conditions have changed, increasing the risk. Configuration/hygiene*

This is a straight forward requirement and more of process. The vulnerability scans themselves will not understand that it has compensated for the control in some way. We need to track this outside of vulnerability management tool by way of exception, waiver, risk acceptance or compensating control. Perhaps more problematic is the reliance of risk.

This needs some level of assessment and a good understanding of how particular software vulnerability may impact one or more business processes. Assessment to be made based on if this vulnerability is successfully exploited, then how many days it will be down, cost to the company and amount for recovery.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes, partially	Malware reports and compare back to back for remediation issues. No on windows or application patching		no	might now be a good idea to automate

Risk Level d.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	1	1

d.8 Establish a process to risk-rate vulnerabilities based on the exploitability and potential impact of the vulnerability, and segmented by appropriate groups of assets (example, DMZ servers, internal network servers, desktops, laptops). Apply patches for the riskiest vulnerabilities first. A phased rollout can be used to minimize the impact to the organization. Establish expected patching timelines based on the risk rating level. Configuration/Hygiene*

Be sure to assess each of the vulnerability in the context of the organization before prioritizing your assets. A phased rollout can apply to a variety of controls and is something that can certainly help the concern manager aligns with the organization more easily.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		We have the skill to do this, just not following at this point	Yes, for patching process

Risk Level d.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

Overall CSC d Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Low Maturity	Medium Risk

Overall Implementation level CSC d:

- Total Numeric score = **1.5**
- Number of sub controls = **8**
- Percentage implemented = **19%**

Controlled use of administrative privileges. The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.

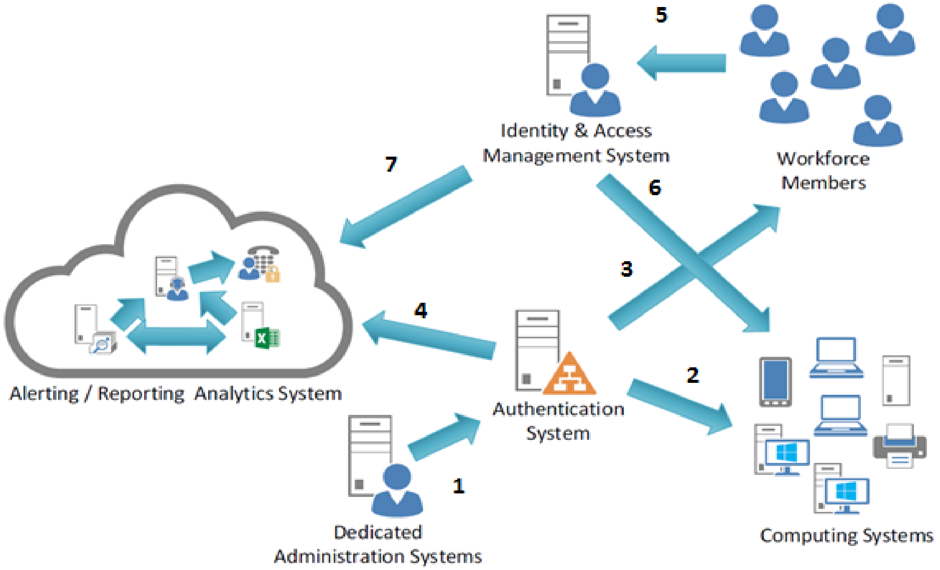


Figure 8. System Entity Relationship Diagram of CSC e.

- Steps 1, 2, and 3: Dedicated administration system, workforce members and computing systems use proper authentication systems.
- Step 4: Authentication system validates, checks and initiates to the alerting system.
- Steps 5 and 6: Using identity and access management system workforce members gets access to the computing systems securely. Identity and access management system reports the log information to the reporting system.

e.1 Minimize administrative privileges and only use administrative accounts when they are required. Implement focused auditing on the use of administrative privileged functions and monitor for anomalous behavior. Quick win*

Windows users need to restrict in setting everyone as local administrator. Create a second account to use when needing to perform admin tasks and disable login from those account through group policy.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, for minimization of use no for anomalous behavior.		Not able to audit to this level.	yes

Risk Level e.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	1	2

e.2 Use automated tools to inventory all administrative accounts and validate that each person with administrative privileges on desktops, laptops, and servers is authorized by a senior executive. Quick win*

Use Host intrusion detection system (HIDS) to monitor these accounts.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		not able to audit to this level	Yes

Risk Level e.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

e.3 Before deploying any new devices in a networked environment, change all default passwords for applications, operating systems, routers, firewalls, wireless access points, and other systems to have values consistent with administration---level accounts. Quick win*

This is a very basic and common-sense requirement and should be part of Asset management system.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
For the most items, this is correct. We do this for servers, routers, switches.	Manual process	Do not change for printing devices, or controllers, maybe time clocks, building security systems	No	Also, will need a process for completing this check and an audit that it is complete

Risk Level e.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

e.4 Configure systems to issue a log entry and alert when an account is added to or removed from a domain administrators' group, or when a new local administrator account is added on a system. Visibility/attribution*

This is a good requirement to implement. If we use a SIEM, we can configure it to examine these events and the context surrounding them in more detail to avoid too many false positives.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No, we do not		Not sure	Yes	

Risk Level e.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

e.5 Configure systems to issue a log entry and alert on any unsuccessful login to an administrative account. Visibility/attribution*

Any admin account on any device/application should be monitored. If enable logging on your domain controllers, the logging is taken care of and this need something that can report on these logs.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Systems are set to log, but not to alert		No logging server	Yes

Risk Level e.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

e.6 Use multi-factor authentication for all administrative access, including domain administrative access. Multi-factor authentication can include a variety of techniques, to include the use of smart cards, certificates, One Time Password (OTP) tokens, biometrics, or other similar authentication methods. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No technology in place to complete	

Risk Level e.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

e.7 Where multi-factor authentication is not supported; user accounts shall be required to use long passwords on the system (longer than 14 characters). Configuration/hygiene*

This requirement is an alternative to multi-factor authentication. This could be a best practice.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Don't complete 5.6 so this one also not being done	

Risk Level e.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

e.8 Administrators should be required to access a system using a fully logged and non-administrative account. Then, once logged on to the machine without administrative privileges, the administrator should transition to administrative privileges using tools such as Sudo on Linux/UNIX, RunAs on Windows, and other similar facilities for other types of systems. Configuration/Hygiene*

This is important requirement. When you assign an individual administrative right and issue them an administrative account their regular account needs to be fully logged. You should also deny logons to your service accounts, but grant them the “log on as service” right in group policy.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		We have not implemented Admin id for our Admins. Currently use admin account as daily account.		Would require a process to be put in place and followed.

Risk Level e.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

e.9 Administrators shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

Configuration/Hygiene*

Administrators should be more operationally secure as to avoid using their administrative accounts for surfing the web.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		We have not implemented an admin machine for all changes		Would require a process to be put in place and followed.

Risk Level e.9:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

Overall CSC e Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Low Maturity	Medium Risk

Overall Implementation level CSC e:

- Total Numeric score = **1.5**
- Number of sub controls = **9**
- Percentage implemented = **17%**

Maintenance, monitoring, and analysis of audit logs. Collect, manage, and analyze audit logs of events that could help detect, understand, or recover from an attack.

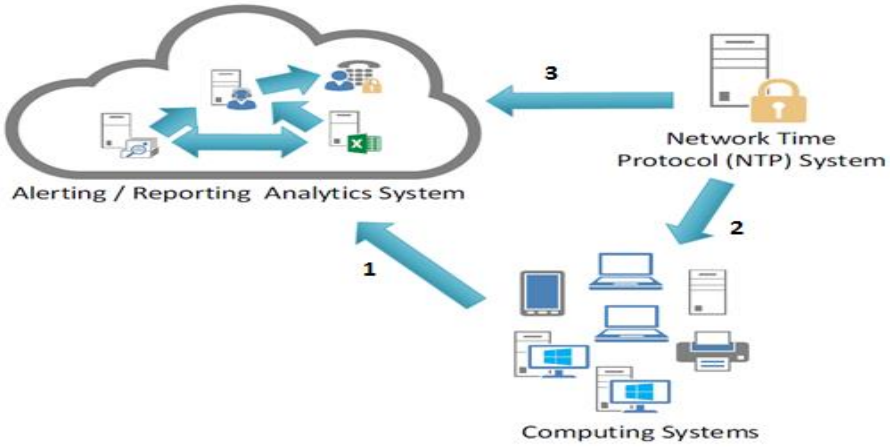


Figure 9. System Entity Relationship Diagram of CSC f.

- Step 1: Computing systems generate logs and send them to the reporting system.
- Steps 2 and 3: Computing system and reporting system synchronize time with Network time protocol system or central time management system.

f.1 Include at least two synchronized time sources from which all servers and network equipment retrieve time information on a regular basis so that timestamps in logs are consistent. Quick win*

If using one internal and another external source be sure that one using internally doesn't reference the same external NTP source the other are using.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No just one source for time jbhqtdc01-Server		No priority	No

Risk Level f.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

f.2 Validate audit log settings for each hardware device and the software installed on it, ensuring that logs include a date, timestamp, source addresses, destination

addresses, and various other useful elements of each packet and/or transaction. Systems should record logs in a standardized format such as syslog entries or those outlined by the Common Event Expression initiative. If systems cannot generate logs in a standardized format, log normalization tools can be deployed to convert logs into such a format. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No logging server, so would not be a benefit for us	Yes	Would need to get a logging server prior to this change

Risk Level f.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

f.3 Ensure that all systems that store logs have adequate storage space for the logs generated on a regular basis, so that log files will not fill up between log rotation intervals. The logs must be archived and digitally signed on a periodic basis. Quick win*

To ensure not only enough space at the outset of the asset's lifecycle but ensuring throughout if you want to log all the things.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No logging server, so would not be a benefit for us	Yes	Would need to get a logging server prior to this change

Risk Level f.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

f.4 Have security personnel and/or system administrators run biweekly reports that identify anomalies in logs. They should then actively review the anomalies, documenting their findings. Quick win*

To be more secure and with right toolset in place this report should happen at least daily and with automation, so that the red flags are brought to the attention of the administrator. Most of the tools will not find you everything, manual work is also needed.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No logging server, so would not be a benefit for us	Yes	Would need to get a logging server prior to this change

Risk Level f.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

f.5 Configure network boundary devices, including firewalls, network---based IPS, and inbound and outbound proxies, to verbosely log all traffic (both allowed and blocked) arriving at the device. Visibility/attribution*

This requirement is more of a best practice.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No logging server, so would not be a benefit for us	Yes	Would need to get a logging server prior to this change

Risk Level f.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

f.6 Deploy a SIEM (Security Information and Event Management) or log analytic tools for log aggregation and consolidation from multiple machines and for log correlation and analysis. Using the SIEM tool, system administrators and security personnel should devise profile of common events from given systems so that, they can tune detection to focus on unusual activity, avoid false positives, more rapidly identify anomalies, and prevent overwhelming analysts with insignificant alerts. Visibility/attribution*

SIEMs and audit logging solutions should be business aware to help you and then customize the default profiles to specific needs. If you have a SIEM tool, should reply as much as possible on the vendor to provide high-quality, out-of-box profiles.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		No, logging server so would not be a benefit for us. Also cost and time to review	Yes	Would need to get a logging server prior to this change

Risk Level f.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

Overall CSC f Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
Low Maturity	Medium Risk

Overall Implementation level CSC f:

- Total Numeric score = **0**
- Number of sub controls = **6**
- Percentage implemented = **0%**

Email and web browser protections. Minimize the attack surface and the opportunities for attackers to manipulate human behavior though their interaction with web browsers and email systems.

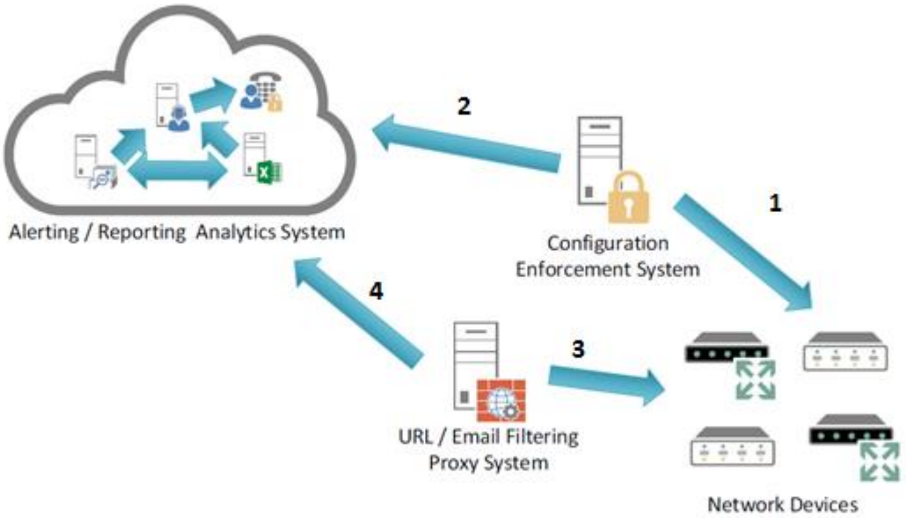

2
1
Alerting / Reporting Analytics System
Configuration Enforcement System
4
3
URL / Email Filtering Proxy System
Network Devices

Figure 10. System Entity Relationship Diagram of CSC g.

- Steps 1 and 2: Configuration enforcement system actively scans network devices for misconfigurations or deviations from baseline and initiates to the Alerting/reporting system.
- Steps 3 and 4: URL/Email filtering proxy system filters the URL/ Email over the network devices and initiates any suspicious activity to alerting system.

g.1 Ensure that only fully supported web browsers and email clients are allowed to execute in the organization, ideally only using the latest version of the browsers provided by the vendor in order to take advantage of the latest security functions and fixes. Quick win*

If using an outdated browser, this might put into a risk from many security threats. Old versions are less stable and more vulnerable to viruses, spyware, malware and other security issues.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	lock down systems		Automated

Risk Level g.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

g.2 Uninstall or disable any unnecessary or unauthorized browser or email client plugins or add-on applications. Each plugin shall utilize application / URL whitelisting and only allow the use of the application for pre-approved domains. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Partially, we do not whitelist URLs.	Lock down systems	Not sure business would agree with this lock down	Yes

Risk Level g.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

g.3 Limit the use of unnecessary scripting languages in all web browsers and email clients. This includes the use of languages such as ActiveX and JavaScript on systems where it is unnecessary to support such capabilities. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Not sure business would agree with this lock down	Yes

Risk Level g.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

g.4 Log all URL requests from each of the organization's systems, whether onsite or a mobile device, to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems. Visibility/Attribution*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	IronPort/srx650		Yes

Risk Level g.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

g.5 Deploy two separate browser configurations to each system. One configuration should disable the use of all plugins, unnecessary scripting languages, and generally be configured with limited functionality and be used for general web browsing. The other configuration shall allow for more browser functionality but should only be used to access specific websites that require the use of such functionality.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Not sure business would agree with this lock down	Yes

Risk Level g.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

g.6 The organization shall maintain and enforce network based URL filters that limit a system's ability to connect to websites not approved by the organization. The organization shall subscribe to URL categorization services to ensure that they are up-to-date with the most recent website category definitions available. Uncategorized sites shall be blocked by default. This filtering shall be enforced for each of the organization's systems, whether they are physically at an organization's facilities or not. Visibility/attribution*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	IronPort/srx650		Yes

Risk Level g.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	3

g.7 To lower the chance of spoofed email messages, implement the Sender Policy Framework (SPF) by deploying SPF records in DNS and enabling receiver---side verification in mail servers. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			

Risk Level g.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

g.8 Scan and block all email attachments entering the organization's email gateway if they contain malicious code or file types that are unnecessary for the organization's business. This scanning should be done before the email is placed in the user's inbox. This includes email content filtering and web content filtering.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Microsoft email scanner and Trend Email scan		Yes

Risk Level g.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	3

Overall CSC g risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC g:

- Total Numeric score = **5.5**
- Number of sub controls = **8**
- Percentage implemented = **69%**

Limitation and control of network ports. Manage (track/control/correct) the ongoing operational use of ports, protocols, and services on networked devices to minimize windows of vulnerability available to attackers.

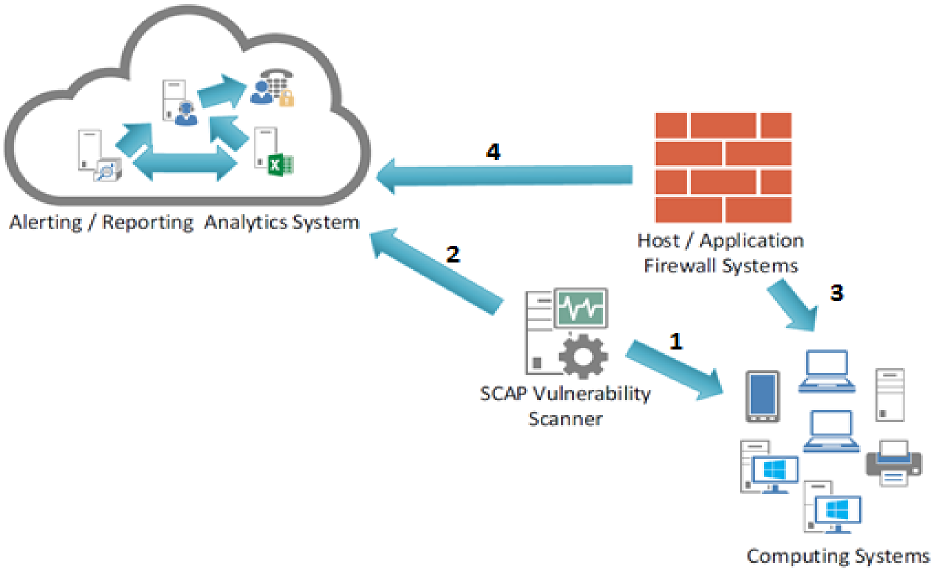

Alerting / Reporting Analytics System
4
2
Host / Application Firewall Systems
3
1
SCAP Vulnerability Scanner
Computing Systems

Figure 11. System Entity Relationship Diagram of CSC h.

- Steps 1 and 2: Vulnerability scanner scan the computing systems and alerts and reports the detected vulnerabilities to alerting/reporting system.
- Steps 3 and 4: Computing systems protected with host-based firewalls, active scanner validates which ports, protocols and services are accessible on computing system and initiates to the alerting/reporting system.

h.1 Ensure that only ports, protocols, and services with validated business needs are running on each system. Quick win*

Network services are vulnerable to exploitation. Based on business needs enable services for systems or disable and uninstall the services if already enabled.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Not a priority	

Risk Level h.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	2	2

h.2 Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed. Quick win*

The host based filtering required for the organization to know what needs to be operated on these endpoints. This is aligned with having a good asset inventory as mentioned in CSC 1 and 2. The windows firewall and GPOs work fine for this requirement.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, partially	Handled on external facing devices by the firewall, not internally	Not a priority	No

Risk Level h.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

h.3 Perform automated port scans on a regular basis against all key servers and compare to a known effective baseline. If a change that is not listed on the organization's approved baseline is discovered, an alert should be generated and reviewed. Quick win*

The baseline should be a standard that is pointed by policy and referenced by procedures. If you scan and detect any deviation from standard baseline for which you have no compensating control, then generate alert. Compensating control thing should be automated as much as possible to avoid unnecessary reviews. This can be done by HIDS.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Not a priority	Yes

Risk Level h.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	1

h.4 Verify any server that is visible from the Internet or an untrusted network, and if it is not required for business purposes, move it to an internal VLAN and give it a private address. Visibility/attribution*

Basically, this requirement is not to put internal only servers out on the DMZ or in the security zone where the public servers reside.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			No

Risk Level h.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	3

h.5 Operate critical services on separate physical or logical host machines, such as DNS, file, mail, web, and database servers. Configuration/Hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			No

Risk Level h.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

h.6 Place application firewalls in front of any critical servers to verify and validate the traffic going to the server. Any unauthorized services or traffic should be blocked and an alert generated. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, partial external facing server not internal facing servers. Block but no alerts	srx650		Yes

Risk Level h.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

Overall CSC h Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC h:

- Total Numeric score = **3**
- Number of sub controls = **6**
- Percentage implemented = **50%**

Data recovery capability. The processes and tools used to properly back up critical information with a proven methodology for timely recovery of it.

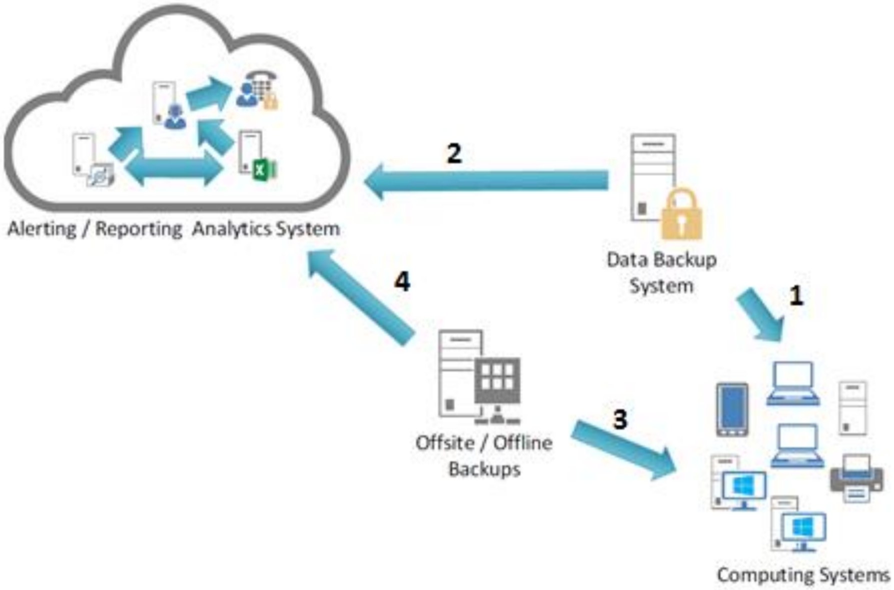

Alerting / Reporting Analytics System
2
Data Backup System
4
1
Offsite / Offline Backups
3
Computing Systems

Figure 12. System Entity Relationship Diagram of CSC i.

- Steps 1 and 2: Computing systems backed up on a regular basis to data backup systems and initiates to the reporting system.
- Steps 3 and 4: Backups created are stored offline/offsite storage facilities.

i.1 Ensure that each system is automatically backed up on at least a weekly basis, and more often for systems storing sensitive information. To help ensure the ability to rapidly restore a system from backup, the operating system, application software, and data on a machine should each be included in the overall backup procedure. These three components of a system do not have to be included in the same backup file or use the same backup software. There should be multiple backups over time, so that in the event of malware infection, restoration can be from a version that is believed to predate the original infection. All backup policies should be compliant with any regulatory or official requirements.

Frequency of backup should be predicted not only on data sensitivity but also on frequency of change. Recommendation is to back up the data and also recover in a timely manner. This requirement ought to be tied back to controls 1, 2 and 3 which cover asset management and configuration management of endpoints.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, some server that change infrequently may be backed up monthly instead of weekly	CommVault, vRanger, NetApp Snaps		Yes

Risk Level i.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

i.2 Test data on backup media on a regular basis by performing a data restoration process to ensure that the backup is properly working.

This is particularly important requirement that dovetails with your data restoration or data backup planning. This is more of a procedure.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	CommVault, vRanger, NetApp Snaps		Yes, but not automated today

Risk Level i.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

i.3 Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.

Encryption of data is preferred most in this requirement. If using outsources provider for remote backup and/or cloud services, you need to determine whether their information security program aligns with the enterprise program.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
yes, but still stored on same campus just different location than DC	CommVault, vRanger, NetApp Snaps		no

Risk Level i.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	3

i.4 Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like Crypto Locker which seek to encrypt or damage data on all addressable data shares, including backup destinations.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	NetApp Snaps		Yes

Risk Level i.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Overall CSC i Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC i:

- Total Numeric score = **3.5**
- Number of sub controls = **4**
- Percentage implemented = **88%**

Secure configurations for network devices. Establish, implement, and actively manage (track, report on, correct) the security configuration of network infrastructure devices using a rigorous configuration management and change control process to prevent attackers from exploiting vulnerable services and settings.

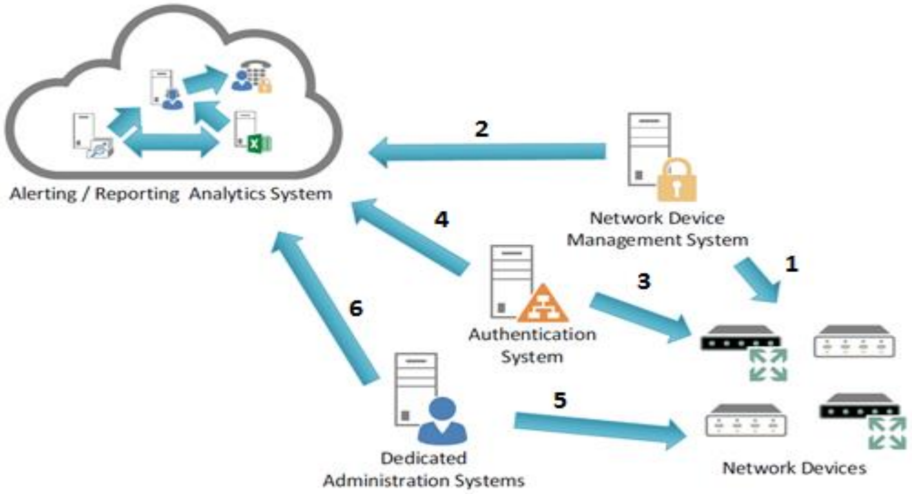


Figure 13. System Entity Relationship Diagram of CSC j.

- Steps 1 and 2: Network device management system validates configurations on Network devices and initiates to the alerting system.
- Steps 3 and 4: Two-factor Authentication system required for administrative access to network devices and the authentication system validates, checks and initiates to the alerting system.
- Steps 5 and 6: Dedicated administration system for network administrators.

j.1 Compare firewall, router, and switch configuration against standard secure configurations defined for each type of network device in use in the organization. The security configuration of such devices should be documented, reviewed, and approved by an organization change control board. Any deviations from the standard configuration or updates to the standard configuration should be documented and approved in a change control system.

This requirement may use some standards to compare the current configuration and is a **quick win*** category. The center for internet security or defense information system agency will be good sources for obtaining some standards. The requirement expects the organization to assume standard configurations unless documented otherwise.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
We use a standard configuration for all devices and use this on all networking devices. We use a change control process and documentation. Then it is approved through the change control process	Manual process and will continue to be manual		Not worth it for the low amount of new networking equipment deployed at J&B

Risk Level 11.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

j.2 All new configuration rules beyond a baseline-hardened configuration that allow traffic to flow through network security devices, such as firewalls and network-based IPS, should be documented and recorded in a configuration management system, with a specific business reason for each change, a specific individual's name responsible for that business need, and an expected duration of the need.

This requirement falls under **configuration/hygiene*** category. Any network boundary moving from one security posture to another should have ingress/egress filtering and be well-controlled. The requirement implied to apply at the network boundary and document the activities.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Change is documented in the log, but we do not record requestor or business need or duration	J:\Hardware Info\Network Hardware Logs\Network Security\STM		No

Risk Level j.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	2

j.3 Use automated tools to verify standard device configurations and detect changes. All alterations to such files should be logged and automatically reported to security personnel.

This requirement falls under **configuration/hygiene*** category.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, nothing in place to compare configuration.		Cost of application vs. return not there. Only 3 people have password to the devices.	Yes, with the right application

Risk Level j.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	2

j.4 Manage network devices using two-factor authentication and encrypted sessions. Configuration/hygiene*

We must configure an authentication server that supports multi-factor authentication.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No Authentication server in place, and they are no AD aware devices as well	Yes, with an authentication server

Risk Level j.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

j.5 Install the latest stable version of any security-related updates on all network devices. **Configuration/hygiene***

This is referring to network device update. Receive notifications from vendors and manufacturers.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, with recommendation from vendors and manufacturers	Manually install patches		N/A

Risk Level j.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

j.6 Network engineers shall use a dedicated machine for all administrative tasks or tasks requiring elevated access. This machine shall be isolated from the organization's primary network and not be allowed Internet access. This machine shall not be used for reading email, composing documents, or surfing the Internet.

This requirement is more like restricting the attacks which occur through emails, internet and getting access to sensitive data and termed as **advanced*** category.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Have not consider it a risk	N/A

Risk Level j.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	3	2

j.7 Manage the network infrastructure across network connections that are separated from the business use of that network, relying on separate VLANs or, preferably, on entirely different physical connectivity for management sessions for network devices.

Following this procedure is better from a security perspective and is **advanced***.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, with VLANS and not physical Networks			N/A

Risk Level j.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Overall CSC j Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
High Maturity	Medium Risk

Overall Implementation level CSC j:

- Total Numeric score = **4**
- Number of sub controls = **7**
- Percentage implemented = **57%**

Data protection. The processes and tools used to prevent data exfiltration, mitigate the effects of exfiltrated data, and ensure the privacy and integrity of sensitive information.

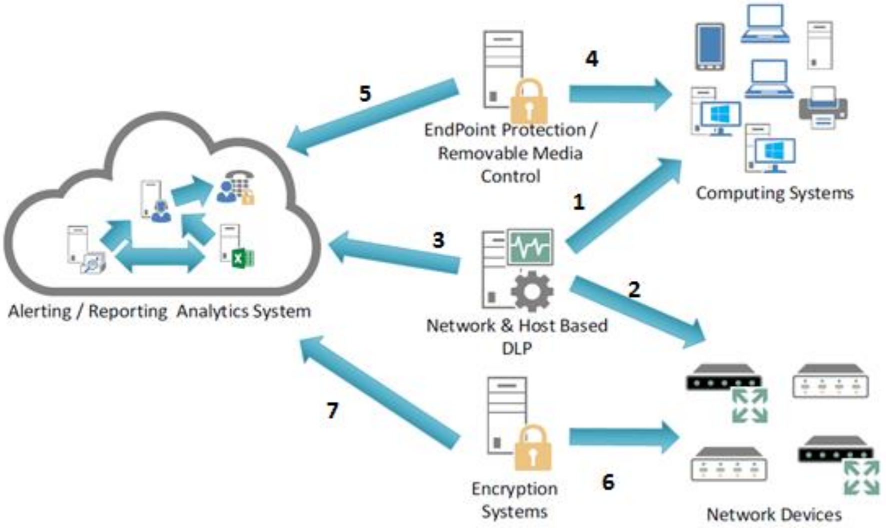

5
4
EndPoint Protection / Removable Media Control
Computing Systems
1
3
Alerting / Reporting Analytics System
Network & Host Based DLP
2
7
Encryption Systems
6
Network Devices

Figure 14. System Entity Relationship Diagram of CSC k.

- Steps 1, 2, and 3: Network and host based DLP scans for sensitive data on network boundaries and computing systems, initiates the alerting system and blocks whenever unauthorized attempts to exfiltrate the data.
- Steps 4 and 5: End-point protection to be deployed on the computing systems which detects malware and initiates the alerting system.
- Steps 6 and 7: Data encryption system ensures that appropriate devices are encrypted that holds the sensitive data and data transfer over the less-trusted network should be encrypted.

k.1 Perform an assessment of data to identify sensitive information that requires the application of encryption and integrity control. Quick win*

Data resides in many places; protection of that data is best achieved through the application of a combination of encryption, integrity protection and data loss prevention techniques.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No data classification process at J&B or encryption	No

Risk Level k.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

k.2 Deploy approved hard drive encryption software to mobile devices and systems that hold sensitive data. Quick win*

Deploying approved software is one thing, but managing and operational security is another. This is quick win unless you want to accept the risk of losing information that is stored on mobile devices.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, not completely		Until the deployment of devices in May 2016-bit locker was not enabled	Yes

Risk Level k.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

k.3 Deploy an automated tool on network perimeters that monitors for sensitive information (e.g., personally identifiable information), keywords, and other document characteristics to discover unauthorized attempts to exfiltrate data across

network boundaries and block such transfers while alerting information security personnel. Visibility/attribution*

This requirement is pertaining to DLP (Data loss prevention).

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No tool owned by J&B to accomplish this, also no data classification exists	Yes

Risk Level k.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

k.4 Conduct periodic scans of server machines using automated tools to determine whether sensitive data (e.g., personally identifiable information, health, credit card, or classified information) is present on the system in clear text. These tools, which search for patterns that indicate the presence of sensitive information, can help identify if a business or technical process is leaving behind or otherwise leaking sensitive information. Visibility/attribution*

This requirement is important, but it will probably take some manpower to get it done. What sensitive information is on your system, what format does it take and where might it be like in data base, binary etc.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No tool owned by J&B to accomplish this, also no data classification exists	Yes

Risk Level k.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

k.5 If there is no business need for supporting such devices, configure systems so that they will not write data to USB tokens or USB hard drives. If such devices are required, enterprise software should be used that can configure systems to allow only specific USB devices (based on serial number or other unique property) to be accessed, and that can automatically encrypt all data placed on such devices. An inventory of all authorized devices must be maintained. Configuration/hygiene*

It is difficult not to use USB devices. The same was covered in asset management (CSC 1) and this requirement needs you to handle on the precise types of devices you'll need to hook to USB.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No			Yes

Risk Level k.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

k.6 Use network-based DLP solutions to monitor and control the flow of data within the network. Any anomalies that exceed the normal traffic patterns should be noted and appropriate action taken to address them. Configuration/hygiene*

This requirement tells to control the flow of data within the network which is the prevention part of DLP.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No			Yes

Risk Level k.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

k.7 Monitor all traffic leaving the organization and detect any unauthorized use of encryption. Attackers often use an encrypted channel to bypass network security devices. Therefore, it is essential that organizations can detect rogue connections, terminate the connection, and remediate the infected system. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		No logging of traffic so could only see it in real time. Would need a SIEM	Yes

Risk Level k.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	3

k.8 Block access to known file transfer and email exfiltration websites. Advanced*

Subscribe to a service that offers this requirement. Ensure the tools you use understand how to import those lists.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, Partially	Built into the SRX650		Yes

Risk Level k.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	1	3

k.9 Use host-based data loss prevention (DLP) to enforce ACLs even when data is copied off a server. In most organizations, access to the data is controlled by ACLs that are implemented on the server. Once the data have been copied to a desktop

system, the ACLs are no longer enforced and the users can send the data to whomever they want. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No		Not sure we have the application to accomplish this	Yes

Risk Level k.9:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

Overall CSC k Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
Low Maturity	High Risk

Overall Implementation level CSC k:

- Total Numeric score = **0.5**
- Number of sub controls = **9**
- Percentage implemented = **5.5%**

Wireless access control. The processes and tools used to track/control/prevent/correct the security use of wireless local area networks (LAN), access points, and wireless client systems.

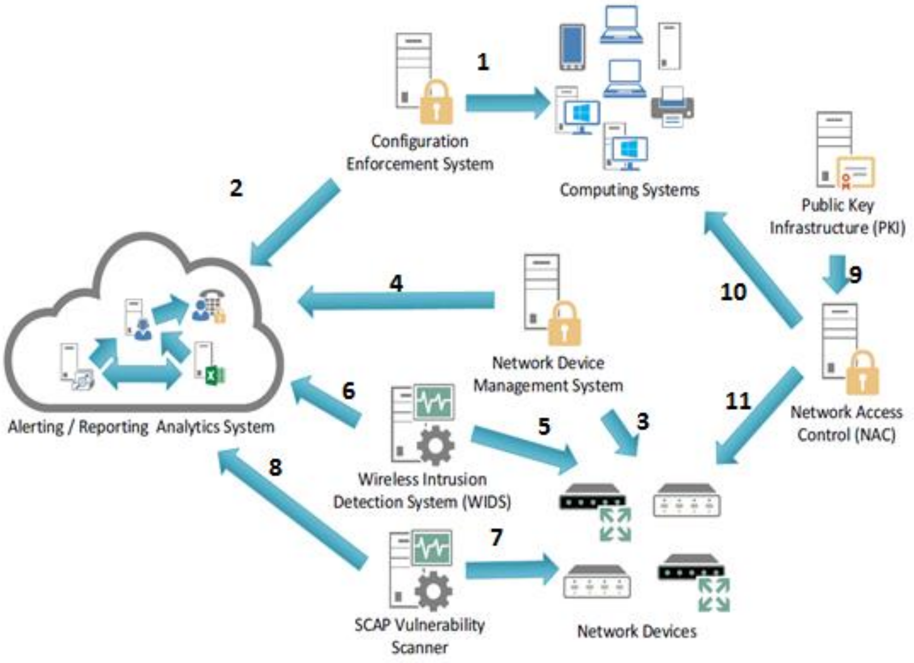

Configuration Enforcement System
1
Computing Systems
Public Key Infrastructure (PKI)
2
4
9
10
Network Device Management System
Network Access Control (NAC)
6
11
Alerting / Reporting Analytics System
5
3
8
Wireless Intrusion Detection System (WIDS)
7
SCAP Vulnerability Scanner
Network Devices

Figure 15. System Entity Relationship Diagram of CSC l.

- Steps 1 and 2: Configuration enforcement system checks and validates the proper configuration of computing systems.
- Steps 3 and 4: Network device management system analyzes network traffic and initiates any suspicious events to alerting system.
- Steps 5 and 6: Wireless IDS monitor usage of wireless communications.
- Steps 7 and 8: Vulnerability scanner scan the network devices and report the detected vulnerabilities to alerting/reporting system.
- Steps 9, 10, and 11: Utilize client certificates to validate and authenticate systems prior to connecting to computing systems and network devices controlled by Network access control.

l.1 Ensure that each wireless device connected to the network matches an authorized configuration and security profile, with a documented owner of the connection and

a defined business need. Organizations should deny access to those wireless devices that do not have such a configuration and profile. Quick win*

Use Network access control on wireless network uses 802.1x.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No NAC, exercise control over wireless devices.	Enable windows NAC		

Risk Level l.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	2	2

l.2 Configure network vulnerability scanning tools to detect wireless access points connected to the wired network. Identified devices should be reconciled against a list of authorized wireless access points. Unauthorized (i.e., rogue) access points should be deactivated. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Ruckus wireless		Yes

Risk Level l.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

l.3 Use wireless intrusion detection systems (WIDS) to identify rogue wireless devices and detect attack attempts and successful compromises. In addition to WIDS, all wireless traffic should be monitored by WIDS as traffic passes into the wired network. Visibility/attribution*

To be more effective, running commercial wireless scanning, detection and discovery tools as well as commercial wireless intrusion detection systems are recommended. The security team should periodically capture wireless traffic and use analysis tools to determine whether the wireless traffic was transmitted using weaker protocols.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Ruckus wireless		Yes

Risk Level l.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

l.4 Where a specific business need for wireless access has been identified, configure wireless access on client machines to allow access only to authorized wireless networks. For devices that do not have an essential wireless business purpose, disable wireless access in the hardware configuration (basic input/output system or extensible firmware interface). Visibility/attribution*

Manage your assets, know where they are, who owns them, who uses them. This is more relied on a policy rather than a tool. Make sure that these devices are monitored for wireless connections using any of the tools mentioned in the above sections.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, must be allowed based on business needs.			

Risk Level l.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	3	2

Procedures:

l.5 Ensure that all wireless traffic leverages at least Advanced Encryption Standard (AES) encryption used with at least Wi---Fi Protected Access 2 (WPA2) protection. Configuration/hygiene*

This is deterrent to small-minded hackers. Recent attacks have traces of WPA2 being compromised. Best practice would be absolutely enable the protection, but be updated and keep a track of the attacks as they may change and adjust your protection appropriately. At the very least use AES with WPA2.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Ruckus		N/A

Risk Level l.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

l.6 Ensure that wireless networks use authentication protocols such as Extensible Authentication Protocol-Transport Layer Security (EAP/TLS), which provide credential protection and mutual authentication. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, we need authentication server.			

Risk Level l.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	3	2

l.7 Disable peer-to-peer wireless network capabilities on wireless clients. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			

Risk Level l.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Procedure:

GPO: Computer configuration>Policies>Administrative templates>Network>Microsoft Peer-to-peer networking services.

Disable Ad-hoc GPO-Computer configuration>windows settings>Security settings>Wireless Network (IEEE 802.11) policies>set the policy to "Network to access: Access point (Infrastructure) networks only".

l.8 Disable wireless peripheral access of devices (such as Bluetooth) unless such access is required for a documented business need.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
We are not actively doing this.			

Risk Level l.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	2

l.9 Create separate virtual local area networks (VLANs) for BYOD systems or other untrusted devices. Internet access from this VLAN should go through at least the same border as corporate traffic. Enterprise access from this VLAN should be treated as untrusted and filtered and audited accordingly. Configuration/hygiene*

802.1x in section 1.5 can aid in this situation. Small businesses should have the ability to configure their wireless routers to provision clients on a segregated network and deny that network from accessing internal resources. VPN access may or may not be blocked as per policy.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Guest network controlled by DMZ for BYOD.		

Risk Level l.9:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Overall CSC l Risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
High Maturity	Medium Risk

Overall Implementation level CSC l:

- Total Numeric score = **5.5**
- Number of sub controls = **9**
- Percentage implemented = **61%**

CSC m: Controlled access based on the need to know. The processes and tools used to track/control/prevent/correct secure access to critical assets (e.g., information, resources, systems) according to the formal determination of which persons, computers and applications have a need and right to access these critical assets based on an approved classification.

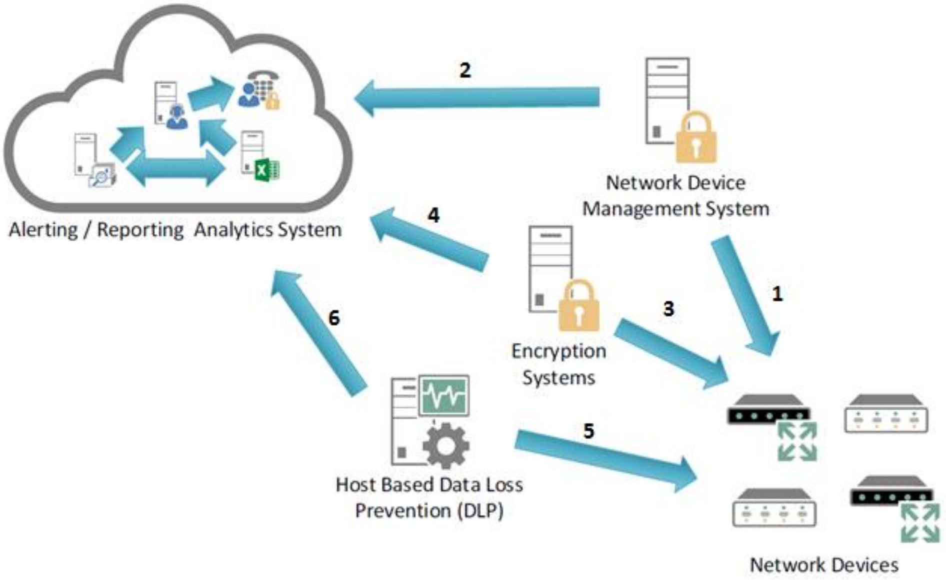


Figure 16. System Entity Relationship Diagram of CSC m.

- Steps 1 and 2: Network device management system analyzes network traffic and initiates any suspicious events to alerting system.
- Steps 3 and 4: Data encryption system ensures that appropriate devices are encrypted that holds the sensitive data and data transfer over the less-trusted network should be encrypted.
- Steps 5 and 6: Host based DLP validates and checks all access requests and initiates to the alerting system.

m.1 Segment the network based on the label or classification level of the information stored on the servers. Locate all sensitive information on separated VLANS with firewall filtering to ensure that only authorized individuals are only able to communicate with systems necessary to fulfill their specific responsibilities. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Somewhat done	We segment all servers on a vlan. Also segment public servers from private. We do not exclude any J&B associates from any server networks		No, should be automated

Risk Level m.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	1

m.2 All communication of sensitive information over less-trusted networks should be encrypted. Whenever information flows over a network with a lower trust level, the information should be encrypted. Quick win*

Encryption should be done not only over the less trusted networks but also over the trusted networks, especially if there are separations of duties with in the organization.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes, for the most part		So, EDI is not encrypted but there is probably no sensitive information in these transactions. There is a possibility that email might contain sensitive information.	No	Need to clarify what sensitive information is and have a classification system

Risk Level m.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
	2	1

m.3 All network switches will enable Private Virtual Local Area Networks (VLANs) for segmented workstation networks to limit the ability of devices on a network to

directly communicate with other devices on the subnet and limit an attacker's ability to laterally move to compromise neighboring systems. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, some exceptions which does not apply to organization.			

Risk Level m.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	1

m.4 All information stored on systems shall be protected with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principal that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Using access control lists		No

Action Items: Develop a policy and schedule a review cycle for critical roles.

Risk Level m.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

m.5 Sensitive information stored on systems shall be encrypted at rest and require a secondary authentication mechanism, not integrated into the operating system, to access the information. Visibility/Attribution*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Somewhat done,	The FTP server does encrypt information at rest	We do not classify data a sensitive or not	No	We would need an application to search for sensitive information and alert us to information and then encrypt it.

Risk Level m.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	1	3

m.6 Enforce detailed audit logging for access to nonpublic data and special authentication for sensitive data. Configuration/hygiene*

Special authentication to sensitive data might require a re-authentication or use of separate accounts with special, specific privileges.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No		We do not classify data a sensitive or nonpublic data, no two-form authentication and no detailed audit logging.	No	Would need a data classification and SEIM product

Risk Level m.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

m.7 Archived data sets or systems not regularly accessed by the organization shall be removed from the organization's network. These systems shall only be used as stand-alone systems (disconnected from the network) by the business unit needing to occasionally use the system or completely virtualized and powered off until needed. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Yes	Done by best practice		Yes, with data retention policies	An official policy should be created around how and when we do this

Risk Level m.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	1

Overall CSC m Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
Medium Maturity	Medium Risk

Overall Implementation level CSC m:

- Total Numeric score = **3**
- Number of sub controls = **7**
- Percentage implemented = **43%**

Account monitoring and control. Actively manage the life cycle of system and application accounts-their creation, use, dormancy, deletion—to minimize opportunities for attackers to leverage them.

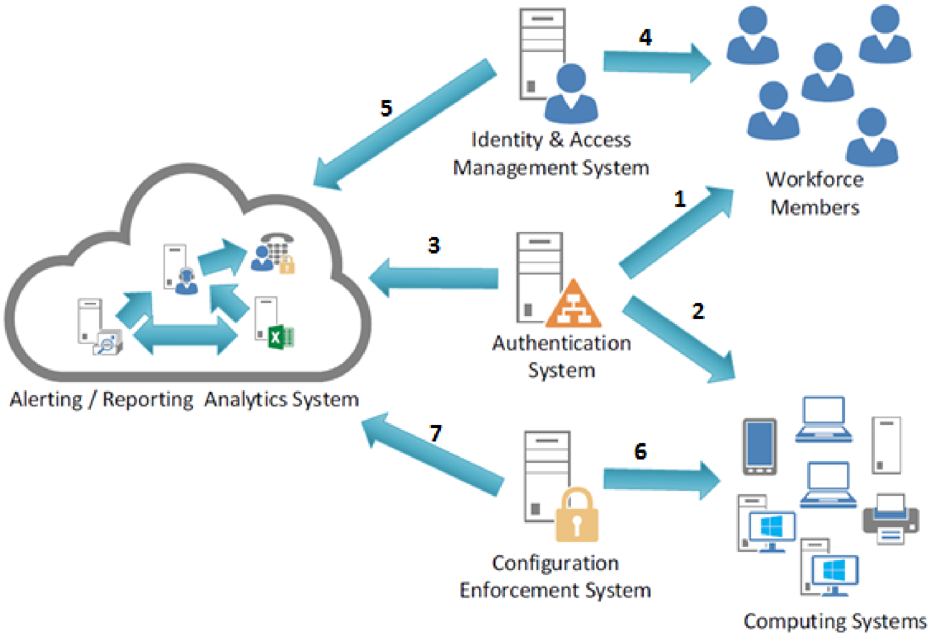

4
5
Identity & Access Management System
Workforce Members
1
3
2
Authentication System
Alerting / Reporting Analytics System
7
6
Configuration Enforcement System
Computing Systems

Figure 17. System Entity Relationship Diagram of CSC n.

- Steps 1, 2, and 3: Workforce members and computing systems use proper multi-factor authentication and the authentication system initiates to the alerting system in case of any unauthorized user login.
- Steps 4 and 5: Identity and access management system monitors, checks and validates the workforce members on the domain.
- Steps 6 and 7: Configuration enforcement system checks and validates the proper configuration of computing systems.

n.1 Review all system accounts and disable any account that cannot be associated with a business process and owner. Quick win*

Each account has an owner and is associated with at least one business process. Review the accounts and disable as per the rule requirement.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, for AD and No for redpraire.	Monthly script for review.		

Risk Level n.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	1

n.2 Ensure that all accounts have an expiration date that is monitored and enforced. Quick win*

This could probably be a good idea to have an expiration date.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, not conducive to AD but implement it for vendors/contractors.			

Risk Level n.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	1

n.3 Establish and follow a process for revoking system access by disabling accounts immediately upon termination of an employee or contractor. Disabling instead of deleting accounts allows preservation of audit trails.

There should be an account management process in place of which account revocation is a part and it should be tied to HR. On termination of employees, disable the existing account.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			

Risk Level n.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.4 Regularly monitor the use of all accounts, automatically logging off users after a standard period of inactivity. Quick win*

This is a general requirement.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	Not automatically log off, but restrict the access to domain.		

Risk Level n.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.5 Configure screen locks on systems to limit access to unattended workstations. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	AD		

Risk Level n.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.6 Monitor account usage to determine dormant accounts, notifying the user or user's manager. Disable such accounts if not needed, or document and monitor exceptions (e.g., vendor maintenance accounts needed for system recovery or continuity operations). Require that managers match active employees and contractors with each account belonging to their managed staff. Security or system administrators

should then disable accounts that are not assigned to valid workforce members. Quick win*

This is a kind of requirement that had to be built in to operating systems, LDAP, NIS etc. From a security perspective documenting the files in the system which is disabled would be a good practice.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	PowerShell		

Risk Level n.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.7 Use and configure account lockouts such that after a set number of failed login attempts the account is locked for a standard period of time. Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes	AD		

Risk Level n.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.8 Monitor attempts to access deactivated accounts through audit logging. Visibility/attribution*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, we audit			

Risk Level n.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.9 Configure access for all accounts through a centralized point of authentication, for example Active Directory or LDAP. Configure network and security devices for centralized authentication as well. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes			

Risk Level n.9:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

n.10 Profile each user's typical account usage by determining normal time-of-day access and access duration. Reports should be generated that indicate users who have logged in during unusual hours or have exceeded their normal login duration. This includes flagging the use of the user's credentials from a computer other than computers on which the user generally works. Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Can log the information but not for reports.			Automated	No restrictions of logon hours with in J & B.

Risk Level n.10:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	1

n.11 Require multi-factor authentication for all user accounts that have access to sensitive data or systems. Multi-factor authentication can be achieved using smart cards, certificates, One Time Password (OTP) tokens, or biometrics. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No	OTP			Implement on Admin accounts, for systems having sensitive data and M3.

Risk Level n.11:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

n.12 Where multi-factor authentication is not supported; user accounts shall be required to use long passwords on the system (longer than 14 characters). Quick win*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
No				To get in place soon. Evaluating self-service password reset portal- To be in Place as replacement /alternative for Multi auth. Password.

Risk Level n.12:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	3	2

n.13 Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
M3, AD, VPN-To check on red prairie and priya.			

Risk Level n.13:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

n.14 Verify that all authentication files are encrypted or hashed and that these files cannot be accessed without root or administrator privileges. Audit all access to password files in the system. Advanced*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
M3, AD, VPN-To check on red prairie and priya.			

Risk Level n.14:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	2

Overall CSC n risk level:

Maturity of IT to Implement this Control	Current Risk to J&B
High Maturity	Low Risk

Overall Implementation level CSC n:

- Total Numeric score = **10.5**
- Number of sub controls = **14**
- Percentage implemented = **75%**

Application software security. Manage the security life cycle of all in-house developed and acquired software to prevent, detect, and correct security weaknesses.

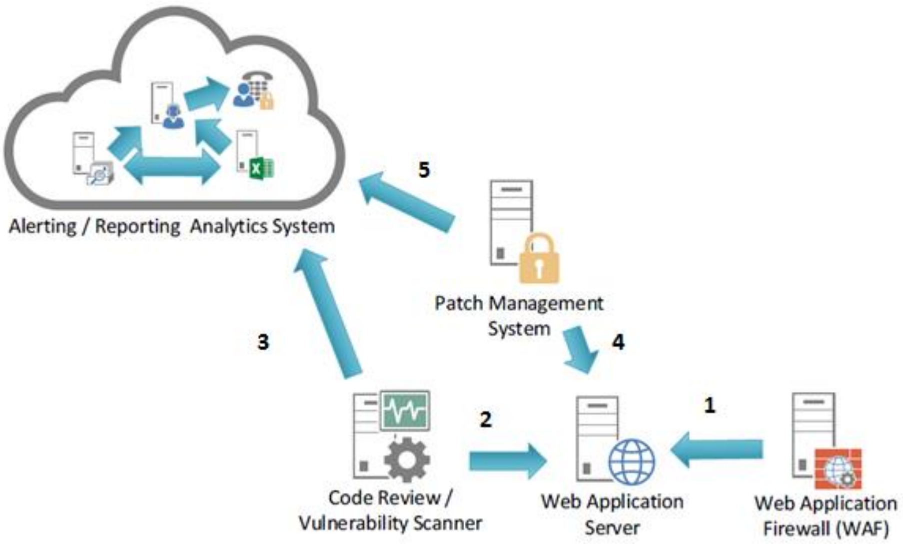

Alerting / Reporting Analytics System
5
Patch Management System
3
4
2
1
Code Review / Vulnerability Scanner
Web Application Server
Web Application Firewall (WAF)

Figure 18. System Entity Relationship Diagram of CSC o.

- Step 1: Web application firewall protect connections to internal web application server.
- Steps 2 and 3: Code analysis and vulnerability scanner scan application systems and database systems and initiates to the alerting system.
- Steps 4 and 5: Patch management system applies updates to web application server.

o.1 For all acquired application software, check that the version you are using is still supported by the vendor. If not, update to the most current version and install all relevant patches and vendor security recommendations. Quick win*

All the application software, update to the latest version for better security and this is linked to CSC c.2.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes
Not, often we do this.				Develop a template and process to check the upgrade for the applications.

Risk Level o.1:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	2

o.2 Protect web applications by deploying web application firewalls (WAFs) that inspect all traffic flowing to the web application for common web application attacks, including but not limited to cross-site scripting, SQL injection, command injection, and directory traversal attacks. For applications that are not web-based, specific application firewalls should be deployed if such tools are available for the given application type. If the traffic is encrypted, the device should either sit behind the encryption or can decrypt the traffic prior to analysis. If neither option is appropriate, a host-based web application firewall should be deployed. Quick win*

This requires automated tool to inspect traffic and provide analysis. Cross site scripting, SQL injection, command injection and directory traversal attack is something that is critical to look for. Securing your SDLC would mitigate these attacks.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Marc to check on Juniper-inspection of traffic web application attacks.			

Risk Level o.2:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	1

o.3 For in-house developed software, ensure that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. Visibility/attribution*

This is more of a process than a tool.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, log in library that catches all the entries.			

Risk Level o.3:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	2	1

o.4 Test in-house-developed and third-party-procured web applications for common security weaknesses using automated remote web application scanners prior to deployment, whenever updates are made to the application, and on a regular recurring basis. Input validation and output encoding routines of application software should be reviewed and tested. Visibility/attribution*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, we do. Integration compatibility check.	Test plan spread sheet, use cases etc. Unilevel testing.		

Risk Level o.4:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

o.5 Do not display system error messages to end-users (output sanitization). Visibility/attribution*

This is more of a process per application.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Except for label manager, rest all is locked down.			

Risk Level o.5:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

o.6 Maintain separate environments for production and nonproduction systems. Developers should not typically have unmonitored access to production environments. Visibility/attribution*

Certainly, for critical systems you are going to have some non-production system you can use to test and mitigate some problems like the system that processes sensitive information, the mock data needs to resemble the real world without needing to be real data. Developers should not have access to development that isn’t monitored.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
We have logs, but not monitoring the logs.			

Risk Level o.6:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0.5	3	2

o.7 For applications that rely on a database, use standard hardening configuration templates. All systems that are part of critical business processes should also be tested. Configuration/Hygiene*

If performing configuration management which is CSC c, then it is already ensuring that the OS and database are appropriately configured.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No, we don't have any template in place.			

Risk Level o.7:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	3	2

o.8 Ensure that all software development personnel receive training in writing secure code for their specific development environment. Configuration/hygiene*

Create a culture of security-mindedness around your SDLC and give them the training they need. This all comes down to training.

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
No training or policy in place.			

Risk Level o.8:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
0	1	2

o.9 For in-house developed applications, ensure that development artifacts (sample data and scripts; unused libraries, components, debug code; or tools) are not included in

the deployed software, or accessible in the production environment.

Configuration/hygiene*

J & B GROUP:

Do we do this?	If so, how	If not, why?	Can this be automated?
Yes, release built process, code optimization.			

Risk Level o.9:

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B
1	3	1

Overall CSC o Risk Level:

Maturity of IT to Implement this Control	Current Risk to J&B
High Maturity	Medium Risk

Overall Implementation level CSC o:

- Total Numeric score = **5**
- Number of sub controls = **9**
- Percentage implemented = **55%**

Summary

Every attempt was made to cross-reference between sources to validate the data and during compilation. Multiple tests were performed and results are consistent. This consistency was confirmed of the legitimacy of source data. This chapter provides the tools and techniques used for this research.

Chapter IV: Analysis of Results

Introduction

Security is all about managing risk. This means no amount of security can fully protect a system from the loss but there will be risks to the confidentiality, integrity, and availability of data. The best way to the loss is to understand the risk and implement appropriate controls to minimize and manage it. Data collected from the organization is analyzed in this chapter; critical controls are selected and in detail explanation of the importance of selected controls are presented. Also, implementation is done using the SIEM tool integrating with other software for collecting log data and finally monitoring rules are established.

Data Presentation

Data collected by running over the security controls and questionnaire are quantified using the formula (Sum of Implementation Level Score of sub controls in each control/ Total number of sub-controls in each control) * 3 and represented in a table format (Table 4). See Appendix B for complete details.

Table 4

Overall Security Controls Implementation, Risk and Maturity Levels

Control	Description	No. of Sub-Controls	Implementation Level Score	Maturity of IT to Manage this risk	Risk to J&B	Percentage Implemented
1	Inventory of Authorized and Unauthorized Devices	6	2.00	Low Maturity	Medium Risk	33%
2	Inventory of Authorized and Unauthorized Software	4	2.00	Med Maturity	Medium Risk	50%
3	Secure Configurations for Hardware and Software on mobile devices, laptops, workstations and servers.	7	4.00	Med Maturity	Medium Risk	57%
4	Continuous Vulnerability Assessment and Remediation	8	1.50	Low Maturity	Medium Risk	19%
5	Controlled Use of Administrative Privileges	9	1.50	Low Maturity	Medium Risk	17%
6	Maintenance, Monitoring, and Analysis of Audit Logs	6	0.00	Low Maturity	Medium Risk	0%
7	Email and Web Browser Protections	8	5.50	Med Maturity	Medium Risk	69%
8	Malware Defenses	6	2.50	Low Maturity	Medium Risk	42%
9	Limitation and Control of Network Ports, protocols, and services	6	3.00	Med Maturity	Medium Risk	50%
10	Data Recovery Capability	4	3.50	Med Maturity	Medium Risk	88%
11	Secure Configurations for Network Devices such as firewalls, routers, and switches.	7	4.00	High Maturity	Medium Risk	57%
12	Boundary Defense	10	4.50	Med Maturity	High Risk	45%

Table 4 Continued

Control	Description	No. of Sub-Controls	Implementation Level Score	Maturity of IT to Manage this risk	Risk to J&B	Percentage Implemented
13	Data Protection	9	0.50	Low Maturity	High Risk	6%
14	Controlled Access Based on the Need to Know	7	3.00	Med Maturity	Medium Risk	43%
15	Wireless Access Control	9	5.50	High Maturity	Medium Risk	61%
16	Account Monitoring and Control	14	10.50	High Maturity	Low Risk	75%
18	Application Software Security	9	5.00	High Maturity	Medium Risk	56%

Data Analysis

Analyzing the presented data with SIEM tool capabilities, current resource maturity levels to handle the risk and risk levels for implementation, below are the critical controls selected from the 20 are Malware Defenses and Boundary Defense.

Malware defenses. One of the most popular end-point security tools is anti-virus. Malware defense is not limited to the use of anti-virus tools but extends to managing additional threats, the scope of infection, breaches related to many risks and activities. Organizations should routinely monitor for critical anti-virus which should be prioritized by the system, type of issue, operations, and probably spread of infection. SIEM offer the means to centralize malware monitoring and reporting processing which also measures overall malware infection and assessing operational impact. This is done by correlating event log data from the anti-malware management system, here the software used is FireEye.

Integrating FireEye to IBM QRadar SIEM tool for receiving the event data which includes IP addresses of the source and target machines, type of malware, ports, time of the event, action taken from FireEye to endpoint etc. It also provides the means to centralize malware incident response, facilitate processes to identify infected systems to quarantine and remediate by correlating unusual port activity from firewall log, DNS requests, and warnings from IDS/IPS on outbound communications to a known malicious site and identified port scanning.

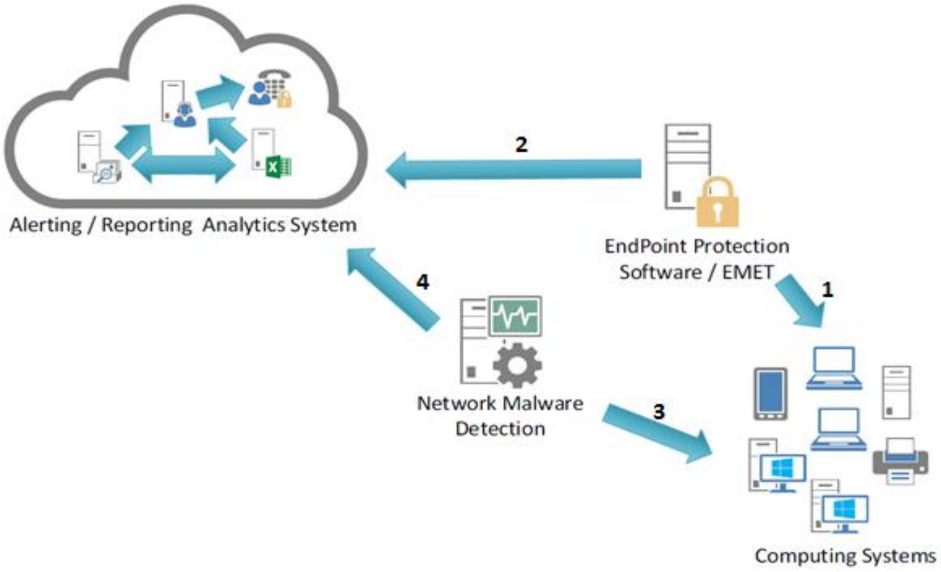


Figure 19. System Entity Relationship Diagram of Malware Defenses.

- Steps 1 and 2: Endpoint protection software tool is deployed on the computing systems which protects them even before new and undiscovered threats are addressed by security updates and antimalware software and reports the log information to the reporting system.
- Steps 3 and 4: Network malware detection tool use techniques other than signature-based detection to identify and filter out malicious content before it arrives at the endpoint and initiates the alerting system in case of any malicious activity.

FireEye Logs into QRadar. QRadar SIEM open source ISO file is downloaded and installed on one of the old machines organization has purchased before. This device is having an

IP address allocated to it an application is installed up and running. The event data is forwarded from FireEye to QRadar by providing IP address details of QRadar in FireEye. Similarly, a log source is created in QRadar with the IP address of FireEye to ensure receiving of events from FireEye to know the event originating from that log source.

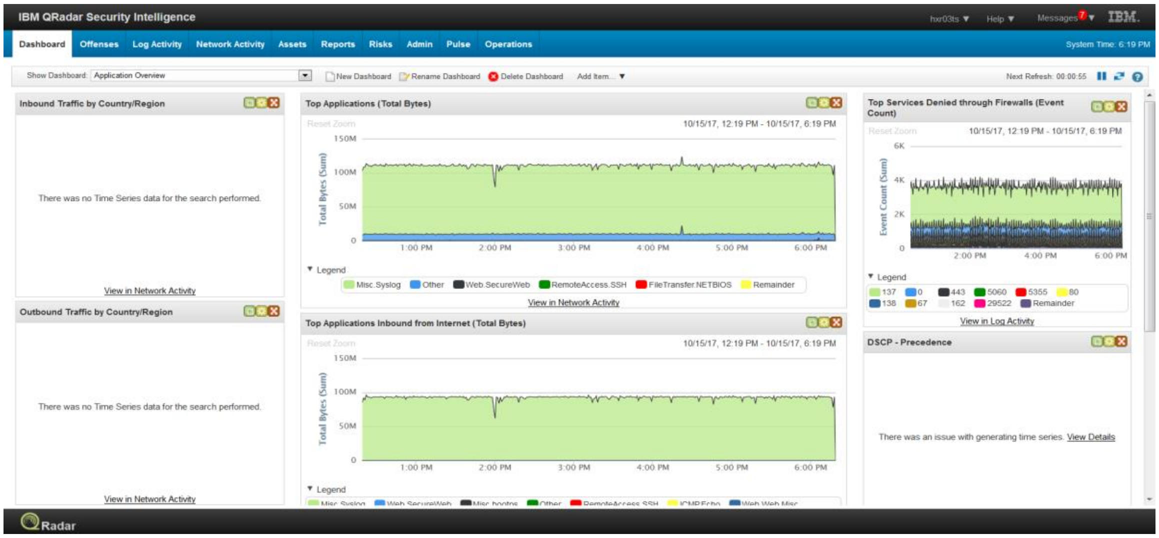
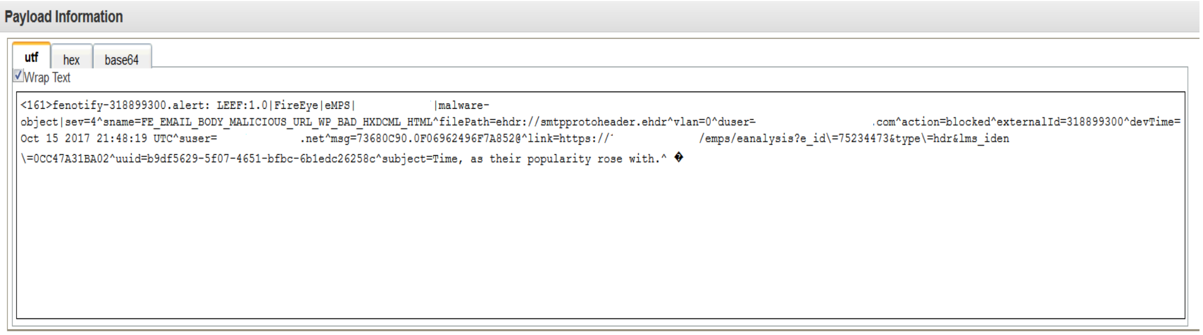
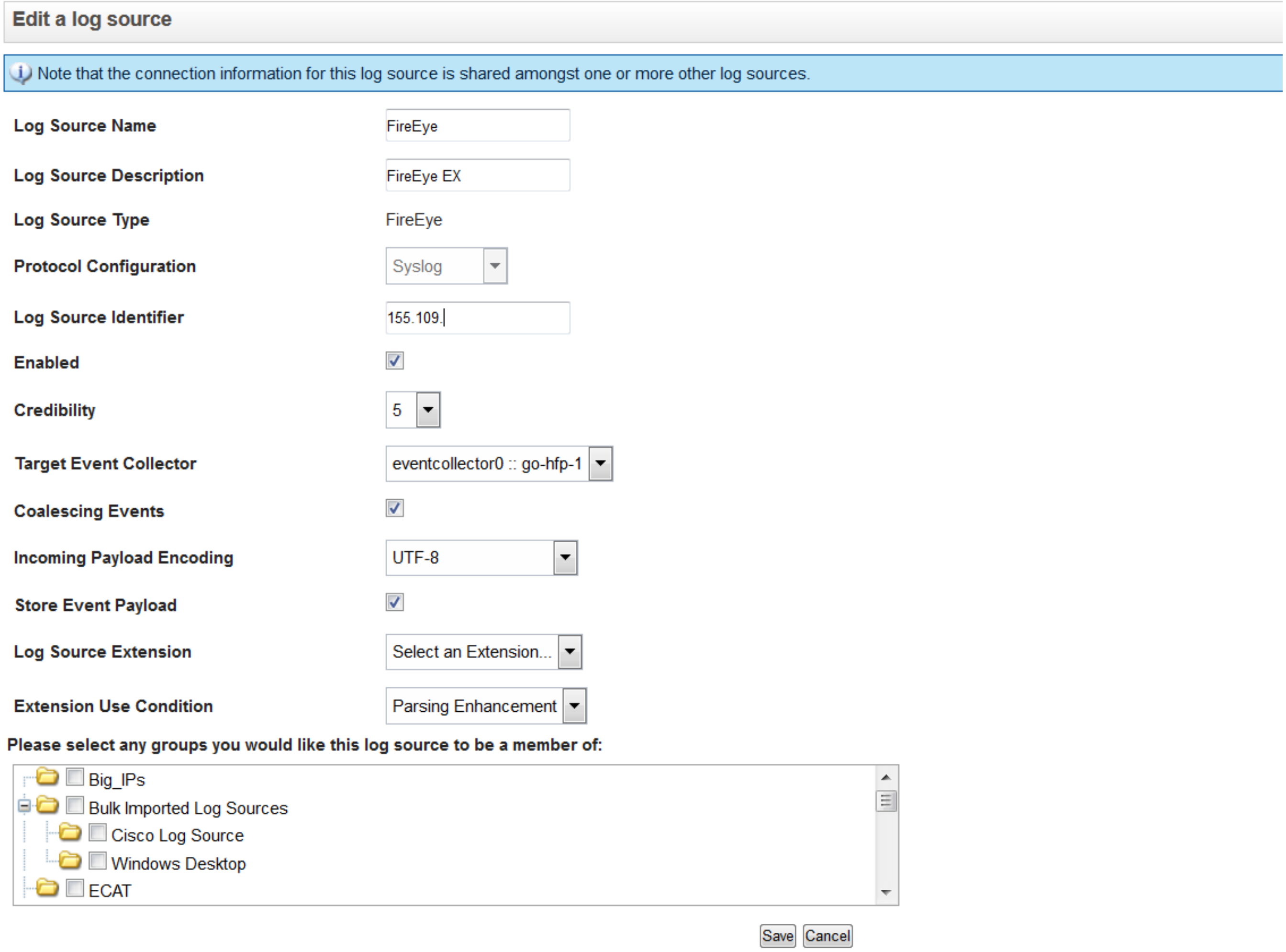


Figure 20. QRadar SIEM Application.



```
<161>fenotify-318899300.alert: LEEF:1.0|FireEye|eMPS|            |malware-
object|sev=4^sname=FE_EMAIL_BODY_MALICIOUS_URL_WP_BAD_HXDCML_HTML^filePath=ehdr://smtpprotoheader.ehdr^vlan=0^duser=                .com^action=blocked^externalId=318899300^devTime=
Oct 15 2017 21:48:19 UTC^suser=           .net^msg=73680C90.0F06962496F7A852@^link=https://`            /emps/eanalysis?e_id\=75234473&type\=hdr&lms_iden
\=0CC47A31BA02^uuid=b9df5629-5f07-4651-bfbc-6b1edc26258c^subject=Time, as their popularity rose with.^ �
```

Figure 21. Sample Event Payload from FireEye Device to QRadar.



Edit a log source

Note that the connection information for this log source is shared amongst one or more other log sources.

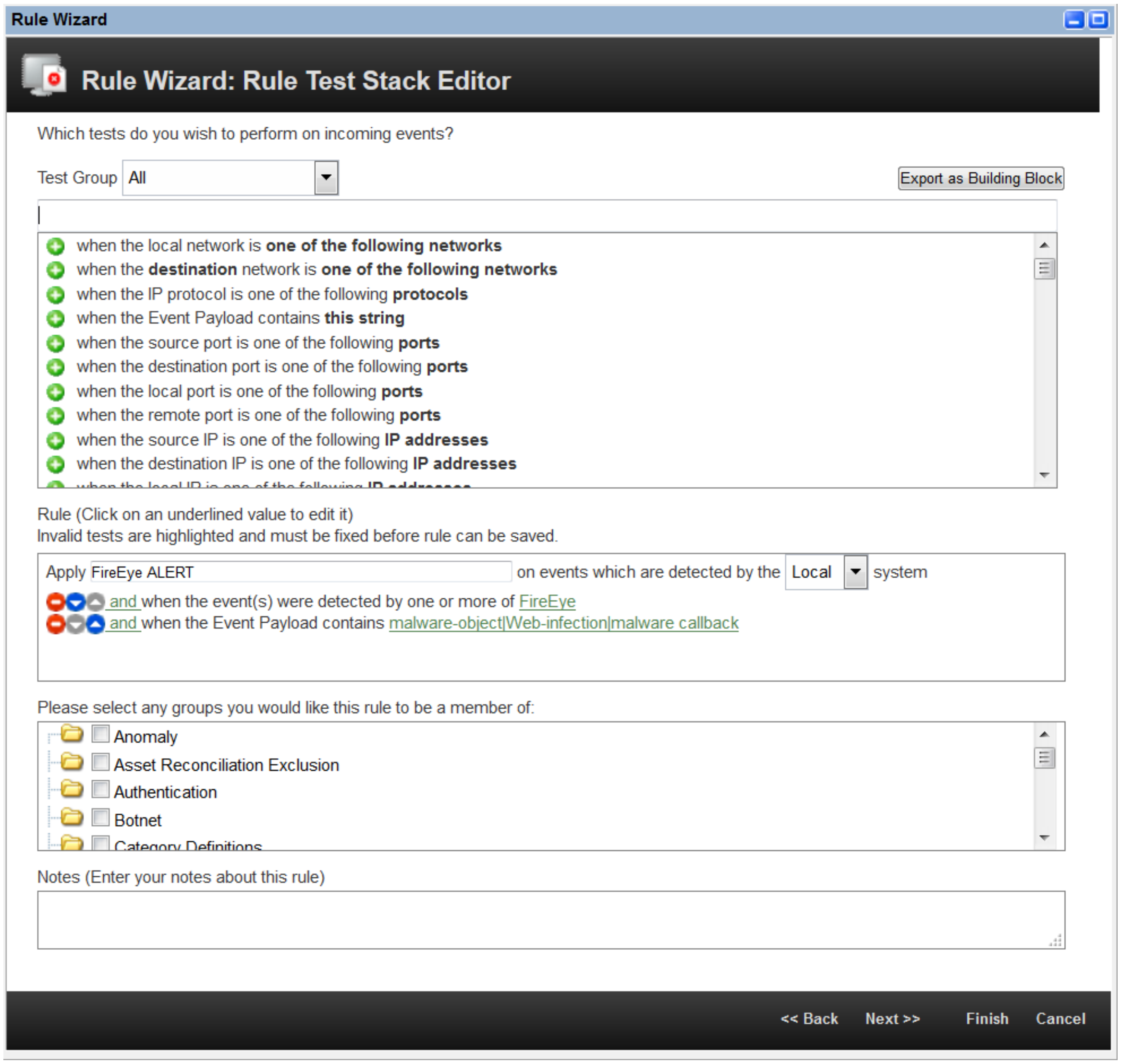
Log Source Name	FireEye
Log Source Description	FireEye EX
Log Source Type	FireEye
Protocol Configuration	Syslog
Log Source Identifier	155.109.
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: go-hfp-1
Coalescing Events	☑
Incoming Payload Encoding	UTF-8
Store Event Payload	☑
Log Source Extension	Select an Extension...
Extension Use Condition	Parsing Enhancement

Please select any groups you would like this log source to be a member of:

- □ Big_IPs
- □ Bulk Imported Log Sources
  - □ Cisco Log Source
  - □ Windows Desktop
- □ ECAT

Figure 22. Establishing FireEye Log Source in QRadar.

Monitoring rule. Custom rules are developed in QRadar under rules tab. Rules are built on pre-determined procedures and logic. We have FireEye sending events to QRadar but not all events are required to monitor unless there is an impact. To mitigate the false positives as well as non-critical events a rule is developed to monitor the events which contain web-infections, malware-object, and malware-callback. Once QRadar sees any event matching these conditions an alert in the form of an email is sent to the owner of the system or concern foreseeing and an offense is created in the offenses tab for tracking and investigation purposes.



Which tests do you wish to perform on incoming events?

Test Group All

when the local network is **one of the following networks**
when the **destination** network is **one of the following networks**
when the IP protocol is one of the following **protocols**
when the Event Payload contains **this string**
when the source port is one of the following **ports**
when the destination port is one of the following **ports**
when the local port is one of the following **ports**
when the remote port is one of the following **ports**
when the source IP is one of the following **IP addresses**
when the destination IP is one of the following **IP addresses**
when the local IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

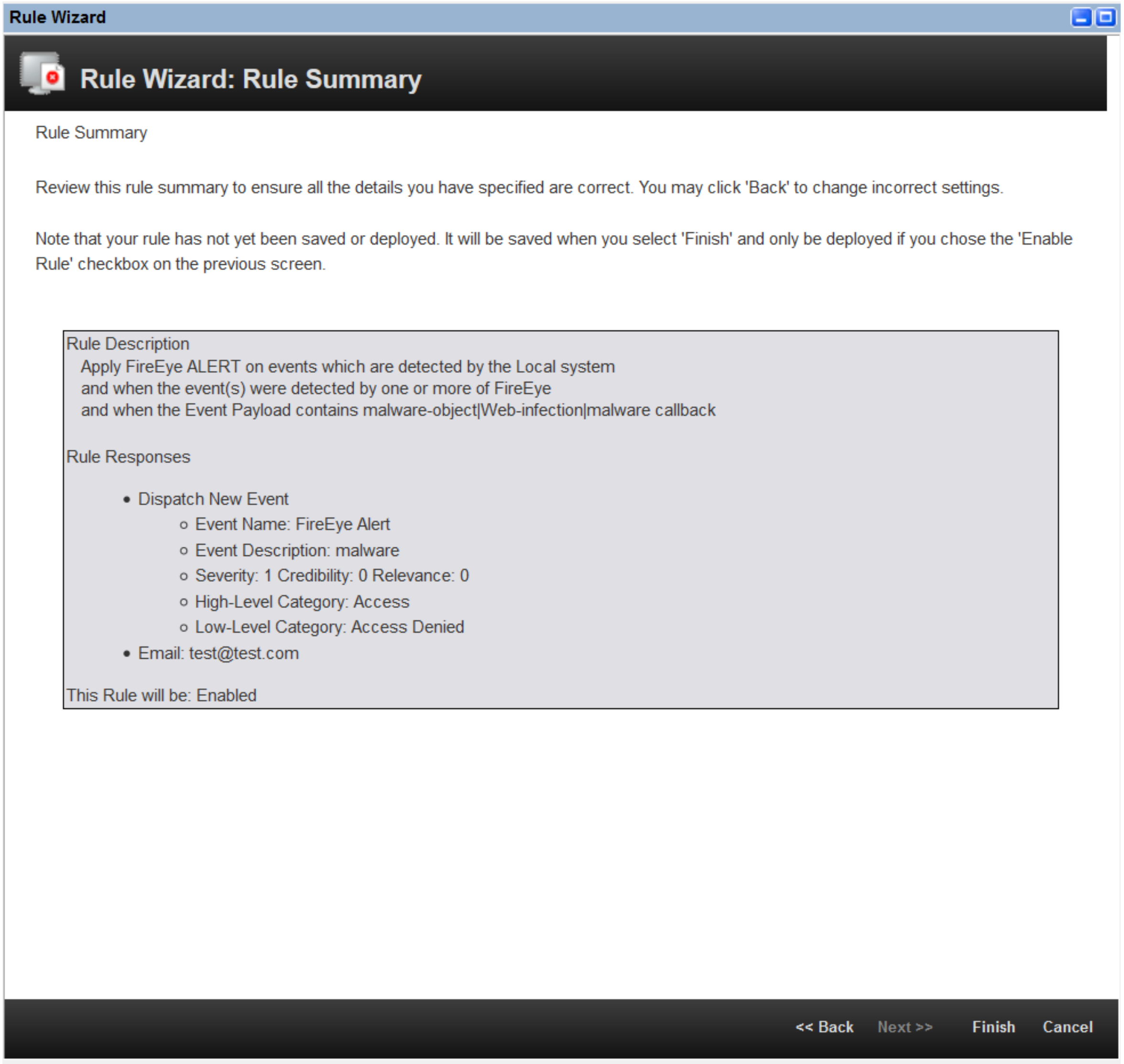
Apply FireEye ALERT on events which are detected by the Local system
and when the event(s) were detected by one or more of FireEye
and when the Event Payload contains malware-object|Web-infection|malware callback

Please select any groups you would like this rule to be a member of:

□ Anomaly
□ Asset Reconciliation Exclusion
□ Authentication
□ Botnet
□ Category Definitions

Notes (Enter your notes about this rule)

Figure 23. Developing FireEye Monitoring Rule in QRadar.



Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description
Apply FireEye ALERT on events which are detected by the Local system
and when the event(s) were detected by one or more of FireEye
and when the Event Payload contains malware-object|Web-infection|malware callback

Rule Responses

- Dispatch New Event
  - Event Name: FireEye Alert
  - Event Description: malware
  - Severity: 1 Credibility: 0 Relevance: 0
  - High-Level Category: Access
  - Low-Level Category: Access Denied
- Email: test@test.com

This Rule will be: Enabled

Figure 24. Summary of the Developed Rule for Monitoring FireEye Events in QRadar SIEM.

Boundary defense. This critical control detects, prevents, monitor and report on key status, configuration changes, violations/attacks and anomalous activity associated with perimeter defenses. The boundary defenses include firewalls, routers, VPNs and other means of network-based access controls. This research paper concentrates on firewalls devices logs to get them to QRadar. Firewalls filter acceptable inbound and outbound connections, in terms of allowing or denying communications based on rules. These rules are different from the QRadar rules.

- Steps 1 and 2: Network device management system validates configurations on Network devices and initiates to the alerting system.
- Steps 3 and 4: Two-factor Authentication system required for remote access to the network and the authentication system validates, checks and initiates to the alerting system.
- Steps 5 and 6: Configuration enforcement system checks and validates the proper configuration of network devices and initiates to the alerting system.
- Steps 7 and 8: Network monitoring system analyzes network traffic and sends events to the reporting system.
- Step 9: Outbound traffic passes through and is examined by network proxy devices and initiates to the alerting system.

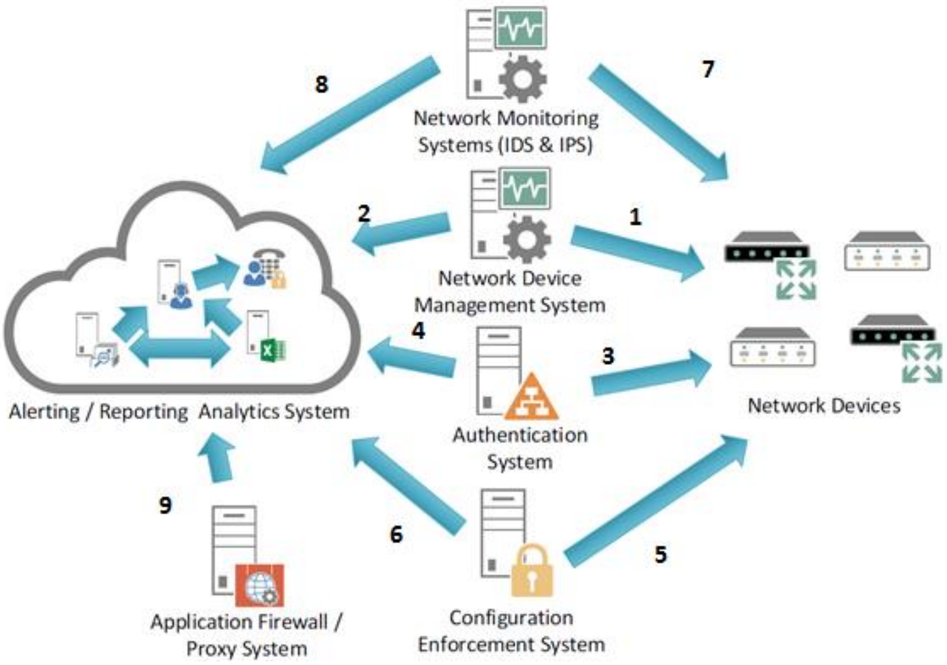
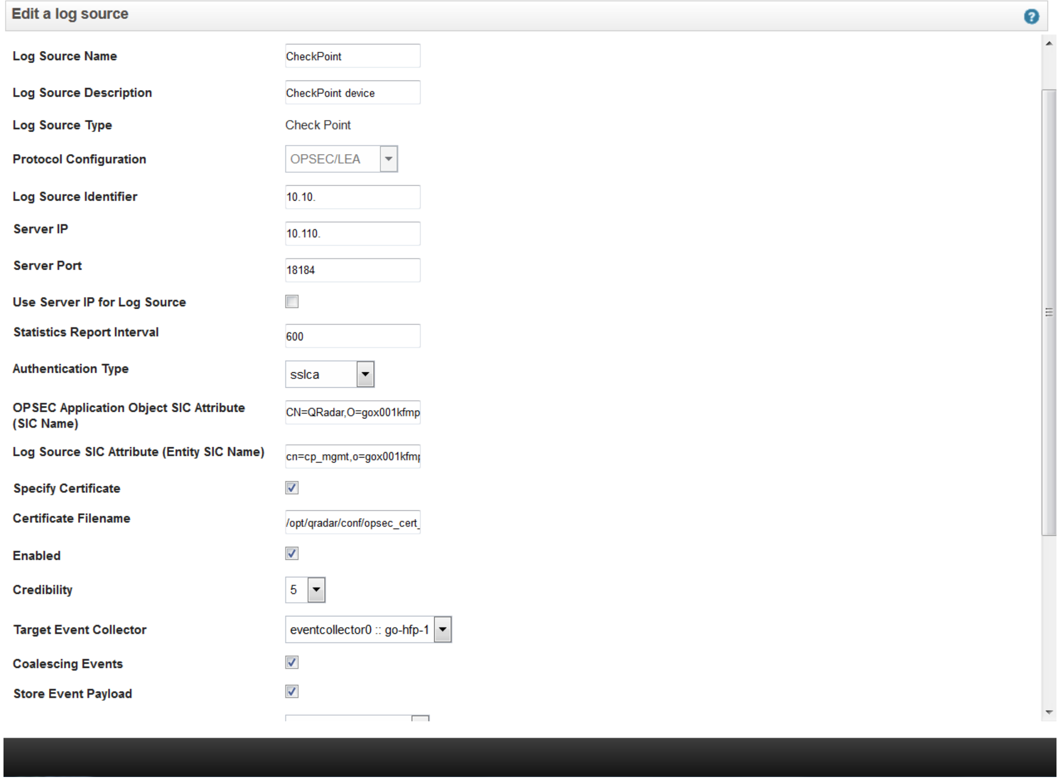

8
7
Network Monitoring Systems (IDS & IPS)
2
1
Network Device Management System
4
3
Authentication System
Alerting / Reporting Analytics System
Network Devices
9
6
5
Application Firewall / Proxy System
Configuration Enforcement System

Figure 25. System Entity Relationship Diagram of Boundary Defenses.

SIEM can be used to monitor the access activity from various boundary defenses. QRadar can serve as a centralized point to capture boundary state, changes and issues.

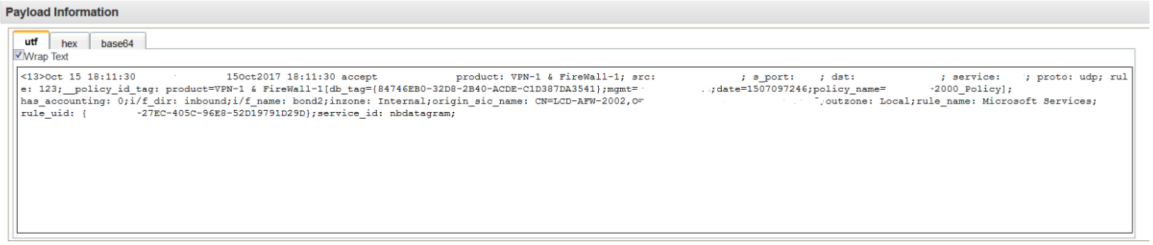
Check point firewall logs into QRadar. Unlike the FireEye implementation, Firewalls or Checkpoint devices event logs are brought into QRadar by just creating the log sources and QRadar has inbuilt event collector capabilities to check for that log source and grab the data.



Edit a log source

Log Source Name	CheckPoint
Log Source Description	CheckPoint device
Log Source Type	Check Point
Protocol Configuration	OPSEC/LEA
Log Source Identifier	10.10.
Server IP	10.110.
Server Port	18184
Use Server IP for Log Source	□
Statistics Report Interval	600
Authentication Type	sslca
OPSEC Application Object SIC Attribute (SIC Name)	CN=QRadar,O=gox001kfmp
Log Source SIC Attribute (Entity SIC Name)	cn=cp_mgmt,o=gox001kfmj
Specify Certificate	☑
Certificate Filename	/opt/qradar/conf/opsec_cert_
Enabled	☑
Credibility	5
Target Event Collector	eventcollector0 :: go-hfp-1
Coalescing Events	☑
Store Event Payload	☑

Figure 26. Establishing Firewall Log Source in Log Sources Tab in QRadar SIEM.

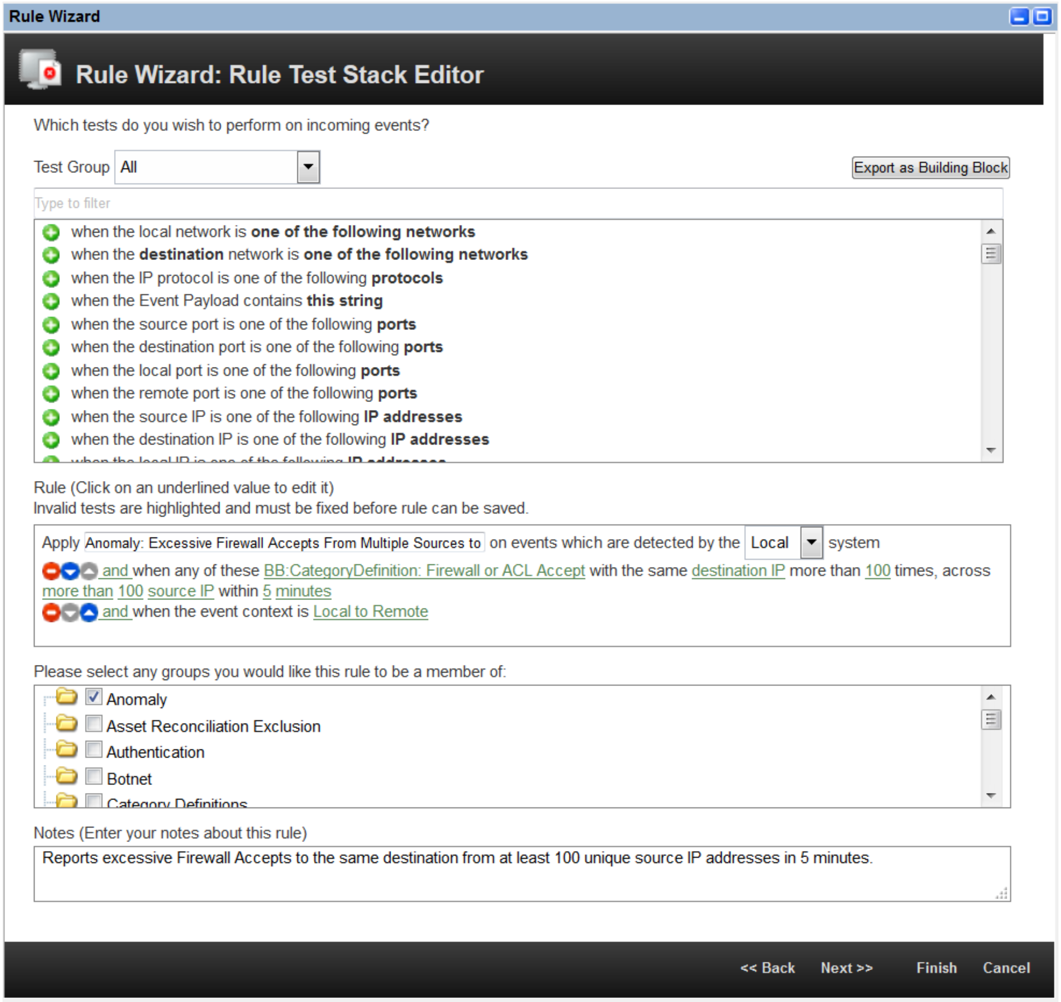


Payload Information

☑ Wrap Text

```
<13>Oct 15 18:11:30                15Oct2017 18:11:30 accept            product: VPN-1 & FireWall-1; src:                ; s_port:    ; dst:              ; service:    ; proto: udp; rul
e: 123;__policy_id_tag: product=VPN-1 & FireWall-1[db_tag={84746EB0-32D8-2B40-ACDE-C1D387DA3541};mgmt=            .;date=1507097246;policy_name=       -2000_Policy];
has_accounting: 0;i/f_dir: inbound;i/f_name: bond2;inzone: Internal;origin_sic_name: CN=LCD-AFW-2002,O=                    ,outzone: Local;rule_name: Microsoft Services;
rule_uid: {         -27EC-405C-96E8-52D19791D29D};service_id: nbdatagram;
```

Figure 27. Sample Event Payload from Firewall Log Source to QRadar.



Rule Wizard: Rule Test Stack Editor

Which tests do you wish to perform on incoming events?

Test Group: All

- when the local network is **one of the following networks**
- when the **destination** network is **one of the following networks**
- when the IP protocol is one of the following **protocols**
- when the Event Payload contains **this string**
- when the source port is one of the following **ports**
- when the destination port is one of the following **ports**
- when the local port is one of the following **ports**
- when the remote port is one of the following **ports**
- when the source IP is one of the following **IP addresses**
- when the destination IP is one of the following **IP addresses**
- when the local IP is one of the following **IP addresses**

Rule (Click on an underlined value to edit it)
Invalid tests are highlighted and must be fixed before rule can be saved.

Apply Anomaly: Excessive Firewall Accepts From Multiple Sources to on events which are detected by the Local system
and when any of these BB:CategoryDefinition: Firewall or ACL Accept with the same destination IP more than 100 times, across more than 100 source IP within 5 minutes
and when the event context is Local to Remote

Please select any groups you would like this rule to be a member of:

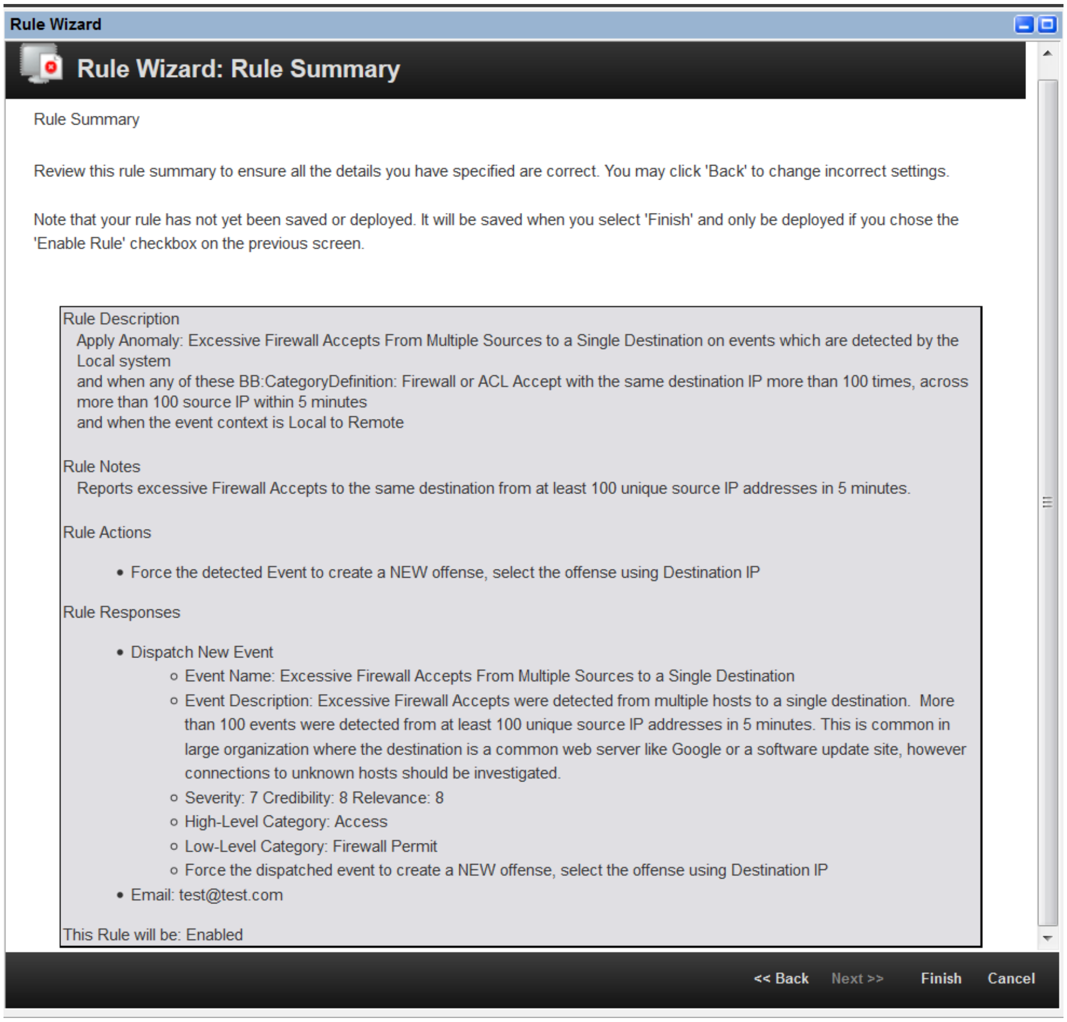
- ☑ Anomaly
- ☐ Asset Reconciliation Exclusion
- ☐ Authentication
- ☐ Botnet
- ☐ Category Definitions

Notes (Enter your notes about this rule)

Reports excessive Firewall Accepts to the same destination from at least 100 unique source IP addresses in 5 minutes.

Figure 28. Developing Monitoring Rule for Firewall Event Logs in QRadar.

Monitoring. Excessive firewall accepts from multiple sources to single location triggers suspicious activity for a possible compromise. The rule is developed with building block firewall accepts with same destination IP for more than 100 times across more than 100 source IP in 5 minutes and event context being local to remote. This correlation logic triggers an offense and alerts via an email to the Analyst. Refer Figure 28 above.



Rule Summary

Review this rule summary to ensure all the details you have specified are correct. You may click 'Back' to change incorrect settings.

Note that your rule has not yet been saved or deployed. It will be saved when you select 'Finish' and only be deployed if you chose the 'Enable Rule' checkbox on the previous screen.

Rule Description
Apply Anomaly: Excessive Firewall Accepts From Multiple Sources to a Single Destination on events which are detected by the Local system
and when any of these BB:CategoryDefinition: Firewall or ACL Accept with the same destination IP more than 100 times, across more than 100 source IP within 5 minutes
and when the event context is Local to Remote

Rule Notes
Reports excessive Firewall Accepts to the same destination from at least 100 unique source IP addresses in 5 minutes.

Rule Actions

- Force the detected Event to create a NEW offense, select the offense using Destination IP

Rule Responses

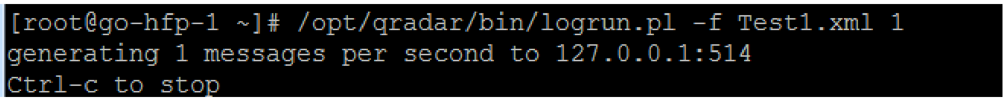
- Dispatch New Event
  - Event Name: Excessive Firewall Accepts From Multiple Sources to a Single Destination
  - Event Description: Excessive Firewall Accepts were detected from multiple hosts to a single destination. More than 100 events were detected from at least 100 unique source IP addresses in 5 minutes. This is common in large organization where the destination is a common web server like Google or a software update site, however connections to unknown hosts should be investigated.
  - Severity: 7 Credibility: 8 Relevance: 8
  - High-Level Category: Access
  - Low-Level Category: Firewall Permit
  - Force the dispatched event to create a NEW offense, select the offense using Destination IP
- Email: test@test.com

This Rule will be: Enabled

Figure 29. Summary of Developed Rule for Monitoring Firewall events in QRadar SIEM.

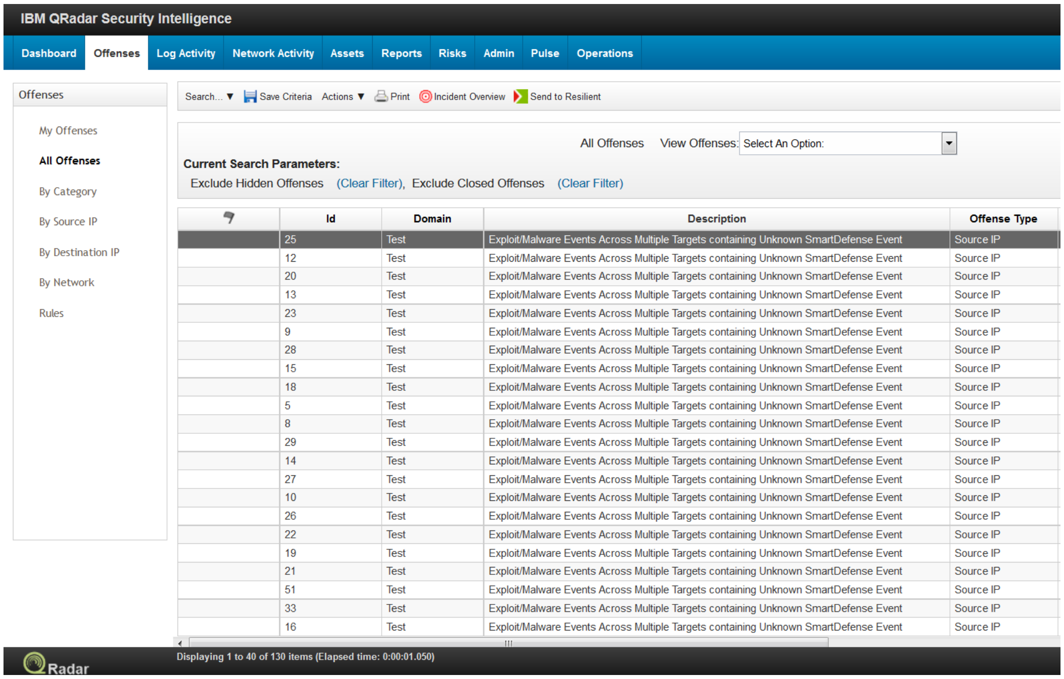
Rule Testing

A sample payload is used to test the rule to create an offense and send an email using log run command through the command line of QRadar as it runs on Red Hat Linux OS. Sample payload is loaded in an XML file and stored in the root folder. Using the command /opt/radar/bin/logrun.pl -f test1.xml 1 the event is generated in QRadar.



```
[root@go-hfp-1 ~]# /opt/qradar/bin/logrun.pl -f Test1.xml 1
generating 1 messages per second to 127.0.0.1:514
Ctrl-c to stop
```

Figure 30. Command to Generate Sample Events in QRadar SIEM for Testing.

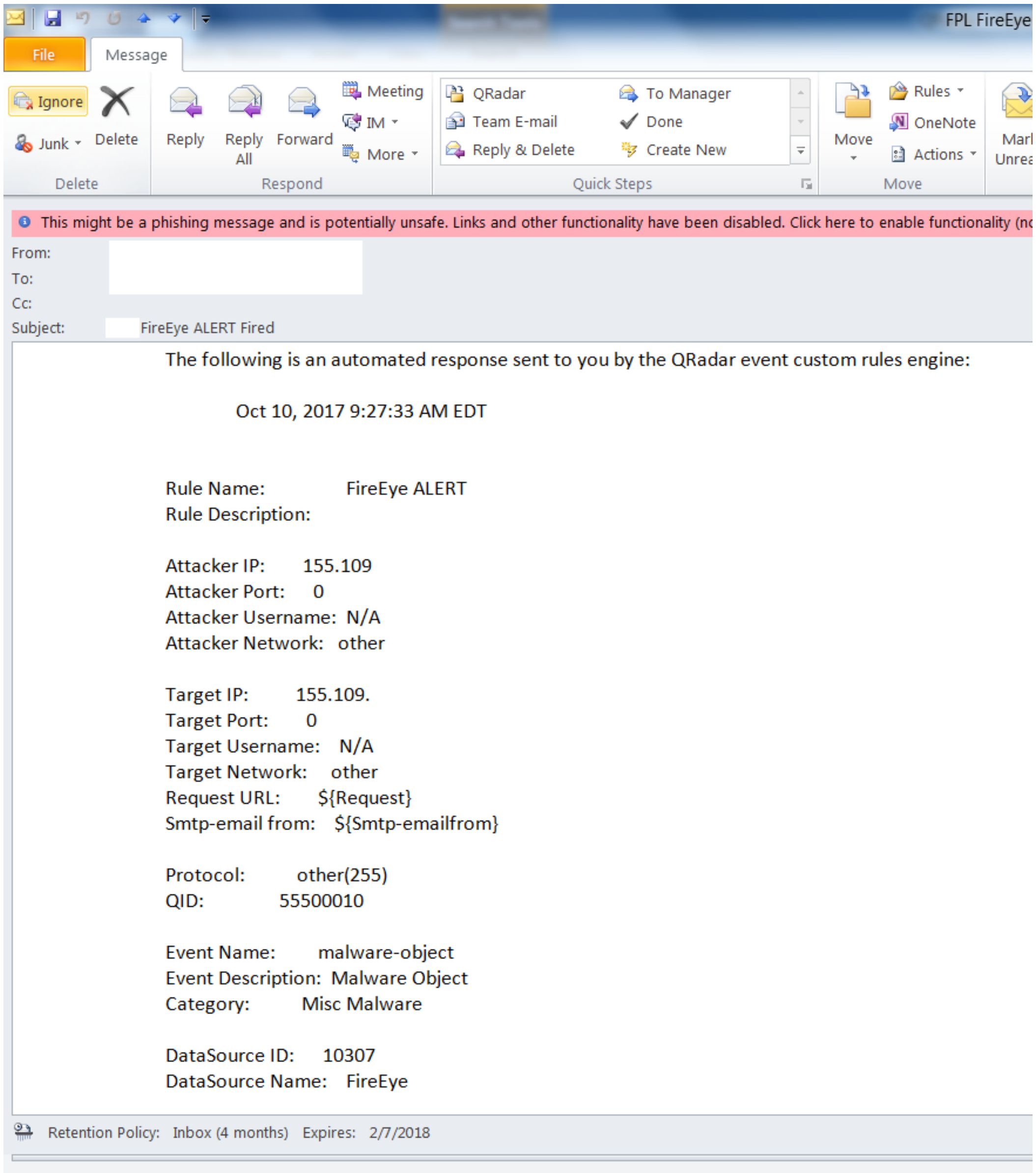


Current Search Parameters:
Exclude Hidden Offenses (Clear Filter), Exclude Closed Offenses (Clear Filter)

	Id	Domain	Description	Offense Type
	25	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	12	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	20	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	13	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	23	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	9	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	28	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	15	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	18	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	5	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	8	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	29	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	14	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	27	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	10	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	26	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	22	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	19	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	21	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	51	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	33	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP
	16	Test	Exploit/Malware Events Across Multiple Targets containing Unknown SmartDefense Event	Source IP

Displaying 1 to 40 of 130 items (Elapsed time: 0:00:01.050)

Figure 31. Testing: Offenses Created from Generating Sample Event.



This might be a phishing message and is potentially unsafe. Links and other functionality have been disabled. Click here to enable functionality (no

From: [redacted]
To:
Cc:
Subject: [redacted] FireEye ALERT Fired

The following is an automated response sent to you by the QRadar event custom rules engine:

Oct 10, 2017 9:27:33 AM EDT

Rule Name: FireEye ALERT
Rule Description:

Attacker IP: 155.109
Attacker Port: 0
Attacker Username: N/A
Attacker Network: other

Target IP: 155.109.
Target Port: 0
Target Username: N/A
Target Network: other
Request URL: ${Request}
Smtp-email from: ${Smtp-emailfrom}

Protocol: other(255)
QID: 55500010

Event Name: malware-object
Event Description: Malware Object
Category: Misc Malware

DataSource ID: 10307
DataSource Name: FireEye

Retention Policy: Inbox (4 months) Expires: 2/7/2018

Figure 32. Testing: Email Received from QRadar to Alert on Suspicious Activity Triggered by the Custom Rule.

Results and Summary

The existing risk position is analyzed by CIS 20 controls and their sub-controls on organization’s IT environment. Risk level is determined based on the score from the sum of all the sub-controls implemented to the total number of sub-controls. Also, two critical security controls are chosen and implemented accordingly for having visibility of malware activities as well as firewall event logs. Established rule are also tested using log run command.

Chapter V: Conclusions and Future Work

Conclusion

A thorough risk analysis is the foundation of a good security plan and helps the measure that will take to reduce or control risk. Risk assessment is done on basis of likelihood of the threat occurring and assigned high, medium and low probabilities. The result is a clear picture of the actual, quantifiable risks to the system. With the increase in viruses, worms and identity theft implementing security controls is no longer an option, organizations are finding themselves to implement security with minimum cost, by following this process outlined in this study, businesses can enhance the security of their systems and data. But the level of detail required will differ from organization to organization and basis on their risk levels. Implementing and monitoring integrations of QRadar with an anti-virus (FireEye) and a Firewall are essential components of information security.

Future Work

Currently, FireEye deployed on all endpoints would be running and checks for malware based on the signature patterns and send the event data to QRadar. Once the QRadar receives the event and matches the rule an alert is generated to the Analyst to start the remediation process like removing the system from the network and quarantine the malware. This is a reactive process and takes a significant amount of time which also increases the mean time to detect and contain the malware.

This process can be automated by adding an additional orchestration tool which is available in the market. The tool integrates with QRadar, FireEye and the endpoint systems using API (Application program interface). QRadar forwards the offenses to the orchestration tool with an ID like the ID generated by FireEye to identify the infected system. The orchestration tool interfaces QRadar offense and FireEye ID and removes the system from the network. This requires python script to automate the process. The orchestration tool also looks for the malware signatures over the web using Virus total and utilizes domain lookups for identifying the infected system. Meantime to detect and contain the malware significantly reduces with this approach. To implement this work, huge investment is required for a dedicated python developer and orchestration tool.

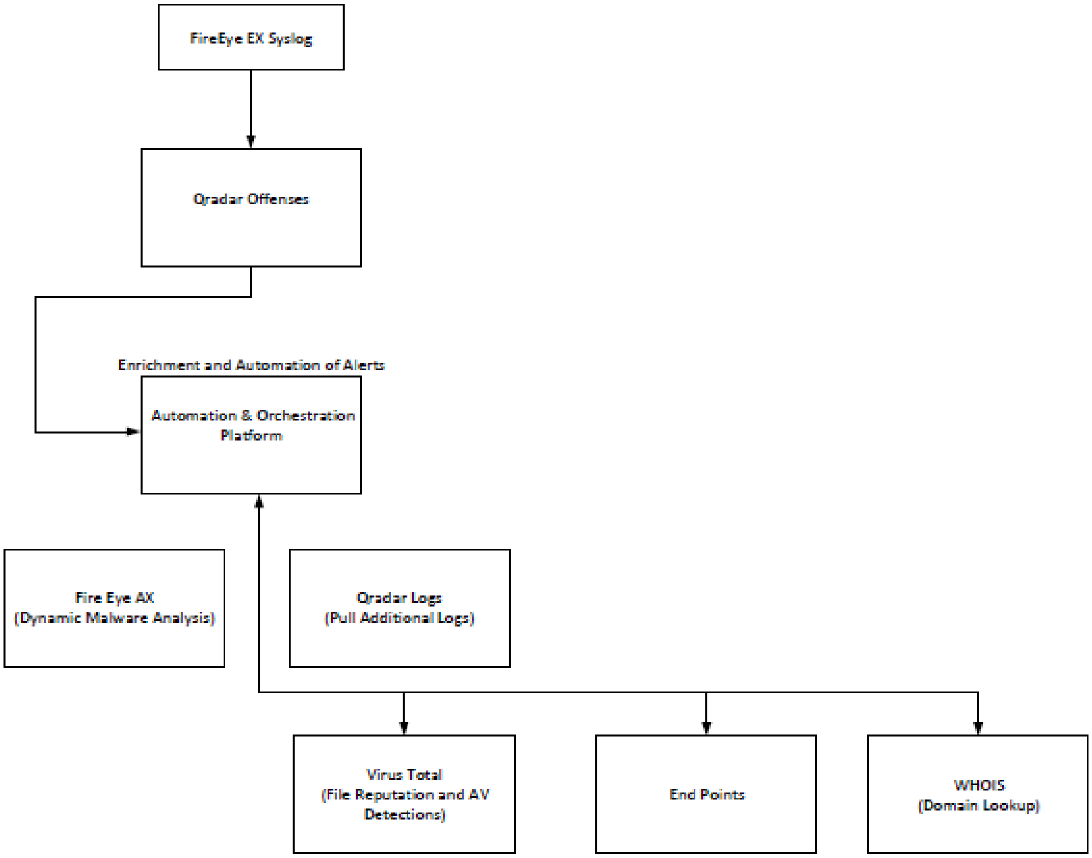

FireEye EX Syslog
Qradar Offenses
Enrichment and Automation of Alerts
Automation & Orchestration Platform
Fire Eye AX (Dynamic Malware Analysis)
Qradar Logs (Pull Additional Logs)
Virus Total (File Reputation and AV Detections)
End Points
WHOIS (Domain Lookup)

Figure 33. Flow Diagram of Proposed Future Work (Automation).

References

Armstrong, D., Carter, S., Frazier, G., & Frazier, T. (2004). Autonomic defense: Thwarting automated attacks via real-time feedback control. *Complexity, 9*(2), 41-48.

Beauregard. J. E. (2001). *Modeling information assurance* (Master's thesis). Air Force Institute of Technology, Ohio.

Berger, B. (2003). *Data-centric quantitative computer security risk assessment*. Retrieved from http://www.sans.org/rr/papers/index.php?id=1209

Bragg, R. (2003). *CISSP: Certified information systems security professional training guide*. Indianapolis, IN: Que Publishing.

Brown, J. S., & Duguid, P. (2002). *The social life of information*. Boston, MA: Harvard Business School Press.

Cahill, T. P. (2003). *Cyber warfare peacekeeping*. Paper presented at the 2003 IEEE Workshop on Information Assurance.

Canavan, S. (2003). *An information security policy development guide for large companie*s. Bethesda, MD: SANS Institute.

Cisco. (2016). *Annual security report*. Retrieved from http://unleashingit.com/docs/C15/Cisco_Annual_Security_Report_2016.pdf

Gollmann, D. (1999). *Computer security*. New York, NY. John Wiley & Sons Ltd.

Hamill, J. T., Deckro, R. F., & Kloeber, J. M. Jr. (2005). Evaluating information assurance strategies. Decis*ion Support Systems, 39,* 463-484.

Henauer, M. (2003). *Early warning and information sharing*. Paper presented at the Workshop on Cyber Security and Contingency Planning: Threats and Infrastructure Protection, Zurich, Switzerland.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations. *Decision Support Systems*, *47*, 154-165.

Howard, M. (1979). The forgotten dimensions of strategy. *Foreign Affairs, 57*(5), 975-986

International Organization for Standardization. (2015). *ISO/IEC 15504 Information technology: Process assessment standard*. Retrieved from https://www.iso.org/standard/38932.html

Lampson, B. W. (2004). Computer security in the real world. *Computer, 37*(6), 37-46.

Liu, S., Sullivan, J., & Ormaner, J. (2001). A practical approach to enterprise it security. *IEEE IT Professional*, *3*(5), 35-42.

McDermott, J. P. (2000). *Attack net penetration testing*. Paper presented at the 2000 Workshop on New Security Paradigms, Ballycotton, County Cork, Ireland.

Mercer, A. (2013). *Security information and event management for small and medium-sized enterprises* (Master thesis). Lulea University of Technology, Department of Computer Science.

National Institute of Standards and Technology. (2013). *NIST special publication 800-53* (Rev. 4). Washington, DC: U. S. Department of Commerce.

Pfleeger, C. P. (1997). *Security in computing* (2nd ed.). Upper Saddle River, NJ: Prentice Hall.

Ponemon Institute LLC. (2015). *2014: A year of mega breaches*. Retrieved from http://www.ponemon.org/local/upload/file/2014%20The%20Year%20of%20the%20Mega%20Breach%20FINAL_3.pdf

Riffat, M. (2015). *Risk management: Principles and guidelines*. Canberra, Australia: Australian Government.

SANS Institute. (n.d.). *About SANS*. Retrieved from https://www.sans.org/about/

SANS Institute. (2017). *SANS glossary of terms used in security and intrusion detection.* Retrieved from http://www.sans.org/resources/glossary.php

Sebastiaan, H., Solms, V., & Eloff, J. (2003). *Information security*. Leyland, Lancashire: B & D Printers.

Stolfo, S. J. (2004). Worm and attack early warning: Piercing stealthy reconnaissance. *IEEE Security and Privacy, 2*(3), 73-77.

Symantec. (2016). *Symantec internet security threat report* (Vol. 21). Retrieved from http://www.symantec.com/threatreport/

Symantec. (2017). *Symantec internet security threat report, Ransomware 2017*. Retrieved from https://www.symantec.com/content/dam/symantec/docs/security-center/white-papers/istr-ransomware-2017-en.pdf

Tirenin, W, & Faatz, D. (1999). *A concept for strategic cyber defense*. Paper presented at the Military Communications Conference (MILCOM) '99.

Trend Micro. (2016). *Addressing the SANS TOP 20 critical security controls for effective cyber defense*. Trend Micro Whitepaper. Retrieved from https://resources.trendmicro.com/rs/945-CXD-062/images/sans_top20_csc_trendmicro2016.pdf

Tryfonas, T., Kiountouzis, E., & Poulymenakou A. (2001). Embedding security practices in contemporary information systems development approaches. *Information Management and Computer Security, 9*(4), 183-197.

Varney, C. A. (1996). *Consumer privacy in the information age: A view from the United States*. Washington, DC: Remarks before the Privacy and American Business National Conference.

Vijayan, J. (2014). *In a rare move, banks sue Target's security auditor*. Retrieved from http://www.computerworld.com/article/2489063/datasecurity/in-rare-move--banks-sue-target-s-security-auditor.html

Visintine, V. (2003). *An introduction to information risk assessment*. Retrieved from http://www.sans.org/rr/papers/index.php?id=1204

Whitman, M., & Mattord, H. (2005). *Principles of information security* (2nd ed.). Boston, MA: Course Technology

Wysocki, R. K. (2004). *Project management process improvement*. Norwood: Artech House, Inc.

Appendices

Appendix A: Questionnaire/Template

Questionnaire/template used for each sub-control

Do we do this?	If so, how	If not, why?	Can this be automated?	Notes

Implementation Level Score	Maturity of IT to Implement this Control	Current Risk to J&B

Appendix B: Research on SIEMS

Research on available SIEMs, their capabilities and Licenses

SIEM	**REPORTING CAPABILITIES**	**LINCESING & PRICING**
Hewlett-Packard Enterprise's Arc Sight ESM	"Most SIEM products offer robust reporting capabilities, and HPE's ArcSight ESM is no exception. It offers built-in support for many security compliance initiatives, including the following: •Federal Information Security Management Act of 2014 •Health Insurance Portability and Accountability Act •International Organization for Standardization/International Electrotechnical Commission 27001/27002, Information Security Management •North American Electric Reliability Corporation Critical Infrastructure Protection •Payment Card Industry Data Security Standard •Sarbanes-Oxley Act"	Although HPE provides a link to a 30-day free trial of HPE's ArcSight ESM, following the link actually leads to a free trial of HPE's ArcSight Application View, also known as App View. A free trial of the HPE ArcSight ESM product itself could not be located, and additional licensing information was also unavailable.
EMC RSA Security Analytics	"An important feature provided by most SIEM products is extensive reporting capabilities. EMC RSA Security Analytics comes with nearly 100 reporting templates that provide built-in support for many security compliance initiatives, including the following: •Federal Information Security Management Act of 2014 •Gramm-Leach-Bliley Act •Health Insurance Portability and Accountability Act •International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 27001/27002, Information Security Management •North American Electric Reliability Corporation Critical Infrastructure Protection •Payment Card Industry Data Security Standard •Sarbanes-Oxley Act "	Due to the modularity and complexity of the EMC RSA Security Analytics offerings, it is beyond the scope of this article to provide detailed information on component licensing and pricing. Organizations interested in seeing component options and their pricing should visit the EMC store
Alien Vault OSSIM	AlienVault OSSIM doesn't have any built-in reporting support for compliance initiatives. It offers three reporting templates, but nothing specific to compliance reporting. By contrast, AlienVault USM offers over 150 customizable reports, including compliance reports for the Payment Card Industry Data Security Standard, HIPAA and SOX.	"AlienVault OSSIM is open source, so its latest version is available for free download here. A link to download the source code and documentation is also available from the same URL. AlienVault USM is a commercial product. A 30-day free trial is available for download here. Pricing information for AlienVault USM virtual appliances for small

		organizations is posted here, as is the cloud service hourly rate. AlienVault must be contacted directly for pricing on other AlienVault USM models. "
Splunk Enterprise	"According to Splunk documentation posted here, Splunk offers reporting capabilities for various security compliance initiatives, including the following: •Federal Information Security Management Act (FISMA) of 2014 •Gramm-Leach-Bliley Act •Health Insurance Portability and Accountability Act •International Organization for Standardization/International Electrotechnical Commission 27001/27002, Information Security Management •North American Electric Reliability Corporation Critical Infrastructure Protection •Payment Card Industry Data Security Standard •Sarbanes-Oxley Act At least some of these reporting capabilities are provided by specialized apps added onto Splunk Enterprise, such as the Splunk App for PCI Compliance and the Splunk App for FISMA Continuous Monitoring. "	A 60-day free trial of Splunk Enterprise is available here. The Splunk Enterprise software is available for various Windows, Linux, Solaris, Mac OS X, FreeBSD and AIX platforms. The free trial supports processing of up to 500 megabytes of log data each day. After the 60-day trial ends, an organization can change the deployment to use a free license, or the organization can purchase an enterprise license, which provides more functionality than the free license and also enables larger volumes of daily log data processing. See here for additional information on Splunk Enterprise licensing.
SolarWinds Log and Event Manager	"Robust built-in reporting capabilities are offered by SolarWinds SIEM product, including over 300 reporting templates. These templates address the requirements of many security compliance initiatives, including the following: •Federal Information Security Management Act of 2014 •Gramm-Leach-Bliley Act •Health Insurance Portability and Accountability Act •International Organization for Standardization/International Electrotechnical Commission 27001/27002, Information Security Management •North American Electric Reliability Corporation Critical Infrastructure Protection •Payment Card Industry Data Security Standard •Sarbanes-Oxley Act "	"Organizations can download a free 30-day trial of SolarWinds Log and Event Manager here. SolarWinds Log and Event Manager are licensed by the maximum number of nodes a model supports. See here for current pricing by model. "
IBM Security QRadar	IBM QRadar provides support for several major compliance reporting requirements initiatives such as the Health Insurance Portability and Accountability Act (HIPAA) and Payment Card Industry Data Security Standard (PCI DSS),	Because IBM QRadar SIEM is a modular product with multiple options per component, explaining its licensing and pricing in detail is outside the scope of this article, but the charge metric is generally

	Gramm-Leach-Bliley Act (GLBA), North American Electric Reliability Corporation (NERC) and Federal Energy Regulatory Commission (FERC), Sarbanes–Oxley (SOX) and more. The product also offers a report builder wizard so security teams can create custom reports.	based on usage such as log source events per second and network flows per minute. Organizations interested in better understanding the options can get the latest pricing information for all the available IBM QRadar SIEM licenses. Free community version with100EPS license available.
Log Rhythm's Security Intelligence Platform	"The reporting capabilities offered by the Log Rhythm SIEM product are more extensive than any other major enterprise SIEM product, with built-in support for over 800 report formats. This built-in support includes reporting for many major security compliance initiatives, including: •Federal Information Security Management Act of 2014 •Gramm-Leach-Bliley Act •Health Insurance Portability and Accountability Act •International Organization for Standardization/International Electrotechnical Commission 27001/27002, Information Security Management •North American Electric Reliability Corporation Critical Infrastructure Protection •Payment Card Industry Data Security Standard •Sarbanes-Oxley Act "	Because the components of the platform are available in so many models and combinations, it is outside the scope of this article to explain the possible licensing and pricing arrangements.