Czech University of Life Sciences Prague

Faculty of Economics and Management

Department od Information Technologies

Master's Thesis

Network monitoring and implementation of security systems in the company

Written by (Author): Bc. Rehmat Ullah Usman Ullah

Thesis Supervisor: Ing. Martin Havránek, Ph.D.

CZECH UNIVERSITY OF LIFE SCIENCES PRAGUE

Faculty of Economics and Management

DIPLOMA THESIS ASSIGNMENT

Bc. Rehmat Ullah Usman Ullah

Informatics

Thesis title

Network monitoring and implementation of security systems in the company

---

Objectives of thesis

The aim of the Diploma thesis is to implementation a proposal for enhancing the security system that can successfully defend the computer network of an organization from a cybersecurity standpoint. Partial aim of the thesis is to conduct an analysis of methods and systems of monitoring, based on the contemporary risks and vulnerabilities in an organization.

Methodology

The Diploma thesis will consist of two sections, a theoretical and a practical, respectively. The theoretical section will explore the theoretical foundations of network monitoring as an element of the security system, cybersecurity, contemporary risks, threats of network attacks and classification of vulnerabilities or corporate systems. In the practical section, a multi-level check of the existing condition of the security system will be carried out using analytical technique, namely system analysis. The method of synthesis of requirements will be used to generate a proposal for the construction of the security system based on the identified vulnerabilities and organizational features.

The proposed extent of the thesis

60-80p.

Keywords

Network infrastructure, monitoring, firewall, server, cybersecurity, DLP, SIEM, vulnerability, attack, configuration.

Recommended information sources

BEJTLICH, Richard. The practice of network security monitoring: understanding incident detection and response. San Francisco: No Starch Press, [2013]. ISBN 978-1593275099.

BONDAREV, V. Security analysis and monitoring of computer networks. Moskva: MGTU, 2017. ISBN 978-5-7038-4757-2.

MAURO, D., SCHMIDT, K. Essential SNMP, Second Edition. Beijing: O'Reilly Media, 2005. ISBN 05-960-0840-6.

NORTHCUTT, S., NOVAK, J. Networking intrusion detection. Indiana: Indianapolis, 2003. ISBN 0-7357-1265-4.

SKABTSOV, N. Information systems security audit. SPB: Peter, 2018. ISBN 978-5-4461-0662-2.

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: 14. 7. 2022

doc. Ing. Jiří Vaněk, Ph.D.

Head of department

Electronic approval: 28. 11. 2022

doc. Ing. Tomáš Šubrt, Ph.D.

Dean

Prague on 29. 03. 2023

Declaration

I hereby declare that I have worked on my master's thesis titled "Network monitoring and implementation of security systems in the company" by myself and I have used only the sources mentioned at the end of the thesis. As the author of the master's thesis, I declare that the thesis does not break any copyrights. I also declare that this dissertation is my original work and has not been submitted before to any institution for assessment purposes.

I understand that the provision of incorrect information may have legal consequences.

In Prague on 30/03/2023 _____

Acknowledgement

I take this opportunity to express gratitude to all the department faculty members for their help and support through out the study period. I would like to extend and express my sincere gratitude and respect towards my honourable teacher and thesis supervisor, Ing Martin Havránek, Ph.D., for his immense guidance and support for the successful completion of my thesis

Last but not the least, my sincere gratitude to the Czech University of Life Sciences in Prague for allowing me to experience and gain technical as well as personal knowledge through their education and culture.

Network monitoring and implementation of security system in the company

Abstract

This Diploma Thesis concerns network monitoring and implementing a proposal to reinforce the security system that can well defend the computer network of an organizational environment or infrastructure. The work aims to protect the organization and its employees from a cybersecurity perspective and raise awareness about the potential cyber attacks on the rise. The theoretical part of the thesis explores the theoretical foundations of network monitoring such as for network attacks, threats, risks and classification of vulnerabilities. In addition, the organizational policies, security tools used, detection techniques and risk assessment are analysed.

The practical part of the thesis generates a proposal for the construction of the security system based on the organizational features and the existing condition of the security system. The outcome of this work can be used as a future prospect with other details and augmentations.

Keywords: Network Infrastructure, monitoring, firewall, Cyber security, DLP, SIEM, server, log management, attack, vulnerability, development, deployment, configuration.

Monitoring sítě a implementace bezpečnostního systému ve firmě

Abstrakt

Tato diplomová práce se zabývá monitorováním sítě a implementací návrhu na posílení bezpečnostního systému, který dokáže dobře bránit počítačovou síť organizačního prostředí nebo infrastruktury. Cílem práce je chránit organizaci a její zaměstnance z hlediska kybernetické bezpečnosti a zvýšit povědomí o potenciálních kybernetických útocích na vzestupu. Teoretická část práce se zabývá teoretickými základy monitorování sítí, jako jsou síťové útoky, hrozby, rizika a klasifikace zranitelností. Kromě toho jsou analyzovány organizační zásady, používané bezpečnostní nástroje, detekční techniky a hodnocení rizik.

Praktická část práce generuje návrh konstrukce zabezpečovacího systému na základě organizačních vlastností a stávajícího stavu zabezpečovacího systému. Výsledek této práce lze využít pro výhled do budoucna s dalšími detaily a augmentacemi.

Klíčová slova: Síťová infrastruktura, monitoring, firewall, Kybernetická bezpečnost, DLP, SIEM, server, správa protokolů, útok, zranitelnost, vývoj, nasazení, konfigurace.

Table of content

Introduction

Technology has evolved so rapidly that it is no surprise that where our human society stands today with millions of computers and other IoT being connected to the internet and used in our personal and professional lives. According to some reports, an estimate of 5.03 billion people around the world uses the internet today which is equivalent to 63.1 percent of the world's total population. The extent of data processed by computing devices also increases everyday, which leads to an increase in information breaches and leaks either for personal, political or monetary gains, thus giving a significant rise in Cybercrimes and Cyberwars.

Information security is in high demand due to its complexity and the limited numbers of experts in the field. Since the COVID-19 pandemic, working from home or in other words home offices have become frequent which gives hackers an easy chance to carry out their exploits. Entities like registered offices, companies, governmental bodies and other legal entities are the areas where Information security is required and if the information security system is not appropriately designed or deployed, it may face cyberattacks costing large sums of money along with the reputation of the organization, in the worse case leading to the shutdown of the organization. Therefore, it is very crucial to monitor the network and look for any security issues to avoid any attacks. Regular network monitoring can help redesign the security system if needed.

Some of the main objectives that a security professional or expert should include is securing the entire infrastructural network such as servers, routers, switches firewalls and any devices that moderate network communications within the enterprise as well as outside it. Securing servers can protect the enterprise databases and regular monitoring can help the Business and IT operations run effectively without any outages and thus minimize the negative impacts, from the business point of view.

Objectives and Methodology

Objectives

The aim of the Diploma thesis is to implementation a proposal for enhancing the security system that can successfully defend the computer network of an organization from a cybersecurity standpoint. The partial aim of the thesis is to conduct an analysis of methods and systems of monitoring, based on the contemporary risks and vulnerabilities in an organization.

Methodology

The Diploma thesis will consist of two sections, a theoretical and a practical, respectively. The theoretical section will explore the theoretical foundations of network monitoring as an element of the security system, cybersecurity, contemporary risks, threats of network attacks and classification of vulnerabilities or corporate systems. In the practical section, a multi-level check of the existing condition of the security system will be carried out using an analytical technique, namely system analysis. The method of synthesis of requirements will be used to generate a proposal for the construction of the security system based on the identified vulnerabilities and organizational features.

Literature Review

1. Basic Computer Network

A network is any collection of independent computers that communicate with one another over a shared network medium. A computer network is a collection of two or more connected computers. When the computers are joined in a network, people can share files and peripherals such as modems, printers, back up drives or USB drives. When networks at multiple locations are connected using services available from phone companies, people can send e-mails, share links to the global internet, or conduct video conferences in real-time with other remote users. When a network becomes open-sourced, it can be managed properly with online collaboration software. As companies rely on applications like electronic mail and database management for core business operations, computer networking becomes increasingly more important (Sangay Yeshi, 2011).

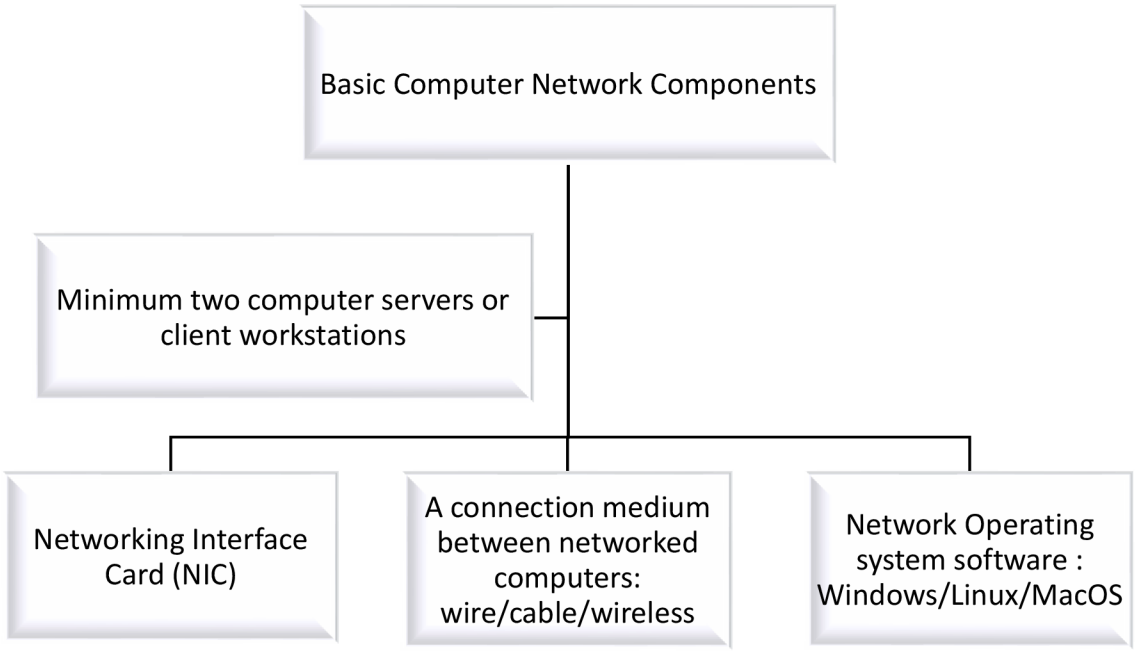

Figure 1: Basic Computer Network and its Components (Source: Author)

1.1.1 Types of Enterprise Network

When we speak of an Enterprise network, it is a regular internet but peculiar to an organization or a company. In other terms, Enterprise network can be referred to as the physical, virtual, or logical connectivity framework that enables employees, systems and applications to share data, communicate, run different services and programs and analyze the performance of the system that carries the business operations. It is configured in such a way that only a limited number of users, authorized systems and application are connected which then acts as a secure and systematized channel for communication related to particular business operations.

To set up an enterprise connection to users or employees who are at geographically different locations, then ***Virtual Private Network (VPN)*** *must be used to connect these users/employees.*

Some of the common types of enterprise networks include:

i. Local Area Network (LAN)

A LAN can be defined as a computer network that associates or link systems within a small occupied space such as a room or a building. This type of network is typically used for personal and non-commercial uses. LANs can also be set up logically or virtually inside a bigger network, for instance, each sector within the enterprise network can administer a small LAN where multiple computers are connected to the same switch but dissociated from other sectoral LANs.

ii. Wide Area Network (WAN)

WAN connection is different from that of LAN in terms of protocols and components across the layers of the OSI model which is used to transmit the data. In contrast to LAN technology, WANs are used for communication connectivity that is secure, long-ranged and dependable (Energy efficient as well). WANs are usually set up by the Internet Service Providers (ISPs) and are deployed as either a private or a public network.

*A **software-defined WAN** (SD-WAN) provides more flexible and reliable connection services which can be managed at the application level, without the need of sacrificing security and quality of service (QoS)*

iii. Cloud Network

Cloud networks and data centers provide the majority of business IT services. The IT environment may include both on-site servers and remote cloud servers.

The cloud stack may consist of multiple cloud computing models- private, public and hybrid cloud (Muhammad Raza, 2020).

- **Public Cloud** is cloud computing that is delivered via the internet and shared across the organization
- **Private cloud** is cloud computing that is dedicated solely to your organization
- **Hybrid cloud** is any environment that uses both public and hybrid clouds

Cloud networks nay be conceptualized as a WAN (typically an SD-WAN) that may include various subnets of networks that are distributed privately among clients of cloud computing services or shared among them.

1.1.2 Network Protocols

Standards called Network protocols enable computers to communicate. A protocol specifies how computers can communicate with one another through a network, the format in which data should be sent and the actions that must be taken with the data once it reaches the destination. Protocols also specify the handling of the transmissions or packets that are lost or damaged.

The three main types of network protocols used today are:

- **Communication Protocols**: include basic data communication tools like *TCP/IP* and *HTTP*.
- **Management Protocols**: the network is maintained and governed by protocols like *ICMP* and *SNMP*.
- **Security Protocols**: include *HTTPS, SFTP* and *SSL*.

Some important protocols and their functions

	Protocol	Abbreviation	Function
Communication	Hyper Text Transfer Protocol	HTTP	An application layer protocol that allows the browser and server to communicate
	Transmission Control Protocol	TCP	Separates data into packets that can be shared over a network. Sent by devices like switches and routers
	User Datagram Protocol	UDP	Sends packets of data over the internet. Works in a similar way to TCP but does not ensure a connection is made between the application and the server
	Internet Relay Chat	IRC	Text-based communication protocol. Uses software clients to communicate with servers and send messages to other clients
Management	Simple Network Management Protocol	SNMP	Used for monitoring and managing network devices. Allows admins to view and modify endpoint information to change the behavior of devices over the network
	Internet Control Message Protocol	ICMP	Used for diagnostic purposes. Managed devices on the network can use this protocol to send error messages, giving information related to connectivity issues between devices
Security	Secure Socket Layer	SSL	Ensures secure internet connections and protects sensitive data. Transferred data is encrypted
	Secure File Transfer Protocol	SFTP	Secures transfer files across a network. The client and server are authenticated
	Secure Hyper Text Transfer Protocol	HTTPS	Secure version of HTTP. Data sent is encrypted to provide protection

Table 1: Important Protocols and their functions (Source: Author)

1.2 The OSI Model

The OSI model was first created to promote vendor compatibility and provide precise standards for network communications. The earlier TCP/IP paradigm, however, is still widely used as the standard architecture for internet communications today (bmc, 2018).

1.2.1 The 7 layers of the OSI Model

Unrelated to the underlying technological infrastructure, the Open Systems Interconnection (OSI) reference model is a conceptual framework that covers networking or telecommunications system operations. To ensure the interoperability inside the communication system regardless of the technology type, vendor and model, it splits data transmission into seven abstraction layers and standardizes protocols into suitable groupings of networking capabilities.

Enterprises continue to have the most anxiety about cybersecurity, especially small firms. Any layer in the OSI Model maybe the target of a DDoS (Distributed Denial of Service) attack, but with timely monitoring and the use of security measures like zero trust, an IT admin could immediately isolate the issue before it spread to other layers.

There are several portions of the OSI Model that do match to TCP/IP. Basically, one may divide ant TCP or UDP packets into various portions and assign a layer number to each section. The image (Figure 2, Pg.17) illustrates the seven layers of the ISO model. The OSI model is a reference model and does not define any specific protocol or technology. It provides a standard for the development of communication protocols and ensures that devices from different manufacturers can interoperate with each other. The OSI model is vendor-neutral and does not favour any specific technology or protocol. This ensures that the model can be applied to a wide range of networking technologies, and allows for innovation and competition in the industry.

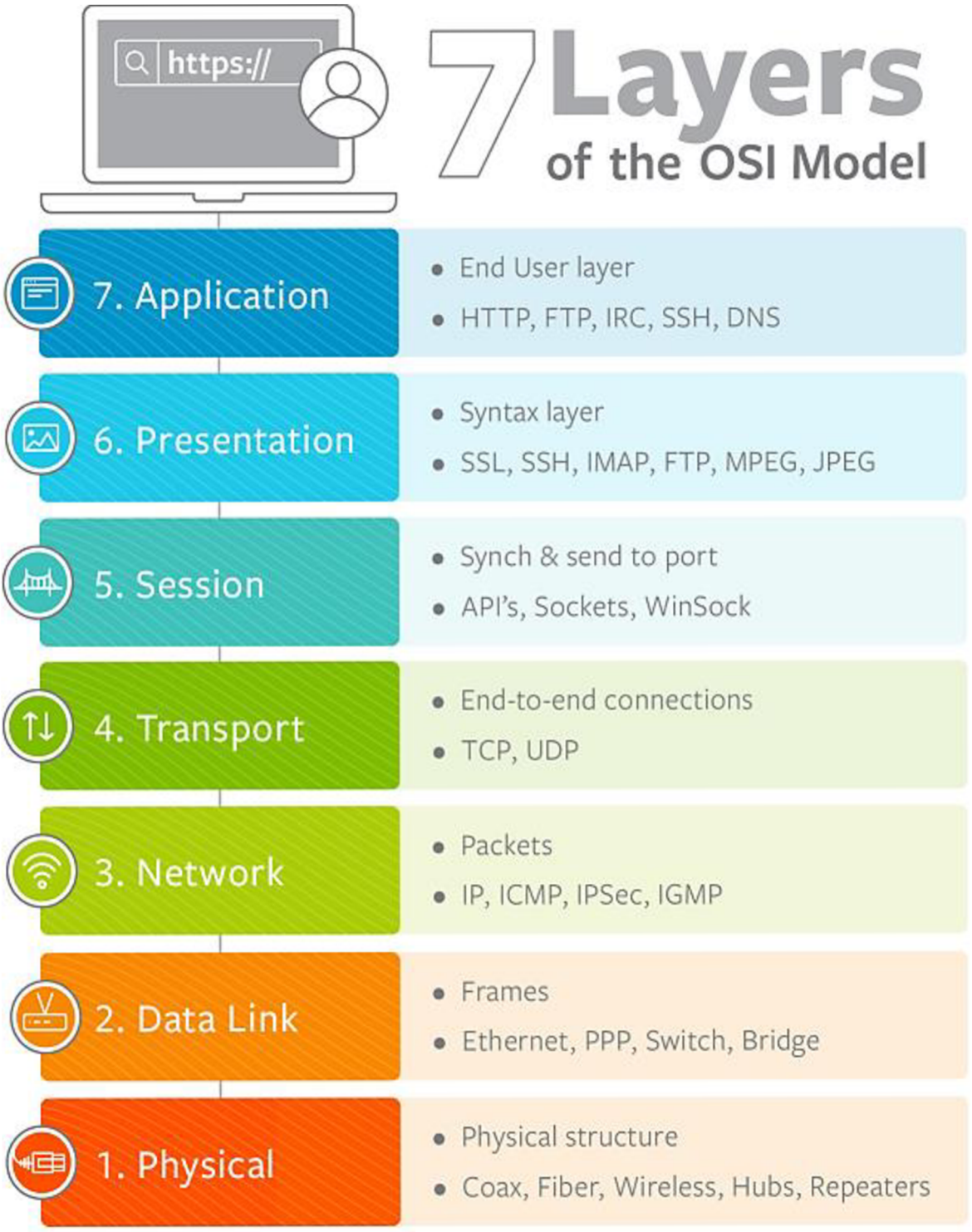

Figure 2: The seven layers of the OSI Model (Source: bmc, 2018)

1.3 TCP/IP Internet Model

TCP/IP is a protocol that specifies how data is dent from a sender to a receiver. Although a web server response might appear to be virtually instantaneous, several infrastructures and procedures support this seemingly unimportant task in the background.

1.3.1 Functions of TCP/IP Model

The functionality of TCP/IP model is divided into four layers and each layer includes specific protocols. TCP/IP is a layered server design framework in which each layer is characterized according to a particular work to perform.

Figure 3 below illustrates the layers of TCP/IP

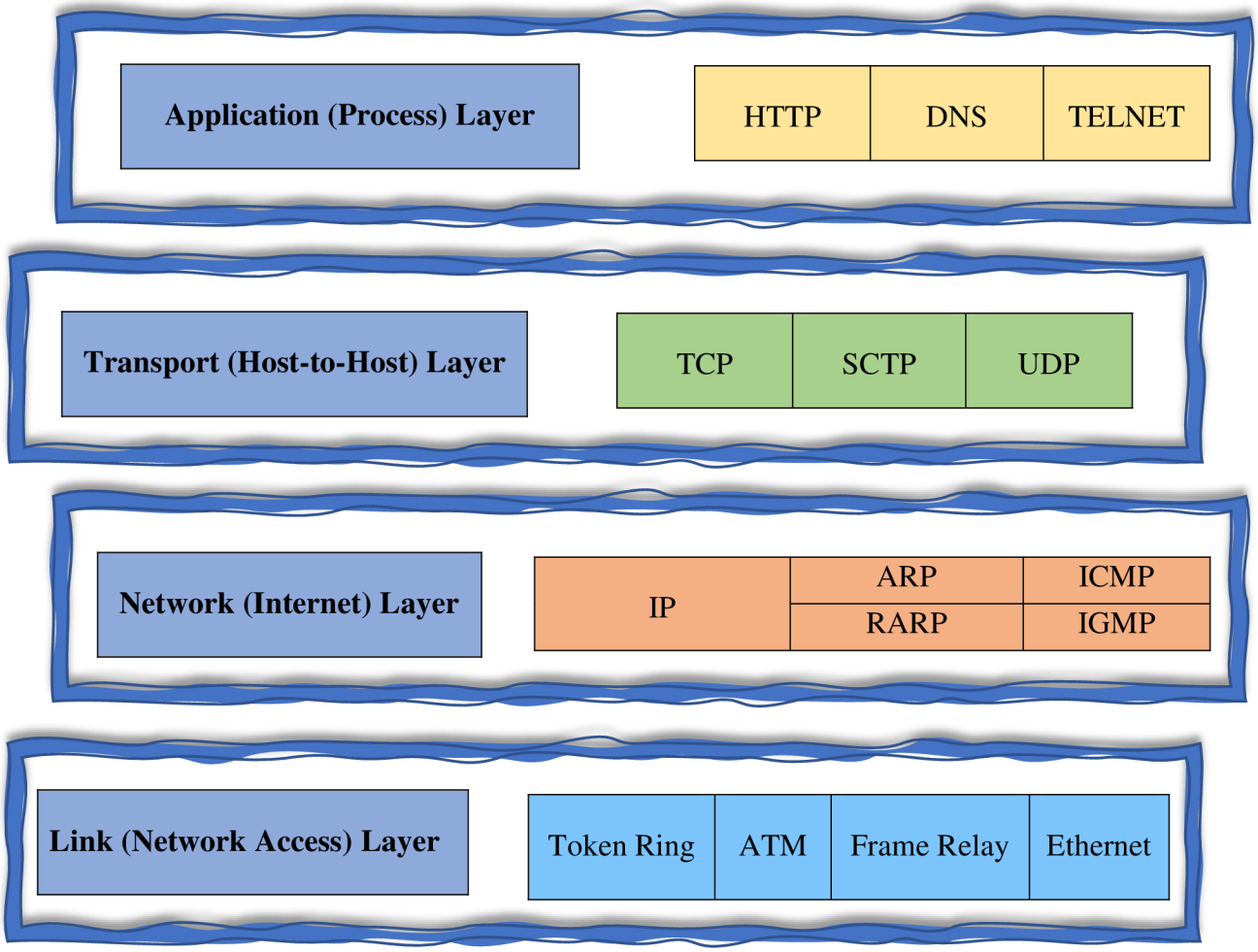

Figure 3: The four layers of the TCP/IP Internet Model (Source: Author)

1.3.2 Application Layer

The Application layer is the topmost layer of the OSI and TCP/IP layered models. It is in charge of high-level conventions and typical concerns. It is through this layer that the client may associate with the program and when one application layer protocol desires to associate with another, it sends its data to the transport layer (NORTHCUT, S., NOVAK, J., 2003). One may find few instabilities in the application layer. But for those that interface with the communication framework, no application may be conveyed inside the application layer.

The most common **application layer** protocols are:

SNMP: Simple Network Management Protocol is a framework that uses the TCP/IP protocol stack to manage devices over the internet. SNMP is usually linked to managing routers but also it can be used to manage many other types of devices such as switches and servers etcetera (MAURO, D., SCHMIDT, K., 2005).

HTTP: Hyper Text Transfer Protocol is a protocol for transferring data over the internet into a variety of forms such as audio, video and plain text.

SMTP: Simple Mail Transfer Protocol is an e-mail handler protocol in the TCP/IP when the data is being sent from one e-mail to another e-mail address.

TELNET: Terminal Network links local and faraway terminals so that the local terminal appears to be a remote terminal.

DNS: Domain Name System is a service that converts a host's name to an IP address. It is a disseminated database that is executed as a ranking order of name servers and this service lets clients and servers send and receive messages.

FTP: File Transfer Protocol is a protocol that is responsible for transferring data from one computer to another. FTP uses two parallel TCP connections (control and data connections) to transfer a file.

1.3.3 Transport Layer

The Transport layer is below the application layer which handles information dependability, flow control, and redress as information moves over the network. At the Transport layer, two protocols are used: *User Datagram Protocol* and *Transmission Control Protocol*.

User Datagram Protocol (UDP)

The User Datagram Protocol recognizes the issue and the ICMP protocol informs the sender that the user datagram has been corrupted or damaged. Since UDP has a checksum, it does not have any data segment ID and cannot specify how a packet is lost.

Transmission Controlling Protocol (TCP)

TCP is a reliable protocol since it identifies botches and retransmits corrupted frames. Thus, all fragments must be received and recognized prior to the transmission is considered complete and a virtual circuit is eliminated. TCP separates the complete message into minor pieces known as fragments at the transmitting end. Each fragment carries an arrangement number utilized to reorder the frames to reconstruct the original message.

1.3.4 Network Layer

The Network layer is below the transport layer and is referred to as a reliable protocol since its mechanism ensures data delivery, and User Datagram Protocol, which makes no promise of reliable delivery. For example, TCP is required because of the unacceptability of data loss (NORTHCUT, S., NOVAK, J., 2003).

The primary protocols of the **network layer** are:

IP: Internet Protocol is accountable for transmitting packets from a source host to a destination host based on the IP addresses in the packet headers. IPs are divided into two categories: *IPv4* and *IPv6*.

ICMP: Internet Control Message Protocol is stored within the datagrams and is necessary for providing hosts with network issues.

ARP: Address Resolution Protocol is used to identify the hardware address of a host-based on a given IP address. There are four types of ARPs namely, *reverse ARP, proxy ARP, gratuitous ARP* and *inverse ARP*.

1.3.5 Link Layer

The Link layer is the bottom most layer of the TCP/IP and is largely responsible for data transmission between two networked devices, performing functions such as encapsulating IP datagrams into network infrastructure and converting IP addresses to physical addresses.

One interesting fact about the Link layer is that it can use different access methods to transmit data over a physical link. The most common access methods used by the Link layer are the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) and CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) methods.

Some of the Link layer protocols are:

Token Ring: This protocol was initially developed by IBM but then standardized by IEEE with 802.5 specifications. It is a LAN protocol that uses a token-passing media access technology in physical ring that creates a logical ring topology.

Ethernet: Ethernet is not called a protocol. It is one of the most popular and oldest LAN technology and is frequently used in LAN environments which includes almost all networks like offices, homes, enterprises and public places. 802.3 Ethernet is the most common ethernet and provides a means of encapsulating data frames that are to be sent between computers. Ethernet has acquired mass popularity due to its maximum rates over longer distances using optical media.

Frame Relay: It is a complete set of protocols to a provide circuit-emulating packet transport mechanism. Generally, it is used to carry high-level protocols like IP.

ATM: The Asynchronous Transfer Mode protocol is designed to support the transfer of data with a range of guarantee for the quality of service. The ATM protocol divides the user data into small and fixed-length packets and transports it via virtual connections.

1.4 Encapsulation and Decapsulation in TCP/IP

When the data moves from the upper layer to the lower level of TCP/IP protocol stack (active transmission), each layer incorporates a bundle of important data collected called a header along side the real data. The information bundle containing the header and the data from the upper layer at that point gets to be the data that is repackaged at the following lower level with the lower layer's header (*header is the supplemented information put at the starting of the block of information when it is transmitted*). The supplemented data is utilized at the accepting side to extricate the information from the encapsulated data packet. The packing of information at each layer is known as **data encapsulation** (see Figure 4). The reverse process of encapsulation, called **decapsulation**, happens when data is received on the destination computer (Dr, Raid Alubady, 2017).

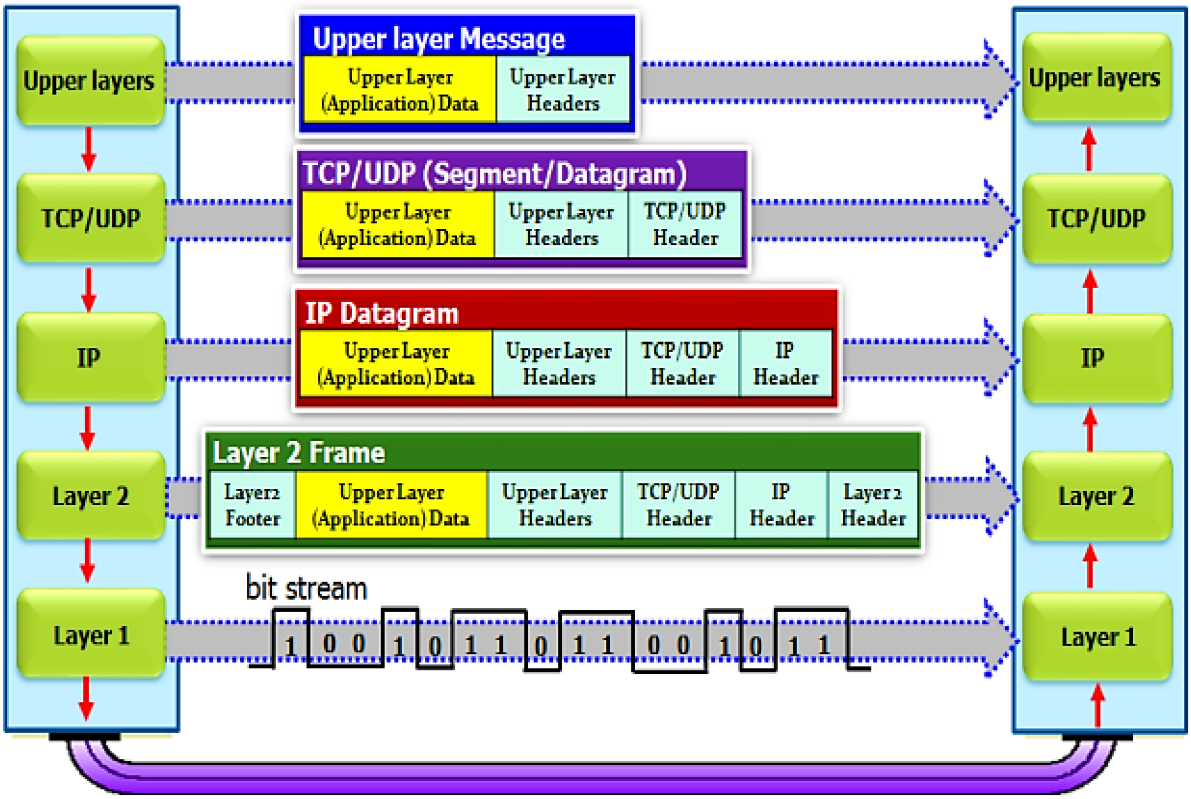

Figure 4: Encapsulation & Decapsulation TCP/IP (Source: Dr. Raaid Alubady, 2017)

1.5 Devices on Enterprise Network

An Enterprise Connected Device (ECD) is any device that interacts with, stores or processes an organization's data. Thanks to the wide range of devices, ECD can also cover other categories of devices depending on their purpose.

ECD can cover several other classes of devices, including:

- **End User Devices**: Laptops and smartphones.
- **Internet of Things**: IoT is the physical devices connected to the internet which collect and share data. IoT has added sensors and mechanism to interact with their surrounding environment to communicate in real-time data without a human being.
- **Distinct ECDs**: Devices That are primarily designed for use in an enterprise setting.

Risks, Vulnerabilities, data theft, malware in Enterprise Connected Devices

ECDs are a very attractive targets for various types of attackers because they can contain valuable, sensitive or personal information. Due to the vendor's limited security efforts, large attacks surface and lateral movement attack base, they become an easy target for compromise. The sheer number of ECDs connected to the internet brings with it a wave of products that are potential targets for both espionage and financially motivated cyber crimes.

The COVID-19 pandemic has increased remote work, and ECD has played an important role in supporting business continuity worldwide during the COVID-19 crisis. This has given organizations to be more innovative while creating new opportunities for threat actors.

One of the greatest threat to ECDs are botnets malware which creates IoT botnets and therefore attacking enterprise on a wider range. Generally, botnets have been used for coordinated DDoS attacks, however there are also botnets that are capable of exfiltrating sensitive information. Therefore, it is very crucial to secure the ECDs by carrying out regular risk assessments, vulnerability scans, hardening, patching, mitigation and remediation.

The below flow chart represents the hardening of all the possible ECDs along with its application and operation systems for stricter security.

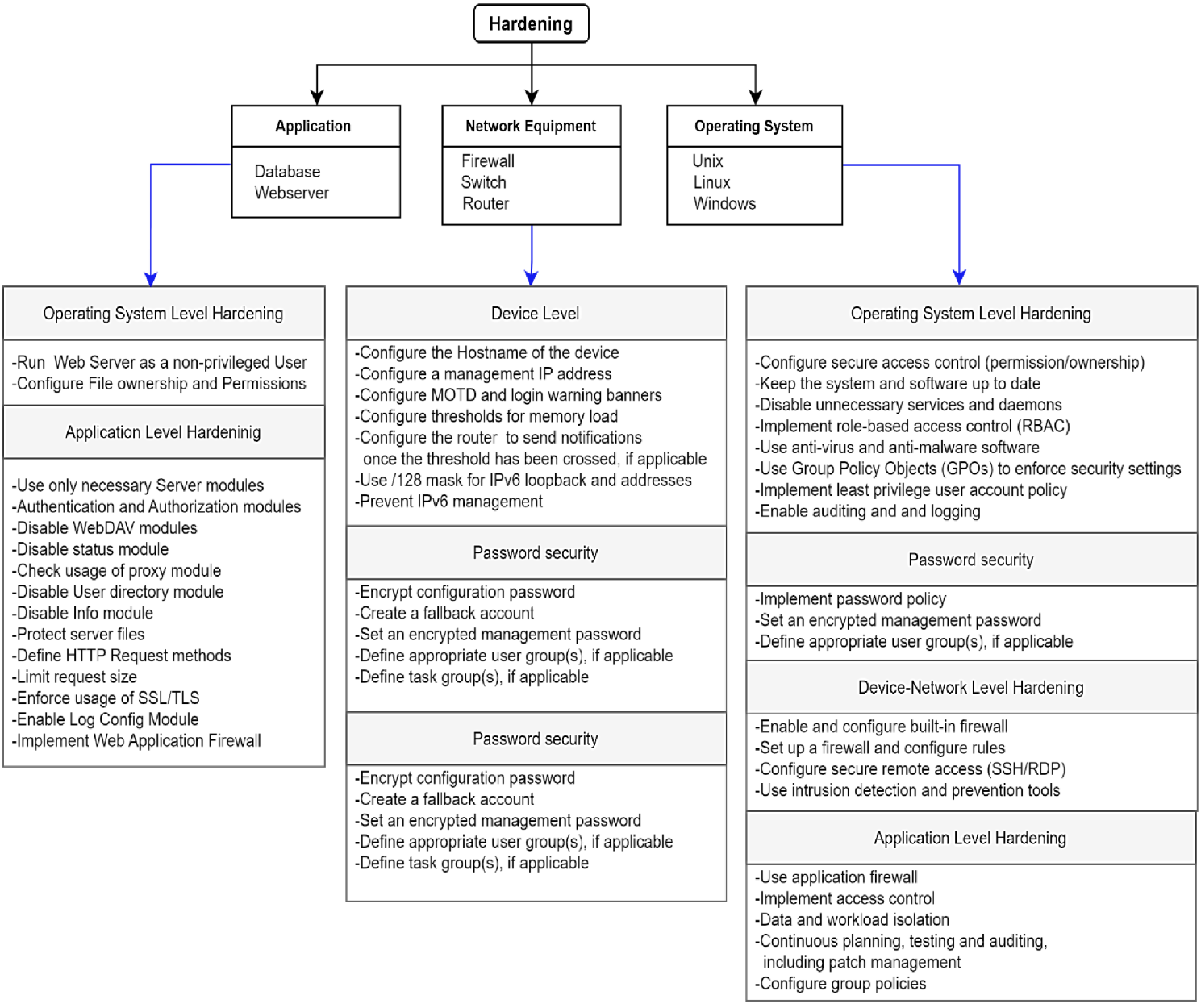

Figure 5: Hardening of ECDs (Source: Author, UML – Unified Modelling Language)

1.6 Network Monitoring

1.6.1 Network Security

Network security is the requirement needed for the implementation of secure networks, network infrastructure, system and services zones, wireless local area networks and remote access solutions within an enterprise or organization.

Network security outlines the controls required to secure all elements of enterprise's network, whether it is internal or internet-facing (external). According to the **Cyber and Information Security** policies, first and foremost, it is a must to secure the connections between systems, both internally and externally, to protect communications from an unauthorised access or modification first.

The main scope of Network Security are as follows:

- Internal networks
- Fixed line networks
- Cloud/Hosted Networks
- Mobile networks
- 3rd Party/External connections

1.6.2 Network Monitor

The process of continuously checking a computer network for errors or flaws to maintain network performance is known as network monitoring, sometimes known as network management. Although the two concepts are identical in practice, network monitoring maybe thought of as a subset of network management technically. Network monitoring collects data which is filtered and analyzed to identify the variety of network problems such as:

- device failures
- link outages
- interface errors
- packet loss
- application response time
- configuration changes

Some basic requirements and policies implemented by enterprises in network monitoring:

1. The network parameter must be monitored to detect Distributed Denial of Service (DDoS)attacks. Network traffic from unidentified sources must be redirected in order to prevent service degradation

2. Services and access must be monitored for misuse, malicious behavior, and operational stability

3. In case of any unapproved changes to a network are identified these must be reversed, and a risk assessment must be performed to identify whether a security incident has occurred or not

4. SMS and MMS traffic must be filtered, and malicious or suspicious messages which meet pre-defined filter criteria must be blocked

5. Outgoing user web traffic must be monitored and blocked as required to prevent access to inappropriate or malicious content.

6. IP Route Hijacking, BGP connected internet networks must be monitored for threats and unauthorized route changes.

7. The network traffic and perimeter to and from the Internet must be monitored to detect cyber-attacks and block malicious traffic to prevent service degradation and intrusion attempts.

8. Potential attacks must generate alerts which are responded and remediated as required

*A **Zero-Trust Model** is a security model that requires strict authentication for every user and device trying to access resources on a network, regardless of whether they are located within or outside the network perimeter. This model is a comprehensive approach to security that can help organizations protect their sensitive resources from potential threats. By assuming that all users, devices, and traffic are potentially malicious, the Zero Trust model helps organizations to ensure that only authorized users and devices are granted access to sensitive resources.*

1.6.3 Logging and Monitoring

Logging is the process of collecting and recording information about events while ***Monitoring*** is the provision of a business process that provides the review of possibly filtered/ aggregated/ consolidated/ correlated logging information, investigations initiated where necessary to detect potential misuse, breach, attacks and other follow-up as required.

Logging and Monitoring in an enterprise/organization are applied to its IT and Network systems, and other supporting Infrastructure.

Logging and Monitoring can be further classified into Logging Scope; Logging Management; Logging Attributes; Monitoring and Response; Reporting Requirements and Retention and Archiving.

1.6.3.1 Logging Scope

The scope of systems that require logging and monitoring must be defined using a security impact assessment and the assignment of a risk level to each system.

a) Areas of the greatest risk must be addressed first, with priority given to critical applications, servers, databases, core network elements and security devices

b) All the systems that are in the scope of logging activities must be recorded and retain logging information sufficient to answer the following questions:

- What activity was performed?
- Who/What performed the activity?
- What system or asset was the activity performed on?
- From which location or on what system was the activity performed?
- When was the activity performed?
- What tool(s) was the activity performed with?
- What was the status, outcome, or result of the activity?

1.6.3.2 Logging Management

Log management is the best practice of continuously gathering, storing, processing, synthesizing, and analyzing data from disparate programs and applications to optimize system performance, identify technical issues, manage resources well, strengthen security and improve compliances.

a) Logs must be protected from unauthorized access, modification and deletion according to their classification and the requirements of the Information Classification and Protection requirements set by the individual organization, both during storage and when in transit.

b) Sufficient space must be allocated for log storge on all systems. Systems must be configured to continue logging without disruption even if event log storage reaches a maximum size, to prevent log data from being lost.

c) Design and maintenance documentation for all systems must include information on how and when logging should be configured (e.g., event types, access, storage).

d) Secure access control must be used to restrict access to logs to only those users who have a legitimate requirement.

e) Where logging is required, it must be enabled at all times, performed on a standardized basis using a standard format and configured to corporate sufficient event attributes to answer the questions defined in the requirement set by the corporate/organization.

f) Alerts must be configured to:

    i. Identify an activity that could affect log integrity or availability, e.g., log resets, error conditions and storage failures

    ii. Identify when logging is inactive without proper authorization

    iii. Identify any amendment or deletion of logs

Logging management is a critical component of enterprise security and compliance. Organizations must demonstrate that they are collecting and storing logs in accordance with regulatory requirements. In addition to security and troubleshooting, logging management is also important for auditing purposes.

1.6.3.3 Logging Attributes

Each log entry must have enough details to support the desired monitoring and analysis in the future. Although there could be entire content data, an extract or only summary of attributes are most likely to suffice. Each event "when, where, who, and what" must be documented in the application logs.

As a minimum, logs must be created whenever any of the following activities are requested to be performed by the system:

i. Create, read, update, or deletion of information
ii. Initiate a network connection
iii. Accept a network connection
iv. User authentication and authorization, e.g., user login and logout
v. Activation and deactivation of protection mechanisms such as anti-malware
vi. Application process start-up, shutdown, or restart
vii. Detection of suspicious/malicious activity from IDS/IPS, anti-malware or EDR

Logging must avoid capturing any confidential information that is not required for identifying security events of interest, e.g., unnecessary personal data collection. If this information must be captured for a specific purpose, then it must be protected.

1.6.3.4 Monitoring and Response Plan

In Monitoring Plan, data is collected to check the ongoing health of the improved process. It is the initial stage set for the Response plan. The Response plan creates a threshold level for each measure in the Monitoring Plan. Monitoring and analysis of logs and security events must focus on identifying the following attack types using the global standard MITRE ATT&CK Framework:

i. Malicious, compromised, or exploited software
ii. Vulnerability exploitation
iii. Account hijack
iv. Social engineering
v. Denial of service
vi. Website attacks
vii. Access abuse
viii. Telecoms interception
ix. Data exfiltration

1.6.3.5 Reporting Requirements

Reporting on the performance of logging and monitoring activities must be provided to management which covers as a minimum:

i. Trends of events over the period, including a breakdown by business area and geographic location and event type
ii. Outcomes of monitoring (events/incidents raised, results of analysis etc.)
iii. Performance of detection and defense mechanism
iv. Summary of current audit and compliance check results
v. Log integrity concerns such as log rests, error conditions, failure, and threshold exceptions
vi. Operational status and availability of logging/monitoring platforms and storage

1.6.3.6 Retention and Archiving

Generally, all logs must be retained for the periods stated by the organization, unless local legal, regulatory, or contractual requirements dictate a change of longer/shorter retention periods. All logs are stored online (with exceptions) to allow timely access to log data during investigations and stored in a format that can be accessed in an effective manner by the users who require access to them, even if they have been archived.

1.7 SNMP

In today's complex network of routers, switches and, and servers, it can seem like a daunting task to manage all the devices on your network and make sure they are not only up and running but performing optimally. The core of SNMP (Simple Network Management Protocol) is a simple set of operations (and the information these operations gather) that gives administrators the ability to change the state of some SNMP-based devices (MAURO, D., SCHMIDT, K., 2005).

SNMP is based on a client-server model, where the network devices act as servers and the network management system (NMS) acts as a client. The NMS sends demands/requests to

the devices and the devices react with data about their current status and performance. SNMP utilizes a various leveled structure called the Management Information Base (MIB) to organize the data is gathered. The MIB characterizes a set of factors (also known as Object identifiers or OIDs) that compare the diverse viewpoints of the device's execution and performance.

SNMP can be sued to monitor a wide range of information/data, including:

- Device uptime and availability
- CPU and memory usage
- Network traffic and bandwidth usage
- Temperature and power status
- Error and event logs and many more

SNMP can be utilized in various diverse network monitoring and management scenarios, such as:

- Monitoring the execution and accessibility of network devices
- Gathering of performance information for capacity planning and forecasting
- Identifying and investigating network issues
- Detecting and cautioning on security breaches and security-related incidents.

SNMP has several versions, the foremost broadly utilized are SNMPv1, SNMPv2c, and SNMPv3. SNMPv3 is considered to be the most secure form of SNMP because it incorporates highlights such as authentication and encryption to prevent unauthorized access to network devices.

It is important to note that SNMP can be vulnerable to certain security dangers and threats, like SNMP enumeration and SNMP amplification DDoS attacks. Subsequently, it is recommended to use SNMPv3 and legitimately configures the SNMP settings, including access control and encryption, to secure against these kinds of attacks.

1.8 Cyber Security Testing

Cybersecurity testing is the process of evaluating the effectiveness of the security controls in place to protect against cyber threats. It is an essential aspect of overall cybersecurity strategy, as it helps to identify vulnerabilities and weaknesses in the system and provide actionable recommendations to mitigate them (Mark Stone, 2021).

There are different types of cybersecurity testing, each with a specific purpose and scope. Some of the common types of cybersecurity testing are:

I. **Penetration testing:**

Also known as Pen Testing, this sort of testing reenacts the attacker's activities to distinguish and misuse vulnerabilities. Penetration testing is ordinarily more in-depth than vulnerability scanning and can incorporate manual testing strategies, such as social engineering and phishing attacks.

II. **Compliance testing:**

This type of testing is used to determine whether and organization is compliant with regulations and standards such as HIPAA, PCI-DSS, and others.

III. **Network security testing:**

This type of test centers on assessing the security of the network infrastructure, including firewalls, routers, switches, and other network devices. It can recognize issues such as misconfiguration, weak passwords, and other vulnerabilities that maybe exploited by an attacker.

IV. **Application security testing:**

This type of test focuses on evaluating the security of applications, both web and mobile. It can identify vulnerabilities such as cross-site scripting, SQL injection, and other issues that can be abused by an attacker.

V. **Vulnerability scanning:**

This type of testing includes automated tools that can scan the network, servers and other devices for known vulnerabilities. It can also identify missing patches, misconfigurations, and other issues that could be exploited by an attacker,

VI. **Red team testing:**

This type of test mirrors a real-world attack scenario, simulating a comprehensive attack campaign to test the capacity of the organization to detect and respond to a cyber attack.

It is critical to note that cybersecurity testing should be an ongoing process, as threats and vulnerabilities advance over time. It is suggested to conduct tests regularly and update security controls accordingly. Moreover, it is also critical to have an incident response plan and to conduct regular incident response and disaster recovery testing to ensure readiness in case of a security breach.

1.8.1 Lifecycle of a Penetration Test

1. Raising and scheduling a demand
2. Test scoping and requirements gathering
3. Testing or retesting
4. Report writing
5. Quality assurance
6. Report delivery
7. Post test clean-up

1. **Raising and scheduling a demand**

The test must be requested in line with testing frequency and coverage requirements. The company must specify the System Owner of the target system(s), if the company is not the System Owner, then System Ownership information must be provided in advance of the penetration test start date.

An engagement questionnaire has to be completed and submitted within the demand, and comprises the following questions:

- ✓ Is this a Flagship Internet-facing asset? [Yes/No]
- ✓ Is this a Mission Critical asset? [Yes/No]
- ✓ Is this a Critical asset? [Yes/No]
- ✓ Is this asset internet accessible? [Yes/No]

- ✓ Has a penetration test been conducted in the last 24 months? [Yes/No]
- ✓ Was a penetration conducted at the last major release? [Yes/No]
- ✓ Is this an application enrolled in web application vulnerability scanning? [Yes/No]

2. **Test scoping and requirements gathering**

The tester scoping the penetration test must ensure they have collected sufficient data from project teams to ensure the penetration tester has enough information to accurately understand and test the target system. During the scoping call, the scoping tester should ensure that all the target testing is performed on non-production systems which are representative of the production build, such as contingency or pre-prod systems where possible.

Limitations may include:

- Inability to accurately fuzz parameters due to potential for Denial of Service
- Inability to perform exploits that may unintentionally have an adverse effect on the target system
- Testing scope may be reduced to limit exposure to sensitive production-level information

Although every attempt will be made to minimize the potential impact of testing on production, risks may include:

- Denial of Service, users may not be able to access the production system
- Unintended side effects or impacts on other production systems
- System or data corruption
- High levels of alerting
- Inaccurate system logs full of activity generated by the penetration test
- Skewed analytics

Minimum information required for the penetration testing: Source IP address, Target IP address, Timeframe for testing, Tester contact information, Demand ID, Test requestor contact information, Local market or Group Entity hosting the target system(s), Technical contact, where the testing is happening on the internal network, the MAC address of the source machine should be provided as well.

3. **Testing or retesting**

Testing must always be restricted to assets inside the agreed scope. Any vulnerabilities discovered or suspected on assets connected to it. In case of automated testing, it must be performed with care, making sure that the testing does not exhaust the resources of the target system. Upon test completion, testers must keep all logs from testing for a defined period of time after the report has been delivered to the project etc. The tester is obliged to alert the System Owner to any critical findings identified that could impact a production system as soon as possible on the day of discovery.

4. **Report writing**

Due to the report being the only deliverable seen by a Test requestor, the tester has to ensure the report is written with the utmost care and attention. All reports must contain, at a minimum the following elements:

- ***An executive summary***: outlining the tester's knowledge of the application and how the findings discovered during the test affect the risk of the application and the business. Executive summaries are ought to avoid complex technical language and be written to ensure comprehension by non-technical individuals.

- ***Finding writeups***: that are presented in a comprehensible and reproducible format. Testers may ensure that their guidance is suitable for those who may not have experience in penetration testing and utilize tooling that is easily accessible to all.

- ***Finding remediation***: Where possible testers should provide high-level guidance to developers an System Owners to assist in the remediation of the finding. Remediation information must be relevant to the technologies and system versions tested.

- ***Approved reporting template***: Use of the approved reporting template which can be either provided by the System Owner of the tester and must not contain any sensitive information such as HTTP authorization headers, sensitive cookies values, session tokens, API (Application Programming Interface) tokens, Personal data that could result in unauthorized access to the environment.

5. **Quality assurance**

All security test reports must undergo quality assurance before they are distributed to the Test requestor, comprising of both a peer review and a technical management review. Peer review is an in-depth look at the report, which must evaluate and identify the following as a minimum:

- Potentially missed findings, e.g., the tester shows a HTTP response with an outdated server in the 'server' header but has not raised an individual finding
- Potentially missed exploit paths
- Automated tooling outputs have been entered verbatim into the report
- Comprehension of the target application and impact of vulnerabilities
- Spelling, grammar or explanation of the finding
- Report layout
- Methodology sheet is included and completed
- The redaction of sensitive information stored within screenshots or snippets
- Adequate risk ratings have been applied to the findings

6. **Report delivery**

The security testing team has a Service Level Agreement of predefined days (e.g., 5 days) for report delivery following completion of penetration testing. This time is inclusive of report creation, peer review and management QA, testers should account for this time when writing the report.

7. **Post test clean-up**

The are required to ensure any modifications or uploads made to the target system are removed and reverted where possible. In the event the tester is not able to revert changes they have made; they must inform the Test requestor. Testers should make use of the appendix section of the report to inform the project of any changes that could not be reverted.

1.9 Incident management

1.9.1 Definitions

Availability: Maintaining and assuring the ability to access data at the required time, in the required format, for the required purposes.

Chain of Custody/Continuity: The chronological documentation of paper trail showing the seizure, custody, control, transfer, analysis, and disposition of physical or electronic evidence.

Confidentiality: The property that information is not available or disclosed to unauthorized individuals, entities, or processes.

Corporate Invoicing: When a product is given to a customer so is an invoice. It must contain certain information such as a unique identification number, a clear description of the goods and company contact information.

Electronic/Forensic Evidence: Electronic evidence is information in a digital format (including records and digital media) that is used to establish proof of factual allegations or arguments.

Integrity: Maintaining and assuring the accuracy and completeness of data over its entire life cycle to prevent unauthorized or undetected modification of that data.

Intrusion Detection System (IDS) or Intrusion Prevention System (IPS): Security measures deployed in the network to detect and stop potential incidents. IDS analyses network traffic for signatures that match known cyber-attacks. IPS analyses but can also stop an attack depending on what it detects.

Personal Data: Any information relating to an identified or identifiable natural person: one who can be identified directly or indirectly by reference to an identifier such as a name, an identification number, location data, an online identifier, to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person.

1.9.2 Definition of a Cyber-Incident

A Cyber-Incident occurs when there is a breach of explicit or implied digital security policy or when any activity requires corrective action because it threatens the confidentiality, availability, and integrity of an information system or the information the system processes, stores or transmits. Cyber-Incident may originate from a single or multiple cyber-security events. Examples of cyber-incidents include, but are not limited to:

- Denial of Service attacks (DoS) that affect system or service availability
- Virus or malware outbreaks, including ransomware
- Compromise or disclosure of sensitive or personal information
- Compromise of network credentials or an email account

1.9.3 Cyber-Incident Management

Cyber-Incident management is the process of handling all cyber-incidents in a structured and controlled way. Incident management brings together and governs the coordinating functions that guide, inform, and support the whole response process. It includes:

- Tracking, documenting, assigning, and correlating all findings, tasks and communications which could be reviewed by regulators or courts.
- Arranging of regular update meetings or calls and involvement of relevant teams
- Escalating serious incidents to senior management
- Ensuring the incident is communicated appropriately
- Ensuring that the full incident lifecycle is covered from initial identification through to lessons learned.

Key points for Cyber Incident Management:

1. Preparation: Having an incident plan in place before an incident occurs.
2. Speed: The faster an incident is detected and contained; less damage will be caused.
3. Communication: Establishing clear lines of communication both with internal and external stakeholders is essential.
4. Document everything: keeping detailed records of the incidents
5. Continuously improve: Incidents can provide valuable lessons for improving incident response processes and security measures.

1.9.4 The Problem Management Process

Information Technology Infrastructure Library (ITIL) defines the purpose of Problem Management as "reducing the likelihood and impact of incidents by identifying actual and potential causes of incidents and managing workarounds and known errors" (ITIL, Problem Management).

BMC (The governing body of ITIL practice) describes three phases of Problem Management.

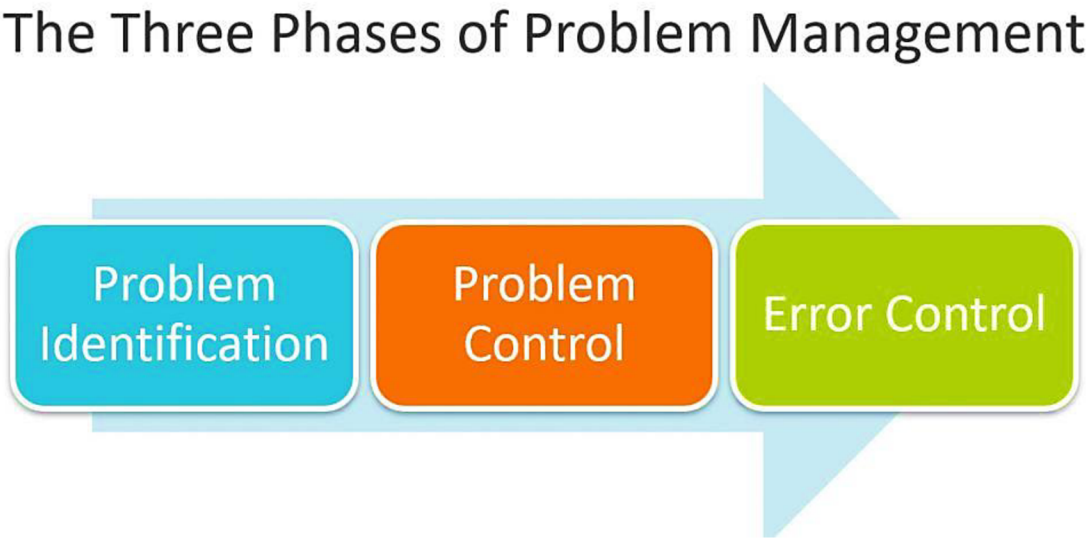

Figure 6: The three phases of Problem Management (Source: bmc, 2018)

1.9.4.1 The Three Phases in More Details

1. **Problem Identification**

The goal of problem identification is to identify and record Problem Management cases. The Problem Management process is carried out through many activities that are often referred to as **Reactive** or **Proactive**.

Reactive (as a result of a Problem Management investigation following an incident)
Proactive (based on patterns or other markers and not an action directly from an incident)

Examples of these activities are:

- Conducting a trend analysis of incident records
- Identifying repeat incidents
- Identification of risks, potential reoccurrence or worsening of impact
- Analyzing information received from colleagues, partners, and vendors or project teams, including the incident timeline.

2. **Problem Control**

Problem control activities include an overall analysis of the incident, including symptoms, services affected, and the risk internally and externally, what occurred, what was done to intervene, and how well the intervention worked. Control activities can also include recording known errors, managing the transition from temporary fix and containment to a permanent resolution or acting proactively based on intelligence received on known threats and vulnerabilities.

An essential activity in the Problem Control phase is ensuring that any actions that are carried out are recorded and tracked, including all containment actions, lessons learned and impacts to the Cyber security control framework. ITIL describes temporary fixes as "Workarounds" and defines them as actions taken before a root cause is fully known or fully fixed. In Cyber Security, a workaround may include containment activities such as isolation of assets or resetting of credentials. To this end, Problem Management should contribute to the upkeep of the guidelines used to plan and execute the incident response. A workaround or containment action can become the permanent fix in rare cases, i.e., if it is impossible to introduce a permanent solution through technical or financial constraints.

3. **Error Control**

Error control activities cover the management of known errors known as threats and vulnerabilities. When a known threat or vulnerability is found during a PIR (Post Incident Review), it is the responsibility of the Problem Manager to document the threat or vulnerability and invoke the required processes. Other proactive error control activities can include the periodical assessment of trend data such as root cause reporting and tracking.

<u>Key points of Error Control</u>

- Identifying the root cause
- Implement solutions
- Monitor the effectiveness of the solutions
- Continual improvement
- Communication
- Documentation
- Compliance

1.9.4.2 Problem management Relationships with other ITIL Functions

a) Incident Management

Problem management activities are closely related to Incident management. It is essential that a Problem Manager has a clear understanding of the incidents and works closely with Incident Management to ask the right questions and resolve gaps.

b) Risk Management

Problem management activities aim to identify, assess, and control risks; therefore, it is necessary for Problem Management to work closely with the risk management functions and adopt a local risk management process. Any identified risks should be tracked and recorded in a local register.

c) Change Enablement

Change Management will typically be managed by the affected local market; however, Problem management should document post-incident change management activities within the problem case file and be conscious of local market change restrictions.

d) Knowledge Management

Knowledge management is a crucial function of effective reactive and proactive Problem Management. A Problem Manager must record findings and recommendations and ensure that they are cascaded to the relevant teams to take the necessary actions. Effective Knowledge Management within a Problem Management process can also be utilised as a tool by other teams during the assessment and diagnosis of incidents.

e) Continual Service Improvement (CSI)

Often the output from Problem management cases identifies opportunities for service improvement. These opportunities and any subsequent resolutions should be documented in Post Incident Review actions (PIR) and a Continual Service Improvement Register which is then highlighted within the Problem Management reporting.

1.10 Intrusion Detection System (IDS)

Monitoring activity within a computer system or network and looking for indications of intrusion-defined as attempts to compromise the confidentiality, integrity, and availability of a computer system or network is called the process of Intrusion detection. Attackers using the internet to gain access to the systems authorized users attempting to obtain privileges they are not authorized to have, and authorized users abusing those privileges are all examples of intrusions. The monitoring and analysis process is automated by intrusion detection systems (IDSs), which can be either software or hardware.

The most common way to classify IDSs is to group them together by information source. To identify attackers, some IDSs examine network packets that have been captured from LAN segments or network backbones. Other IDSs search for signs of intrusion in information produced by the operating system or application software. Types of IDSs are Network-Based IDSs (NIDS), Host-Based IDSs (HIDS), and Application-Based IDSs (AIDS) (NORTHCUT, S., NOVAK, J., 2003).

1.10.1 Network-Based Intrusion Detection Systems (NIDSs)

Network-Based intrusion detection systems make up the vast majority of commercial systems. These IDSs track and examine network packets to find attacks. One network-based IDS can monitor the network traffic affecting multiple hosts connected to the network segment by listening on the network segment or switch, protecting those hosts. Network-based IDSs frequently consist of a collection of dedicated hosts or sensors positioned throughout the network. These devices keep an eye on network activity, analyse it locally and report attacks to a centralized management console.

1.10.2 Host-Based Intrusion Detection Systems (NIDSs)

Host-Based IDSs use data gathered for a specific computer system to operate. Host-Based IDSSs, in contrast to Network-Based IDSs, can directly access and monitor the data files and system processes that attacks typically target, allowing them to “see” the results of an attempted attack. Operating systems audit trails and system logs are two main types of information sources that Host-Based IDSs typically use.

1.10.3 Host-Based Intrusion Detection Systems (NIDSs)

An exclusive subset of Host-Based IDSs called Application-Based IDSs examines events taking place inside a software application. The application's transaction log files are the most frequent data sources used by Application-Based IDSs. Application-Based IDSSs can identify suspicious behaviour caused by authorized users exceeding their authorization because of the ability to directly interface with the application and the significant domain or application-specific knowledge included in the analysis engine.

1.11 Proxies

Web proxies are particularly common in professional settings. A particular kind of web proxy is designed to manage traffic coming from web clients and going to web servers. Proxy servers are popular among some network and security administrators due to the performance and security advantages they offer. When using proxies, users can sometimes access content more quickly because, after the first user views it, the content is cached and subsequent users can quickly access the cached copy. Administrators can try to safeguard the network by restricting user's access to malicious websites when they are required to send all of their traffic through a proxy. (1)

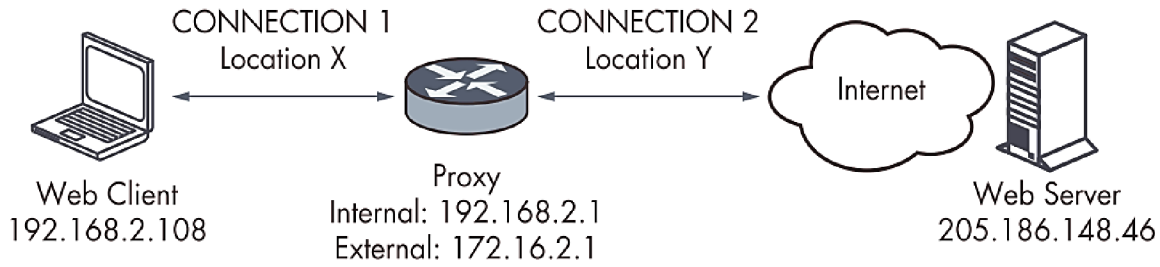

Figure 7: Sample Web proxy setup (Source: BEJTLICH, R., 2013)

As shown in the Figure above, administrators who use proxies can lose some aspects of visibility. We see internal and external IP addresses for the proxy in addition to the true IP address for the web client and the true destination IP address for the web server. Web client communicates with a web server. The direction is reversed when the web server responds.

1.12 Firewall

The network security architecture of every organization must include firewalls. The types of traffic that can cross the perimeter between the private corporate network and the public network are restricted by a firewall. However, the needs for firewalls and security vary depending on the organization. An enterprise firewall provides the size and functionality required to defend a network against cutting-edge cyber threats.

1.12.1 How an Enterprise Firewall Works

A conventional firewall filters packets by looking at the contents of packet headers and applying rule based on IP addresses and port numbers. This, however, does not suffice defence against current or modern cyber threats.

Some of the features that should be included in an enterprise firewall include (Enterprise Firewall, CheckPoint):

- Network Segmentation
- Network Access Control (NAC)
- Remote Access VPNs
- Email Security
- Web Security
- Data Loss Prevention
- Intrusion Prevention Systems (IPS)
- Sandboxing

1.12.2 The Main Features of an Enterprise Firewall

Some of the key factors to consider when evaluating enterprise firewall solutions include (Enterprise Firewall, CheckPoint).:

- Threat Prevention: Minimizing the damage that a cyberattack can cause to a network requires threat prevention.

- App and Identity-based Inspection: A firewall should support granular app policy creation and enforcement based upon user identity.

- Hybrid Cloud Support: The firewall should be easily deployable and scalable in any major cloud environment and be available as a cloud service as well as on-premises.

- Scalable Performance: Hyperscale is necessary to build a robust and scalable distributed system.

- Unified Security Management: A firewall with integrated Unified Security Management (USM) functionally enables an organization's security team to easily and efficiently manage and enforce security policies across their entire network environment.

Any firewall that wants to successfully stop cyberattacks needs to have these five features and abilities. Rack form factor, network port capacity, network interface types (copper, fibre, port line rate), and security throughput are additional features. Businesses and enterprises have a wide range of options available for firewalls by considering throughput, security features, and other elements which should be taken into account when buying a firewall.

1.12.3 Web Application Firewall

A "web application firewall" is an application firewall for HTTP applications. It applies a set of rules to an HTTP conversation. Generally, these rules cover common attacks such as Cross-site Scripting (XSS) and SQL Injection. While proxies generally protect clients, WAFs protect servers. A WAF is deployed to protect specific web application or set of web applications. A WAF can be considered a reverse proxy. WAFs may come in the form of an appliance, server plugin, or filter, and maybe customized to an application. The effort to perform this customization can be significant and needs to be maintained as the application is modified (OWASP, Web Application Firewall).

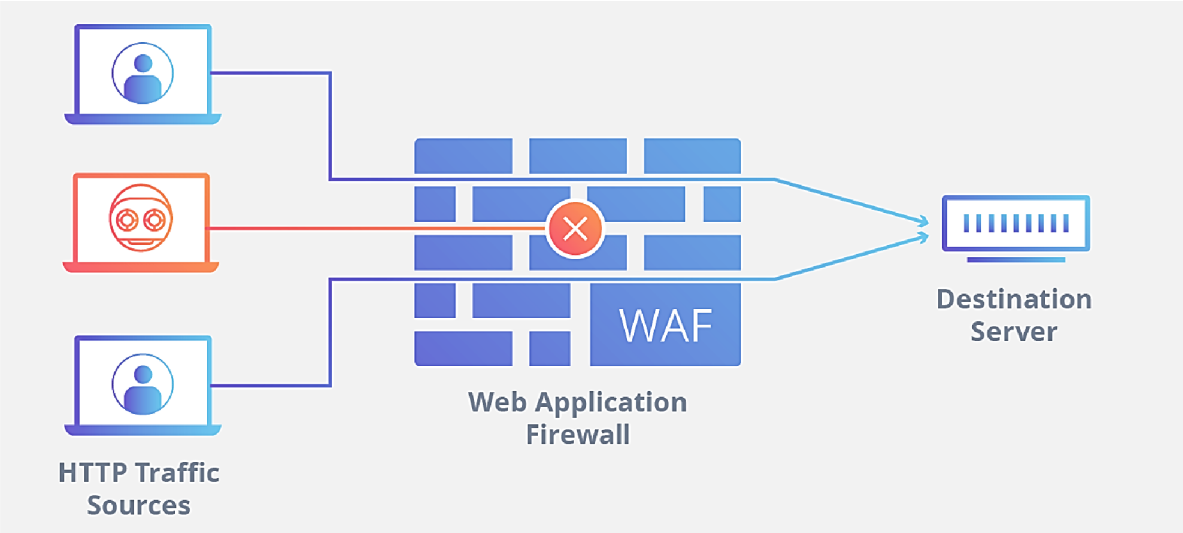

Figure 8: Web Application Firewall (Source: Cloudflare, WAF)

A WAF can be implemented through one of the three different ways, each with its own benefits and shortcomings:

- A network-based WAF is generally hardware-based. Because they are placed locally, they reduce latency; nevertheless, network-based WAFs are the most expensive solution and necessitate the storage and maintenance of actual hardware.
- A host-based WAF can be entirely incorporated into the software of an application. This approach is less costly and more customizable than a network-based WAF. A host-based WAF's disadvantage include the user of local server resources, implementation complexity, and maintenance expenses. These components usually need engineering work and might be pricey.
- Cloud-based WAFs provide an economical and simple to implement solution; they often provide a turnkey installation that is a s simple as DNS (Domain Name System) update to reroute traffic. Cloud-based WAFs also have low initial investment/cost. The drawback of a cloud-based WAF is that users delegate responsibility to a third party, therefore some elements of the WAF maybe black box to them.

1.13 Security Information and Event Management (SIEM)

SIEM, or security information and event management, is a tool that enables businesses to identify, assess, and respond to security threats before they have a negative impact on daily operations. SIEM technology gathers event log data from various sources, analyzes it in real-time to spot activity that differs from the norm, and then takes the necessary action. To put simply, SIEM gives businesses visibility into network activity so it can prevent potential cyber attacks and adhere to regulatory requirements (Microsoft Security, SIEM).

Through the use of artificial intelligence, SIEM technology has advanced over the last ten years to make threat detection and incident response quicker and smarter. For security teams to recognize and thwart attacks, SIEM tools gather, aggregate, and analyze a large amount of data from an organization's applications, devices, servers, and users in real-time. Security teams can define threats and produce alerts with the help of SIEM tools by using pre-defined rules. The cybersecurity ecosystem of an organization should include SIEM. To streamline security workflows, SIEM provides security teams with a central location to gather and analyze large data across and enterprise. Additionally, it offers operational features like dashboards that rank threat activity and compliance reporting and incident management.

Concept	Description
Function	Centralizing and correlating security event data
Purpose	Offers threat detection and incident response in real time
Features	Alerting, Normalization, Correlation, Event aggregation, Dashboards, and Reporting
Components	Log collectors, Event processors, Event storage, Data sources, and Reporting
Benefits	Reduced incident response time, enhanced threat detection, regulatory compliance, and increased security visibility
Use cases	Security monitoring, Incident response, Compliance reporting, and Forensics analysis
Challenges	Complexity, Data overload, and False positives/negatives
Vendors	Splunk, ArcSight, IBM Security QRadar, LogRhythm, McAfee Enterprise Security Manager, and AlienVault USM

Table 2: Security incident and event management (Source: Author)

1.13.1 ArcSight

ArcSight is a vulnerability scanning program that, from a single platform, employs machine learning to identify threats, organize investigations, create prioritized event lists, and more. Employees can monitor events and behavior across a wide range of users, IP addresses, servers, and workstations by extracting entities from log files (MindMajix, SIEM).

ArcSight can help administrators identify problems like privileged account abuse, behavior of recently terminated employees, data staging, email exfiltration, malicious tunneling, and mooching. Using the timeline view, employees can browse entity alerts chronologically, which improves their ability to evaluate risk. Additionally, it enables IT staff to assess the context of earlier alerts, including associated entities and the model that raised the alarm.

Feature	Description
Incident Response	Provides an integrated platform for managing and tracking security incidents for incidents response team
Threat Intelligence	Integrates with platform and threat intelligence feeds to give context for potential threats
Risk Assessment	Identifies high-risk areas and prioritizes remediation efforts by analyzing data and generating risk scores
Compliance Reporting	Offers built-in compliance reporting for law regulations like PCI DSS, HIPAA, GDPR and others
Advanced Threat Detection	Uses behavioral analytics and machine learning to find new or sophisticated threats
Log Management	Logs from various sources are collected, normalized, and stored for analysis and reporting
Dashboards and Visualizations	Gives analysts access to fully customizable dashboards and visualization tools to aid in the quick identification of potential threats
Integration with Other Security Tools	Provides a complete security solution by integrating with a wide range of security tools and technologies

Table 3: Features of ArcSight (Source: Author)

Customers can use ArcSight to organize and manage incident response operations, identify and prioritize security threats and speed up audit and compliance procedures. ArcSight is now a Hewlett-Packard subsidiary since 2010.

The diagram below shows how ArcSight is structured:

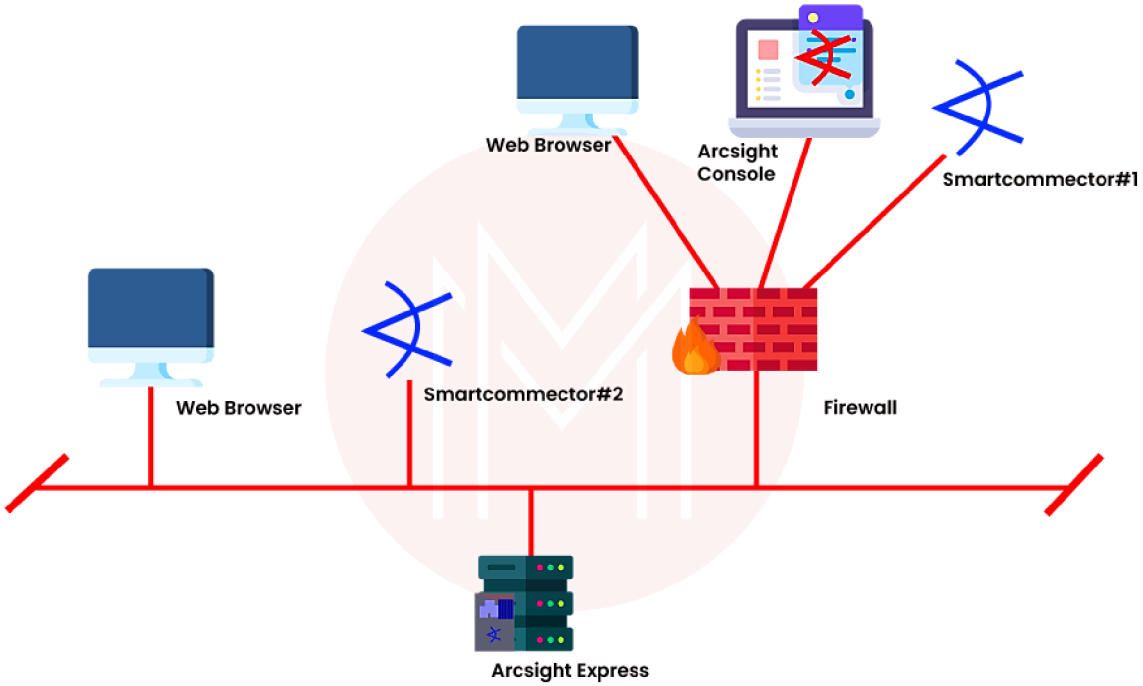

Figure 9: ArcSight Architecture (Source: MindMajix, SIEM)

For the optimum operational performance of SIEM, ArcSight is a high-availability security system that can be integrated with a number of service architectures. Hardware, commit, communications, caching, and recovery components are all present by default. One can use a web browser or the ArcSight interface to access ESM (Enterprise Service Management), Logger, and CA (Certificate Authority). The improved ESM events that the logger receives will be saved for a very long time. All smart connection events will be delivered to the ESM instances (MindMajix, SIEM).

Overall, ArcSight architecture is created to be adaptable, scalable, and user-friendly. Smart connectors gather log and event data from various sources and send it to the ArcSight Data Platform so that the ArcSight ESM (Enterprise Security Management) component can process and analyse it. The ArcSight console, which can be accessed by a web browser or thick client, offers a user-friendly interface for managing security events and issues. ArcSight Express is a condensed version of the software created for smaller enterprises, and it can be used as a firewall to safeguard the system from unauthorized access.

1.13.2 Splunk

Splunk is a piece of software that examines and interprets enormous amounts of data from machines and other sources. A web server running on a CPU, IoT devices, mobile app logs, and other sources produce this machine data. For end users, this information is not necessary and therefore has no economic value. Contrarily, it is crucial to comprehend, monitor, and improve the equipment's performance (MindMajix, SIEM).

Feature	Description
Alerts	Users of Splunk can configure alerts to keep track of particular conditions and receive notifications when predetermined thresholds are reached
Machine learning	Machine learning features are already incorporated into Splunk to assist users in identifying abnormalities and forecasting future events
Security	To safeguard sensitive data, Splunk provides strong security features like access limits, data encryption, and audit trails
Indexing	Regardless of its location or format, Splunk can index any sort of machine-generated data, making it simple to search for and examine this data
Search	Splunk's primary function is the real-time search and analysis of massive amounts of machine-generated data from diverse sources
Dashboards	Splunk allows users to construct personalized dashboards to visualize data in real-time, making it easy to discover patterns and trends
Scalability	Splunk can handle terabytes of data every day and grow to accommodate companies of any size, from small businesses to large enterprises
Integrations	Numerous third-party solutions, such as well-known IT operations, security, and DevOps applications, can be integrated with Splunk
Cloud Support	Splunk provides options for cloud-based deployments in addition to connections with top cloud service providers including AWS, Azure, and Google Cloud

Table 4: Features of ArcSight (Source: Author)

Unstructured, semi-structured, and occasionally structured data can all be read by Splunk. Once the data is read, it allows to search, categorize, and create reports and dashboards using it. Thanks to the rise of big data, Splunk can now use large data from numerous sources, including machine data, and perform analytics on it.

The diagram below shows the structure of Splunk:

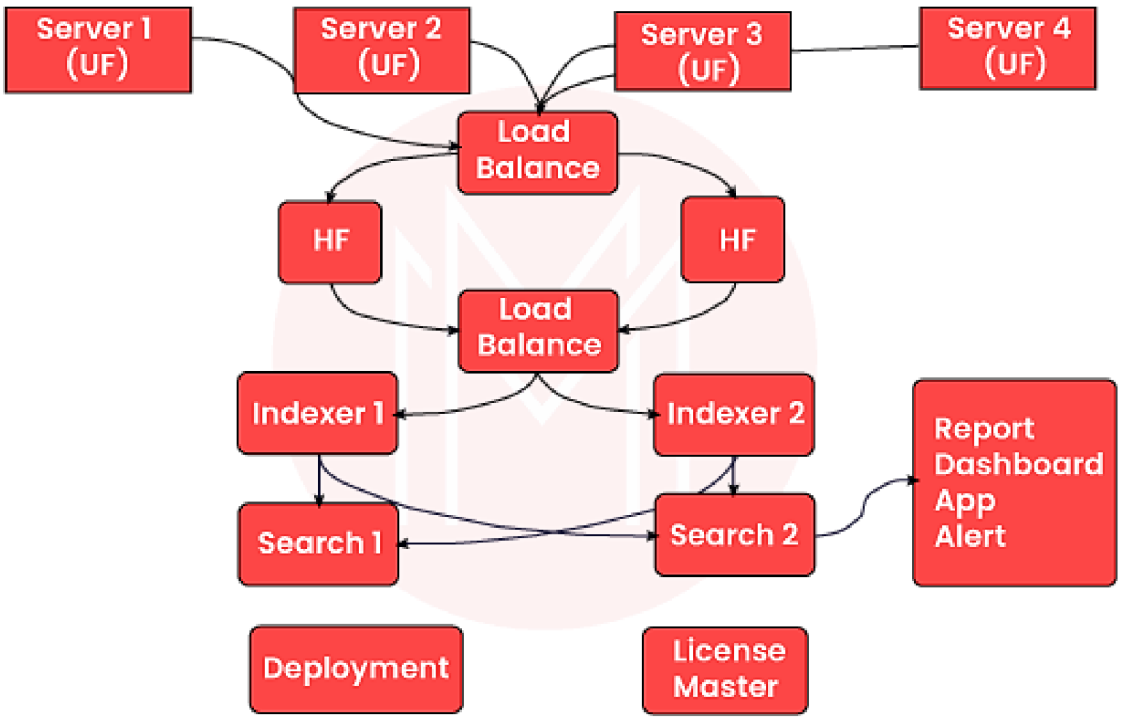

Figure 10: Splunk Architecture (Source: MindMajix, SIEM)

In a typical Splunk architecture, data is collected by Universal Forwarder (UF) or Heavy Forwarder (HF) and sent to the Indexer for storage and indexing. The Search Head is used to search and analyse the data, while the Deployment server and License Manager are used to manage the configuration and licensing of the environment. The Load Balancer can be used to distribute the load of incoming data across multiple Heavy Forwarders (HF), providing a scalable and high-performance solution for large environments.

While both Splunk and ArcSight are powerful solutions for IT and Security operations, Splunk is often preferred for its flexibility, ease of use, real-time processing, scalability, and extensibility. Both ArcSight and Splunk have advantages and disadvantages, and their use is determined by the demands of the organization.

Practical Part

2. Scope and Elements

- Main scope of network security: Internal networks, Fixed line networks, Cloud/Hosted networks, Mobile networks, 3rd Party/External connections
- Network Monitoring: Device failures, link outages, interface errors, packet loss, application response time, configuration changes
- Logging and monitoring: Applied to an enterprise/organization IT & Network system, and other supporting infrastructure
- Incident Management: Incident response plan, Incident Classification, Incident handling procedures, post-incident review
- Tools: CheckPoint, ArcSight, Splunk, IBM SOAR Resilient, Elastic, F5, Tufin Orchestration, Imperva etc.

Note* : To keep the anonymity, confidentiality and due to the sensitive nature of the data that may relate to company XY's findings, the data below maybe subject to modification and partial removal.

2.1 Incident Management of XY Company

The XY company is a multinational telco company with over two thousand of internal and external employees. The XY company with over 1 million customers in the Czech Republic. The company is committed to providing high-quality services and innovative solutions to its customers. The Incident Management team of the XY company comprises of several representatives that are responsible for managing incidents, either directly or indirectly:

Team	Role
Cyber Security Testing	• Identifies security weaknesses • Provides pen testing services including infrastructure, application, mobile and physical security testing
Cyber Security Operations Centre (CSOC)	• Near real-time monitoring focusing on known Indicators of Compromise (IoC) and attack tactics, techniques and procedures • Hunting on available security logs and monitoring platforms
Cyber Defense Threat Intelligence (CDTI)	• Identify and respond to threats • Global communication of threats

Forensics and e-Discover (CERT)	• Incident response and coordination • E-Discovery • Dead box forensics
Cyber Defense Incident Management (CDIM)	• Governs and leads a cyber-incident • Communicates and coordinates • Drives actions and overall progress
Mandiant Incident Response	• Incident response
Privacy	• Incident response and privacy practices • Assessing individuals' privacy and advising Incident response team • Ensuring Compliance • Providing guidance and training on privacy-related matters
Legal	• Legal analysis and providing legal advice • Coordinating with external counsel • Conducting legal review of incident response plans
Fraud	• Identifying fraudulent activities • Assessing the impact of fraud • Developing fraud prevention strategies

Table 5: Teams and Roles for IM (Source: Author)

All the members of the IM teams are responsible for supporting effective Cyber Incident Management by reporting suspected malicious or inappropriate activity through the relevant local channels, emails and calls. When reporting a cyber incident, it is important to collect as much information as possible to help assign a severity level to the incident. This will determine whether the cyber incident needs to be referred to an incident manager. Key information includes:

- The affected business area
- The "potential" impact of the incident
- The nature of the incident
- Description of the activity and supporting evidence e.g., logs
- 24/7 contact information of the person reporting the incident or any other key stakeholders
- Hostnames and IP addresses of suspected impacted systems/assets
- Any containment actions which have been taken
- Any current business, financial or customer impact

2.2 Incident Severity Classification

The severity of an incident will determine the urgency of the response. The Cyber Security Matrix of Impact to which the Incident Management Global Standard refers will help ensure that the correct people are involved from the outset.

	Impact				
Cyber Risk Impact Rating	4	3	2	1	Negligible
Cyber Severity Level	S0	S1	S2	S3	S4
Cyber Incident Descriptor	Crisis	Major	Significant	Moderate	Minor
IT Impact Rating	Critical	High	Medium	Low	Negligible
IT Level	P0	P1	P2	P3	P4

Figure 11: Priority and Severity Alignment (Source: Author)

The Objectives of the Cyber Severity Matrix of Impact are:

- To simplify Cyber Defense triage by creating a fit for all model
- To align with XY's Digital and IT
- To incorporate the Global Risk Management Framework
- To adhere to National Cyber Security Centre (e.g., NÚKIB- Národní Úřad Pro Kybernetickou a Informační Bezpečnost) best practice

The matrix provides indicators to consider when determining whether a cyber-incident is increasing or decreasing in impact and severity. The Cyber Severity Matrix of impact must be used to assign severity levels to all cyber incidents. Every cyber incident assigned a severity level S0 or S1 must be handled by Cyber Defense. Local teams may choose to handle incidents with a severity of S2 but the incident must be reported to CDIM.

2.3 Cyber-Incident Categories in company XY

A list of common cyber-incidents including XY's cyber-incident categories that will be investigated:

I. **Account Hijack:** A process through which an individual's account associated with a computing device or service is accessed without authorization

II. **Denial of Service (DoS):** Suspected, attempted or actual instances where an entity places an excessively high demand on a given information or asset. A malicious attempt to cause a victim, website, or node to deny service to its customers

III. **Malicious Compromised or Exploited Software:** Suspected, attempted or actual installation/execution of unauthorized or malicious software on XY's device. Included malware detection by anti-malware software (even if mitigated successfully) and detections by application whitelisting solution

IV. **Network Intrusion, Enumeration or other Probe:** Suspected, attempted or actual network intrusion, enumeration or probe. Includes intrusion alerts generated by network security equipment such as a firewall or IDS/IPS

V. **Social Engineering/Phishing:** Suspected, attempted or actual instances when an unauthorized person attempts to gain access to XY's data or IT systems by deception or extortion of authorized users (staff, customers or third parties)

VI. **Suspicious privilege amendment:** Suspected, attempted or actual instances where a genuine user appears to have been placed in an appropriate user group or to otherwise have gained excessive privileges

VII. **Suspicious uses of legitimate privileges:** Suspected, attempted or actual instances where a user appears to have abused legitimate access privileges; e.g. by accessing a large number of files/records, e-mailing data to unauthorized recipients, copying data to removable media or unusual network locations etcetera

VIII. **Telecoms Interception:** Eavesdropping on a legitimate communication channel. Suspected, attempted or actual instances where XY's data appears to have been intercepted by an unauthorized party. Includes instances where sensitive data is transferred to authorized recipients in unencrypted form

IX. **Vulnerabilities:** Weakness that can be exploited to perform unauthorized action within a computer system or business process

X. **Website Attacks:** Attacks that exploit web browsing or websites. Includes fake XY websites.

2.4 Security Incidents

The below chart (Fig.12) shows a number of events and incidents detected in a period of 3 months (*Timestamp 23.12.2022-23.03.2023*)

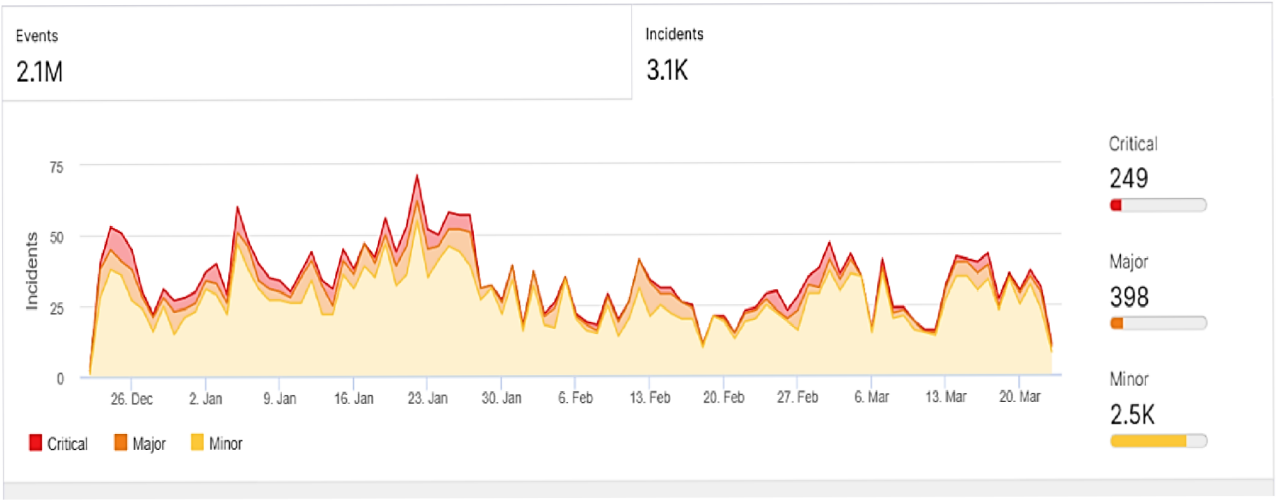

Figure 12: Events and Incidents chart (Source: Author)

If there is no Incident Management mechanism in place, security incidents might be difficult to resolve. Security issues are on the rise and some recent statistics and common security issues at XY are as follows (Fig.13 and Fig.14):

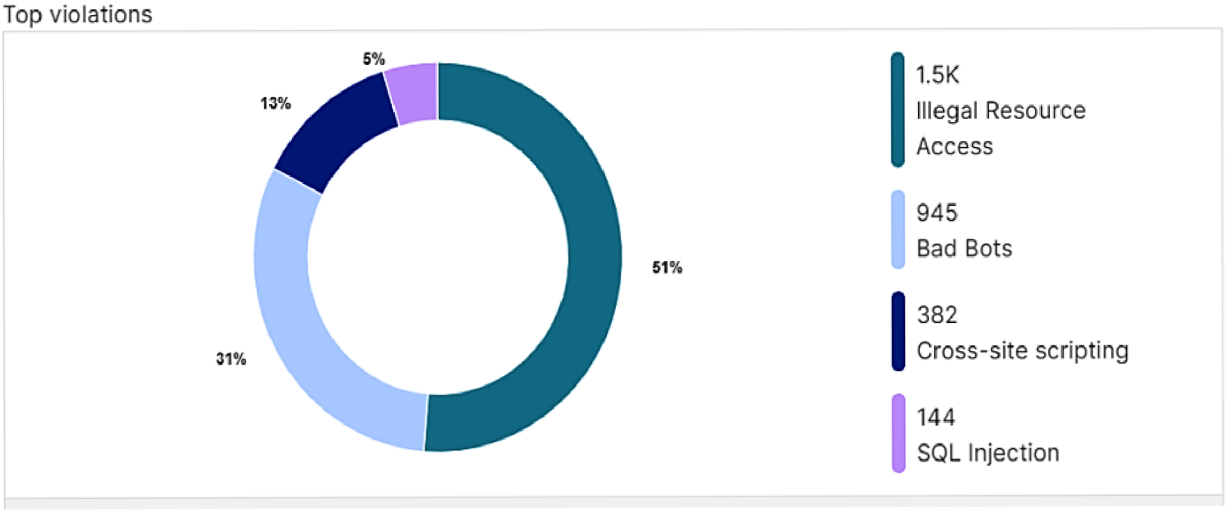

Figure 13: Top violations chart 2022-2023 (Source: Author)

- Illegal Resource Access – 51% rise in illegal resource access since 2022
- Bad bots – 31% increase in bad bots
- Cross-site scripting – 13% year-over-year increase
- SQL injection – 5% rise from 2022 to 2023

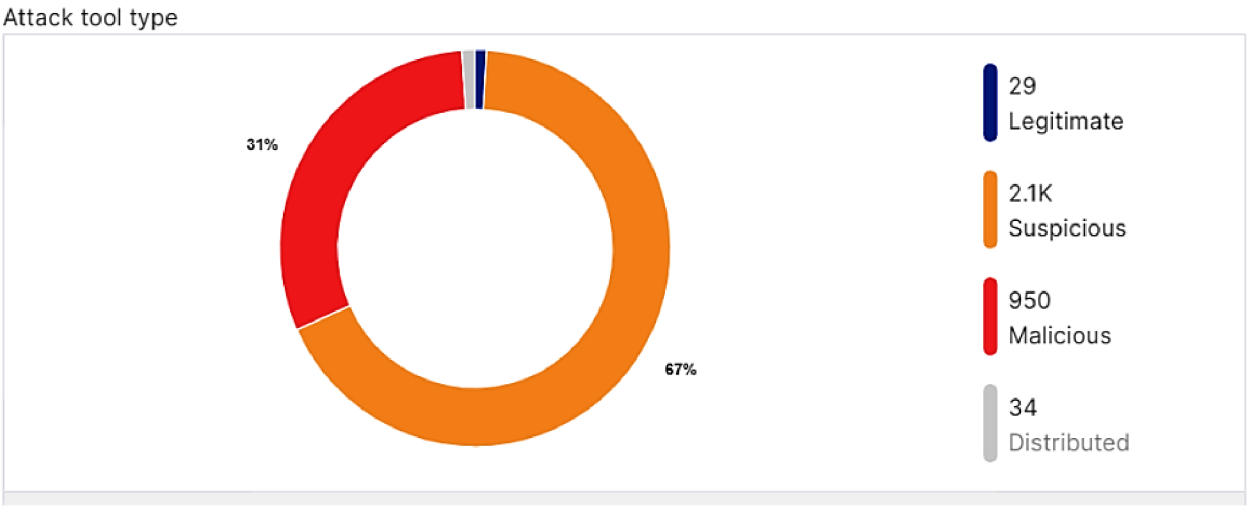

Figure 14: Attack type chart 2022-2023 (Source: Author)

- Legitimate – around 29 attacks were carried out with explicit permission and authorization

- Suspicious – 2.1 thousand of indicated suspicious attacks that may either be an attempt or compromise to the security (DoS, Malware, Phishing, Port scanning etc.)

- Malicious – 950 intentional and unauthorized attempts to compromise the security to steal data, cause damage, or gain unauthorized access to systems or networks

- Distributed – a number of 34 Distributed or DDoS attacks carried out in the form of volumetric attacks, protocol attacks and application layer attacks

2.5 Incident Lifecycle

The Incident lifecycle is a six-stage process used by XY organization to manage and respond to incidents. The stages include Preparation, Identification, Containment, Investigation, Remediation, and Recovery. Organization may efficiently recognize and respond to incidents/events, contain damage, investigate the source, remediate the issue, and recover from the incident by following this procedure (Fig.15).

Figure 15: Incident Management Lifecycle (Source: Author)

Lately, the existing Incident lifecycle has resulted in many incidents due to incident response procedures which were poorly defined or not followed correctly, incident detection and response capabilities were insufficient, incident response staff were not adequately trained or lacked necessary skills, communication and collaboration between teams was poor, and the incident response process was not reviewed and updated on a regular basis.

Incident instances and its management during the unoptimized incident lifecycle

Instance 1

On 2022-12-27 at 12:43:29 UTC, Mandiant alerted on activity related to Locky Ransomware on "**w5bkup04**"
Analysis of the alert data revealed that this activity is consistent with a file write event for the file:
_516_HOWDO_text.html (MD5: feb9203f01e0424e3ab39d027c77b5d8) to the directory D:\Restore\BackLine Angels\OLD\BackOffice\Vykazy\Noční směna\Roaming\procedury_516_HOWDO_text.html, that was spawned by the process tar32.exe located in D:\Program Files\Veritas\NetBackup\bin, under the system account NT AUTHORITY\SYSTEM.

MDE Timeline Details :
nbpas.exe >>
"bpcd.exe" -root_bpcd
D:\Program Files\Veritas\NetBackup\bin\bpcd.exe>>
d:\program files\veritas\netbackup\bin\tar32.exe>>
D:\Restore\BackLine Angels\OLD\BackOffice\Vykazy\Noční směna\Roaming\procedury_516_HOWDO_text.html
4c9d161662f259ccfe3497922c28aaf625c28598bfce5fb86bcc6af48e307d47

Summary narrative:

Mandiant alerted on activity related to Locky Ransomware where one html file "_516_HOWDO_text.html" under file path- "D:\Restore\BackLine Angels\OLD\BackOffice\Vykazy\Noční směna\Roaming\procedury\" has been detected as Locky Ransomware. File was executed from tar32.exe which belongs to Veritas. As per machine timeline "tar32.exe" created multiple zip, png and html files. Among all alerts, one was detected as malicious, however file hash is not available publicly. Tar.exe seems to be a NetBackup setup which helps in netbackups.

Recommendations:

- Contain the system(s) identified
- Restore the potentially encrypted files from the latest valid backup
- Ensure antivirus software is installed on the affected system(s) and that it is up to date and functioning properly
- Restrict write permission and/or limit access to network share
- Operate on a least privilege access model when distributing file network permissions
- Install OS security updates that could help to mitigate the infection from spreading to other endpoints

Instance 2

Name
Account Hijack - Brute Force - Credential Stuffing Attack by Multiple IPs
Incident Source
ArcSight
Incident Type
Account Hijack:Brute Force
Detection Time
1 hour
Technical facts
Name : Account Hijack - Brute Force - Credential Stuffing Attack by Multiple IPs

Start Time : 15 Jan 2023 09:34:35 UTC
End Time : 15 Jan 2023 09:50:00 UTC
Manager Receipt Time : 15 Jan 2023 09:50:07 UTC

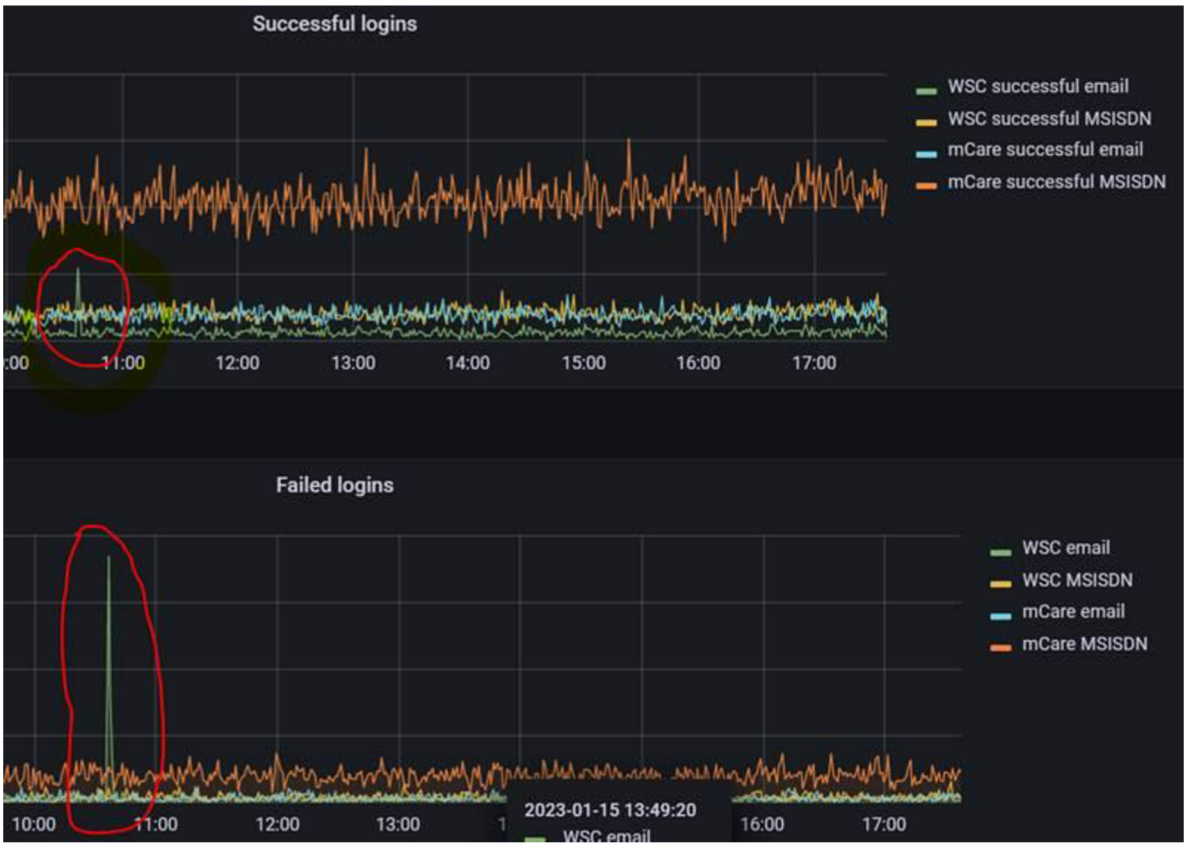

Figure 16: Visuals of Account Hijack - Brute Force - Credential Stuffing Attack by Multiple IPs (Source: Author)

Summary narrative:

Alert triggered for signature "Account Hijack – Brute Force – Credential Stuffing Attack by Multiple IPs". Ran logger for last 3 Days and observed 30K plus logs for below search: 217.77.163.138 AND deviceVendor CONTAINS "F5" AND deviceEventClassId CONTAINS "Brute Force: Maximum login attempts are exceeded", couldn't download the logs due to high count. Device Action captured as "Alerted". It is observed that multiple source Ips were observed. All the captured source IPs belongs to geo location CZ, via ArcSight logs. Need to know whether CAPTCHA and MFA is implemented and required security measures are in place. Also need to understand the reason behind such multiple failed logons, impacted asset type - server, and reason for initial severity.

Recommendations

- Identify the root cause of the alert/traffic
- Identify whether this an expected behavior or not?
- If yes, provide justification so that the same can be removed from monitoring scope
- If no, investigate further to understand the implications and to deduce a mitigation action points/plan
- Share the findings/outcome with CSOC (Cyber Security Operation Center)

There are several ways to optimize incident lifecycle process such as automating incident detection and response, establish clear roles and responsibilities, continuously monitor and improve the incident response process, conduct regular training and exercises, and implement a feedback loop for continuous improvement. These measures can help ensure that the incident response process is effective, efficient, and responsive to the needs of the organization.

2.6 Tool used for Incident Management communication at XY

The most common way or tool used in incident management communication is done via email in most of the corporates and organizations. Email can be a useful tool for IM communication but it may not be the most effective or efficient approach in all cases.

The following are some benefits of utilizing email for incident management communication:

I. Emails serve as a record of communication that may be referred to later for analysis, auditing, or inquiry

II. Emails can be used to follow the status of an issue, assign ownership or accountability, and ensure that all relevant parties are kept up to date

III. Emails maybe sent to a large number of people at the same time, making it simple to communicate with many stakeholders, teams, or department

There are, however, certain drawbacks to utilizing email for incident management communication, the following are some of them:

I. Emails may not be viewed or responded to promptly, resulting in incident resolution and escalation delays

II. Emails can be misconstrued, and tone or meaning might be lost in translation. This can lead to misunderstandings, and even confrontation or conflict

III. Emails, especially in busy or high-volume situations, can be lost or buried in inboxes. This can make ensuring difficult that all key stakeholders are informed and engaged

The decision to use email for incident management communication is influenced by a number of factors, including company policy, incident severity, team size and location, and organizational culture. Email can be important for documentation, traceability, and reaching a large number of people, but it can generate delays, misunderstandings, and spam. The choice to utilize email should be founded on a thorough assessment of the company's goals and capabilities, as well as the possible benefits and drawbacks of utilizing email as a communication medium.

2.7 Technical Description, Clean Up and Optimization

The below network architecture (fig.17) is fairly simple in comparison to standard corporate networks, yet it has all of the fundamental building pieces. The first is the perimeter firewall nsxedge-fw01, which also includes a DMZ zone for servers with internet connectivity. A central switch operating in L3 mode is another component of networking architecture that assure network routing traffic at the network's core. At this time, the form was simplified by replacing the switch with a router. The simplification is done solely for the purpose of virtualization on the VirtualBox platform because switches are typically powerful devices with key functionality in ASIC chips and thus are not virtualizable on the x86 platform; theoretically, only the emulation of the switch function is possible. As a result, the switch was replaced with a virtualized router running Cisco IOS.

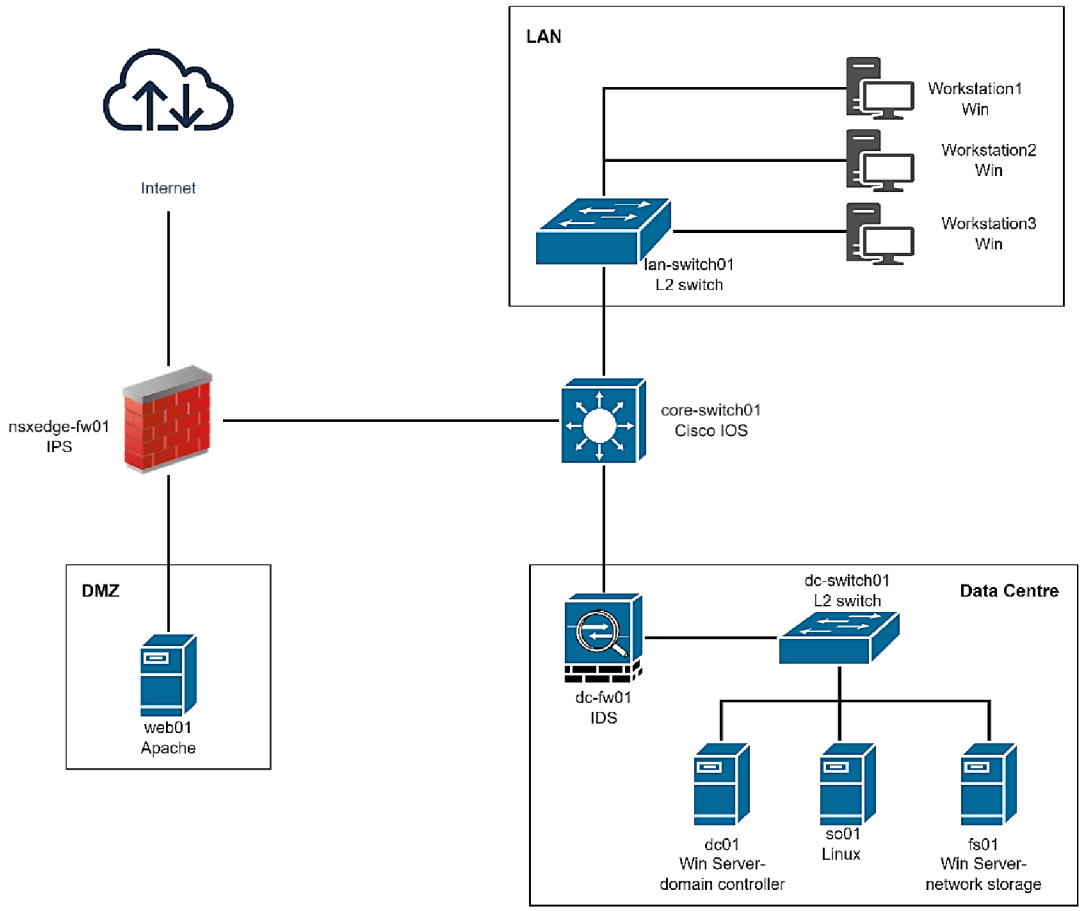

Figure 17: Network Topology (Source: Author)

The entire environment runs in the VirtualBox virtualization environment and is connected to internal networks. Connection to the outside world is only through the external interface of the firewall nsxedge-fw01 which is in bridge mode, which allows it to receive IP address from external network. The choice of network topology affects how data is transmitted and communicated within the network, the ability of the network to grow and adapt, the level of security provided, the cost of the infrastructure, and the ease of network management and maintenance.

Understanding the topology of the network is essential for effective incident management. It assists incident responders in rapidly identifying affected regions, troubleshooting, and remediating the issue, mitigating the damage, and preventing future incidents. Responders can restrict incidents to specified portions of the network by understanding network topology, pinpoint the root cause of incidents, divert traffic to avoid impacted areas, and take proactive actions to prevent repeating of incidents.

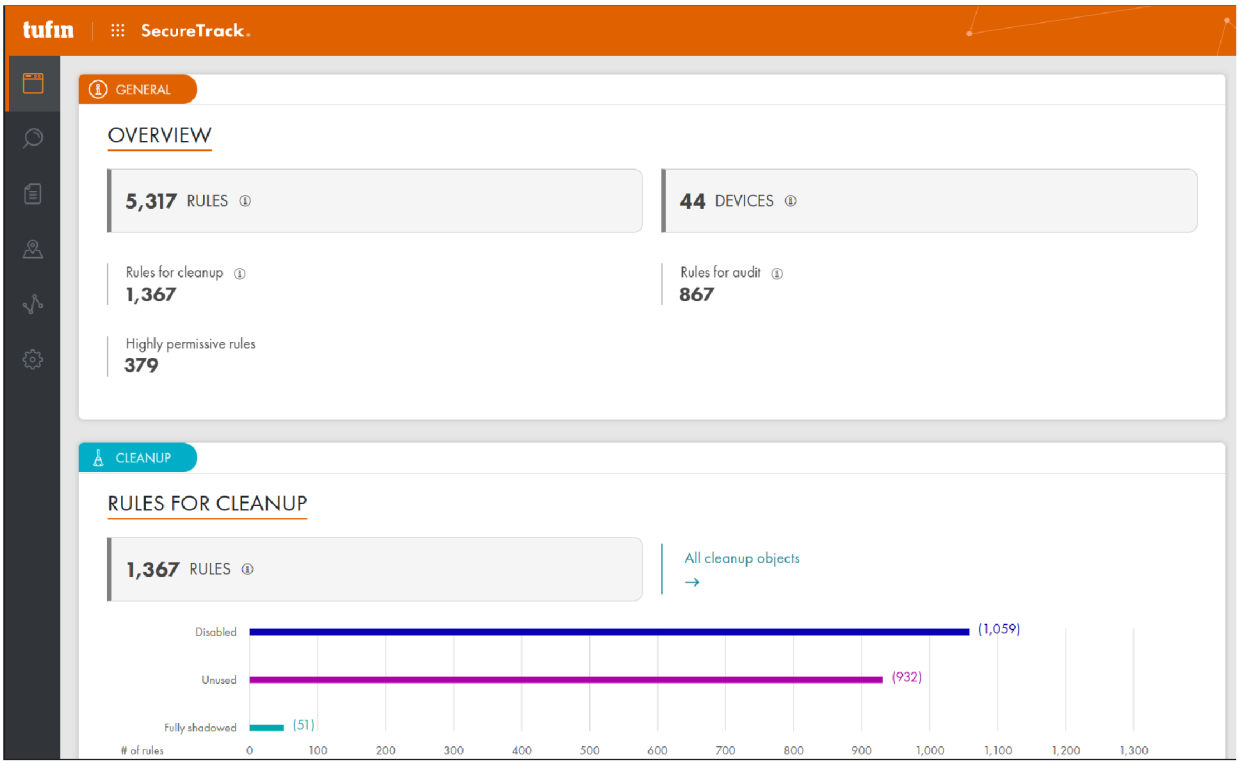

Figure 18: Rules Overview and Clean Up (Source: Author)

Tufin is a security policy management platform that includes a Clean Up module to help organizations in identifying and removing unused, duplicated, or obsolete security rules and objects. The Clean Up module prioritizes rules and objects for removal based on risk, and it includes a mechanism for evaluating and approving changes before they are applied. This contributes to the simplification and optimization of security rules, making them more effective and easier to maintain.

Some of the rules that the Clean Up module follows are:

- Unused rules and objects
- Redundant rules and object
- Outdated rules and objects
- Shadowed rules and objects
- Risk-based removal

These rules help to simplify and optimize security policies, making them more effective and easier to manage.

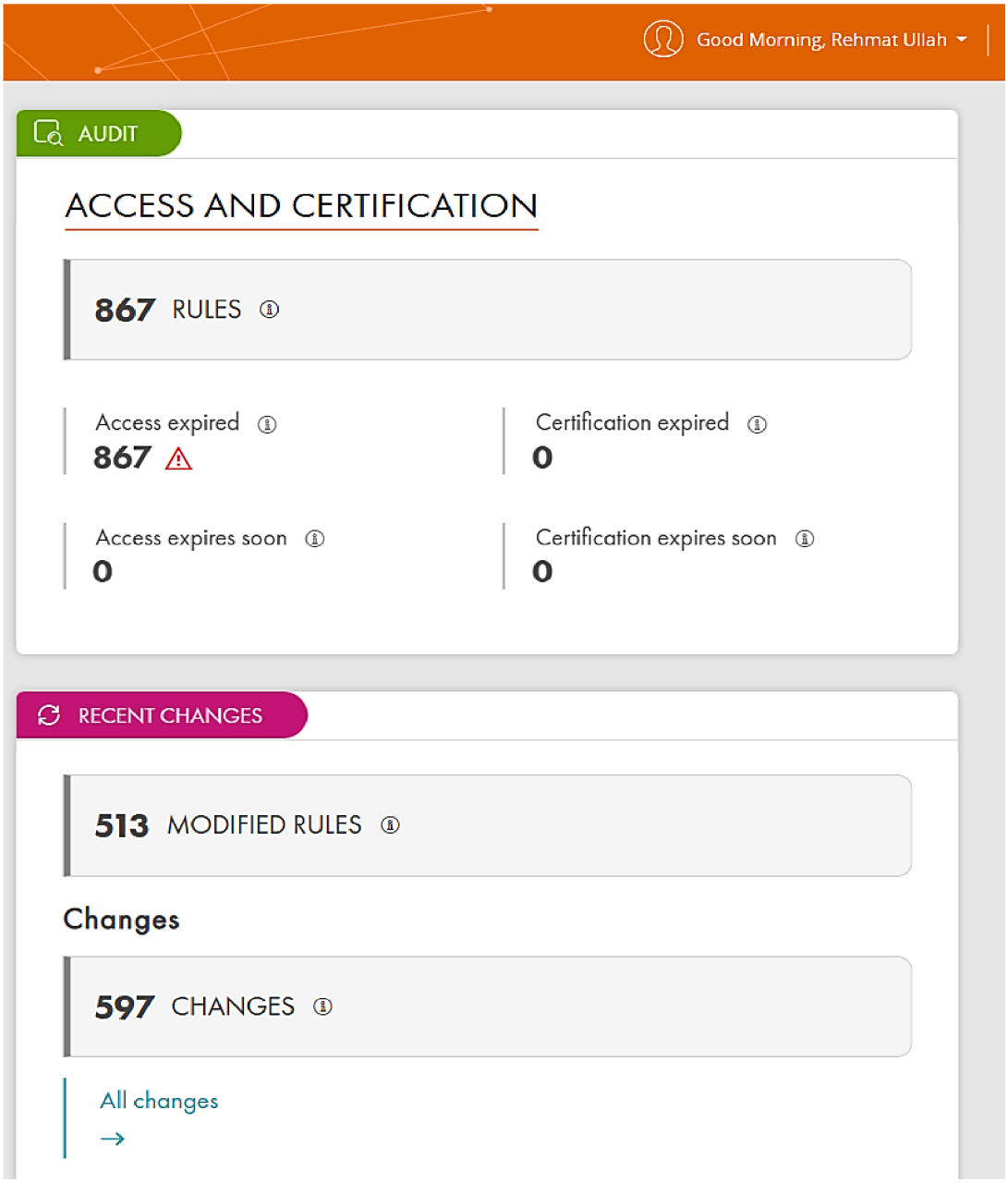

Figure 19: Rules Mods and Changes (Source: Author)

Overall, setting up correct rules and removing unused objects can help incident management process by improving visibility, providing real-time risk assessment, simplifying policy management, automating incident response, and ensuring compliance with regulatory requirements. This can help organizations to minimize the impact of incidents and prevent similar incidents form occurring in the future.

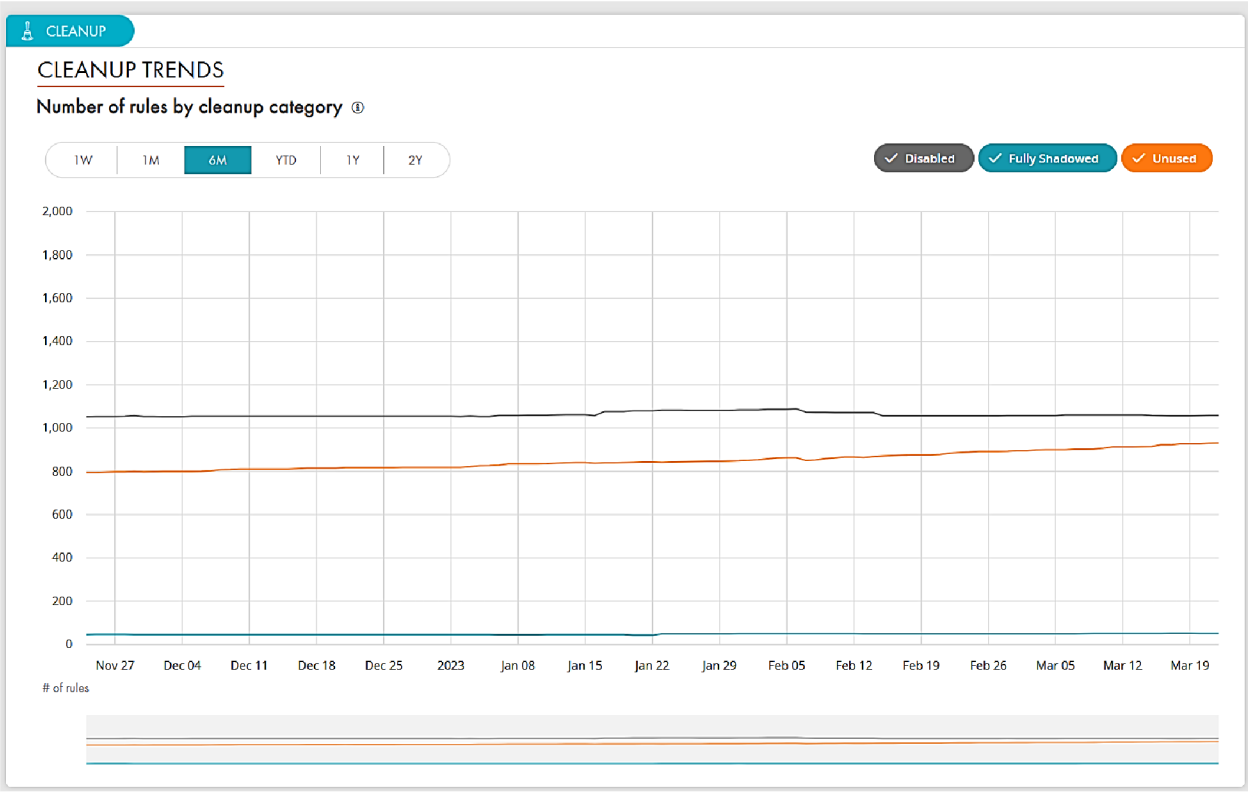

Figure 20: Statistics of rules by clean up category (Source: Author)

The below graphs represent the stats of closed tickets (rules, objects and firewalls), service-level history and its status

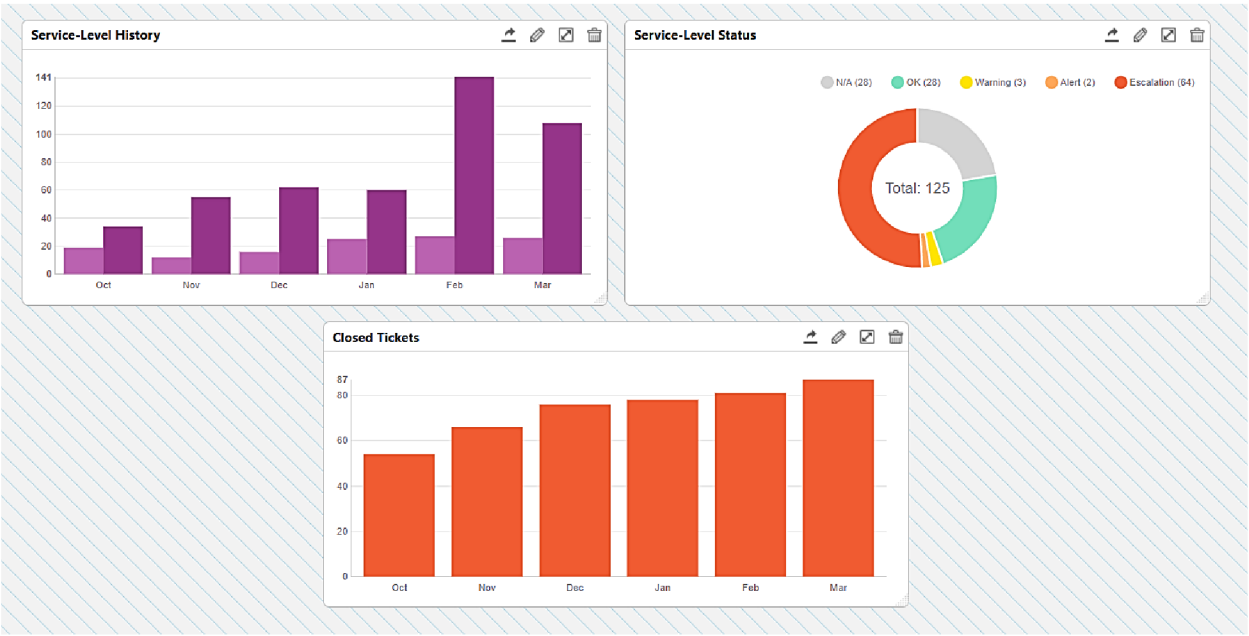

Figure 21: Rules Overview and Clean Up (Source: Author)

Incidents after the Optimization and clean up

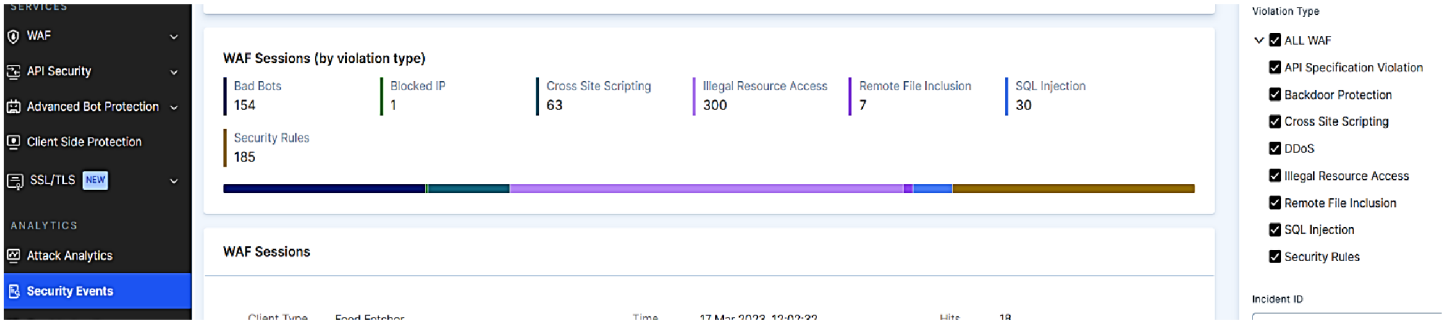

Figure 22: Security Events-WAF sessions (Source: Author)

The number of events and incidents showed a significant drop by monitoring the WAF sessions, this could be directly or indirectly connected with the optimization of web applications, servers and implementing a strict access control by using a reputable WAF (Web Application Firewall).

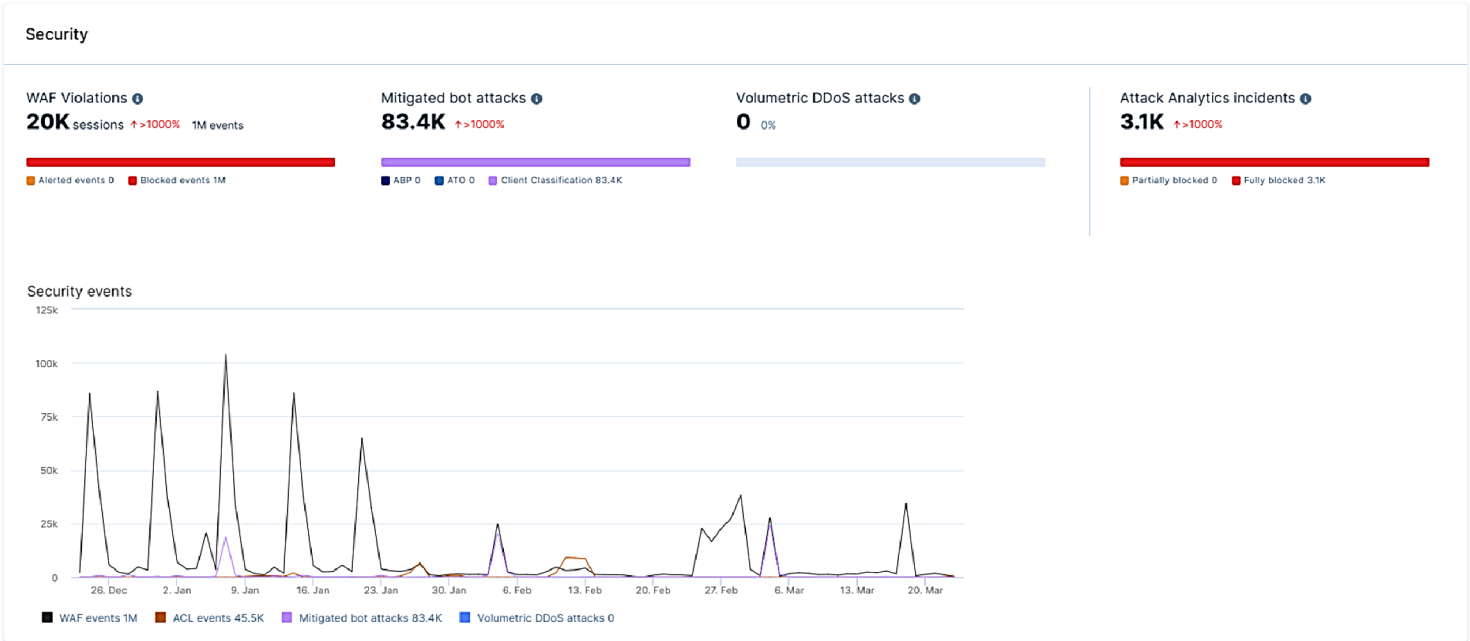

Figure 23: Web Application Firewall (Source: Author)

Having a WAF can significantly help in incident management by preventing and mitigating attacks against the web applications. It can detect and block malicious traffic, alert security teams to potential incidents, provide detailed logs and reports, and mitigate the impact of incidents.

2.8 Incident Management Playbook

A playbook for incident management is essential for assuring consistency, speed, preparation, compliance, and ongoing improvement in response to security incidents. It provides clear guidelines and processes for detecting, responding, and recovering from incidents, and helps organizations improve their overall security posture.

The following playbook aims to support XY's Incident Management by outlining the best practices. The existing Incident lifecycle and other significant factors affecting Incident management process of the company XY were taken into consideration as well.

	Task	Role (Responsible)	Comment
Identification	Identify the attack	CDIM/CERT/ CSOC/ Other intelligent leads	
	Identifying the total number of impacted systems to confirm	CDIM/CERT/ Mandiant/Local market	
	Perform business impact assessment	Local market	
	Identify the threat actor gained access to data and determine a longer-term loss of availability to data	CERT/ Mandiant/ Local market	If Cyber Data breach is confirmed, refer to legal, privacy and data breach policies
	Obtain a list of all impacted assets	Local market	Local market to fill asset tracker template and return data to CDIM
	Create and maintain trackers	CDIM	Trackers such Actions tracker, Alerts tracker, etc.
	Identify initial containment actions taken by the affected market/third party	Local market/ Third party	
	Identify if additional containment is needed to stop the spread of the infection	CERT/Mandiant	
	Identify the attack vector	CERT/Mandiant	
	Identify the root cause	CERT/Mandiant	
	Obtain a copy of the attack	Local market	

	Provide a copy of the attack to CDTI/CERT/CSOC	CDIM	
	Obtain network diagrams (High-level Diagrams or Low-level network Diagrams)	Local market	
	Identify any alerts for the impacted assets	CSOC	
	Run a logger search on identified IoCs (Indicators of Compromise)	CSOC	
Identification	Identify presence of other malicious activity and develop lines of enquiry	CSOC/CERT/ CDTI/Mandiant	
	Provide instructions for required forensic acquisition to the affected market	CERT	
	Provide forensics artefacts to CERT for analysis	Local market	
	Identify if the attack type is capable of lateral movement	CERT/Mandiant	Cable of being turned into network attack (such as worm)
	Identify asset level security controls, e.g., Antivirus solution, HIPS, EDR, others	Local market	
	Identify network level security controls, e.g., web proxy, firewall, IDPS, others	Local market	
	Share identified IoCs with CDTI for intelligence enrichment	CDIM	Network and Host-based indicators
	Perform threat intelligence analysis on the identified IoCs, asses whether there is a need to issue a Cyber security action notice for IoC blocking	CDTI	CDTI to provide recommendations and actions on gathering intelligence
	Identify clean backup images of the impacted assets	Local market	The clean image must be used during recovery

	Task	Role (Responsible)	Comment
Containment	Execute actions captured under: "Identify if additional containment is needed to stop the spread of the infection"	CDIM	
	Isolate the infected asset(s)	Local market	• Isolate by disconnecting the network cable and disable Wi-Fi (if applicable). **Do not power off the asset or**, • Disable switch port • Isolate using a secure VLAN where available
	Protect other domains that are connected to the infected domain	Local market	Identify the domain with infected hosts, has connection to any other domains. Stop the infection from spreading
	Block attacker's domain/IP on Group web proxy	Network security	To identify if the local market is covered by the Group web proxy
	Issue a Cyber Security Action Notice (CSAN)	CDTI market	This can be done either by emailing them or over the technical call etc.
	Reset password of any compromised account	Local market	
	Disable compromised account	Local market	If any evidence of credential dumping is observed, then consider disabling the user account
	Propose new/custom detection rules (IPS, Anti-Malware/Virus, Log Correlation, others)	CSOC	
	Submit the sample of the malicious file to AV vendor and CERT	CSOC/CDTI/CERT	

	Task	Role (Responsible)	Comment
Eradication	Rebuild infected systems from known-good media	Local market	Use clean backup image. If no backup available, then use a vanilla image
	Confirm endpoint protection (AV, EDR, etc.) is up to date and enabled on all systems	Security engineering	
	Deploy custom signatures to endpoint protection and network security tools based on discovered IoCs	Local market/ Security engineering	
	Monitor for re-infection: consider increased priority for alarms/alerts related to this incident	CSOC	

	Task	Role (Responsible)	Comment
Recovery	Confirm patches are deployed on all systems (prioritizing targeted systems, OSes, software, etc.). Preview against the Hardening standard for devices managed by the XY company	Local market	
	Ensure the asset(s) has anti-virus solutions and EDR tooling installed and verified	Local market	
	Check backups for indicators of compromise	Local market	
	Consider partial recovery and backup integrity testing	Local market	This step should only be done surgically, run up to date AV to confirm, then removal of all evidence, and then tactically back up

Lessons Learned	Task	Role (Responsible)	Comment
	Provide IR report	CERT/Mandiant	This needs to be reviewed on a case-by-case basis. If CERT is leading an investigation, then they have to produce an IR report/CERT narrative A Mandiant IR report can be downloaded from their secured infrastructure. A more detailed forensics reports can be requested depending upon the severity and impact
	Ensure all IoCs are uploaded to IBM SOAR	CDTI	

Implementing an incident management playbook might be difficult. However, it can be successfully implemented if the following steps are considered:

- Defining goals
- Creating a comprehensive playbook
- Communicating with stakeholders
- Providing training
- Testing and refining the playbook
- Continuous improving

These steps will help to ensure that the team is well-prepared to respond to incidents and minimize their impact.

Results and Discussion

XY is a multinational company with over one million customers. Its Incident Management team handles cyber incidents reported via relevant channels, emails, and calls. Severity levels are determined using the Cyber Severity Matrix of Impact, which is used to assign levels to all incidents. The practical part of this work represents and shows the importance of incident management and the Incident Lifecycle process, which involves Preparation, Identification, Containment, Investigation, Remediation, and Recovery. It also presents the statistics about the common security issues faced by organizations, such as illegal resource access and bad bots. The work also examines the use of email for incident management communication, its benefits, and drawbacks. The network architecture is explained and the impact of network topology of incident management is discussed, outlining the important assets and their values. The Tufin security policy management platform's Clean Up module was introduced to assist in identifying and removing unused or obsolete security rules and objects, that would lead to incidents events and alerts. The Clean UP module helped in the optimization of the Incident management process and lifecycle. Lastly, an Incident management Playbook was generated specifically for the company XY, which could also be used for any large enterprise/organization, keeping in mind the existing challenges faced by the company and its incident management team.

However, there is always a room for improvement in each and every organization. Focusing on the company XY, several areas in incident management procedures, communication, network topology, and security policy management could be improved. The organization should focus on updating and defining incident management procedures, exploring more efficient communication tools available in the market, understanding and maintaining their network topology, and utilizing security management platform to prioritize rules and objects for removal based on risk. The company should consider utilizing automation tools to help identify and respond to security incidents more quickly and establish clear communication channels. Over all, the organization should aim to continuously enhance their incident management capabilities to prevent and respond to security incidents effectively.

Conclusion

In today's digital age, cybersecurity threats have become a significant concern for organizations worldwide. As such, implementing a strong security system that can effectively defend an organization's computer networks, its customers and employees is crucial. The Diploma Thesis aims to contribute to this by proposing an enhanced security system that is capable of defending against contemporary risks and vulnerabilities. It also aimed to gather and analyze theoretical knowledge related to security monitoring, including its processes, use cases, data sources and methods, tools for data evaluation, and necessary organizational and process measures. The study also emphasizes the importance of exploring new and open standards and methodologies to provide a comprehensive framework for security monitoring. The theoretical part of the thesis also explores the foundations of network monitoring such as for network attacks, threats, risks and classification of vulnerabilities.

The second part of the work describes an anonymous organization and its infrastructure, along with legislative requirements. The practical part incudes conducting an analysis of the existing security systems and procedures used, based on the identified vulnerabilities and organizational features. The existing solution of the company is capable of detecting security events and incidents, including advanced attacks, and could meet legislative requirements with further improvements. Although, there are no compromised assets, risk analysis and vulnerability management process are in place along with the incident management process and lifecycle, the current framework or solution still needs fine-tuning for better adaptation of technical parameters, elimination of problems and potential incidents that may cause harm or damage to an organization's assets. Incidents may arise due to a combination of risks and vulnerabilities, therefore, managing risks and vulnerabilities and implementing a proper incident management plan are crucial strategies for an organization to invest and focus on.

The results of this thesis work could be used as a guideline for/by any enterprise or organization, who aims to protect its computer network, customers and employees. The results provide insights of an organization, how risk and vulnerabilities can lead to incidents and hence uniform and regular revision of such processes are to be maintained for effectiveness.

Bibliography

BEJTLICH, Richard. The practice of network security monitoring: understanding incident detection and response. San Francisco: No Starch Press, [2013]. ISBN 978-1593275099.

bmc. OSI Model: The 7 Layers of Network Architecture (29.06.2018) [online]. Available at https://www.bmc.com/blogs/osi-model-7-layers/

BONDAREV, V. Security analysis and monitoring of computer networks. Moskva: MGTU, 2017. ISBN 978-5-7038-4757-2.

Cloudflare -WAF [online]: https://www.cloudflare.com/learning/ddos/glossary/web-application-firewall-waf/

Dr. Raaid Alubady. Data Communication and Networking, Network Models II (12.12.2017) [online]. Available at https://www.uobabylon.edu.iq/eprints/publication_12_12504_6270.pdf

Enterprise Firewall-CheckPoint [online]: https://www.checkpoint.com/cyber-hub/network-security/what-is-firewall/what-is-an-enterprise-firewall/#:~:text=A%20firewall%20defines%20the%20boundary,different%20firewall%20and%20security%20needs.

ITIL (Information Technology Infrastructure Library) Problem Management [online]. Available at https://www.ivanti.com/glossary/problem-management

Joseph Mathenge, John Stevens-Hall. Problem Management in ITIL 4 and Beyond, BMC Blogs (16.05.2019) [online]: https://www.bmc.com/blogs/itil-problem-management/

Mark Stone. What is Cybersecurity testing? Reviewing testing tools, methodologies for proactive cyber readiness (09.02.2021) [online]. Available at https://cybersecurity.att.com/blogs/security-essentials/cybersecurity-testing-explained

MAURO, D., SCHMIDT, K. Essential SNMP, Second Edition. Beijing: O'Reilly Media, 2005. ISBN 05-960-0840-6.

Microsoft Security-SIEM [online]: https://www.microsoft.com/en-us/security/business/security-101/what-is-siem#:~:text=SIEM%2C%20pronounced%20%E2%80%9Csim%2C%E2%80%9D,analysis%2C%20and%20takes%20appropriate%20action.

MindMajix-SIEM, ArcSight vs Splunk [online]: https://mindmajix.com/arcsight-vs-splunk

Muhammad Raza. Public vs Private vs Hybrid: Cloud Differences Explained (31.08.2020) [online]. Available at https://www.bmc.com/blogs/public-private-hybrid-cloud/

NORTHCUTT, S., NOVAK, J. Networking intrusion detection. Indiana: Indianapolis, 2003. ISBN 0-7357-1265-4.

OWASP-Web Application Firewall [online]: https://owasp.org/www-community/Web_Application_Firewall

Sangay Yeshi. Basic Networking Tutorial (08.10.2011) [online]. Available at https://www.mowhs.gov.bt/wp-content/uploads/2011/08/What-is-a-computer-Network.pdf

SKABTSOV, N. Information systems security audit. SPB: Peter, 2018. ISBN 978-5-4461-0662-2.

List of Figures

List of Tables

Abbreviations

DLP – Data Loss Prevention

SIEM – Security Information and Event Management

VPN - Virtual Private Network

LAN – Local Area Network

WAN – Wide Area Network

OSI – Open System Interconnection

ISP – Internet Service Provider

SD-WAN – Software-Defined Wide Area Network

QoS – Quality of Service

TCP – Transmission Control protocol

IP- Internet Protocol

HTTP – Hypertext Transfer Protocol

HTTPS - Hypertext Transfer Protocol Secure

ICMP – Internet Control Message Protocol

SNMP – Simple Network Management Protocol

SFTP – Secure File Transfer Protocol

SSL – Secure Sockets Layer

UDP – User Datagram Protocol

IRC – Internet Relay Chat

DDoS – Distributed Denial of Service

DoS – Denial of Service

DNS – Domain Name System

SSH – Secure Shell Protocol

API – Application Programming Interface

IPsec - Internet Protocol Security

SCTP – Stream Control Transmission Protocol

ARP – Address Resolution Protocol

RARP – Reverse Address Resolution Protocol

IGMP – Internet Group Management Protocol

ATM – Asynchronous Transfer Mode

FTP – File Transfer Protocol

CSMA/CD – Carrier-sense Multiple Access with Collision Detection

CSMA/CA - Carrier-sense Multiple Access with Collision Avoidance

IBM – International Business Machines Corporation

IEEE – Institute of Electrical & Electronics Engineers

ECD – Enterprise Connected Devices

IoT – Internet of Things

SMS – Short Message Service

MMS – Multimedia Messaging Service

BGP – Border Gateway Protocol

IDS – Intrusion Detection System

IPS – Intrusion Prevention System

EDR – Endpoint Detection and Response

NMS – Network Management System

MIB – Management Information Base

OID – Object Identifier

CPU – Central Processing Unit

HIPAA – Health Insurance Portability and Accountability Act of 1996

PCI-DSS – Payment Card Industry Data Security Standard

MAC – Media Access Control Address

QA – Quality Assurance

ITIL – Information Technology Infrastructure Library

PIR – Post Incident Review

CSI – Continual Service Improvement

NIDS – Network Based Intrusion Detection System

HIDS – Host Based Intrusion Detection System

AIDS – Application-Based Intrusion Detection System

NAC – Network Access Control

GDPR – General Data Protection Regulation

ESM – Enterprise Service Management

CA – Certificate Authority

AWS – Amazon Web Services

UF – Universal Forwarder

HF – Heavy Forwarder

SOAR – Security Orchestration, automation and Response

F5 – BIG IP / Distributed Cloud Services

CSOC – Cyber Security Operation Center

CDTI – Cyber Defense Threat Intelligence

IoC – Indicator of Compromise

CERT – Computer Emergency Response Team

CDIM – Cyber Defense Incident Management

IM – Incident Management

NÚKIB – Národní Úřad Pro Kybernetickou a Informační Bezpečnost

SQL – Structured Query Language

MFA – Multi-Factor Authentication

DMZ – Demilitarized Zone

ASIC – Application Specific Integrated Circuit

IOS – Internetworking Operating System

WAF – Web Application Firewall

HIPS – Host Intrusion Prevention System

AV – Anti-Virus

CSAN – Cyber Security Action Notice

IR – Integrated Report

XSS – Cross-Site Scripting

Appendix

Incident Instance 1

```
The properties associated with this event were:
closed: 1
dataAtLowestOffset:
 PCFET0NUWVBFIGh0bWw+CjxtZXRhIG5hbWU9J0Rlc2NyaXB0aW9uJyBjb250ZW50PSd1YWdh
 oc2JkYnlulHJoZA==
devicePath: \Device\HarddiskVolume4
eventReason: File closed
fileExtension: html
fileName: _516_HOWDO_text.html
filePath: Restore\BackLine Angels\OLD\BackOffice\Vykazy\Non smna\Roaming\procedury
fullPath: D:\Restore\BackLine Angels\OLD\BackOffice\Vykazy\Non
smna\Roaming\procedury\_516_HOWDO_text.html
lowestFileOffsetSeen: 0
md5: feb9203f01e0424e3ab39d027c77b5d8
numBytesSeenWritten: 9556
openDuration: 0
openTime: 2022-12-27T12:43:37.734Z
parentPid: 16068
parentProcessPath: D:\Program Files\Veritas\NetBackup\bin\bpcd.exe
pid: 10668
process: tar32.exe
processPath: D:\Program Files\Veritas\NetBackup\bin
size: 9556
textAtLowestOffset: <!DOCTYPE html>.<meta name='Description' content='uaghsbdbyn rhd
timestamp: 2022-12-27T12:43:37.734Z
username: NT AUTHORITY\SYSTEM
```

Incident Instance 1

```
MDE Timeline Details :
nbpas.exe >>
"bpcd.exe" -root_bpcd
D:\Program Files\Veritas\NetBackup\bin\bpcd.exe>>
"tar32.exe" -x -v -Y -p -P -l 1679660404 -U 13 -E /D/Programŕ€
 Files/Veritas/NetBackup/logs/ALTPATH/ALTPATH.029 -k -J clnt_lc_messages=CSY -J
 clnt_lc_time=CSY -J clnt_lc_ctype=CSY -J clnt_lc_collate=CSY -J clnt_lc_numeric=CSY -J
 restoreid=27026.001 -J job_total=4 -J shm_restore -J client=w2bkup02.oskarmobil.cz -J
 requesting_client=w2bkup02 -J browse_client=wc03ad02 -J backup_time=1679079600 -L
 /D/Programŕ€ Files/Veritas/NetBackup/logs/user_ops/jirik000/logs/NBWIN001 -f - -J
 shm_restore_fd=900 -dte 0 -tk root_root
d:\program files\veritas\netbackup\bin\tar32.exe>>
D:\Restore\BackLine Angels\OLD\BackOffice\Vykazy\Noční
směna\Roaming\procedury\_516_HOWDO_text.html
4c9d161662f259ccfe3497922c28aaf625c28598bfce5fb86bcc6af48e307d47
```

Incident Instance 2

Customer Name : PV-HRK

Device Severity : Warning
Device Action : alerted
Device Receipt Time : 15 Jan 2023 09:48:19 UTC
Device Event Class ID : rule:107
Device Address : 85.205.85.182
Device Vendor : F5
Device Product : ASM

Source Attack :
212.4.152.90
178.255.168.208
185.52.173.25
109.183.140.58
86.49.125.226
78.80.123.140
95.80.223.76
46.167.221.102
89.203.218.252
46.167.221.125
46.167.221.147
85.160.47.94

Incident Instance 2

Source Address : 107.174.124.75
Source Dns Domain : seznam.cz
Source Port : 41755
Source User Name : majda1912@seznam.cz
Source User ID : 816b035e2ef4feb0

Old File Permission : | multisensortouched | wafEnrichment|MainChannel-10 touch

Request Method : POST

Device Custom Date1.policy_apply_date : 25 Oct 2022 02:14:31 UTC
Device Custom Number1.response_code : 401
Device Custom Number2.violation_rating : 5
Device Custom Number3.device_id : 0
Device Custom String1.policy_name : /WebSupport/vs-muj-asm.class
Device Custom String2.http_class_name : /WebSupport/vs-muj-asm.class
Device Custom String3.full_request : POST /muj/en/login-check HTTP/1.1
Proxy-Connection: keep-alive

Incident Instance 2

```
Connection: keep-alive
Accept-Encoding: gzip,deflate
Content-Type: multipart/form-data; boundary=------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Length: 583
Accept: application/json, text/plain, */*
Accept-Language: en-US,en;q=0.9
Cache-Control: no-cache
Pragma: no-cache
sec-ch-ua: " Not A;Brand";v="99", "Chromium";v="90", "Google Chrome";v="90"
sec-ch-ua-mobile: ?0
Sec-Fetch-Dest: empty
Sec-Fetch-Mode: cors
Sec-Fetch-Site: same-origin
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like
Gecko) Chrome/90.0.4430.212 Safari/537.36
Cookie: WSCSID=68nnr5h6ish576qgu2rvfcs5j1; hl=cs; persist-
101=rd10o00000000000000000000ffff505f63c4o20000;
TS016e7c23=018d647fa36562309a548bc842eafc34020fd8ac1527794f55a5e1a9c41fe2f17c1
182c66f572921792ea29172ae4d6e821b442cf5
X-Forwarded-For: 107.174.124.75
X-Secure-Transfer: true
X-Forwarded-Proto: https
```

Incident Instance 2

```
--------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Disposition: form-data; name="_username"
majda1912@seznam.cz
--------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Disposition: form-data; name="_password"
3xc7veZyxrsP
--------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Disposition: form-data; name="_type"
login
--------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Disposition: form-data; name="_api_call"
true
--------WebKitFormBoundaryqalvfgcexhhupdyl
Content-Disposition: form-data; name="_context_mode"
DEFAULT
--------WebKitFormBoundaryqalvfgcexhhupdyl--
Device Custom String4.attack_type : Brute Force Attack
Device Custom String5.x_forwarded_for_header_value : 107.174.124.75
Device Custom String6.geo_location : US
Flex String1.IP Intelligence Category : N/A
```