DEVELOPMENT OF STRATEGIES FOR EFFECTIVE DETECTION OF DATA LEAKAGE

CEM KÜLEKCİ

JUNE, 2022

DEVELOPMENT OF STRATEGIES FOR EFFECTIVE DETECTION OF DATA LEAKAGE

A THESIS SUBMITTED TO THE

GRADUATE SCHOOL

OF

BAHÇEŞEHİR UNIVERSITY

CEM KÜLEKCİ

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR

THE DEGREE OF

CYBER SECURITY MASTER'S PROGRAM

JUNE, 2022

BAHÇEŞEHİR UNIVERSITY

GRADUATE SCHOOL

...../...../.....

MASTER THESIS APPROVAL FORM

Program Name:	
Student's Name and Surname:	
Name of The Thesis:	
Thesis Defense Date	

This thesis has been approved by the Graduate School which has fulfilled the necessary conditions as Master thesis.

Prof. Dr. Ahmet ÖNCÜ

Institute Director

This thesis was read by us, quality and content as a Master's thesis has been seen and accepted as sufficient.

	Title, Name	**Signature**
Thesis Advisor:		
2. Member:		
3. Member:		

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Name, Last Name :

Signature :

ABSTRACT

DEVELOPMENT OF STRATEGIES FOR EFFECTIVE DETECTION OF DATA LEAKAGE

CEM KÜLEKCİ

Cyber Security Master Program

Thesis Supervisor: Prof. Dr. Ahmet Naci ÜNAL

June 2022, 60 Pages

Nowadays, data enters and leaves enterprises' cyberspace at record rates. For a typical enterprise or financial institute such as banks, millions of emails are sent and received and thousands of files are downloaded, saved, or transferred via various channels or devices on a daily basis. Meanwhile, companies hold sensitive data that customers, business partners, regulators, and shareholders expect them to protect. Unfortunately, companies constantly fall victim to massive data loss and high-profile data leakage involving sensitive personal and corporate data continue. Data loss could substantially harm a company's competitiveness and reputation and could also invite lawsuits or regulatory crackdowns for lax security. Therefore, organizations should take measures to understand the sensitive data they hold, how it is controlled, and how to prevent it from being leaked.

Many financial firms invest significant time and energy into identifying sensitive information. Still, many fall short in their ability to detect and control the unauthorized leakage of that information. Data loss comes in many forms. These range from the malicious insider seeking to sell a competitor's proprietary information to an undertrained administrative assistant accidentally attaching the wrong file to an email message. Data loss prevention (DLP) technology offers information Security staff at financial companies the ability to monitor hosts and networks for potential leaks and stop any loss before it is too late. The software offers

a comprehensive, content-aware solution designed to monitor and protect confidential data wherever it is stored or used.

In this thesis, I have worked on what kind of strategies we should follow and which detection and mitigation methods on SIEM environment so that we may use to prevent data loss and exfiltration as Cyber Security Professionals.

Keywords: DLP, SIEM, insider

ÖZET

VERİ SIZINTILARININ ETKİLİ TESPİTİ İÇİN STRATEJİLERİN GELİŞTİRİLMESİ

CEM KÜLEKCİ

Siber Güvenlik Yüksek Lisans Programı

Tez Danışmanı: Prof. Dr. Ahmet Naci ÜNAL

Haziran 2022, 60 Sayfa

Günümüzde veriler, kurumların siber alanına rekor oranlarda girip çıkmaktadır. Bankalar gibi tipik bir işletme veya finans kurumu için, günlük olarak milyonlarca e-posta gönderilip alınmaktadır ve binlerce dosya çeşitli kanallar veya cihazlar aracılığıyla indirilip, kaydedilmekte veya aktarılmaktadır. Bu arada şirketler, müşterilerin, iş ortaklarının, düzenleyicilerin ve hissedarların korumalarını beklediği hassas verileri elinde bulundurur. Ne yazık ki, şirketler sürekli olarak büyük veri kayıplarına maruz kalmakta ve hassas kişisel ve kurumsal verileri içeren yüksek profilli veri sızıntıları devam etmektedir. Veri kaybı, bir şirketin rekabet gücüne ve itibarına önemli ölçüde zarar verebilir veya sıkı olmayan güvenlik politikalari nedeniyle dava edilebilir veya düzenleyici kurumlar tarafından uyarılabilirler. Bu nedenle kuruluşlar, sahip oldukları hassas verileri, nasıl kontrol edildiğini ve sızdırılmasını nasıl önleyeceklerini anlamak için önlemler almalıdır.

Birçok finans firması, hassas bilgileri belirlemek için önemli miktarda zaman ve enerji harcamaktadır. Yine de birçoğu, bu bilgilerin izinsiz şekilde sızmasını tespit etme ve kontrol etme yeteneklerinde yetersiz kalmaktadır. Veri kaybı birçok biçimde gelir. Bunlar, bir rakibin özel bilgilerini satmaya çalışan kötü niyetli içeriden bilgi sahibi olmayan bir yönetici asistanına yanlışlıkla yanlış dosyayı bir e-posta mesajına eklemeye kadar uzanır. Veri kaybını önleme (DLP) teknolojisi ve buna bağlı birçok uygulama, finans şirketlerindeki bilgi güvenliği personeline, ana bilgisayarları ve

ağları olası sızıntılara karşı izleme ve çok geç olmadan herhangi bir kaybı durdurma yeteneği sunmaktadır. Yazılım ve uygulamalar (güvenlik ürünleri), saklandığı veya kullanıldığı her yerde gizli verileri izlemek ve korumak için tasarlanmış kapsamlı, içeriğe duyarlı bir çözüm sunmaktadır.

Bu tezde, Siber Güvenlik Profesyonelleri olarak veri kaybını ve sızmayı önlemek için ne tür stratejiler izlememiz gerektiği ve SIEM ortaminda hangi tespit ve azaltma yöntemlerini kullanabileceğimiz üzerinde çalıştım.

Anahtar Kelimeler: DLP, SIEM

ACKNOWLEDGEMENTS

First, I would like to thank everyone who helped me to conduct this project throughout the thesis preparations and for all encouragement and inspiration.

Further, I would like to thank my supervisor of the Master of Cyber Security at Bahçeşehir University Prof. Dr. Ahmet Naci ÜNAL; he has been thoughtful and supported in this period even pandemic put many difficulties and obstacles in front of us. However, I believe that we did overcome the obstacles with excellent collaboration and commitment.

Finally, I would like to thank my marvelous family for their absolute support.

İSTANBUL, 2022 CEM KÜLEKCİ

TABLE OF CONTENTS

LIST OF FIGURES

FIGURES

LIST OF TABLES

TABLES

ABBREVIATIONS

HIPAA	Health Insurance Portability and Accountability Act
PCI	Payment Card Industry Data Security Standard
PII	Personally Identifiable Information
DLP	Data Leakage/Loss Prevention
CIS	Center for Internet Security
DPO	Data Protection Officer
EU	European Union
GDPR	General Data Protection Regulation
IDS	Intrusion Detection System
ISO	International Organization for Standardization
IT	Information Technology
PC	Personal Computer
PCI	DSS Payment Card Industry Data Security Standard
SSH	Secure Shell
VPN	Virtual Private Network
ACL	Access Control List
AD	Active Directory
C2	Command and Control
DNS	Domain Name System
EDR	Endpoint Detection and Response
GRC	Governance Risk and Compliance
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
IOCs	Indicators of Compromise
IPS	Intrusion Prevention System
IT	Information Technology
MFA	Multi-Factor Authentication
MITRE	MITRE Adversarial Tactics, Techniques, and Common Knowledge®
NIDS	Network Intrusion Detection System
NIST	National f Standards and Technology

Chapter 1

Introduction

Information is a fundamental asset to institutions where large amounts of information are regulated every day in numerous methods and through many individuals. IT technologies, for instance, computers, the internet, e-mail, portable devices, external data storage, and social media, improve the possibility of unauthorized exposure and failure of data that leave an institution's limitations available to unauthorized commodities. Data loss creates a considerable risk to the private and government sectors. It can negatively affect the credibility of the private sector in the market, competitive benefits, collaborations, and consumer credentials, while in the government sector, data loss can impact public and diplomatic connections and national security.

The significance of data causes the need to have a vital security strategy and plan to protect information sensitivity. Network security technologies like firewalls and IDSs were presented in the first place to stop outbound threats; nevertheless, the same hazard can reach inbound sources via data leakage. Therefore, the DLP adoption has been presented to confound the insufficiency of internal threats. Nonetheless, despite the potential of DLP programs, very few associations thrive in following the proper technique for adoption. A successful DLP adoption strategy boosts the recommendation for a DLP adoption standard as work designed from the existing study analyses and surveys accomplished by education and professionals from the standpoint of data protection. This study paper delivers a model that should operate as a starting point for institutions to successfully embrace DLP and handles the eleven elements of the DLP Adoption Model. Nonetheless, since the model could confront several challenges during implementation, these must be regarded and preached before adopting the model.

1.1 Motivation

As part of the corporate structure, solutions to protecting security data are maintained with constantly changing and updated versions. Data integrity provides the unity of financial information, strategic goals, market plans, customer portfolio, budget applications and personal information. This information is essential for the future of institutions. In recent years, there have been significant amount of data breach incidents happen, leaks affecting data security have started and continue to increase today. Data leakage prevention systems first started to make their name with this event. This situation brought an existing problem to the surface. The importance of preventing corporate data leakage from various sources outside the institution has begun to be understood. The need for solutions that will control the data flow of users and ensure data security within the institutional structure is increasing day by day. The new technologies will offer some practices to minimize data breaches. This thesis has been prepared to develop a solution and strategy that will control the data flow within the institution and prevent the flow of sensitive data. The thesis aims to create an integrated approach for data leakage protection. The developed techniques and software will detect and monitor critical ratings, including data leakage prevention, data in use, and data in motion, and provide data protection by intervening when necessary. The way to prevent data leakage is to cut off statements that contain meaningful data. While giving direction to the thesis by looking at the general problems of the developed data leakage prevention systems, the difficulties of data classification in client-based data flow and network-based content analysis have been addressed. An effective and efficient architecture has been designed for data leak prevention.

1.2 Goals and Objectives

The objectives of this research are as follows:

- Identify threats
- Integrate recent security models and concepts with the detection capabilities
- Develop usecases using SIEM and Cloud solutions to detect leakage or any

exfiltration

- Develop holistic, scalable and proactive strategy

1.3 Methods, Concepts And Tecnologies

This research aims to provide a comprehensive approach and strategy to implement security measures and controls to detect, identify and remediate all the Data Leakage related incidents and activities within the business.

1.4 Literature

Data leakage (or information leakage) is the forbidden transfer of information (or data) from inside an enterprise to the outside or storage. Data leakage could happen in different forms, such as an electronic or physical form consciously or viciously by an insider or foreigner within the enterprise. Cyber Security Professionals must always observe security events in different systems and technologies to detect suspicious activity, exploring artefacts of data leakage in increased magnitudes of data. According to Khan et al., data leaks may be originated from an external or internal source and are normally the consequence of using exploits for vulnerabilities.

Luft dealt with the general VSE definitions in his thesis and made procedural explanations. The solutions of Mcafee and Websense security products were examined. He also included the results in his thesis (Luft, 2009).

Xiaosong and others are trying to prevent the leakage of sensitive data, whether intentionally or unintentionally, in the corporate environment. The application offers mandatory and transparent filtering. The emphasis on user flexibility and data security has been the subject of the study (Xiaosong, 2009).

Mohammed, Babak and Pavel are immersed in the strong security design and strategy to safeguard data sensitiveness. Predominantly they have emphasised insider threats because legacy safety approaches such as next-generation firewalls and IPS were presented long ago to contain outbound hazards; nevertheless, the actual risk can come from internal assets through data leakage.

Alneyadi, Sithirasenan, and Muthukkumarasamy (2016) examined data

leakage detection and prevention to investigate the specific DLP system from a theoretical study standpoint. They explored data leakage prevention techniques; nonetheless, there is no natural perception or suggested benchmark on successfully modifying the data leakage detection and prevention as a comprehensive technique for protecting information from disclosure and how it supports digital researchers in discovering the evidence efficiently.

Raman, Kayacık, and Somayaji (2011) indicated that data leakage methods comprehended by various retailers manage just the hazard of data leakage, which is part of the entire approach of data leakage detection and prevention execution. Their research also revealed that as data leakage prevention execution is complex, choosing the type of data to protect, deciding the use of data, and how the data can be leaked needs an understanding of the enterprise functions before starting the execution. Furthermore, other vital comprehensiveness elements of data leakage prevention adoption are scrapped, such as the procedure, function, data classification, data management, training, awareness, and reporting. The writers suggest more data leakage prevention studies to determine the associated issues.

1.5 Contribution

In this thesis, Splunk has been used to detect potential detections there including Data Exfiltration after Data Staging, Multiple DLP events by User, and more. Meanwhile, one of the most used cybersecurity frameworks, MITRE ATT&CK will be used while creating use-case and building a structure. Although Microsoft 365 Compliance has been used to create organizations with sensitive data under control, such as financial data, health records, proprietary data, social security numbers, and credit card numbers, to support protect this sensitive information and decrease risk, they require a method to contain their users from unauthorized transferring it with individuals who should not hold it. This method is named data loss prevention (DLP). Microsoft 365 implements data loss prevention by clarifying and using DLP policies. With a DLP guideline, it is possible to determine, monitor, and automatically protect sensitive data across:

- Windows 10, Windows 11 and macOS (Catalina 10.15 and higher) endpoints
- Microsoft 365 products : Exchange, SharePoint ,Teams and OneDrive
- Office applications such as Word, Excel, and PowerPoint
- on-premises file shares and on-premises SharePoint
- non-Microsoft cloud apps

Microsoft 365 can identify sensitive things utilizing deep content analysis, not only with a basic text scanning. Content has been examined for direct data matches to keywords by assessing regex(regular expression), internal function verification, and secondary data matches immediately to the primary data match. Furthermore, DLP even utilizes machine learning algorithms and other techniques to detect content corresponding to the DLP methods.

Chapter 2

Data Leakage/Loss Prevention

2.1 DLP Definitation

Data Leakage is the not approved transfer of data from within an association to an external destination or recipient. It may be electronic or maybe through a physical way. Data Leakage is interchangeable with the phrase Information Leakage. The anthology is encouraged to be aware that unauthorized does not automatically imply intentional or adversary. Unintentional or accidental data leakage is also not permitted.

Data Leakage Prevention is a solution developed to detect potential data violation incidents and prevent them by monitoring data while in use, in motion, or at rest. DLP is regarded as a paradigm transformation in information security. It manages threats; these threats are focused on handling certain types of data with information security risk, such as personally identifiable, credit cards, financial and legal information. Exposing this data outside a corporation's security frame leads to outcomes damaging to the company. DLP solutions support protecting data from moving outside the company.

DLP persists in being a complicated business-centric protection industry for enterprises to overwhelm. The complicated essence is primarily attributed to the numerous attack surfaces and unlimited exfiltration tactics. Being compromised is a more subordinate criticality type than being breached; a centre is a prototype event to the violation. The sophistication is not necessarily a technical obstacle, but the many methods that a DLP program must distinguish between "known-good" activity and the proportionate plan of the detection settings to detect exfiltration; are iterative and potentially endless. Describing "known-good" notation allows the enterprise to preserve work. Designing detection mechanisms for the exfiltration requires DLP proficiency to think like an attacker and gain visibility within the different attack surfaces that may be leveraged in orchestrating the exfiltration. The findings plan to resume enriching and extending the corporate DLP programs leased to protect

against the hazard of losing sensitive information.

Data Leak Prevention, also known as Data Leak Prevention, is a program that integrates technologies, policies, and methods to prevent unauthorized personnel from gaining access to an organization's sensitive data. DLP solutions are developed to protect organizations against insiders' misuse of confidential data. DLP also directs to tools and methods that support network administrators monitoring and controlling transmitted data. This helps prevent workers from sharing personal information outside of an organization. These solutions observe various transmission mechanisms, including email, peer-to-peer (P2P) transmissions and social networks, removable media, and mobile devices. When a DLP tool sees an apparent leak of private and personal information, it will thwart the communication and information security admins so that it may take any further action needed.

2.2 Data Types

Data is held in two different formats, structured and unstructured. The type of procedure utilizing the data dictates the kind of information. A traditional structured data model is a database process that stores and indexes binary digits in a structured format, also authorizing reference and repeatable associations or recognition. The inputs and outputs of each method are consecutive and guessable, which are components of structured information types. Predictability use is limited; hence, DLP check logic about structured data is finite. Unstructured data forms might have short message service (SMS) notifications, audio/visual interchanges, document processing, emails, or imagery. DLP confronts a challenge with these data types as they deliver automated and unlimited processing. Unlike structured data forms, unstructured data forms do not present repeatability or predictability. For instance, document processing applications that authorize users to abuse and hold individual documents are supposed to be unstructured data. Nevertheless, resolving what makes the content or context of the document sensitive becomes the challenge, so this is not a limited process.

Four main types of data leaks – analytics, trade secrets, client data and firm data.

Customer information:

Some of the most important data breaches included consumer data leaks involving PII. Consumer information is unique to each enterprise. Consumer confidential data could consist of any of the following.

- Usernames
- Payment's history
- Product browsing habits
- Credentials
- Customer names
- Addresses
- Phone number
- Email addresses
- Card numbers

Company data; leaked enterprise data expose the sensitive internal activity. Such information leaks cultivate be in the cross-hairs of unethical enterprises following the trade plans of their competitions.

- Performance metrics
- Company data leaks could include the following:
- Internal communications
- Marketing strategies

This is the deadliest form of data leak to an enterprise. Stealing intellectual property eliminates an company's potential, driving it to the ground.

- Trade secret data leakage might contain the following:
- Proprietary technology information
- Upcoming product plans
- Software coding

Analytics: Analytics data leaks might contain the following:

- Modelled data
- Psychographic data
- Customer behaviour data

2.3 Data Leakage Types And History Of Breach

2.3.1 Data Leakage Types. First, to enforce the proper defensive measurements understand what must be protected. According to the publicly disclosed data violations, the kind of data leaked is broken down as follows:

Table 1 Type of Information Leaked (Peter Gordon, 2007)

Type of information leaked	Percentage
Confidential Information	15
Intellectual property	4
Customer data	73
Health records	8

Institutions with top information security programs layer almost all available data loss prevention measures —others pick and choose:

- Those that grade their data security as red (35%)
- Those that grade their data security as orange (65%)

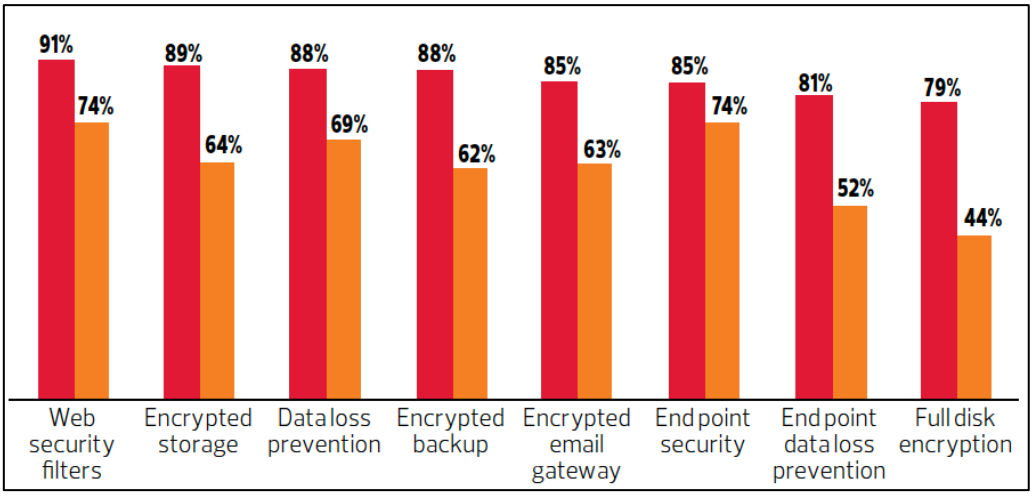

Figure 1 2012 CDW Data Loss Straw Poll

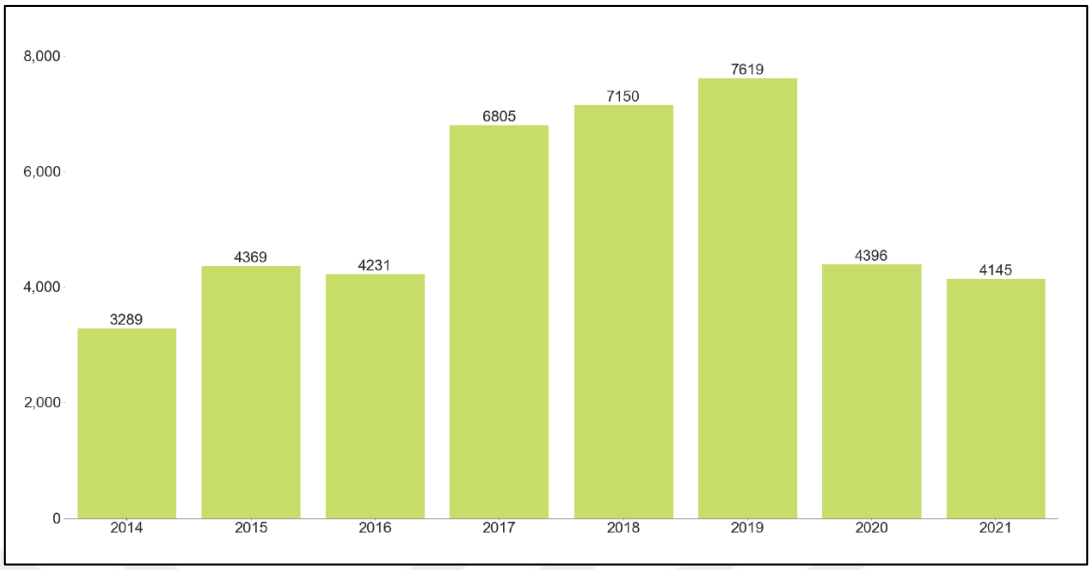

Figure 2 Number of breaches reported by eight years

2.3.2 History of Data Breach. Information breaches whether might be financially motivated or not. Some violations are even politically motivated by publicly disclosing government information as a form of activism or social righteousness. Violations can be motivated by thrill-seekers witnessing how far they can take their notorious hacking talents. Data breaches generally arise because of human errors (falling victim to social engineering or phishing schemes) and inadequate security best practices (such as poor passwords). Any sensitive information type can be concerned in a breach. However, breaches generally point to PII, the most smoothly monetized by adversaries.

Breached PII has consist of:

- Drivers license information
- Dates of birth
- Personal health information
- Email addresses
- Usernames
- Passwords and hashed passwords
- Home addresses and contact information
- Full names
- Social security numbers

- Credit card and other personal financial data
- Insurance information
- Family and friends' PII
- Security question answers

Breaches may aim at non-PII information. It is often the case in politically motivated breaches, either by hacktivists or threat actors supported by nation-states. Non-PII breached information can include:

- Classified government documents or communications
- Internal business, such as trade secrets, business relationships, plans, or budgets
- Proprietary source code
- Infrastructure data, such as building, device, or defense blueprints

Top 10 data breaches shown below:

Facebook user leaked (2019)

- Records: 533 million
- Compromise: The phone numbers and account details for a calculated 533 million Facebook users contain Facebook ID numbers, profile names, email addresses, location information, gender data, job data, and anything else users could have joined in their profiles.
- Who attacked: N/A
- What happened: The data is presently being presented in 106 separate download packages, with the information split on a per-country ground. While the platform is publicly available and anyone may register a profile, the download links for these packages are only available to users who bought forum credits.

SolarWinds supply chain data breach (2020)

- Records: N/A
- Who attacked: The U.S. Attorney General said it seems to be Russia-backed hackers; nevertheless, Microsoft briefed it had caught two different attacks that compromised SolarWinds software updates.
- Compromise: more than 18,000 institutions and government entities at risk; attacks activated against around 50 organizations, including U.S. government agencies.

- What happened: For 18,000 enterprises and governments worldwide, software updates come from an IT management firm called SolarWinds, especially its Orion product. Nation-state backed hackers (think of them as digital soldiers) somehow got inside the SolarWinds update operation and privately positioned malware into a few months of updates. They even operated to digitally "sign" the updates, creating them seem legitimate.

The outcome is that when SolarWinds sent out the software updates, obtaining networks visited the legitimate data but not the sheltered malware, and enterprises unknowingly received both. It is a supply chain attack which operates as a Trojan horse.

Adobe data breach (2013)

- Records: 153 million
- Damages: $1.1 million in legal fees and $1 million to affected customers
- Compromise: debit and credit card information, usernames, and passwords
- Who attacked: unknown
- Summary: In 2013, Adobe noted that nearly three million clients had their encrypted data pilfered by hackers. After that, they raised their calculated 38 million clients in the same month. The same week's report indicated that more than 150 million accounts had been accessed. In 2015, a concession was reached for disregarding the U.S. Customer Records Act and unfair business procedures.

LinkedIn data breach (2012)

- Records affected: 165 million
- What was compromised: usernames and passwords Damages: paid $1.25 million to breached victims in the U.S. who paid for premium services
- Who attacked: Russian hacker group
- Summary: The organisation was attacked in 2012 when usernames and passwords were published in a Russian hacker forum. The same adversary selling MySpace's data sold personal user information for 5 Bitcoin (approximately $5,000 in 2012). It was not until 2016 that LinkedIn disclosed the full scope of the attack.

MySpace data breach (2013)

- Records affected: 360 million

- What was compromised: email addresses, usernames, and passwords for some but not all affected accounts
- Damages: leaked accounts could be hacked
- Who attacked: Russian hacker
- Summary: MySpace was attacked in 2013, though the attack was not made public knowledge until 2016. The stolen accounts were leaked to LeakedSources and also available to purchase on the Dark Web market The Real Deal for 6 Bitcoin (roughly $3,000 in 2013). The passwords were stored as SHA-1 hashes of the first 10 characters of the password, converted to lowercase.

U.S. Office of Personnel Management data breach (2015)

- Records: 21.5 million
- Damages: extremely personal information stolen.
- Compromise: Social Security numbers, fingerprints, and highly sensitive information used for background checks
- Who attacked: state-sponsored attackers working for the Chinese government, according to U.S. officials
- Summary: The OPM was the target of two cyberattacks in 2015. The first attack was conducted to steal state workers' data, including names, birth dates, home addresses, and social security numbers. The second directed to stolen private information of current, former, and forthcoming federal employees who had background checks. Background checks contain interview conclusions, mental health histories, financial records, and other information, but no proof shows this data was affected.

Target data breach (2013)

- Records: 60 million
- Damages: $18.5 million multistate settlement, $10 million class-action lawsuit settlement, and $10,000 payments to customers with evidence they suffered losses.
- Compromise: names, phone numbers, email addresses, payment card numbers, credit card verification codes, and other sensitive data
- Who attacked: unknown third party
- Summary: The adversaries acquired access to Target's networks in 2013 via

stolen credentials of a third-party vendor—the firm that serviced HVAC systems. They then acquired access to a client service database and uploaded malware to grab sensitive data. A consequent lawsuit came from 47 states and the District of Columbia, where a settlement was reached and new measures set for Target to enhance its security methods.

- Explicit attribution for the attack has never been appraised. Nonetheless, a Latvian computer programmer is accomplishing 14 years in jail for designing malware that person used in this data violation.

Adult FriendFinder Networks data breach (2016)

- Records: 412.2 million
- Damages: sensitive leaked account information
- Compromise: names, email addresses, and passwords
- Who attacked: N/A
- Summary: The stolen information arrived from six databases with 20 years of data. A preponderance of the passwords was protected by the vulnerable SHA-1 hashing algorithm, which resulted in 99% of the credentials. This information violation was extremely unfortunate for users due to the essence of the website, which presented informal hookups and adult content.

Marriott International data breach (2018)

- Records: 500 million
- Damages: U.K. fine of approximately $24 million and class-action lawsuits filed
- Compromise: some variety of contact data, passport numbers, Starwood Preferred Guest numbers, travel info, credit card numbers and expiration dates, and other personal data.
- Who attacked: Chinese intelligence group seeking to gather data on U.S. citizens using a Remote Access Trojan (RAT) and MimiKatz
- Summary: Marriott bought Starwood in 2016 but did not incorporate the Starwood platform into the Marriott reservation system. In 2018, they were even using the ageing IT infrastructure, which had been compromised in 2014. It is unknown if the stolen credit card data was ever decrypted and used.

Equifax data breach (2017)

- Records: 148 million

- Damages: $700 million to help people affected by the data breach; reputational damage; congressional inquiries
- Compromise: Social Security numbers, birth dates, addresses, and in some cases driver license numbers and credit card information

2.4 Data Leakage Vectors

2.4.1 Insiders and Insider Threats. According to report studied by Ponemon Institute, 62% of Data Security breaches are from employee or contractor, %23 of Data Security breaches are from criminal-malicious insider and %15 from Credential thief (impostor risk). (2020 COST OF INSIDER THREATS GLOBAL REPORT)

Insider threats present a complex and dynamic risk affecting all critical infrastructure sectors' public and private domains. An individual with privileged access to or understanding of an institution's resources, including personnel, facilities, data, tools, networks, and systems can be defined as Insider.

Insider examples:

- A person is given a badge or access device identifying them as someone with regular or continuous access (e.g., an employee or member of an association, a contractor, a vendor, a custodian, or a repair person).
- An individual who is acquainted with the institution's firm strategy and goals, authorized with projects, or the means to sustain the organization and deliver for the welfare of its people.
- An individual the association trusts, including workers, community members, and those to whom the institution has given sensitive information and access.
- A person to whom the organization has supplied a computer and/or network access.
- An individual who develops the institution's products and services includes those who know the secrets of the products that deliver value to the association.
- An individual-oriented with the organization's fundamentals, including pricing, costs, corporate resilience and imperfections.
- In the context of administrative procedures, the insider may be someone with access to sensitive data, which, if compromised, could cause damage to

national security and public safety.

Insider threat is the potential for an insider to use their privileged access or knowledge of an institution to harm that association. This harm can contain malicious, arrogant, or unintended deeds that negatively affect the association's integrity, confidentiality, availability, data, personnel, or facilities. External stakeholders and clients of DHS can find this generic description politely suited and adjustable for their association's use.

Following insider behaviors:

- Espionage
- Terrorism
- Unauthorized disclosure of information
- Corruption, including participation in transnational organized crime
- Sabotage
- Workplace violence

The insider threat can be defined as either unintentional or intentional.

Intended threats are actions taken to damage an institution for personal benefit or act on a personal grievance. Intended insider threats are mostly referenced as “malicious insiders.” The reason is a personal benefit or damage to the institution. As an example, most insiders are motivated to “get even” because of unmet expectations linked to a lack of distinction or even termination. Insider threat actions include leaking sensitive data, sabotaging equipment, harassing associates, or committing crimes. Others have misappropriated proprietary data or intellectual property in the false hope of advancing their careers.

Negligence – An insider of this kind discloses an association to a threat through imprudence. Negligent insiders are ordinarily knowledgeable about security practices and IT procedures but decide to skip them, creating risk for the organizations. Examples include allowing individuals to “piggyback” via a safe entry point, mislaying or failing a mobile storage appliance, including sensitive data, and ignoring messages to install security patches and new updates.

Incidental – An insider of this kind wrongly causes an unintentional risk to an association. Associations may successfully perform to minimize accidents, but they will emerge; they may not be prevented entirely, but those that occur may be mitigated. Instances contain accidentally sending a sensitive business document to a

competitor, mistyping an email account, unknowingly or inadvertently clicking on a URL, opening a malicious attachment within a phishing email, or improperly disposing of sensitive documents.

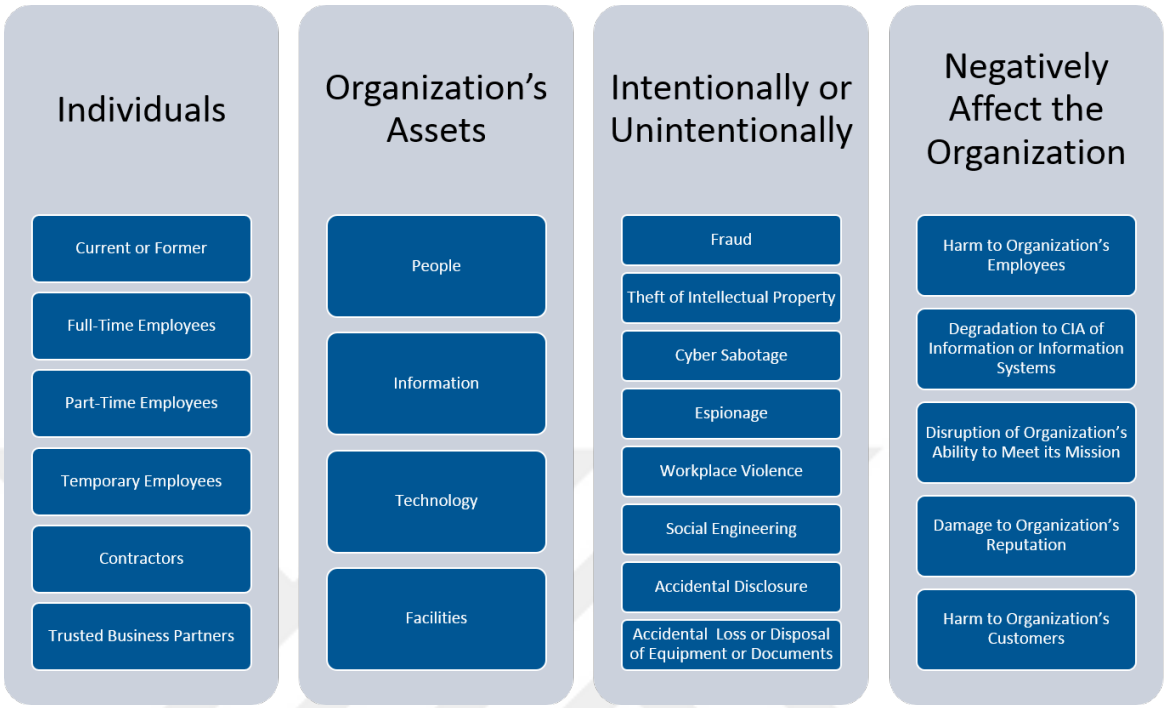

Figure 3 Insider Threat Scope Diagram

Insider threats manifest in many manners, such as espionage, sabotage, violence, theft, and cyber actions. Expressions of insider threat are defined in detail below.

Espionage is the undercover or criminal practice of spying on an organization, an alien government, entity, or individual to acquire private and confidential information for strategic, military, political, or economic benefit.

Government Espionage is confidential intelligence-collecting artefacts by one country against another to acquire a military or political benefit. It may have a country(s) spying on corporate entities such as consulting firms and aeronautics firms. Government espionage is referred to as intelligence gathering by authorities.

Financial Espionage is the hidden practice of acquiring trade information from a foreign country (e.g., procedures, processes, techniques, economic, technical, scientific, codes for manufacturing, all forms and types of financial, business, or engineering information and methods, programs).

Sabotage represents intentional actions to damage a company's infrastructure like noncompliance with maintenance or IT systems, contamination of clean areas, physically damaging facilities, or removing code to stop regular processes.

Theft is the basic action of stealing, whether money or intellectual property such as patents, copyright, industrial design rights, trademarks, plant variety rights, trade dress, geographical indications and, in some jurisdictions, trade secrets.

Financial Crime is the unauthorized taking or illegal use of an individual, enterprise', or institution's capital or property to profit from it.

Intellectual Property Theft would be stealing someone or a company's ideas, innovations, or creative expressions, including proprietary products and trade secrets, even if the stolen concepts or things originated from the stealer.

Cyber - Digital threat contains stealing, spying, brutality, and sabotage anything related to technology, computers, devices, or the internet.

Unintentional Threats are the non-malicious (often incidental or unintentional) disclosure of a company's IT infra and data that unintentionally damage the company. Examples include rogue software, phishing emails, malicious freeware and PUAs.

Intentional Threats are adversarial activities conducted by malicious insiders who utilise technology to interrupt or suspend an organization's routine business processes, determine IT deficiencies, acquire protected data, or further an attack technique via access to IT systems. This activity may implicate altering data or inserting malicious files, codes, or other elements of offensive software into systems and networks.

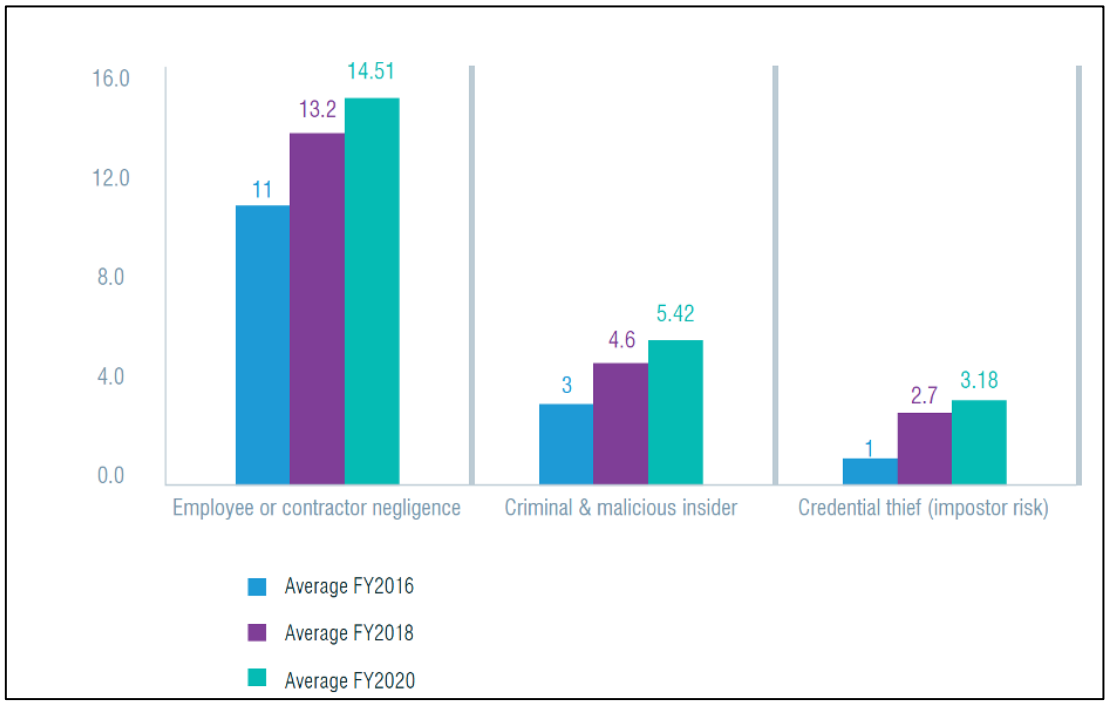

Figure 4 Frequency for three profiles of insider incidents (INSIDER THREATS GLOBAL REPORT)

To allow the identification of insiders and insider threats across organizational boundaries, an adequate taxonomy of insider threats is an essential foundation for further work by both researchers and practitioners. Taxonomies provide a means to order problems; in the situation considered here, such ordering is necessary to differentiate types of insiders and types of insider threats and make precise the key dimensions that serve as the basis of the differentiation. We may begin systematically creating prevention and response strategies by identifying the key sizes.

Negligibly, some formal approval of the dimensions of such a taxonomy is required; professionals may conflict about how the measurements are used (as in determining who an insider is), but by pushing an explicit debate of various interpretations, taxonomies may act as a vital role.

2.4.2 Internal Data Leakage Channels

2.4.2.1 Email. Traditional email clients, such as Microsoft Outlook, Lotus Notes, Eudora, etc., are omnipresent. An internal user with the motivation might email a confidential document to an unauthorized individual as an attachment. They may also decide to compress and/or encrypt the file or embed it within other files to disguise its presence. Steganography can also be utilized for this intent. Instead of attaching a document, the text might be copied into the email message body.

Email also represents a vector for unintentional exposure due to worker oversight or insufficient business procedure. An employee might attach the incorrect file inadvertently, select the wrong recipient in the email, or even be fooled into sending a file via social engineering.

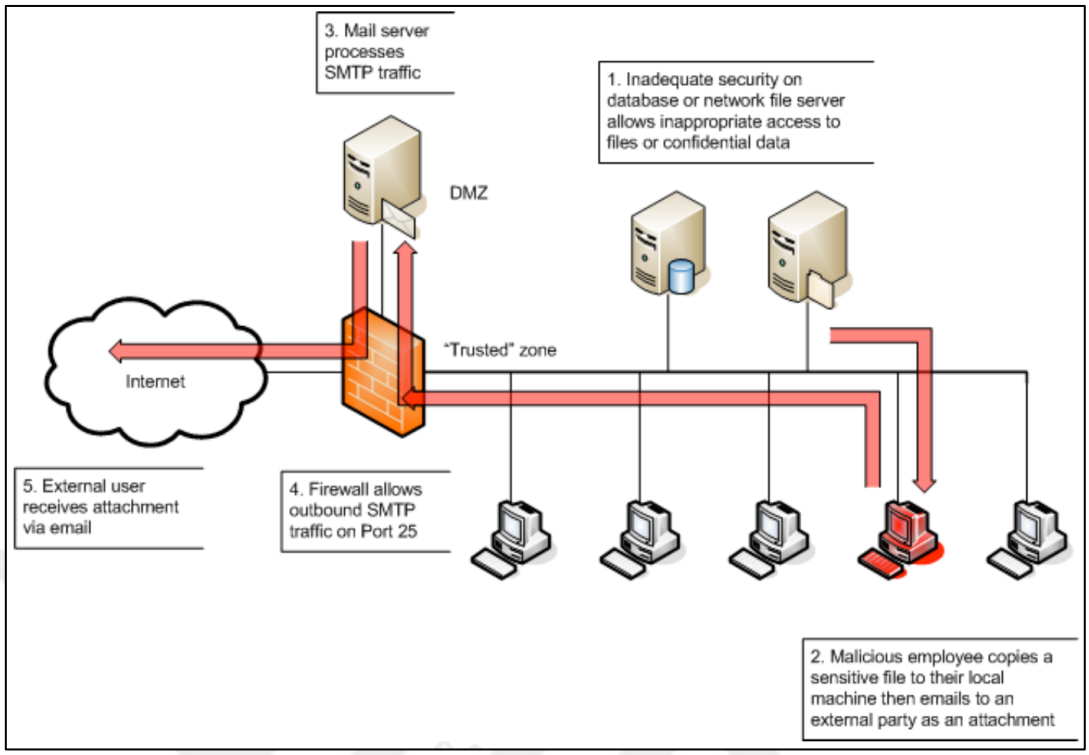

Figure 5 Illustration Email Data Leakage (Data Leakage – Threats and Mitigation Peter Gordon, 2007)

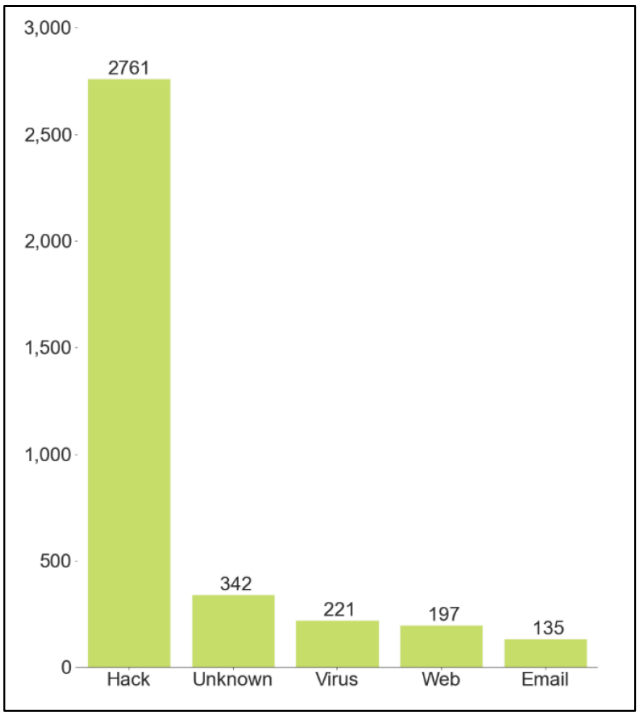

Figure 6 Number of breaches by breach type, reported by EOY 2021

(2021 Year End Report Data Breach QuickView, Flashpoint 2021)

2.4.2.2 Web Email. WebMail is well entrenched with users. Nowadays, Gmail, Yahoo, and Yandex are famous examples. It represents another way for someone to leak confidential information, either as an attachment or in the email's message body. Because WebMail runs over HTTP/S a firewall can accept it without inspection as port 80 or 443 will be allowed in most organizations, and the connection initiates from a private internal IP address. HTTPS(SSL) represents a more complex challenge due to the encryption of the traffic.

2.4.2.3 Instant Messaging, P2P Apps. Most companies do not have an adequately strict policy to block employees' usage of Instant Messaging and P2P apps. Today there are various applications which can be used for daily communications however these applications are coming with some additional features that companies needs to deal with it such as file transferring. Whatsapp, Telegram, Signal and numerous others are most common applications that have been using for last couple years. It would be a fundamental process for someone to send confidential information within the document (such as a Word file containing sensitive trade or financial information) to a third party. Equally, a user might disclose confidential data in an Instant Messaging chat session. In addition to that Peer-to-peer (P2P) also presents a considerable threat to information confidentiality. Popular P2P clients include qBittorrent, BitTorrent, Deluge, and uTorrent, appearing to have around 75% share of global P2P traffic.

2.4.2.4 Malicious Website. Websites that are either compromised or malicious present the risk of a user's computer being infected with malware simply by visiting a website, including a malicious script with an endpoint that contains a vulnerability. The malware could be in the form of a keylogger, Trojan, etc. With a keylogger, the risk of data theft is introduced.

2.4.2.5 VPN Anonymizer Services. In order to obfuscate data, a user may try to utilize a shared proxy service via an SSL connection. They access the proxy service via a browser or browser extension, type in the URL of the site they wish to visit, and their entire session is then encrypted or the extension will do that redirection automatically. Neither a Stateful Packet Inspection firewall nor next-generation

firewalls will not be able to examine the data as it will be encrypted. Therefore, sensitive data can be leaked via this method without being detected. For example, the private Proxy and VPN services, Tor or VPN browser extensions provide this capability.

2.4.2.6 Network File Transfer Protocol. First of all, as FTP is a popular protocol, it is likely to be permitted by the firewalls. It uses TCP-20 or TCP-21 FTP is presumably more likely to be used in intentional leakage than unintentional leakage since uploading a document to an FTP server that is outside of the network or organization is naturally not something average user do daily, nor would it do inadvertently, as compared to attaching the document to an email. Although the traffic is not encrypted, any adversary may sniff it and use it which poses risk for organizations.

2.4.2.7 Removable Devices. Symantec reported in March 2007 that "Theft or loss of a computer or data storage medium, such as a USB memory key, made up 54 percent of all identity theft-related data breaches" (Turner, D. et al. 2007)

2.4.2.8 DNS Tunneling. as companies ensure their networks and assets by enforcing Defense in Depth Strategies, adversarial actors still can find methods to bypass the controls. DNS is often ignored for security since no one thought DNS uses the protocol for data transmission.

Companies' internal DNS servers are usually dependent on DNS servers from their Service Providers or organizations that provide DNS services. If the DNS provider is not scanning their DNS servers for malicious domains, the malicious domain may be resolved using the company's DNS server. It is up to the organization to secure and monitor its DNS services. An adversary could tunnel any information in and out of the network without monitoring an organization's DNS services.

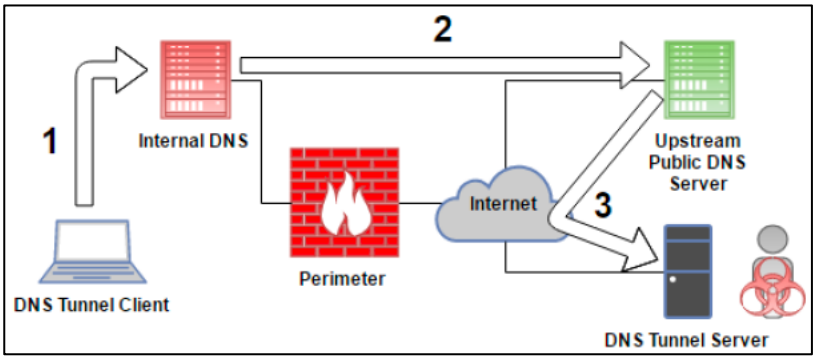

Figure 7 DNS Tunneling Flow (Jaworski S., 2016)

2.4.3 External Threats

2.4.3.1 SQL Injection. Web sites that use an SQL Server as the backend database can be vulnerable to SQL Injection attacks if they fail to parse user input rightly. This situation is usually a direct result of insufficient coding. SQL Injection attacks can result in content within the database being stolen. A site that does not accurately sanitize user input can cause a server error. The initial step of the attack might be to enter a single quote within the input data in a POST part on a website, which can cause an SQL statement.

A server error may occur should the application not sanitize the user input accurately. It indicates to the adversary that the user input is not being sanitized and that the website is vulnerable to exploitation. Further preparation and error by the adversary might ultimately show table names, field names, and other information that, once obtained, will permit adversaries to create a POST SQL query that yields confidential information.

2.4.3.2 Malware. After infecting a computer, malware would scan through the My Files folder and send a file at random out through email to the user's email contacts. Suppose malware is categorised as a zero-day threat and has no known signature. In this case, there is a higher probability that the malware will avoid next-generation endpoint security measures and desktop AV agents. Once this malware infects the endpoint, it can then start outbound traffic, potentially sending out files that may contain sensitive information. One part of being mindful is that the traffic is from an internal source to a firewall. It can be an essential point because most firewalls or perimeter security systems will not block the traffic initiated internally through an

acceptable protocol.

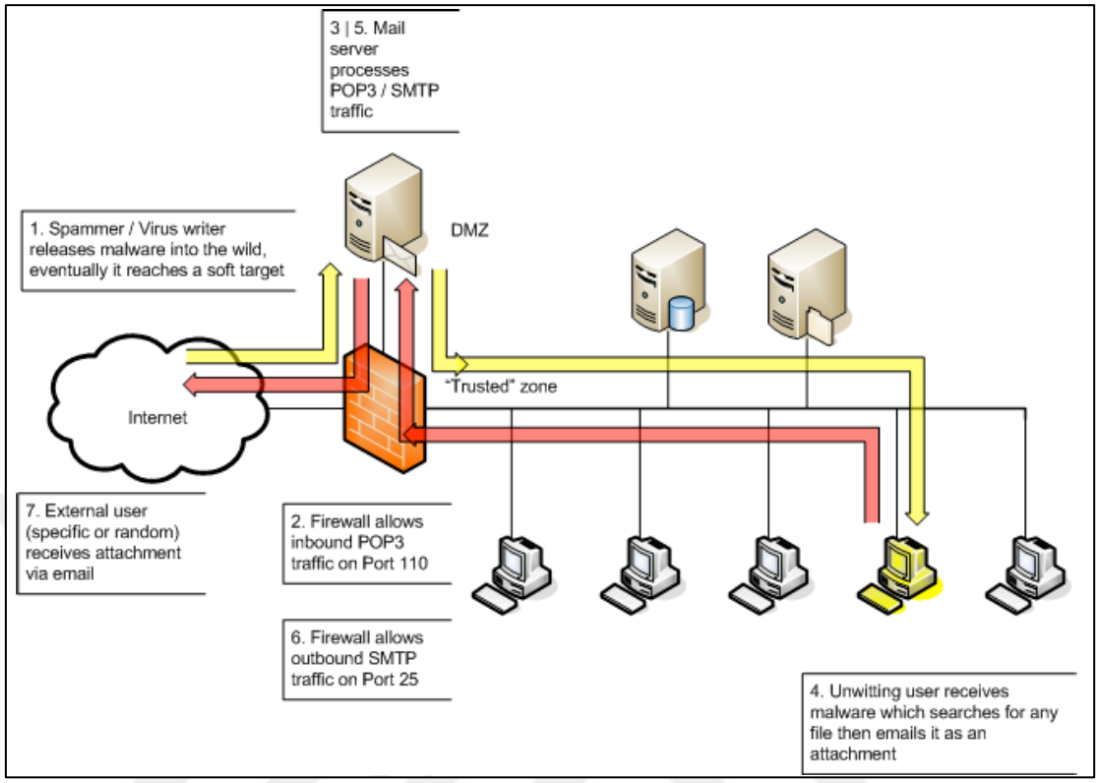

Figure 8 Illustration Malware Data Leakage Vector (Data Leakage – Threats and Mitigation Peter Gordon, 2007)

2.4.3.3 Dumpster Diving. Organizations that do not follow proper policy regarding the destruction of hard copy data bear the risk of confidential information falling into unauthorized persons. Rather than having such data destroyed in a secure way, enterprises may throw their data (perhaps unintentionally) into the rubbish. An adversary may choose to raid the company's dumpster and find this information. This extends to the information stored on media such as CDs and DVDs and printed material.

2.4.3.4 Phishing. Phishing websites and the spam email that summons visits pose a threat to organizations and not just people. Phishing email can be received at peoples' work email address. Should they be fooled into visiting the phishing site, they may lose personal information and or financial information. It is also possible that the spam received directs them to a site hosting malware, which could download a key logger. Phishing is, of course, a form of social engineering. (Gordon, P., 2007.)

Phishing deceives people into sharing confidential information such as passwords and credit card numbers. For example, a victim might receive an e-mail or text message that impersonates a different person or organization they trust, such as a friend, a company, or a government agency. When the victim opens the e-mail or the text message, they are directed to imitate a legitimate website. The victim feels safe login in with his username and password. In this way, access information is sent to thieves who use it to steal identities, steal bank accounts, and sell personal data on the black market.

Companies' internal emails may contain private customer data, making it challenging to categorise it as personal or business-related information. An acceptable information security policy that specifies each document's privacy concerns and secrecy levels must be implemented to mitigate this problem. To create this information security policy, companies can implement the recommendations of ISO/IEC 27001:2013—Information Security Management Systems (https://www.iso.org/standard/54534.html). (Avila, R., Khoury, R., Khoury, R., Petrillo F., 2021)

2.4.3.5 Network Sniffing. is a method by which the adversary may capture and analyse all the data, including sensitive data passing via given network traffic. Sniffers may be hardware or software installed in the system. This program captures packets that arrive at the computer's network interface and allows them to analyse. Sniffing is to gain legitimate access or steal data. Some network applications can transmit data in text form (HTTP, FTP, SMTP, POP3, etc.), and cybercriminals may find helpful and sometimes confidential information (for example, usernames and passwords). Intercepting usernames and passwords is dangerous because users often use the same username and password for various features and applications. (Guillen D., Morales-Rocha V., Martinez F., 2020)

2.4.3.6 Theft of Equipment. According to the Ponemon Institute, 63% of small and medium-sized enterprises suffered a data leakage in 2019. The main reason is the loss or theft of equipment when an adversary obtains a device, easing access to the internal network since the user's systems are already correctly configured. Most individuals do not understand that a naive action like using a pen drive may result in adversaries' corporate information theft. Theft or the loss of a corporate notebook

that is not encrypted, for instance, may compromise sensitive company data. (Ponemon Institute, 2020)

2.4.3.7 Cross-Site Scripting. (XSS) is an attack type in which an adversary exploits a vulnerability present in web applications to insert code (such as JavaScript) and obtain certain types of advantage over victims. It is usually used on pages familiar to all users, such as a website's homepage or even pages where users can leave their comments. For the attack to occur, the page must contain a form that allows the attacker to interact with the system, such as a search field or a field for entering comments. Cross-site scripting is an application layer attack method that injects malicious scripts into a web application to gather data from a different machine. (Johns M., 2011)

2.4.3.8 Session hijacking. is interchangeable with a stolen session. An adversary intecepts and takes over a legitimately established session between a user and a host. The user-host connection may apply to any authenticated resource, such as a web server or another TCP-based connection. Adversary stands between the user and the host, letting them monitor the user's traffic and launch specific attacks. Once a successful session hijacking occurs, the adversary may accept the legitimate user's position or scan the traffic to inject or gather specific packets to make the desired effect. In possession of the user's session, the attacker impersonates them and performs any action that falls within the user's privileges. (Johns M., 2011)

2.4.3.9 Brute Force. attack occurs when an adversary tries many passwords to find the victim's credentials and access her account or system. Different brute-force attacks exist, for example, credential stuffing and reverse brute force attacks. Bruteforce attacks are usually successful when weak or relatively predictable passwords are used. This attack aims to gain authorized access via discovered credentials since they use a weak username and password combination. Bruteforce attacks generally use a dictionary of common passwords and comprehensively try them. This user behaviour pattern facilitates techniques such as brute force and account hijacking.

Chapter3

DLP Technology, Framework And Implications

3.1 Technology

DLP technologies detect and prevent the unauthorized usage and transmission of confidential data in three phases.

- The data is being used (“in use”)
- The data is being transferred across a network (“in motion”)
- The data is stored for future usage (“at rest”)

These technologies protect confidential data by conducting three critical security procedures:

Inventorying sensitive information: Once a company has run through a data classification activity and determined its most sensitive information components, DLP solutions may support identifying all of the locations in the company where that data is stored, processed or transferred. The technology is exceptionally dependable in the financial area, where many sensitive information components pursue known and recognizable patterns. For instance, Social Security numbers can use a 10-digit pattern in the form XXX-XX-XXXX as well as Credit card numbers tend to use the same patterns and include a confirmation code that provides additional security.

Monitoring the flow of information: Determining the locations where sensitive data is held is only part of the technology. IT professionals must be confident about what they are doing regarding the flow of confidential data around the company. DLP technologies may support a business detect the pinpoints where sensitive data enter, logging its routes and noting where it exits the infrastructure. Using a DLP technology in monitoring mode can discover earlier unknown company processes that abuse sensitive data, provoking a thorough data security review.

Blocking data leaks — The most crucial reason that many financial companies prefer to implement a DLP solution is to prevent a data breach from happening at a vulnerable moment: since the information leaves the company environment. Furthermore, DLP solutions include the capability to interfere and stop a violation

from taking place to detect possible data breaches.

DLP solutions may be an essential tool in the arsenal of a business's security unit. They are developed to use other controls as a defence-in-depth information security procedure. When integrated with next-generation firewalls, encryption, intrusion detection and prevention systems (IDPS), and a security information and event management (SIEM) system, DLP technologies deliver a stable, managed environment to protect sensitive data.

DLP technologies fall into four categories developed to protect sensitive data while in use, in motion, and at rest. These enclose endpoint protection, network protection, storage protection and cloud protection.

3.1.1 Endpoint DLP systems. It resides at the endpoint level and consist of software agents installed on the end-user computer to monitor data while it is in use or stored on the host machine. These agents have privileged access to the OS (operating system) such as root, local admin or superuser to detect data stored on or transferred by the endpoint system. In various cases, this privileged access allows them to circumvent encryption mechanisms and detect even covert attempts to remove sensitive data.

3.1.2 Network-based DLP systems. These are connected to the network edge and monitor data traffic as it enters or exits the company's internal network. These solutions are often designed to merge with firewalls, email security gateways and other solutions to provide a secure border and prevent the unauthorized expatriation of sensitive information data.

3.1.3 Storage-based DLP systems. They provide reliable security for data at rest. These solutions present technical monitoring of network-attached storage (NAS) and storage area network (SAN) systems, determining sites that keep confidential data and notifying unauthorized use.

3.1.4 Cloud-based DLP systems. Cloud DLP systems protect companies that have assumed cloud storage by providing sensitive information that does not make its method into the cloud without being encrypted and sent to official known cloud systems. Many cloud DLP systems remediate or alter classified or sensitive

information before data is transmitted to the cloud environment to assure that the information is secure when in transit and cloud storage.

Key elements of having a cloud DLP system include:

- Combine with cloud storage providers to monitor servers, identify, and encrypt sensitive information before the data is shared in the cloud.
- Scanning stored data in the cloud and auditing it at any time.
- Accurately classified sensitive data in the cloud
- Constantly audit uploaded data.
- Automatically enforce controls (prompt, block, encrypt) to sensitive information following company guidelines.
- Alert appropriate admins and data owners when information is put at risk.
- Retain the visibility and control required to comply with privacy and data protection regulations.

3.2 DLP Framework

3.2.1 CIS Controls. The CIS Critical Security Controls started as a simple grassroots activity to identify the most common and essential real-world cyber-attacks that affect companies every day, translate that knowledge and experience into positive, constructive action for security professionals, and then share that information with a broader audience. The original objectives were modest—to support people and enterprises, concentrate their awareness and get started on the most important steps to defend themselves from the attacks that mattered. (CIS Controls V8, 2021)

Structure of CIS Controls:

- Overview. A brief description of the intent of the Control and its utility as a defensive action
- Why is this Control critical? A description of the importance of this Control in blocking, mitigating, or identifying attacks, and an explanation of how attackers actively exploit the absence of this Control
- Procedures and tools. A more technical description of the processes and technologies that enable implementation and automation of this Control
- Safeguard descriptions. A table of the specific actions that enterprises should take to implement the Control

Data is no longer only retained within the enterprise; it is in the cloud as well for user devices that work from home and is usually shared with partners or online services that could have it anywhere in the globe. Furthermore, there might also be numerous international regulations for personal data protection to sensitive information a company maintains related to finances, intellectual property, and customer information. Data privacy has become significantly important, and companies are experiencing that privacy is about the appropriate use and management of data, not just encryption. Data should be adequately managed through its entire life cycle. These privacy rules can be complicated for multi-national enterprises; nevertheless, some fundamentals may apply.

Once adversaries have infiltrated a company's infrastructure, their first aim is to find and exfiltrate data. Companies could not be aware that sensitive information is leaving their network since they are not monitoring data flows.

While many suspicious attempts happen in the environment, other adversaries involve physically stealing mobile end-user machines and attacks on service providers or other partners having sensitive information. Other sensitive company assets can have non-computing appliances that provide management and control of systems, for instance, Supervisory Control and Data Acquisition (SCADA) systems.

The company's loss of authority over sensitive information or security is a severe and often reportable business impact. When some information is lost or compromised due to stealing or espionage, most consequences are from inadequately comprehended information management practices and user error. Data encryption for adoption, both at rest and transit, may deliver excellent ease against information compromise, and, also much more significant, it is a regulation prerequisite for most regulated information.

Table 2 Safeguards (CIS Controls v8, 2021)

Number	Title/Description	Asset Type	Security Function
3.1	Establish and Maintain a Data Management Process	Data	Identify
3.2	Establish and Maintain a Data Inventory	Data	Identify
3.3	Configure Data Access Control Lists	Data	Protect
3.4	Enforce Data Retention	Data	Protect
3.5	Securely Dispose of Data	Data	Protect
3.6	Encrypt Data on End-User Devices	Devices	Protect
3.7	Establish and Maintain a Data Classification Scheme	Data	Identify
3.8	Document Data Flows	Data	Identify
3.9	Encrypt Data on Removable Media	Data	Protect
3.10	Encrypt Sensitive Data in Transit	Data	Protect
3.11	Encrypt Sensitive Data at Res	Data	Protect
3.12	Segment Data Processing and Storage Based on Sensitivity	Network	Protect
3.13	Deploy a Data Loss Prevention Solution	Data	Protect
3.14	Log Sensitive Data Access	Data	Detect

3.2.2 MITRE ATT&CK. Mitre ATT&CK Framework is a knowledge base that shows the techniques, tactics and procedures that show the actions that attackers may take to the system in the cyber world. Miter ATT&CK (Adversarial Tactics, Techniques and Common Knowledge), which Miter has developed since 2013. It is a worldwide accessible knowledge base of adversary tactics and techniques based on real-world statements. The ATT&CK knowledge base is used to develop specific threat models and methodologies in the government, private sector and the cybersecurity technology and service society. ATT&CK and MITRE fulfil their mission to unravel problems for a secure environment — by carrying communities together to produce more suitable cybersecurity. ATT&CK is open and known to any individual or institution for use at no charge. (https://attack.mitre.org/)

Data Loss Prevention (DLP) technologies may help determine malicious attempts to exfiltrate functional information, such as scientific plans, trade secrets, recipes, intellectual property, or telemetry. DLP functionality can be produced into other security technologies such as firewalls or standalone suites driving on the network and host-based agents. DLP can be configured to contain transmitted information through corporate sources.

The attacker is attempting to collect information of interest to their goal. The collection consists of methods attackers can use to collect data, and the sources of information are gathered that apply to following the attacker's goals. After collecting data, the next goal is to steal (exfiltrate) the data continuously. Common target sources include various drive types, browsers, audio, video, and email. Common collection methods include capturing screenshots and keyboard input. (https://attack.mitre.org)

The attacker is trying to steal data. Exfiltration includes techniques that attackers can use to steal information from the network. Once they have gathered information, attackers pack it to avoid being detected while removing it. It may have encryption and compression. Methods for acquiring information from a target network generally contain transmitting it over the command-and-control or alternate channels. It can furthermore have size limits on the transmission.

3.2.3 Zero Trust. Zero trust model approaches system design where innate trust in the network is dismissed. Instead, the network is considered adversarial, and each access request is verified based on an access policy. Trust in the reliability of a request is accomplished by building context, which relies upon solid authentication, authorization, machine health, and the value of the information being accessed.

The network can be assumed to be compromised and thus hostile, which means it is necessary to remove trust from the network. In a zero-trust model, ingrained trust is removed from the network. Just because being connected to a network does not mean it should be able to access into the network. Every request to access information or service should be authenticated and authorized against an access policy. If the connection not comply with the access policy, the connection is declined. It is common to see an adversary acquire laterally in breaches. Furthermore, it can be even possible since everything and everyone already on the network is authorized with access to the rest of the network. In a zero-trust model, the network is regaled

as confrontational, so every data or service access request is continually verified against an access policy. It will enhance the detection and monitoring of tries at lateral movement by an adversary, corresponding to a conventional garden, but zero trust will not remove the threat altogether.

Data loss prevention (DLP) needs discovery and classification. DLP does not provide security by default. Endpoint DLP generally permits data to stay unsecured when closing the egress of data off the device. Technologies like information rights management (IRM) and file encryption are not zero trust. Those technologies solely secure the initial transfer of information. A worker may encrypt a document and send the file to an external associate.

Nevertheless, once the associate has decrypted the document to consume it, the associate — not the worker or enterprise — has control of the data. Using these data security techs has contributed to a data breach and headline after headline after a data breach. What enterprises need to do is implement zero-trust data security principles. Zero Trust principles are:

- Device health - Trust that a device is compliant with configuration policies and is in a good state. For instance, the most recent patches have been installed.
- Policy Enforcement Point - Reconciles submissions from a user or a device to a service or information using the Policy Engine to decide if the submissions may be approved.
- Policy Engine - The element that takes signs and analyzes them with access policies to determine an access conclusion.
- Signal - A piece of data like machine health or location that can be used to trust an asset's reliability. There are many signals to determine whether to grant access to a resource.
- Configuration Policy - Guidelines that define design prospects for machines and services.
- Access Policy - The prerequisites for a permit request to be authorized and entrusted.

3.3 DLP Implications

3.3.1 Legal Liability. People and enterprises that are the targets for the organization's information stolen can select to sue the company because of the injuries. As well as the legal expenses concerned, if the court rules favour the prosecution, the company will be responsible for the damages. It can put the enterprise out of business.

3.3.2 Regulatory compliance. Institutions are going to require to fulfill the obedience prerequisites of Acts, relying on the drive. The broad-based prerequisites are to assure client privacy. It is crucial to be able to contain personal details such as social security information, addresses, credit card information, etc. From disclosing through data loss (including theft by the adversary) to jeopardizing identification theft and fraud. The Federal Trade Commission enforces this prerequisite in the United States and seeks organizations that fail to concede to the prerequisites. This has the unfairness and Deception regulations about managing and securing personal information, Protecting the Fair Credit Reporting Act, and the Children's Online Privacy Act.

The Gramm-Leach-Bliley Act35 implements the Financial Privacy Rule, the Safeguards Rule, and Pretexting. These regulations apply to financial institutions and protect customers' data that does business with these organizations. The FPR "mandates financial organizations to provide their customers privacy statements that define the financial institution's information collection and sharing procedures. Customers have the right to specify sharing their data". The Safeguards Rule "mandates financial organizations to have a security plan to manage the confidentiality and integrity of personal customer data." Pretexting protects the customer from organizations divulging customers' data under pretenses (such as impersonation or fraud).

The Dodd-Frank Act, signed into regulation in July 2010, enforces a wide-ranging set of financial reforms invented to respond to the recession gripping the government during the years leading up to its passage. The most important requirement of the act for financial services firms is that it eradicates a secure dock earlier afforded to many financial consultants and needs them to comply with Security and Exchange Commission (SEC) regulations.

The 1999 Gramm–Leach–Bliley Act (GLBA) mandates that financial companies embrace a set of security measures developed to provide the privacy of sensitive financial data.

The Gramm–Leach–Bliley Act Safeguards Rule mandates that firms:

- Implement administrative, technical and physical safeguards that ensure the security and confidentiality of customer records and information.
- Protect against any anticipated threats or hazards to the security or integrity of such records.
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.

DLP technology can offer the proactive prevention called for by GLBA and limit the chance of exposing sensitive data. (Data Loss Prevention and the Financial Firm)

Established in 1996, Health Insurance Portability and Accountability Act (HIPAA) sets privacy and security prerequisites for healthcare providers, health insurance programs and healthcare information clearinghouses. Although financial companies cannot provide this definition initially, the human resources departments within such companies can manage HIPAA-regulated data or have customers in the health care industry that provide data demanding HIPAA protections. DLP strategies may help protect this data from unauthorized exposure.

PCI DSS is a contractually imposed set of prerequisites that impact any association that processes, stores or transfers card information. Companies subject to PCI DSS can use DLP technology to prevent potential cardholder data security violations. Furthermore, DLP solutions can serve as a "neutralizing control" — an alternative security technique used when a PCI-regulated company cannot fulfill one or more PCI DSS prerequisites. As a neutralizing control, DLP needs explicit permission from the company's merchant bank.

The Sarbanes–Oxley Act (SOX) requires that publicly traded companies institute controls to assure the integrity of financial statements. It contains a commitment to safeguarding financial data from unauthorized actions. DLP technologies may be used in partial completion of this condition.

EU General Data Protection Regulation (GDPR) It defines *personal data* as "any information that relates to an identified or identifiable living individual" and stresses that "different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data." The EU framework also emphasizes that personal information that has been de-identified or encrypted but may be used to re-identify someone remains personal information and falls within the scope of the law.

Another significant impact that the GDPR will have is on the information about data breaches and data leaks. Under GDPR, breach notification will be mandatory and failure to inform the individuals and the supervisory authorities about any loss of data as fast as possible will result in fines for the organization or enterprise in question (European Commission, 2015).

3.3.3 Lost Productivity. An organization can lose sufficient time by employees following sensitive data leakage (or complete loss). Examples might include the loss of productivity by the need to manually re-enter information into a system following the intended deletion by a third party. As another option, if an organization has intellectual property robbed, time and effort will need to move into redesigning/redevelopment of the Intellectual Property. For example, suppose an enterprise with a secret chemical recipe has that recipe stolen by a contestant. In that case, they need to redevelop a superior product, or encounter the loss of competitive benefit in the market.

Also, the time of Security personnel reacting to the loss and deployment of future countermeasures must be considered.

3.3.4 Business Reputation. It is difficult to measure a broken business reputation as it is not directly quantitative. However, it may indeed result in a measurable drop in sales. Publicity about a data loss or leak, whether intended or not, assumably leads to a negative reaction to the organization's image.

Chapter 4

Design And Implementation

4.1 Splunk

Splunk is a software widely used by SOC teams for monitoring, searching, analyzing and visualizing the machine-generated data in real-time as a SIEM solution. It captures, indexes, and correlates the real-time data in a searchable container and creates graphs, alerts, dashboards, and visualizations. Splunk provides easy access to information over the whole organization for easy diagnostics and solutions to different business problems.

Splunk Monitoring software provides a bunch of benefits for an organization. Some of the benefits of utilizing Splunk are:

- Provides enhanced GUI and real-time visibility in a dashboard
- It eases troubleshooting and determining time by providing instant results.
- It is the best-suited software for root cause analysis.
- Generate graphs, alerts, and dashboards.
- Easily search and investigate specific results using Splunk.
- Troubleshoot any condition of failure for improved performance.
- Monitor any business metrics and make an informed decision.
- Incorporate Artificial Intelligence into the data procedure.
- Gather useful Operational Intelligence from the machine data
- Summarizing and gathering valuable data from various logs
- Accept any data type such as .csv, JSON, log formats, etc.
- Most effective search analysis and visualization abilities to empower users of all types.
- Create a central repository for searching Splunk data from different source types.

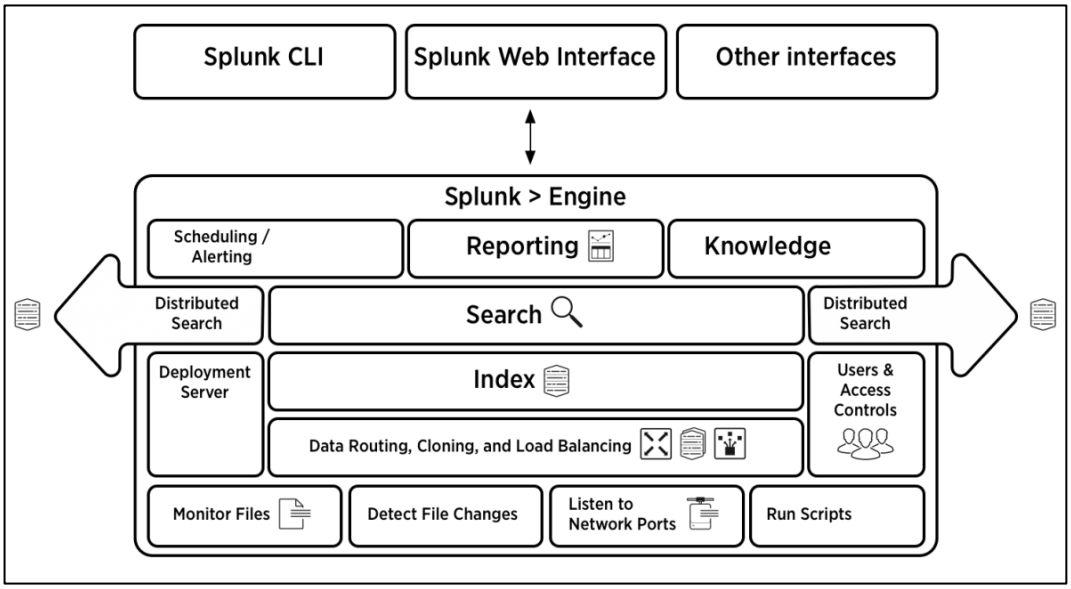

Figure 9 Splunk Architecture

Splunk consists of three different components. Forwarder, Indexer, and Search Head. Forwarder collects all the data from various remote machines and sources and then forwards data to the Index in real-time. Indexer process the incoming data in real-time. It also stores & Indexes the data on disk. End-users interact with Splunk through Search Head. It allows users to do search, analysis & Visualization.

SPL is the abbreviation for Search Processing Language. Splunk designs SPL for use with Splunk software. SPL encompasses all the search commands and their functions, arguments, and clauses. Its syntax was originally based on the Unix pipeline and SQL. The scope of SPL includes data searching, filtering, modification, manipulation, insertion, and deletion. For example, utilising a command to exclude avoided information, extract more data, evaluate new fields, estimate statistics, reorder the outcomes, or create a chart.

Some search queries have functions and statements related to them. Using these queries and the statements defines how the queries work on the results and which fields they work on. For example, it may format the information in a chart, represent what kind of stats to estimate, and prescribe what fields to assess. Some queries even use clauses to prescribe how to group the search results. (Splunk https://docs.splunk.com/)

The Incident Review dashboard shows notable events and their current status for SOC Analysts. Also, it is possible to filter notable events based on specific fields and accelerate the triage of notable events through an investigation workflow.

A notable event defines one or more bizarre incidents detected by a correlation search across data sources. For example, a notable event may represent:

- The repeated occurrence of an abnormal spike in network usage over some time
- A single occurrence of unauthorized access to a system
- A host communicating with a server on a known threat list

As a SOC analyst, use the dashboard to gain insight. Into the severity of the system or network events. Using the panel and dashboard to triage new notable alerts. Set events to SOC analysts for inspection and review notable alert details for investigative tips. Splunk Enterprise Security catches marks in the logs and automatically checks events for security-relevant incident alerts using correlation searches. When a correlation search catches a suspicious pattern of activity, the correlation search creates a new notable event. The Incident Review dashboard surfaces all notable alerts and categorizes them by possible severity to quickly triage, assign and track issues.

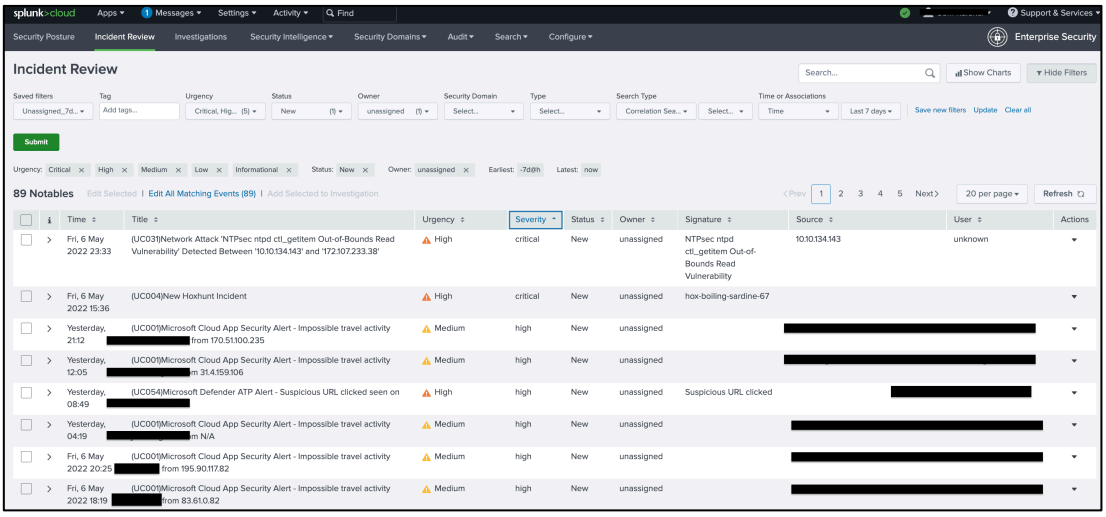

Figure 10 Incident Review Dashboard

4.2 Splunk DLP Usecases

Credentials In File Detected

Description: Detect known ceredential patterns inside data indexed in Splunk.

Security Impact: Attackers can dump credentials into local files using OS Credential Dumping, or credentials could have been left in files by mistake. Authenticated user credentials are usually kept in local configuration and credential files in cloud environments. This search aims to look for common credential patterns in log files in Splunk utilizing a list of regexes in a lookup file.

SPL:

```
index=* ((source IN("*.log","*.bak","*.txt","/tmp*","/temp*","c:\tmp*")) OR (tag=web dest_content=*))
| eval comment="Match against the regexes in the lookup"
| rex max_match=0
    [| inputlookup credential_patterns WHERE type="regex" AND include="1"
    | eval rexValue="(?<P_"+replace(description," ","_")+">"+value+")"
    | stats values(rexValue) AS regexMerge
    | eval regexMerge=mvjoin(regexMerge,"|")
    | eval search="\"(".regexMerge.")\""
    | fields search
        ]
| foreach P_*
    [| eval PatternStringMatch=if('<<FIELD>>'!="", mvappend(PatternStringMatch,'<<FIELD>>'),PatternStringMatch)
    | eval PatternStringDescription=if('<<FIELD>>'!="", mvappend(PatternStringDescription,"<<MATCHSTR>>"),PatternStringDescription)
        ]
| fields - P_*
| where isnotnull(PatternStringMatch)
| eval comment="Find the field that had the Pattern value"
| foreach *
    [| eval PatternStringField=if("<<FIELD>>"!="PatternStringMatch" AND like('<<FIELD>>',"%".PatternStringMatch."%"),"<<FIELD>>",PatternStringField)
        ]
| table _time PatternStringMatch PatternStringDescription PatternStringField source sourcetype host src dest http_user_agent
```

Figure 10 Credentials in File Detected Usecase SPL

How to Implement: This search is designed for known log file dump locations by default, but we could want to include or exclude specific locations before deploying. To get adequate coverage or exclude false positive matches, we may also add/modify/disable the regex patterns in the lookup file credential_patterns.csv. Please note that this search is very resource heavy and will run very slow. If we enable this search, we must keep the time window short or the schedule to be infrequent.

Known False Positive: This search could trigger a false positive if some of the credentials patterns match other strings that might exist in the files. If that is the case in the environment, we can modify the lookup to include or exclude certain patterns.

How to Respond: This alert triggers when clear text credentials are found within Splunk. It might signify a mistake or an adversary performing credential dumping actions. Recommended next steps will be to investigate why the credentials are in the file and how the file finished up in Splunk. The basic concept behind this search

is to take a set of known credential patterns from a lookup file (credential_patterns.csv) and dynamically build up a statement for the rex command. It is a little-known technique with SPL and has wide-ranging relevancy beyond this detection search. Another round of matching occurs to see which field we found the offending value in if a match is found. The last lines of the search make it straightforward to read for the analyst.

Hosts Receiving High Volume of Network Traffic From Email Server

Description: This search looks for increased data transfers from the email server to the clients. It could indicate adversary collecting data using the email server.

SPL:

```
| tstats `security_content_summariesonly` sum(All_Traffic.bytes_in) as bytes_in
from datamodel=Network_Traffic
where All_Traffic.dest_category=email_server by All_Traffic.src_ip _time span=1d
| `drop_dm_object_name("All_Traffic")`
| eventstats avg(bytes_in) as avg_bytes_in stdev(bytes_in) as stdev_bytes_in
| eventstats count as num_data_samples avg(eval(if(_time < relative_time(now(), "@d"), bytes_in, null)))
as per_source_avg_bytes_in stdev(eval(if(_time < relative_time(now(), "@d"), bytes_in, null)))
as per_source_stdev_bytes_in by src_ip
| eval minimum_data_samples = 4, deviation_threshold = 3
| where num_data_samples >= minimum_data_samples AND
bytes_in > (avg_bytes_in + (deviation_threshold * stdev_bytes_in)) AND
bytes_in > (per_source_avg_bytes_in + (deviation_threshold * per_source_stdev_bytes_in)) AND
_time >= relative_time(now(), "@d")
| eval num_standard_deviations_away_from_server_average = round(abs(bytes_in - avg_bytes_in) / stdev_bytes_in, 2),
num_standard_deviations_away_from_client_average = round(abs(bytes_in - per_source_avg_bytes_in) / per_source_stdev_bytes_in, 2)
| table src_ip, _time, bytes_in, avg_bytes_in, per_source_avg_bytes_in, num_standard_deviations_away_from_server_average,
    num_standard_deviations_away_from_client_average
| `hosts_receiving_high_volume_of_network_traffic_from_email_server_filter`
```

Figure 11 Hosts Receiving High Volume of Network Traffic From Email Server Usecase SPL

How to Implement: This search needs network traffic and populating the network traffic data model. Email servers must be classified as "emailserver" for the search to work. Change the deviation threshold and minimum datasamples values based on the network traffic in the domain. The "deviationthreshold" field is a multiplying factor to handle how much variation is expected to tolerate. The "minimum datasamples" field is the minimum number of connections of data samples needed for the statistic to be accurate.

Known False Positives: The false-positive rate will differ based on setting the

deviationthreshold and datasamples values. It is recommended to adjust these values based on the network traffic to and from the email servers.

Email Servers Sending High Volume Traffic To Hosts

Description: This search looks for increased data transfers from the email server to the clients. It might indicate a malicious actor collecting data using the email server.

SPL:

```
| tstats `security_content_summariesonly` sum(All_Traffic.bytes_out) as bytes_out
from datamodel=Network_Traffic
where All_Traffic.src_category=email_server by All_Traffic.dest_ip _time span=1d
| `drop_dm_object_name("All_Traffic")`
| eventstats avg(bytes_out) as avg_bytes_out stdev(bytes_out) as stdev_bytes_out
| eventstats count as num_data_samples avg(eval(if(_time < relative_time(now(), "@d"), bytes_out, null)))
as per_source_avg_bytes_out stdev(eval(if(_time < relative_time(now(), "@d"), bytes_out, null)))
as per_source_stdev_bytes_out by dest_ip
| eval minimum_data_samples = 4, deviation_threshold = 3
| where num_data_samples >= minimum_data_samples AND
bytes_out > (avg_bytes_out + (deviation_threshold * stdev_bytes_out)) AND
bytes_out > (per_source_avg_bytes_out + (deviation_threshold * per_source_stdev_bytes_out)) AND
_time >= relative_time(now(), "@d")
| eval num_standard_deviations_away_from_server_average = round(abs(bytes_out - avg_bytes_out) / stdev_bytes_out, 2),
num_standard_deviations_away_from_client_average = round(abs(bytes_out - per_source_avg_bytes_out) / per_source_stdev_bytes_out, 2)
| table dest_ip, _time, bytes_out, avg_bytes_out, per_source_avg_bytes_out, num_standard_deviations_away_from_server_average,
    num_standard_deviations_away_from_client_average
| `email_servers_sending_high_volume_traffic_to_hosts_filter`
```

Figure 12 Email Servers Sending High Volume Traffic To Hosts Usecase SPL

How to Implement: This search needs network traffic and populating the network traffic data model. Email servers must be classified as "emailserver" for the search to work. Change the deviation threshold and minimum datasamples values based on the network traffic in the domain. The "deviationthreshold" field is a multiplying factor to handle how much variation is expected to tolerate. The "minimum datasamples" field is the minimum number of connections of data samples needed for the statistic to be accurate.

Known False Positives: The false-positive rate will differ based on setting the deviationthreshold and datasamples values. It is recommended to adjust these values based on the network traffic to and from the email servers.

User with Increase in Outgoing Email

Description: To detect data exfiltration and compromised account, we can analyze users sending out dramatically more data than normal. This search looks per source email address for big increases in volume.

SPL:

```
| from datamodel:Email
| bucket _time span=1d
| stats count by Sender, _time
| eventstats max(_time) as maxtime
| stats count as num_data_samples max(eval(if(_time >= relative_time(maxtime, "-1d@d"), 'count',null))) as "count"
avg(eval(if(_time<relative_time(maxtime,"-1d@d"),'count',null))) as avg
stdev(eval(if(_time<relative_time(maxtime,"-1d@d"),'count',null))) as stdev by "Sender"
| eval lowerBound=(avg-stdev*2), upperBound=(avg+stdev*2)
| eval isOutlier=if(('count' < lowerBound OR 'count' > upperBound) AND num_data_samples >=7, 1, 0)
| table "Sender", num_data_samples, "count", avg, lowerBound, upperBound, isOutlier
```

Figure 13 User with Increase in Outgoing Email Usecase SPL

Known False Positive: It is a strictly behavioral search, so we define "false positive" slightly differently. Every time these fires, it will accurately reflect a spike in the number we monitor. It is nearly impossible for the math to lie. Nevertheless, while there are no "false positives" in a traditional sense, there is much noise.

How we handle these alerts depends on where we set the standard deviation. If we set a low standard deviation (2 or 3), we are likely to get many useful events only for contextual information. If we set a high standard deviation (6 or 10), the noise can be reduced enough to send an alert directly to analysts.

How to Respond: When this query returns results, initiate the incident response process and capture the time of the event, the sender, recipient, subject or the mail and attachments, if any. Contact the sender if it is authorized behaviour, a document that this is authorized and by whom. If not, another party may use the user credentials, and additional investigation is warranted.

High Volume Email Activity to Non-corporate Domains by User

Description**:** Detect when there is high volume email activity by a user to non-corporate domains.

SPL:

```
| tstats `summariesonly` sum(All_Email.size) as bytes, values(All_Email.recipient) as recipient
from datamodel=Email.All_Email
where NOT `cim_corporate_email_domain_search("All_Email.recipient")` by All_Email.src_user, All_Email.src_user_bunit
| rename "All_Email.*" as *
| apply app:email_activity_to_non_corporate_by_user_1h upper_threshold=0.1
| search "IsOutlier(bytes)"=1
```

Figure 14 High Volume Email Activity to Non-corporate Domains by User Usecase

Known False Positive: Some users within the company might need to send emails outside of the organization as part of their role.

How to Respond: When this query returns results, start the incident response method and grab the time of the event, the sender, recipient, the mail or subject and attachments. Get the sender if it is accepted behaviour, data that this is authorized and by whom. Question the user regarding the activity.

Detect Outbound SMB Traffic

Description: Detect outbound SMB connections made by hosts within the network to the Internet. One of the techniques often used by adversaries involves retrieving the credential hash using an SMB request made to a compromised server controlled by the threat actor. Also, it might be an indicator for data exfiltration via SMB.

SPL:

```
| tstats `security_content_summariesonly`
earliest(_time) as start_time latest(_time) as end_time
values(All_Traffic.action) as action
values(All_Traffic.app) as app
values(All_Traffic.dest_ip) as dest_ip
values(All_Traffic.dest_port) as dest_port
values(sourcetype) as sourcetype count
from datamodel=Network_Traffic
where ((All_Traffic.dest_port=139 OR All_Traffic.dest_port=445 OR All_Traffic.app="smb") AND
  NOT (All_Traffic.action="blocked"
  OR All_Traffic.dest_category="internal"
  OR All_Traffic.dest_ip=10.0.0.0/8
  OR All_Traffic.dest_ip=172.16.0.0/12
  OR All_Traffic.dest_ip=192.168.0.0/16
  OR All_Traffic.dest_ip=100.64.0.0/10)) by All_Traffic.src_ip
```

Figure 15 Detect Outbound SMB Traffic Usecase SPL

Known False Positive: The outbound Server Message Block (SMB) traffic is likely legitimate if the organization's internal networks are not well-defined in the Assets and Identity Framework. Categorize the internal CIDR blocks in the lookup file to avoid creating notable events for traffic destined to those CIDR blocks. Any other network connection going out to the Internet must be investigated and blocked. Best practices recommend preventing external traffic of all SMB versions and related protocols at the network perimeter.

Detect SMB Traffic Spike

Description: Detecting spikes in the number of Server Message Block (SMB) traffic connections.

SPL:

```
| tstats `security_content_summariesonly` count
from datamodel=Network_Traffic
where All_Traffic.dest_port=139 OR
All_Traffic.dest_port=445 OR
All_Traffic.app=smb
by _time span=1h, All_Traffic.src
| eventstats max(_time) as maxtime
| stats count as num_data_samples max(eval(if(_time >= relative_time(maxtime, "-70m@m"), count, null))) as count
avg(eval(if(_time<relative_time(maxtime, "-70m@m"), count, null))) as avg
stdev(eval(if(_time<relative_time(maxtime, "-70m@m"), count, null))) as stdev by src
| eval upperBound=(avg+stdev*2), isOutlier=if(count > upperBound AND num_data_samples >=50, 1, 0)
| where isOutlier=1
| table src count
```

Figure 16 Detect Outbound SMB Traffic Usecase SPL

Known False Positives: A file server can experience high-demand loads that might cause this analytic to trigger.

Detect TOR Traffic

Description: This rule aims to detect the network traffic identified as The Onion Router (TOR), a benign anonymity network that may be abused for various purposes such as data exfiltration.

Security Impact: Any results from this search might be an indicator of compromised.
SPL:

```
| tstats summariesonly=t
    count,
    min(_time) as earliest,
    max(_time) as latest,
    sum(All_Traffic.bytes_in) as bytes_in,
    sum(All_Traffic.bytes_out) as bytes_out,
    values(All_Traffic.dvc) as firewall_names,
    values(All_Traffic.rule) as firewall_rules,
    values(All_Traffic.user) as users,
    values(All_Traffic.app) as firewall_app,
    values(All_Traffic.vendor_product) as firewall_product
    from datamodel=Network_Traffic
    where All_Traffic.protocol=tcp AND
          (All_Traffic.dest_port=9001 OR
          All_Traffic.dest_port=9030 OR
          All_Traffic.app="tor" AND
          (All_Traffic.src_ip="10.0.0.0/8" OR All_Traffic.src_ip="172.16.0.0/12" OR All_Traffic.src_ip="192.168.0.0/16" )
          NOT (All_Traffic.dest_ip="10.0.0.0/8" OR All_Traffic.dest_ip="172.16.0.0/12" OR All_Traffic.dest_ip="192.168.0.0/16" ))
    by All_Traffic.dest_ip, All_Traffic.dest_port, All_Traffic.src_ip, All_Traffic.action
| where count>1
| rename "All_Traffic.*" as *
| eval first_time = strftime(earliest, "%Y-%m-%d %H:%M:%S"), last_time = strftime(latest, "%Y-%m-%d %H:%M:%S")
| rename action as firewall_action
| table src_ip, dest_*, count, first_time, last_time, bytes_in, bytes_out, firewall_*, users _time
| lookup ip_intel ip as dest_ip OUTPUT description as threat_description, threat_key, weight
| rename clienthost as desthost
| lookup dnslookup clientip as dest_ip OUTPUT clienthost as dest_dns
| lookup whitelist_lookup domain AS dest_dns OUTPUTNEW domain AS isWhitelisted
| where isNull(isWhitelisted)
| fillnull dest_dns value="null"
```

Figure 17 Detect TOR Traffic Usecase SPL

Known False Positive: None

Detect Large Outbound ICMP Packets

Description: This search is created to detect outbound ICMP packets with a packet size larger than 1,000 bytes. Various adversaries have used ICMP as a command-and-control channel for the attack infrastructure. Large ICMP packets can indicate data exfiltration activity from an endpoint to a remote host.

SPL:

```
| tstats `security_content_summariesonly` count earliest(_time) as firstTime latest(_time) as lastTime
values(All_Traffic.action) values(All_Traffic.bytes)
from datamodel=Network_Traffic
where All_Traffic.action !=blocked All_Traffic.dest_category !=internal (All_Traffic.protocol=icmp OR
All_Traffic.transport=icmp) All_Traffic.bytes > 1000 by All_Traffic.src_ip All_Traffic.dest_ip
| search ( dest_ip!=10.0.0.0/8 AND dest_ip!=172.16.0.0/12 AND dest_ip!=192.168.0.0/16)
```

Figure 18 Detect Large Outbound ICMP Packets Usecase SPL

Known False Positives: ICMP packets are used to help troubleshoot networking issues and assure the proper flow of traffic. As such, a large ICMP packet can be legitimate. If large ICMP packets are associated with command-and-control traffic,

there will typically be a large number of these packets monitored over time. If the search provides many false positives, we can add specific IP addresses to an allow list.

DNS Query Length with High Standard Deviation

Description: Identify DNS requests and compute the standard deviation on the length of the names being resolved, then filter on two times the standard deviation to show those unusually large queries for the environment.

SPL:

```
| tstats `security_content_summariesonly` count
from datamodel=Network_Resolution
where NOT DNS.message_type IN("Pointer","PTR") by DNS.query
| `drop_dm_object_name("DNS")`
| eval tlds=split(query,".")
| eval tld=mvindex(tlds,-1)
| eval tld_len=len(tld)
| search tld_len<=24
| eval query_length = len(query)
| table query query_length record_type count
| eventstats stdev(query_length) AS stdev avg(query_length) AS avg p50(query_length) AS p50
| where query_length>(avg+stdev*2)
| eval z_score=(query_length-avg)/stdev
```

Figure 19 DNS Query Length with High Standard Deviation Usecase SPL

Known False Positives: There might be long domain names that are legitimate.

Detect Credit Card Numbers using Luhn Algorithm

Description: Detect if any log file in Splunk contains Credit Card numbers.

SPL:

```
index=* ((source IN("*.log","*.bak","*.txt", "*.csv","/tmp*","/temp*","c:\tmp*")) OR (tag=web dest_content=*))
| eval comment="Match against the simple CC regex to narrow down the events in the lookup"
| rex max_match=1 "[\"\s\'\,]{0,1}(?<CCMatch>[\d.\-\s]{11,24})[\"\s\'\,]{0,1}"
| where isnotnull(CCMatch)
| eval comment="Apply the LUHN algorithm to see if the CC number extracted is valid"
| eval cc=tonumber(replace(CCMatch,"[ -\.]",""))
| eval comment="Lower min to 11 to find additional CCs which may pick up POSIX timestamps as well."
| where len(cc)>=14 AND len(cc)<=16
| eval cc=printf("%024d", cc)
| eval ccd=split(cc,"")
| foreach 23 22 21 20 19 18 17 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 0
    [| eval ccd_reverse=mvappend(ccd_reverse,mvindex(ccd,<<FIELD>>))
        ]
| rename ccd_reverse AS ccd
| eval cce=mvappend(mvindex(ccd,0),mvindex(ccd,2),mvindex(ccd,4),
mvindex(ccd,6),mvindex(ccd,8),mvindex(ccd,10),mvindex(ccd,12),
mvindex(ccd,14),mvindex(ccd,16),mvindex(ccd,18),mvindex(ccd,20),
mvindex(ccd,22),mvindex(ccd,24))
| eval cco=mvappend(mvindex(ccd,1),mvindex(ccd,3),mvindex(ccd,5),
mvindex(ccd,7),mvindex(ccd,9),
mvindex(ccd,11),mvindex(ccd,13),mvindex(ccd,15),mvindex(ccd,17),
mvindex(ccd,19),mvindex(ccd,21),mvindex(ccd,23))
| eval cco2=mvmap(cco,cco*2)
| eval cco2HT10=mvfilter(cco2>9)
| eval cco2LT10=mvfilter(cco2<=9)
| eval cco2LH10dt=mvmap(cco2HT10,cco2HT10-9)
| fillnull value=0 cco2LT10 cco2LH10dt
| eventstats sum(cce) as t1 sum(cco2LT10) as t2 sum(cco2LH10dt) as t3 BY cc
| eval totalChecker=t1+t2+t3
| eval CCIsValid=if((totalChecker%10)=0,"true","false")
| fields - cc ccd cce cco cco2 cco2HT10 cco2LT10 cco2LH10dt t1 t2 t3 totalChecker raw time
| where CCIsValid="true"
| eval comment="Find the field where we found the CC number"
| foreach _raw *
    [| eval CCStringField=if("<<FIELD>>"!="CCMatch" AND like('<<FIELD>>',"%".CCMatch."%"),"<<FIELD>>",CCStringField)
        ]
| table _time CCMatch CCStringField source sourcetype host src dest http_user_agent
```

Figure 20 Detect Credit Card Numbers using Luhn Algorithm Usecase SPL

Security Impact: It is fairly common for enterprises to get fined for disclosing Credit Card data. One typical mistake is accidentally having debug logs enabled for an application in production, which could dump PII and Credit Card information into different log files. The fines for a breach like that might be massive, and we should have security mechanisms in place to contain it from happening, and further, we should have monitoring in place to detect it if it does happen. This detection may be run on a daily or weekly schedule and should include locations and files where we could find Credit Card being present. In addition to developer errors, an adversary might stage Credit Card and PII information in a location before being exfiltrated.

Known False Positives: The false-positive rate should be low, although a number series may appear in a log file that happens to be a valid CC number.

How to Respond: Immediately find the offending log file and investigate how the Credit Card numbers got written there. It might be an application or an attacker that have placed the numbers in the file.

Gsuite Drive Share in External Email

Description: Detect suspicious google drive or google docs files shared outside or externally. This behaviour could be a good hunting query to monitor the exfiltration of information made by an attacker or insider to a targetted machine.

SPL:

```
sourcetype=gsuite:drive:json NOT (email IN("", "null"))
| rex field=parameters.owner "[^@]+@(?<src_domain>[^@]+)"
| rex field=email "[^@]+@(?<dest_domain>[^@]+)"
| where src_domain = "internal_test_email.com" AND NOT dest_domain = "internal_test_email.com"
| eval phase="plan"
| eval severity="low"
| stats values(parameters.doc_title) as doc_title, values(parameters.doc_type) as doc_types,
        values(email) as dst_email_list, values(parameters.visibility) as visibility,
        values(parameters.doc_id) as doc_id, count min(_time) as firstTime max(_time) as lastTime
        by parameters.owner ip_address phase severity
| rename parameters.owner as user ip_address as src_ip
```

Figure 21 Gsuite Drive Share in External Email Usecase SPL

Known False Positives: Network admin or normal user may share files to customer and external team.

DNS Exfiltration Using Nslookup App

Description: Detect potential DNS exfiltration using nslookup application. This technique is seen in a couple of malware and APT groups to exfiltrate collected data in an infected machine or infected network. This detection is looking for the unique use of nslookup. It tries to use specific record types, TXT, A, and AAAA, generally used by adversaries and the retry parameter designed to query C2 DNS multiple tries.

SPL:

```
| tstats `security_content_summariesonly`
values(Processes.process) as process
values(Processes.process_id) as process_id
values(Processes.parent_process) as parent_process count
min(_time) as firstTime max(_time) as lastTime
from datamodel=Endpoint.Processes
where Processes.process_name = "nslookup.exe" Processes.process = "*-querytype=*" OR
Processes.process="*-qt=*" OR
Processes.process="*-q=*" OR
Processes.process="-type=*" OR
Processes.process="*-retry=*" by Processes.dest Processes.user Processes.process_name
```

Figure 22 DNS Exfiltration Using Nslookup App Usecase SPL

Known False Positives: admin nslookup usage

Excessive Usage of Nslookup App

Description: Detect potential DNS exfiltration using nslookup application. This technique is seen in a couple of malware and APT group to exfiltrate collected data in an infected machine or infected network. This detection is looking for the unique use of nslookup. It tries to use specific record types (TXT, A, AAAA) commonly used by adversaries, and the retry parameter is designed to query C2 DNS multiple tries.

SPL:

```
sourcetype=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational OR
source=XmlWinEventLog:Microsoft-Windows-Sysmon/Operational EventCode = 1 process_name = "nslookup.exe"
| bucket _time span=15m
| stats count as numNsLookup by Computer, _time
| eventstats avg(numNsLookup) as avgNsLookup, stdev(numNsLookup) as stdNsLookup, count as numSlots by Computer
| eval upperThreshold=(avgNsLookup + stdNsLookup *3)
| eval isOutlier=if(avgNsLookup > 20 and avgNsLookup >= upperThreshold, 1, 0)
| search isOutlier=1
```

Figure 23 Excessive Usage of Nslookup App Usecase SPL

Known False Positives: Unknown

Sources Sending a High Volume of DNS Traffic

Description: A common data exfiltration method is sending out a huge volume (in bytes) of DNS or ping requests, embedding data into the payload. It is usually not logged.

Security Impact: DNS Exfiltration is an advanced but increasingly common technique used by adversaries inside a network to exfiltrate data. The method is becoming famous due to organizations' increased monitoring of data exfiltration, specifying their monitoring to common protocols yet failing to monitor DNS as an exfiltration vector. There are several techniques to exfiltrate data via DNS. Nevertheless, one way to monitor activity is to measure the total bytes transferred and look for abnormalities and deviations from normal traffic levels.

SPL:

```
| from datamodel:Network_Traffic
| bucket _time span=1h
| stats sum(bytes*) as bytes* by src_ip _time
| eventstats max(_time) as maxtime avg(bytes_out) as avg_bytes_out stdev(bytes_out) as stdev_bytes_out
| eventstats count as num_data_samples avg(eval(if(_time < relative_time(maxtime, "@h"),bytes_out,null))) as per_source_avg_bytes_out
stdev(eval(if(_time < relative_time(maxtime, "@h"),bytes_out,null))) as per_source_stdev_bytes_out by src_ip
| where num_data_samples >=4 AND bytes_out > avg_bytes_out + 3 * stdev_bytes_out AND
bytes_out > per_source_avg_bytes_out + 3 * per_source_stdev_bytes_out AND
_time >= relative_time(maxtime, "@h")
| eval num_standard_deviations_away_from_org_average = round(abs(bytes_out - avg_bytes_out) / stdev_bytes_out,2),
num_standard_deviations_away_from_per_source_average = round(abs(bytes_out - per_source_avg_bytes_out) / per_source_stdev_bytes_out,2)
| fields - maxtime per_source* avg* stdev*
```

Figure 24 Sources Sending a High Volume of DNS Traffic Usecase SPL

Known False Positives: False positives for this rule should be infrequent for hosts with static IPs. A curiously configured free-standing IOT webcam was the only host that hit and was easy to filter out in one testing environment. If we have a small number of DHCP hosts that routinely send a large volume of DNS (first off, why?), we may need to filter out those destinations to reduce noise.

How to Respond: Initiate your incident response process and identify the other systems the alerting system is communicating. Capture the time, applications, destination systems, ports, byte count and other appropriate information. Contact the system admin of this action. If systems being communicated to are internal, contact the owner(s) of those systems. If authorized, make a note that this is authorized and by whom. If not, additional investigation is warranted to determine if DNS is used as a covert channel to exfiltrate data.

O365 Suspicious Admin Email Forwarding

Description: Detects when an admin configured a forwarding rule for multiple mailboxes to the same destination.

SPL:

```
sourcetype=o365:management:activity Operation=Set-Mailbox
| spath input=Parameters
| rename Identity AS src_user
| search ForwardingAddress=*
| stats dc(src_user) AS count_src_user
earliest(_time) as firstTime
latest(_time) as lastTime
values(src_user) AS src_user
values(user) AS user by ForwardingAddress
| where count_src_user > 1
```

Figure 25 O365 Suspicious Admin Email Forwarding Usecase SPL

Known False Positives: Uknown

Many USB File Copies for User

Description: Create a baseline of how many file copies each user does to USB media, and detect when the user copies an uncharacteristically large number of files.

Security Impact: Data exfiltration is top of mind for most security organizations. Copying data to USB is a top means for exfiltrating large and small volumes of data, so detecting that type of activity is key.

SPL:

```
index=* source="*WinEventLog:Security"
EventCode=4663 Object_Name=*
(Accesses="WriteData *" OR Accesses="AppendData *")
| regex Object_Name!="^.Device.HarddiskVolume\d*.\s*$"
| bucket _time span=1d
| stats count by user _time
```

Figure 26 Many USB File Copies for User Usecase SPL

Known False Positves: It is a strictly behavioural search, so we slightly define "false positive" differently. Every time this fires, it will reflect a spike accurately in the number we are monitoring... it is nearly impossible for the math to lie. Nevertheless, while there are no "false positives" in a traditional sense, there is the opportunity for lots of noise.

Increase in Pages Printed

Description: Find users who printed more pages than normal.

Security Impact: It can seem inefficient and old-fashioned, but employees who suddenly start printing many more pages from networked printers than is “normal” might signify data exfiltration. Sensitive information might be leaving your company. It is quite interesting to correlate this activity to a watchlist which can contain the user IDs of personnel that are considered higher risk: contractors, new employees, employees that never go on vacation, and employees with access to especially sensitive information.

SPL:

```
| inputlookup uniflow_printer_log_sample.csv
| bucket _time span=1d
| stats sum(Page_Count) as Pages by User _time
```

Figure 27 Increase in Pages Printed Usecase SPL

Known False Positives: It might be legitimate activity such as bunch of print required due to business need.

How to Respond: Initiate the incident response process and validate the user account running these print jobs. Determine which printer and what files are being printed and the time frame during which the printing occurred. Contact the user to determine if it is an authorized document. If not, the user credentials can have been used by another party and further investigation is warranted as excessive page prints could be a way to exfiltrate sensitive data.

4.3 Microsoft Defender for Cloud Apps

Companies have health records, credit card numbers, sensitive financial data, social security numbers or proprietary information. Decrease risk and to protect this sensitive information so they need a way to stop their people from inappropriately sharing it with people who should not have it. This exercise is stated as data loss prevention (DLP).

DLP catches sensitive things using deep content analysis, not just a straightforward text scan. The content is examined for primary data matches to keywords by estimating regular expressions, internal function validation, and secondary information matches close to the primary information match. Furthermore, DLP uses machine learning algorithms and other ways to detect content that matches the DLP policies.

We may apply DLP to data at rest, data in use, and data in motion in locations, such as:

- Exchange Online email
- SharePoint Online sites
- OneDrive accounts
- Teams chat and channel messages
- Microsoft Cloud App Security
- Windows 10, Windows 11, and macOS (Catalina 10.15 and higher) devices
- On-premises repositories
- PowerBI sites

Microsoft Defender for Cloud Apps is a Cloud Access Security Broker (CASB) that supports various deployment modes, including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyber threats across your Microsoft and third-party cloud services. (Microsoft)

Cloud Access Security Broker acts as a doorkeeper to broker access in real-time between the company users and cloud resources they use, wherever the users are located and regardless of their device. Cloud Access Security Brokers can do this by discovering and providing visibility into Shadow IT and app use, monitoring user actions for abnormal behaviours, containing access to your resources, and delivering the ability to organise and prevent sensitive data leaks, protecting against adversaries evaluating the compliance of cloud services. (Microsoft)

4.3.1 Data Loss Prevention Policies. Microsoft Data Loss Prevention (DLP) may take defensive actions to prevent the unintended sharing of sensitive information. When an action is taken on a sensitive item, we may be notified by configuring signals for DLP.
These are the policies that can be defined

- EU Social Security Number (SSN) or Equivalent ID
- EU National Identification Number
- EU Passport Number
- EU Debit Card Number
- Credit Card Number
- Unusual external user file activity
- Unusual volume of file deletion
- Creation of forwarding/redirect rule(Email)
- Mass download(Potential insider threat-potential leaver)

4.4 Azure Information Protection

Azure Information Protection (AIP) is a cloud-based technology that allows enterprises to discover, categorise, and protect data such as documents and emails by

using labels to content. AIP is part of the Microsoft Information Protection (MIP) solution and boosts the labelling and classification functionality delivered by Microsoft 365.

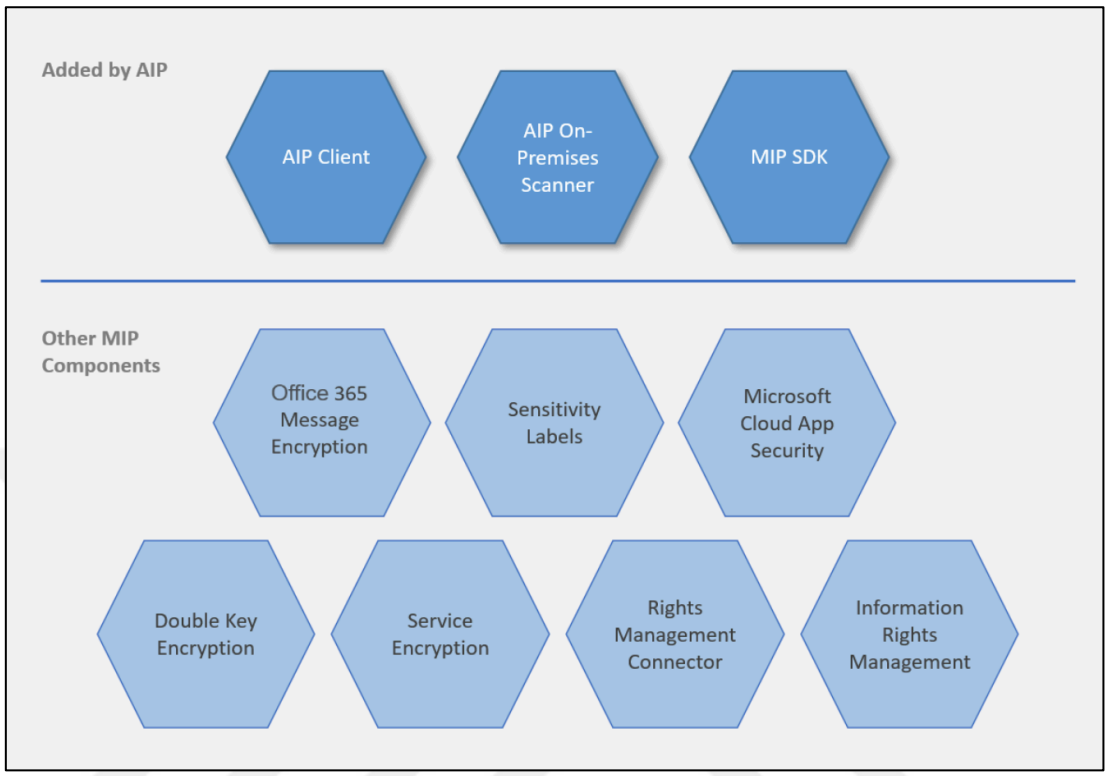

Figure 28 Azure Information Protection (AIP) Components

The Azure Information Protection on-premises scanner allows admins to scan their on-premises file storage for sensitive data that must be marked, categorised, and protected. The on-premises scanner is established using PowerShell cmdlets provided as part of the unified labelling client and may be managed using PowerShell and the Azure Information Protection site in the Azure portal.

For instance, utilise the scanner data displayed on the Azure portal to find repositories on your network that might have sensitive content at risk:

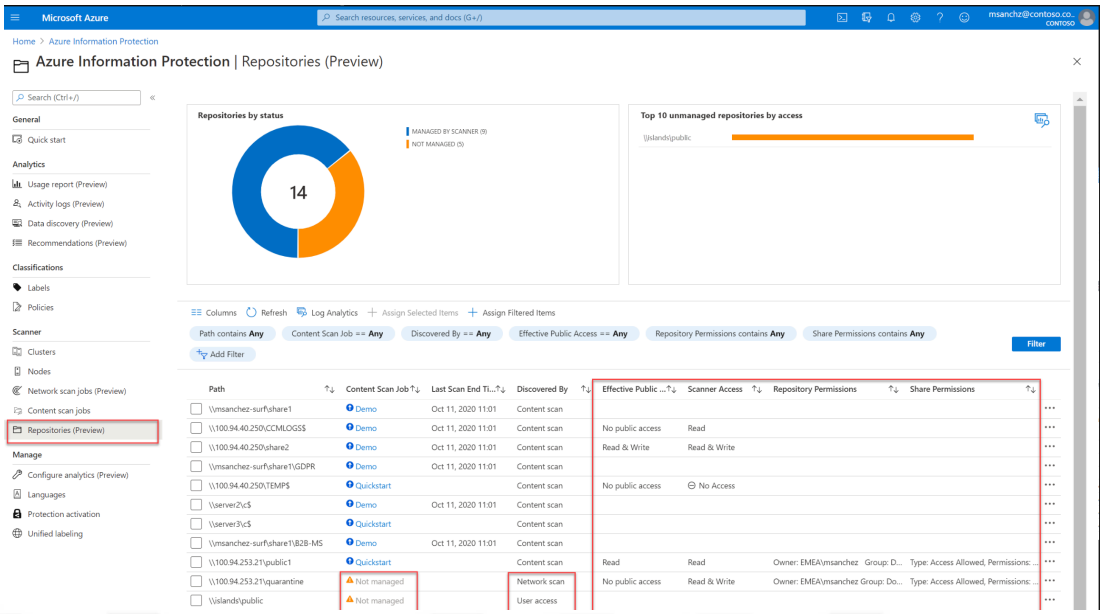

Figure 29 Azure Information Protection Portal

Chapter 5

CONCLUSIONS

I have worked on a DLP architecture to develop an overall strategy for this thesis. Then, I studied the use-cases that will provide end-to-end solutions for the organizations and make them available to be used by SIEM products. I aimed to create more sophisticated use-cases to detect recent cyberattacks and trends such as Insider threats and Zerotrust. Assembling the correlation rules using these artifacts will help the enterprises to react quickly to these kinds of attacks and support them learn about which security solutions they will need in the future.

Data loss prevention (DLP) has finished its growth from a niche instrument to an essential component of more overall information-centric security architecture. However, security professionals are still hard-pressed to recognize the importance of this technology. This thesis has shown a structured approach to effectively deploying and using DLP technology from various perspectives.

In future work, I am proposing an improved version of this system that might include machine learning mechanism and more Artificial Intelligent to increase the detection rate and accuracy with Cloud computing. Data leakage or loss will be detected way before it happens.

REFERENCES

Al-Fedaghi S. (2011). "*A Conceptual Foundation for Data Loss Prevention*". International Journal of Digital Content Technology and its Applications. Volume 5. Number 3.

"*CIS Critical Security Controls v8*" May, 2021.

CDW LLC. PEOPLE WHO GET IT, Data Loss Prevention and the Financial Firm Available at: http://mike.chapple.org/wp-content/uploads/2014/09/dlp financial-whitepaper_1.pdf

CNBC, (2019). The Capital One breach is unlike any other major hack, with allegations of a single engineer wreaking havoc. Available at: https://www.cnbc.com/2019/07/30/capital-one-hack-allegations-describe-a rare-insider-threat-case.html.

Crowd Research Partners. (2018). 2018 Insider Threat Report. [Online]. Available: https://crowdresearchpartners.com/insider-threat-report/

Devlin R. (2015). "*Data Loss Prevention*" SANS White Paper.

Gordon P. (2007). "*Data Leakage – Threats and Mitigation*" SANS White Paper.

Intuate Group (2011). 'Components of a Data Leak Prevention System | ITWeb.' Available at: https://www.itweb.co.za/content/o1Jr5MxjpbRvKdWL

Kitten T. (2014) Bank Info Security. "7 Lessons from Target's Breach". Available: https://www.bankinfosecurity.com/

Lawrence C.M. (2009). "*Data Leakage for Dummies*", Wiley Publishing.Ubois, J. (2007). "*Reinventing data loss prevention*". The Security Report.

Le D. C., Zincir-Heywood N. and Heywood M. I., "Analyzing Data Granularity Levels for Insider Threat Detection Using Machine Learning", IEEE Transactions on Network and Service Management, VOL. 17, NO. 1, MARCH 2020

Studies in Big Data Volume 84 Warsaw, Poland:Springer, 2021

National Institute of Standards and Technology, (2004). 'FIPS 199, Standards for Security Categorization of Federal Information and Information Systems. Available at: https://csrc.nist.gov/publications/detail/fips/199/final. Last accessed 11/02/2022.

Nageswaran Kumaresan. 'Key Considerations in Protecting Sensitive Data Leakage Using Data Loss Prevention Tools' (2014) 1. Available at: https://www.isaca.org/Journal/archives/2014/Volume-1/Pages/Key Considerations-in-Protecting-Sensitive-Data-Leakage-Using-Data-Loss Prevention-Tools.aspx. Last accessed 16/01/2022.

Sans Institute 2008, Data Loss Prevention, (2018, December 2), from https://www.sans.org/reading-room/whitepapers/dlp/paper/32883

Tagarev T., Atanassov K. T., Kharchenko V. and Kacprzyk J., "Digital Transformation, Cyber Security and Resilience of Modern Societies" in

Tessian (2021) The State of DLP 2021 "*Data Loss Prevention in Financial Services*" [Online]. Available: https://www.tessian.com/research/the-state-of-data-loss-prevention-2020/

Probst C. W., Hunker J.,Gollmann D. and Bishop M. "Insider Threats in Cyber Security" USA:Springer, 2010.

Zhang E, 'What Is Log Analysis? Use Cases, Best Practices, and More' (Digital Guardian, 16 October 2017). Available at: https://digitalguardian.com/blog/what-log-analysis-use-cases-best-practices and-more. Last accessed 25/03/2022.