Czech University of Life Sciences Prague

Faculty of Economics and Management

Department of Information Technology

Master's Thesis

Implementation of Security Systems for Network Monitoring in the Company

Miah Md Rasel

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Md Rasel Miah

Informatics

Thesis title

Implementation of security systems for Network monitoring in the company

---

Objectives of thesis

The objective of implementing security systems for network monitoring in a company (bank) is to ensure the confidentiality, integrity, and availability of sensitive data and financial transactions. The security systems should be able to detect and prevent unauthorized access, unauthorized modifications, and other security threats that may compromise the security of the bank's network

Methodology

Following, there are some methodologies that would be used to implement security systems for network monitoring in a bank:

Risk Assessment: Conduct a comprehensive risk assessment to identify potential threats and vulnerabilities to the bank's network. The assessment should consider factors such as the bank's size, location, infrastructure, and types of data and transactions processed.

Security Policies: Develop and implement security policies that define the bank's security objectives, responsibilities, and procedures for network monitoring. The policies should also specify the types of security systems and tools to be used, and how they should be configured and managed.

Access Controls: Implementation of access control system to limit access to sensitive system and data. Use strong authentication and authorization mechanisms such as two-factor authentication, biometric authentication, and access control lists (ACLs).

Intrusion Detection and Prevention: Install intrusion detection and prevention systems (IDPS) to monitor the network for suspicious activities and prevent unauthorized access. IDPS can detect and block attacks such as malware, phishing, and denial-of-service (DoS) attacks.

Network Segmentation: Segment the network to limit the impact of security breaches. Use firewalls, routers, and switches to separate the network into smaller, more manageable segments, and apply different security policies to each segment.

Data Encryption: Use of encryption to protect sensitive data in transit and at rest. Using industry-standard encryption protocols such as SSL/TLS, IPSec, and AES to ensure the confidentiality and integrity of data.

Security Monitoring and Incident Response: Monitor the network for security events and incidents, and establish an incident response plan to quickly and effectively respond to security incidents. Use security information and event management (SIEM) systems to collect and analyze security event data from various sources.

Overall, the above methodologies can help in implementing effective security systems for network monitoring in a bank and minimize the risk of security breaches and financial losses

The proposed extent of the thesis

60-80p.

Keywords

Network, Security, Infrastructure, Cyber Attack, Risk Management, Authentication, Phishing, Malware, Viruses, SSL, TLS, AES , SIEM, IPS, IDS

Recommended information sources

https://ediss2.sub.uni-hamburg.de/bitstream/ediss/8930/1/haas20diss_published.pdf
https://researchbase.com.ng/design-and-implementation-of-network-security-a-case-study-of-uba-bank/
https://www.degruyter.com/document/doi/10.1515/jisys-2022-0032/html
https://www.researchgate.net/publication/286734042_Development_of_an_intelligent_system_for_bank_securit
Luis Miguel dos Santos, Vilar Ferreira, A multi-level model for risk assessment in SIEM,
https://repositorio.ul.pt/bitstream/10451/31288/1/ulfc123950_tm_Luis_Miguel_Ferreira.pdf

---

Expected date of thesis defence

2022/23 SS – FEM

The Diploma Thesis Supervisor

Ing. Martin Havránek, Ph.D.

Supervising department

Department of Information Technologies

Electronic approval: 4. 9. 2023

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 3. 11. 2023

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 29. 03. 2024

Declaration

I confirm that the thesis "**Implementation of Security Systems for Network Monitoring in the Company**", which I authored independently, solely resorted to references of the thesis. I will introduce myself as the writer of the master's thesis and say that I argue that it does not abandon the copyright laws.

In Prague on 30-03-2024 _____

Miah Md Rasel

Acknowledgement

I thank the Almighty for His divine leadership, direction and the continuous guidance and support which has led me this far, despite the challenges of completing the dissertation perfectly. Indeed, it goes without saying that the gratification shared is on another level, as I honestly and from my heart express my ingenuity thanks to my mentor, Ing. Martin Havránek Ph.D., from Department of Information Technology, which is the Faculty of Economics and Management at Czech University of Life Sciences.

I adhered the much-sought period in the framing of this issue thanks to his unvarying support and unconditional approval and ultimately privileged by his scientific wisdom too. As an academic assistant partner, Professors so and so not only provided me with defences skilfully, but also greatly strengthened my academic abilities and gifting abilities which are reflected in the thesis. To me, the real meaning of gratitude is what comes from his deep-rooted affectionate and always accessible coaching that he has continuously lent me in relation to my academic and professional progress is beyond any count. Additionally, I want to thank the advisors; this can be dean, professors, colleagues, relatives, and friends for the unreservedly support that has, through encouragement and direction, helped me to focus, to pursue the course, and to continue. They always lift me up as almost always, they indeed their confidence towards me and trust in my abilities.

However, I would first of all appreciate the young generation at the end of this list and every group of scholars who provided us with new and more knowledge as evident in this thesis. They got the world of theory moving, became the inspirers and evolutionalists of the field, and had some advanced ideas which got the whole field of evolution on the move. To tell the truth, I feel so very lucky, a part of all this conversation. Every individual whom I can assure of being the lucky one among all, each has gained a huge influence on my academic life, and the credit goes to those fortunate people.

Implementation of Security Systems for Network Monitoring in the Company

Abstract

Networks, for the most part, having gained a larger and larger importance across domains leveraging the network systems even more strengthens the need for practical implementation of the effective network security protocols. Therefore, this work explores one of the biggest security problems in network monitoring nowadays: Reinforcing the current security system or installing a new security system. The system exploits the capability of its multi-layered defenses such as intrusion detection systems, firewalls, network scanners as well as the machine learning algorithms that are used to bring additional abilities for detection and blocking of possible threats and all these in a faster way as compared to the other systems. A network with only few nodes to observe the whole range of security and comfort from the attachment capacity to the partial intolerance would be fully tested which is of importance for the seek of network protection improvement.

The designed security system is the main principle of the essay that has been deploying, managing, and being replenished. Researchers not merely check the accuracy of the tool but also look for ways in which it save time and can be used in large scale projects in the long run which would basically make security infrastructure effective. It also includes assessment of scalability and viability of the system in a wide variety of settings including examples where the system has shown resilience to threat changes which keep on evolving. Unlike many other studies, this thesis is more penetrating, has invested a lot to get a highly skilled critical reviewer, and is very innovative in its approach. The net result is a dramatic increase in network monitoring security. Such studies not only provide general knowledge to the healthcare providers and professionals but also contribute to the development and refinement of healthcare policies, systems, and practices.

To sum up, sensors should also be incorporated in proactive security systems, since they offer the lowest demand for security services, because they are expensive. As innovation technology accomplishes in-depth integrated fused testing used in network security solution, the effectiveness in strengthening network defense in this mixing-up motion is proved to be progressive. Being a reliable technology with the strong advantage of being able to delete various threats such as cyber security, it has a believable chance of

being utilized by the agencies that are responsible for identifying and protecting the critical assets which come from different fields.

Keywords: Network, Security, Infrastructure, Cyber Attack, Risk Management, Authentication, Phishing, Malware, Viruses, SSL, TLS, AES, SIEM, IPS, IDS

Implementace bezpečnostních systémů pro monitorování sítě ve společnosti

Abstrakt

Sítě, které z větší části získaly větší a větší význam napříč doménami, využívající síťové systémy ještě více posiluje potřebu praktické implementace účinných protokolů síťové bezpečnosti. Tato práce proto zkoumá jeden z největších bezpečnostních problémů v současném monitorování sítí: Posílení současného bezpečnostního systému nebo instalace nového bezpečnostního systému. Systém využívá schopnosti svých vícevrstvých obran, jako jsou systémy detekce narušení, firewally, síťové skenery a také algoritmy strojového učení, které se používají k tomu, aby přinesly další schopnosti pro detekci a blokování možných hrozeb a to vše rychleji. ve srovnání s ostatními systémy. Síť s pouze několika uzly, která by dodržela celý rozsah bezpečnosti a pohodlí od kapacity připojení až po částečnou netoleranci, by byla plně testována, což je důležité pro hledání zlepšení ochrany sítě.

Navržený bezpečnostní systém je hlavním principem eseje, který se nasazuje, řídí a doplňuje. Výzkumníci nejen kontrolují přesnost nástroje, ale také hledají způsoby, jak ušetřit čas a mohou být dlouhodobě používány ve velkých projektech, které by v zásadě zefektivnily bezpečnostní infrastrukturu. Zahrnuje také posouzení škálovatelnosti a životaschopnosti systému v široké škále nastavení včetně příkladů, kdy systém prokázal odolnost vůči změnám hrozeb, které se neustále vyvíjejí. Na rozdíl od mnoha jiných studií je tato práce pronikavější, hodně investovala do získání vysoce kvalifikovaného kritického recenzenta a je velmi inovativní ve svém přístupu. Čistým výsledkem je dramatické zvýšení zabezpečení monitorování sítě. Tyto studie poskytují nejen všeobecné znalosti poskytovatelům zdravotní péče a odborníkům, ale také přispívají k rozvoji a zdokonalování politik, systémů a postupů v oblasti zdravotní péče.

Shrneme-li to, senzory by měly být začleněny také do proaktivních bezpečnostních systémů, protože nabízejí nejnižší poptávku po bezpečnostních službách, protože jsou drahé. Vzhledem k tomu, že inovační technologie provádí hloubkové integrované sloučené testování používané v řešení zabezpečení sítě, účinnost při posilování obrany sítě v tomto směšovacím pohybu se ukazuje jako progresivní. Jelikož se jedná o spolehlivou technologii se silnou výhodou schopnosti eliminovat různé hrozby, jako je kybernetická bezpečnost, má

uvěřitelnou šanci, že bude využita agenturami, které jsou odpovědné za identifikaci a ochranu kritických aktiv pocházejících z různých oblastí.

Klíčová slova: Síť, Zabezpečení, Infrastruktura, Kybernetický útok, Řízení rizik, Autentizace, Phishing, Malware, Viry, SSL, TLS, AES, SIEM, IPS, IDS

Table of Contents

1. Introduction

Given the steadily evolving digital world where networks stipulate enterprise security, information saves come in as a great weapon. These infrastructures, which have grown more equipped and connected, i.e., linked, have put extra weight on ensuring the networks and systems are free from threats such as malware infections, unauthorized access attempts, and security vulnerabilities The ramifications of these risks, however, might be more severe that an unpleasant experience that it causes and affect businesses' finances, reputation, and legal position. Deployment of network security systems with the instantaneous capability to identify and respond to vulnerability breaches will to a very large extent minimize this risks, hence, improving the overall resilience of the business. The capability to track network traffic immediately and activities, especially those emanating from a threat actor, becomes an essential aspect of all comprehensive security plans, thus affording a timely detection of and assessment of security incidents as they happen. Yet, powerful as it sounds, well-crafted surveillance has its own drawbacks, with necessity of specific skills, software, and hardware (Chorafas & Steinmann, 2016).

The aim of this thesis is to show the best example of a network monitoring security system which would enhance the existing defenses within corporate organizations. The proposed system combines old type intrusion detection, firewalls and network scanners with a learning machine which is used all the time to examine network traffic and mark the abnormal patterns. The system works in this way with it has the ability to dectect anomalies that can point to security problems. Of note, in this regard, its modular design and configurability make it a choice option for numerous different deployment contexts.

The fundamental purpose of this thesis is determining whether or not the security solution recommended is successful in running the operational networks. We focus our evaluation on the reliability of the system decomposition accuracy, efficiency, and scalability, beneficial aspects of the system implementation and the ability of the system to identify and respond to the different security risks. To achieve this, we put the system through a series of tests in a sandboxed environment which had been

thoroughly controlled. We considered the system to be good enough only when it achieved the set criteria.

The structure of this thesis is as follows:

- ✓ Chapter 2 draws the theoretical underpinnings and research methodologies of the thesis.

- ✓ Chapter 3 presents a thorough and anonymous overview of those research activities that are connected with network monitoring and protection.

- ✓ The chapter 4 of the book presents a brilliant description pertaining to experimental design, results, and theoretical discourse specifying the most efficient way of monitoring of a network with the subsequent remediation of vulnerabilities.

- ✓ To conclude, this chapter is the last one reviewing the whole thesis, and include the research strength and limitations.

2. Objectives and Methodology

2.1 Objectives

The core target of each bank's network monitoring security system is to secure completely all the financial information of their clients as well as its transactions centralized in its database management system. In the current digital world, where banking, transaction processing, and customer service usually function through networked technologies, the dangers caused by cybercrimes have become cumulative and frightening. Modern financial organizations are subject to severe penalties including losses, besmirching to their good name and possible legal liability in the event of eavesdropping on their network.

The function and target of the electronic banking system network security is to foresee and prevent such misuses as hacking or unauthorized interference with the bank's internal computer network. These security systems have been installed with built-in codes that would help in instantaneously acting upon the security incidents like intrusions, detections and instant responses among other. This is made possible by monitoring the network traffic on a 24-hour basis. Prompt action and reaction are the fundamental ingredients of timely detection and to prevent a cyberattack from becoming worse and disclosing crucial information without the proper permission.

Cyber threats in today’s world are ever-changing and becoming harder to counter. This makes network security systems to be robust, scalable and adaptable. The bank entrenches the latest intrusion detection technology, firewalls, and network scanners in its security systems to prevent a wide range of attacks, and thus maintain its security standards. # Integration of the machine learning techniques provides for operability as they facilitate the abnormality and a typical behavior identification, bettering the routine rule-based monitoring.

In addition to this, shoring up the bank's defense systems for network monitoring and security has both the effect of making the bank more secure and also helping the bank reach compliance with industry standards and regulations. Strict implementation of regulations on data security as set forth by agencies like the European Union and

the Payment Card Industry Data Security Standard is a must in order to eliminate legal risks and preserve customers and shareholders' trust.

2.2 Methodology

Monitoring for cyber threats by a bank means use of any number of security techniques that can help protect the network fully. These methodologies include:

1. **Risk Assessment:** Conduct a comprehensive risk assessment to identify the nature of the threats that may target the bank's network and pay attention on the size and location of the bank and the process of data recorded.

2. **Security Policies:** A network monitoring policy should be defined, and established that states the roles and security objectives, and includes the configuration and management of security devices and technologies.

3. **Access Controls:** Apply strong access controls to gain an insight of the secret information and infrastructure through the use of secure authentication methods, including multi-factor authentication, biometric authentication and ACLs.

4. **Intrusion Detection and Prevention Systems (IDPS):** IDPS target to distinguish and avoid unauthorized access tries and uncover network activities, therefore security issues including malware, phishing and denial-of-service attacks can be countered successfully.

5. **Network Segmentation:** Isolate the network into segments in order to limit the effect of attacks by usage of firewalls, routers, stretches, and applying different policies for every segment.

6. **Data Encryption:** Implement packets encryption protocols like SSL/TLS, IPSec and AES to protect the confidential data against unauthorized disclosure.

7. **Security Monitoring:** Constantly monitor the network operations for any unauthorized activities and quickly respond to such threats or vulnerabilities; besides, utilize the SIEM systems to identify the breaches in the security and ensure timely solutions.

8. **Validation and Testing:** Certify and confirm the effective work of implemented security measures with help of threat simulation to check the strength of the system against intrusions. Refine system configurations and set the parameters based on trial results for the best system optimization.

9. **Training and Education:** IT personnel at the bank together with security staff have to be equipped with the right training and education on operation, as to instill a culture of cybersecurity awareness to deal with human error.

10. **Continuous Monitoring and Evaluation:** Embark on regular monitoring and tracking of the network's security activities as this helps to maintain understanding of the present security status of the network, while data from the security systems need to be analysed periodically to pinpoint flaws and then security measures can be enhanced.

However, through applying such tactics, financial organizations will be able to reduce the probability of cyber attacks and the negative impact of these acts on their network monitoring architecture.

3. Literature review

How well the candidate absorbed and debated the cyber security monitoring technology used during the research represents the candidate's grasp of the topic. Achieve this by scrutinizing its history through the strong scientific studies, theoretical tenets that were formulated earlier, present methods and instruments that all developed the foundation of the field, not excluding The introduction is briefly summarized here. Here is the main idea in the introduction, which can be simply stated as.

The main objective of this chapter is to give a basic outline of the present knowledge in the area of network security and monitoring by which security experts could utilize such information within their fields. This section accomplishes many really important aims. This part can effectively introduce several very significant themes.

Contextualize the Research: The first and foremost segment of this section will be evaluation and overview, which aims to give you a better insight into the issue being addressed, as it is a requirement for you to have a background knowledge not only on the problem but also on its dimensions X-factor you need to demonstrate the creation of a new change and the taking into account details that are not considered in others` approaches.

Identify Research Gaps: When it comes to the book background of the literature notation, we will focus only on the part of the summary of that story. Alternatively, you can bring out that your result is one facet of the whole truth and the demand for more extensive study still exists and that your study is considered to be complementary to research of related topics.

Show Familiarity with the Field: Further analyse works that are advocating the area of network security and time tracking. Convince that I am acquainted with the filed and wraps the gist of the subject with theory, techniques, and core that no subject could be sighted without this.

Justify the Research: When the time to pick your own research study is coming, you need to probably review the works of others. On this reasoning, you will then incorporate how they can be used to increase network control security, and so you can convince the legislators to consider your idea.

Provide a Foundation for the Proposed Approach: On the other hand, to achieve the expected outcome, when you have a safety plan, a well-defined introduction is paramount, and without such, dealing with the people's safety effectively would not be possible. To make your work contextualize you can say that there is good in your method as it overcomes drawbacks of existing networks that have inefficiency as their main concern. This development aims to introduce better methods of building strong network security measures.

3.1 Network Security

The rate of transmitting information and the network safety are the primary ingredients for network communication. The execution of numerous operations and equipment are demonstrated to be significant in protecting network data from being deformed or misinterpreted. Here are some key aspects of network security.

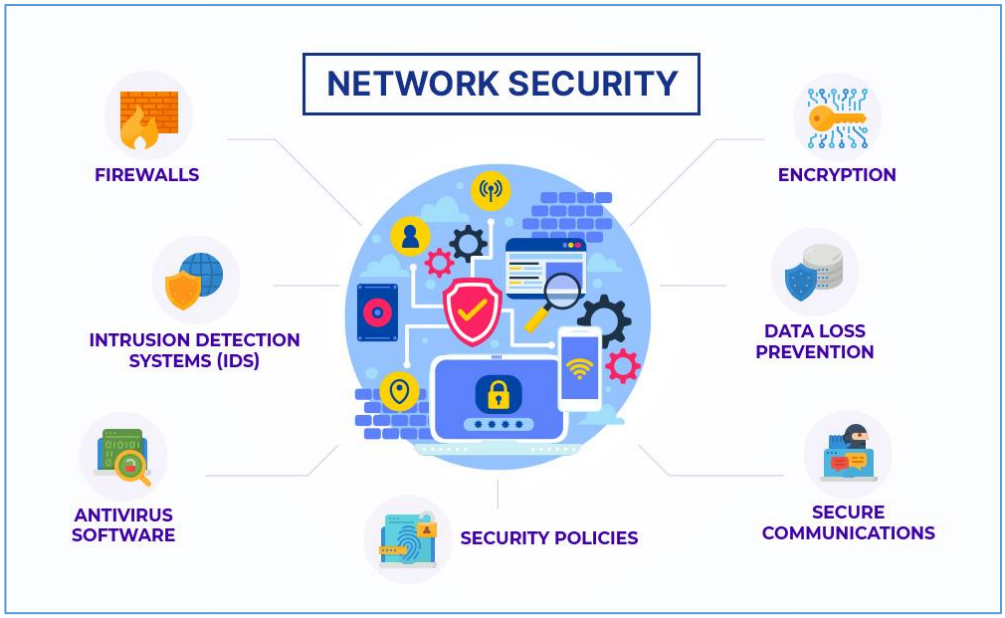


Figure 1: Network secureity overview

Source: https://www.extnoc.com/learn/computer-security/network-security

- ✓ Firewalls: The firewalls are the real walls in computer networks, which is critical to privacy protection and data flow policies based on specific internet security policy (Canavan, 2001).

- ✓ Intrusion Detection and Prevention Systems (IDS/IPS): IDS and IPS are security control techniques that watch for patterns on packets of data for malicious activities on a network. IDS just record and broadcast the suspected attacks while IPS is actively negotiate and block or swapping unwanted traffic to prevent the dangerous attacks (Canavan, 2001).

- ✓ Virtual Private Networks (VPNs): VPN's will help to create a secure connection across the network's like Internet; and thus, firms can be able to see their data safe as usual while in their transit and also enabling the workers who are far away from the company's network to get access to it through a secure network (Thomas & Stoddard, 2012).

- ✓ SSL/TLS Protocols: The protocols SSL and TLS are two encryption and authentication protocols that are functionally used to encapsulate the data into a protected transmission medium. The worldwide network is used to secure the communicating parties such as email and internet transmissions for the timely and safest sharing of information (Thomas & Stoddard, 2012).

- ✓ Network Access Control (NAC): NAC ensures only the authorized computers and mobile devices are within the network perimeter with each computer and mobile device requiring authentication and status information compliant with security requirements to be admitted to the network (Thomas & Stoddard, 2012).

- ✓ Wireless Network Security: The security implementation for the wireless networks involves using complex passwords, deactivation of inactive services, and rebooting firmware in order to fight off the perpetual cyber threats (Canavan, 2001).

- ✓ Network Segmentation: Network segmentation is an effort to prevent profusion of the attacks by secluding sensitive parts of a network and isolates the rest of the network as soon as the network parts are compromised (Canavan, 2001).

- ✓ Regular Patching and Updates: Timely maintenance and update of all network hardware, OS, and apps needs to be a priority for thwarting the use of any possible exploits and vulnerabilities (Canavan, 2001).

- ✓ Security Audits and Monitoring: Using regular audit, log analysis, traffic monitoring and security assessments we see to it that we comply with the security rules and deny any suspicious activity (Canavan, 2001).

- ✓ Employee Education and Awareness: Promote a security-awareity that includes training in password-creation and identification of phishing attempts.Awareness in cybersecurity also means that employees are well aware of how best to handle information and keep it from falling into the wrong hands.

Network security is a very adaptable and dynamic field which mandates organizations to be very innovative and adopt tailor-made solutions. When you do this, it enables one to identify the true, unique requirements of every individual or organization. Cooperation with the hardware and software technicians as well as the security analysts is important to identify the most effective set of measures and technology for network protection and for implementation.

3.2 Network Monitoring

One of the key tests in providing a network that is available, performing well and secure is the network traffic monitoring. It is characterized by the continual supervision of network traffic flows, devices, and systems for the purpose of identifying and acting on any possible issues as soon as the need arises. Here's an overview of some fundamental aspects of network monitoring

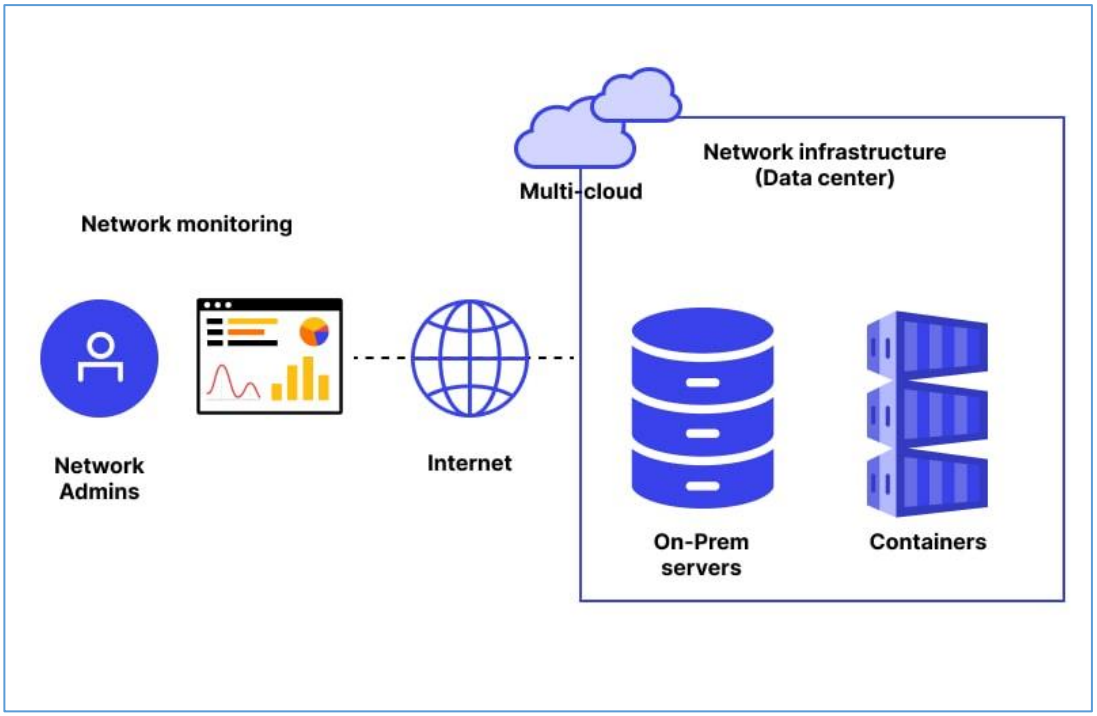


Figure 2: Netowrk monitoring overview

Source: https://www.wallarm.com/what/what-is-network-monitoring-definition-benefits-tools

- ✓ Network Performance Monitoring (NPM): NPM utilities are capable of tracking and optimizing an infrastructure's performance in real-time which can be achieved by measuring indicators such as throughput, latency, packet loss, and response time. This information is a helpful tool to network managers in order to achieve the best resource allocation and focus on bottleneck occurrence (Chiu & Sudama, 1992).

- ✓ Device Monitoring: Tracking the on and off/uptime/connection status of network devices like routers, switches, servers, and firewalls is crucial. It helps in the discovering of as well as the resolvig issues which are related to hardware or software faults and putting the right status with the use of inputs like CPU and memory usage and interfaces and device status (Chiu & Sudama, 1992).

- ✓ Traffic Analysis: Analysing software can verify a large amount of network traffic for the purposes like protocol identification, prediction of trends and threats (security or network congestion) detection. Analysis can be carried out on data at different levels such as tracking packets at the lowest level and tracking behaviours of application at the highest level (Blokdyk, 2018).

- ✓ Security Monitoring: Network monitoring may be one of the key factors in the detection and prevention of security issues as it provides a timely reply to network administrators when some breaches or unusual network activities occur, which generalizes the severity and helps administrators to combat them (Blokdyk, 2018).

- ✓ Event Logging and Log Analysis: Network monitoring systems save a history of such actions done by devices and user, which contribute to forensics, auditing and debugging. Scan logs pattern identification, outliers, and potential security threats (Blokdyk, 2018).

- ✓ Bandwidth Usage and Traffic Shaping: Watching bandwidth consumption preserves fair distribution and allows network administrators to apply network management technique traffic shaping or Quality of Service (Blokdyk, 2018).

- ✓ Distributed Network Monitoring: Large size networks benefit from the centralized monitoring platforms that gather information from individual nodes in order to create a global bird's eye view (Blokdyk, 2018).

- ✓ Network Visualization: Gaining network architecture, device connections and traffic pattern insights through visualization tools directly contributes to better network interdependencies and flows understanding. Thus, monitoring networks is streamlined (Blokdyk, 2018).

The workload of network monitoring is everlasting due to fact how much it depends on professional knowledge and utilization of sophisticated tools. Both operations or freeware solutions are available, then taken into account the factors, namely a network size, a complexity, and a set of the organizational requirements to make the tool choice.

3.3 Security Systems for Network Monitoring

Being data centers of the entirety of any IT infrastructure, the IT Security has to be devised very critically and integrated to insure proper maintaining of computer networks and all of their connected devices from the threat of Internet attacks and malicious activities. Network monitoring is really the key element here, because it provides continuous monitoring of traffic and behavior, and so it is easy to spot suspicious occurrence and prevent any violation of the system security rules. In this particular part we will learn about different options that are applicable for the effective network monitoring hence boosting the network security (Monitor, 2000).

3.3.1 IDS (Intrusion Detection System)

In the area of cybersecurity, the observing the Intrusion Detection System (IDS) as a powerful armour standing up against viruses and hackers, these systems can monitor every detail of the network traffic, system log and other important data for any security vulnerabilities. IDSs come in two primary categories.

- ✓ Network-based IDS (NIDS): NIDS utilizes filtered detection techniques with network traffic in real time, which helps with the discovery of any network breach by examining data packets as they are accorded with routing via routers and switches. Through the discovery of patterns, NIDS are able to challenge known cyber threats. Based on the findings, the resulting alerts can be swiftly acted on to minimize further damage (Blokdyk, 2018).

- ✓ Host-based Intrusion Detection Systems (HIDS): HIDS is a host-based attention system that inspects single hosts closely, continuously searching

for disparate operations or changes. By scouting the host-specific data that include the system logs, file integrity checks and virus scans, HIDS has the ability to further enhance the anti-attack and breach response capabilities, at the host level. Moreover, incorporating HIDS in network based monitoring is an application that boosts visibility and security as a whole both in the network visibility and at the host level (Monitor, 2000).

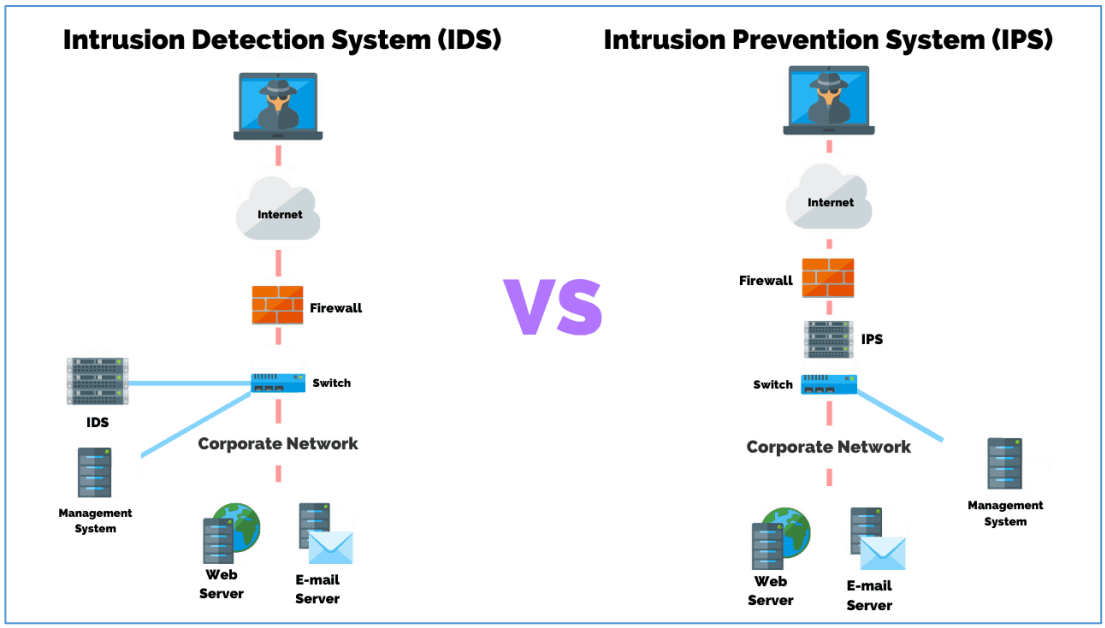


Figure 3: High level IDS vs IPS

Source: https://purplesec.us/intrusion-detection-vs-intrusion-prevention-systems/

Although IDSs consist of both signature-based and anomaly-based detection techniques, they may not provide 100% protection against the latest attacks. The signaturality way of detection implies using databases with attack signatures to get a match and thus allowing attacking commonly used host or network data. Conversely, anomaly detection is the process of setting standard normal values and raising flags when there is a substantial departure from those normal status as potential security risks.

3.3.2 Hacking Protection Software (IPS)

In terms of cybersecurity, IPS stands for Intrusion Prevention System-a security initiative that takes the lead in stopping malicious attacks in contrast to IDS and its

role, which is to warn of cyber threats. For instance, though IDS and IPS do the same thing of gathering network data, IPS is more powerful in the aspect that it not only looks into data but it also filters or blocks the packets to keep attacks from happening. While IDS acts as a standalone application that can passively capture and analyze traffic data, IPS functions in line, permitting faster responses to given blocks (Kurniawan & Prakoso, 2020).

IPSs usually rely on effective policy framework of both signatures and anomalies that spot the malicious attempts as well as a set of specific rules to effectively block cyber attacks. If one of the packets has been recognized as an attack pattern, is distrustful or breaks up a security policy, IPS may be able to either drop or alter such causing packet. Also many times when IPS spot a threat there are quick alerts given out and they immediately involve administrators on the given problem and they even take some preventive measures which are used to reduce the risk..

3.3.3 Firewalls

Firewall is the cohesive for an entire network security where it will be established as a demarcation between the private networks and the vast domain of the Internet. A firewall is responsible for filtering the data circulating in the network carefully and ensure their access by setting standards and presetting criteria (Monitor, 2000).

The firewalls are specifically the part of network stack which can be detected by different elements, like proxy or the stateful inspection based on the transport layer. The security at the packet filtering and network layer, which is the capital of network-layer firewalls, ensures the use cases are monitored carefully by going through key network elements like industrial protocol, port numbers, and protocols (Monitor, 2000).

3.3.4 SIGINT stands for Security Intelligence, Threat Intelligence, and Event Intelligence

In the cyber security's world of the modern era, SIEM systems come forward as the oldest but still vigorously utilized tracking devices, which are used by many businesses to watch over their networks. Such mechanisms work by consolidation of

a huge number of data from various network nodes, applications, and security tools that have essential analytical functions to detect security anomalies and provide up-to-date alarms (Boddu & Lamppu, 2024).

SIEM systems are based on live network monitoring, quick incident responses measures, and compliance management functions which are the key aspects of these systems. Applying different techniques from a method assorted to the range of technologies (that includes firewalls, IDS/IPS, antivirus software, and authentication systems) SIEM systems collect the amount of logs, events and alerts. The combination of several information packing and unique features shows SIEM systems where they are focused in finding the link between the elements, and discover the anomalies within the data, and provide useful insights that can help in formulating actionable plans (Boddu & Lamppu, 2024).

The AI-driven SIEM systems today proficiently monitor the data network and take advantage of advanced analytics like machine learning for detecting breaches in the cybersecurity mechanism with nearly perfect precision. In a comprehensive manner that can vary from stationary analysis and through the behavioral analysis atlant, the rules-based heuristics, and so through, SIEM systems able to discover the inordinate and suspicious events or behavior. Additionally, security analysts with SIEM elicit the reporting and visualization abilities embedded in the SIEM systems to build the menace assessment and to shrink the reaction time. (Boddu & Lamppu, 2024)

3.3.5 Challenges in Security Systems for Network Monitoring

One of the main issues to consider when design the dependable network security systems now is the fact that cybersecurity is dynamic continuously changing. In this context, complexity and the scope of the issue are the obstacles which stake the most claims to solve them. Among the myriad of network nodes and configurations and scaling solutions that can do the same as Internet traffic gets larger, it is a must that there are scalable solutions capable of handling the voltage of network traffic while the speed is maintained (Strebe, 2006).

Also, the fact that malicious incidents are frequently changing makes the adoption of inventive measures to tackle the dynamically changing threats imperative. Real time updates and threat intelligence become vital notifications to security systems because they help fight against the threats that are outside of their grasp as per static research. On the one hand, despite the fact that a balance between false positives and false negatives remains challenging, it is clear that there have been significant advancements in the field of prenatal testing in the past decade. Besides unnecessarily cluttering security analysts with false positives, a gap in the security net is ensured if the detection algorithm lacks accuracy, thereby exposing networks to cyber threats (Strebe, 2006).

Interacting and interchanging data is a further complexity, as often businesses may use different detection and protection tools. It is important by doing this complete compatibility and synchronization with different systems of security and risk management will be maintained to provide the maximum protection. Also, the protection of privacy and compliance become fundamental for managing data privacy. Complying with the stipulation of the GDPR and data mining activities requires one to place premium on the user privacy and data security by being careful (Strebe, 2006).

Security policy rules, profiles matching and pattern detection are the techniques that are widely used in security risk identification and solving. While obstacles like the abundance of threat actors, network complexities, false positives and negatives, integration problems, and data privacy are the prerequisites for network monitoring improvements, it is important to resolve these problems. Usually organizations chose scalable and trusted security solutions which help make their security postures more robust, immune to emerging threats and preserve the organization’s valuable assets and valuable data. (Strebe, 2006)

3.4 Network Safety and Statistical Learning Machines

As a process in which machine learning aspects get more attention at the moment is network security improvement, machine learning techniques are considered by many people. This emerging technology has highly intellectual algorithms to analyze the seized network data in bulk, it gives early warning of the attacks, could be in form

of anomalies and emerging trends. Hereby, this part answers the question about the ability, uses today, and prospects of machine learning in the field of cybersecurity (Strebe, 2006).

Machine learning prospect in network security has been plenty enchanting as emphasized by Thompson's study of AI utilizing to fortify network security. From the use of the latest statistical learning machines, businesses can keep up the fight and ensure sustained advancement against the increasingly dynamic cyber weapons. However, the algorithms are capable of searching through excessive network traffic, differentiating various alterations which could result into malicious activity undetected by traditional security procedures (Strebe, 2006).

Machine learning in network security today covers various implementations embodied with intricate applications. From the detection of anomalies and the collection of threat intelligence to predictive analysis and forecasting, the methods are not single-sided but multi-sided, allowing customized safeguard of networks against cyber threats including a number of others. Analysis of historical data is nevertheless the source of wisdom, and algorithms can use data emerging threats adopting and proactive threat mitigation and incident response accordingly.

Besides, the horizon of machine learning in network security seems limitless since this field still has many areas to explore for even more novel developments. Research and development updates suggest the flow of evolution in machine learning systems created to improve the networking security monitoring. Additionally, incorporating complementary strategies of using AI and deep learning which are immensely powerful, hold the promise of coming up with new ways for future network security and reliability (Kizza, 2020).

In summary, implementing statistical learning machines as part of a security framework is the backbone of the evolution and transition from traditional to modern network security. Through using the characteristics of machine learning, organizations will be able to more effectively monitor and control cyber risks, and consequently, protect information and critical assets from external and internal threat. It is the fact

that research push the limits and that machine learning is a smaller part of the whole process it will be to open the door for the safest and the most resilient network in the history.

3.4.1 Machine Learning for Cybersecurity Applications

Machine learning of today has already come out to be the revolutionary area of the internet security system, which suggests numerous applications for improving robustness and weakening the damaging cyberines (Malik et al., 2022). Below are some of the prominent uses of machine learning in cybersecurity:Below are some of the prominent uses of machine learning in cybersecurity

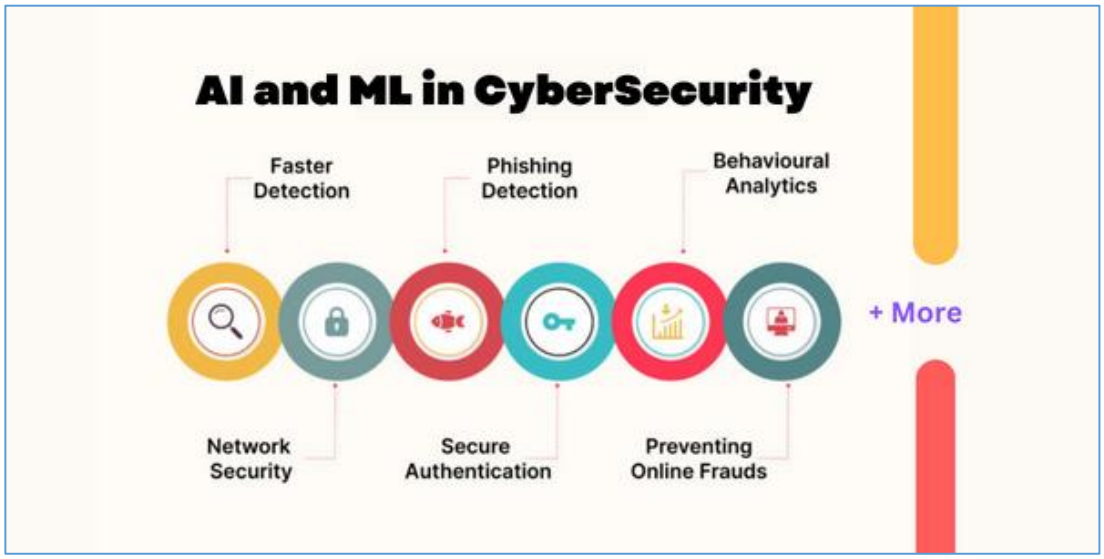


Figure 4: AI & ML benefits in cyber security

Source: https://www.analyticsvidhya.com/blog/2023/02/ai-in-cyber-security/

1. Machine learning algorithms, it's worth noting, are highly skilled in spotting significant deviations, since they have been already trained. The algorithms of these systems act quickly to identify deviations or anomalies with the modeled data or compared in real-time mode that indicate intrusion, insider threat or some suspicious activity. Such an active approach to detecting anomalies empowers organizations to provide a firm security shield against new hazards. Consequently, they have a chance to lead in the emergency of new threats (Malik et al., 2022).

2. Intrusion Detection and Prevention: The process of characteristic analysis and traffic patterns recognition for machine learning algorithms is intended for making the difference between the benign and malicious traffic. This ability lies at the heart of many intrusion detection and prevention systems (IDS/IPS), being used to counter DDoS attacks, malware infections, and unauthorized access attempts as they try to take hold (Malik et al., 2022).

3. Malware Detection: Machine intelligence powered by the scrutiny of the many network data sources, such as email, downloads and network traffic for evil malware signs is competent enough. By educating machine learning models through labeled datasets that already contain existing malware exemplars, businesses can distinguish between safe and malicious network traffic, thereby reinforcing the organization's cybersecurity against growing cyber menaces (Malik et al., 2022).

4. User Behavior Analysis: Machine learning methods can be employed by organizations to analyze that which happens within the network, to find the abnormalities or vulnerabilities. A closer look at logins, accessing and data moving is an art that these models master. They pinpoint anomalous behaviors that could indicate hacked accounts or insider threats facilitating the early detection of security breaches (Malik et al., 2022).

In brief, the inclusion of machine learning into the cybersecurity/network applications is precisely a changing process of the network security approach. Obviously the use of machine learning prediction algorithms, organizationcan prevent and avoid the ongoing cyber attacks forcing remarkable numbers of important assets and data to be stolen in the faster pace of digital world.

3.4.2 Machine Learning Algorithms for Network Security

The field of network security is largely powered by the multitude of machine learning methods that promotes defense and earlier detection of cyber threats. Here are some of the key machine learning algorithms utilized for network security:Here are some of the key machine learning algorithms utilized for network security:

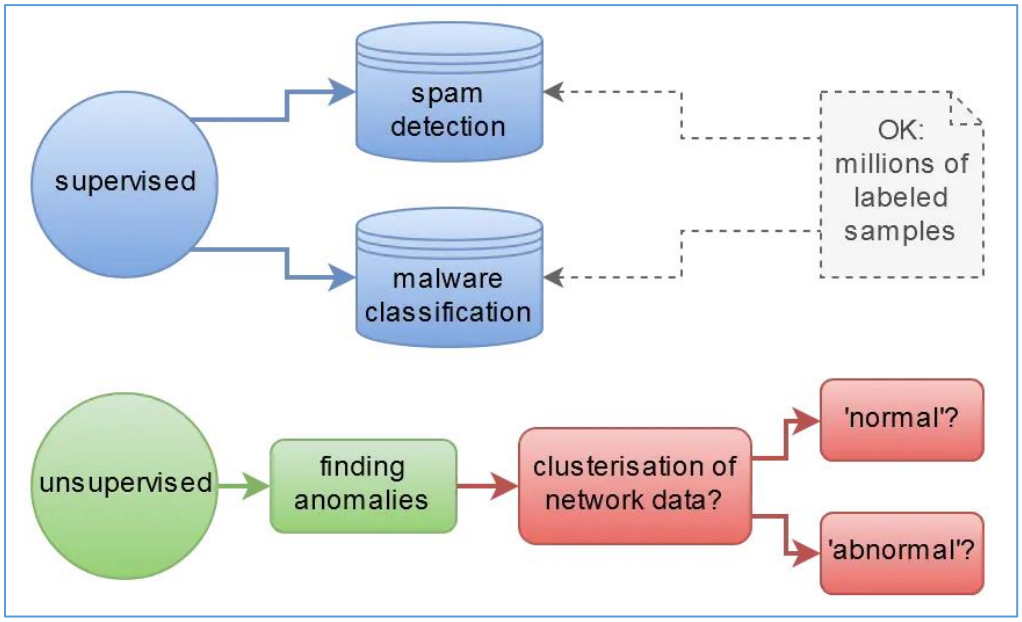


Figure 5: ML algorithm workflow for network security

Source: https://www.botreetechnologies.com/blog/machine-learning-in-cybersecurity/

1. Supervised Learning Algorithms: These algorithms implement training of data that have been labeled previously, to single out structures that are not labeled in the given data, like network traffic. Techniques, such as decision trees, random forests, support vector machines as well as neural networks are among the most frequently used algorithms to combat network security flaws. SVMs become known in supervised learning settings and remarkable in such jobs (Malik et al., 2022).

2. Unsupervised Learning Algorithms: Unsupervised learning techniques are the ones that work very well without any labeled training data. Those are basically to spot certain patterns and anamalies within network data. Strategy of clustering algorithms like k-means clusters and DBSCAN helps gather network data and identify any anomaly patterns which improves anomaly detection (Malik et al., 2022).

3. Deep Learning Algorithms: In the recent past there have been many innovative applications of deep learning algorithms to various security functions within networks. The most notable of these applications is the deep neural network technology. Among other things, convolutional neural networks (CNNs) can quickly process layer-by-layer packet headers and payloads, with recurrent neural networks (RNNs) being an important tool for predicting temporal correlations from within an array of network data streams, which then enhances the overall threat detection functionality (Malik et al., 2022).

4. Reinforcement Learning: Although Reinforcement learning algorithms could be quite effective for solving games related to network security tasks that need the system to take certain actions under rewards or penalties, they do not get rid of hackers. To illustrate, reinforcement learning can play a significant role in creating deterrent security rules that not only adapt dynamically according to various network states but also perceive and react to changing threats at real-time (Malik et al., 2022).

In fact, the use of machine leaning algorithms to build network security solutions opens up a new perspective in the struggle against hackers and other cyber threats. Utilization of supervised, unsupervised, deep learning algorithms as well as reinforcement learning algorithms by the organizations is leveraging their ability to efficiently detect and block any damaging attacks on their critical infrastructure and assets.

3.4.3 Concern Safety of Computer Networks and Automatic Learning Systems

Securing computer networks in the wake of automatic initiatives poses to be a stand-alone task that involves a number of issues and concerns.

Data Quality and Availability: Recent development and training of machine learning models depends on the accessibility of good enough and well tagged training data. Nevertheless, the capability to get proper and homogeneous network information is often identified as a problem, in particular, in those research fields in which the

security issues are rarely met or new. Data labeling goes through the rigorous process that involves multi-stage validation for it to be perfect. Such a process is time-consuming, consuming a significant number of resources for perfecting data labeling (Kizza, 2020).

Feature Selection: The design of rigorous machine learning models depends on the meticulous extraction of significant information components from previously existing network data. It is also expertises in the network security that are needed to analyze the significant facilities for timely detection of the threats (Kizza, 2020).

Adversarial Attacks: The actors have a proficiency of altering network data or injecting malicious components to deceive machine learning systems. One prominent example of a method of adversarial attacks is generating divergence in security detection systems, such as false positives, or false negatives, which ultimately result in inaccurate interpretation and, thereby, reduce trust in automated security measures (Kizza, 2020).

Interpretability and Explainability: Machine learning models, however, can lack in some areas; among those is the fact that they may not be easy to explain or interpret, therefore providing a kind of challenge when it comes to understanding the reason for the specific decision made or prediction given. For network security, the explainability and the interpretability are the most crucial during the detection of threats because it helps analysts to develop trust and also gain insight from detected threats (Kizza, 2020).

Scalability: The strategy of a more secure network requires designing smart learning algorithms with high scalability for processing high volumes of traffic and prompt data processing. Scalability concern is a vital piece of the scale that is needing involving the average growing rate, speed, and diversity of data on current networks (Kizza, 2020).

To mention, to overcome the problems stated earlier, one must make full use of automatic learning systems to develop solid network security schemes that can sustain cyber threats that evolve to continue to improve its cyber-defenses.

3.4.4 Next Steps for Network Security Using Machine Learning

Right now, addressing the present vulnerabilities creates opportunities to extend the domain of using the machine learning methods for the network security.

Adversarial Machine Learning: One of the fundamental areas related to research is designing a sturdy machine learning model that tolerates these types of attacks. Strategies such as adversarial training, ensembling, and anomaly detection are currently being investigated all the time to make the machine learning models indestructible even for computer aggression (Halder & Ozdemir, 2018).

Explainable AI for Network Security: In order to secure the network and reach its safe target, it is necessary to improve the interpretability and transparency of machine learning models. The cybersecurity research is oriented towards the development of tools that would help in reasoning the machine learning based security decisions in order to increase the level of either transparency or trust in the automated systems (Thomas & Stoddard, 2012).

Federated Learning: Usage of the federated learning technique makes it possible to train machine learning algorithms on a wide spectrum of distributed devices or connected networks without storing data centrally. Humanize this sentence: This approach enables the privacy aspect while at the same time deriving the network collective wisdom the the network traffic monitoring, setting the way to more secured and privacy-preserving network conducting (Thomas & Stoddard, 2012).

Online Learning and Stream Mining: Dynamic fast-paced network security requires models well-versed in quickly learning with fresh streams of network data and well system-flexible models. Streamline algorithms within online learning coupled with the applications of mining techniques enables continual educating processes while seeking to combat newly forming network vulnerabilities by

instrumentalizing a quick reaction and proactive response measures (Thomas & Stoddard, 2012).

Hybrid Approaches: Blending various machine-learning algorithms, for example, supervised and unsupervised learning or stacking machine learning on top of rule-based systems, seems to be a prominent development approach that will result in more robust and precise security solutions for networks of all sizes. Hybrid approaches builds on the most appropriate tools, allowing for integrating their strengths, to boost the general security readiness and functioning (Thomas & Stoddard, 2012).

To summarize, aligning oneself with these approaches not only resolves present problems, but also catapults network security into the realm of future security which is advanced and effective in vanquishing cyber threats.

3.4.5 Machine learning has revolutionized Network Security

By the analysis of the large scale databases, the advent of machine learning has brought a significant breakthrough in network security, as it is able to identify the unseen risks earlier. AI can now detect the patterns in user behavior, get viruses, threats or the anomalies, which will help you to have stronger network defenses.

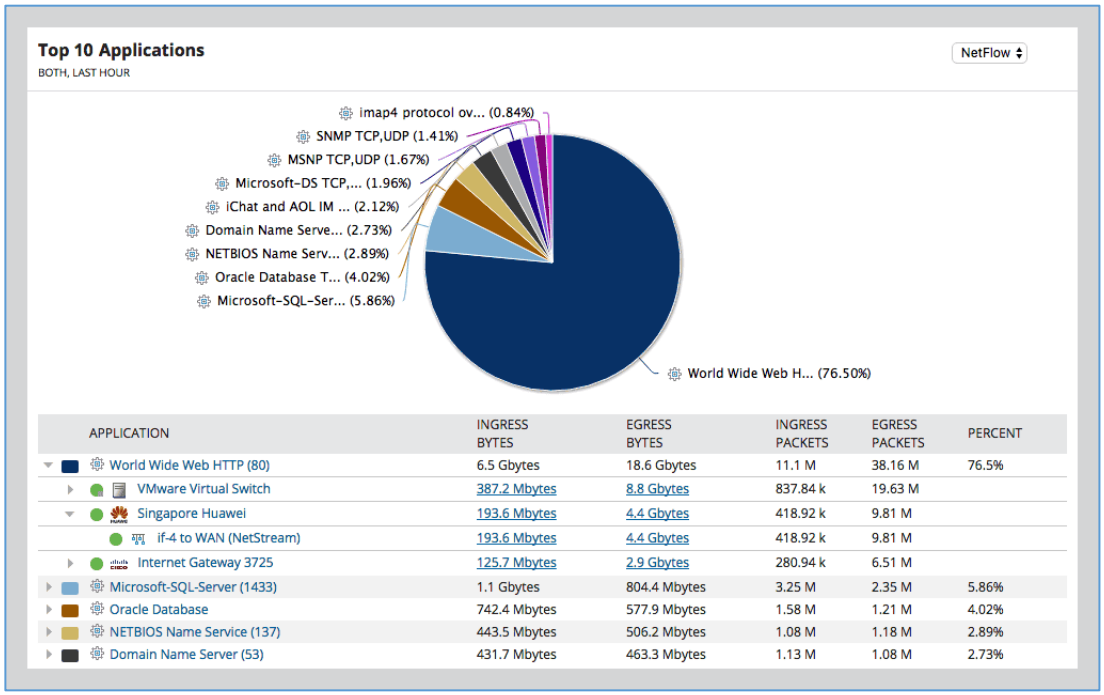
More innovative methods, like deep learning and reinforcement learning, give networks an ability to (inaudibly) when under attack. Although the machine learning holds great promise in various applications, data quality, feature selection, adversarial attacks, interpretability and scalability are still some of the hurdles that need to be addressed (Halder & Ozdemir, 2018).

Innovative research approaches are composed of analogy based methods, federated learning, online learning, adverse approaches and explainable AI. Through these efforts the whole industry will become a powerful growth engine, while the network perimeter will be strengthened at the same time (Halder & Ozdemir, 2018).

Humanize: Apart from adding to threat detection, machine learning in network security equips security systems with a capacity to identify unknown threats and devising proactive defensive tactics, a hedge against emerging cyber risks.

3.5 Network Traffic Analysis

The network traffic analysis that is focused on assessing a network's security, performs this role by intercepting, analyzing, and evaluating the packets of traffic. These packets make it possible to detect network traffic, spot issues, and get early warnings about a possible threat or malicious behavior. Therefore, the system administrators can take advantage of this information as they take proactive measures to defend an existing network (Blokdyk, 2019).



APPLICATION	INGRESS BYTES	EGRESS BYTES	INGRESS PACKETS	EGRESS PACKETS	PERCENT
World Wide Web HTTP (80)	6.5 Gbytes	18.6 Gbytes	11.1 M	38.16 M	76.5%
VMware Virtual Switch	387.2 Mbytes	8.8 Gbytes	837.84 k	19.63 M	
Singapore Huawei	193.6 Mbytes	4.4 Gbytes	418.92 k	9.81 M	
if-4 to WAN (NetStream)	193.6 Mbytes	4.4 Gbytes	418.92 k	9.81 M	
Internet Gateway 3725	125.7 Mbytes	2.9 Gbytes	280.94 k	6.51 M	
Microsoft-SQL-Server (1433)	1.1 Gbytes	804.4 Mbytes	3.25 M	2.35 M	5.86%
Oracle Database	742.4 Mbytes	577.9 Mbytes	1.58 M	1.21 M	4.02%
NETBIOS Name Service (137)	443.5 Mbytes	506.2 Mbytes	1.08 M	1.18 M	2.89%
Domain Name Server (53)	431.7 Mbytes	463.3 Mbytes	1.13 M	1.08 M	2.73%

Figure 6: Network traffic analysis demo

Source: https://www.solarwinds.com/netflow-traffic-analyzer/use-cases/network-traffic-analysis

Among the primary techniques being utilized for network activity analysis include capturing and sorting of data packets while they area flowing from one network device to another. This approach lets us monitor the first and later packets'

headers plus payloads. Such details give important clues about the connections origin, destination, and content (Blokdyk, 2019).

The second major contributing factor is deep packet inspection (DPI), which serves as a technique of network traffic analysis. DPI involves in-depth looking at data packets under every layer, including the application layer, with an aim to discover anomalous patterns, signatures and behavior that hint of suspicious or rule violation activities. DPI is now a powerful tool that allows scrutiny of the packet payloads. Network administrators use this feature to detect and repress various security threats, malware infections, hacking attempts, and data leakages (Blokdyk, 2019).

Another technique of the flow-oriented data analysis which consists of the cumulative evidence of per network endpoints is the flow-based approach to analyze the network traffic. Through the monitoring and the analysis of the traffic flows, Network Administrators can get the information and the preparation on how the network is acting, the traffic patterns, and the performance metrics. The flow-based approach is especially effective for pinpointing malicious behavior patterns, such as distributed denial of service (DDOS attacks), port scanning, or network discovery (Blokdyk, 2019).

In conclusion, network traffic analysis is an unjustifiable vital measure to make sure the network's security and integrity. Through the use of methods such as sniffer, both deep inspection and flow-based analysis administrators are capable of plenty to intellectualize, analyze, and respond to further risks of network threats and avert them, thereby securing all the critical assets.

3.5.1 Packet Sniffing

What is interesting is that packet sniffing is often applied by various information security methods as a way of digging into the translent's networks details. Thorough analysis by matching, tracing and examining the individual network packet will provide insights about the traffic by determining its origin, destination and content. The culture of lying in organizations stems from the desire for self-preservation, fear

of repercussions or vulnerability, unclear ethical standards, collective culture of acceptance, and external pressures (Blokdyk, 2019).

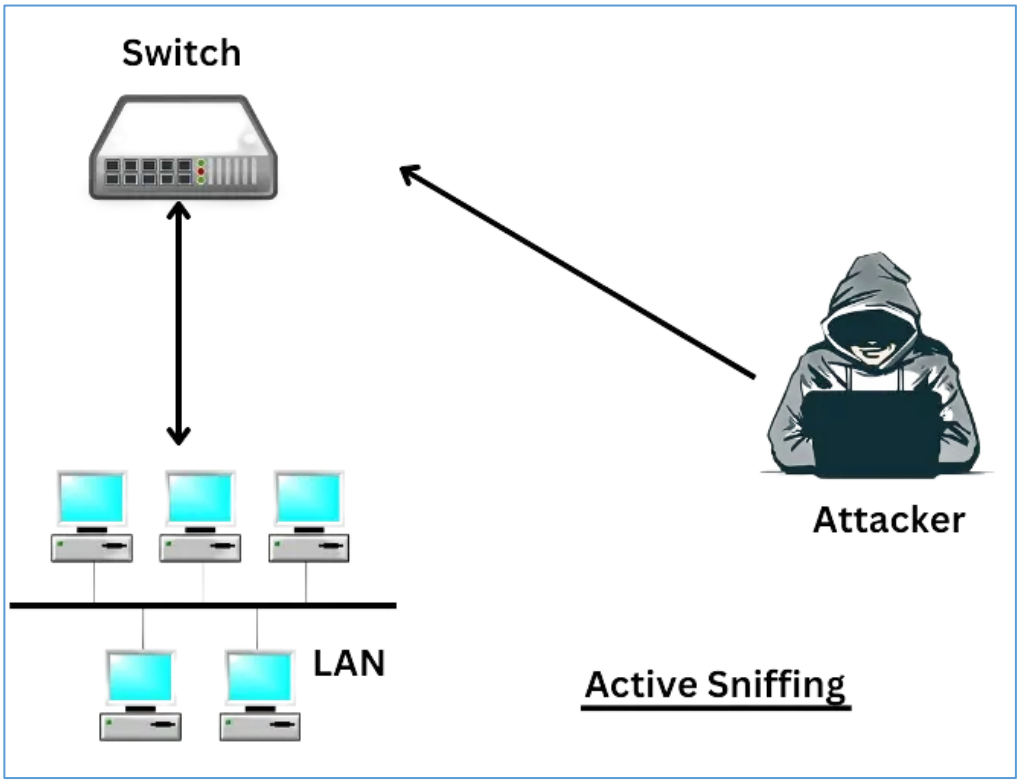


Figure 7: Packet sniffing overview

Source: https://techofide.com/blogs/what-is-packet-sniffing-how-to-perform-packet-sniffing-practical-demo-on-wireshark/

Playing roles in transmission of the network protocol, they have the functionality to obtain the information packets in the transit while they are still in a data link layer. By having an edge in network traffic, they thus become able to pave the way to cache, and control the flow of the packets that are continuously moving along the interconnected routing system. Techniques as pseudomode, traceroute, ORAR are used by intermediate network tasks to intercept and probe all network traffic passing through the network interface even those the are not destined for (Blokdyk, 2019).

Although this work might be viewed as performing a task with a risk involved, however, it's very important to follow the rules. Undoubtedly packet sniffering which is a passive form of monitoring may accidentally leak sensitive information such as IP addresses, ports, protocols and payload content. However, notwithstanding these

dangers the packet sniffing provides impressive capabilities. It offers the isolating of connectivity at the individual device level, as well as the opportunity to detect the active protocols and applications, and to inform about traffic patterns and trends (Blokdyk, 2019).

Simply put, network traffic inspection that relies on packet sniffing is an extremely effective method of cracking down on whatever hides behind the network traffic. Through the use of the deep packet sniffers, network administrators can achieve the level of understanding expected about the network behavior, find the network security threats possibilities and the specific effective optimization of network performance (Blokdyk, 2019).

3.5.2 DPI refers to Deep Packet Inspection

Within the context of networks, the expression “DPI – deep packet inspection” meaningfully stands out. Unlike conventional packet analysis that checks only packet headers generally, DPI also digs deeper into the meaning carried in the packet content. Therefore, it enables the user to capture information not only for the packet level level, but also interact and gain a perspective from the traffic level (Blokdyk, 2019).

The scrutiny of packets content is one compelling argument in favor of Transparency Inspection. This function makes it possible to spot especially the domain or layer of protocols employed by the applications and also the security of every packet. DPI technology, by inspecting the packet payload, is able to determine the point of origin and the detail through which it was used – it can tell whether the traffic is from web browsing session, email communication, file transfer or some other application specific protocol. Now, with this specific details, administrators will be able to analyze the user behavior in a more detailed way, discovering the potential musicals problems and issuing the more strict policies for network (Blokdyk, 2019).

Deep packet inspection is no longer a narrow field discipline – it is a complex network issue that goes far beyond its original use. DPI functions as a multifaceted approach to facilitate network security by the ability to separate benign data and harmful data entering the network traffic. Special feature of DPI in the area of

analyzing the payload of TCP has provided capability to identify malicious activities of neurotic programs or attempted attacks. Besides that, combining DPI with IDS (Intrusion Detection System), is able to strengthen the networks defense, by the ability to detect and stop potential threats early (Blokdyk, 2019).

In brief, DPI joins an important array of network administrator equipment, allowing them to look deep into the network traffic and detect hidden threats as well as the improve security of their network with a highly-targeted approach.

3.5.3 Flow-Based Analysis

Given that there is traffic monitoring and analysis, flow-based analysis rises up as an appealing alternative, since it provides a comprehensive view about global traffic by compiling data packets into coherent packets, named the flows. The flows are behavioral bur similar attributes like the source of the request (IP address), ports and protocols. They provide visible display of network activity, helping to promptly detect anomalies and collating them to get to the root cause of the problem (Pescapè et al., 2012).

Both, flow-based analysis and the data it relies on, are derived from the flow monitoring process, which employs specialized flow monitoring equipment. Instead of closely watching single substrings, the flow monitoring toolsets group them into groups as defined in the parameters, thus revealing the complete picture of what all traffic is. Such an informational content of a flow data (packet counts, byte counts,s timestamps, durations, and so on) forms a really substantial backbone for administrators to get complete grasp of network behavior (Pescapè et al., 2012).

Applying a network structure for analysis yields significant benefits while accomplishing objectives effectively on a large scale. This approach obtains a neat representation of the essence of many network data, hence, it makes it possible for administrators to navigate through web of networks and detect faults such as congestion and bottlenecks. Furthermore, the continuous monitoring capability has spared the flow-based analytics administrators from the burden of demarcating offline

building of the network performance so that they can focus their attention exclusively on the resolution of emerging issues (Pescapè et al., 2012).

For the flow-based analysis, it is the robustness and diversity of the statistical tools that play a key role, as these enable flow data processing to offer the most accurate depiction of concealed relations and behaviors. The detection of malicious behavior in the network traffic patterns, anomalies, intrusions, breaches, and/or compromised hosts are rapidly accomplished through the rigorous examination of flow data. Hence, admins can be immediately familiarized with issues and address them in a timely manner to ensure the robustness of the network's security (Pescapè et al., 2012).

To conclude, flow-based analysis continues to distinguish itself as a desired tool for a network administrator by encompassing the fundamental concepts and principles of network analysis in an extensive and scalable manner. With the help of flow data gathering, as well as statistical methods a system administrator can obtain a full understanding of any modern web of networks, including security threats, and can thereby achieve better network performance.

3.5.4 Challenges in Network Traffic Analysis

However, network traffic analysis is far from being a cakewalk. This digital realm presents network managers with a myriad of challenges which could be very much related to the complexity and birthing in the amount of traffic of a network. The volume of information moving over networks grows larger every day. This creates serious challenges for the entities that traffic is carried – from the ability to capture, store and analyze such large amounts of data to the need for reliable resources to manage high-volume traffic across vast networks (Pescapè et al., 2012).

In consequence of the rising layer of complexity in network traffic analysis due to the high use of encrypted data. Although the statistical methods of analyses based on scanning of transmitted data (payload) are getting more and more sophisticated, the growing tendency to encrypt information for privacy purposes turns these methodologies into less efficient tools of analysis. One of the original network traffic

analysis methods, deep packet inspection, now has challenges that stop it from deciphering encrypted communications, and so, there is a need to thoughtfully invent new decryption strategies so that network monitoring tools stay effective (Pescapè et al., 2012).

Additionally, all ethical and moral aspects of network traffic must, therefore, be profoundly stated and examined. Due to privacy problems much more often users disapprove using network analysis, as sometimes it starts invading private or secret data. Administrators should anticipate a balancing act of sorts, making sure that the two sides of the equation are equally happy, as the two sides of the equation are privacy standards and robust procedures to keep the network secure against possible breaches, although the users themselves have a right to keep their information private (Pescapè et al., 2012).

Network traffic analysis, in a nutshell, consists of several components that feed into one another: as networks grow and traffic loads surge, the studies to be conducted become even more complicated. Through the use of up-to-date technologies, novel crypographic strategies, and the by-passing strong privacy policies, network executives inactively deal with these challenges maintaining security and data integrity plus the privacy of their networks in the world of interconnection.

3.5.5 Future Directions in Network Traffic Analysis

Digital network will grow in no time grossing complex in nature and more sophisticated security threats will keep on emerging, hence the network traffic analysis the future is in more advanced approaches and techniques. AI and machine learning solutions hold the key to deal with the massive amounts of data from the networks that can identify their patterns, predict behavior, deviations and ultimately thwart threats before they materialize.

Network traffic monitoring scaling to the cloud is designed to employ big data analytics and cloud computing capabilities allowing real-time analysis of huge amounts of network traffic through distributed computing and scalable data storage alternative. The technology of SDN and NFV introduces novel directions of

applications research which aims at further adapting and improving the programmability of network management as well as enabling a simpler and more affordable implementation and scalability of monitoring and analysis procedures (Pescapè et al., 2012).

Involving, the phenomenon of IoT (Internet of Things) industry also calls that to be appropriate approaches to network traffic analysis because IoT devices communicate with various protocols. In order to deal with IoT vulnerabilities it is required to come up with advanced analytics methods which could be able to uncover the intricacy of IoT data (Pescapè et al., 2012).

Finally, what the future of network traffic analysis depends on are perpetual invention and adjustment to any environment that advances. Although the issues of encrypted data and privacy concerns endure, the optimal way is not simply using the newest technologies or complying with dynamic network patterns; it is also the act of arming administrators with the method of guaranteeing network integrity in the ever-evolving environment.

3.6 Security Information and Event Management is an acronym for this process

The marriage of Security Information Management (SIM) and Security Event Management (SEM) revolutionizes secure governance of the network environment, summing up as the unified strategy to shield digital assets. The Security Information and Event Management (SIEM) system, which aspires to be the brain of the transition at the forefront, is a great example of the new facility that performs the real-time data analysis and gathering from different inputs for an increased incident response (Thomas, 2018).

3.6.1 Components of SIEM

The integration of multiple vital elements within a SIEM system will be the one which will lend credibility to a comprehensive security monitoring and management solution. These constituent elements include:

1. Data Collection: SIEM systems can accurately monitor multiple endpoints, including computers, routers, firewalls, and another device sensitive better. It here means logs, events and traffic statistics are stored in the centralized repository for their analysis and links sake (Thomas, 2018).

2. Log Management: The subject of log management of SIEM systems is one of the activities that involves the aggregation of logs, their storage, and final analysis, obtained from different IT infrastructure entities. It includes network node, server, firewall, and other useful sources logs. This enables investigation of the network activity, user audit, syslaw and even system security gaps (Thomas, 2018).

3. Event Correlation and Analysis: The data that's generated via SIEM systems undergoes in-depth analysis and correlation; these techniques are applied to distinguish security trends, to find the outliers and to bring down the potential security breaches. Amongst the techniques used to detect and prevent potential threats, we have things such as data inspection and trend analysis leading the way when it comes to completing this task (Thomas, 2018).

4. Alerting and Notification: In this regard, a SIEM system is a fundamental part of the proactive threat detection as it gives security administrators about events that happen in real time when a threat or potential security incidents are identified. Theses alerts are determined according to the predefined standards, rules, as well as based on anomaly detection algorithms and give security teams a chance to process correctly and quickly detect risks (Thomas, 2018).

5. Incident Response and Workflow: One of the capabilities of SIEM systems that are worth mentioning is a fast response incident which can mitigate incidents within minutes through automated process. SIEM systems set up the workflows that unite the activities of ticket tracking, management and

escalation procedures which in turn enables security teams to handle security incidents collectively and with time as well (Thomas, 2018).

6. Reporting and Compliance: SIEM helps organizations toward meeting compliance goals by enabling the creation of complete security reports and documentation to comply with the rules. By means of powerful reporting features, this type of systems enables the organizations to demonstrate the compliance with the compliance rules and within the industry best practices (Thomas, 2018).

A SIEM system workflow that consolidates the components together is a good move that would help the security team to perform their work easily and at each stage of architecting cyber defences from detection to response on security threats.

3.6.2 Benefits of SIEM

SIEM systems offer a multitude of advantages that enhance a company's network security posture. SIEM systems offer a multitude of advantages that enhance a company's network security posture:

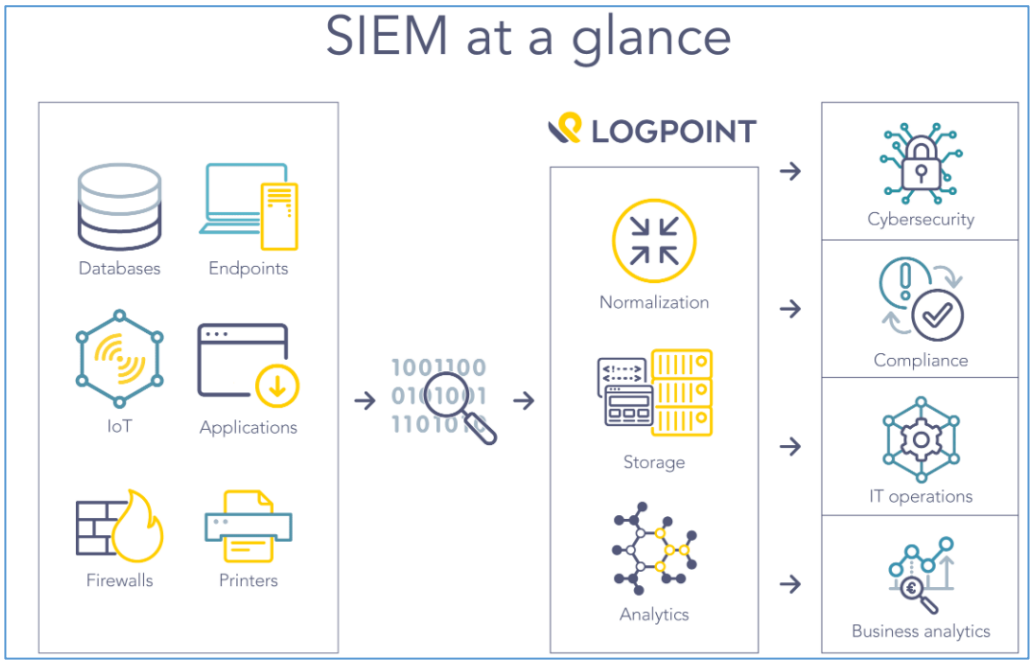


Figure 8: High level SIEM workflow

Source: https://www.logpoint.com/en/what-is-siem/

1. Centralized Visibility: SIEM systems, as the name suggests, resume this function by combining and analyzing security events and network activities from different places. Through the means of collecting the data from many endpoints and security devices, the SIEM system is responsible for the business giving full visibility for the users of the system, the events of the system, and the possible security risks or threats to the network (Thomas, 2018).

2. Early Threat Detection: By incorporating advanced correlation algorithms and analysis techniques SIEM systems provide real-time monitoring for any emerging threats. SIEM systems carry out that by inspecting the network traffic, the log data etc. they can find the exceptions which otherwise remain unnoticed which are indicative of the attacks or something which has been breached. This critical ability of early warning sign detection enables organizations to send out warnings in advance of actual danger, giving organizations time to implement prevention measures that can be used to reduce the risks earlier (Thomas, 2018).

3. Efficient Incident Response: SIEM systems act as key pieces in an expedited and guided incident response by declaring alerts, notifications and automated workflows. For a security team empowered with SIEM, the rapid identification, probing, and reporting of security anomalies allows the organization to respond and minimize event-related cost, disruption, and exposure (Thomas, 2018).

4. Compliance Adherence: SIEM systems simplify compliance efforts regulating reputation by examining collected and analysed security-related data to generate detailed reports demonstrating compliance with security legal standards and norms. The declaring of breaches of security flaws or threats through the automation of processes of auditing and monitoring is

therefore a form that is assisting organizations to meet the requirements of security regulations and avoid the possibility of penalties (Thomas, 2018).

5. Threat Intelligence Integration: SIEM systems can gain a new dimension in their detection of threats by providing the external threat data feeds. The utilization of these supplementary resources in security, such aids in rapid response to emerging threats and vulnerability, and encourage the organization's proactive threat mitigation. This eventually help in boosting the security posture of the organization (Thomas, 2018).

Overall, SIEM systems are an important part of the network security which allows having all events in a single place, finding threats in the network long before they may cause damage, reduce the time period when the operators must respond, integrate organizations' data with external sources about threats to know potential danger better and sooner. SIEM systems are the means for the organizations to build a solid wall and defense against advanced cyber threats through keeping the assets protected digitally.

3.6.3 Challenges in SIEM Implementation

Implementing and managing SIEM systems can be fraught with challenges that organizations must overcome to effectively enhance their security posture. Implementing and managing SIEM systems can be fraught with challenges that organizations must overcome to effectively enhance their security posture:

1. Data Overload: SIEM systems are actual subject to the flood of data as they manually gather data and then analyze the information in form of datasets. The high volume of data is the main concern that makes it difficult to determine whether the threats are genuine in the sense of outstandingly suspicious situation or simply noise coming from the regular activities and the process of sorting out the most significant security concerns becomes more complicated (Thomas, 2017).

2. Data Consistency and Accuracy: SIEM systems feed on procurement and utilization of data with sufficient accuracy and consistency for proper analysis and correlation. Ensuring of exact data normalization other than the data format celebacy may be impossible to achieve, which can influence the reliability and accuracy of the security insights from the SIEM platforms (Thomas, 2017).

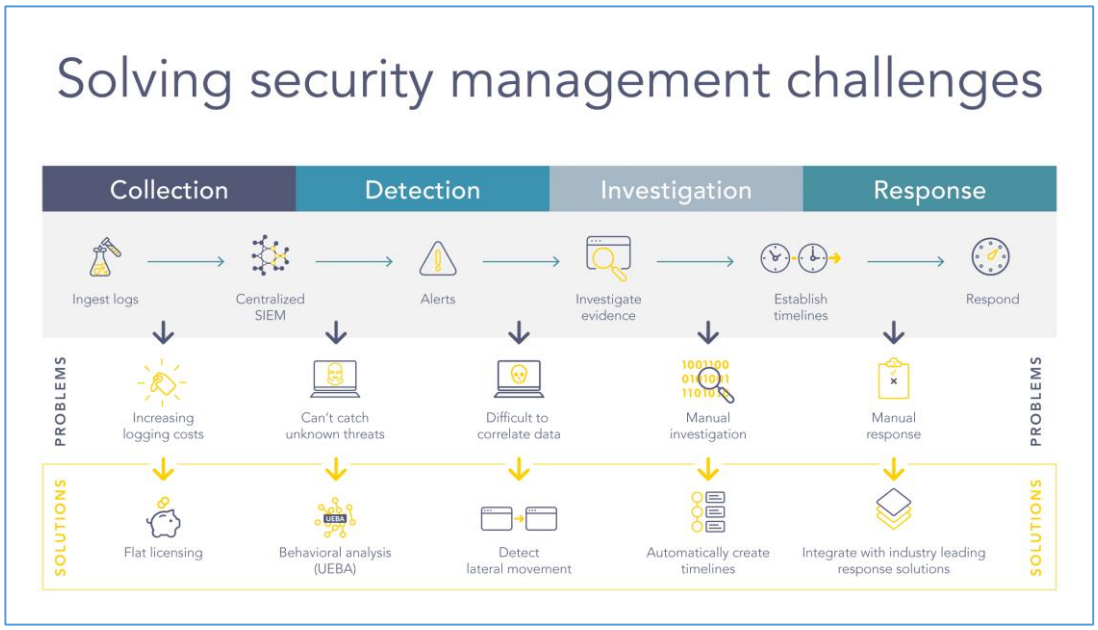


Figure 9: Workflow of security management challenges

Source: https://www.logpoint.com/en/what-is-siem/

3. False Positives and False Negatives: SIEM solution could be resulting a tremendous amount of the so-called false positive signals, therefore that could lead to the alert fatigue and can make difficult to detect the real security threats. However, the path of overstressing the reduction of false positives may mislead to problems of false negatives when the cases with security concerns pass unnoticed. Finding the balance between no false alarms and not missing out on the main targets while being challenging at the same time can easily make it even harder (Thomas, 2017).

4. Expertise Requirements: To benefit the most from using SIEM systems, one needs a professional who can be in charge of pointing out security

breaches, finding their origins, and fixing the complaints made by the user through a monitoring process. Organizations have to give priority to it in their hire and training process of highly skilled security person to get maximum advantage from SIEM investments (Thomas, 2017).

5. Scalability and Interoperability: SIEM technology should be scalable for expanding to a variety of network and security devices that rg and applications may be used. Interoperability and scalability could be the greatest problems arising from difficulties in expansions of the network and any other changes as technological development is not easy to predict and it requires careful planning and resourceful allocation for trouble-free operation (Thomas, 2017).

Organizations can become more confident in SIEM implementations by pinpointing these challenges, thereby elevating their level of detecting and responding to cyber threats. The security of an organization's digital assets and infrastructure can be expanded with investment in the resources of cutting edge data management practices, experts' development and scalable infrastructure that will provide the full power of SIEM systems.

3.6.4 Future Directions in SIEM

As Security Information and Event Management (SIEM) systems continue to evolve, future research and development efforts should focus on several key areas to overcome challenges and enhance capabilities. As Security Information and Event Management (SIEM) systems continue to evolve, future research and development efforts should focus on several key areas to overcome challenges and enhance capabilities:

1. Automation and Orchestration: Seek automated increase of SIEM and the degree of orchestration to make easier security tools coordination and quick execution of an incident response plan. The SIEM systems are able to do such things as automating the daily routine tasks to orchestrate complicated processes. This way, SIEM systems bring an efficiency

improvement to the process and also reduce the response time (Murdoch, 2018).

2. Advanced User Behavior Analytics (UBA): Additionally, CIO today will look to incorporate more enhanced UBA functions via user profiling, anomaly detection, and behavioural modelling for SIEM systems so they can be able to identify the key indicators of insider threats and other unknowing suspicious activities. SIEM systems can recognize human pattern activity, and this way identify possible undetected risks related to internal breach originating from within the organization (Murdoch, 2018).

3. Cloud Security Monitoring: Adapting to cloud-based system, SIEM has to be in a position to completely cover cloud-based platform and infrastructure to ensure their security at the same time. The real-time threat detection capability should be leveraged also for cloud environments and this ability to cover a hybrid and multi-cloud deployments is a lot essential in this connection as this gives comprehensive security coverage (Murdoch, 2018).

4. Threat Intelligence Integration: One of the SIEM systems' merits is that it can provide a powerful study of cyber attacks due to its capability of integrating threat intelligence feeds. That's where the SIEM systems come into the picture as they allow for the monitoring of real-time threat data. This way, they can be proactive in correlating the emerging threats, such as the zero-day attacks and the unidentified risks (Murdoch, 2018).

5. Data Privacy Preservation: The major challenge today is that of balancing data security and quality of privacy during penetration testing to prevent data breach. The data privacy guideline is yet one of the important future SIEM system requirements. The systems should be able to implement privacy protecting strategies; they should also comply with the requirements of regulators and safeguard sensitive information during both, monitoring and analysis process (Murdoch, 2018).

Through these areas of emphasis, Smart Information Monitoring systems can be more accurate, intelligent and more effective in keeping network protected thus ensuring they safeguard security of network. Analytics, automation, integration, and privacy preservation technologies will benchmark the continuous innovations in SIEM solutions, thus, to help the organization defending against the new cyber threats.

3.7 Challenges and Future Directions

As for the sector of network security, the challenges are abundant and the most prospective ways to move on seem to emerge in this area. The risk comes from the fact of how intricate modern computer networks are and the speed at which cyber threats emerge and change at. It is very difficult for the people who fight this fight. As in many areas, issues like data overload, encryption, false alarms, and cadre of experts present obstacles to the successful replication of measures. These are the challenges. Yet, these new technologies, such as artificial intelligence, machine learning, and those generated in the cloud, suggest good possibilities. And in the other direction the network security will be developed by automation, true intrusion detection, and better cryptographic processes. Through addressing these weaknesses and implementing preventive fields, the organizations become strong and resilient competing in an inter-dependent cyber environment (Nguyen, 2018).

3.7.1 Difficulties in Keeping Track of Networks

While ensuring secure monitoring for networks is essentially cumbersome as technology advancements and the complexity of networks are, it is still a non-trivial undertaking. The list of contributing factors that lead to the complications of network activity includes cloud computing, virtualization, and the top-spin of IoT devices. Security measures need to be coupled with the ability to adapt to various endpoints, channels of communication and design of infrastructure architectures in order for them to duly control and track network activity (Nguyen, 2018) .

Cyber-attacks are being carried out through advanced persistent threats (APTs) or polymorphic malware which keep on developing, making the issue of keeping the security of network systems even more critical. Timeworn signature-methodology

could be proven to be not strong enough for zero-day attacks and unidentified threats, therefore, it becomes important to apply up-to-date process which can include for instance anomaly detection or behavior analysis to enable real-time threat detection (Nguyen, 2018).

The previous growth in the number and quality of network traffic will require highly efficient data processing and analysis to identify and respond in such a short time when threats occur. Scalable security solutions are currently considered to be a prerequisite to the effective control of the increasing volume of network traffic together. Yet, the question of privacy and conformance to legislation arises when data is collected and analysed through network access. The delicate task of balancing stiff security measures whilst still respecting private user information constitutes well-followed rules and guidelines (Nguyen, 2018).

The challenges discussed above should be taken into account by any network security implementation for the future of network monitoring landscape to be constant.

3.7.2 Future Directions in Network Monitoring

To address the challenges in network monitoring and enhance its capabilities, future research and development should focus on several key directions. To address the challenges in network monitoring and enhance its capabilities, future research and development should focus on several key directions:

1. Intelligent and Adaptive Security Systems: The combination of AI and machine learning techniques in recognition of systems will enable them to keep past records, discover patterns and foresee threat to come. Adaptive security mechanisms can be adjusted to change and redefine current network environment and their dynamics that have to be in harmony with changing security problems (Choi et al., 2011).

2. Integration of Threat Intelligence: Intelligence threat feeds is a tool that allows to perform security audits in a more precise way through network

monitoring and proactive threat hunting. Sharing monitoring and anomaly data externally with threat intelligence services provides a feed of information which in turn makes prevention and response more efficient (Choi et al., 2011).

3. Automation and Orchestration: Automation and orchestration will improve the speed of turning on repetitive tasks, enhancing title duties of security specialists and also reduce considerably their workload. The infusion of security orchestration, automation, and response (SOAR) technology complements the expeditiousness of event responses and grants the privacy solutions the ability to collaborate (Choi et al., 2011).

4. Enhanced User Behavior Analytics: Developing more sophisticated behavior analytics approaches with ML and AI assits in the detection of such behavioural deviations and security risks with a greater precision and accuracy. Upgraded UBA tools intelligently identify fake or compromised IDs and help the system arrest the insider threats effectively (Choi et al., 2011).

5. Integration of Network Segmentation: Sophisticated network segmentation algorithms on the other side are smart enough to keep an eye on network fluctuations and even then complete information exchanges across network compartments without compromising the whole network. The investigation of ways of network segmentation can also be regarded as a means of increasing the network security as it reduces the general impact of possible network vulnerabilities (Choi et al., 2011).

6. Privacy-Preserving Network Monitoring: Importantly, research on the non-intrusive way of network monitoring through the cryptography, anonymization, and differential privacy purposes that do not compromise users' privacy is essential to enable detailed analysis of the network data while simultaneously protecting users' privacy (Choi et al., 2011).

7. Cooperation and Information Sharing: Raising the level of cooperation and transparency between businesses and security service providers is a useful approach to deepen the level of network monitoring. Network attack response is developing guidelines and tools for a secure information exchange and collaborative threat analysis that leads to a more proactive approach (Choi et al., 2011).

An ethical network monitoring can be significantly enhanced by taking advantage of these opportunities, to prevent emerging cyber threats and counteract against anything new. Utilizing latest technology, automation as well as associate elevation can make the network security reinforced and effective.

3.7.3 Opportunities for future advancements in Network Monitoring

The fact that networks are complicated systems with advanced cyber attacks able to react in real-time, the scalability requirement along with the privacy considerations which comes with customers' expectations in a digital society makes network monitoring a task requiring great skill. While it is a huge challenge to keep updating the system, the future developments of the system also bring about these opportunities. Through smart and adaptive security solutions, utilizing threat intelligence, process automation and standardization, advanced user behavior analytics, network segmentation, consuming a little privacy but being transparent, teams of network management should be included into overall security schemes, and cyber threats will become a thing of the past. Next research direction includes the discovery of approaches to the given challenges and also exploring prosperous routes to the future network monitoring to strengthen its security position (Choi et al., 2011).

3.8 Future Directions in Network Monitoring

Network monitoring is a very powerful tool for network security experts as it helps them to respond quickly to threats and attack. Therefore by applying intrusion detection systems, network administrators are able to react immediately to various threats and attack vector. The advent of new hazards while technology is progressing at an accelerating rate, research into the network monitoring of the future for increased performance becomes necessary. In this article, several research fields which are

considered as the most critical and have the capability to break into establishment of network monitoring are reviewed (Blokdyk, 2018).

3.8.1 Advanced Analytics and Artificial Intelligence

Avanced analytics and AI (AI) tends to pioneer new ways in network monitoring through proper and accurate monitoring. The machine learning algorithms can be applied to large-scale data breaches from the background to detect the trends in historical data indicating of any threat. Also, the predictive role of AI-empowered analytics will turn out to be paramount in proactive anti-data breach efforts, as it discloses and eliminates security risks prior to their escalation. Approaches as the anomaly detection and behavior analysis supported by AI can enhance the role of network monitoring systems and hence the research-based decisions on thwarting the malicious activities. The progress in AI and Machine Learning is critical in the development of unique types of network security, and creating segmented networks beyond current available security inventions that will ensure comfortable transition to the emerging security concerns (Maleh et al., 2020).

3.8.2 Network Behavior Analysis

Network Behavior Analysis (NBA), is an invaluable [tool] which helps the network monitoring to identify both usual [and] anomalous functioning patterns which is evident through the network activities. In network monitoring innovations of the future, priority must be given to improvement in the NBA features in order to allow much shorter response time when it comes to detection and addressing an emergent security issue. It is possible to take this even further through combining anomaly detection and machine learning approaches with conventional scoring rules. Additionally, the authors argue that ultimately, the need for in-depth studies about the coordination with the other anti-hacking systems like IDS, IPS should also be considered in depth. This integration would be helpful in the network outage comprehensive understanding of network activity and facilitate faster incident response and direct the responders to the best places. Through the development of about NBA instruments, taking into account contextual data, users' actions and network structure, the accuracy and efficiency of a network monitoring can be drastically improved (Maleh et al., 2020).

3.8.3 Threat Intelligence Integration

The network supervision progress is connected to the quest to outlay NBA techniques. Such methods allow chip professionals to take a deeper look into the network operation processes, both normal and irregular, which in turn help with on-time danger detection and prevention. In order to do this, combine the quality of anomaly detection and machine learning with traditional rule based techniques. In addition, I too think that the studies related to the combination of NBA with other security protocol like IDS, IPS and SIEM is a necessity. Through this holistic approach, a deeper understanding of network activity will be developed and incident response will be speeded up, which is another characteristic of this solution. The data-driven and context-based strategies of network monitoring may lead to improved accuracy and efficacy once previously complex threats are identified and dealt with (Maleh et al., 2020).

3.8.4 Privacy-Preserving Network Monitoring

As the privacy issues of data getting more and more relevant, this obstacles future progress of network monitoring should be based on findings ways to balance security and users privacy. Reasearching should identify the methods by which both privacy rights and network monitoring are enabled, but at the same time the systems ought to be developed either effective or unobtrusive. Techniques like encrypting data, secret keys applications and more can be adopted to achieve these goals. Besides, the implementation of user-oriented network traffic monitoring regimes, where users have dominant role in their data personal activity and legal liability for their data privacy is very important. Through observing the individual privacy choices and the clearce company dealing with the data usage, there can be mediation of confident between the business and the users. The enhanced trust eventually leads to better network security (Maleh et al., 2020).

3.8.5 Cloud-Based Network Monitoring

A growing number of organizations have substantially relied on cloud computing, which has led to the emergence of some issues related to network monitoring for instance, in this regard, the development of new methods to answer the

demand for the dynamic resource allocation, virtualization, and multi-tenancy has become paramount. The prospective studies should focus on design of the mechanisms network monitoring system that is specialized in the sense of its capability to perform an efficient intrusion detection and prevention of breach of cloud-based infrastructures and apps (Maleh et al., 2020).

The network monitoring framework would be much more effective in the cloud seamlessly integrated with client-side hardware securing the endpoints and the cloud administration. Thereby, a similar type of platform can be used to sustain the successful implementation of cloud-level security services (Maleh et al., 2020).

It is cloud-based network monitoring services reducibility, scalability and real-time data analysis capabilities that makes them efficient and effective. Stand-out necessities are the capacity to ensure seamless integration with on-premises security systems and making sure that the security will stand the pressure of the cloud environment. Through cloud-native augmentation for monitoring mechanisms, organizations can give them the security cover they need for their cloud infrastructure (Maleh et al., 2020).

3.8.6 Collaboration and Information Sharing

Since network monitoring is being refined, partnership and information sharing between corporates and security businesses will accelerate to the extent that they will be more productive in the battle against cyber security risks. Developing safe, interoperable functionalities for traffic data exchange and joint threat analysis incorporations into monitoring network should be an important focus. Organizations can provide the necessary know-how about security practices and share the information about a threat and partners on the threat intelligence. As a result, businesses can become ready to and respond more effectively to the emerging threats (Maleh et al., 2020).

Efforts of harmonization should be directed at the development of common data formats, exchange methods and interoperability standards of information exchange to provide a safe environment for the transfer of sensitive information. Such data formats

should be simple so that it becomes faster and easy for the secret information to flow around. Not only do we need to secure possible and non-privacy breaches, it is also crucial to investigate privacy-preserving mechanisms of mutual cooperation to facilitate information exchanges, and help us in the fight against sophisticated threats (Maleh et al., 2020).

Ultimately, the future of network monitoring will make use of new methods of learning, artificial intelligence, and data analytics that will be used for threat detection and incident response As well, the analysis platform should continue to be tackled through development efforts which focus on evaluating network operations, integrating threat data, retaining safety of users privacy, and observing cloud networks. Through promoting partnership and information sharing, companies can improve their network security imperunes thereby making certain that they are always ahead in countering the evolving threatscape and saving all user information from unauthorized breaches (Maleh et al., 2020).

3.9 Summary and Research Gap Identification

Network security gets thumbs up being highlighted as an effective solution to ward off cyberattacks, which points to the absolute necessity for strong monitoring systems to ensure data security. While empirical data on the outcome of network surveillance has some gaps, there are nonetheless some benefits and disadvantages of such monitoring practices.

3.9.1 Summary

The security of base of expanding networks is becoming more and more critical as it has to safeguard against attack from malicious cyber attacks. This research paper focused on the criticality of network security and explored how an unauthorized use and cyber attack can be easily overcome with the help of network security. The course of practical investigations into different security systems brought about the realization of their strengths, weaknesses and perspectives for further development. For instance, analyzed data from the networks passes through thorough screening to help out in identifying irregularities, vulnerabilities, as well trends that are future-oriented. Machine learning is almost one of the best solutions for solving the problem of fast

growing data in networks. Machine learning algorithms allow analysing large data volumes in a short time and detecting behavioural patterns suggesting security breaches. Furthermore, IDS/IPS systems are as significant as they are tasked to detect suspicious traffic in the network before it leads to a breach. The internal networks hold data within highly fortified boundaries that can be monitored centrally, where incidents are responded to swiftly as per the regulations.

3.9.2 Research Gap Identification

Several areas within network security research present opportunities for further exploration and development. Several areas within network security research present opportunities for further exploration and development:

1. Advanced Techniques in Network Traffic Analysis: Developing advanced methods of scanning and analysing the traffic on the network is vitally important in the continuous improving of the means of threat detection, since cyber threats are quickly changing and are growing in numbers.

2. Integration of Diverse Security Measures: The time has come for the research that will be combining (or meshing) different software and hardware security solutions in order to have the network secured in all times and the devices able to function in compliance.

3. Real-Time Threat Detection and Response: While studying for the future, researchers should try to develop a technology that can reliably detect and deal with cyber threats immediately, relying on automation, machine learning, and advanced analytics to handle incident mitigation quickly.

4. Ethical and Privacy Considerations: Furthermore, efficient measures i.e. encryption and anonymization techniques, need to be taken into consideration, if the ethical and privacy issues in the network data collection and analysis are to be resolved, and user privacy rights are maintained without the undermining of security practices.

5. Standardized Evaluation Frameworks: Implementing the evaluation frameworks and metrics that are standardized is the key to properly assessing the utility and speed with which security measures are applied, which in turn contributes to the data-driven decision making and the comparing of the actions of one organization with another.

6. Integration of Human Expertise: Attempts to create a union between human knowledge and intelligent security technologies by developing interfaces and decision assistance systems will also accelerate efficiency and response capabilities to achieve a higher degree of network security.

The enumeration of these research gaps will provide a strong basis for network security procedures, making them impermeable to the assault of new threats with the observance of not only ethics but also privacy of everyone.

4. Practical part

The hallmark of the present chapter is the focus on the implementation of an advanced security solution within the banking sector network. In this regard period the Course will cover theoretical background and a critical evaluation of the importance of network security systems to the banking firm.

4.1 System Architecture

The preceding chapters dwelt on the theoretical aspects, the significance of networking in a banking context and the multitude of issues a comprehensive network management system faces. Here we put into practice the proposed solution, as we go deep down to the grains and details of it to be applied as a network component of an actual financial society.

Given a myriad of security processes which are meant to protect the network infrastructure and keep track of network actions, there is a need to develop a system which will be reliable in terms of security. The scope of this section encompasses the stages of developing a system for network monitoring and security comprising of different points to ponder.

It is not uncommon to see a concept for a network monitoring security system that consists with different parts and functions that allow your to perform the specified tasks. The basic make-up, components, and characteristics of such a system are briefly outlined in this article:

The basic make-up, components, and characteristics of such a system are briefly outlined in this article.

Structures

- Agents and sensors
- Layer for Data Collection and Analysis
- Analysis and Processing Layer
- Reporting and Visualisation Layer
- Mitigation and Response Layer

4.1.1 Network Sensors

They are placed in point-to-point communication routes between different points of the banking system to ensure that data is collected and analysed on the move. Network data packets communicating through sensors are picked up and examined, which sends an alarm any time anomalies or risks are noticed by the sensor system.

4.1.2 Centralized Monitoring Server

The courtesy server acting as the optic nerve commits the data from the restaurant to the central nervous system. As soon as there is some movement in a secured area cameras high definition camera feeds and voice over signals are activated for the security team based on network sensor obtained sensors data. Another function that is performed by the server is to store information that could be needed to be retrieved, analyzed, and reported at a later time.

4.1.3 Intrusion Detection System (IDS)

Virus and intrusion detection is done by IDS systems that examine data packets as they travel over the network, and other unauthorised accesses via machine learning and systems similar to rule based systems.

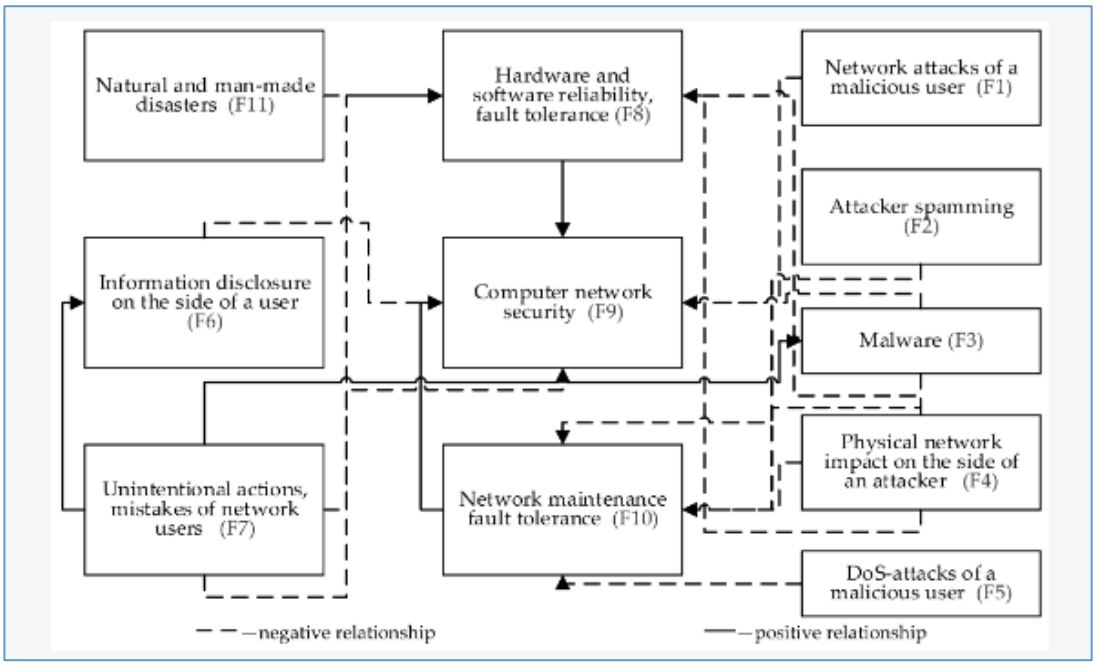


Figure 10: Overview of IDS

Source: https://www.sciencedirect.com/science/article/pii/S219985312200021X

4.1.4 Firewall

The bank highly protected its internal network with the help of the firewall from the outside dangers. It stops the data packets that is either coming into the network or going out based on the rules applied for security. These data packets which are unwanted or not admissible for the network are being prevented.

4.1.5 System for the Management of Security Incidents and Events

The security information event management system combines data from different security sources into single, common picture. The sources of that information may include network sensors, firewalls, intrusion detection system (IDS) and so on. Helpful also to network security analysts who have the picture of whole network security which gives them opportunity to detect easily and to remove the weak points.

A business can monitor its networks in real time and respond to any possible security issues on the fly as they emerge.

Figure 11: Splunk login dashboard

Source: Author

Let's take a look at how logs are set and transmitted, as well as how Splunk monitors them, along with the architecture of the system, its components, and the capabilities it provides. Let's take a look at how logs are set and transmitted, as well as how Splunk monitors them, along with the architecture of the system, its components, and the capabilities it provides:

Splunk Architecture:

Splunk provides a functional framework with the ability to distribute and extract large number of unstructured data set such as logs and events to system's operational data. This paragraph covers the organization fundamentals of Splunk and explains what are they.

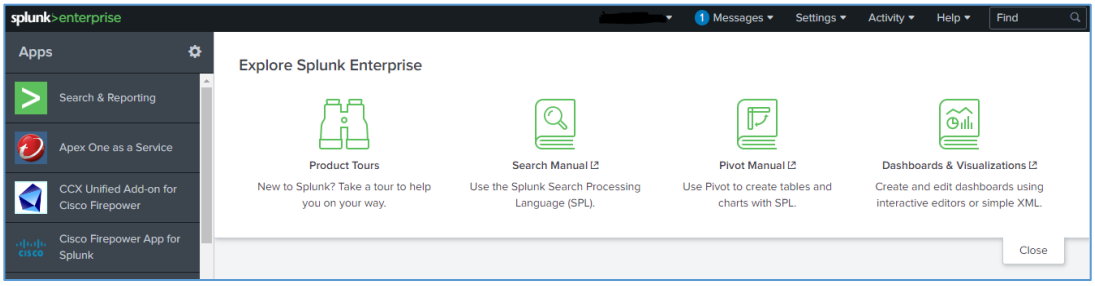


Figure 12: Splunk user dashboard

Source: Author

Data Collection: Splunk refers to an array of methods which data can be mined, and among these are:

Splunk Universal Forwarder is a low-resource data collection agent, very suitable for installation on source machines or computers. The traffic goes to the network through the forwarder and arrives at the indexer with the data in an encrypted form.

It is worth noting that Splunk can be set up to receive log data via the standard syslog method. Splunk can receive logs from its sorce devices through syslog forwarding setting.

Splunk's in-built connectors provide a window of opportunity to feed practically any data source that could be say, a database, an app or a networked device that makes use of the cloud for storing data. These bridges super power the data by enabling the processes to be done independent and without any help.

Splunk may automatically capture any new log data, that are being generated in a group of files or directories as the monitoring system aimed to detect any modification takes place in that group.

The indexing and storage layer of Splunk recognizes, undergoes processing and storage the data. It is composed of the following parts. It is composed of the following parts:

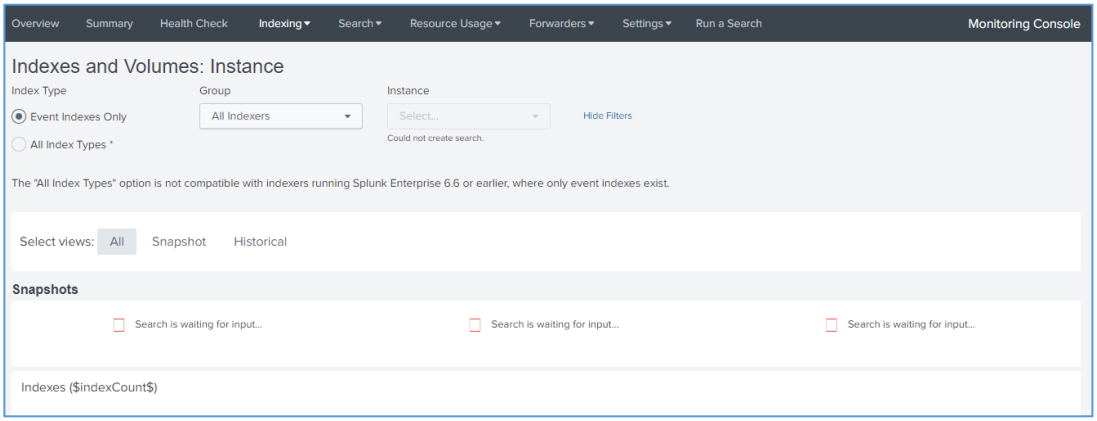


Figure 13: Splunk indexing

Source: Author

Indexers: Indexers take data from collectors, ‘storing’ it out, ‘categorising’ it and ‘indexing’ it for future reference. The brain has a very high speed to go through incoming data, single out relevant bits and then stow them into areas of long-term memories. The subject of data retention rules includes holding some data for a given amount of time, which falls to the indexers as well.

Splunk places the data into indexes for easy access and stores them by putting them in “buckets” or logical groups related to each other. Secondly, time and an index are key drivers to sort events and the data stored in buckets are tried.

Multiple Splunk instances can be connected together by clustering so that the machine is available all the time, downtime is decreased, and scalability is improved. Instead of using a single node for data indexing, clustered indexers group data over several nodes thus improving lookup and retrieval time.

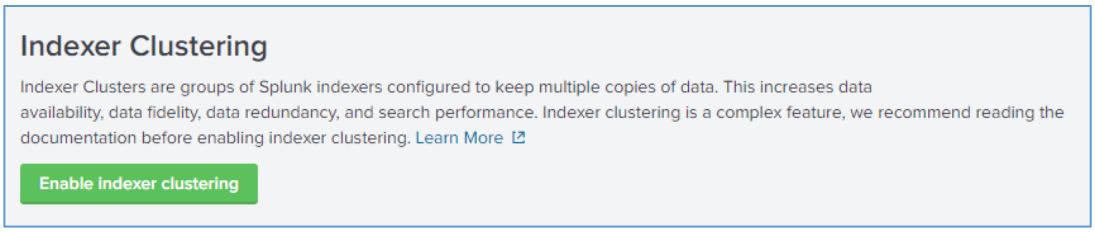


Figure 14: Splunk clustering

Source: Author

Index Replication: As example, a failover indexer in a cluster is configured such that if indexer A fails, then it will mirror data from it onto indexer A.

Splunk's tiered storage system allows customers to decide how they wish to classify their data in the structure as new, frequently accessed, or cold, i.e., based on the usage each level gets. Items belonging to "hot" data are stored in high-performance storage, while data of "warm" status is stored in medium-term storage, and the last category of "cold" data is archived in long-term storage.

Splunk's search and analysis layer provides robust capabilities for searching, analysing, and visualising data. Splunk's search and analysis layer provides robust capabilities for searching, analysing, and visualising data:

Search Heads: The look for the user-inputted item on the web is the responsibility of the search head, who then sends these results to the user afterwards. They can give an online UI to interact with the Splunk platform, which allow to doing a search and visualize data.

Splunk Basic Language (SPL) serves as the search functionality in Splunk. End users may craft complex queries, filter options, statistical analysis, a dashboard designer, real-time alerts and reports are all extracted.

Consult Your Peers: Work of the search load is an exemplification of that whereby multiple instances of Splunk distributed could achieve broadening search performance, search speed, and scalability.

Splunk offers multiple options of visualisation such as charts, graphs, topographies and dashboards to provide analysed data and search results in a way, which ranges from easy to understand to one that is also informative and visually appealing. Personal input tab and summary may be made using report generation functions in reporting tools.

Splunk's app and plugin ecosystem: Due to the architecture of Splunk that is adaptable, it can be changed to satisfy the unique needs of any user. There will be individual cases where you can use apps that have been already built for the Splunk platform, these tools include dashboards, reports, and workflows in their features.

Splunk’s architecture is flexible and scalable, making it possible for organizations to implement an efficient approach that involves collect, index, search, and analyze huge volumes of machine data. Implementing distributed nodes, maintaining updated indexes.

Data Ingestion and Log Configuration:

Next to common ruters, switches, active databases (servers), applications, operating systems, firewalls, and hardware; Splunk is capable of collecting data from a significant variety of other systems and devices. Common practises for configuring logs for ingestion into Splunk include the following:Common practises for configuring logs for ingestion into Splunk include the following:

Supply Chain and Inventory Management: Where do We Get Our Numbers? Determine which data instruments to use for logging purposes as well as which data sources that will be reliable for security tracking. The logs may be created in several different forms, for example, Syslog, Windows Event Logs, API data, databases logs and logs created by the end-users.

Techniques for Gathering Logs: Determine the best way of transferring logs from each source that soaks up your time as well as effort. Splunk may draw data from various sources such as Agents (Splunk Universal Forwarder), syslogs, files, and API connections.

Enable Splunk to work together with your different data repositories and perform the log forwarding. The purpose of this step is to monitor the log files and you can configure Syslog or logfile inputs for the source devices.

In order to process and recognize the logs' information, users of Splunk make use of the prop.conf and transform.conf configuration files, respectively. Produced by customizing the settings, the potential of Splunk to run index and probe logs based on their structured formats could be enhanced.

Log Forwarding and Indexing:

Once Splunk is configured to be passed the log data then Splunk it will index and analyse this data. Scroll down or click next below to get the step-by-step instruction for the following procedure.

Transmitting Logs: The most common ways in which logs can flow into Splunk include via an ingest pipeline, webhooks, the API or using application-specific signatures. While Splunk Universal Forwarder is sent to source Devices to transfer logs to Splunk indexer once they have been deployed there. latter could be also employed through source API or syslog support.

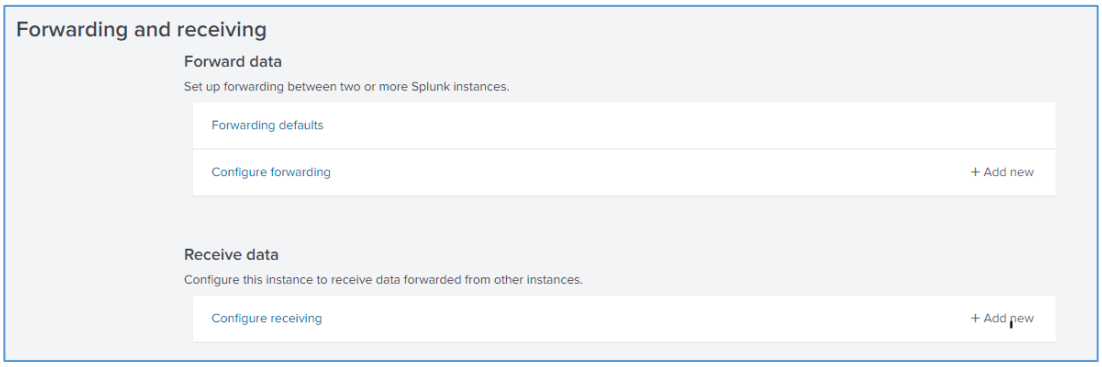


Figure 15: Splunk Forwarder

Source: Author

Indexing: Splunk actually saves logs after adding them to the pipeline by indexing and keeping them in an efficient manner. Searches, processing of statistics, and correlation of the logs may be accelerated by indexing the logs. In order to identify and collective enormous maxes of logs and maintain the scalability of Splunk, indexes are have to break down into and pass the partition information to several indexer.

Metadata Extraction: At the time of indexing, Splunk retrieves log fields and stores them with other metadata. The dates and times, user address, and event type are all metadata components. Metadata helps discoverability and leads into investigation, further studies.

Monitoring and Analysis:

After logs have been ingested and indexed, Splunk offers a number of tools for the monitoring and assessment of security incidents, including the following. After logs have been ingested and indexed, Splunk offers a number of tools for the monitoring and assessment of security incidents, including the following:

The Security Aggregation Language of Splunk allows security professionals analyse and investigate the logs in a Splunk environment for a events, patterns, and vulnerabilities. This ensures that getting the information you need is now much easier thanks to the fact that you can look stuff up and inquire about what it is. In order to gain understanding, log data analysts might need to execute deep data research and then make use of various operators, functions as well as statistical instructions.

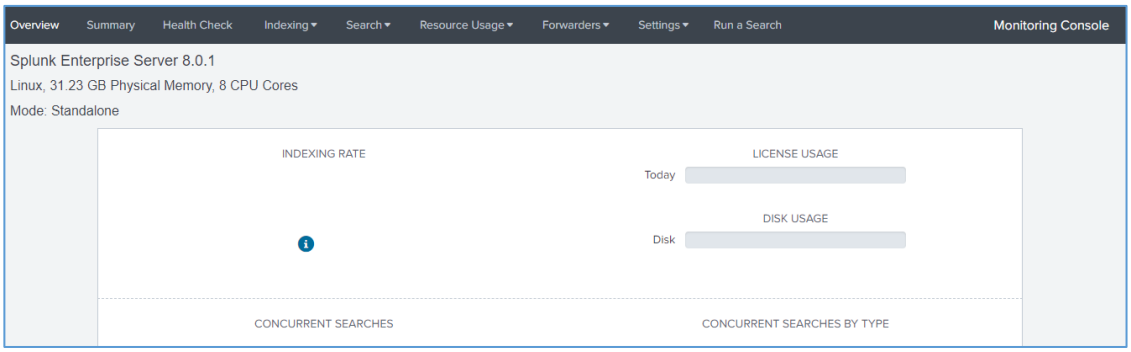


Figure 16: Splunk monitoring storage view

Source: Author

Real-time Monitoring: Splunk through its real-time monitoring system is always on and absorbing log data as soon they are being created. Security bosses engage in proactive identification of security incidents and quick response times by setting up alarms and throwers on basis of patterns, threshold breaches, and anomalies.

Splunk may however, look at its correlation and visualisation features and compare variation from different loggings, in an attempt to discover strange patterns. It can be presented as a desktop form as well as a mobile form, according to a client's preferences, providing analytical information through data visualisation, such as charts, dashboards, and graphs, which are interactive also.

Attacker activity logs may be marked off with more descriptive information about the attackers such as threat gauges, IOCs (indicators of compromise), or malicious IP addresses, if Splunk is integrated with other sources of threat intelligence. This capability of the SIEM system has now been further enhanced through the integration and coupled with the responsiveness of the system to security threats.

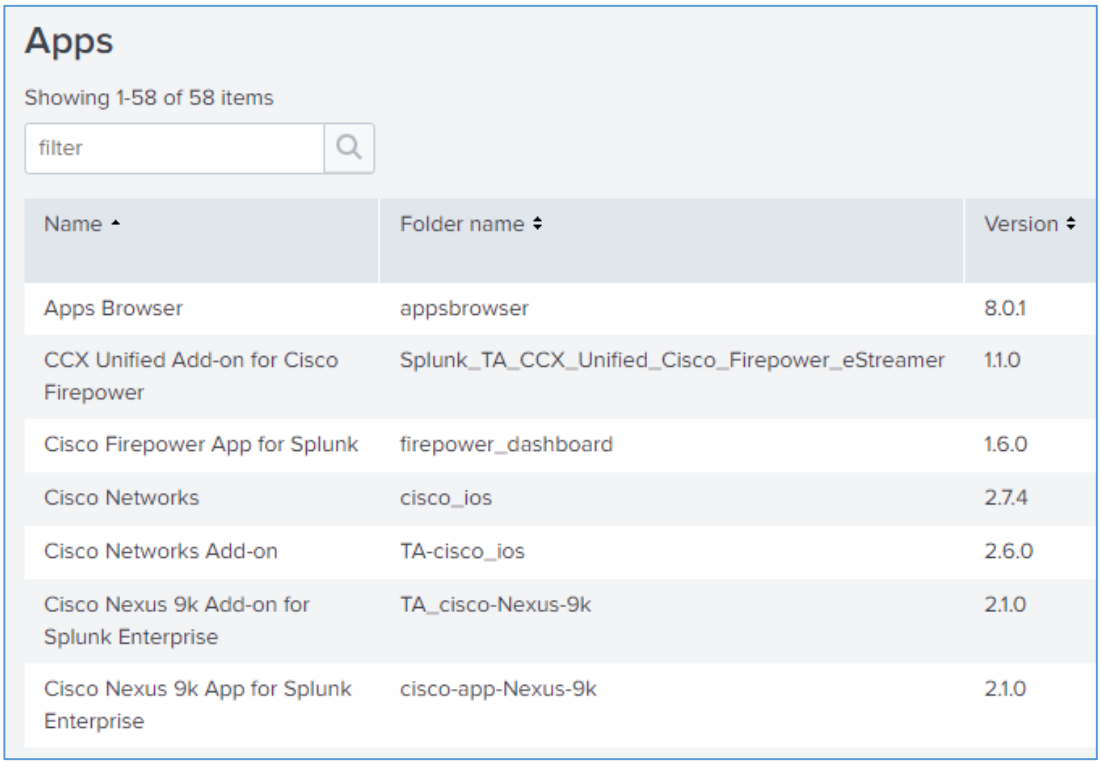


Figure 17: Splunk apps

Source: Author

Splunk is aimed to aid you in sustaining regulations, monitoring legislation, showing the evidence that you are using the best security practices and so on by the reports generation. The report building feature is outfitted with compliance modes and custom templates so you can get ready-made reports based on your business's compliance requirements.

Splunk has ML capabilities that discover insights in the firm's data as well as user behaviour analytics (UBA) that help in locating threats that weren't apparent before. Machine learning fed algorithms for monitoring any suspicious activity may list out any danger and provide warnings in the wake of it.

A wide selection of extensions as well as third-party apps are designed for Splunk expansion and development in specific areas. Solutions include the application-based options, such as Splunk Enterprise Security (ES), normally crafted for ease of use with protected security use cases, dashboards, and correlation searches.

Splunk Apps and Add-ons

Thanks to its flexible and scalable structure, Splunk is the most popular choice for SIEM (Security Information and Event Management) system. This feature is desirable in providing security and incident response since it might process data from several sources, keep a close track of events on real-time, have a thorough search feature, and analytical techniques for data processing.

4.2 Implementation Steps

Planning of building a security system for network monitoring has to be done in the sequence of organizational security needs, regulatory statements as well as operational purposes. These two, Planning and RQ gathering, the most important stages of the implementation among others are discussed in this stage.

4.2.1 Planning and Requirement Gathering

Identification of Security Requirements:

Before the end of planning stage getting a detailed and elaborated knowledge about bank's safety inquiries is needed. It shouldn't be overlooked that it is necessary for all the participants to take part in the process, from IT experts and security specialists to compliance officers and top executives The following topics were discussed. The ability of education to lift individuals out of poverty and increase their earning potential cannot be overemphasized.

Risk Assessment For a proper risk assessment learn the different sources of danger, identify your own vulnerability, and estimate what might occur. There may be special guidelines put in place to guarantee everyone's welfare when this fact is known.

Demand for Operations Intelligence Familiarize with bank's needs in terms of Processing traffic, peak demand and critical tasks. Applying the understanding, the process of designing our monitoring systems further and the decisions on sensors placement can be intensified across the whole networks.

Determining Sensor Placement: The bank should utilize network sensors that are deployed across the network in critical locations to impede any attacks thus safeguarding the infrastructure. At this point, you'll be able to. At this point, you'll be able to:

Tracing Connections: Retrace the device back to the place it came from by requiring the age of routers, switches, servers and endpoint devices. Look out for the networks that information melt down to.

Network Footprint Analysis: Outline active areas by communities based on historical information. High-traffic regions should be well monitored and equipped with sensors which will position them for higher efficiency in detecting any unusual trends.

The Need for Market Segmentation and Defence of Key Assets: A good imperative is to determine the parts of the network that host the most crucial information, such as the clients' database and the statements of the organization. Installing detectors is an option for monitoring the traffic in and out the zones of observation.

Defining IDS Rules and Firewall Policies: We cooperated with technology experts and ICT technicians to come up with rules and directives for the detection system as well as firewall.

What we mean by "IDS" is "intrusion detection system:What we mean by "IDS" is "intrusion detection system:

- ✓ Define determined attackers patterns based on known cyber attacks history.
- ✓ Encompass anomaly detection level to distinguish between regular activity and malicious attempts.
- ✓ Create new defenses methodologies using machine learning approaches.
- ✓ Firewall Policies:

- ✓ Make policies which the firewall is supposed to understand and then refer to them when doing needful with connection requests.
- ✓ So, if you arrange the firewall rules so that you can guarantee that this communication can only happen the way it is documented under the umbrella of least privilege.

Resource Allocation and Budgeting: This will enable the purchase of new technologies, staff retraining, and continued upskilling. Sensors, network statistis servers, intrusion prevention tool, and firewall which provide a great security on the host vioring the budget very affordable.

Project Timeline and Milestones: Set out in detail an approach that is realistic and attainable during the term of operation, from designing to deployment and testing to ongoing monitoring. Make sure you know when the major milestones will be reached like sensors deployment, IDS software setup and full integration of the system. Choose one for every part of the process.

To perform the task of implementation (the operation issues, the standards of compliance and the security requirements) to be in fullest compliance with the bank's objectives, the bank closely scrutinizes the subject in question through performance inspect and checking standards. The monitoring process will be a source of information for the creation of a holistic system of infrastructure protection consisting of the network of client information and financial data.

4.2.2 Hardware and Software Deployment

In this part, we will look at the technical components that we need to set up for network sensors, an IDS(Intrusion detection system), firewalls, and a Centralised monitoring server.

Network Sensor Deployment

Without the inter-variables (sensors) a facility for the identification of the network traffic and its interpretation would not be possible. Here are the steps involved in a deployment. Here are the steps involved in a deployment:

Consider the junction of various network nodes as a central position here some investors may locate their priced investor, which are the center of their investments, can be found.

Installing Sensing Units: Employ traditional installing techniques to provide network sensors at key points. Therefore, mounting, rack mounting, or whatever option that is sensibly selected can be used. Check the power cords' distance and that the devices are all ready.

Make ready sensors to trace the intruder. Decide which of the protocols to monitor, pick the IP addresses to handle, and do the whole thing at the same time.

Centralized Monitoring Server Setup

Of the main points is server which has vital role with the monitoring tasks. First, it assesses information in networked sensor to depict situation. In order to set up a server, you will need to:In order to set up a server, you will need to:

System monitoring is impossible without corresponding physical parameters such as computing power, memory, and space of adequate capacity. High-speed central processing units, enough RAM for storing log data, and a large enough storage space, are examples of hard disk requirements.

Put up software to be runing on the computer, for gathering/storing the data, and monitoring things. MySQL and PostgreSQL are familiar names in the Linux database management systems.

Data Collection and Storage: Begin to find sensors and uplink to the server from the network. Design a way to store the traffic data both securely and operatively.

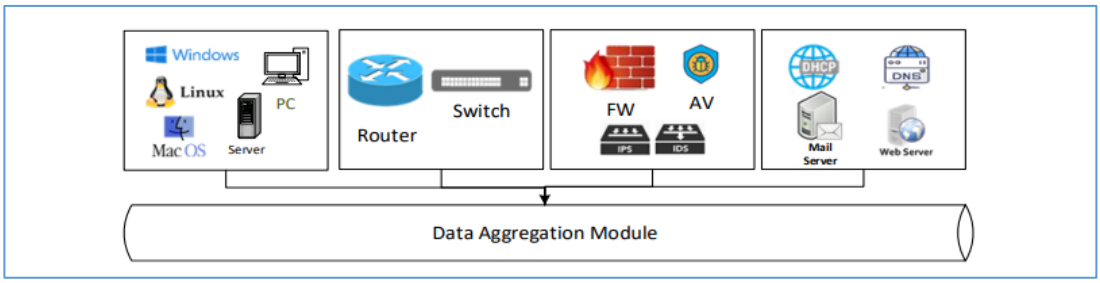


Figure 18: Data Sensor and aggregation overview

Source: https://save-aal.eu/wp-content/uploads/2021/03/DELIVERABLE_D.1.2-Sensors-and-Sensors-Networking-Description.pdf

Data Transfer Approaches:

Figure 18 shows how the Techniques of Pull and Nudge are used to feed the SIEM system which is described in the following paragraph. The route of this method is the one which/that data travels from its original source to the center of filtering.

Unlike the previous case, the SIEM solution tunnels the needed data to the data processing module. In Syslog client-server architecture, where the push mechanism is utilised, the client sends requests for data to the application server. SIEM system is hosted at this IP which will be the target of a master configuration file on the syslog client. Pull systems impede unauthorized access by employing password protected databases. SSL/TLS and encryption are mandatory for the use of AAA-compliant network protocols or for the SIEM solution. Ensuring safety and security by imposing more extra costs on individuals comes with greater fees.

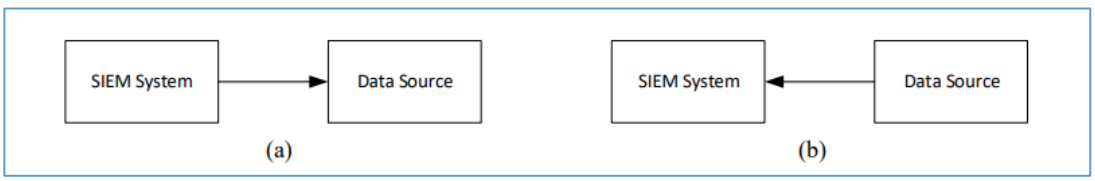


Figure 19: SIEM system with data source

Source: https://medium.com/wso2-learning/7-streaming-integration-patterns-with-wso2-9534d7f6bc93

Suppose that the system uses an IDS, or an Intrusion Detection System.

To generate data output and log activities run real time also you need anomaly detection system. There are many critical phases during the IDS rollout:There are many critical phases during the IDS rollout:

A New Programme Installation: For the purpose of thwarting the bank’s attempts, please use an IDS (like Snort or Suricata). Install an intrusion detection system (IDS) programme on your monitoring server as you do this.

The Limitations Will be Here The Goal Is to Keep the Demand-Side Management Within This Range Per such exemplary requirements, AI would detect abnormalities typically achieved through analysis leveraging on machine learning or based on the features of regular beating.

Firewall Deployment

Firewalls offer you a formidable obstacle that keeps away your network from a possible threat like hackers, and malware of malicious origin. Firewall setup requires the following:Firewall setup requires the following:

Picking Out Your Gadgets: Different types of firewall configurations are available including hardware-based and software-based. You may want to choose a suitable firewall based on the bank's very own network architecture and data transfer requirements. Make assure that the network can be expanded to accommodate new members.

Developing Procedures: Arouse a comprehensive set of firewall rules that would in charge of traffic inside your network. The bank's security requirements, for example, by using whitelisting to allow only required services and disallowing the known harmful IPs to, should be prescribed in the policies.

Verification and Examination: Every extensive testing should not be missed so that the firewall rules can work up to the design and not be the cause of any network

downtime. Make possible a range of checks in order to appropriately capture illicit or legitimate communications bypassing the regulations.

Lastly, all the pieces must be put together and the system be subjected to a series of rigorous prefinals or qualification games to ensure that it was performing as expected.

Streamline the communication and data sharing processes by connecting network sensors; then attach to the centralized monitoring server, Intrusion Detection System/Intrusion Prevention System (IDS/IPS), and firewalls.

Testing applications meantime through a huge amount of test cases to make sure their proper functioning is time-consuming and labor-consuming. It is advised to check about the validity of the IDS alerts, how extensively is the network traffic captured, and how monitoring the access control by firewall is done.

Individuals holding the role of a penetration tester deliberately make use of systems to determine any pivots of weakness that are present. This approach thus makes the system (i.e. individual and society) resilient to the real-world threats.

This turns out to be the main difficulty of network security in banks which is related to monitoring a bank's network with high security level. The bank adopted a considerate stance in network protection by applying firewalls, intrusion detection systems, a central monitoring server, and a network sensor.

4.2.3 Integration and Testing

Integrating, and testing is necessary when preparing to add a monitoring system to a network of a bank. Integration of the hardware and software components is no more essential than testing at this stage to make sure the systems will function properly, get the right results for the people and deliver all that is expected out of them. Therefore, in meeting the set requirement, we will include this here under the mentioned sections.

Integration of Components

1. Network Sensors and Centralized Monitoring Server Integration:1. Network Sensors and Centralized Monitoring Server Integration:

    - Shield sensor network operational link from a third party through encryption and secured channels to the monitoring server.

    - Set up such things as data collection and storage process from sensors data drawn from several sensors which all can be found in one space.

    - Perform data normalisation in order to ensure that sensor data will be displayed in the uniformed way.

2. Intrusion Detection System (IDS) and Centralized Monitoring Server Integration. Intrusion Detection System (IDS) and Centralized Monitoring Server Integration:

    - Take care that it is the IDS that is sending the warnings and the relevant data to the central monitoring hub .

    - Design an application programming interface (API) or interaction to make the IDS data share with the monitoring server as easy as possible.

    - Tie up IDS alerts and network traffic statistics by drawing each alarm to context of traffic.

3. Firewall Integration:

    - Join firewalls to the central monitoring machine for the purpose of regularly tracking and recording events, and rules.

- Set up the firewall to provide the data to the monitoring server and report to it occasionally.

- Design a monitoring platform for detected firewall events and strategies that are enforced.

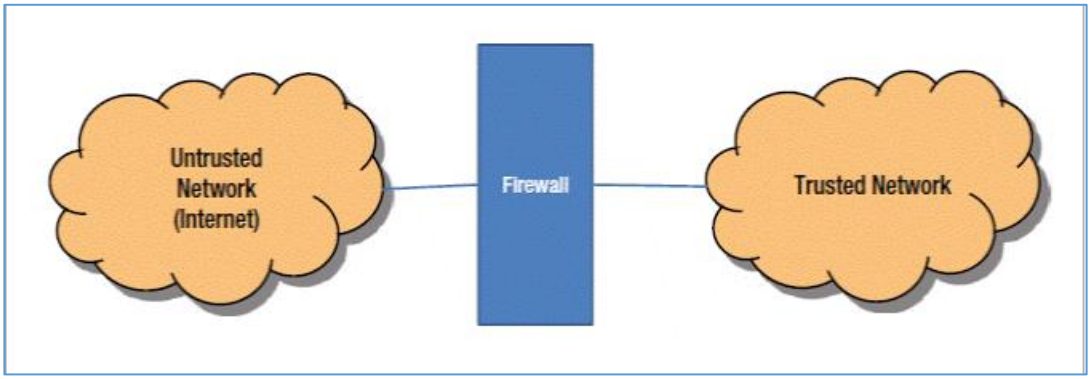


Figure 20: Integration of firewall

Source:https://ebrary.net/26717/computer_science/firewall_deployment_architecture

Functional Testing

1. **Network Sensor Testing:**

- Verify that all incoming and outgoing network sensors are picking up the correct sorts of traffic.

- Keep an eye on sensor activity to check for signs of network slowdown or congestion.

- Make that the central monitoring server is correctly aggregating data from all of the sensors.

2. **Intrusion Detection System (IDS) Testing:**

- Conduct controlled testing to trigger specified warning circumstances and ensure that the IDS delivers correct alerts; Test the IDS's capacity to identify different sorts of attacks, such as known signatures and anomalies.

- Figure out the IDS's true positive and false negative rates, then adjust the rules as needed.

3. **Firewall Policy Testing:**

- Build test cases that include both expected and unexpected circumstances, such as normal and malicious traffic.

- To make sure that only authorised data may get through the firewall and that all other traffic is denied, you should do regular testing.

Performance Testing

1. **Scalability Testing:**
   - Measure response times and resource utilisation during peak traffic periods; evaluate the system's capacity to manage increased loads without degrading performance.

2. **Load Testing:**
   - The network's efficiency may be evaluated by subjecting it to artificially high levels of traffic.

   - Ensure that the monitoring server can process a high volume of data without degrading its performance.

Penetration Testing and Security Assessment

1. **Penetration Testing:**
   - To find security gaps and determine how well a system can withstand an assault, it is necessary to conduct controlled penetration testing.
2. **Vulnerability Scanning:**
   - Use vulnerability scanning techniques to find security flaws in the system's software and hardware, then fix them before putting the system into production.

User Acceptance Testing

1. **End-User Testing:**
   - User acceptability testing should include input from both security analysts and IT staff by giving them access to the system in a simulated setting where they may report any problems they encounter.

Documentation and Training

1. **Documentation:**
   - Document all phases of integration, all tests and their results, and any issues and their resolutions.
2. **Training:**
   - Instruct the security operations staff on the proper use of the monitoring equipment.

- Educate the group about the dashboard's alerts, alert methods, and reporting capabilities.

In this process, the foundation is set up for an impactful and reliable banking system that will deliver the most secure environment for all sensitive data and the bank as an entity. In order to detect, analyze, and meet the demands of security risks, the network monitoring security system of the bank also needs to have an excellent integration and trial. The testing during the implementation process will include performance, operation and security checks on the system. In this way, the bank will be able to find and fix any issues before it goes live.

4.2.4 Alert Management and Incident Response

A warning scenario and a technique for addressing the breaches are presented here.

Alert Management Process

1. Alert Generation and Prioritization:1. Alert Generation and Prioritization:

   The observational security system gives attentive service for all the activities on the network and immediately notifies if it shows any bit of the malicious nature.

   Alerts are supplemented to the level of severity ranging from the critical to the high to the medium to the low.

2. Alert Correlation and Enrichment:2. Alert Correlation and Enrichment:

   The performance of the warnings is made more efficient when data about affected assets, users and network traffic concerned with these are fed along with the warnings, giving way to well-equipped decisions.

3. Alert Aggregation and Filtering:3. Alert Aggregation and Filtering:

   To prevent monotony or the possible mental disorders of security personnel, alarms might be grouped in groups and tagged so that if the

tagged ones have similar characteristics they would be treated as one alarm.

Filters can be utilized to reduce the rates of undue positives, which makes the alert stream easier to manage.

4. Notification and Escalation:

In case of an alert about highly sensitive information, the platform will stop and alert security officials.

For sure there are specified escalation procedures which are meant for dealing with a very important or with an alarm that couldn't be dealt when it was announced.

Incident Response Process

1. Incident Identification and Triage:

The first response action will involve the team’s determining whether the warning is credible or not.

The auditors will also examine and assess the consequences of the cyberspace event in terms of the potential effect it may bring to the bank's safety and operations.

2. Incident Containment and Mitigation:

The Incident is investigated after which the procedures for containment are executed to avoid its dramatic extension.

as causes of incidents are determined and mitigation measures are further developed, the intensity of the incident is reduced while the danger it poses are also minimized.

3. Forensic Analysis:

Be it for legal or investigative purposes, digital forensic analysts gather and secure evidence that could have implications for the overall process; they use the available information to investigate and know the cause, intrusion routes and scope of damage respectively.

4. Recovery and Remediation:

When everything is done with updating of patches, updates, and the other security improvements, we will bring regular and normal functioning to the system. These changes strengthened their system with the purpose of closing down the holes that led to the intrusion.

5. Post-Incident Review and Reporting:

Thus, the effectiveness of emergency response procedure would be evaluated after the occurrence of the event via the final evaluation.

Improvement suggestions are measured and documented aiming at drawing lessons to be taken into consideration for future similar operations.

Continuous Improvement and Learning

1. Threat Intelligence Integration:

The integration of threat information feeds into the security system is essential not just for more accurate warnings but also for a richer knowledge of the Smart City against emerging risks.

2. Regular Drills and Simulations:

Let's do the exercising and performing simulations for the incidents again so as to develop possible processes and better cohesion among the team.

3. Feedback Loop:

Input from security analysts and responders into the alerting criteria, response protocols can be improved This makes incident documentation more reliable and accurate.

4. Adaptive Measures:

Take a standing part in the precipitation events, and you can learn some helpful smart ways for the making of the security system's principles, norms, and detection algorithms.

The bank has a come up with the alert management system which acts as a mean by which to secure its financial data which is in many cases is the most sensitive part of the business and also runs its business smoothly. This is because of the system which will be the center point of the business incident response structure.

4.2.5 Continuous Monitoring and Maintenance

In the banking industry, the effectiveness of network security control systems relies heavily on continuous, persistent, and careful maintenance practices. Continuous monitoring plays a crucial role in ensuring the security and integrity of the network system.

Real-time traffic analysis and anomaly detection are essential components of continuous monitoring. Utilizing deep packet inspection techniques, every packet in the network is scrutinized for potentially hazardous behavior. Machine learning algorithms aid in automatically detecting abnormal functions, contributing to the identification of emerging security risks.

Advanced threat detection and threat hunting involve active investigation by experts to seek out evidence of attacks or penetration. The exchange of threat intelligence feeds facilitates timely sharing of threat information, enabling the detection and response to emerging threats in real-time.

Behavioural analysis and user monitoring are vital for detecting insider threats or anomalous activity. By comparing current user and device behaviors with established routines, red flags are raised whenever anomalies are observed.

Maintenance and upkeep are equally important aspects of network security. Dynamic rule and policy management involve continuous assessments and audits of IDS and firewall rules to ensure their accuracy and effectiveness amidst changing security landscapes. Patch management and vulnerability remediation involve routine patching and rechecking of operating systems, software, and network security devices to maintain a secure environment.

Log retention and analysis enable the preservation of necessary information while identifying trends and deviations. Performance optimization and scaling ensure the capability to handle rising traffic volumes and growing needs.

Regulatory compliance and audits are paramount, requiring regular reviews and audits to ensure compliance with corresponding regulatory rules.

Incident response review and improvement involve post-incident analysis and lessons learned to continually improve response strategies. Tabletop exercises and simulations provide security teams with valuable experience in simulating different security processes.

Employee training and awareness are critical for maintaining a strong security posture. Ongoing training programs ensure that IT professionals remain equipped against evolving threats, while security awareness campaigns educate all bank staff about cybersecurity threats and the importance of reporting suspicious behavior.

In summary, reliable network monitoring security solutions in the banking sector are built on continuous monitoring, maintenance, and employee education. By staying vigilant, implementing effective response strategies, and fostering a security-aware culture, banks can ensure the safe storage of critical financial data, build client trust, and maintain operational efficiency in the face of evolving digital threats.

4.3 Challenges and Mitigation Strategies

Comprehensive security networks must be established with safeguarding business and personal data, as well as overall integrity in mind. Nevertheless, such networks inescapably becoming more complex as threats become more and more diverse, the businesses are in need of some innovative measures that will help in strengthening the monitoring and security systems. Here in this article, we deep-dive into core topics related to network monitoring and security paradigm and make suggestions to resolve those issues.

4.3.1 Complexity and Scalability

The architecture of current networks includes numerous integrated parts which are based on intricate ecosystems. Consequently, they are difficult to safeguard as any single element might be weak and susceptible to attacks when others are attacked. Network design scalability is an integral part of planning for accessibility and attendant growth involving huge numbers of users as well as devices. Lack of scaling may bring down the perfomance, it may also brings latency spikes, which may cause the traffic handling issues.

Mitigation Strategies:

Designate the nodes in the network with logical zoning and make sure, data couldn't be exchanged between the non-identified nodes. Incorporate centralized management solutions for apprehending rules management and attacks for computers setting. Automate security solution implementation, configuration, and monitoring which is time, resource, and effort saving. As value of virtual currencies keep on exponentially growing more people are inclined to use this payment means which brings a consequent rise in network traffic, hence require presence of reliable scalable measures to secure the network from any unexpected service disruption amid enhanced need for security implementation.

Case Study: Cloud Environment:

Take into account a company that is moving operations to the cloud to meet the increased demands switching off the onsite resources causing complexity due to the network infrastructure design. Make use of micro-segmentation to construct perimeters between different cloud services and avoid the lateral data leakage incidents. Employ CSPM (Cloud Security Posture Management) platforms that enable monitoring of the cloud resources for security weaknesses and mistakes. Implementing applications-running-container-security helps in creating safe environments in containerized environments.

Today's modern networks are made increasingly susceptible to evolving cyber threats by their heightened complexity and scalability. A preventative and foresighted security strategy that covers surveillance and monitoring is of utmost importance to mitigate this problem. The company can address the risks by means of segmentation, centralized governance, automation, or buying security solutions that are vertically scalable. Modification of the security rules under the assumption that the new technologies, like cloud environments, will be used is crucial for the successful network security. The reason for that is that without it the required security would not be achieved. Complexity and scalability need to be tackled directly; businesses should become more effective in locating and safeguarding their networks and turn cybersecurity into a nuisance to cybercriminals.

4.3.2 Evolving Threat Landscape

Nowadays, companies go to huge risk of facing major threats linked to cyber security, leaving them dumbfounded when it comes to monitoring and protecting their networks. The cyber warfare is carried in methods highly dynamic, and this forces organizations to remain on the alert always and to adapt to the changing circumstances.

A key challenge is the swift change of attacks that are emergent and stealthy. Cybercrimer's use the vulnerabilities hopes for loopholes that enable them to escape in the eventuality of patching the software. Businesses are highly exposed to multiple

risks as data breaches, service interruptions and financial losses are all potential issues of this kind.

On the other hand, the rapid development of these technologies act as a challenge as well since the hackers and cyber criminals have invented various complicated attack techniques. From viruses with multiple forms to social engineering or the use of supply chain, adversaries of cyberspace are always updating and inventing new methods, which will make the classical security systems obsolete.

There are various measures the organizations should apply according to their hazard types and levels. It empowers real-time awareness that facilitates the detection of emerging threats and prompts the pre-emption and the implementation of required security measures in a timely manner. Updating on a regular basis and patching are critical in working towards the elimination of this vulnerability that leaves hackers with an opportunity by providing them with an updated system where all software have been updated to the latest security fixes. Moreover, behavioural testing permits watching users' and network behaviour, hence, leading to the timely detection of any malicious actions such as employees' insider attacks.

Out of all the examples that we can mention here, the rise in ransomware attacks which largely happen on critical infrastructures and across various industries. is a really significant one. Traditional security approaches can no longer achieve the same effectiveness in today's complex threat landscape. Security measures should now be reinforced with complimentary measures like robust backup and recovery, network segmentation and etc. His final advice is to invest in endpoint detection and response (EDR) solutions to tackle ransomware attacks effectively and provide continuous business operations.

At last, to defend oneself and other businesses against the cyberclyper threat, which is changing and evolving on a seemingly daily basis, as the principal strategy, they must be able and to adapt to the changes promptly and efficiently. Bringing intelligence threat into play, implementing strong security measures and adopting behaviour analytics are among the most effective ways to boost companies' capability

to timely detect and thwart threats. Ultimately, wants to finish the sentence by a very meaningful sentence that conveys that organizations should be farmers as they actively work their business premises day in day out preventing it to share of the daunting cyber security threats that are common.

4.3.3 False Positives and False Negatives

If not able to obtain the correct balance in identifying the real threats, and the avoidance of both false positives, and negatives, the security operations will remain unsuccessful and its image will be depreciated. This paragraph discusses the realities of determining true affirmatives and false positives and it suggests a set of steps that will help a company to strive for the best triumph one.

Challenges: Positives and Negatives

The effects of incorrect positives cannot be ignored, partly leading to alert fatigue among security operators causing them to misinterpret the alerts and hence divert the precious resources away from real attacks. However, false negatives are a severe risk factor, as they hide the true threats that are deprived of being revealed, making them more vulnerable to breaches as well as long-term consequences.

Mitigation Strategies:

1. Tuning and Optimization Policy: The conduct is most relevant to adjusting security rules and parameters so that false positive alerts are reduced which considerably scales up the accuracy of threats.
2. Machine Learning and AI: Machine learning and AI algorithms function as both reducing the frequency of false positives as well false negatives by analysing behavioural patterns

Conceptual Framework:

A framework which is in place for network behaviour comparison helps to differentiate between innocent and malevolent network activities and also prevents the agent being careful just because of a single event.

Case Study: A component of a security system that serves to identify attacks that could enable an unauthorized user.

In addition to delivering reports, IDS sets off the bells just to find the security operators are tired of the continuous echoing in the ear. Techniques for example rule modification and correlation assist in correcting false-positives and in isolation of attack patterns or trends.

The difficulty of the minimization of false positive and negatives cases in Spy Quality requires a sophisticated method. Organizations can refine their policies, deploy machine learning, and initiate behavior analytics management, in order to improve threat accuracy. Intensified examples, such as ransomware attacks, are indicating the need for readiness and targeted practical security programs. Nowadays, being able to react fast, adapt easily and have strong security strategies are the key factors in constantly changing cybersecurity environment.

4.3.4 Integration and Interoperability

Among other things, cybersecurity integration and interoperability network defenses are two of the major factors that need to be addressed while trying to build a united defense against cyber threats. For instance, as the number and type of security strategies used by businesses for their networks increase, interoperability and intergration concerns may come into play. There is a compelling need to efficiently interlink these technologies with absolute security and robust monitoring. Integration and interoperability issues are the source of the most important challenges in the process of coordination a cyber defense at the comprehensive level.

In a distributed security environment, you have these providers, the integration trouble and interoperability issues are quite usual. Compatibility problems between various security systems produce an envirointment which reduces the effectiveness of detection and response mechanism in attacks. In addition, the data islands bar the ability to draw the truthful insights as well as coordination of the reactions to complex threat patterns since these islands contain the generated data from different security

systems that are stored separately. Correlation from this data is not available which in turns makes the problem at hand worse.

To overcome these challenges, organizations should rely on mitigation approaches and measures like standardization, API integration, and security orchestration which have proved to be highly reliable in improving data management and security. The standardization part of the tasks involves adopting common set of data formats, common protocols and APIs (Application Programming Interfaces), to simplify the integration and streamlining process, enabling security technologies to be integrated and the information sharing to occur more efficiently. Whether I choose to establish security system integration using the API-based model or not, it must adopt well-defined APIs in its communication processes for facilitating effective interoperability in order to enable products to coordinate and present a consolidated network overview. Moreover, employing security orchestration enables platform automation amongst multiple security apps that may produce unified responses to security incidents with speed and co-efficacy.

The integration and automation demonstrated by SIEM in the study is showcased as the major advantage for the efficient detection and response time of threats. Organizations through SIEM solutions integration make use of one central alert aggregation as well as information linking to amplify threat detection. In addition, playbooks, which already comes with SIEM, allow arrangement of all of the incident responses related to different devices for response to certain events, which improves whole incident response capabilities.

Actually, the challenging issue of networks integration and interoperation in network security and monitoring requires collaborative efforts of different strategies involving: architecture, API-integration, and security orchestration. It is the embracing of the approaches that the organizations can be able to build a collaborative security circle and also ensure that they are detecting and responding to cyber threats effectively. Getting rid of those information silos and implementing cross-functional collaboration are fundamental steps that will help to improve cybersecurity resilience and act as earlier warning for potential cyberattacks.

Among other things, cybersecurity integration and interoperability network defenses are two of the major factors that need to be addressed while trying to build a united defense against cyber threats. For instance, as the number and type of security strategies used by businesses for their networks increase, interoperability and intergration concerns may come into play. There is a compelling need to efficiently interlink these technologies with absolute security and robust monitoring. Integration and interoperability issues are the source of the most important challenges in the process of coordination a cyber defense at the comprehensive level.

In a distributed security environment, you have these providers, the integration trouble and interoperability issues are quite usual. Compatibility problems between various security systems produce an envirointment which reduces the effectiveness of detection and response mechanism in attacks. In addition, the data islands bar the ability to draw the truthful insights as well as coordination of the reactions to complex threat patterns since these islands contain the generated data from different security systems that are stored separately. Correlation from this data is not available which in turns makes the problem at hand worse.

To overcome these challenges, organizations should rely on mitigation approaches and measures like standardization, API integration, and security orchestration which have proved to be highly reliable in improving data management and security. The standardization part of the tasks involves adopting common set of data formats, common protocols and APIs (Application Programming Interfaces), to simplify the integration and streamlining process, enabling security technologies to be integrated and the information sharing to occur more efficiently. Whether I choose to establish security system integration using the API-based model or not, it must adopt well-defined APIs in its communication processes for facilitating effective interoperability in order to enable products to coordinate and present a consolidated network overview. Moreover, employing security orchestration enables platform automation amongst multiple security apps that may produce unified responses to security incidents with speed and co-efficacy.

The integration and automation demonstrated by SIEM in the study is showcased as the major advantage for the efficient detection and response time of threats.

Organizations through SIEM solutions integration make use of one central alert aggregation as well as information linking to amplify threat detection. In addition, playbooks, which already comes with SIEM, allow arrangement of all of the incident responses related to different devices for response to certain events, which improves whole incident response capabilities.

Actually, the challenging issue of networks integration and interoperation in network security and monitoring requires collaborative efforts of different strategies involving: architecture, API-integration, and security orchestration. It is the embracing of the approaches that the organizations can be able to build a collaborative security circle and also ensure that they are detecting and responding to cyber threats effectively. Getting rid of those information silos and implementing cross-functional collaboration are fundamental steps that will help to improve cybersecurity resilience and act as earlier warning for potential cyberattacks.

4.3.5 Privacy and Compliance

The two essential considerations of privacy and complying are non-neglectable factors in the case of network monitoring and security. With time, firm's ability to strengthen its fronts in security field increases. However, this area is an active playground where breaches of privacy and confidentiality laws do exist. Security of utmost importance is one meaningful aspect. However, privacy concerns and compliance with laws and regulations of the country we are in is a crucial factor as well. This part of the work, in which will reflect the privacy and compliance requirements, with an objective to authorize the network security practices by law.

The regulations like GDPR and CCPA are the privacy act that all companies which operate in any way on the grounds of Europe or US must obey and these laws require companies to handle data very carefully. The non-compliance with GDPR can cost the company much due to fines that may exceed tens of millions, legal cases, and reputational damage among customers. More so, many people would claim that the reasons behind data privacy and those with unauthorized access can be justified is this because of the huge use of network security with meets the need of collection and analyzing of sensitive data. Data breaches and malicious access of users' information carries privacy issues that could cause loss of credibility among fans.

Combating these obstacles involves application of few methods. Data minimization represents the person’s information preservation only for as long as required for meeting legitimate security goals, it could reduce damaging data breaches and, of course, it ensures compliance with privacy laws. Encryption as well as anonymization methods also can be used to protect essential information, but no one can take away one's privacy during the analyses. Users should give their explicit consent before their personal data is collected or used, while the data companies should communicate openly as to why this data is needed, which will improve trust and accountability and therefore make privacy concerns lighter.

GDPR Compliance: A Case Study showcases the significance of detailed maintenance of data for engineering of as stringent as the GDPR protection rules. In-depth analyses and impact studies must be done to outline the specified security solutions that are mission compliant with standards and legal requirements. Through deliberately including privacy factors in the network construction and monitoring policies business will achieve the balance between security, privacy and lawful regulation. Although compliance with privacy laws and regulatory mandates on data protection can pose significant security challenges, a trusted and accountable data management environment is possible where privacy standards are followed and which will in turn lead to a better system accountability in data handling.

4.3.6 Resource Constraints

Organizations grapple with the challenge of establishing robust network monitoring and protection mechanisms, often hindered by resource constraints like limited budgets, staffing shortages, and technological limitations. These constraints can significantly impede an organization's cybersecurity efforts, leaving them vulnerable to various threats. Limited funding often translates to the inability to invest in up-to-date security tools, subscribe to threat intelligence services, and provide ongoing employee training. As a result, organizations may struggle to implement adequate security measures, leaving critical vulnerabilities unaddressed.

Staffing shortages in cybersecurity can lead to inadequate network monitoring, delayed response to security incidents, and inefficient system administration. With a shortage of skilled employees, organizations may experience decreased responsiveness and heightened vulnerability to cyber threats. Identifying and prioritizing critical assets enables organizations to allocate resources effectively, focusing on protecting the most essential aspects of their network infrastructure.

Automation of manual tasks such as log analysis and incident response can expedite complex security operations, allowing security personnel to dedicate their time and expertise to more strategic tasks. Outsourcing security to Managed Security Service Providers (MSSPs) offers organizations an alternative approach to leveraging expertise and resources without compromising professional standards. MSSPs provide specialized knowledge and capabilities to augment an organization's internal security efforts.

Small businesses facing budget and IT constraints often opt for affordable security solutions such as cloud-based alternatives and contracting MSSPs for expert services and continuous monitoring. This approach allows small entities to benefit from professional security expertise while navigating resource limitations effectively.

Limited resources working in the domain of maintaining the network monitoring system involve a special set of problems. Asking yourself smart questions, automate what is possible, and looking for outside support are strategies that will help organizations improve their security results while still keeping their budget low and under control. The creative use of wits, budgetary discipline, and cautiousness means not only that organizations of this kind can toughen their security as such, but also that they will be able to observe the way the threat landscape has diversified with a degree of foresight.

Sr. No	Risk	Description	Mitigation Strategies
1	Infrastructure Vulnerabilities	There is a risk of compromising current infrastructure when integrating security solutions.	Perform thorough vulnerability evaluations, keep up-to-date patch management, and correct any misconfigurations before releasing.
2	Integration Challenges	Compatibility problems arise when new security solutions are integrated into an existing technological stack.	Before deploying, be sure you undertake thorough compatibility testing, test in isolated settings, and work closely with IT departments.
3	False Positives and Negatives	False positives and real threats overlooked due to inaccurate threat detection.	Improving detection accuracy over time requires regular testing, the use of machine learning techniques, and the refinement of detection criteria.
4	Overwhelming Alerts	Overwhelming security analysts with too many notifications might cause them to overlook serious situations.	To efficiently manage alert traffic, it is recommended to implement sophisticated filtering techniques, to prioritise alerts by severity, and to automate first alert triage.

Sr. No	Risk	Description	Mitigation Strategies
5	Resource Constraints	Inadequate deployment of systems may occur from insufficient allocation of resources.	Successful system installation relies on accurate cost estimates, proper allocation of resources, and ongoing training and education.
6	Regulatory Compliance	Consequences may be incurred for noncompliance with data protection laws.	Maintain legal compliance by working with attorneys, learning about applicable rules, and performing frequent audits and system updates.

Table 1: Risk cause and treatment

4.3.6 Insider Threats

However, the safety of a network is not that simple, because the network can equally be attacked from out-side by employees, contractors, or partners. These threats can be purposeful if, for instance, the instigator is a dissatisfied employee or a person with profit-oriented predisposition, or may be accidental: sometimes, the source of the threat could be the carelessness of employees who don't mind their job duties or simple negligence. To a resounding degree, insider threats stem from different reasons, not the least of which is disruption of the organizational life and breaches of both the type and idiosyncratic data, which eventually lead to compromising the entity’s image.

Malicious insiders pose a big threat as there are specific sabotage-oriented actions, which are devoted directly to causing damage in the company, This can mean a spy getting into secret data, data leaks, cyber assaults, which may be the worst that will happen. On the one hand, intentional carelessness of insiders, including misconfigured settings, can be caused by those insider mistakes and it will lead to

unauthorized access to sensitive information. However, on the other the hand, unintentional mistakes for insiders, for example, misconfigured settings and accidental data sharing, can also cause these security breaches.

Addressing insider threats including the threats coming from insiders, organizations can use different methods. Through the actions user behavior monitoring it is possible to monitor and analyse user actions to detect if any unusual behavior or patterns emerge that could signal insider threat. Another good example is role-based access control, as it restricts users' reach to only the necessary information and resources to facilitate them execute their roles, and at this way the risk of breaking private information by insider threats is minimized.

Security awareness training is a chief weapon used to prevent insider attacks through the back door introduction of employees to best practices in security and the passing of suspicious messages. When people in the organization learn to recognize threats as being the potential insider attacks, the organizations are made less susceptible to this attack type.

A case involving an employee straying corporate data and hence creating leakage gives a strong narrative for implementing technology of Data Loss Prevention (DLP) and providing user education in order to avoid accidental data leakage. In this regard, the integration of different solutions into the technological aspects like educating and training the personnel of an organization will help to create an effective system in countering insider threats.

4.4.1 Assessment and Planning

Guarding Against Insider Threats: The Securement of Protection of Networks (INS) and of the participation of the safety measure for handling of the insider attack.

Since both malicious and unconscious employees, contractors, or business partners may trigger insider threats that lead to network security and monitoring hazard, such threats bring huge risks. Implementation of such systems to be able to

detect and disarm such attacks and address the difficulties of countering insider attacks is necessary to address the problem.

Challenge: Malicious Insider Activities

If the organization has discontentful workers, contractors with the bad attitudes, or the people planning to make money, they will become inside threats. Breaches of information security that include data leaks, illegal access, or a negative reputation of the organization may occur as a result.

Challenge: Unintentional Insider Mistakes

Leaks due to security flaws usually occur due to unintentional mistakes like misconfiguration of settings, negligence of data, and so forth. The ramifications of these mistakes can be presented through the misuse of the sensitive information (including data breaches).

Mitigation Strategies

1. User Behavior Monitoring: Tracking systems should be put in place, and they should be used to monitor users' actions, as well as identifying any unusual behavior that might indicate insider threats.

2. Role-Based Access Control: Place access level restrictions for the users depending on their roles which will help to soften identified weaknesses to insider threat.

3. Security Awareness Training: Carry out the regular security awareness training for the employees of any company so that they are able to recognize and report unusual activities which can eventually lead to a successful preventive measure against insider attacks.

Case Study: Employee-Driven Data Outflow or Leakage

A situation can be assumed where an employee who enjoys good relations with the company lets the confidential information out for some reason. Mitigating strategies may include the employment of data loss prevention (DLP) mechanisms combined with the constant users' learning process that should discourage the intentional disclosure of data.

Ensuring security measures along with teaching users to identify insider threats is important in the process of properly tackling an insider threat. Through the integration of technical solutions with staff training and culture aimed at security awareness, organizations will definitely reduce any risk of insider attacks with the ultimate objective of ensuring the networks' integrity. Case studies like the one about The suffering of the disclosure of confidential information demonstrated the sense of organization to take preventive measures and to cultivate a culture of loyalty within the organization.

4.4 Stages

Observing that the true and all inclusive safety measures of a computer network calls for a structured multi-stage approach, is the fact. These are the main processes the system process of constructing a network monitoring and security system consists of follwing sub chapters.

4.4.1 Assessment and Planning

Network implementation starting with an assessment and planning is simply the beginning of laying an unshakable foundation of network security. At this point in the project stakeholders join in discussion of their organization needs to understand the risks and set their objectives as well. Crucial responsibilities consist of exploring the system assets inventory, performing risk analysis, creating security rules, and designing the incident response procedure. The leadership of all these different teams are from the IT department, selucrity department, consequences specialization, procurement particularly the training team.

Comprehending capacities of the enterprise is the key to the information gathering task. Engaging stakeholders proves a vital manner in collecting information from the organization on its security challenges and objectives. Collaborating with members of IT staff, security experts, leadership and lawyers stakeholders can not only get an accurate but well-rounded and complete view of the organization's security parameters. Also in action, should be the researching and studying dangers and vulnerabilities of the network, assessing regulatory requirements, and, finally, formulation of security objectives are the main activities at this stage.

Sigmaing the process as well as knowing the possible problems and restrictions is included in the assessment and planning phase too. When sizing project scope gets on the question of network segmentation, data measurement points and coverage areas. And lastly, assessing how this will impact our budget, limitations using technology, and availability of resources helps to discover potential barriers that may affect the implementation process. Performing comprehensive evaluations and planning an action plan can guide organizations to identify viable solutions specifically fulfilling their certain conditions in security implementation process.

4.4.2 Requirements Definition

In the requirements definition stage, organizations will delineate between the technical and functional requirements of network monitoring software leveraging feedback derived from the assessments via input. In this stage, the security system design will be tested to assess its ability to mitigate unique security challenges and goals of the chosen organization. The main activities are: the specification of data collection needs, assuring defensive objectives, examining the technical obstacles, formulating the alert and response framework, and documenting the user requirements.

Translation finding assessment into requirement implies to identify data to be collected source, which are user activity, system logs, security event and network traffic. Standards for documentation which encompass derivative transactions, regulatory requirements, and data retention are set up in order to guarantee adherence and successful historical research. Besides that, the protection means also include the

setting of guidelines for the threat detection, performance indicators, and reporting requirements, in order to meet the security goals in a meaningful manner.

When comes to the technical constraints, it becomes a must that the security network system is rationalized in terms of its feasibility and function. World then (Is marked by), the integration with the existing systems, scalability needs, and resource limitations which will have to, be considered. Another procedural aspect of building the threat intelligence is defining the alerting and response mechanisms through setting up triggers, conveying notifications, and detailing workflows for the reaction to security events. Through identifying the role of the security system users such as system analysts, IT staff and end-users organigations avail systems that will satisfy the needs of these users through access controls which are not compromised , good user experience design and training provisions. To achieve optimum implementation of a network environment with regard to the security, it is important to perform a detailed requirements definition to seamlessly converge business objectives with technical acts.

4.4.3 Infrastructure Cost

Making sure the infrastructure costs are dealt with spells prudence as far as the security solution is thought through. Ensuring network security investment plays a vital role in protecting digital assets and sustained operations. Nevertheless, care should be taken of cost projections in the infrastructure before saving. It entails acquiring various pieces of equipment including computing systems software, plans for building networks as well as storing data, licensing fees and staffing cost. The estimation of this amount engages vendors quoting, evaluating the overall costs of ownership, examine the scalability, and to ensure the professional services are included. Through the implementation of budget strategies such as prioritizing investments, utilization of open source softwares, the renovation of cloud services, negotiation with vendors and the provision of security solutions in stages, the organizations can adequately be on the safe side of cost efficient network infrastructures and optimal network security.

Lots of tactics can be used by these organizations for the purpose of saving on infrastructure costs. Investments are concentrated on the particular bases of risk

assessment, whereas security resource allocation is assigned to the places where their impact would be most intensive. Freeness of open-source software saves on licensing; nevertheless, it necessitates customization and maintenance against the competitors.

Sr. No	Components of Infrastructure Cost
1	Hardware (servers, switches, routers)
2	Software (licenses, operating systems)
3	Data Center Facilities (rent, power)
4	Network Connectivity (ISP, bandwidth)
5	Security Equipment (firewalls, IDS/IPS)
6	Storage Solutions (SAN, NAS)
7	Backup and Disaster Recovery Solutions
8	Virtualization (hypervisors, licenses)
9	Monitoring and Management Tools
10	Installation and Setup Costs
11	Maintenance and Support Contracts
12	Contingency/Unexpected Costs

Table 2: Components of Infrastructure cost

Harnessing cloud based services on a pay-as-you-go basis ensures the avoidance of most of the equipment acquisition cost. Implementing protection measures in stages, step by step, enables organizations to begin with the necessary components and later gradually expand. Like our service? Request an order now! Furthermore, vendor negotiations give organizations options to bargain differently in accordance with their requirements and financial capabilities. Outlaying infrastructure cost, making effective allocation, and delivering effective saving plans can enable an entity to achieve a viable network security alongside financial management.

4.4.4 Strategies for Managing Infrastructure Costs

While the strategies of prioritization, open-source software and cloud services, phased rollout, as well as vendor negotiation, come to play in managing all aspects of expenditure reflecting infrastructure. Through clearly assessing involved components, estimating costs and using problem-solving methods, organizations may define the security goals of their network and fulfill the financial limits.

4.4.5 Configuration and Tuning

Tuning and configuration are crucial stages in network security implementation providing the best implementation performance and detection capabilities aiming at

the perfect resource using. After deploying the required hardware and software, the organizations may need to tweak the security system such that the behavior fits with their objectives, network specifications and security in general. Tasks comprise of traffic shaping, QoS setup, some filtering and proper resource allocation. Employing this method to create a security environment which is both secure and fast, organizations will have effective threat detection without slowing the network performance. Optimally adjusted configuration and tuning, as we all know, boost the security architecture in the process of dealing with threats and maintaining the services driven by network.

4.4.6 Ongoing Support and Maintenance

Maintaining an excellent network security level needs not only an effective implementation but also continuing maintenance effort after that initial stage that included such efforts. Releasing patches and updates on a regular basis may help to mitigate security risks and faults and ultimately improve the security and stability of the website. The list of activities is represented by such tasks as looking into how control flows change, designing maintenance plans, and testing upgrade releases prior to publishing them. Periodic validation and refinement will be done by auditing the security level, analysing system performance records and gathering user opinions, and then going over this data in order to identify areas for further optimization. Through performing these effective regular hygiene measures, companies assure the long-term good working condition and effectiveness of their network security system that ensures the provision of protection for their digital assets and data.

5. Discussion and Recommendations

5.1 Discussion of findings

At present, one of the most important security challenges for the banks is a large body of highly confidential financial data that is kept safe. To guarantee that the workflows run smoothly and to build trust among customers and regulators, financial institutions are required to develop network security systems with elaborate system monitoring and strict response speeds in case a threat is detected. Specifically, it probes into the advantages associated with embracing networking security technology in the area of banking, which will be highlighted in the following subsections.

5.1.1 Enhanced Cybersecurity

A dependable cyber security system will not only enable financial institutions to counter these risks but also lessen the probability of revenge attacks being launched on them. Network monitoring systems perform this crucial role of observant guards by constantly scanning network traffic to detect and timely mitigate security risks before they become a major issue.

5.1.2 Early Threat Detection

oth conventional and modern information technology monitoring techniques have proven to be the best defence against network defacement and intrusion by detecting abnormal activities in real time. Active defence system of financial institutions assists them in fighting quickly against the data breaches that could cause great damage to their operations by minimizing the impact of cyber-threats on the operations of their institutions, thus safeguarding financial data.

5.1.3 Operational Continuity

Network security solutions are the way of securing operational continuity by related events like security incidents which can stop regular banking service. Frequent checks and real-time response to any threats keep banking services running uninterruptedly, thus customers remain loyal and financial institution retain its reputation.

5.1.4 Efficient Incident Response

Data security solutions are instrumental in category tracking and real time identification with the financial institutions having the ability to put in place efficient incident response process, minimizing downtime and eradicating the financial and reputational outcomes of security incidents. Formalized crisis management techniques help in quick intervention and evaluation, which in consequence builds the organizational capability to bounce back.

5.1.5 Network Performance Optimization

The variety of the tools for surveillance of network activity and performance give outstanding of possibilities for optimization and improvement of network performance as well as service level. By the implementation of the process improvement technique of the network analysis, financial institutions will be able to detect and eliminate performance problems, guaranteeing customers the quick and seamless banking transactions, thus, increase customer satisfaction and operational efficiency.

5.1.5 Threat Intelligence

Through the network monitoring systems, threat intelligence is gathered and developed by identifying the common strands of cyberattacks. Financial institutions thus will be able to prepare themselves against the emerging threats and also create a better security for themselves through security posture. The network traffic inspection and activity log analysis help identify newly emerging threats patterns and boost the firewall defences in the face of ever-evolving cybersecurity threats.

5.2 Recommendations

Based on the insights gleaned from our discussion, we offer the following recommendations for financial institutions seeking to enhance their network security. Based on the insights gleaned from our discussion, we offer the following recommendations for financial institutions seeking to enhance their network security:

1. Invest in Robust Network Security Solutions: Banks and other financial institutions have the responsibility of deploying the most effective security

systems that use analytic means capable of detecting issues early and react to them as soon as they happen.

2. Implement Regular Security Audits and Assessments: Conduct periodical risk evaluations and audits on security to adjudge the safety positions and the performance of the measures.

3. Foster a Culture of Cybersecurity Awareness: Educate employees on cybersecurity best practices, vigilance and vigilance in cybersecurity, and the risks that they can cause to the organization.

4. Collaborate with Industry Partners: Partner with the sectoral partners and regulatory agencies to pool the threat intelligence and expert guidance on network security to stay updated.

5. Stay Abreast of Emerging Threats: Continuously watch for any emerging cybersecurity hazards as well as trends to ensure that security measures as well as being up to date are continuously improving so that they can deal with possible risks that may arise.

6. Continuously Evaluate and Improve Security Measures: The adoption of operating standards to review the effectiveness of network security measures on a routine basis and also putting in place the necessary improvements to strengthen overall security posture.

With the implementation of the insinuated recommendations, financial institutions will be able to reinforce their offensive cyber defence measures, to detect and prevent as many cybersecurity risks as possible, and to preserve the integrity and confidentiality of the most guarded financial databases and data.

6. Conclusion

In general, in-depth research into network security and monitoring systems is not only stressing the necessity of their function, but also drawing a picture of their implications as far as financial institutions are concerned, i.e. security of sensitive data, whether it is confidential, available or not. Adhering to the specific purpose and methods that we had predetermined, our work study has afforded us a clear picture on the complexity networking security that is full of downs and ups.

Applying risk assessment, strategic thinking, and detailed project planning we accomplished the important work of laying the foundation from where we could build more detailed research. Our in-depth surveying of the literature showed how network security emerged as a multi-dimensional phenomenon. Discussed the unsinkability of SIEM systems, how network security vulnerabilities will always exist and how machine learning was gradually gaining acceptance.

During the journey of constructing a streamlined system for the functional monitoring, we overcame awkwardness of the design issues inherent in these situations, from the initial planning to routine maintenance. Firstly, the results this study throws out cannot be overemphasized. The findings validate the importance and application of network monitoring as well as clearly bring out the gap that exists that security solutions can fill. Thorough security stance, sensed threat detection, and rapid response functioning are some of the endless benefits shown by our research.

In essence, our conclusions echo the overarching objectives of our thesis: In conclusion, the significance of network security and monitoring in the business world should not be relegated to the background, and it is high time that holistic approach covering both technological skills, foresight and ongoing watchfulness is embraced as key to effective and efficient operations in the contemporary business scene. Our study draws attention to the fact that it would be wise of us to remain agile and connected in the context of a changing threat space.

When we glimpse into the future, our research continues to indicate that networking security solutions are ongoing and are progressing through data analytical

advancements, artificial intelligence and incorporating the intelligence of threats. It relays the continuation of the surveys and security systems upgrades required to keep up with the evolving risks and the commitment of our team to perpetual progress and innovation in handling network security issues.

Ultimately, this is our thesis's response to the fact that no matter how resilient someone becomes, cybersecurity and surveillance will help protect your business and personal resources. By applying strict methodologies and objectives, we have already set the stage for more network security advances, this clearly shows the need of awarding more attention and collaboration in the attempt to make cybermen more resilient.

7. References

Maleh, Y., Shojafar, M., Alazab, M., & Baddi, Y. (2020, December 14). *Machine Intelligence and Big Data Analytics for Cybersecurity Applications*. Springer Nature. http://books.google.ie/books?id=p_sOEAAAQBAJ&printsec=frontcover&dq=cyber+security+Advanced+Analytics+and+Artificial+Intelligence&hl=&cd=1&source=gbs_api

Blokdyk, G. (2018, May 3). *Network Monitoring*. Createspace Independent Publishing Platform. http://books.google.ie/books?id=UurItgEACAAJ&dq=network+monitoring&hl=&cd=4&source=gbs_api

Choi, B. Y., Zhang, Z. L., & Du, D. H. C. (2011, June 14). *Scalable Network Monitoring in High Speed Networks*. Springer Science & Business Media. http://books.google.ie/books?id=yhaVAeFK8_sC&printsec=frontcover&dq=network+monitoring&hl=&cd=2&source=gbs_api

Nguyen, N. H. (2018, February 3). *Essential Cyber Security Handbook In English*. Nam H Nguyen. http://books.google.ie/books?id=XkJKDwAAQBAJ&printsec=frontcover&dq=cyber+security&hl=&cd=4&source=gbs_api

Murdoch, D. (2018, August 26). *Blue Team Handbook*. Createspace Independent Publishing Platform. http://books.google.ie/books?id=pai1uwEACAAJ&dq=SIEM+cyber+security&hl=&cd=10&source=gbs_api

Thomas, A. (2017, September 27). *Security Operations Center - Analyst Guide*. http://books.google.ie/books?id=q19LtAEACAAJ&dq=SIEM+cyber+security&hl=&cd=5&source=gbs_api

Thomas, A. (2018, March 26). *Security Operations Center - SIEM Use Cases and Cyber Threat Intelligence*. http://books.google.ie/books?id=zlyGtQEACAAJ&dq=SIEM+cyber+security&hl=&cd=2&source=gbs_api

Hermans, K. (n.d.). *Mastering SIEM*. Cybellium Ltd. http://books.google.ie/books?id=SsnKEAAAQBAJ&pg=PA3&dq=SIEM&hl=&cd=1&source=gbs_api

Pescapè, A., Salgarelli, L., & Dimitropoulos, X. (2012, March 1). *Traffic Monitoring and Analysis*. Springer Science & Business Media. http://books.google.ie/books?id=vQuda86Zps0C&printsec=frontcover&dq=Network+Traffic+Analysis&hl=&cd=8&source=gbs_api

Blokdyk, G. (2019, August 15). *Network Traffic Analysis A Complete Guide - 2019 Edition*. 5starcooks. http://books.google.ie/books?id=XI5-yAEACAAJ&dq=Network+Traffic+Analysis&hl=&cd=3&source=gbs_api

Halder, S., & Ozdemir, S. (2018, December 31). *Hands-On Machine Learning for Cybersecurity*. Packt Publishing Ltd. http://books.google.ie/books?id=LR2CDwAAQBAJ&printsec=frontcover&dq=machine+learning+cyber+secruity&hl=&cd=1&source=gbs_api

Malik, P., Nautiyal, L., & Ram, M. (2022, December 5). *Machine Learning for Cyber Security*. Walter de Gruyter GmbH & Co KG. http://books.google.ie/books?id=Z7WbEAAAQBAJ&printsec=frontcover&dq=Machine+Learning+for+Cybersecurity+Applications&hl=&cd=3&source=gbs_api

Kizza, J. M. (2020, June 3). *Guide to Computer Network Security*. Springer Nature. http://books.google.ie/books?id=eTfpDwAAQBAJ&printsec=frontcover&dq=netowrk+security&hl=&cd=7&source=gbs_api

Strebe, M. (2006, February 20). *Network Security Foundations*. John Wiley & Sons. http://books.google.ie/books?id=qiDsEgYKXRAC&printsec=frontcover&dq=netowrk+security&hl=&cd=5&source=gbs_api

Boddu, R., & Lamppu, S. (2024, February 29). *Microsoft Unified XDR and SIEM Solution Handbook*. Packt Publishing Ltd. http://books.google.ie/books?id=X6n4EAAAQBAJ&pg=PA19&dq=SIEM&hl=&cd=3&source=gbs_api

Kurniawan, R., & Prakoso, F. (2020, January 17). Implementasi Metode IPS (Intrusion Prevention System) dan IDS (Intrusion Detection System) untuk Meningkatkan Keamanan Jaringan. *SENTINEL*, *3*(1), 231–242. https://doi.org/10.56622/sentineljournal.v3i1.20

Monitor, I. (2000). Network Security Fundamentals. *Information & Security: An International Journal*, *4*, 121–122. https://doi.org/10.11610/isij.0411

Blokdyk, G. (2018, May 3). *Network Monitoring*. Createspace Independent Publishing Platform. http://books.google.ie/books?id=UurItgEACAAJ&dq=Network+Monitoring&hl=&cd=4&source=gbs_api

Chiu, D. M., & Sudama, R. (1992, January 1). *Network Monitoring Explained*. Prentice Hall PTR. http://books.google.ie/books?id=S_VSAAAAMAAJ&q=Network+Monitoring&dq=Network+Monitoring&hl=&cd=1&source=gbs_api

Thomas, T. M., & Stoddard, D. (2012, January 1). *Network Security First-step*. Cisco Press. http://books.google.ie/books?id=VYlm5qzXUscC&printsec=frontcover&dq=Network+Security&hl=&cd=1&source=gbs_api

Canavan, J. E. (2001, January 1). *Fundamentals of Network Security*. Artech House. http://books.google.ie/books?id=bSPsPmtSMboC&printsec=frontcover&dq=Network+Security&hl=&cd=2&source=gbs_api

Lovett, W. A. (2005, January 1). *Banking and Financial Institutions Law in a Nutshell*. West Academic Publishing. http://books.google.ie/books?id=D3c9AQAAIAAJ&q=Banking+and+Financial+Institutions+Law+in+a+Nutshel&dq=Banking+and+Financial+Institutions+Law+in+a+Nutshel&hl=&cd=1&source=gbs_api

Ozkaya, E., & Aslaner, M. (2019, January 31). *Hands-On Cybersecurity for Finance*. Packt Publishing Ltd.

http://books.google.ie/books?id=CGSGDwAAQBAJ&printsec=frontcover&dq=Cybersecurity+for+Banking+and+Financial+Institutions&hl=&cd=4&source=gbs_api

Pomerleau, P. L., & Lowery, D. L. (2020, August 29). *Countering Cyber Threats to Financial Institutions*. Springer Nature. http://books.google.ie/books?id=ZA76DwAAQBAJ&printsec=frontcover&dq=Cybersecurity+for+Banking+and+Financial+Institutions&hl=&cd=2&source=gbs_api

Cybersecurity in Banking. (2022, November 28). GRIN Verlag. http://books.google.ie/books?id=MEOeEAAAQBAJ&printsec=frontcover&dq=Cybersecurity+for+Banking+and+Financial+Institutions&hl=&cd=1&source=gbs_api

Wright, C. (2020, April). Essentials for selecting a network monitoring tool. *Network Security*, *2020*(4), 11–14. https://doi.org/10.1016/s1353-4858(20)30043-x

Nikolaidis, I. (2000, March). Network security essentials: applications ond standards [Books]. *IEEE Network*, *14*(2), 6–6. https://doi.org/10.1109/mnet.2000.826358

Chorafas, D. N., & Steinmann, H. (2016, July 27). *Implementing Networks in Banking and Financial Services*. Springer. http://books.google.ie/books?id=WMODAAAQBAJ&pg=PA20&dq=Implementation+of+Security+Systems+for+Network+Monitoring+in+the+Company(Bank)&hl=&cd=3&source=gbs_api

Sennewald, C. A., & Christman, J. H. (2011, August 29). *Retail Crime, Security, and Loss Prevention*. Elsevier. http://books.google.ie/books?id=y_KyHUtfYIEC&pg=PA82&dq=Implementation+of+Security+Systems+for+Network+Monitoring+in+the+Company(Bank)&hl=&cd=5&source=gbs_api

Buecker, A., Ashley, P., Borrett, M., Lu, M., Muppidi, S., Readshaw, N., & Redbooks, I. (2008, May 29). *Understanding SOA Security Design and Implementation*. IBM Redbooks. http://books.google.ie/books?id=w-i1AgAAQBAJ&pg=PA133&dq=Implementation+of+Security+Systems+for+Network+Monitoring+in+the+Company(Bank)&hl=&cd=10&source=gbs_api

Chorafas, D. N., & Steinmann, H. (2016, July 27). *Implementing Networks in Banking and Financial Services*. Springer. http://books.google.ie/books?id=WMO-DAAAQBAJ&pg=PA20&dq=Implementation+of+Security+Systems+for+Network+Monitoring+in+the+Company(Bank)&hl=&cd=3&source=gbs_api

Rao, H., Gupta, M., & Upadhyaya, S. J. (2007, June 30). *Managing Information Assurance in Financial Services*. IGI Global. http://books.google.ie/books?id=9Wq9AQAAQBAJ&pg=PT133&dq=Implementation+of+Security+Systems+for+Network+Monitoring+in+the+Company(Bank)&hl=&cd=1&source=gbs_api

Bank security systems: ATM security, Vault & Safe Lock Integration. (2020, April 5). PACOM. https://pacom.com/en/access-control-and-security-solutions/bank-security/

Bank Security Surveillance Systems & Alarms | Solutions. (n.d.). https://info.verkada.com/industry-solutions/surveillance-for-banks/

P. (2023, July 13). *Smart Security Alarm System for Banks and ATMs | Securico*. Securico. https://www.securicoelectronics.com/solutions/bfsis/

L. (2024, January 28). *Network Bank Alarm Monitoring System Solution - Athenalarm*. Athenalarm. https://athenalarm.com/network-alarm-system/network-bank-alarm-monitoring-system-solution/

8. List of pictures and abbreviations

8.1 List of Table

8.2 List of Figure

8.3 List of abbreviations

IPSec: Internet Protocol Security

AES: Advanced Encryption Standard

IDPS: Intrusion Detection and Prevention Systems

SSL/TLS: Secure Sockets Layer/Transport Layer Security

ACLs: Access Control Lists

SIEM: Security Information and Event Management

VPN: Virtual Private Network

NAC: Network Access Control

NPM: Network Performance Monitoring

HIDS: Host:based Intrusion Detection System

NIDS: Network:based Intrusion Detection System

AI: Artificial Intelligence

GDPR: General Data Protection Regulation

CNNs: Convolutional Neural Networks

RNNs: Recurrent Neural Networks

DDoS: Distributed Denial of Service

DPI: Deep Packet Inspection

SIM: Security Information Management

SEM: Security Event Management

IT: Information Technology

SDN: Software:Defined Networking

NFV: Network Functions Virtualization

IoT: Internet of Things

UBA: User Behavior Analytics

SOAR: Security Orchestration, Automation, and Response

NFS: Network File System

DNS: Domain Name System

API: Application Programming Interface

RAM: Random Access Memory

CPU: Central Processing Unit

SQL: Structured Query Language

TCP/IP: Transmission Control Protocol/Internet Protocol

IPv4/IPv6: Internet Protocol Version 4/Version 6

GUI: Graphical User Interface

CSPM: Cloud Security Posture Management

EDR: Endpoint Detection and Response

MSSPs: Managed Security Service Providers

CCPA: California Consumer Privacy Act