Cyber Security Management – Technical Report

7808ICT

Gowtham Ravi

s5190712

Executive Summary

This report is a technical report which critically analyses different security systems.The report enumerates three possible solutions for each security system that are currently avaliable in the market and recommends one solution for deployement for the CIO. The report concludes with a priority list which prioritises each system in the order of implementation.

Table of Contents

Executive Summary

The Security system plays an integral part in protecting the information. There are various security systems used for different purposes in an organisation. The security systems such as Security Information and Event Management, Vulnerability Management, Endpoint Security and Network Security are researched, and solutions are provided in the paper.

Security Information and Event Management (SIEM)

SIM stands for Security Information Management, and SEM is abbreviated as Security Event Management which composes the security information and event management (SIEM). Though SIM deals with organisational administration, collection, preservation of historical log records, and report creation for compliance purposes, SEM includes risk control, real-time security incident detection, and inducing appropriate responses in the event of an incident. Therefore, the information collected is collated to minimise information volume and Enable the user to respond adequately to security breaches. However, SIEM has now developed from a simple implementation of these two technologies to a more comprehensive and interconnected security approach, integrating the benefits of SIM and SEM in one unified security implementation(Vielberth & Pernul, 2018).

SIEM systems collect essential information and carry out contemporary data analysis of security incidents from a wide range of different event types or subjective sources of information. It also facilitates regulatory monitoring and forensic analysis by reviewing the available information retrieved from the very same origins. SIEM 's significant features include its wide variety of incident sources and their ability to compare and examine these incidents covering diverse sources.

SIEM Tools

Splunk Enterprise Security
Splunk supports management of logs, analysis, and computational commands to promote the analysis and visualisation in real-time. The Splunk Software for Enterprise Security running on Splunk Enterprise provides standardised dashboards, searches, reports, and alerts to enable the use of cases for security monitoring and analysis.

IBM QRadar
IBM Monitoring QRadar can be executed as all-in-one approaches for smaller fields, or it tends to be progressively conveyed with cutting edge occasion assortment, handling and comfort machines in bigger situations. A unique feature of the software is the collection and processing of NetFlow data to provide behavioural analysis of the network and application, and behavioural analysis capabilities for all incidents gathered of any source.
IBM Security also provides an optional function, QRadar Risk Manager, that supplements event analysis with network and firewall configuration monitoring and configuration specific case.

SolarWinds Security Event Manager
SolarWinds Security Event Manager is a SIEM solution tool which supplements its functionality to current security tools and improves their performance in managing, administering and monitoring their network's security policies.
SEM offers forensic and troubleshooting access to the log data and tools that help you handle log data. SEM optimises the logs collected, analyses them in real-time and notifies you of an issue before causing any harm.
For instance, advanced persistent threats may come as a result of network events such as software installations, authentication incidents, and network traffic inbound and outbound. All data about these events are stored in log files. The SEM correlation engine detects advanced threat activities and tracks any anomalies to the company.

Recommendation:

From the above three solutions SolarWinds Security Event manager is recommended to the CIO. This tool apart from collecting logs also helps establish relatinoshoip between vital events, provides enhanced searching features and also enalbes automated actions on malicious threats. This SEM stands out as it has the capabilty to autotically detect malicious anomalies and patterns. SolarWinds is also recognised by Garter to be the best SIEM in the market.

Vulnerability Management

Vulnerability management is the process by which IT vulnerabilities are recognised, and these vulnerabilities threats are assessed. This identification contributes to the modification of threats and the elimination of risk or a systematic recognition of threat by an organisation's management. Vulnerability management is the process of scanning vulnerability, also taking into consideration other factors such as identifying risks and recovery.

Vulnerability Management Tools

Rapid7 – Nexpose
NeXpose is an active vulnerability scanner (i.e. it searches remote hosting for records) supportive of both authenticated and unauthenticated scanning. NeXpose presents data about the network structure, including all devices that communicate through TCP or UDP, such as computers, firewalls and printers. The scanner detects the operating systems or software running on the scanned devices, and any programmes running on them.
NeXpose has around 53,000 existing signatures in its system, with each signature referring to a specific vulnerability. NeXpose is also compatible with SCAP and therefore comply with a series of six widely used protocols published by the national institute of Standards and Technology(NIST): (i)XCCDF, (ii)OVAL, (iii)CPE, (iv)(CCE), (v) CVE and (vi) CVSS.

Nessus – Tenable
Nessus dictionary consists of more than 57,000 Common Vulnerabilities and Exposures(CVE) and also has the least false positive detection in the field. Nessus searches for identified exploits on both the software and hardware. It tracks systems running for suspicious activity and even measures trends of network traffic. Nessus is a type of antivirus/firewall platform but not wholly. Although providing mitigation protocols, it is not as robust as would be a traditional endpoint security system in the solutions segment.

OpenVAS

It is considered to be a complete vulnerability scanner including unauthenticated and authenticated testing, high-level and low-level internet protocols, setting performance for large-scale scans that enables this tool to perform all types of vulnerability test. It performs the following functions to perform the vulnerability test in a system.

- It is capable to detect RedHat backported package to avoid false-positive that is caused in all version of package.
- It provides a bug report and blocks the scanner on reaching maximum limit for overpassing database.
- It has library that provides details of protocols and enable communication between services.
- It has a greenbone-security assistant that is considered to be a web interface for launching scans.
- It enables the administrator to protect their server from malicious attacks.

Recommendation

Analysing all these vulnerability tools Nessus is the recommended tool for deploment. Nessus captures data with minimal impact on the network and ensuring high-performance at all times.

Nessus being an open source product has significantly low cost of ownership when compared to the other tools. Nessus is also compatible acroos diofferernt pa;tforms making it more scalable and usable. From specific vulnerability checks to more contral over the network Nessus offeres several advanced features.

EndPoint Security Analysis

Endpoint security is a robust group of software that is used to protect the devices from viruse, malware threats of both online and offline. It provides a great support in increasing the profit and digital safety in a business. It performs the activities of protecting the device against virus, diagnonising and treating the ailments, managing the IT infrastructure and the devices involved and most importantly it prevents data loss. This software provides a great support in blocking the cyber attacks through antivirus. The main purpose of this tool is to protect the data and the systems that supports the growth of business (O' Shaughnessy, 2017).

An endpoint is a device used by the end-user to facilitate the usage of any device connected to the internet and protect the device and data from virus and other malicious threats. It is considered as the replacement for antivirus systems used in business. It addresses the security issues faced by the end-user (Cooper, 2020). It emphasises more on internal threats but also provide protection to devices prone to all type of threats in order to prevent the employees from losing large volume of valuable data. In relation to the cyber attack being targeted to the low operating systems that was originally developed by the developers was already patched, which when neglected becomes highly vulnerable to threats. This was overcome with the endpoint protection central security management that notifies the administrator to patch all the updates instantly. It is an extended and advanced antivirus security software designed to prevent the system from all possible threats (O' Shaughnessy, 2017).

EndPoint Security Tools

Symantec Endpoint Detection and Response:
It is considered to be the most integrated endpoint security tool to deliver cloud-based protection supported by AI on a single console. It was first developed by Broadcom Inc with firewall features supporting server and desktop. It was first tested with the anti-spam in emails and when the end user open unauthorised links found on the web. This symantec endpoint detection and response was pinned as an extension to block access to unauthorised sites. It performs the following operations:

- Performs behavioural analytics to identify the suspicious activity and prioritise incidents.
- Hunts for anomalies and indicators across all endpoints in real-time increasing the incident responder productivity.
- Blacklist and whitelist files for deleting the malicious files impacted on end-users enabling quick fix and ensuring that the threats do no affect the system again.
- It integrates the data and actions into infrastructures like Splunk and ServiceNow and provides visibility to the end-users.

ESET Endpoint Security:
It is a complete security solution for a long-term effort to combine maximum protection from malware threats. It is primarily designed to use in small business. It manages the endpoint products incuding antivirus for Linux. This tool had enhanced device control feature with high granularity to address threats from viruses, trojans, keyloggers, adware, spyware and rootkits. It performs the following authorisations to protect the systems from malicious threats (Schaffhauser, 2012):

- It run automatically without administrator support or user intervention and provides access only upon the request from administrator with specification to the tasks that requires access.
- It runs in the background and observes the working of the system enabling the administrator to review and modify the policies and rules.
- It filters certain function limiting the web access and allowing the security administrator to define policies for 140 categories complying to company policies.
- It adopts a firewall feature mainly focussing on the users who use portable desktops.

- It provides an anti-spam feature which improved the usability and spam detection.

Malwarebytes Endpoint Protection:

It is a security solution developed for protecting against zero-hour threats, threat detection and remediation of endpoints. It scans and blocks all the detected malicious websites and malware threats exploiting unknown vulnerabilities on systems. This tool is suitable for both desktop and portable systems working both online and offline and supports all windows server operating systems. The stages of protection in every attack is describes as follows (Calif, 2018):

- It performs continuous monitoring and visibility to get powerful insight. It tracks the activity of files stored on local drive and cloud providing extra safety.
- It provides multi-layered protection using a seven layered approach including statis and dynamic detection techniques to protect against all types of threats ranging from tradition to advanced threats.
- It uses a linking engine to provide a complete remediation and minimise the impact on the end-user. It uses a rollback technology negating the impact of ransomware due to the infection caused during the backup process.
- It offers three ways to isolate the endpoint inorder to restrict the intereaction between the process user, network and the desktop to limit damage and lock the attackers remotely.

Recommendation:

After critically anlysis all tools, the symantec endpoint detection and response tool is recommended to prevent the system from malicious threats. On comparing the usage of each tool it is evident that the symantec tool was highly preferred in businesses. It has alerting capablity, tracking of AI and behavioural analytic threat across the different end users.

It is considered to be the top security among the other third party security tests with ease of usage and high value as it uses advanced features. It has the ability to handle advanced malware attack. It is capable to track malicious threat across different networks including cloud. It is considred to have a rich and high effcicient features to provide strong security. It involves standard features and configuration management. It is evident that Symantec has a well integrated EPP and EDR with good automation features and time saving response which enable symantec endpoint detection and response tool to be highly recommended for securing the data and the systems from any kind of possible malicious threats in an organisation.

Network Security

With the advancements in technology and development of complex networks, network security has become vital for organisations. The advent of internet has raised several security concerns and has created new ways of vulnerability and threats for a network. The necessity of a secure network has become the need of the hour for all organisations.

The design of a network is a well-developed and organised process with OSI (Open Systems Interface) model being the base for the development (Daya, 2008).

Network security offers:

Computer protection: A network involves several devices connected with one another thereby making them highly vulnerable. An unsecure network is prone to several threats from malwares, ransomware and other viruses. To avoid such expensive threats, a network must be highly secure. An attack on a single device connected to a network can have a significant impact on the entire network affecting all connected devices.

Identity theft prevention: The identity information of every individual is highly valuable and confidential. An individual logging into an unsecure network poses a risk to the individual's identity information and revealing the information to untrusted third-parties. Network security is very much essential to avoid such situations.

Protection of shared data: Every organisation must ensure that its shared data is protected by incorporating security measures and policies. This can be achieved by the application of network security with different access levels for different computer devices.

Network connection stabilisation: Stabilisation of network is essential for a network as intense network traffic makes the network unstable and vulnerable to external attacks.

Network Security Tools:

Firewall:

A firewall is a network security device which acts as a gateway to allow or blow specific traffic into the network. It monitors the incoming traffic and outgoing traffic and is operated based on a set of security rules that can be set by the network administrator. Firewall serves as a barricade and a frontline defence to restrict access from one network to the other network (Blansit, 2009).

This is achieved through several techniques such as packet filtering, stateful firewall and application layer firewall. Firewall can be implemented either ways as a software or a hardware (Imran, Ahmad & A. Alghamdi, 2015).

- Packet filtering firewall inspects individual packets in isolation and allows/disallows data based on individual packet headers.
- Stateful firewall monitor data packets and help determine their connection state thereby making them more flexible than packet filtering firewalls. Similar packets are collected together until the state of the connection is determined and firewall rules are applied to the traffic.
- Application firewall analyses the transmitted data and compares the data to the given firewall rules. This firewall is also referred to as proxy-based firewall.

Intrusion Detection System

An intrusion detection system (IDS) is used to identify and determine an attack on the network. The IDS's help to determine anomalies in a network and stop any network outage. There are two types of IDS, host-based and network based. Network based IDS is built on a network whereas a host based is built on the user's computer (Innella, 2001).

The working of IDS is categorised into Pattern matching and statistical anomaly.

Pattern Matching
The IDS works by analysing the network and comparing it to signatures of known attacks/ threats. If the system identifies any that matches to a threat, then the IDS alerts the network administrator. This monitoring takes place in the protocol and application layer. The signature database must be kept updated frequently to boost the effectiveness of the system.

Statistical Anomaly
This anomaly-based detection compares the network traffic and identifies if there is any deviation to the normal usage patterns. Any new network behaviour is picked out by the system and flagged to the administrator. There are several models that can be adopted to achieve this such as metric model, neural network and machine learning classification.

Intrusion Prevention System

The intrusion prevention system (IPS) is a prevention technology that monitors the incoming and outgoing network traffic to detect and prevent malicious attacks and vulnerability exploits.

An IPS is usually deployed behind the firewall of a system. The IPS is an active system when compared to the passive IDS as it detects threat and simultaneously takes automated actions on the traffic to prohibit the network from destruction. The two dominant detection mechanisms for IPS are signature-based detection and statistical-anomaly detection. The detection mechanisms are similar to the mechanisms in IDS.
There are several actions that can be assigned to the system to be carried out immediately after a threat is detected.
Produce-alert: As soon as a threat is matched with a signature the system raises an alarm and send out a warning.
Deny packet inline: Here, the detected packet which contains the signature is dropped. However, the network connection is not reset.
Reset TCP connection: After signature match occurs, the system sends out a TCP reset to the attacker and the destination host.
Deny attacker inline: This action utilises the dynamic access list to block traffic from the IP address of the offending traffic.
Deny connection inline: This action also utilised the dynamic access list but restricts and blocks traffic from the offending traffic session.

Recommendation:
Comparing and contrasting all of the above three solutions, the recommendation would be to deploy a strong firewall to secure the network.'

IDS only helps in detecting the threat and doesn't help in preventing or blocking malicious attacks. An IDS does not stand by itself as it relies on other comprehensive measures to mitigate the identified threats. Both IDS and IPS need experience network engineer to administer the and are still susceptible to protocol based attacks. Firewall serves as an entry point for all network traffic. It serves as a gateway to check the entry and exit if network traffic. The other benefits of incorporating firewall include stopping trojans, keyloggers, hacker threats and network surveillance. Firewall also enables efficient enforcing of policies by creating network/user specific rules.

Conclusion

Prioritisation

Priority Table	
System Name	**Priority**
Network Security	1
Vulnerability Management	2
Security Information and Event Management (SIEM)	3
End Point Security Analysis	4

The above table prioritises and lists out the systems in the order of implementation. Firstly, the CIO must ensure there are no vulnerabilities and threats in the network. Implementing network security will help analysing the network for any intrusions and threats using Intrusion Detection System and applying firewalls. On application of firewalls the security of the network is enhanced. Secondly after ensuring that the network is secure vulnerability management system can be deployed to make sure the network within the organisation is not vulnerable to malicious threats and attacks. After ensuring that the network is less vulnerable to threats the CIO can then decide if or not to implement SIEM. Implementing SIEM will ensure monitoring all the security systems in place and surveillance of all data logs. This will help improve business efficiency and gain competitive advantage in the market. The final priority is given to end point security analysis as it is a business enhancement feature. This increases the profit and digital safety of the organisation.

References

Blansit, B. (2009). Firewalls: Basic Principles and Some Implications. *Journal Of Electronic Resources In Medical Libraries*, *6*(3).

Calif, S. (2018). Malwarebytes Introduces Easy-ti-use endpoint protection and response solution for monitoring, detection and remediation.

Cooper, S. (2020). 11 Best Endpoint Protection Solutions.

Daya, B. (2008). Network Security: History, Importance and Future. *University Of Florida Department Of Electrical And Computer Engineering*.

Imran, M., Ahmad, B., & A. Alghamdi, D. (2015). Role of firewall Technology in Network Security. *International Journal Of Innovations And Advancement In Computer Science*, *4*(12).

Innella, P. (2001). The evolution of Intrusion Detection Systems. *Tetrad Digital Integrity, LLC*.

O' Shaughnessy, K. (2017). Endpoint Antivirus vs Endpoint Security: A Comprehensive Comparison of the Difference Between Them.

Schaffhauser, D. (2012). ESET Releases New Editions of AV and Endpoint Security Software. *Media's Education Publications THE Journal, Campus Technology*.

Symantec Endpoint Detection and Response, Rapid threat discovery and remediation. (2018). *Cost Of Data Breach Report*.

Vielberth, M., & Pernul, G. (2018). A Security Information and Event Management Pattern. In *12th Latin American Conference on Pattern Languages of Programs (SLPLoP)*.