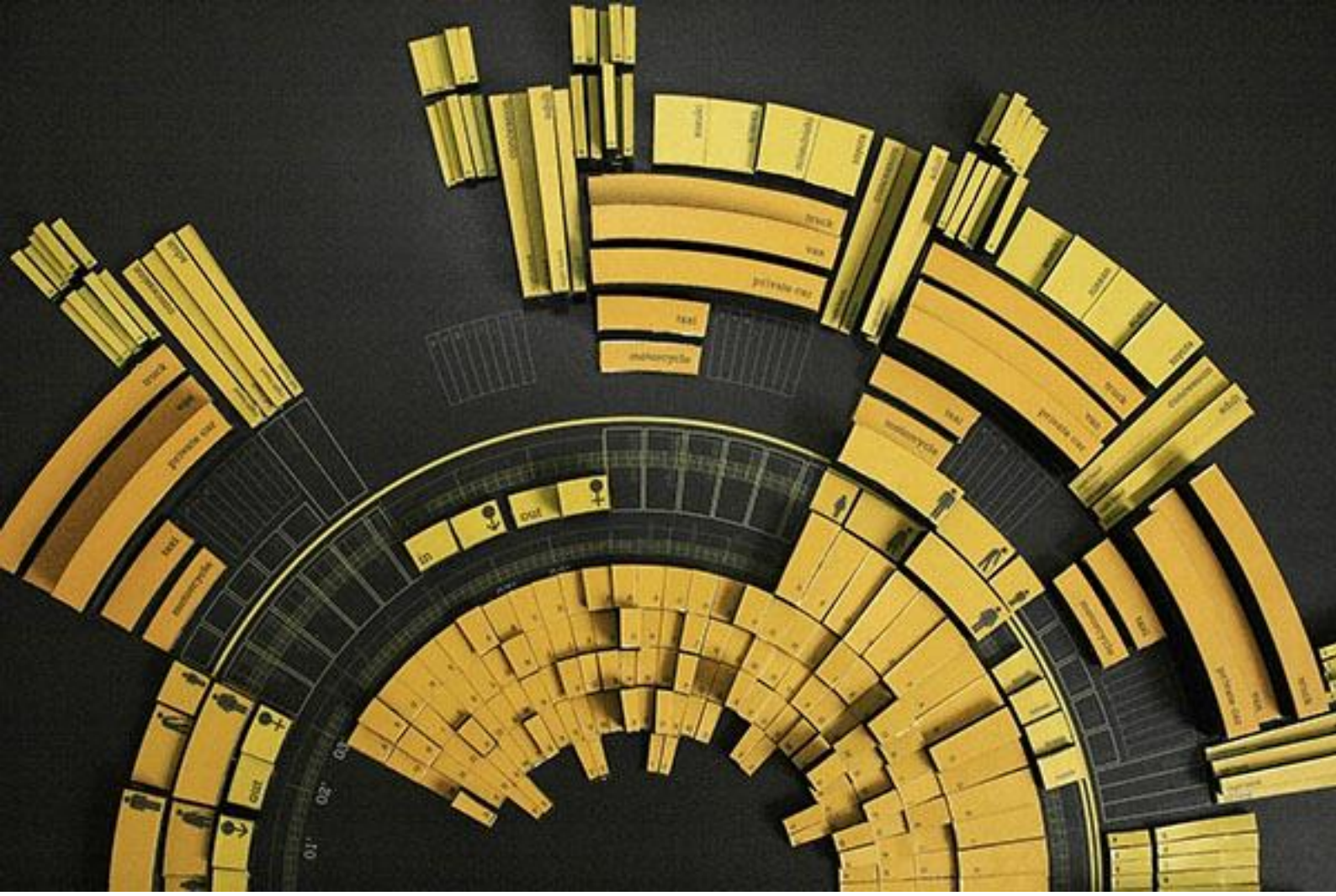


Master of Advanced Studies in Information Security

Methodology to select Security Information and Event Management (SIEM) Use Cases

Author Pascal Imthurn

Submitted 13th of May 2019

Lucerne University of Applied Sciences and Arts

Lucerne University of Applied Sciences and Arts

Master of Advanced Studies in Information Security

Methodology to select Security Information and Event Management (SIEM) Use Cases

Supervisor:
Reto Zeidler
reto.zeidler@ch.ibm.com

Second Assessor:
Craig Fletcher
craig.fletcher@ispin.ch

Author:
Pascal Imthurn
pimthu@gmail.com

Submitted: 13th of May 2019

Abstract

The advancing digitalisation forces companies and organisations to build up defences against cyber-attacks. The latter of which are now mostly silent, sophisticated and often tailor-made. To protect themselves, they need equally professional machinery to detect these attacks systematically and combat them efficiently. In most cases, this is achieved through a Security Operations Centre (SOC) or a Cyber Defence Centre (CDC) as the focal point for coordinated countermeasures.

Companies and organisations that are in the planning, development or expansion phase of a security operation centre (SOC) or cyber defence centre (CDC) need guidelines for detection and how to proceed in a structured manner once detection has taken place. These requirements are generally referred to as Security Information and Event Management (SIEM) Use Cases.

Driven by the personal objective of the author to mitigate the impact of cyber-attacks, this research has shown that it is possible to have a unified approach in using SIEM Use Case focus areas necessary for their selection and combine them with the relevant cybersecurity standards and frameworks. The result is a flexible best practises solution allowing for various parameters to be configured to receive a list of applicable SIEM Use Cases

The result of this Master of Advanced Studies (MAS) work is a methodology for selecting Security Information & Event Management (SIEM) Use Cases based on the catalogued techniques in the Mitre Att@ck Framework. The research has shown that a formal SIEM Use Case selection process can be defined based on actual threats, SME input, regulations, available detection methods, organisational requirements and risk management. This methodology takes into account following technical and regulatory standards: Critical Security Control (CSC) by the Centre for Internet Security (CIS), the ISO/IEC 27001 standard, the Cobit 5 Business Framework, North American Electric Reliability Corporation (NERC) CIP standards, the National Institute of Standards and Technology (NIST) SP 800-53 standards and their Cybersecurity Framework (CSF), The Payment Card Industry Data Security Standard PCI-DSSv3.2 and the Health Insurance Portability and Accountability Act (HIPAA).

The resulting methodology allows a comprehensive selection process of SIEM Use Cases based on log sources, industry, standard or framework. The output is given in the form of a roadmap based on prioritisation factors such as the size of organisation or cybersecurity maturity. The methodology can be extended either by adding own mappings or by using the output to undergo another assessment for further prioritisation.

Table of Contents

Index of Figures

Index of Tables

Abbreviations

Generic ICT abbreviations are not included in the following table.

Att&ck	Adversarial Tactics, Techniques, and Common Knowledge
BSI	Federal Office for Information Security
CDC	Cyber Defence Centre
CIP	Critical Infrastructure Protection
CIS	Centre for Internet Security
COBIT	Control Objectives for Information and Related Technologies
CSC	Critical Security Controls
HIPAA	Health Insurance Portability and Accountability Act of 1996
IRP	Incident Response Procedures
ISACA	Information Systems Audit and Control Association
ISMS	Information Security Management System
ISMS	Information Security Management System
ISO	International Organization for Standardization
NERC	North American Electric Reliability Corporation
NIST	National Institute of Standards and Technology
NIST CSF	NIST Cyber Security Framework
RBAC	Role Based Access Control
SEM	Security Event Management
SIDR	Security Incident Detection and Response
SIEM	Security Incident and Event Management
SIM	Security Information Management
SME	Subject Matter Expert
SOC	Security Operation Centre

[] Image source of title page: https://datavizproject.com/data-type/sunburst-diagram/

1. Introduction

The advancing digitalisation forces companies and organisations to build up defences against cyber-attacks. These are now mostly silent, complex and often tailor-made. To protect them, they need equally professional machinery to detect these attacks systematically and combat them efficiently (Zeinali, 2016). For this purpose, in most cases, a Security Operations Centre (SOC) or a Cyber Defence Centre (CDC) is the focal point for coordinated countermeasures.

Companies and organisations that are in the planning, development or expansion phase of a security operation centre (SOC) or cyber defence centre (CDC) need guidelines for detection and how to proceed in a structured manner once detection has taken place. These requirements are generally referred to as Security Information, and Event Management (SIEM) or Security Incident Detection and Response (SIDR) (Perniola & Gray, 2019) Use Cases.

An integral part of protecting a company is to have a structured way of doing this; therefore, SIEM Use Cases are a measurable way of controlling any environment.

1.1 Problem statement

The cybersecurity industry and individuals leading the research on defensive mechanisms in safeguarding the world's data have developed increasingly advanced tools over the past 20 years. One of the main advancements in this field is the development of Security Information and Event Management (SIEM) solutions assisting in detecting adversaries by processing a vast amount of data. The technology offers detection capabilities built on top of available log sources. The SIEM was meant to be the one solution to tie together many different cybersecurity products to visualise the security health of an organisation, to detect attacks and to coordinate response activities.

However, the reality is that a tool does not solve an inherent problem. Most organisations have struggled with the implementation of such tools as SIEM (Perniola & Gray, 2019). The author itself has had 43 discussions with prospects and customers in 2018 alone on the topic of SIEM Use Case selection. Next, to the operational difficulties, there is no globally accepted guidance as to which detection principals should have a focus. If one does not know what to monitor to defend its significant information data assets, then a tool does not take away that decision process.

In response to this problem, this study proposes to investigate a possible methodology in assisting organisations and cybersecurity professionals in selecting SIEM Use Cases based on the catalogued techniques in the Mitre Att@ck Framework. This methodology should consider the respective technical and organisational environment, internal and external requirements, as well as best practices and the available security know-how of the company or organisation.

1.2 Statement of purpose

David Grey and Angelo Perniola have summarised the current state of Use Case selection in their 2016 SANS DFIR talk. They claim that a compelling SIEM Use Case needs to address following key areas: Objective, Threat, Stakeholders, Data Requirements, Logic, Testing, Priority and Output (Perniola & Gray, 2019, pp. 5-14). They conclude in their presentation that prioritisation and a SIEM Use Case library built upon the organisation’s cybersecurity risks is the most effective way in detecting attacks (Perniola & Gray, 2019, p. 35). Specific attention is given to the Mitre Att&ck Framework (Mitre, 2019) and its strength regarding the techniques and methodologies of attackers (Perniola & Gray, 2019, p. 29).

Various drivers such as risk management, regulators, stakeholders or subject matter experts (SME) can influence the content of the mentioned vital areas as Ryan Faircloth points out in his Splunk .conf2016 speech (Faircloth, 2016). All these stakeholders have different views on prioritisation, time pressure and budget issues make it challenging to select and define the Use Case Roadmap (Faircloth, 2016, p. 11).

This paper is trying to include the drivers mentioned by Faircloth, the objective and threat key areas mentioned by Grey and Perniola into a unified approach. The aim is to develop a methodology in assisting organisations and cybersecurity professionals in selecting SIEM Use Cases based on a combined approach of utilising the log sources as documented in the Mitre Att&ck Framework and the combination of various cybersecurity standards or frameworks.

The primary objective of this research is to mitigate the impact of cyber-attacks by providing a method to best match the current attack methodologies with detection capabilities.

The author acknowledges that attacks are run against organisations of all sizes and any number of individuals (The Council on Foreign Relations, 2019) (Hackmageddon, 2019). However, this research does not analyse the effectiveness of current SIEM installations and detection capabilities.

1.3 Research questions

A central point for this research is that detection of any threats is considered to be centrally managed while sensors are delivering telemetry data in the form of raw events or aggregated or correlated alerts. For ease of understanding, this is referred to as to be managed within a Security Information and Event Management (SIEM) solution. SIEM technology or other detection technologies will not be addressed by research questions.

Based on the problem statement and the statement of purpose, the following research questions have been fleshed out to reflect the objectives of the research.

1.3.1 The central research question of this thesis

The central research question of this thesis is:

If cybersecurity risks are managed by frameworks and standards, can we combine the requirements listed in these documents with actual threat data to drive the SIEM Use Case selection process?

1.3.2 Sub-question: SIEM Use Case selection

The first sub-question supporting the central research question is:

What are the current drivers or focus areas in the selection process of SIEM Use Cases?

1.3.3 Sub-question: Threats & Detection

The second sub-question supporting the central research question is:

Is there a central repository listing all relevant cybersecurity threats and are there documented methods in detecting these within a SIEM?

1.3.4 Sub-question: Standards

The third sub-question supporting the central research question is:

How can existing cybersecurity standards and frameworks be mapped to threats and detection capabilities?

1.3.5 Sub-question: Selection

The fourth sub-question supporting the central question is:

How can organisations select the suitable detection methods for implementation considering cybersecurity threats and requirements defined in standards and frameworks?

1.4 Overview of methodology

The thesis is structured into six key areas as outlined in the following graph.

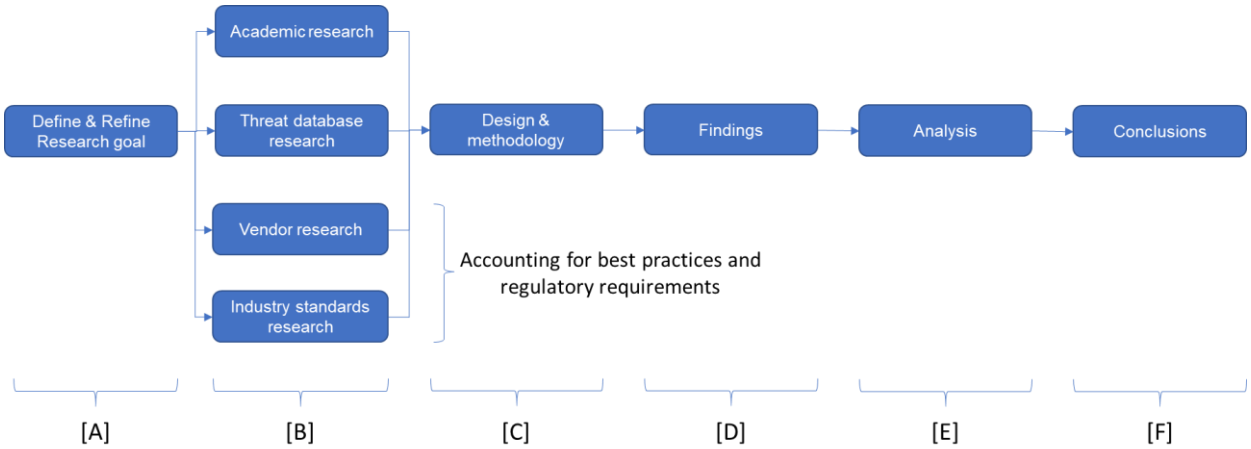


Figure 1: Research approach

Source: Graph has been created by the author

Section [A] is included in the first chapter. The reader is receiving an introduction to the research topic. As outlined the problem statement, the statement of purpose and holds the research questions driving this research.

All literature research will be discussed in section [B]. The focus is to find existing data to answer the research questions. The chosen approach is to research four areas in the field of cybersecurity containing or referencing data for SIEM Use Case selection. The four areas cover the academic research, threat databases containing real-world datasets of attackers, the industry standards and lastly, the vendor data to have actual information on the SIEM Use Case selection process.

Section [C] explains the bounds of the research conducted. It is partly influenced by the research questions raised in section [A] but also takes into consideration some of the key findings

out of the literature review in section [B]. In section [D] all research from the sections [B] and [C] is evaluated, and a proposal statement is collected in order to answer the research question. In this section also, the data of the standards are injected to be included in the findings procedure.

The section [E] analysed the accumulated data in [D] and verified the proposal raised. Finally, section [F] holds the conclusion to the research and closes the thesis.

1.5 Rationale and significance

The rationale behind this study is to provide an answer to the missing generalised approach assisting organisations in organising their detection capabilities best matching their risk exposure. It is a significant risk for organisations to re-invent the wheel and possibly end up with a solution sub-standard of the best practises – whatever these might be. If research identifies the missing gaps of the SIEM Use Case selection process and this thesis can provide a suitable methodology to fill these gaps, then there is a satisfying answer to all responsible in the SIEM selection process.

The benefit becomes obvious. The focus can shift on the technical expertise of the implementation and shifts away from manufacturing a selection framework influenced by many stakeholders. Selecting the measures on how to detect attackers is a very challenging task for an organisation. Especially if people involved are not experienced in detecting adversaries, the mindset of uncovering malicious behaviour is particular and, in some respects, cannot be automated or completely operationalised. Further, stakeholders have different interests, views and responsibilities. Combining all these views into one approach is not feasible and will result in lengthy discussions.

By combining the available standards and real attack data, the problem becomes measurable. The moving target becomes static, and if backed by a standard and real attack data, there is a guided and standardised approach. There is an additional cost benefit as possibly consulting fees and project costs required in designing a selection process is reduced. Additionally, there is clear guidance on priorities, and budgetary requirements can be derived thereof.

1.6 Role of the researcher

The author has been exposed to the fundamental question of how to protect organisations throughout his career. The involvement has been either in a role as being directly responsible for building and operating Security Operation Centres, delivering detection capabilities or in a capacity to consult or build detection capabilities within a project.

The decision process to select the best fitting SIEM Use Cases is being influenced not just by one person or one entity but is being the result of a complicated process. That process is then being iterative influenced by other parameters.

The work is comparable to as being asked to install security cameras in a thousand different buildings, with a thousand different make and models of cameras, a thousand different types of perimeters around the buildings, a thousand different types of indoor lighting, a thousand different types of objects to protect, the perimeter windows are arranged a thousand different times and have many different protection levels, a thousand different doors and locks, some have a heliport, some have access to a train stop and most offer car access. We then need to separate eligible people allowed to access these facilities from those who should not have access.

Finally, we then must realise that there are 1’000 other persons like the author whom each have a 1’000 of these houses to protect as well.

The role of anyone participating in the cybersecurity industry needs to be in reducing complexity, to standardise and to create guides in achieving a level of security which can be compared and measured.

With the previous experience and the research focus on the selection process of making attacks visible, the author wants to shine a light on existing approaches of the selection process, use available data to support that selection process and research ways of standardising or assist that selection process.

1.7 Researcher assumptions

Through the experience gained over the last 20 years in the field of cybersecurity, the author of this paper, believes that based on his role as a managed service professional in cyber defence, that he can support his work by showing his customers the benefit of a structured and standardised process in selecting SIEM Use Cases. Within a best-case scenario, this research might also assist other professionals in their daily work.

Within the near future, the answer to the problem is not within technology itself – such as machine learning- and must be solved by carefully selecting the Use Cases to detect adversaries. This is best solved by utilising real attack data.

A not so farfetched comparison are the attacks executed by terrorists. We seem to encounter a steady stream of new tactics employed by terrorists to hurt human life. Disregarding the advanced counter-terrorist techniques preventing some of the attacks, we still need to rely on the essential human capacity to recognise a person doing the crime. Due to social media, the data is collected and consumed on a global scale, and police and civilians alike are conditioned to detect malicious behaviour. Resulting in that a truck driving with a slightly increased speed close to a pedestrian area as perceived as danger. We must employ the same techniques in defending against cyber criminals. New technology is not always needed but better ways of utilising the existing technology in place.

The author believes that combining existing methods developed within standards and actual fact-based data is producing a guided approach to select the best sets of SIEM Use Cases, to protect any organisation.

The danger is that by exposing the methods on how attackers are being detected, this can be used to evade detection. Therefore, it is crucial that the SIEM Use Case selection and implementation process is enclosed within a lifecycle process. It needs to be ensured that new attacks are evaluated continuously and if relevant added to the Use Case portfolio.

1.8 Definition of key terminology

The following chapters provide definitions of the key terminology used in this thesis. All commonly used terminologies in ICT or specifical terminologies in the realm of cybersecurity are not vital in understanding the content of this thesis. Abbreviations are mentioned following the table of content.

1.8.1 Security Information Management (SIM)

Security Information Management (SIM) (Security information management, 2019) stems from the need for Long-term storage as well as analysis and reporting of log data.

1.8.2 Security Event Management (SEM)

Security Event Management (SEM) (Security Event Management, 2019) stems from the need for Real-time monitoring, correlation of events, notifications and console views.

1.8.3 Security Information and Event Management (SIEM)

The term Security Information and Event Management (SIEM) (Security information and event management, 2019) were coined by the need to combine Security Information Management (SIM) and Security Event Management (SEM).

1.8.4 SIEM Use Case

The term SIEM Use Case is generally accepted and a well-understood term in the cyber security industry. That said, differences exist in the understanding of what the specific components of a use case should, can or must be. Gartner (Chuvakin, Anton; Barros, Augusto;, 2019) , for example, focuses on the technical implementation of detection capabilities within a SIEM. RSA (Perniola & Gray, 2019) and Splunk (Faircloth, 2016) include the overall view of detection and response in their definition. That includes technical implementation and response capabilities in the form of processes. The proper steps include the definition of the objective, the threat, the operational structure, the data requirements, the detection logic and the output.

In the end, the relevance for an organisation to choose and implement a Use Case is the defined goal of the Use Case – what it will detect, and the requirements to get the Use Case implemented – from a technical and operational perspective.

As Pernicola and Gray put it, “Methodology used by the SOC team to identify and organise technical and organisational requirements for detection and response to specific threats.” (Perniola & Gray, 2019, p. 3)

Another definition is by Gartner’s Chuvakin and Barros: “Specific condition or event (usually related to a specific threat) to be detected or reported by the security tool” (Chuvakin, Anton; Barros, Augusto;, 2019)

1.8.5 Security Operation Centre (SOC)

The Security Operation Centre (SOC) (Security Operation Center, 2019) is a central, mostly physical but sometimes virtual, the organisation responsible for monitoring, detecting and defending against threats within a company or organisation. Sometimes the SOC is also referred to as Cyber Defence Centre (CDC) and vice versa.

1.8.6 Mitre Att&ck Framework

The Mitre Att&ck Framework (Mitre, 2019) is a brainchild of Mitre and is the result of observing attacks from around the world and describes the tactics, techniques and procedures deployed. Essentially it is a threat and model knowledge base.

1.8.7 Cyber Kill Chain

Lockheed Martin has developed the Cyber Kill Chain. The seven steps of the Cyber Kill Chain enhance visibility into an attack and enrich an analyst's understanding of an adversary's tactics, techniques and procedures (Lockheed Martin, 2019).

1.8.8 Standards

1.8.8.1 CIS CSC

The Centre for Internet Security (CIS) publishes 20 Critical Security Controls (CSC) (CIS, 2019). The controls are split up in three different groups. There are the Basic CIS Controls, which are controls 1 to 6. There is the Foundational CIS Controls, which are controls 7 to 16 and there are the Organizational CIS Controls, which are covering controls 17 through to 20.

1.8.8.2 NIST Cybersecurity Framework

The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) (NIST, 2019) is part of the U.S. Department of Commerce. The institute has produced a very versatile Cyber Security standard. The framework receives an increased adoption rate. Relevant for Switzerland is the 2008/21 circular (Switch, 2019) of FINMA and also adopted in the Swiss Minimal ICT Standard (Minimal ICT Standard, 2019).

The standard focuses on five disciplines to form a comprehensive cybersecurity management strategy. These five areas are: Identify, Protect, Detect, Respond and Recover.

1.8.8.3 Minimum ICT Standard

The Minimum ICT Standard has been put together by the Swiss government in order to comply with its mission to protect its citizens, the economy and its institutions and public administration (Minimal ICT Standard, 2019).

1.8.8.4 ISA 62443

ISA 62443 is a standard for the security of industrial automation and control systems (ISA, 2019).

ISA 62443-2-1:2009 focuses on the elements of a cybersecurity management system of industrial automation control systems (ISA, 2019).

ISA 62443-3-3:2013 provides security level requirements for industrial automation and control systems (ISA, 2019).

1.8.8.5 ISO/IEC 27001:2013

The ISO/IEC 27001 standard helps organisations to manage their assets in terms of security (ISO, 2019). The standard puts the management in charge of all security risks, implement information security controls and adopting a management process. A strong focus is on the latter. Only in conjunction with an Information Security Management System (ISMS) can controls such as defined within ISO/IEC 27001 be continuously verified.

1.8.8.6 ISO/IEC 27019:2013

The standard ISO/IEC 27019:2013 is based on ISO/IEC 27002 used to describe ISMS. The primary focus of ISO/IEC 27019:2013 is on process control systems for the power systems (ISO, 2019). The standard has been superseded by ISO/IEC 27019:2017 (ISA, 2019) but is still being referenced in the Minimum ICT Standard (Minimal ICT Standard, 2019) and NIST mappings (NIST, 2019).

1.8.8.7 BSI-Standard

The “Bundesamt fuer Sicherheit in der Informationstechnik” (BSI) - Federal Office for Information Security has produced several catalogues with methods, processes, procedures, approaches and measures relating to information security (BSI, 2019).

1.8.8.8 IEC 62351-8

The IEC 62351-8 is the eight technical specifications of the IEC 62351 standard, which describes the security standard of power systems and the dependent electronic data exchange. IEC 62351-8 is focusing on the topic Role Based Access Control (RBAC) (Obermeier, Schneider, & Schlegel, 2019).

1.8.8.9 HIPAA

The Health Insurance Portability and Accountability Act of 1996 or HIPAA (US Department of Health & Human Services, 2019) is an Act of the United States of America on regulating the handling of healthcare information. Section Title II contains the procedures and policies on preventing health care fraud and abuse relevant to this paper.

1.8.8.10 COBIT 5

The Control Objectives for Information and Related Technologies (COBIT) is a framework created by ISACA (ISACA, 2019) to ensure ethical practices in ICT governance and management (COBIT, 2019).

1.8.8.11 NERC-CIP

The North American Electric Reliability Corporation (NERC) is a reliability standard (NERC, 2019) for bulk power systems. The standard includes the interconnected power systems of the U.S., Canada and Mexico. The NERC-CIP or Critical Infrastructure Protection (CIP) is an additional set of controls focusing on cybersecurity (NERC, 2019).

2. Literature Review

2.1 Introduction

Over the last twenty years (Chuvakin, 2019), the development of SIEM platforms has been driven by several large corporations. Based on the authors' professional experience, every product created closed ecosystems of professionals and services to serve customers focused on the features and capabilities of the individual product implemented. It has been a very tool-centric approach in which techniques and processes have not been at the centre of the problems to be solved.

The question is, how the development of SIEM platforms has helped to detect attackers better and how to drive these detection capabilities in a structured way forward. Which parameters have been helping the selection process and how has this improved the capability to defend against attackers?

This paper tries to:

- research shared approaches of vendors selling SIEM solutions,
- research freely available threat resources,
- research the most relevant cybersecurity frameworks,
- also, conduct academic research in the field of SIEM Use Case selection.

The premise is that by researching the methods employed by well-known cybersecurity, vendors must provide us with the best defence capabilities through empiric result gained by professionals. We further must be able to reflect these methods within the threat databases, which contain the actual attack methods used by attackers – at least the publicly known. We then can compare that data with academic research done in the area of cyber defence.

2.2 Review of literature

There have been significant advancements in the area of adversary detection, and with the introduction of SIEM technologies, everyone had a platform to detect and visualise attackers and to orchestrate responses to defend the organisation against these attacks. The issue is that most organisations have struggled with the implementation of SIEM solutions (Perniola & Gray, 2019). Apart from the technical implementation and the operational activities needed to operate a SIEM successfully, there is also a significant gap in know-how and guidance which detection capabilities or SIEM Use Cases to implement. The author advised 43 customers on the subject in 2018 alone. These accounts ranged from SME to Enterprise in size covering banking, manufacturing, pharmaceutical, insurance, healthcare, defence, telecommunication, aviation and high-tech industries. There is a definite lack of guidance on what to watch out for when it comes to attack detection.

For that reason, the purpose of this paper is to address the lack of a methodology to select SIEM Use Cases. It should provide a generalised method to guide the selection process and help the selectee to utilise the existing standards and the assistance of actual proven techniques to select the detection methodologies best suited to help their organisation.

The research is primarily focused on the research questions of this paper:

- If cybersecurity risks are managed by frameworks and standards, can we combine the requirements listed in these documents with actual threat data to drive the SIEM Use Case selection process?

- What are the current drivers or focus areas in the selection process of SIEM Use Cases?
- Is there a central repository listing all relevant cybersecurity threats and are there documented methods in detecting these within a SIEM?
- How can existing cybersecurity standards and frameworks be mapped to threats and detection capabilities?
- How can organisations select the appropriate detection methods for implementation considering cybersecurity threats and requirements defined in standards and frameworks?

2.2.1 Academic research

The review of research papers in the field of SIEM technologies or SIEM Use Cases has shown that there is a good understanding on how to design a SIEM Use Case, but there is no in-depth analysis of the many different SIEM Use Cases available.

Research has also been conducted on various subscription free academic research platforms such as Google Scholar (Google Scholar, 2019), Semantic Scholar (Semantic Scholar, 2019), SiteSeerX (The Pennsylvania State University, 2019) and DBLP (University of Trier, 2019). Search terms (literature containing all listed search terms) used to perform the searches where:

- *Cybersecurity SIEM*
- *SIEM detection*
- *SIEM rules*
- *SIEM use case*

Following types of research paper have been identified:

- The focus lies with the SIEM technology only. There are particular concepts of designs and implementations discussed. Generally, there are a handful of primary SIEM Use Case samples given, but the responsibility of what is being detected is then given to the reader.
- The focus is on specific detection capabilities. There are many research papers which focus on single topics such as denial-of-service or HTTP based attacks. One of these research papers would equate to one single SIEM Use Case. The research on these topics are significant, but the proposed solutions are mostly concerned with solving a specific detection problem within the cybersecurity spectrum. The approach is mostly lacking a grander picture and the interrelationship between the various detection capabilities.

A small portion of research documents has been found to relate to this research. In the following section, two texts are analysed.

2.2.1.1 Academic text one – SIEM Implementations

The work of Sander Dorido focuses on the implementation methodologies of SIEM solutions (Dorigo, 2012). In his work, there is a fair amount of guidance on the definition of a Use Case given by cybersecurity professionals, ICT operations, risk management and with focus on the business. In the design process, it is not a selection of Use cases out of an existing pool but

instead, the definition of Use Cases from scratch based on risks of the organisation. He argues that Use Cases need to be defined as part of the project and are an integral part of the design of a SIEM. He states that the success factor of an accurate definition of a Use Case is to connect it to the business of the company. A Use Case can only be fully understood if that alignment is a close as possible. On one side with the focus on cybersecurity and on the other of utilising business visibility, transparency and full integration into the risk management of the company.

He continues with classifying Use Cases into three groups. The first one is compliance-, the second one is security- and lastly, there is an operations-based Use Case. Use Cases within these three groups fulfil specific needs and have different stakeholders interested in monitoring, detection and remediation.

He proposed a requirements management process collecting requests from standards and experts from the respective fields to compile a Use Case. The focal points within the requirements gathering are the following topics:

- Data collection requirements and covers the specific needs of the data to be collected to perform the monitoring and detection activity for the Use Case. During this step, it must be established which fields within the data stream are relevant. If required, the sources generating these data entries need to be adjusted to fulfil that requirement. Other necessary verifications need to be done for:
    - Data compliance - to ensure that national and international privacy laws and regulations are being followed
    - Filtering of data - only relevant data needs to be collected
    - Licensing and costs - consideration of how much additional costs will occur for data acquisition
    - Data integrity – ensure that data is not lost
    - Transport bandwidth – ensure that the infrastructure can deliver the needed data
    - Disk storage – ensure that enough disk space is available for data processing
    - CPU and RAM – ensure that enough computational power is available to the processes
    - Monitoring – to catch erroneous behaviour
- Reporting requirements to satisfy automated reporting. The reporting should also follow the guideline of using business language for all three Use Case areas – compliance, security and operations.
- The requirements must also cover incident management, which covers alerts and event reporting. It must be clearly defined what is being analyzed, and the author makes a strong statement on privacy. That is not to violate any regulations or of user privacy.

To summarise the approach as proposed in Sander Dorido’s master thesis.

- Use Cases are built based on risk assessment of the business because of operational, compliance and security risks.
- No utilisation of a central Use Case database

2.2.1.2 Academic text two – Determining focus areas and their coverage within IT risk frameworks

The other academic text “Determining focus areas and their coverage within IT risk frameworks” written by Jarno van de Moosdijk and Daan Wagenaar (van de Moosdijk & Wagenaar, 2015) focuses on the overall strategy in defining focus areas for the SIEM implementation by utilising IT risk frameworks. The authors also compare their findings to SIEM implementations they have reviewed.

The identified focus areas are organisations requirements, operational requirements, log management, correlation, alerting, responding and evaluation. As a basis for the evaluation served the IT risk frameworks ISO/IEC 27002, COBIT 5, NIST CSF 1.0, PCI-DSS 3.0 and Standard of Good Practise for Information Security (ISF SoGP). The researchers were analysing data of two financial institutions.

During their research, they have identified several deficiencies within the frameworks. All the mentioned frameworks do not put a high emphasis on operational requirements. The two analysed institutions had the following two areas as primary drivers for their own SIEM implementation: threat management and compliance.

In their research, they have found that most organisations are willing to implement a SIEM program to secure their assets. Most of them fail in completing their mission due to missing know-how, inadequate resources, tool-centric approach and lack of management support.

The authors point out that one needs to know what they must protect (van de Moosdijk & Wagenaar, 2015, p. 17). Without knowing what to protect, there can be no risk scenarios been defined. Without risk scenarios, there are no Use Cases to implement or at least not Use Cases relevant for the protection of an organisation.

To summarise the findings in Jarno van de Moosdijk and Daan Wagenaar research.

- An organization needs to define risk scenarios to select SIEM Use Cases
- There must be adequate funds in implementing a mature level of cyber defence of an organisation
- The selected frameworks are not adequately supporting an implementor in building a world-class SIEM solution

2.2.1.3 Summary

The review of the literature provided some interesting insights, which were not overall expected. It is generally seen that the sciences are driven by academic research and real-world implementations are directly derived from research. The lack of research papers in the area of SIEM technologies can be an indicator that the area of SIEM technology is primarily driven by vendors. There is the introduction of new technology into the available SIEM technologies, but it has the appearance of mending pieces together, instead of the ground-up rebuilding of SIEM technology. This is somewhat a controversial statement as new companies have been founded claiming to be the one-stop-shop for identifying all attackers and threats. Even though the technologies used are intriguing and of the machine learning sort, the claim that these products are the final solution for every organisation is not founded.

It also has shown in the literature that anyone serious about stepping up their level of maturity in detecting adversaries, need to understand what they must protect. It needs to be fully understood what the valuable assets of an organisation are, to be able to decide on measures to potentially detect misuse of these assets.

There are however many research papers on various detection technologies. The research is mostly focused on a single topic. The positive aspect is that the author can focus on a limited field of view, which allows providing a very technologically advanced method in detecting an adversary. These methods can be brilliant at times and will provide a new edge in detecting attackers. Overall it does not directly help an organisation in bettering their security posture. A new product can be purchased, but that will result in additional expenditure in acquiring the product and then to integrate and operationalise it. A cost not everyone can afford.

Another finding was that there is no general SIEM Use Case design approach. It is mainly left to vendors and the organisations to define a model for creating Use Cases (Dorigo, 2012). Unfortunately, these are not standardised and cannot be commonly shared, at least not over the boundaries of the implemented SIEM technologies. This is also equivalent to a global Use Case library. It is generally assumed that organisations know how to protect their assets. How one selects and writes Use Cases is not covered in research – at least not as a universal approach.

The research paper of Jarno van de Moosdijk and Daan Wagenaar (van de Moosdijk & Wagenaar, 2015) also states that current standards are not providing enough or specific guidance on use case implementation. The positive aspects of the standards are that they are doing an excellent job in identifying risks and setting focus points to building the level of protection against cybersecurity attacks. When it comes to the implementation to protect the identified risks, the answers are too vague and lead to alternative ways of interpretation and implementation. This is a central find for this research paper. The proposition is solving not having enough clarity in implementing SIEM Use Cases by mapping standards to real-time attack data.

The research of Jarno van de Moosdijk and Daan Wagenaar (van de Moosdijk & Wagenaar, 2015) also analyse the focus areas of building SIEM implementations. Taking into consideration the focus of the research goal of this paper, the focus areas of organisations and operational requirements and correlation are relevant and will be referenced to.

2.2.2 Freely available threat resources

An integral part of this research is to include factual based data. The research conducted is within an area, which has progressed over the last 20 years (Chuvakin, 2019). It is, therefore, to assume that activities collected based on the data generated are valuable to assess and to incorporate into any conclusion. The enhanced visibility would strengthen any argument in favour or against the set research goals. It is also the author's belief that it will support suggested methodologies as a result of this research.

The selection process to identify said public sources are based on two principles:

- Current best practises as perceived by the author's professional experience
- Internet-based research on threat resources

Even though the first principle is not directly measurable, it is reflected a great extent in the publications of highly regarded individuals (Smith, 2019) in the area of cybersecurity or mentioned in published content by the significant cybersecurity firms (Stoner, 2019) around the globe. The author interprets that data as evidence of relevance and importance. The data source referred to is the Mitre Att&ck Framework and is currently being adopted and incorporated into cybersecurity products (Carbon Black, 2019).

The second principle is inferred by available resources on threat databases on the Internet. There are many valuable datasets available, and it is difficult to dissect the more relevant sets due to missing KPIs. The selection process for this research was based on popularity within the cybersecurity industry.

The Exploit DB dataset was selected as it provides the individuals working in the cybersecurity industry with a database containing information and details to known vulnerabilities and defence mechanisms to test, to protect and to actively defend against cyber-attacks, groups and organisations have come forward in producing free services (Offensive Security, 2019). It's popularity also is explained with the indirect affiliation with Metasploit (it, 2019), the popular penetration testing framework (Metasploit, 2019).

The databases contain a profoundly robust set of facts on how attacks have been carried out. Researching those databases alone will be a guiding factor in how defences should be built. The limiting factor might be the associated costs in implementing every single possibility to protect the assets of an organisation.

As a second database, the Hackmageddon source was selected. The page produces a valuable resource on attack timelines and statistics (Hackmageddon, 2019).

2.2.2.1 Manual Research

Manual research on cyber-attacks is a very time-consuming task. Even though there are a plethora of resources on the Internet, sifting through the data, organising it and dismissing incorrect or imprecise entries is not recommended.

Example of two very public attacks:

WannaCry aka WannaCrypt

Date:	12.05.2017	**Attack Vector(s):**	E-Mail, Dropbox links, Advertisements
Description:	WannaCry[1] was a Ransomware worm impacting the Windows operating system. The worm used two NSA-leaked tools (EternalBlue, DoublePulsar) and it is believed that systems in 150 countries were impacted.		

Petya aka NotPetya

Date:	June 2017	**Attack Vector(s):**	MEDoc software, SMB exploit, File shares
Description:	Petya[2] was a Ransomware worm impacting the Windows operating system. The worm used the EternalBlue exploit and systems in over 64 countries were impacted.		

Example of attacks targeting large corporations holding a large amount of user data:

Yahoo

Date:	late 2014	**Attack Vector(s):**	Forged cookies
Description:	In the Yahoo hack,[3] there were 500 million Yahoo E-Mail addresses exposed. In Aug 2013, there were all 3 Billion E-Mail addresses impacted, but it is not clear how the attackers gained access. (Outpost 24, 2019)		

[1] (Malware Wiki, 2019)

[2] (Malware Wiki, 2019)

[3] (Vindu & Nicole, 2019)

Marriot			
Date:	2014 – Sep 2018	**Attack Vector(s):**	Unknown
Description:	The Marriot hack (Nicole, Amie, & Adam, 2019) impacted 500 million customers. Data has never resurfaced, and there are strong believes that a state actor executed the hack. (Outpost 24, 2019)		

Adult Friend Finder

Date:	2016	**Attack Vector(s):**	LFI (Local File Inclusion) breach
Description:	The 2016 Adult Friend Finder hack exposed data of 400 million accounts. There was also a hack the previous year, but that did not expose as many account records. (Outpost 24, 2019)		

Equifax

Date:	July 2017	**Attack Vector(s):**	Vulnerability in Apache Struts
Description:	The Equifax hack exposed 143 million customers. (Outpost 24, 2019)		

Alteryx

Date:	July 2017	**Attack Vector(s):**	Publicly accessible AWS S3 storage cache
Description:	The Alteryx hack exposed 123 million U.S. households. (Outpost 24, 2019)		

Target

Date:	Dec 2013	**Attack Vector(s):**	Cash Registers
Description:	The Target hack exposed 110 million customers. (Outpost 24, 2019)		

Various

Date:	Aug 2014	**Attack Vector(s):**	SQL Injection
Description:	The company Hold Security reported 1.2 billion stolen usernames and passwords from 420’000 websites. (Outpost 24, 2019)		

Sony PSN

Date:	April 2011	**Attack Vector(s):**	SQL Injection
Description:	The Sony PSN hack impacted 77 million accounts. (Outpost 24, 2019)		

Sony PSN

Date:	April 2014	**Attack Vector(s):**	Malware, SMB Worm, poor infrastructure

			management (firewall, routers and servers)
Description:	In November 2014 Sony Pictures Entertainment (Wikipedia, 2019) was hit by malware, and around 100 terabytes of data were stolen. (Outpost 24, 2019)		

Adobe

Date:	Oct 2013	**Attack Vector(s):**	Security practices (password management)
Description:	The Adobe hack impacted 150 million accounts. There was also source code of Adobe products stolen. (Outpost 24, 2019)		

2.2.2.2 Attack vectors from vendor reports

Assessing vendor data seems to be providing a more focused approach without the need to verify each piece of data manually. The list of vendors is not exhaustive, but the purpose of the extracted data is to show the introduced variance.

Source	Year	Attack vector(s)	Type
FireEye[4]	2019	• Business email • Spear Phishing	Phishing
Checkpoint[5]	2019	• Cryptomining • Ransomware • Cloud Risks	Cryptomining, Infrastructure
Cisco[6]	2019	• Email	Phishing
Microsoft[7]	2018	• Phishing • Protocol downgrading • Cookie hijacking • Cross-site-scripting	Phishing, Web
Forcepoint[8]	2019	• Vulnerabilities in cloud infrastructure	Infrastructure
Kaspersky[9]	2019	• Supply Chain attacks • Online payment systems • Planting of physical devices inside the perimeter	Supply Chain, Web, Infrastructure, Social Engineering

[4] (FireEye, 2019)

[5] (Checkpoint, 2019)

[6] (Cisco, 2019)

[7] (Microsoft, 2019)

[8] (Forcepoint, 2019)

[9] (Kaspersky, 2019)

		• Web API • Social Engineering	
Symantec[10]	2019	• Exploit AI systems • Attacks based on 5G networks • IoT devices (DDoS attacks) • Data in transit attacks • Supply chain attacks (OS, UEFI, Firmware, hardware)	AI, Infrastructure, Supply Chain
BAE Systems[11]	2019	• Online payment systems • Exploit AI systems • Cryptocurrency	Web, AI, Cryptocurrency

IBM[12]	2018	• LFI attacks
		• Ransom worm
		• Insider
		  ○ Misconfiguration
		  ○ Phishing
		  ○ Weak password
		  ○ Personal devices
		• Cryptocurrency
			Phishing, Infrastructure, Cryptocurrency

Table 1: Attack vectors from vendor reports

Source: Table produced by the author

[10] (Dr. Hugh & Steve, 2019)

[11] (BAE Systems, 2019)

[12] (IBM, 2019)

IBM also delivers visual representations of their data and also highlighting that Insider threats in the form of misconfigurations constitute a significant threat to organisations.

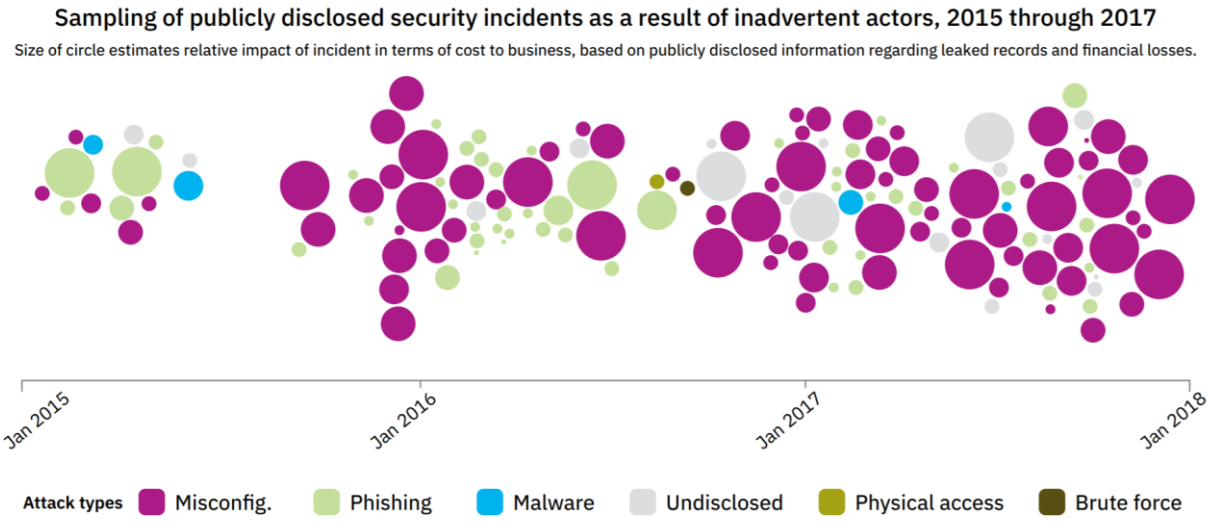


Figure 2: Inadvertent Insider / Human error (IBM, 2019)

Source: Screenshot taken out of the IBM report

As we can see from *Table 1: Attack vectors from vendor reports*, vendors also do not make the analysis much more straight forward. There is no universal form of KPI's used to communicate the threats. It is then upon the reader to capture the produced output, categorise it and then apply it to the internal risk view.

However, it is the view of highly professional cybersecurity organisations. If the variously reported attack vectors are grouped, then we get the following focus areas:

Type	Score
Infrastructure	5
Phishing	4
Web-based attacks	3
Cryptocurrency	3
Social Engineering	2
Exploiting AI technologies	2
Attacks on the supply chain	2

Table 2: Vendor attack vectors

Source: Table produced by the author

Other cybersecurity attack resources worth mentioning:

- CSIS - the focus is on government, tech companies and more significant financial losses (CSIS, 2019)
- CFR - Cyber Operations Tracker (CFR, 2019)

2.2.2.3 **Disclosed vulnerabilities**

Other relevant identified resources are vulnerability databases. If an organisation is using software products to provide its core business, then we must assume that these products will impact the risk exposure of these organisations as well. That is reflected by the importance of these products for the organisation to conduct business. An organisation, therefore, is well advised to consider threats against their products. An example of a public vulnerability database is shown below (Özkan, 2019).

CVSS Score Distribution For Top 50 Products By Total Number Of "Distinct" Vulnerabilities

	Product Name	Vendor Name	Number of Total Vulnerabilities	# Of Vulnerabilities									Weighted Average	% Of Total								
				0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+		0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9+
1	Debian Linux	Debian	2449		25	93	54	647	475	470	552	7	126	6.40	0	1	4	2	26	19	19	23	0	5
2	Linux Kernel	Linux	2207	1	91	330	47	680	135	178	613	6	126	5.90	0	4	15	2	31	6	8	28	0	6
3	Mac Os X	Apple	2196	1	20	153	21	364	265	468	434	10	460	7.00	0	1	7	1	17	12	21	20	0	21
4	Android	Google	2149		2	58	13	456	177	155	464	28	796	7.70	0	0	3	1	21	8	7	22	1	37
5	Firefox	Mozilla	1771		3	55	8	323	343	224	298	1	516	7.30	0	0	3	0	18	19	13	17	0	29
6	Chrome	Google	1763			14	1	368	253	379	536	1	211	7.10	0	0	1	0	21	14	21	30	0	12
7	Iphone Os	Apple	1637		28	110	21	309	171	565	143	5	285	6.70	0	2	7	1	19	10	35	9	0	17
8	Ubuntu Linux	Canonical	1581		27	91	38	426	298	281	322	4	94	6.30	0	2	6	2	27	19	18	20	0	6
9	Windows Server 2008	Microsoft	1187		76	105	10	174	42	98	341	9	332	7.10	0	6	9	1	15	4	8	29	1	28
10	Acrobat	Adobe	1130				1	171	49	49	30		830	8.90	0	0	0	0	15	4	4	3	0	73
11	Flash Player	Adobe	1070			1		41	57	23	57	1	890	9.40	0	0	0	0	4	5	2	5	0	83
12	Windows 7	Microsoft	1047		74	106	7	159	30	89	308	6	268	7.00	0	7	10	1	15	3	9	29	1	26
13	Safari	Apple	1026		3	18		214	99	416	49	3	224	7.10	0	0	2	0	21	10	41	5	0	22
14	Internet Explorer	Microsoft	979		1	30		109	19	32	180	2	606	8.70	0	0	3	0	11	2	3	18	0	62
15	Opensuse	Opensuse	915		15	40	45	182	209	161	166	1	96	6.50	0	2	4	5	20	23	18	18	0	10
16	Acrobat Dc	Adobe	912				1	188	64	76	15		568	8.40	0	0	0	0	21	7	8	2	0	62
17	Acrobat Reader Dc	Adobe	912				1	188	64	76	15		568	8.40	0	0	0	0	21	7	8	2	0	62
18	Acrobat Reader	Adobe	878			4	2	158	50	45	34		585	8.60	0	0	0	0	18	6	5	4	0	67
19	Thunderbird	Mozilla	869			20	2	123	125	98	141		360	7.90	0	0	2	0	14	14	11	16	0	41
20	Enterprise Linux Desktop	Redhat	859		5	51	15	222	149	157	178	1	81	6.50	0	1	6	2	26	17	18	21	0	9
21	Windows Vista	Microsoft	828		8	31	3	118	27	54	291	9	287	7.90	0	1	4	0	14	3	7	35	1	35
22	Windows Server 2012	Microsoft	821		83	109	12	109	38	81	206	4	179	6.50	0	10	13	1	13	5	10	25	0	22
23	Enterprise Linux Server	Redhat	792		4	34	14	212	137	158	165	1	67	6.50	0	1	4	2	27	17	20	21	0	8
24	Windows 10	Microsoft	775		84	110	13	145	19	85	182	3	134	6.20	0	11	14	2	19	2	11	23	0	17
25	Windows 8.1	Microsoft	757		80	106	10	99	31	79	181	4	167	6.50	0	11	14	1	13	4	10	24	1	22
26	Enterprise Linux Workstation	Redhat	757		4	26	14	207	130	149	160		67	6.50	0	1	3	2	27	17	20	21	0	9
27	Windows Xp	Microsoft	740		1	25	3	74	71	42	282	4	238	7.90	0	0	3	0	10	10	6	38	1	32
28	Seamonkey	Mozilla	697			11	2	130	88	72	61		333	7.90	0	0	2	0	19	13	10	9	0	48
29	Mac Os X Server	Apple	640		6	48	6	91	109	170	137	2	71	6.70	0	1	8	1	14	17	27	21	0	11
30	IE	Microsoft	631			49		86	167	23	140	1	165	7.20	0	0	8	0	14	26	4	22	0	26
31	Windows Rt 8.1	Microsoft	631		44	94	10	87	23	62	160	4	147	6.70	0	7	15	2	14	4	10	25	1	23
32	Firefox Esr	Mozilla	619			7	3	68	73	111	155	1	201	7.80	0	0	1	0	11	12	18	25	0	32
33	Enterprise Linux	Redhat	601		24	48	32	146	109	71	138	1	32	6.00	0	4	8	5	24	18	12	23	0	5
34	JRE	Oracle	600	2	2	28	11	83	186	55	50		183	7.10	0	0	5	2	14	31	9	8	0	31
35	Itunes	Apple	592			5	1	38	13	337	100	1	97	7.50	0	0	1	0	6	2	57	17	0	16
36	JDK	Oracle	591	2	2	29	11	83	185	53	48		178	7.10	0	0	5	2	14	31	9	8	0	30
37	Mysql	Oracle	588		22	23	101	327	44	50	16		5	5.00	0	4	4	17	56	7	9	3	0	1
38	PHP	PHP	588		1	21	4	64	180	76	200	1	41	6.90	0	0	4	1	11	31	13	34	0	7
39	Sunos	SUN	569		14	56	27	115	80	29	189	2	57	6.40	0	2	10	5	20	14	5	33	0	10
40	Wireshark	Wireshark	563			24	32	185	247	7	46	3	19	5.80	0	0	4	6	33	44	1	8	1	3
41	Fedora	Fedoraproject	559		7	24	15	128	145	92	122		26	6.30	0	1	4	3	23	26	16	22	0	5
42	Windows Server 2016	Microsoft	557		80	88	12	116	14	66	101	3	77	5.80	0	14	16	2	21	3	12	18	1	14
43	Edge	Microsoft	530			28		97	15	5	336		49	7.30	0	0	5	0	18	3	1	63	0	9
44	IOS	Cisco	517	1		9	11	40	100	65	250	4	37	7.20	0	0	2	2	8	19	13	48	1	7
45	Windows 2000	Microsoft	514	1		26	5	44	91	24	177	2	144	7.60	0	0	5	1	9	18	5	34	0	28
46	Office	Microsoft	511			6		48	26	10	20	1	400	9.10	0	0	1	0	9	5	2	4	0	78
47	Imagemagick	Imagemagick	497			2		271	41	85	90		8	6.00	0	0	0	0	55	8	17	18	0	2
48	Solaris	SUN	465		8	47	9	111	49	21	162		58	6.60	0	2	10	2	24	11	5	35	0	12
49	Watchos	Apple	462			18	2	74	41	133	60	3	131	7.40	0	0	4	0	16	9	29	13	1	28
50	Windows 2003 Server	Microsoft	444		2	13	4	28	48	26	191	3	129	7.90	0	0	3	1	6	11	6	43	1	29

Figure 3: Top 50 products by the total number of vulnerabilities based on CVSS scores

Source: Screenshot of the www.cvedetails.com web page (Özkan, 2019)

2.2.2.4 Mitre Att&ck

As Adam Glick points out in his published article (Glick, 2019) the Mitre Att&ck (Adversarial Tactics, Techniques & Common Knowledge) Framework (Mitre, 2019) has become an invaluable resource of attack details, especially regarding Advanced Persistent Threats (APT). He further mentions that the framework has managed to provide a holistic view of the attack lifecycle, providing “a real-world understanding of the attacker’s intent” (Glick, 2019).

The Framework (Mitre, 2019) is a brainchild of Mitre and is the result of observing attacks from around the world and describing the tactics, techniques and procedures deployed. Essentially it is a threat and model knowledge base.

The Framework is presented as a matrix and shows the relationships between attacker tactics and techniques to penetrate defences and to acquire the intent of the attackers. The top-level view comprises the adversary tactics and is split up into 11 different groups as shown in the following graph.

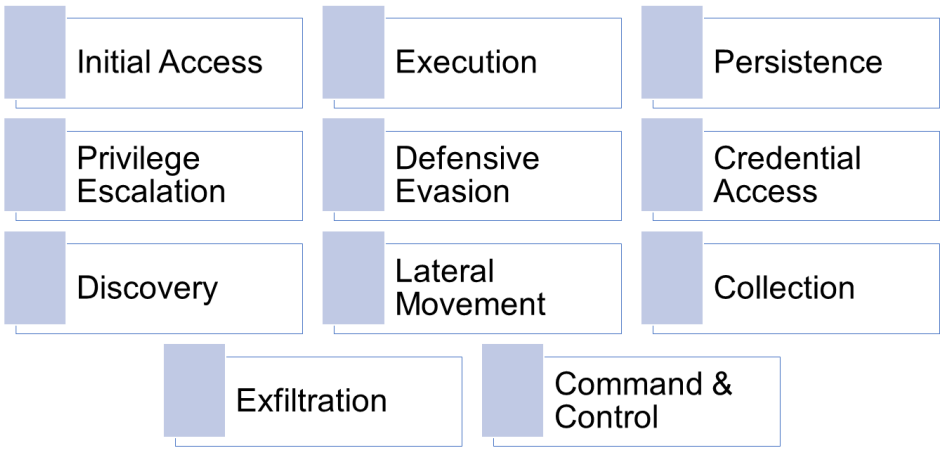


Figure 4: Mitre Att&ck attack stages

Source: (Mitre, 2019)

Every tactic holds a list of techniques and represents the way the attacker is achieving its tactics goal. The complete list cannot be shown within this chapter, but a full extract can be found in Appendix 7.1.

Privilege Escalation	Defense Evasion	Credential Access
Access Token Manipulation	Access Token Manipulation	Account Manipulation
Accessibility Features	BITS Jobs	Bash History
AppCert DLLs	Binary Padding	Brute Force
AppInit DLLs	Bypass User Account Control	Credential Dumping
Application Shimming	CMSTP	Credentials in Files
Bypass User Account Control	Clear Command History	Credentials in Registry
DLL Search Order Hijacking	Code Signing	Exploitation for Credential Access
Dylib Hijacking	Compiled HTML File	Forced Authentication
Exploitation for Privilege Escalation	Component Firmware	Hooking
Extra Window Memory Injection	Component Object Model Hijacking	Input Capture
File System Permissions Weakness	Control Panel Items	Input Prompt
Hooking	DCShadow	Kerberoasting

Figure 5: Mitre Att&ck techniques details

Source: (Mitre, 2019)

The data has also been linked to adversary groups and to software being used in attacks. The Framework collects a wide range of data from publicly available data such as:

- Threat intelligence reports
- Conference presentations
- Webinars
- Social media
- Blogs
- Open source code repositories
- Malware samples

Next to present data to better understand adversaries, the Framework also provides additional benefits to its user base:

- Attack enumeration providing detection capabilities
- Best practices for investigations
- It is a collaboration project

The current database of the Att&ck Framework (Release October 2018) contains the following three main structures. These structures are Techniques, Groups and Software. The entities from each of these structures are shown in the following table.

Techniques	Software	Groups
Entry Title	Techniques Used	Techniques Used
Tactic	Aliases	Alias Descriptions
Description	Groups	Software
Mitigation	Contributors	Contributors
Detection		
Examples		
Platform		
Data Sources		
Permissions Required		
Effective Permissions		
Defense Bypassed		
System Requirements		
Network Requirements		
Remote Support		
Contributors		

Table 3: Mitre Att&ck parameters

Source: Data extracted by the author

The first relevant data point within the data set investigated, is the parameter “x_mitre_data_sources”. This value collects all log sources relevant to detect all attack techniques as listed as in the Framework. That parameter is a compelling reference to anyone building detection capabilities against adversaries. Since the Mitre Att@ck Framework becomes the de facto standard for adversarial techniques and tactics, which includes the most relevant attack techniques in the cybersecurity world, it also means, that it includes all relevant know-how needed to define every organisation's detection capabilities needs.

It needs to be emphasised why this find is so fundamentally important. By investigation of the most advanced attacks in the history of cybersecurity, data has been gained to show how these attacks were executed. Thereof detection capabilities have been postulated to allow any organisation to be able to detect these attacks potentially. This is evidence enough that the data displayed within the Mitre Att&ck Framework reflects the most effective detection capabilities to date.

The data is extracted from the full JSON extract found on the Mitre (Mitre, 2019) website. The command used for the json manipulation:

```
> jq '.objects[].x_mitre_data_sources' enterprise-attack.json|grep -v '\['|grep -v '\]'|grep
-v null|sed 's/\"//g'|sed 's/\,//'|sort|uniq -c|sort -nr
```

The data produced is shown in the below table:

Count	Data Sources
157	Process monitoring
90	File monitoring
87	Process command-line parameters
41	API monitoring
37	Process use of network
34	Windows Registry
32	Packet capture
28	Authentication logs
24	Netflow/Enclave netflow
19	Windows event logs
18	Network protocol analysis
18	Binary file metadata
17	DLL monitoring
12	Loaded DLLs
9	System calls
9	Malware reverse engineering
8	SSL/TLS inspection
7	Network intrusion detection system
7	Anti-virus
6	Data loss prevention
5	Application logs
4	Windows Error Reporting
4	Web proxy
4	User interface
4	Network device logs
4	Kernel drivers
4	Host network interface
4	Email gateway
3	Third-party application logs
3	Services
2	Web logs
2	MBR
2	Mail server
2	Environment variable
2	Detonation chamber
2	BIOS
1	WMI Objects
1	Web application firewall logs
1	VBR
1	Sensor health and status
1	PowerShell logs
1	Named Pipes
1	EFI
1	DNS records
1	Disk forensics
1	Digital certificate logs
1	Component firmware
1	Browser extensions
1	Asset management
1	Access tokens

Table 4: Mitre Att&ck Data Sources

Source: Data extracted by the author

The graphical representation of the above table is shown in the next graph:

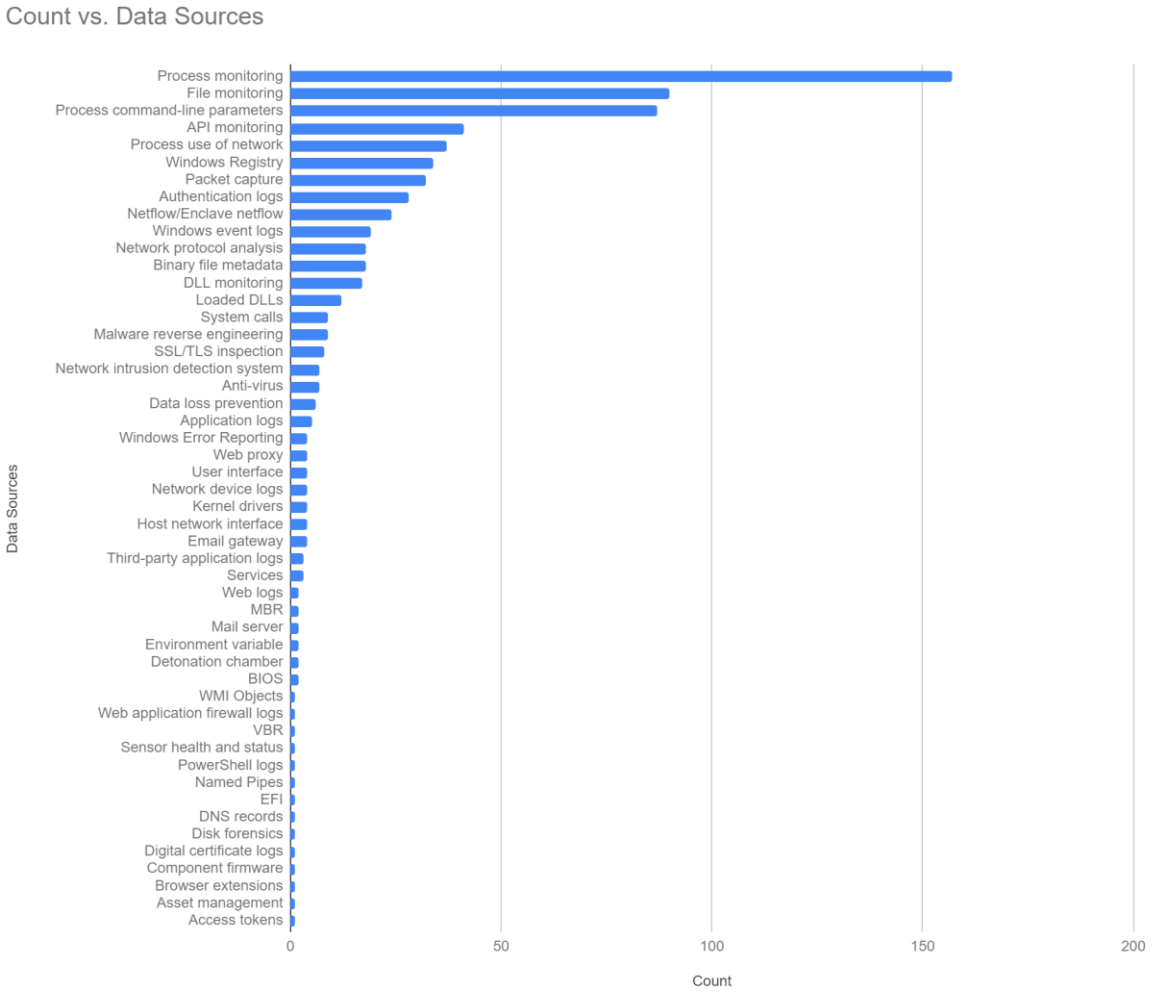


Figure 6: Mitre Att&ck Data Sources

Source: Data extracted and graphed by the author

The list produced is by no means equating the quality of detection capabilities but a show of numbers of possibilities to detect attacker techniques. However, it highlights how valuable a data source can be for an organisation in regard to how many different techniques can be detected by focusing on a specific data source.

It becomes quite apparent that the focus on detecting attacks should be with the most valuable data sources available within the organisation. The following list contains a ranking of the top 10 of the most listed data sources for all listed attack techniques.

1. Process monitoring
2. File monitoring
3. Process command-line parameters
4. API monitoring

5. The process uses of network
6. Windows registry
7. Packet capture
8. Authentication logs
9. Netflow
10. Windows Event logs
11. Network protocol analysis

Some interesting findings are that network log data only comes in fifth place, log data from infrastructure services such as E-Mail and Web proxy logs are not as relevant in the numbers of detection capabilities as recommended by vendors. Exabeam, for example, mentions in their online SIEM architecture advisory following log sources: IDS, Antivirus, DLP, VPN, Web Filters, Honeypots and Firewalls (Exabeam, 2019). These log sources are not even mentioned in the top 10 (Table 2.) of the Mitre Att&ck log sources.

It would be false to assume that Exabeam is not right with their proposal, but it would be wrong not to consider the actual data of the Framework. There are different approaches to solve a problem, but there must also be a logical structure and reasoning behind the recommended measures. At this stage, it must be assumed that Exabeam is recommending its implementation based on its customer base and on the experience of their workforce. That data is unfortunately not available for research.

The advantage of selecting log sources based on real attack data is that it can be directly related to. If an organisation is utilising equipment with SCADA controllers, then it would want to protect its assets according to past experience. The company would want to consult past attacks on SCADA controllers and would want to implement the same protective measures without detour.

What cannot be identified within the Framework are the means to reference external standards. From the point of the author, there is still a distinctive gap between the Mitre Att&ck Framework and the business side of organisations. The Framework is mainly addressing the technical experts in the field of cybersecurity. However, it does not address a vital audience relevant to the decision-making process for cybersecurity programs. The Framework is not addressing the industry related business requirements and providing decision makers with a link to existing established processes and frameworks. The reference goes to the various industry standards, frameworks or government requirements such as NIST CSF, ISO/ICE 2700x and COBIT 5. Organisations have invested a significant capital on the implementation of these standards and are required to project cybersecurity risks against their relevant framework. The author sees here a great potential to close that gap and to include the decision makers in the Mitre Atta&ck Framework.

Another identified gap is the added essential target industries. Most of the Framework groups recorded list a number of targets in the form of industries. For example, the group APT18 lists as targets: technology, manufacturing, human rights groups, government and medical (Mitre Att&ck, 2019). That data cannot be queried and needs to be manually extracted across the whole dataset.

2.2.2.5 **Hackmageddon**

The Hackmaggedon platform is collecting data from attacks from around the world (Hackmageddon, 2019). The data contains the date of when the attack was executed, the tar-

get of the attack, a description, how the attack was executed, target classification, attack classification and the country information. The dataset for 2018 contains 1337 recorded attacks and provides a more detailed view of targets and methods used.

The data were analysed in a drill down fashion, and its findings are presented in several graphs and tables. The analysis also showed that the data is not directly relatable to the data extracted through the Att&ck Framework. The author of Hackmageddon selected a different set of definitions and terminologies. The author has chosen to report data on four categories by the names of Cyber Crime, Cyber Espionage, Cyber Warfare and Hacktivism. The source for these categories cannot be identified. The data is then further split into a separate definition of attack techniques and targets. The target classification is taken from the International Standard Industrial Classification of All Economic Activities (ISIC) as referenced on the Hackmageddon website (Hackmageddon, 2019). The terminologies for the categories and the techniques to make sense, and a cybersecurity professional can relate to them. The difficulty arises in associating the terms used with other datasets available. This is not a problem of Hackmageddon, and if the research was conducted in a different sequence, then that finding would have been stated there as well. It merely shows that a wealth of fantastic data is produced in an insular fashion and it adds complexity when data needs to be compared.

The following graph shows the distribution of recorded attacks based on intention. As discussed, the data in itself can provide the reader with value. For the sake of this research, we cannot directly reference it back to the findings of the Mitre Att&ck Framework.

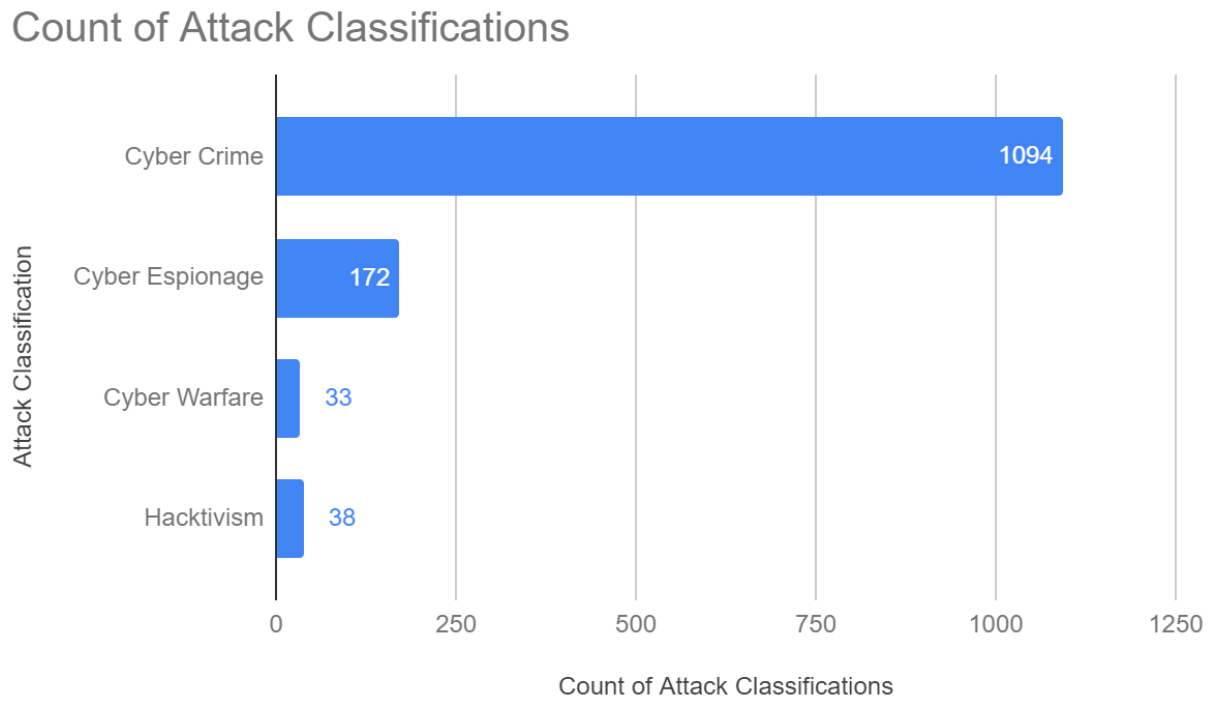


Figure 7: Hackmageddon 2018 Attack Classifications

Source: Data extracted and graphed by the author

The data of Hackmageddon becomes more familiar when investigating the target classification of their dataset. The data has been visualised in the following graph:

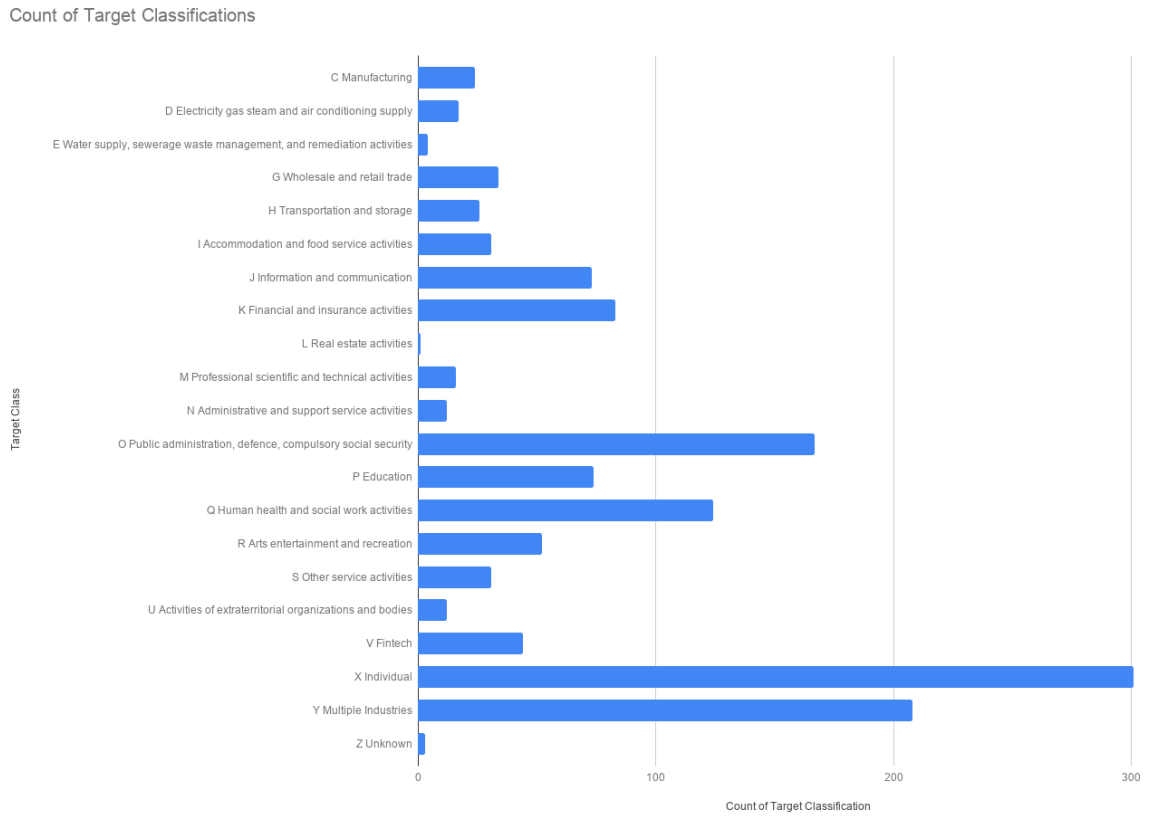


Figure 8: Hackmageddon 2018 Target Classifications

Source: Data extracted and graphed by the author

The data collected by Hackmageddon shows most of the attacks are targeted against individuals. By reviewing the dataset, the association can be made who these individuals are. The most significant portion of 86 is single individuals not further specified. The next group lists Android users as targets and are followed by several operating system platforms, web sites and applications such as Mac, Twitter, Chrome, Facebook or the much-hyped game Fortnite. An extract of the dataset can be seen in the following table showing the top targeted individuals and the count of occurred attacks throughout 2018.

Target	**Count**
Single Individuals	86
Android Users	34
Mac Users	5
Twitter users	5
Chrome Users	3
Facebook Users	3

Fortnite Players	3
Multiple Targets	3
Individuals in the US	2
iOS Users	2
IoT devises Worldwide	2
Mobile Users	2
Python users	2
YouTube Users	2

Table 5: Hackmageddon 2018 Individual Target Classification

Source: Data extracted by the author

The second highest target group are grouped under “Multiple Industries” with 208 occurrences, and then there are government and defence organisations with a count of 167. A complete list with the respective figures is shown below:

Target Classification	**Count**
X Individual	301
Y Multiple Industries	208
O Public administration, defence, compulsory social security	167
Q Human health and social work activities	124
K Financial and insurance activities	83
P Education	74
J Information and communication	73
R Arts entertainment and recreation	52
V Fintech	44
G Wholesale and retail trade	34
I Accommodation and food service activities	31
S Other service activities	31
H Transportation and storage	26
C Manufacturing	24
D Electricity gas steam and air conditioning supply	17
M Professional scientific and technical activities	16
N Administrative and support service activities	12
U Activities of extraterritorial organizations and bodies	12
E Water supply, sewerage waste management, and remediation activities	4
Z Unknown	3
L Real estate activities	1

Table 6: Hackmageddon 2018 Target Classification

Source: Data extracted by the author

By looking at the attack techniques, it shows that the most significant part of the attacks is done via malware. After that, the data becomes diffuse as the data shows repetition such as with a duplicate listing of with Malware or is indifferentiable due to too vague attack type definitions.

Attack	Count
Malware/PoS Malware	376
Account Hijacking	232
Unknown	205
Targeted Attack	167
Malware	66
Vulnerability	44
DDoS	41
Defacement	29
Malicious Script Injection	25
SQLi	10
51% attack	6
Credential Stuffing	6
Malicious code injection	6
>1	5
DNS Hijacking	5
Malvertising	5
Brute-Force	4
Malicious Script	3

Table 7: Hackmageddon 2018 Attack vectors

Source: Data extracted by the author

The Hackmageddon dataset analysis leaves a less than satisfying mark. The source catches the interest of the reader due to the prefabricated graphs shown on the hosting web site. The data even produces country relevant stats and as such becomes very appealing to a researcher or anyone interested in producing attack data graphs. Unfortunately, the data quality expressed through data inconsistencies – just one example: Brute Force (Credential Stuffing) / Brute-Force (Credential Stuffing) / Credential Stuffing – is damping the initial excitement. As already mentioned, the site is using a different taxonomy in reporting its figures than for example the Mitre Att&ck Framework. Initially, the data has been given the benefit of the doubt. After the assessment of the research, it has shown that the taxonomies used are too unique to be of interest to use on a broader spectrum.

Hackmageddon has jumped into an exciting niche and produced a fascinating source of information. It now needs to continuously improve its data to be more attractive to a broader audience.

2.2.2.6 **Exploit-db**

The data provided by Exploit-DB is an extensive database assisting cybersecurity professionals in improving resilience against cyber-attacks. The creators clearly state that the database con-

tains exploits, which can be used by penetration testers or vulnerability researchers, helping to improve security by making that data freely available (Offensive Security, 2019).

The data is structured to assist threat-based research and contains the following search capabilities:

Parameter	Description
Title	Holds relevant information to identify the exploit
Date	Publishing information
CVE	Reference to the CVE
Download	Link to the exploit code
Verified	Provides feedback if another party verified the exploit
Has App	If available, the exploit code also comes with the exploitable software
Attack Types	Attack types such as local, remote, DOS, …
Platforms	An extensive list of platforms to be exploited
Ports	An extensive list of network ports which can be exploited - preferably the software is utilising the ports used.
Author	Lists of authors providing credibility to a provided exploit
Tags	Additional list of filters used based on attack techniques

Table 8: Exploit-DB exploit filters

Source: Data extracted by the author

The database contains 41'155 entries to date. The set covers 59 platforms, each holding exploits for six different types of attacks. The exploit information can either be used directly, or in a 3rd party application such as Metasploit, it also contains source code for the exploitation of the found vulnerability, or it holds proof of concept details for further study. The dataset is using yet another type of definition compared to the previously analysed sets. With this set, it can be strongly assumed that the platforms association are exact due to the nature of the included exploit code, which needs to be tailored to the various platforms being attacked. Mismatching that information would render the exploit code useless. This affirms excellent data integrity concerning platform information. The same can be assumed for the mapping of details to the Common Vulnerability and Exposure (CVE) data sources. The CVE is also a brainchild of Mitre (Mitre, 2019) and is de facto standard for vulnerability information used in many products and services.

The web portal https://www.exploit-db.com/search, unfortunately, does not allow more simple extensive data extraction. The provided data can be accessed via the command line tool "searchsploit" (Offensive Security, 2019).

Data was being analysed by selecting the most useful data fields, which can be related to the previously analysed datasets. The parameters selected were "Attack Types" and "Platforms" as these can be found in both datasets, Mitre Att&ck and Hackmageddon.

The first data pivot was created from the released exploits for all platforms in 2018. In total there were 1936 exploits released for a total of 26 platforms. The most significant portion of released exploits are accounted for by PHP followed by the Windows platform as shown in the following table:

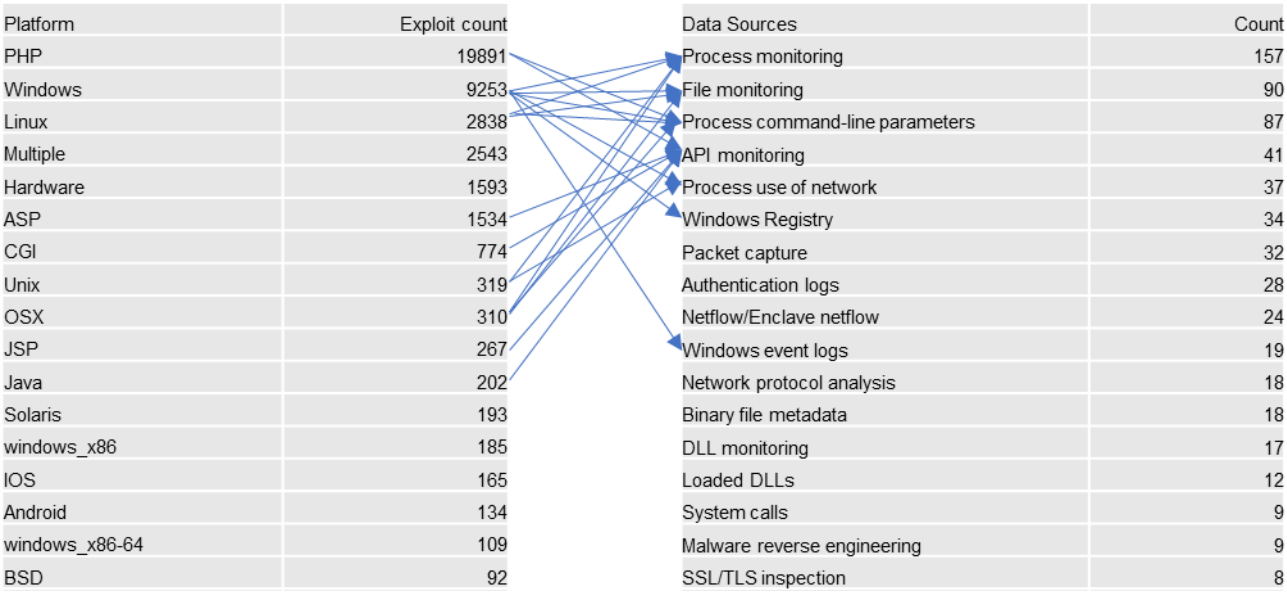
Platform	Count

Grand Total	1936
php	724
windows	370
hardware	201
linux	198
multiple	142
windows_x86	85
windows_x86-64	68
java	33
macos	22
android	16
ios	10
xml	10
asp	9
aspx	9
cgi	7
unix	7
jsp	5
ruby	4
solaris	4
json	3
perl	3
openbsd	2
aix	1
bsd	1
lua	1
nodejs	1

Table 9: Exploit-DB showing all exploits added in 2018

Source: Data extracted by the author

An exciting correlation would be to compare the exploit data with actual attack data. Due to the previously mentioned incompatibility between data-sets, there is no such correlation possible. However, we can reaffirm the results produced by the Mitre Att&ck Framework.



Platform	Exploit count
PHP	19891
Windows	9253
Linux	2838
Multiple	2543
Hardware	1593
ASP	1534
CGI	774
Unix	319
OSX	310
JSP	267
Java	202
Solaris	193
windows_x86	185
IOS	165
Android	134
windows_x86-64	109
BSD	92

Data Sources	Count
Process monitoring	157
File monitoring	90
Process command-line parameters	87
API monitoring	41
Process use of network	37
Windows Registry	34
Packet capture	32
Authentication logs	28
Netflow/Enclave netflow	24
Windows event logs	19
Network protocol analysis	18
Binary file metadata	18
DLL monitoring	17
Loaded DLLs	12
System calls	9
Malware reverse engineering	9
SSL/TLS inspection	8

Figure 9: Exploit-DB targeted platforms versus all Mitre Att&ck data sources

Source: Data extracted and graphed by the author

The above graph is comparing the exploit data made available through the Exploit-DB platform against the identified data sources within the Mitre Att&ck Framework. The graph has been compiled by sourcing all published Exploit DB exploits against the targeted platforms and by extracting all log sources used to defend against attackers in the Mitre Att&ck Framework.

The comparison is not complete; it highlights very clearly the relationship between available exploits and the log sources required to detect attackers. The data allows for a conclusion that the Att&ck Framework data is representing real-world data and the graph also indicates that published exploits are actively used against its targets.

By exploring the Exploit DB further, we also can see a steady stream of exploits being published. The first graph highlights this by plotting the release dates for all platforms and the second graph is focusing on the Windows platform only.

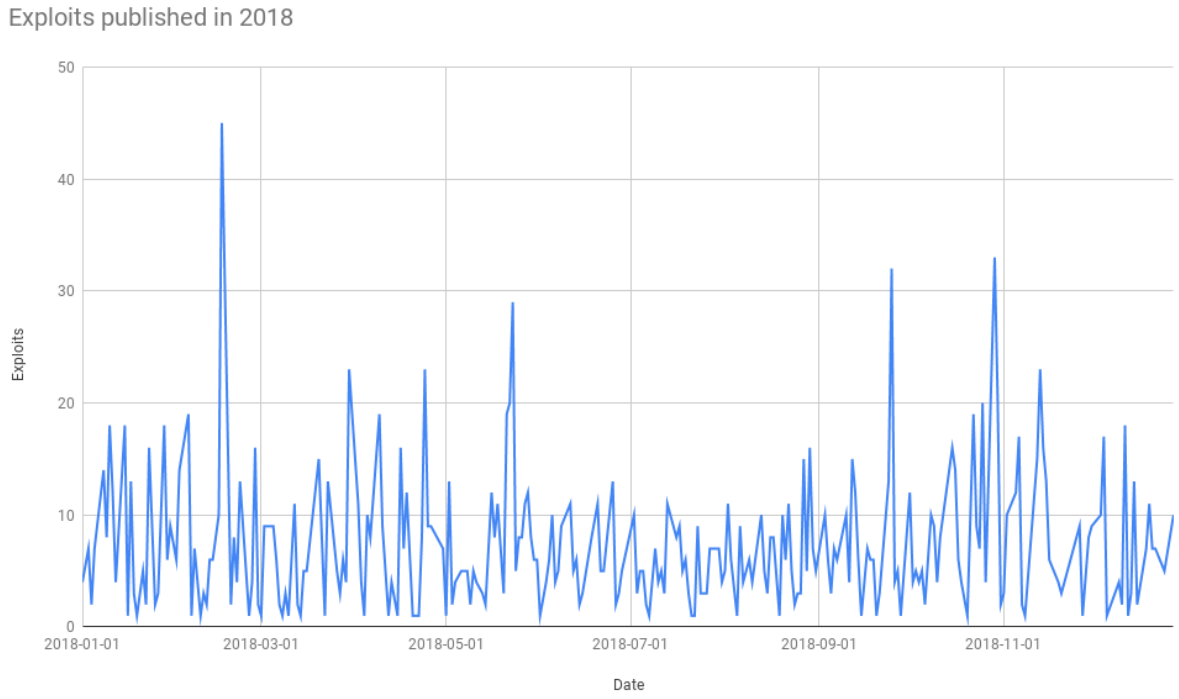


Figure 10: Exploit DB showing all exploits published in 2018

Source: Data extracted and graphed by the author

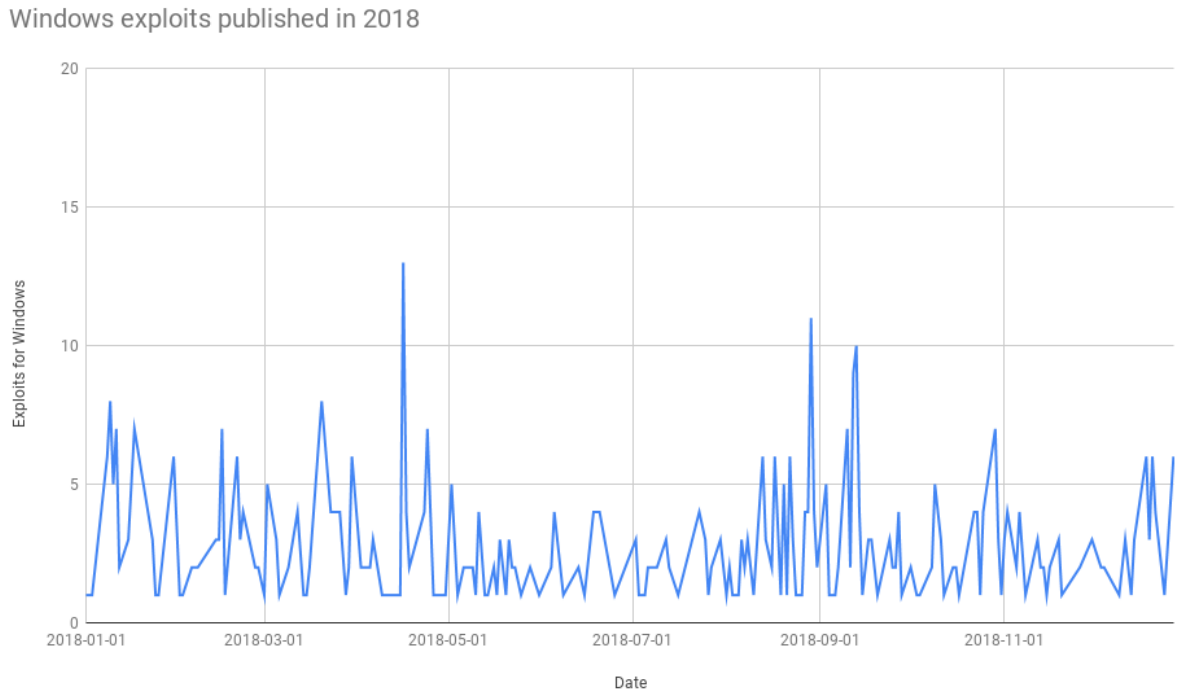


Figure 11: Exploit DB shoeing all Windows exploits published in 2018

Source: Data extracted and graphed by the author

The data published by Exploit DB shows that almost daily, new Windows exploits are being discovered and made public. It is to note that unpublished or 0-Days are not part of the dataset nor are variants or mutations such as used in malware part of the published data. It is also a reminder to protect all platforms in use adequately and to provide adequate detection and visualisations to identify attackers.

By comparing the Exploit DB and the Mitre Att&ck Framework, we were able to conclude that the sources identified by Att&ck are valid.

2.2.2.7 **Summary**

Researching the various datasets provided valuable insights into focus points of adversary detection given the attack data collected by all investigated resources.

The Mitre Att&ck Framework has proven to be the most effective dataset available. By studying the most prolific and advanced cybersecurity attacks, it was possible to create a database not only with the names of the groups and software used, but also techniques on how to detect these attacks by supplying a rule recommendation and the required log sources for the log events to be recorded in. By selecting specific log sources, an organisation can leverage the various detection capabilities the log source allows to implement. In doing so, the organisation can gain a much steeper maturity increase than by adding traditional log sources (Roe, 2019) (Exabeam, 2019). Mainstream cybersecurity vendors are still holding on to traditional log sources (Exabeam, 2019). The real attack data presented by the Mitre Att&ck Framework leads to the conclusion that by focusing on their mentioned data sources, an organisation is more likely to be able to identify an attacker.

There is still a distinctive gap between the Mitre Att&ck Framework and the business side of organisations. The Framework is mainly addressing the technical experts in the field of cybersecurity. However, it does not address a vital audience relevant to the decision-making process for cybersecurity programs. The Framework is not addressing the industry related business requirements and providing decision makers with a link to existing established processes and frameworks. The reference goes to the various industry standards, frameworks or government requirements such as NIST CSF, ISO/ICE 2700x and COBIT 5. Organisations have invested a considerable capital on the implementation of these standards and are required to project cybersecurity risks against their relevant framework. The author sees here a great potential to close that gap and to include the decision makers in the Mitre Att&ck Framework.

A proposed approach is discussed in chapter 4. The proposal is focusing on mapping log sources of the Mitre Att&ck Framework with controls of other standards. This allows for the direct mapping of business requirements to actual attack data information.

The analytics of the available data also highlights one of the huge issues the cybersecurity industry is facing day to day. That is the lack or the wealth of different taxonomies. As Jeff Man points out in his on how an organisation should handle internal communication about cybersecurity (Man, 2019), there is a lack of common ground within the cybersecurity industry. Terminologies and backgrounds differ to a great extent and also from the author's own experience, individuals and companies tend to invent new terminologies all the time.

It was essential to discover that the collected 41'155 exploits by Exploit DB could validate the findings brought forward by the Mitre Att&ck Framework. The Exploit DB data source also once more highlights that enough visibility must be given to protect the platforms in use daily and to have detection and visualisation technology in place to detect any adversaries trying to attack organisations.

By analysing the dataset of Hackmageddon, we get introduced to another set of terms. Not that these were wrong (some mistakes were found) but they differ from the terminologies used by the Att&ck Framework. The obvious challenge is, of course, to assess, which terminology is more suitable for the task at hand. Just because the research started with one dataset, it does not mean that the first one has precedence over the following datasets, but it is a challenge a publisher of data is pushing against the consumer of a source of data. The benefit of utilising a shared taxonomy within the cybersecurity world would much reflect in saving of resources.

2.2.3 Vendors

Compared to the academic research vendor data is more comfortable to access. Vendors, of course, are focused on attracting as many interested parties to consume their ideas and buy their products. Data research was performed with simple web searches in which the top results were farmed and filtered via two parameters.

1. To add credibility to the data sourced, the source needs to be a SIEM vendor listed in the 2018 Gartner SIEM Magic Quadrant.
2. The source needs to hold at least 3 SIEM Use Cases.

The mentioned companies were not contacted to provide more detailed insights into their deployment or recommendation practises. The goal of the research was to utilise the transparent data used by these vendors to acquire new customers.

2.2.3.1 Exabeam

Exabeam recommends Use Cases from three areas and rates them from traditional (compliance) to cutting edge (Insider Threats and Advanced Security) (Exabeam, 2019).

- Compliance: PCI DSS, GDPR, HIPAA, SOX
- Insider Threats: Insider Threats, Privilege Abuse, Trusted host and entity compromise
- Advanced Security: Threat hunting, Data exfiltration, IoT Security

2.2.3.2 Logpoint

Logpoint argues that companies would like to have at their fingertip’s answers to all security and business challenges occurring while doing business (Logpoint, 2019). It is not clearly understood what the marketing department is trying to convey to its customers. There is no mentioning of the methodology used. Logpoint comes straight to the point and recommends following SIEM Use Cases to be implemented. These should provide all the answers relevant to the organisation’s security challenges.

- Authentication activities
- Shared Accounts
- Session activities
- Connection details
- Abnormal administrative behaviour
- Information Theft

- Vulnerability Scanning and correlation
- Statistical analysis
- Intrusion detection and infections
- System change activities

2.2.3.3 **RSA**

RSA provides a Framework to create SIEM Use Cases and a methodology to create a custom Use Case library (Perniola & Gray, 2019).

The described framework in creating Use cases split up into eight distinct steps. These steps are:

- Objective: A description of the need for a Use Case.
- Threat: A clear outline of the threat to defend against.
- Stakeholders: Are the people needed to detect and to respond to threats.
- Data Requirements: The source of data required to detect the threat.
- Logic: A rule to detect the threat inside the data source.
- Testing: Verification that the logic is sound, and threats are being detected.
- Priority: A measure of urgency for the analysts.
- Output: Concern the dashboard and report details.

The framework is rounded off with a workflow detailing the steps required post detection. It lists all required steps such as additional analytics, escalations and protective measures for containment, mitigation and recovery.

The second part is the methodology to create a custom SIEM Use Case library. According to RSA's research, it is to put the mission of the team protecting the organisation's assets at the centre of the design of the cyber defence mechanics.

"What is the mission of our SOC and how can this mission be accomplished in an effective way?" (Perniola & Gray, 2019)

"Adversary modelling – abstract representations of adversary behaviour and characteristics – is central to developing and analysing hypotheses or claims about the effects of technologies, architectural decisions, and/or defender actions on the cyber adversary" (Bodeau & Graubart , 2019).

The RSA team focuses their approach in understanding the adversary activities and on the objectives of the defenders to detect these activities. Their proposed approach consists of:

- Threat identification input from stakeholders such as Risk Management, Business Owners, Security-/Network-/ and Software Architects and anyone relevant in securing data assets of the organisation
- Threat identification input from the SOC
- Attack vectors and TTP's to build attack scenarios
- Use the attack scenarios to build threat indicators

- Map the threat indicators against needed data sources and define detection logic
- Map detection logic against Incident Response Procedures (IRP)

The RSA team summarises that by identifying the organisation's risks and building a SIEM Use Case library, is effectively helping to detect the most relevant threats.

2.2.3.4 **AlienVault**

AlienVault (Roe, 2019) has identified four Use Cases which dramatically improve cybersecurity in any organisation. They claim to have the following four Use Cases implemented -in addition to existing measures- to improve the maturity of detection capability.

- Detect SQL injection attacks via IDS
- Detection of watering hole attacks
- Detection of malware infection
- Compliance status monitoring: HIPAA, GPG13

2.2.3.5 **Splunk**

Splunk (Faircloth, 2016) drives a combined approach of having an extensive Use Case library and having a selection process defined. This approach includes business motivators and a decision process based on goals. That is already a step ahead of the previously analysed vendors, which do not attempt to support a decision process but provide the reader with answers to made-up questions.

Faircloth argues that the goal setters are to be found in the following list:

- Risk frameworks
- The Headlines
- Executive meetings at the golf course
- Keeping up with the Jones Inc.
- Conferences Auditors (based on standards, or Google searching)
- Security Concerns

In his document, he brings forward excellent points one must take into consideration when compiling a list of Use Cases. What we are still missing is a driving consequence on how to handle these goals and put them in order, balance them and give them value relevant to the organisational risks.

The document also includes a description of a framework developing SIEM Use Cases and several SIEM Use Cases. These Use Cases cannot be rated as they have not been put in relevance by Faircloth. The main message of the presentation was not to produce a list of SIEM Use Cases but to provide guidance on how to select Use Cases and to provide some guidance on how to document these.

2.2.3.6 Summary

The results vary in no small extent in which some vendors show a specific approach on how to select SIEM Use Cases. The other group provides a list of recommended Use Cases, and it is assumed that the recommended Use Cases are based on their best practises and professional experience.

By breaking down and simplifying the vendor research data, there is a list of five different approaches as listed in the following table:

Approaches	Count
Compliance	2
Insider Threats	1
Advanced Security	2
Best Practise	1
Custom	2

Table 10: Approaches recommended by the analysed vendors

Source: Data extracted by the author

The table data can be consolidated further and results in three main groups of implementation philosophies:

1. Data supports advocating the existing procedures on how SIEM Use Cases are selected by compliance. This is a safe choice as nobody can argue against an accredited standard.
2. The data shows that the best practices of the respective vendors are used for marketing purposes. The individually listed Use Cases are mostly not matching the competition, which makes it difficult for a customer to assess and understand.
3. The last group supports the build-up of a customer SIEM Use Case library based on identified risks or motivators. This approach matches the general proceedings of a risk management framework (van de Moosdijk & Wagenaar, 2015). It will be the most time consuming out of the listed three approaches but will lead to the most effective results in protecting the assets of an organisation.

The research showed that the market is not aligned and there are different approaches employed by the SIEM technology leaders to protect their customers. Based on this research we can conclude that three out of the five analysed SIEM vendors are supporting the custom based approach. Taking into consideration risk parameters, organisational requirements and the understanding of how adversaries attack their victims.

RSA put out a critical question and confronts its readers with the question of what the mission of the SOC is and how this mission can be accomplished - (Perniola & Gray, 2019). That question brings together the importance and the purpose of this thesis, and that is to mitigate the impact of cyber-attacks.

2.2.4 Cybersecurity Standards and Frameworks

The focus of this chapter is to identify existing mappings between frameworks or standards. As outlined in chapter 3.8, the author has put his focus around the NIST Cybersecurity Framework and used its reach as the basis for the research. Another consideration had to be the Mitre Att&ck Framework.

The research is initiated with the keywords 'NIST' and 'mapping'. The results were analysed, and through iterative processing, the corpus of keywords relevant to this research has increased accordingly. The gain was a list of standards and frameworks either directly addressing cybersecurity or having parts of its controls and measures associated with risks in cybersecurity. The second step included a filtering process to focus on the experience of the author and the perceived popularity of the standards. In this process, a simple hit count on the standards was performed.

In the last steps, the only focus was to select available mappings by the principle of finding the most significant set of standards matching shared mappings. As shown in the following graph, the goal is to find overlaps between mappings relevant for this research.

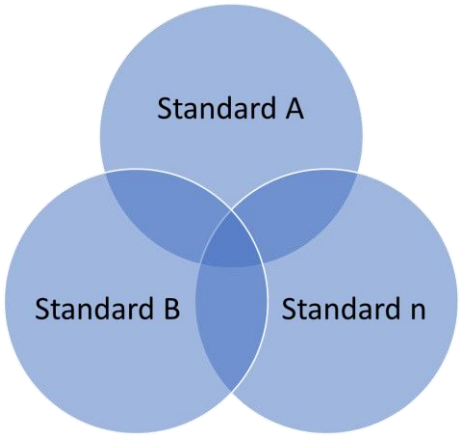


Figure 12: Visual depiction of finding the shared mappings

Source: Graphed by the Author

2.2.4.1 Compile standard and Framework list

The resulting file list of the initial keyword research is used in the identification process of finding the most significant number of shared mappings of specific standards. Each of the following mapping files contains several standards.

- NIST CSF Core (NIST, 2019)
- Minimal ICT Standard (Minimal ICT Standard, 2019)
- CIS v6 (CIS, 2019)
- Tripwire Mapping (Smith, Travis; Tripwire, 2019) (Tripwire, 2019)
- GDPR-ISO/IEC 27001 (Kane, 2019)
- GDPR-ISO27k Mapping (ISO 27001, 2019)
- VDA-ISA EN v4 TISAX (VDA, 2019)

- PCI-DSS and ISO 27001 mapping (Froud, 2019)
- Switch-Cert for Banks (Switch, 2019)
- CIS Controls v7.1 Mapping for Implementation Groups (CIS, 2019)
- AuditScripts (AuditScripts, 2019)
- AuditScripts CSC Manual Assessment Tool (AuditScripts, 2019)
- CIS Controls v7.1 Mapping to NIST CSF (CIS, 2019)

Following standards have been mapped the most: CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO/IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443.

2.2.4.2 Identify mappings

Following mapping files match the list of standards in chapter 2.2.4.1:

- NIST CSF Core (NIST, 2019)
- CIS Controls v7.1 Mapping for Implementation Groups (CIS, 2019)
- AuditScripts (AuditScripts, 2019)
- AuditScripts CSC Manual Assessment Tool (AuditScripts, 2019)
- CIS Controls v7.1 Mapping to NIST CSF (CIS, 2019)

2.2.4.3 Summary

The focal part within this chapter is to identify existing mapping files of frameworks and standards. The identified mapping files will assist in a later stage to perform lookups as required. If for example a specific control from ISO/IEC 27001 has been selected and the goal is to find the matching control within the NIST CSF.

The identification process resulted in the discovery of five mapping files containing a subset of following standards: CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO/IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443.

2.3 Conceptual Framework

The extensive research conducted provided valuable insight into existing SIEM Use Case selection methods, available threat data, standards and frameworks. It allows drawing the first conclusions on the continued design of this research. At the centre is the goal to research the best practise method for the SIEM Use Case selection process. If that is combined with the research data of this chapter, then we can conclude in the following framework for the continuous research.

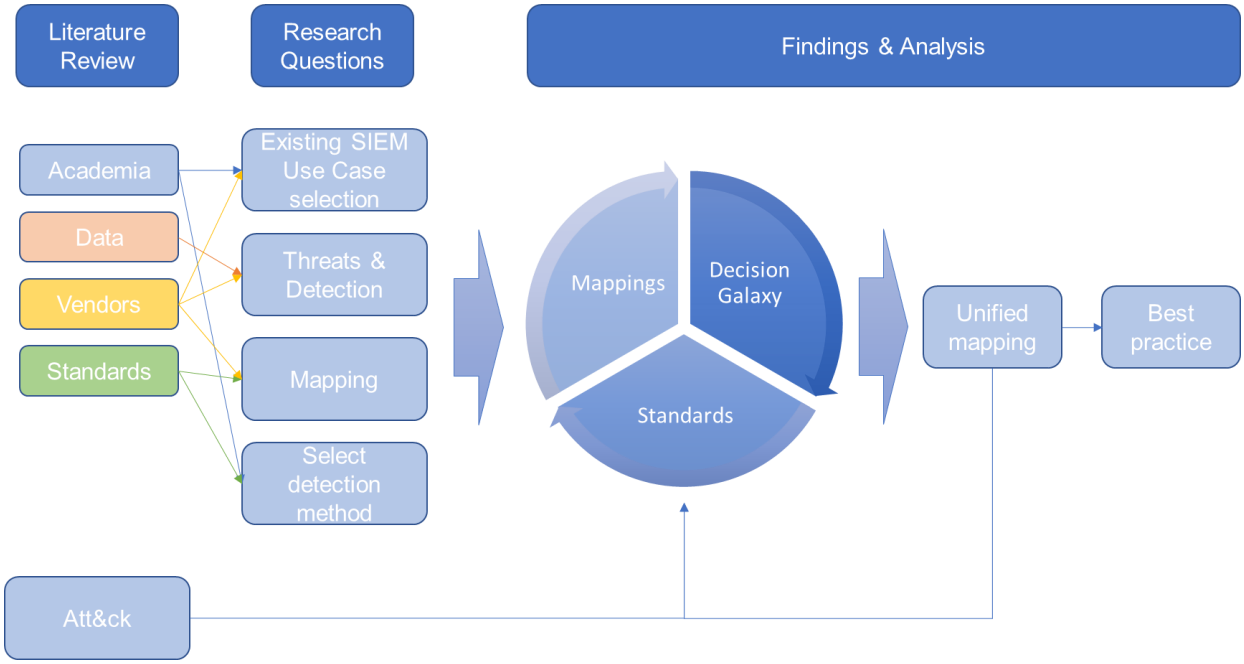


Figure 13: Conceptual framework of the thesis

Source: Graph created by the author

2.4 Summary

The literature review encompasses three significant areas. It was the goal to create a decisive picture of the state of the SIEM Use Case selection process. Overall it can be stated that the results are disconcerting. It was expected that research and the professional industry are well versed in the art on how to discover cyber-attacks. As the data has shown, there is a lack of shared approaches, guidance on how to effectively select the Use Cases relevant for an organisation to protect themselves against attackers.

Academia is not researching a holistic approach to solving the detection problem. Researchers are focused on solving or improving methods in advancing the capabilities of unique technology. However, the authors agree with some of the vendors that a risk-based approach to select SIEM Use Cases and by building a custom Use Case library is the best approach.

The research paper of Jarno van de Moosdijk and Daan Wagenaar (van de Moosdijk & Wagenaar, 2015) states that current standards are not providing enough or specific guidance on use case implementation. The analysis of that research paper relates directly to the problem statement of this thesis.

The Mitre Att&ck Framework has proven to be the most effective dataset available. By studying the most prolific and advanced cybersecurity attacks, it was possible to create a database not only with the names of the groups and software used, but also techniques on how to detect these attacks by supplying a rule recommendation and the required log sources for the log events to be recorded in. By selecting specific log sources, an organisation can leverage the various detection capabilities the log source allows to implement.

There is still a distinctive gap between the Mitre Att&ck Framework and the business side of organisations. The Framework is mainly addressing the technical experts in the field of cyber-

security. However, it does not address a vital audience relevant to the decision-making process for cybersecurity programs. The goal of this thesis is to find a possible answer in closing that gap.

Lastly, manual research to acquire current threats is not recommended as an individual. The amount of time invested, the lack of a unified taxonomy on how to record findings. The conclusion is to rely on large public datasets such as the Mitre Att&ck Framework and contribute back to such a central repository.

3. Design and Methodology

3.1 Introduction

This paper is trying to include the drivers mentioned by Faircloth (Faircloth, 2016), the objective and threat key areas mentioned by Grey and Perniola (Perniola & Gray, 2019) into a unified approach. The aim is to develop a methodology in assisting organisations and cybersecurity professionals in selecting SIEM Use Cases based on a combined approach of utilising the log sources as documented in the Mitre Att&ck Framework and the combination of various cybersecurity standards or frameworks.

3.2 The rationale for the research approach

To fulfil the purpose as outlined in the introduction, a qualitative and quantitative research approach has been chosen. The attention of the research will first fall onto the sub-questions raised.

For the first research sub-question, a combination of theory and factual based review of relevant literature has been conducted. The relevant literature is identified via the following four steps:

- Keyword searches in academic databases
- Expansion of the document corpus based on the inclusion of the references within the identified articles
- Analysis of the abstract to in- or exclude relevant articles
- Full-text analysis of the selected documents

The second sub-question is addressed by quantitative research to assess the relevant figures from the identified literature. The goal is to find similarities, and common ground to either derive a mapping of the data sources or to create a set of arguments to be able to document a possible variant of a data mapping.

The third sub-question is using the results achieved from the second sub-question to propose a solution for mapping the cybersecurity standards to threats and detection capabilities. The data collection supporting mapping and further analytics are conducted with quantitative research. The fourth sub-question connects the findings of the initial mapping, cybersecurity standards and threat to be able to select detection methods. The combined method of quantitative and qualitative research is applied to possibly identify a solution for combining the threats to the standards.

Finally, the main research question ties the previous results into a unified approach by applying quantitative research.

3.3 Research setting/context

Over the last twenty years (Chuvakin, 2019), the development of SIEM platforms has been driven by several large corporations. Based on the authors' professional experience, every product created closed ecosystems of professionals and services to serve customers focused on the features and capabilities of the individual product implemented. It has been a very tool-centric approach in which techniques and processes have not been at the centre of the problems to be solved.

The question is, how the development of SIEM platforms has helped to detect attackers better and how to drive these detection capabilities in a structured way forward. Which parameters have been helping the selection process and how has this improved the capability to defend against attackers?

This paper tries to:

- research shared approaches of vendors selling SIEM solutions,
- research freely available threat database resources,
- also, conduct academic research in the field of SIEM Use Case selection.

The premise is that by researching the methods employed by well-known cybersecurity, vendors must provide us with the best defence capabilities through empiric result gained by professionals. We further must be able to reflect these methods within the thread databases, which contain the actual attack methods used by attackers – at least the publicly known. We then can compare that data with academic research done in the area of cyber defence.

3.4 Research sample and data sources

The data sources and selection process is documented in chapter 2.2.1 for academic literature. The freely available data sources selection process is documented in chapter 2.2.2, the selection process for standards and frameworks in section 2.2.3 and the vendor source and data collection method is explained in chapter 2.2.4.

3.5 Data collection methods

All data collection is done on the personal workstation of the author and is processed there with standard software products such as Microsoft Excel and Notepad++. Further data analytics was moved into a virtual system, which was hosted on that same workstation. The author is more familiar within a Linux environment to do data processing such as data splitting, merging and performing of basic statistical analytics.

The data collection started off with online resources relevant to the research items investigated. The original files were downloaded from public sources hosted directly by the data producer. Data was then moved into a data processing pipeline suited for various tasks to create the needed data constellation. Both sources and processing are described in the following two subchapters.

3.5.1 Data sources

Enterprise-attack.json	
https://github.com/mitre/cti/blob/master/enterprise-attack/enterprise-attack.json	
22.02.2019	Downloaded by author

AuditScripts-Critical-Security-Control-Manual-Assessment-Tool-v7.0a.xlsx	
https://www.auditscripts.com/?attachment_id=3816	
14.04.2019	Downloaded by author

AuditScripts-Critical-Security-Control-Master-Mappings-v7.0d.xlsx	
https://www.auditscripts.com/free-resources/critical-security-controls/	
25.02.2019	Downloaded by author

File-exploits.csv	
https://github.com/offensive-security/exploitdb	
17.04.2019	Downloaded by author

CIS-Controls-Version-7.1-Mapping-to-Implementation-Groups.xlsx	
https://www.cisecurity.org/white-papers/cis-controls-v-7-1-mapping-to-implementation-groups/	
10.04.2019	Downloaded by author

CIS-Controls-V7.1-Mapping-to-NIST-CSF.xlsx	
https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/	
10.04.2019	Downloaded by author

Hackmagedddon 2018 Master Table.xlsx	
https://www.hackmageddon.com/2018-master-table/	
23.02.2019	Downloaded by author

2018-04-16_framework_v1.1_core1.xlsx	
https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11	
21.02.2019	Downloaded by author

ICT-Minimum-Standard - Assessment Tool.xlsx	
https://www.bwl.admin.ch/bwl/en/home/themen/ikt/ikt_minimalstandard.html	
21.02.2019	Downloaded by author

NIST SP 800 53 Rev 4.xlsx	
https://nvd.nist.gov/800-53	
10.04.2019	Downloaded by author

3.5.2 Data processing

Attack Data.xlsx
The file is generated out of the file enterprise-attack.json by importing the JSON file into Excel and pivoting the columns x_mitre_data_sources/[0-11] to receive a unique list of data sources. The list produced was also verified by command line processing with the “jq” Linux command.

During the mapping process, it was relevant to verify findings, and therefore the same file was also used to do manual lookups.	
21.04.2019	Generated by author

Use Case Selector.xlsx	
This file is manually created and contains the CIS Controls mapping. The data included are the columns: CIS, CIS Sub-controls, Assets, NIST CSF, Sensor or baseline, Title, Description, Group 1, Group 2, Group3. The data is merged from the files CIS-Controls-Version-7.1-Mapping-to-Implementation-Groups.xlsx and CIS-Controls-V7.1-Mapping-to-NIST-CSF.xlsx. The goal was to merge CIS, CIS Sub-controls, NIST CSF mapping plus the relationship to the Implementation Groups. The data within was then de-normalised on the columns CIS and CSF mapping, and the result was exported into a CSV for use in the application.	
22.04.2019	Generated by author

Attack-CIS-Mapping.[xlsx|csv]	
This file is manually created from the sources Attack Data.xlsx and Use Case Selector.xlsx. This is resulting mapping file combining the Att&ck data to the standard world. The mapping was done partly in keyword matching of the data sources and logical assignment of matching values. The resulting file contains the log sources matching the CIS Subcontrols.	
22.04.2019	Generated by author

CIS Pivot.xlsx	
The file CIS was manually created by extracting the mapping information from the files AuditScripts-Critical-Security-Control-Master-Mappings-v7.0d.xlsx, CIS-Controls-V7.1-Mapping-to-NIST-CSF.xlsx and 2018-04-16_framework_v1.1_core1.xlsx to study the variances between the mapping efforts of CIS, NIST and AuditScripts. The resulting data is shown in tables and graphs within the research paper.	
08.04.2019	Generated by author

CIS_Implementation_Groups.csv	
This file has been manually generated by extracting the CIS, CIS Subcontrol and Group [1-3] columns of the file CIS-Controls-Version-7.1-Mapping-to-Implementation-Groups.xlsx. The file is used for the application.	
17.04.2019	Generated by author

Attack.csv	
This file has been generated by uploading the file Enterprise-attack.json to http://convertcsv.com/json-to-csv.htm. The generated CSV file contained several hundreds of line break errors, most likely due to a limitation of the hosting service. The error is easily corrected by writing a small Perl script (convert_attack_excel_export.pl 7.2.1). The data is written into Attack-export.csv.	
17.04.2019	Generated by online resource, corrected by the author

Attack-export.csv

This file has been generated by the Perl script (convert_attack_excel_export.pl) processing the file Attack.csv and is used for the application.	
17.04.2019	Generated by author

Relationship.csv	
This file has been generated by the Perl script (relationship.pl 7.2.2) by processing the file Attack-export.csv and is used for the application.	
17.04.2019	Generated by author

Industries.csv	
The file has been manually created by extracting text from the file Enterprise-attack.json. The data was unstructured, and data had to be processed in a two-way process. The initial step was to extract the relevant JSON objects with the group name and thereof extract the values holding the unstructured text data with the industry reference. Following that the texts were extracted by manually selecting the industry names. The extracted text was inserted in a three column CSV. The three columns are: Group ID, Industry, Source The source contains the origin of industry mapping. During the data processing, it was noticed that not all groups had industries assigned. These missing were also added by additional research, and the relevant sources were added into the 3rd column of the file.	
23.04.2019	Generated by author

Mapping-CIS-ALL-AuditScripts	
This file is manually generated of the file AuditScripts-Critical-Security-Control-Master-Mappings-v7.0d.xlsx. The data had to be de-normalised for using in the application and contains the columns: CIS, Mapping, name of Standard.	
21.04.2019	Generated by author

Mapping-NIST-ALL	
This file has been manually generated of the file 2018-04-16_framework_v1.1_core1.xlsx. The data had to be de-normalised for using in the application and contains the columns: NIST CSF, Mapping, name of Standard.	
21.04.2019	Generated by author

3.6 Data analysis methods

Data analysis was required in four areas. These areas were data extraction, table design, graphics design and application design. Each area required a different set of tools to achieve the goal. The most challenging part was the application as that not only required the base dataset but also required software development skills and the need to re-format the available data.

3.6.1 Data Extraction

All included data was analysed with adequate methodologies suitable for the task. Data was available mostly in the formats of CSV, XML, PDF, XLSX and JSON. Apart from PDF, all these formats have explicit delimiters allowing for automated processing. The initial data extraction was performed in an automated manner. During the processing, we came across some software limitations such as the end of line insertions in mid data sections. Thus, requiring manual data clean-up of several hundred lines of data.

Data was then validated via pivoting column entries to account for typographical errors and other data inconsistencies. These activities were generally performed either in Microsoft Excel or online with Google Sheets.

Data manipulation also has been done in the command line on a Linux system due to its familiarity with the author. Commands used in that process were: “jq”, “awk”, “grep”, “sed” and “vi”.

All of the described tools are to the knowledge of the author best suited to perform these tasks in an efficient manner and also ensuring data integrity and validity.

3.6.2 Tables

All information as shown in tables has been produced in Microsoft Excel and Google Sheets. The main reason was to produce tables with a consistent layout and producing them with minimal effort.

3.6.3 Graphics

All graphs were produced with either Microsoft Excel, Google Sheets or Microsoft PowerPoint. All tools provided the author with the most efficient ways to create graphics relevant to convey an important message.

3.6.4 Application

The application development was the most challenging part, and it required various components to work together. That said, the application written, is by no means good quality but serves its purpose as a proof of concept study to present the results of this research. For public release, the code requires a complete rewrite.

All tools used within that project were based on the experience of the author to fast prototype a solution resembling the final product somewhat. Following platforms, tools and language have been used for that project:

The underlying operating system is Linux:

```
name -a
Linux ubuntu 4.4.0-145-generic #171-Ubuntu SMP Tue Mar 26 12:43:40 UTC 2019 x86_64 x86_64
x86_64 GNU/Linux
```

As web server serves Apache:

```
apachectl -V
AH00558: apache2: Could not reliably determine the server's fully qualified domain name, us-
ing 127.0.1.1. Set the 'ServerName' directive globally to suppress this message
Server version: Apache/2.4.18 (Ubuntu)
```

```
Server built:   2019-04-03T13:34:47
Server's Module Magic Number: 20120211:52
Server loaded:  APR 1.5.2, APR-UTIL 1.5.4
Compiled using: APR 1.5.2, APR-UTIL 1.5.4
Architecture:   64-bit
Server MPM:     event
  threaded:     yes (fixed thread count)
    forked:     yes (variable process count)
Server compiled with....
 -D APR_HAS_SENDFILE
 -D APR_HAS_MMAP
 -D APR_HAVE_IPV6 (IPv4-mapped addresses enabled)
 -D APR_USE_SYSVSEM_SERIALIZE
 -D APR_USE_PTHREAD_SERIALIZE
 -D SINGLE_LISTEN_UNSERIALIZED_ACCEPT
 -D APR_HAS_OTHER_CHILD
 -D AP_HAVE_RELIABLE_PIPED_LOGS
 -D DYNAMIC_MODULE_LIMIT=256
 -D HTTPD_ROOT="/etc/apache2"
 -D SUEXEC_BIN="/usr/lib/apache2/suexec"
 -D DEFAULT_PIDLOG="/var/run/apache2.pid"
 -D DEFAULT_SCOREBOARD="logs/apache_runtime_status"
 -D DEFAULT_ERRORLOG="logs/error_log"
 -D AP_TYPES_CONFIG_FILE="mime.types"
 -D SERVER_CONFIG_FILE="apache2.conf"
```

The software was written in Perl:

```
perl --version

This is perl 5, version 22, subversion 1 (v5.22.1) built for x86_64-Linux-gnu-thread-multi
(with 73 registered patches, see perl -V for more detail)
```

Following modules and frameworks are included:

Modul/Framework	
CGI	Perl module to process and handle HTML requests and responses (Stein, 2019)
Bootstrap	“Bootstrap is an open source toolkit for developing with HTML, CSS, and JS” (Bootstrap, 2019)
Chart.js	“Simple yet flexible JavaScript charting for designers & developers” (Chart.js, 2019)

3.7 Issues of trustworthiness

During the research following measures have been undertaken to enhance the study, its validity and reliability:

- The Att&ck data is compared to the Exploit DB database to confirm the validity of the Att&ck log sources. The initial motivation of this thesis is to include the Att&ck data, but it was essential also to show the relevance of the published log sources.
- To establish the concept of mappings between standards, the research takes mappings from three credible sources into consideration. The process of creating mappings be-

tween standards is a normal process and is assisting organisations in relating existing internally used standards to other relevant cybersecurity standards or frameworks.

- The research also included academic research on the topic of SIEM Use Case selection. With the goal to create a common ground between what is to be believed the right way in defending against cybersecurity attacks as pictured by the individual vendors in that field and the academia.
- The same is relevant also for the vendor data. It was crucial not to disregard how vendors are recommending their customers protect against cybersecurity attacks.

3.8 Limitations and Delimitations

This paper has used for its research only freely available information. It was not part of the research to let individuals or companies contribute or assist. It potentially could have contributed to achieve better results and to have a better understanding of approaches, recorded data and data quality. In doing so, the focus of this research would have been diluted.

The term “Use Case” is wildly used and the variations of its use in the Cyber Security world include SIEM Use Case, SOC Use Case or Security Incident Response Use Case. This paper will associate “Use Case” for Security Information and Event Management (SIEM).

In this document, we will refer to the detection capabilities as outlined in the Mitre Att&ck framework as SIEM Use Case.

This research assumes that the detection capability can be based on any type of technology. Relevant for this research is that there is a central technical or operational organisation managing the detection or alerts. The technology of centrally managing these alerts is referred to as SIEM in this document. It is essential, however, that this can be any technology and SIEM has been used to adhere to a common understanding. If for example, an organisation has deployed an Intrusion Prevention System (IPS) to detect cyber threats, then this is on par with the referred SIEM.

The author acknowledges that attacks are being run against organisations of all sizes and any number of individuals (The Council on Foreign Relations, 2019) (Hackmageddon, 2019). However, this research does not analyse the effectiveness of current SIEM installations and detection capabilities.

There have been findings of data inconsistencies, but this document does not discuss quality or completeness of any standards or frameworks (for example IKT). The data analysis of the mapping done by 4 different organisations, showed differences in many of the mapped fields. Analysing these differences could potentially be a topic of different research. Mappings can be seen as weak points as the mentioned differences can produce varying results. For that reason, the reader can select the relevant standard for himself and will receive the mapping details as provided by the standard provider.

There is a wide range of established standards and risk management frameworks. The focus of this paper was not to compare the available Frameworks and go through a selection process to select the most suitable. This paper focuses on the NIST CSF as this standard has become relevant within Switzerland for two reasons:

a) The 2016 revision of the FINMA circular 2008/21 (Borboën, Yan; PwC Switzerland, 2019)

b) Minimum ICT Standard released by the Federal Office for National Economic Supply (FONES)

The author does not consider SIEM technology based on machine learning as the all solving solution in defining SIEM Use Cases. Machine learning algorithms are still in their infants and

deployed solutions need to be trained and must have human supervision. Machine learning can be seen as single types of Use Cases, but it is not seen as the solution an organisation needs to deploy to be secure. At the end of the day, these are products, not concepts protecting the most valuable assets of an organisation.

The resulting application has been written as a fast prototype proof of concept to convey the findings of this research. It was not intended to release to the public as is and would need to be rewritten for that purpose. The author is not a software developer but likes to visualise his ideas.

The data from academia could have been much more comprehensive. Due to the defined scope of this research paper, it was not practical to increase the data corpus for academic literature. By also using, the papers on individual detection technology, there could have been a better sample rate of academic writings.

Data sources can also contain data relevant to privacy laws either impacting employees or customers. Since data sources are an integral part of this research, it is essential to state that data privacy will not be discussed. The purpose of this research shall be to provide a methodology in selecting SIEM Use Cases. The selection process as discussed in this thesis should allow reviewing the results by the responsible person or unit for data privacy.

The research is not taking into consideration the costs accumulated for the selected SIEM Use Cases. When producing a list of recommended SIEM Use cases then that selection is most likely impacting the associated cost. It is out of the boundary of this research to provide any financial figures.

4. Findings

4.1 Introduction

The problem statement described the issue that many organisations are struggling with their implementation of SIEM solutions (Perniola & Gray, 2019). One of the main problems being the selection process for the SIEM Use Cases. The author also has mentioned that he himself had 43 discussions in 2018 alone on the topic of the problematic SIEM Use Case selection process. The main issue is that there is no practical guidance on the mentioned selection process.

The reasons given are that various drivers such as risk management, regulators, stakeholders or subject matter experts (SME) can influence the content of the mentioned key areas as Ryan Faircloth points out in his Splunk .conf2016 speech (Faircloth, 2016). All these stakeholders have different views on prioritisation, time pressure and budget issues make it challenging to select and define the Use Case Roadmap (Faircloth, 2016, p. 11).

In the following chapter, the problem statement and the given purpose are analysed regarding the research questions raised.

4.2 Use Case selection

4.2.1 Introduction

The first sub-question directed the focus of this research on the current drivers or focus areas in the selection process for SIEM Use Cases. The following chapters discuss the findings of the individual focus areas.

4.2.2 Focus areas

The term focus areas are used from the work of (1) van de Moosdijk and Wagenaar (van de Moosdijk & Wagenaar, 2015). They identified the following areas: organisations requirements, operational requirements, log management, correlation, alerting, responding and evaluation. As the basis for the evaluation served the IT risk frameworks ISO/IEC 27002, COBIT 5, NIST CSF 1.0, PCI-DSS 3.0 and Standard of Good Practise for Information Security (ISF SoGP). (2) Perniola and Grey have identified the following focus areas: Business Owners, Risk Management and Subject Matter Experts (SMEs) (Perniola & Gray, 2019, p. 24) and finally, (3) Faircloth has assembled a list with following focus areas: Compliance, Security Visibility, Peer Adoption, Process Effectiveness, Tactical Threat, Secure Configuration Management, Special requests and Product Adoption (Faircloth, 2016, p. 5).

The focus areas from these resources have been compiled into a list, normalised and with the result of a combined list of focus areas this research is continuing.

	(1)	(2)	(3)	Combination
Organisation Requirements	X	X	X	Organisation
Operational Requirements	X		X	
Compliance				Regulations
Log Management	X			
Correlation	X			Detection Capabilities
Alerting	X		X	

Response	X			
Risk Management		X	X	Risk Management
Subject Matter Experts		X	X	SMEs
Threats			X	Threats

Table 11: Combined focus area

Source: Compiled by the author

The combined focus areas are:

- **Organisation**: Organisation and business requirements, organisational maturity, prioritisation
- **Regulations**: regulations, standards, compliance
- **Detection**: This includes everything from log sources, aggregation, correlation, alerting and response
- **Risk Management**: Risk Management framework, as initially stated, this work is using the NIST Cybersecurity Framework
- **Subject Matter Experts**: Experts of their respected fields of expertise such as network, operating systems, security and others
- **Threats**: Actual threats such as vulnerabilities and exploits, best practises and sector goals

By combining these, we can compile a SIEM Use Case decision galaxy.

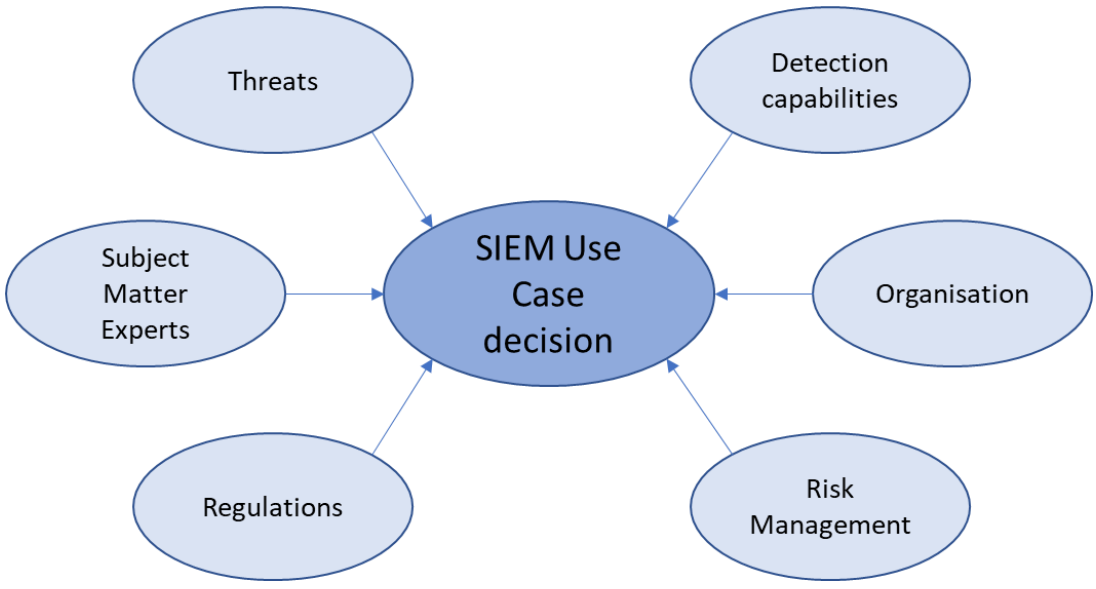


Figure 14: Use Case decision galaxy

Source: Created by the author

4.2.3 Organisation

Within the aspect of the organisational influence on the selection process of SIEM Use Cases, there are the business objectives, the maturity of the organisation and the targeted cybersecurity defences and the prioritisation of the implementation to consider.

The organisational and business requirements, which also consider the aspects of the organisation assets, team sizes and know-how cannot be easily transported into a comprehensible system. Considering all sizes of organisations, this can become an even more complex structure. Standards and frameworks have tried to overcome this difficulty by a model of prioritisation or maturity. The NIST CSF is utilising a measure of implementation tiers (NIST, 2019, pp. 8-11) in which the organisational view on the management of cybersecurity risks are reflected. There are four different tiers with individual maturity on processes, organisational integration and external participation against the management of cybersecurity threats. This allows for high absorption of various requirements and is directly built into an international standard.

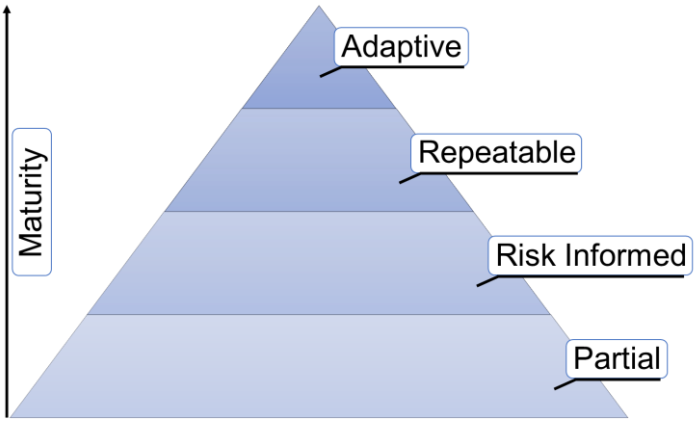


Figure 15: NIST CSF Tier Model (NIST, 2019)

Source: Graphed by the author

A similar approach can be seen with CIS. CIS uses the principle of the implementation group (CIS, 2019). There are three different types of Implementation Groups and are a measure of size, resource and expertise of an organisation to implement Sub-Controls.

Figure 16: CIS Implementation Groups (CIS, 2019)

Source: Graphed by the author

The previous graph shows the three different Implementation Groups and the relationship between them. Implementation Group 1 is considered for home offices or small organisations with low data sensitivity. The Implementation Group 2 focus on helping security teams manage sensitive client or company information. And lastly, the Implementation Group 3 are including the CIS-Subcontrols which reduce the impact of zero-day and targeted attacks.

These methods in grouping organizations can significantly improve the mechanics to select the right SIEM Use Cases according to the maturity or an organization.

4.2.4 Regulations

A list of standards has been identified in chapter 2.2.4.1. These are: CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443. Every organization is associated with at least one industry (International Standard Industrial Classification of All Economic Activities (ISIC)) such as references on the Hackmageddon website (Hackmageddon, 2019).

Each of these standards included a different depth of details on how to protect an organisation against cyber-attacks. Mostly the industry the organisation is operating or serving in (as in suppliers) is defining the standards to follow. In some circumstances it makes sense for an organisation also to implement a standard per choosing, potentially to attract more customers due to the recognisability of a specific standard.

4.2.5 Detection capabilities

In chapter 2.2.2.4 it was established that within the Mitre Att&ck Framework were the most relevant attacking techniques identified based on real cybersecurity attack data. In association with these attacks are also detection methods listed, which can be implemented by any organisation needing protection against these types of attacks. A key ingredient for being able to implement the associated detection methods are the log sources containing the relevant events containing the potential attack information.

There is with the Mitre Att&ck Framework a very potent source of information to base anyone's SIEM Use Case selection process on.

4.2.6 Risk Management

If we argue that the goal of a company is to protect itself against attackers that there is a security program implemented to define that goal and have detailed controls in place to ensure security.

One of the standards is the NIST Cyber Security Framework (CSF) (NIST, 2019) and the following chapter is summarising the content of the CSF as found in the official documentation (NIST, 2019). The NIST CSF is a Cybersecurity Risk Management tool helping an organisation to either describe the current or the future state of its Cybersecurity maturity. These states are known as Framework Profiles. The framework allows to consider the business requirements, risk tolerances, resources of an organisation, sector goals, legal and regulatory requirements, best practices and the risk management priorities. The differences of the current and target state or profiles can be defined as gaps and applied into an action plan part of a broader roadmap to bolster Cybersecurity maturity.

The Framework Core consists of Functions, Categories, Subcategories and Informational References.

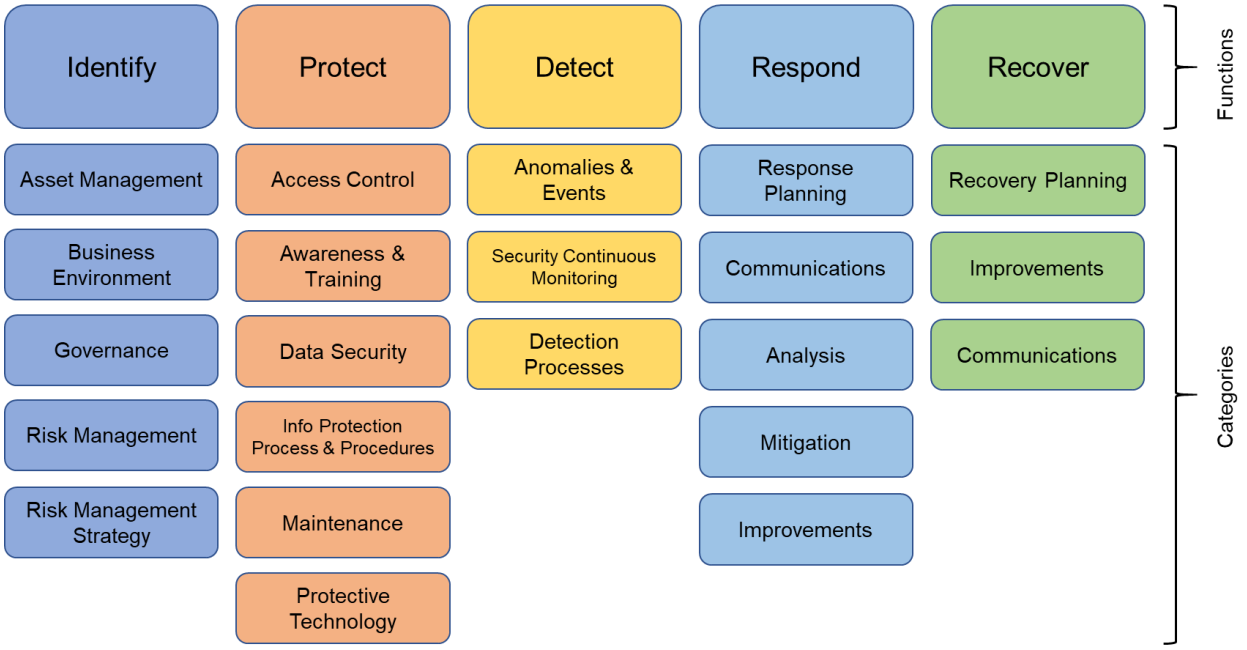


Figure 17: NIST Cyber Security Framework continuous functions (NIST, 2019)

Source: Graph created by the Author

Functions are essential, necessary for cybersecurity activities. These are Identify (ID), Protect (PR), Detect (DE), Respond (RS) and Recover (RC). These simple terms transport a strong management message of its key areas. The Functions can be associated with existing incident management initiatives, and the individual Functions can be directly linked to the impact of investments in bolstering cybersecurity.

Categories are elements of the Functions. These are groups of activities in distinct domains such as Risk Management, Data Security or Recovery Planning.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detection	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Table 12: NIST Functions and Categories

Source: Screenshot (NIST, 2019)

Sub categories tie together the results of technical or management activities. The entries given by the CSF allow for a strong fundament in the own Cybersecurity program and if needed can be extended with own activities not listed.

Informative References link directly to controls or sections of standards, guidelines and best practices. These can be relevant to particular industries and provide methods to gain the needed outcomes as determined in the target profiles. As with Subcategories, the provided mappings to standards, guidelines or best practices are not finite, and anyone is free to extend the list of Informative References.

Function	Category	Subcategory	Informative References
Identify (ID)	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.	ID.AM-1: Physical devices and systems within the organization are inventoried	· CCS CSC 1 · COBIT 5 BAI09.01, BAI09.02 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-2: Software platforms and applications within the organization are inventoried	· CCS CSC 2 · COBIT 5 BAI09.01, BAI09.02, BAI09.05 · ISA 62443-2-1:2009 4.2.3.4 · ISA 62443-3-3:2013 SR 7.8 · ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 · NIST SP 800-53 Rev. 4 CM-8
		ID.AM-3: Organizational communication and data flows are mapped	· CCS CSC 1 · COBIT 5 DSS05.02 · ISA 62443-2-1:2009 4.2.3.4 · ISO/IEC 27001:2013 A.13.2.1 · NIST SP 800-53 Rev. 4 AC-4, CA-3, CA-9, PL-8
		ID.AM-4: External information systems are catalogued	· COBIT 5 APO02.02 · ISO/IEC 27001:2013 A.11.2.6 · NIST SP 800-53 Rev. 4 AC-20, SA-9
		ID.AM-5: Resources (e.g., hardware, devices, data, and software) are prioritized based on their classification, criticality, and business value	· COBIT 5 APO03.03, APO03.04, BAI09.02 · ISA 62443-2-1:2009 4.2.3.6 · ISO/IEC 27001:2013 A.8.2.1 · NIST SP 800-53 Rev. 4 CP-2, RA-2, SA-14
		ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established	· COBIT 5 APO01.02, DSS06.03 · ISA 62443-2-1:2009 4.3.2.3.3 · ISO/IEC 27001:2013 A.6.1.1 · NIST SP 800-53 Rev. 4 CP-2, PS-7, PM-11

Table 13: NIST Subcategories and Informative References

Source: Screenshot (NIST, 2019)

The measurement of all activities within the Subcategories is provided by the Implementation Tier or simply "Tiers" concept. The scale ranges from Tier 1, Partial, up to Tier 4, Adaptive and describe the level of the finesse of cybersecurity risk management practices. Tiers support the decision process and prioritisation of resource expenditure within the cybersecurity program.

Tier 1: Partial

- Risk Management Process – The risk management processes are not formalized, and risks are managed either on the spot or reactive. There is no direct prioritisation of cybersecurity activities out of existing risk management exercises, threats to the organisation or from business requirements.
- Integrated Risk Management Program – Awareness of cybersecurity risk is limited throughout the organisation. Cybersecurity risk management is only implemented in specific needs. Internal knowhow is sparse. There is no transparent process to share cybersecurity information within the organisation.
- External Participation – There is no collaboration with other organisations. No data, best practices or technologies are being shared with anyone. There is no awareness of the cyber supply chain risks of services and products consumed and supplied to others.

Tier 2: Risk-Informed

- Risk Management Process - The risk management processes are approved by management but may not be fully established. There is direct prioritisation of cybersecurity activities out of existing risk management exercises, threats to the organisation or from business requirements.

- Integrated Risk Management Program - Awareness of cybersecurity risk is established throughout the organisation. Cybersecurity risk management is only implemented in specific needs. There is no transparent process to share cybersecurity information within the organisation, but the information is shared informally. There are some considerations in including cybersecurity in organisational objectives or programs. There are no reoccurring risk assessments.
- External Participation - There is some collaboration with other organisations. Selected data, best practices and technologies are being shared, mostly consumed. There is awareness of the cyber supply chain risks of services and products consumed and supplied to others, but there is no process to resolve or act upon those risks formally.

Tier 3: Repeatable

- Risk Management Process - The risk management processes are approved by management and exist as policies. A process is in place which regularly prioritises cybersecurity activities out of existing risk management exercises, threats to the organisation, changes in technology and from business requirements.
- Integrated Risk Management Program – A global process of managing cybersecurity risks is established throughout the organisation. Cybersecurity risk management is well formed in the form of policies, processes and procedures and these are regularly reviewed and updated. There is a transparent process to share cybersecurity information within the organisation and to respond to risks effectively. Organisational assets are continuously monitored against risks. All executives understand and communicate cybersecurity risks and have made that topic part of their respective departments.
- External Participation - There is a collaboration with other organisations. Data, best practices and technologies are being shared and exchanged. There is awareness of the cyber supply chain risks of services and products consumed and supplied to others and has a process to resolve or act upon those risks. There are contracts in place to agree on baseline requirements, governance, policies and monitoring.

Tier 4: Adaptive

- Risk Management Process - - The risk management processes are continuously adapted based on new threats, lessons learned and threat forecasts. A continuous improvement process is in place which cybersecurity activities are adapted to existing risk management exercises, threats to the organisation, changes in technology or to business requirements.
- Integrated Risk Management Program - A global process of managing cybersecurity risks is established throughout the organisation. Cybersecurity risk management is well formed in the form of policies, processes and procedures and these are regularly reviewed and updated. There is a transparent process to share cybersecurity information within the organisation and to respond to risks effectively. Organisational objectives and cybersecurity are well aligned and balanced. All executives value cybersecurity risks at the same level as organisational risks, and budgetary decisions are being adjusted to cater for a balanced risk portfolio. The organisation has embraced cybersecurity risk management and is part of the dynamic growth of its departments, communication and decision making.
- External Participation – It is well understood how the organisation is affecting, impacting and contributing to the ecosystem of its surrounding. There is a robust collaboration with

other organisations. Real-time Data, best practices and technologies are being shared and exchanged continuously to fight new threats and to upkeep readiness against future attack vectors. Responsibility and awareness of the cyber supply chain risks of services and products consumed and supplied to others are fully understood and implements active processes to resolve or act upon those risks. Proactive communication and contracts push strong relationships within its supply change and enforce baseline requirements, governance, policies and monitoring to protect itself and all within its reach.

The strength of the Framework is the break-down of a sophisticated cybersecurity program into digestible portions. The Framework shines with its simplicity during implementation. These phases can be broken down into the following steps:

1. Prioritisation and Scoping – Identification business objectives
2. Assess – Identify regulatory requirements, assets and its vulnerabilities
3. Create Current Profile – Start baseline
4. Conduct Risk Assessment – Assess the likelihood of cybersecurity event
5. Create Target Profile – Set desired goals
6. Gap Analysis – Compare Current and Target Profile, define a roadmap
7. Implementing Action plan – Address gaps

A framework is only valid if it is a dynamic and continuous process to ensure that once established processes and procedures contribute to the current and future cybersecurity resilience of an organisation. Therefore, the CSF is considered as a lifecycle process.

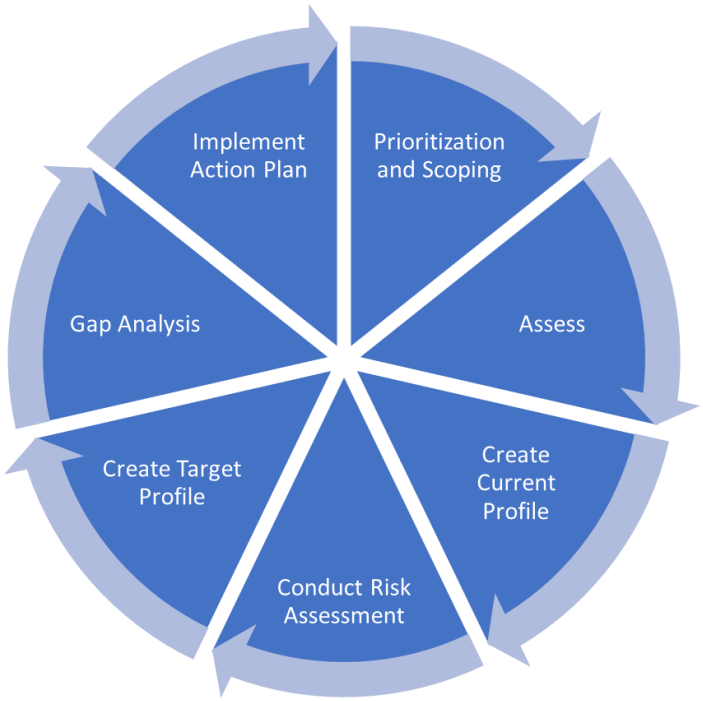


Figure 18: NIST CSF Lifecycle

Source: Compiled and graphed by the author

Taken from the CSF, we have been given focus areas an organisation needs to build up awareness, know-how and management capabilities.

4.2.7 Cybersecurity Subject Matter Experts

Subject Matter Experts in cybersecurity take on an essential role in any organisation. These group of people have not only a unique insight into the processes and technology but also are the organisations expert on the topic of cybersecurity.

Pernionla and Grey point out a number SME's in their RSA presentation document (Perniola & Gray, 2019, p. 24). Since this paper on the SIEM Use Case selection process and we have concluded in chapter 2.2.2.4 that the Mitre Att&ck Framework is providing all the needed intelligence to understand attackers, the concluding fact must be that the accumulated Subject Matter Experts know-how on attacker techniques are consolidated in the Mitre Att&ck Framework dataset.

If there is additional and new input, then this can certainly be added for additional value.

4.2.8 Threats

What is being considered a threat to an organisation can be addressed with accumulated know-how in best practises and the specifics of sectors goals in which specific targets need to be defended against. Also, vulnerabilities or exploits are being considered as threats.

All these types take into consideration what has been proven to be the right approach to mitigate cybersecurity risks. Before one can assert the right approach, mistakes must be made. These mistakes are collected in datasets all over the Internet. The data is taken from real life data of attacks and is a combination of what subject matter experts (SME) or vendors recommend.

To analyse the attack vectors, we must look at data from past attacks for which we have enough information (chapter 2.2.2). We must include predictions of cybersecurity vendors (chapter 2.2.3) and include the information from known vulnerability data sources (chapter 2.2.2.3). This process is graphed in the following picture.

Figure 19: Path to threat defence best practices

Source: Compiled and graphed by the author

The resulting threat database establishes a line of sight for all organisations and all cold profit of the combined research effort. Unfortunately, there is not one global database in which all cybersecurity companies and individuals committed to protecting data around the globe are contributing. However, various groups have established a database on their own.

Chapter 2.2.2.1 is an example of such accumulated data if research is done manually by an individual. Much better data becomes available if considering large dataset with known vulnerabilities or attack data collected in the Exploit DB or Hackmageddon databases such as discussed in chapter 2.2.2.3.

Industry data also becomes more and more critical, and the data sources also contain industry related data as well. Here is an example of the Mitre Att&ck Framework:

```
39 Government
     18 Defence
     15 Finance
     14 NGO
     11 Several Industries
      8 Telecommunication
      8 High Tech
      8 Healthcare
      8 Energy
      8 Education
      8 Aviation
      7 Manufacturing
      5 Media
      4 Supply Chain
      4 Information Technology
      4 Hospitality
      4 Chemical
      3 Legal Services
      2 Transportation
      2 Retail
      2 Restaurant
      2 Pharmaceutical
      2 Mining
      2 Industrial Control Systems
      2 Gaming
      2 Engineering
      2 Critical Infrastructure
      1 Oil
      1 Maritime
      1 Industry
      1 Food
      1 Biotech
      1 Automotive
```

Table 14: Industry data extracted from the Mitre Att&ck Framework

Source: Data compiled by the author (Mitre, 2019)

By analysing the above data sources, it must be recognised that Attack data comes in all shapes and sizes. The criteria which define the data to be added to a database varies greatly and is mostly defined by the author of the database. Hackmageddon, for example, also include country information whereas the other sources do not. At times it is also not feasible to include such information. For the consumer, however, it is crucial that there is a data source which can be relied upon and makes sure that the most significant possible reach of interoperability can be achieved in adopting the data.

When considering how threat data is accumulated and how many essential resources are needed to compile such details then attention needs to go to the Mitre Att&ck Framework as discussed in chapter 2.2.2.4. All the relevant threat details are collected, collaborated on and put into a format that can be quickly digested. With the start of vendors integrating the Att&ck detection capabilities and taxonomy, there is even more relevance and opportunity to benefit as an organisation.

4.2.9 Summary

The focus areas of the SIEM Use Case selection process cover a vast expanse on influencing parameters. Each one of them is relevant and needs to be taken into consideration. On the other hand, organisations also need a structured way of weighing their requirements, considering risks and strategy but also need to pay attention to the economic aspects as well as the feasibility of running a potentially extensive cybersecurity programme.

A strategy is needed.

This chapter has covered the various findings for each of the focus areas and has identified sources able to deliver the needed simplifications.

From this research following focus areas and following simplification source have been identified:

Focus area	Simplification source
Organisation (4.2.3)	NIST CSF Tiers, CIS CSC Implementation Groups
Regulation (4.2.4)	CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443
Detection (4.2.5)	Mitre Att&ck Framework
Risk Management (4.2.6)	NIST CSF
Subject Matter Experts (4.2.7)	Mitre Att&ck Framework
Threats (4.2.8)	Mitre Att&ck Framework

Table 15: Focus areas and their simplification source

Source: Compiled by the author

4.3 Threat & Detection

The research in chapters 2.2.2 has shown that the Mitre Att&ck Framework has proven to be the most effective dataset available. By studying the most prolific and advanced cybersecurity attacks, it was possible to create a database not only with the names of the groups and software used, but also techniques on how to detect these attacks by supplying a rule recommendation and the required log sources for the log events to be recorded in. By selecting specific log sources, an organisation can leverage the various detection capabilities the log source allows to implement. In doing so, the organisation can gain a much steeper maturity increase then by adding traditional log sources (Roe, 2019) (Exabeam, 2019). Mainstream cybersecurity vendors are still holding on to traditional log sources (Exabeam, 2019). The real attack data presented by the Mitre Att&ck Framework leads to the conclusion that by focusing on their mentioned data sources, an organisation is more likely to be able to identify an attacker.

There is still a distinctive gap between the Mitre Att&ck Framework and the business side of organisations. The Framework is mainly addressing the technical experts in the field of cybersecurity. However, it does not address a vital audience relevant to the decision-making process for cybersecurity programs. The Framework is not addressing the industry related business requirements and providing decision makers with a link to existing established processes and frameworks. The reference goes to the various industry standards, frameworks or government requirements such as NIST CSF, ISO/ICE 2700x and COBIT 5. Organisations have invested a significant capita on implementation of these standards and are required to project cybersecuri-

ty risks against their relevant framework. The author sees here a great potential to close that gap and to include the decision makers in the Mitre Att&ck Framework.

4.4 Standard Mappings

4.4.1 Introduction

The relevant standards have been identified in chapter 2.2.4 which will now be investigated more closely in regard to cross-mappings. The goal is to use the standards or frameworks with mapping capabilities and compare them against each other.

The identified standards with mapping capabilities are:

- NIST CSF Core (NIST, 2019)
- Minimal ICT Standard (Minimal ICT Standard, 2019)
- CIS Controls v7.1 Mapping for Implementation Groups (CIS, 2019)
- AuditScripts (AuditScripts, 2019)
- AuditScripts CSC Manual Assessment Tool (AuditScripts, 2019)
- CIS Controls v7.1 Mapping to NIST CSF (CIS, 2019)

4.4.2 NIST CSF

The initial set of details were extracted from the latest release of the CSF. Version 1.1 and has been released in April 2018 (National Institute of Standards and Technology, 2019). There is currently a new release in the works, but it has yet not been released from the draft state. The inner works of the framework are explained in chapter 4.2.6. The relevant part of this chapter is the mapping file (NIST, 2019). The sub-categories are mapped to CIS, Cobit 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO/IEC 27001:2013 and NIST SP 800-53 Rev.4.

It is to note that not all sub-categories always have a mapping to each of the other standards. There are many instances in which a standard has no mapping at all. This is to be expected as the structure and content of every standard differ to one another. There is however no sub-category entry, which has less than two mappings.

4.4.3 Minimal ICT standard

The minimal ICT standard from the Swiss government is for the author as a Swiss national an essential framework. The adoption rate is assumed to be rising since the release in fall of 2018. The framework document (Minimal ICT Standard, 2019) takes as its core the five functions and these are further divided by its categories such as explained in chapter 4.2.6. Each of these categories is then mapped to another standard or framework. The framework currently contains mappings to CIS, Cobit 5, ISA 62443-2-1:2009, ISA 62443-3-3:2013, ISO 27001:2013, ISO 27019:2013, NERC CIP, IEC 62351, BSI Standard and NIST SP 800-53 Rev.4.

The minimal ICT standard from the Swiss government state in chapter 1.4.1 (Minimal ICT Standard, 2019) that their work is based on the NIST Cybersecurity Framework (Federal Office for National Economic Supply FONES, 2018). The document does unfortunately not clearly state the version of the used CSF. By analysis of the data, it becomes apparent that the document published in August 2018 is based on version 1.0 of the CSF.

Following variance has been found in the official framework:

- Mapping to CSC has the label “CCS CSC” (Most frequent)
- Mapping to CSC has the label “CIS CSC” (Variance)
- Mapping to CSC has the entry “CIS CSC: 4.8” (CIS entries are dotted. These are most likely sub-controls, but that information is not referenced)
- Mapping to CSC has the entry “CCS CSC 9” (CSC entries are integers)
- Mapping to CSC has the entry “CIS CSC:” (Empty entry)
- Mapping to CSC has the entry “CIS CSC: CSC 3.3” (Combination with integer and decimals, supposedly controls and sub-controls)

4.4.4 CIS Critical Security Controls

The CIS is also maintaining its own NIST CSF mapping file (CIS, 2019). The latest CIS CSC controls are mapped against the v1.1 of the NIST CSF (CIS, 2019). The CIS Controls takes as its core their main 20 controls. These 20 controls are split up into three groups. The “Basic CIS Controls” group contains six controls. The second group is comprised of ten controls and is called the “Foundational CIS Controls”. The last group is made up of the last four controls and is called “Organisational CIS Controls”. The mapping file is currently on version 7.1 and contains mapping information to the NIST CSF v1.1. The mapping is done from every CIS subcategory to the NIST CSF sub-categories.

There is also a second mapping file containing the mappings from the CSC sub-controls to the implementation group as discussed in chapter 4.2.3.

The CIS is proclaiming a strong sense of collaboration. For that reason, they are referencing AuditScripts on their website (CIS, 2019) as an additional source of compatible frameworks. We will investigate that bond in chapter 0.

4.4.5 AuditScripts

Out of the analysed standards and frameworks is AuditScripts the only non-government or non-profit organisation. AuditScripts came onto the shortlist due to its large mapping file and due to its recommendation by CIS. AuditScript is listed on the CIS website as a companion to their framework (CIS, 2019), which made it very compelling to analyse.

AuditScript is currently on their version 7.0d release (AuditScripts, 2019) and uses at its core the CIS Critical Security Controls (SCS). The mapping file holds a vast number of other standards as shown in the following list:

CSC	IEC 62443-3-3:2013
NIST SP 800-53 Rev.4	NIST 800-171
NIST CSF v1.0	NSA MNP
NIST CSF v1.1	Australian Essential Eight
NIST SMB Guide	AU Top 35
DHS CDM Program	NSA Top 10
ISO 27002:2013	Canadian CSE Top 10
ISO 27002:2005	GCHQ 10 Steps

UK Cyber Essentials
UK ICO Protecting Data
PCI DSS 3.2
PCI DSS 3.1
PCI DSS 3.0
HIPAA
FFIEC Information Security Booklet (2016)
FFIEC Examiners Handbook
FFIEC Cybersecurity Assessment Tool (CAT)
COBIT 5
AICPA SOC 2 & SOC3 TSPC
AICPA's GAPP
IRS Pub1075
SWIFT
SG MAS TRM
Saudi AMA
NERC CIP v7
NERC CIP v6
NERC CIP v5
NERC CIP v4
NERC CIP v3
Cloud Security Alliance
SEC OCIE for AWS
FY 15 FISMA metrics
ITIL 2011 KPIs
NV Gaming MICS v7 2015
MA - CoM 201 CMR 17.00
NY - NYCRR 500
Victorian PDSF v1.0
ANSSI - 40 Measures

AuditScript does have a CIS Control assessment tool (AuditScripts, 2019). It contains next to the CIS sub-controls a link to the relevant NIST CSF functions, and it contains entry to a sensor or baseline (column D). That information of linking NIST CSF function to the information in column D becomes relevant as this will assist in a later stage the mapping efforts to link the standards to the Mitre Att&ck Framework.

4.4.6 Shared features

After reviewing the six mapping files, the files had to be prepped for analysis. Unfortunately, the Minimal ICT standard was excluded from further research as the standard was the only one which was using the NIST CSF v1.0. The NIST CSF v1.0 underwent a substantial change and is not compatible with version 1.1, especially not as the goal is to analyse the shared information between the individual mapping files.

The files AuditScripts CSC Manual Assessment Tool (AuditScripts, 2019) and CIS Control v7.1 Mapping for Implementation Groups (CIS, 2019) were not considered for the following comparison. These files were minor additions to the mapping files of their respective organisation. The files selected for the comparison are:

- AuditScripts-Critical-Security-Control-Master-Mappings-v7.0d.xlsx
- CIS-Controls-V7.1-Mapping-to-NIST-CSF.xlsx
- 2018-04-16_framework_v1.1_core1.xlsx

Every of the above mapping file holds the mapped standards (controls) in a table field. Some table fields contain a comma-separated list of controls. All these entries had to be normalised for every document. The goal was to create a data file containing all mapping information and then do basic data analytics with Microsoft Excel. The file is referenced in chapter 3.5.1 as “CIS Pivot.xlsx”.

To start comparing standards, there was a need to find a common denominator to be able to use basic statistics in comparing the datasets. There was no actual analytics required to find the denominator. The CIS mapping file only contained the mapping between CIS sub-controls and the NIST sub-categories. Both these entries were also present in the NIST and in the AusitScript mapping files.

The one common denominator between the used mapping files was:

NIST sub-controls ⇔ CIS Controls

The final data file had the structure “CIS”, “Controls” and “Framework” as the following example illustrates:

CIS	Categories	Framework
1	ID.AM-1	IKT
1	ID.AM-1	NIST
1	PR.AC-1	NIST
1	PR.AC-7	NIST
1	PR.DS-3	NIST
1	PR.DS-4	NIST
1	PR.PT-1	NIST
1	DE.AE-1	NIST
1	DE.AE-3	NIST
1	DE.CM-1	NIST
1	DE.CM-7	NIST
1	ID.AM-1	AuditScripts
1	ID.AM-3	AuditScripts

Table 16: Extract from "CIS Pivot.xlsx"

Source: Compiled by the author

The first column always contains the CIS Control. The second column contains the NIST CSF sub-category and the last column the mapping information. As a next step, the data was analysed by pivoting against the various “Categories” and “Frameworks”.

The first is analysing the matching mappings between all of the three mappings files from the NIST sub-control to the CIS controls. Following extract is showing the result of that comparison:

Count of Framework	Column Labels																			
Row Labels	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	Grand Total
DE.AE-1	1			1		1			1			2	1		2	1					10
DE.AE-2			1			2							1		1				1		6
DE.AE-3	1		1	1	1	3	2	2			1	1	1	1	1	1					17
DE.AE-4				1		1													1		3
DE.AE-5						2			1										1		4
DE.CM-1	1						2	2				2	1		2	1			1		12
DE.CM-2																			1		1
DE.CM-3					1		1							1		2			1		6
DE.CM-4				1			2	3				1							1		8
DE.CM-5							1	2											1		4
DE.CM-6																			1		1
DE.CM-7	2	2	1	1	1		1		1			2	1		2	1			1		16
DE.CM-7													1								1
DE.CM-8			2	1	1				1		1									1	7
DE.DP-1						1													2		3
DE.DP-2						1															1
DE.DP-3						1															1
DE.DP-4						1													2		3
DE.DP-5						1															1
ID.AM-1	3	1																			4
ID.AM-2		3																			3
ID.AM-3	1										1	1			1						4

Figure 20: Comparison of mappings to NIST sub-categories

Source: Compiled and graphed by the author

The data showed highlights a dire result of the mappings comparison. The coloured entries are the actual hits of the various standards against the mappings. As shown, the matching entries are fewer compared to the individual entries. Overall there were 254 mapped values (coloured entries) as shown in the above excerpt.

By doing the count on the CIS Controls, the numbers are better to understand. In every column, there is the CIS Control and the numbers of matches of at least two NIST sub-controls or more. The results for the single matches are not relevant for this comparison.

	Matches	
CIS	**2x**	**3x**
1	2	2
2	1	2
3	4	
4	2	
5	1	
6	3	2
7	4	

8	3	2
9	2	
10		1
11	2	1
12	6	
13	3	2
14	1	4
15	5	
16	5	1
17	1	5
18		1
19	10	5
20		

Table 17: Shared mappings for every CIS control

Source: Compiled by the author

There was only one single entry which was Overall the matches are distributed as such as that there is a maximum of 21.7% of shared mappings of two. The following table shows the full extent of this analysis:

	Matches	Count	Per cent
Unique Values	1	171	67.3%
In two mappings	2	55	21.7%
In three mappings	3	28	11.0%

Table 18: Shared mapping value between the three files in per cent

Source: Compiled by the author

The next step is to find the standards with the most matching values. Therefore, all mapping files were compared against each other. Having three files means that three comparisons need to be done.

- NIST against CIS
- NIST against AuditScripts
- AuditScripts against CIS

The results of that comparison are shown in the following graph:

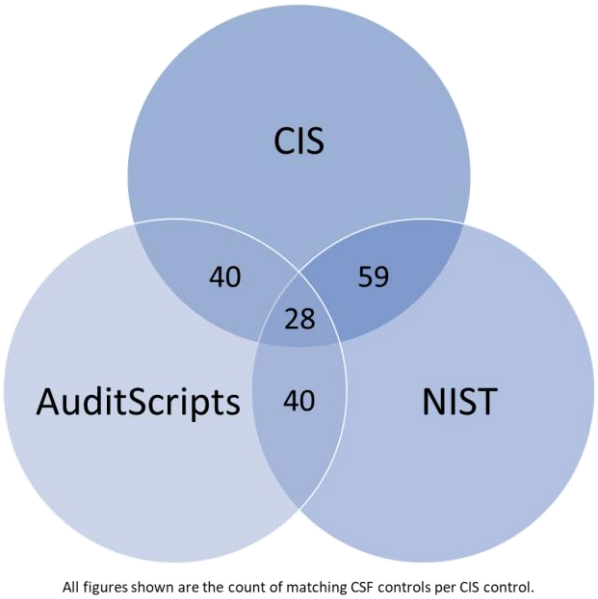


Figure 21: Data comparison of CIS - AuditScripts - NIST mappings to CSC

Source: Compiled and graphed by the author

The following findings are relevant:

- The NIST and CIS mapping are the most overlapping with 59 entries
- AuditScripts share with both, CIS and NIST, 40 shared entries
- Overall, there are 28 overlaps of all three standards
- In total there are 83 overlaps either in two or even three mappings
- AuditScipts shared 50% (not the unique entries included) of its mappings with either CIS or NIST
- It becomes apparent that mappings are a very perceptive technique to the person or group executing that activity. Even though reputable organisations were behind the mappings, there are varying results.

In conclusion, we can see that the CIS and NIST mappings seem to be the most accurate as they are sharing the most mapping entries. There is an indication that the AuditScripts mapping is congruent to the other two standards as they share an equal value of shared mappings.

The data analysed so far does not take into consideration the exact matches of mapped entries. The figures shown are just the overall matching figures on either duplicates or triplicates. It is to assume that when comparing the individual mappings that there we lower number of matches for each compared pair of standards.

The data demonstrate that the results are not allowing a limited selection of a mapping file. However, it became apparent during the analytics that this is not relevant. Organisations can select the needed mapping files. There is no need to have a mapping file from different providers of standards or frameworks. As long as it is declared which mapping file is used, then the organisation has full understanding and transparency. It was a successful exercise to discover that mapping files exist and that the mapped data might not be congruent but that the data shared some common grounds. Possibly useful when developing a method to allow the combination of standards with detection capabilities.

4.5 Combination of threats and standards in the selection process

4.5.1 Introduction

To investigate the fourth sub-question of this thesis, there is a need to combine the previous findings of chapter 4.

The finding from the first sub-question is that the selection process has focus areas and that these focus areas can be found in the associated standards or frameworks.

Focus area	Simplification source
Organisation (4.2.3)	NIST CSF Tiers, CIS CSC Implementation Groups
Regulation (4.2.4)	CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443
Detection (4.2.5)	Mitre Att&ck Framework
Risk Management (4.2.6)	NIST CSF
Subject Matter Experts (4.2.7)	Mitre Att&ck Framework
Threats (4.2.8)	Mitre Atta&ck Framework

Table 19: Focus areas and their simplification source

Source: Compiled by the author

The finding from the second sub-question is that threats and detections are available in the Mitre Att&ck Framework. The third finding is that there is no single mapping file to be used.

The CIS Controls are the only values found in all the mappings files. If there would be a mapping file between Mitre Att&ck Framework and the CIS Controls, then all mapping files identified in chapter 4.4 could be connected to the Mitre Att&ck Framework. The one piece missing now is a mapping file between Att&ck and CIS.

From the findings in chapter 4.4.6, there is proof that mapping files from different sources are not likely to match. This is due to different perspectives of the person or group doing the mapping work.

From this finding we deduct that by creating a mapping file as part of this research will produce a result valid enough for the scope of this research. Should there be a need to revise the map-

ping file for any reason, then as such would not alter the result of this research. The new mapping file would represent the view of the author of that mapping file.

4.5.2 Att&ck and CIS Mapping

Mapping of Att&ck and CIS is done by matching the content of each source logically by terminology. For the remainder with ambiguity or with no direct linkage to sensor technology, the whole framework description and the attack data set had to be compared against each other.

For that reason, a list of log sources has been compiled out of the Mitre Att&ck data set. The CIS data set is comprised of two sources from CIS and lists the following data:

- CIS Control
- CIS Subcontrol
- NIST Function
- NIST Subcategory
- Title
- Description
- Sensor Information

The list of ambiguous log source entries of the Att&ck Framework has been further dissected. Interestingly, the analytics was being done with the web application developed for this paper.

The focus for the mapping was to include Identify, Detect and Respond items from the CIS/NIST frameworks. The mapping also includes Protect activities. The premise is that protective measures also include a backchannel (log data) to communicate a fault or an attempt to bypass the enforcement rule.

Example: The CIS Subcontrol 5.4 states that “Deploy system configuration management tools that will automatically enforce and redeploy configuration settings to systems at regularly scheduled intervals.”. The deployment mechanism will keep a log of its activities and can be used to detect abnormal activity.

The function of the following table is to assist in the mapping process. The assignment process of mapping is described as follows. A log source is selected and either a corresponding entry is found in the file “Use Case Selctor.xlsx” file under the tab “CIS Controls Mapping” in columns “J”, “K”, “L” or a Details entry from the helper table below.

Lo sources	Details
API Monitoring	• Access Token Manipulation • Multi Factor Authentication • Account manipulation (ID 4738) • BITS run as a service • See VBR • See Component Firmware

	• Windows Control Panel process binary • WindowsCommon credential dumpers • DC data replication • Process and command lines • Monitor for COM objects loading DLLs and other modules • DDE execution • API calls related to enumerating and manipulating EWM such as GetWindowLong • Powershell • Monitor for calls to the SetWindowsHookEx and SetWinEventHook functions, • Deleting Windows event logs • API calls include SetWindowsHook, GetKeyState, and GetAsyncKeyState • Failed attempts to load LSA plug-ins and drivers. • Monitor calls to the ZwSetEaFile and ZwQueryEaFile Windows API functions • ADS • Monitor DLLs that are loaded by spoolsv.exe for DLLs that are abnormal • New DLLs written to the System32 directory • Monitor Registry writes to HKLM\SYSTEM\CurrentControlSet\Control\Print\Monitors • Registry key persistence • See also Named Pipes • Monitoring Windows API calls • SID-History attributes using the PowerShell Get-ADUser Cmdlet • SIPs and trust providers (Registry entries and files on disk), specifically looking for new, modified, or non-Microsoft entries. • Dump and inspect BIOS images • Command line monitoring (net.exe) • Registry logs • DLL monitoring
Named Pipes	• Sysmon Event ID 17 & 18
System Environment	• Linux Syslog

	• Windows Event Log (Event ID 4688)
System Calls	• DLL monitoring (Att&ck Techniques) • Linux (Monitor commands like 'apt-get install linux-headers-$(uname -r)', 'yum install kernel-devel-$(uname -r)', mod-probe insmod lsmod rmmod modinfo • Hypervisor Logs • Strange behavior of the browser or Office processes. This could include suspicious files written to disk, evidence of Process Injection for attempts to hide execution, evidence of Discovery, or another unusual network traffic • Memory analytics
Kernel Drivers	• Linux (Monitor commands like 'apt-get install linux-headers-$(uname -r)', 'yum install kernel-devel-$(uname -r)', mod-probe insmod lsmod rmmod modinfo
WMI Objects	• WMI event subscriptions can be monitored by some Sys-internals tools
Component Firmware	• Data and telemetry from the use of device drivers (i.e. processes and API calls) • SMART (Self-Monitoring, Analysis and Reporting Technology) • Disk check • Forensic utilities (memory analytics)
Disk Forensics	• See Component Firmware
EFI	• CHIPSEC framework • Dump and inspect BIOS images
Sensor health and status	• Detect a lack of reported activity from a host sensor
VBR	• Integrity checking on MBR and VBR.
BIOS	• Rootkit protection in Anti-Virus • Rootkit protection in Operating System (Windows Defender) • Unrecognised DLL monitoring • Unrecognised services or services • Monitor changes to MBR • See also "Component Firmware."
Host network interface	• Analyze network traffic for ICMP messages or other protocols that contain abnormal data • Analyze network data for uncommon data flows • Processes utilizing the network that do not usually have

	network communication • Monitor for ARP spoofing and gratuitous ARP broadcasts • To detect compromised network devices do auditing administrator logins, configuration changes, and device images are required to detect malicious changes • Packet capture analysis will require SSL/TLS inspection • User behaviour monitoring
Process use of network	• Abnormal entries in .bashrc or .bash_profile • Monitor application deployments and monitor account login activity on the deployment system • Monitor process file access patterns and network behaviour • Inventory and monitor browser extension installations • Monitor for any new items written to the Registry or PE files written to disk • Use process monitoring to detect and analyze the execution and arguments of CMSTP.exe • See also “Host network interface.” • DLL monitoring • Firewalls and proxies can inspect URLs for potentially known-bad domains or parameters • Unusual processes connecting to an email server within a network • unusual access patterns or authentication attempts on a public-facing webmail server • Monitor processes and command-line arguments for actions that could be taken to gather local email files • Monitor for SMB traffic on TCP ports 139, 445 and UDP port 137 and WebDAV traffic attempting to exit the network to unknown external systems • Detecting remote access tools • Ensure that proper logging of accounts used to log into systems is turned on and centrally collected • Use process monitoring to monitor the execution and arguments of msxsl.exe and wmic.exe
User interface	• Analyze network data for uncommon data flows • Processes utilizing the network that do not usually have network communication or have never been seen before are suspicious. • Analyze packet contents to detect communications that do not follow the expected protocol behaviour for the port that is

	being used. • This technique exploits users' tendencies always to supply credentials when prompted, which makes it very difficult to detect. Monitor process execution for unusual programs as well as AppleScript that could be used to prompt users for credentials

Figure 22: Helper table of Att&ck log sources and events (Mitre, 2019)

Source: Compiled by the author

The CIS Sub-control has a few entries which come by a vague definition:

- 6.2 “Ensure that local logging has been enabled on all systems and networking devices.” (CIS, 2019), For this paper, we will assume that this is the default log format of any capable system.
- 6.3 “Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.” (CIS, 2019). For this paper, we will conclude that these additional logs not part of the default log of any system.

Therefore, in the following mapping file, 6.2 is equal to basic log requirements such as Windows Event logs and 6.3 for Windows are Sysmon logs. The danger is that we will assign subcontrol 6.2 and 6.3 to many Atta&ck log sources due to its ambiguity.

Attack		CIS Subcontrol																	
Process monitoring	Detection	8.3	6.2	6.3	2.8	2.9	6.7												
File monitoring		14.9	5.5	5.3	6.3	6.7	4.8												
Process command-line parameter		8.8	2.9	14.9	6.3	6.7													
API monitoring		8.8	14.9	6.3	5.3	5.4	6.7	11.3	8.3	2.8	5.5	2.9	16.6	6.2					
Process use of network		2.1	2.3	2.4	2.8	2.9	7.4	3.1	3.2	5.5	7.2	8.3	8.7	11.3	12.2	13.3	13.5	6.7	
Windows Registry		5.5	6.3	6.7															
Packet capture		12.5																	
Authentication logs		4.8	16.12	4.9	11.5	12.11	16.10	16.3	20.8	6.7									
Netflow/Enclave netflow		12.5	12.8	11.2	12.2	12.11	13.5	18.10	6.7										
Windows event logs		16.6	6.2	6.3	6.7														
Network protocol analysis		12.6	15.3	12.4	15.2	15.8	6.7												
Binary file metadata		7.10	6.3																
DLL monitoring		2.8	6.3	6.7															
Loaded DLLs		2.8	6.3	6.7															
System calls		2.8	8.3	13.3	14.9	6.3	5.3	6.7											
Malware reverse engineering		7.10	18.7																
SSL/TLS inspection		12.10																	
Network intrusion detection syste		12.6	15.3	9.3	9.4	12.2	12.7	6.7											
Anti-virus		8.1	8.2	8.4	8.6	6.7													
Data loss prevention		13.3	13.5	14.7	14.8	14.5	13.7												
Application logs		9.5	6.3	6.7															
Windows Error Reporting		6.3	6.7																
Web proxy		12.9	12.10	7.4	7.6	7.5	13.4	6.7											
User interface		13.3	6.2	6.3	6.7														
Network device logs		9.1	9.3	11.3	13.3	15.1	15.2	15.3	6.7										
Kernel drivers		5.5	6.3	6.7															
Host network interface		9.1	9.3	11.3	13.3	15.2	15.3	6.7											
Email gateway		7.8	7.10	6.7															
Third-party application logs		3.5	9.5	3.1	3.2	6.3	6.7												
Services		6.3	5.3	6.7															
Web logs		12.9	12.10	18.10	6.7														
MBR		6.3	6.7																
Mail server		20.4	6.7																
Environment variable		8.8	6.3	6.7															
Detonation chamber		7.10	18.7	6.7															
BIOS		8.3	5.3	5.4	6.7														
WMI Objects		6.3	6.7																
Web application firewall logs		18.10	12.9	6.7															
VBR		6.3	5.3	5.4	6.7														
Sensor health and status		6.2	6.3	6.7															
PowerShell logs		8.8	2.9	14.9	6.7														
Named Pipes		6.3	6.7																
EFI		6.3	5.3	5.4	6.7														
DNS records		7.7	8.7	6.7															
Disk forensics		14.9	6.3	5.3															
Digital certificate logs		1.8	6.7																
Component firmware		11.3	6.3	5.3	5.4	6.7													
Browser extensions		7.2	7.3	6.7															
Asset management		1.1	1.2	1.3	1.4	1.5	1.6	1.8	2.1	2.5	4.1	9.1	12.1	13.1	13.7	15.1	16.1	16.6	
Access tokens		4.4	11.5	12.11	15.8	16.3	6.7												

Figure 23: CIS and Mitre Att&ck mapping file

Source: Compiled by the author

The Att&ck Framework receives frequent releases, and new data is added about tactics, techniques, groups and software. The data becomes more relevant as new essential facts are being added and can be used to protect any organisation susceptible to the attack method added or changed. Working with the Att&ck Framework and with mapping files to other standards requires a lifecycle process. It must be ensured that the data is continuously synced, implemented sources and detection rules are verified and updated, and most importantly, new threats must be countered by adding new detection methodologies.

Any change can also impact the standard used. Possibly a new control needs to be referenced as well. On the other hand, there are also changes to the used standards, infrastructure or processes, requiring a review of the implemented controls. These also can impact the mapping or the needed and required log sources. The following picture reflects on the symbiosis of how threats and log sources from the Att&ck Framework are intertwined with the standards managing the cybersecurity risks of an organisation.

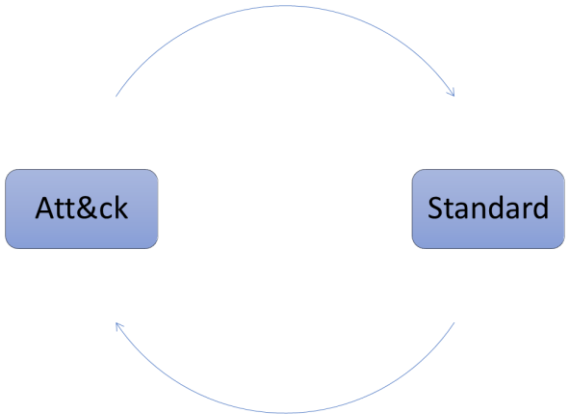


Figure 24: Att&ck data lifecycle process

Source: Compiled and graphed by the author

4.6 Main research question

4.6.1 Introduction

To investigate the main research question of this thesis, there is a need to combine all the previous findings of chapter 4.

The finding from the first sub-question is that the selection process has focus areas and that these focus areas are available in the associated standards or frameworks.

Focus area	Simplification source
Organisation (4.2.3)	NIST CSF Tiers, CIS CSC Implementation Groups
Regulation (4.2.4)	CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443
Detection (4.2.5)	Mitre Att&ck Framework
Risk Management (4.2.6)	NIST CSF
Subject Matter Experts (4.2.7)	Mitre Att&ck Framework
Threats (4.2.8)	Mitre Atta&ck Framework

Table 20: Focus areas and their simplification source

Source: Compiled by the author

The finding from the second sub-question is that threats and detections are available in the Mitre Att&ck Framework. The third finding is that there is no single mapping file to be used. The logical consequence is to use each file separately. Moreover, lastly, the finding to the fourth sub-question, which is a mapping file between the Mitre Att&ck Framework data sources and the CIS sub-controls.

The question is, how can these findings be combined?

4.6.2 Bringing it all together

The first step in trying to answer on how to combine the findings of chapter 4 is to graph the data to get a better understanding. It needs to be understood how the data relates to each other and to find potential relationships.

If we graph the findings, then we get the following picture:

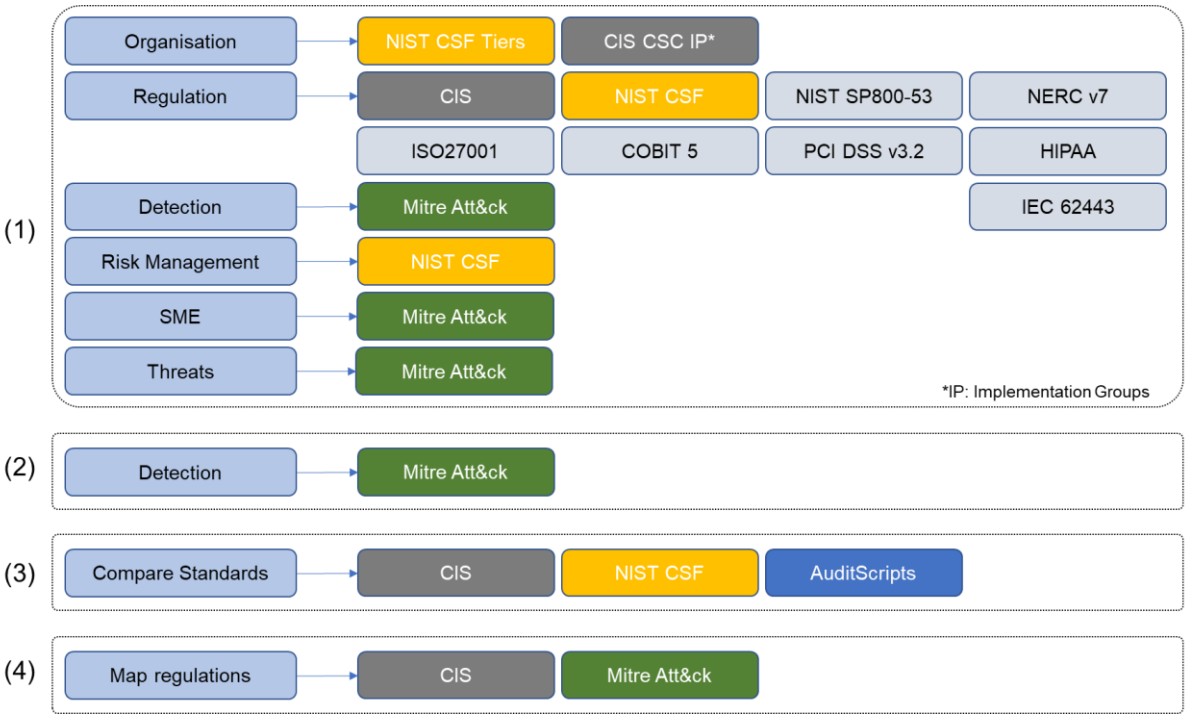


Figure 25: Relationships between all sub-questions

Source: Compiled and graphed by the author

Each focus area out of the first sub-question (1) was associated with a specific standard or framework. In the second sub-question (2) it was established that the most relevant detection methods are available in the Mitre Att&ck Framework. In the third sub-question (3) the trial failed to find a single mapping file. However, the main finding was, that this is not required, and a lookup can be flexible by allowing individual lookups for different standards. The fourth sub-question questioned the possibility to create a mapping file between the Mitre Att&ck Frameworks log sources and the CIS sub-controls. The resulting mapping file allows anyone to select any log source from the Att&ck Framework to receive a list of CIS sub-controls.

The colour coding of the previous graph provides now a visual guide on creating a combined approach. If the Att&ck Framework is centrally hosting all threat information relevant to detecting attackers and is providing to the reader the relevant log sources, following through with the detection, then by mapping these log sources with the CIS controls requirements to collect data and detect threats, there is a bi-directional connection between Att&ck and the CIS controls.

The CIS controls are then related to the other standards via the three different mapping files (yellow, blue and grey in below graph) and thereof the connections to the rest of the standards is done. Moreover, since the CIS sub-controls and the NIST CSF sub-categories have a prioritisation categorisation as discussed in chapter 4.2.3, we can then arrange the results into dif-

ferent groups. These groups we then can call implementation phases, SIEM Use Case priorities or SIEM Use case implementation roadmap.

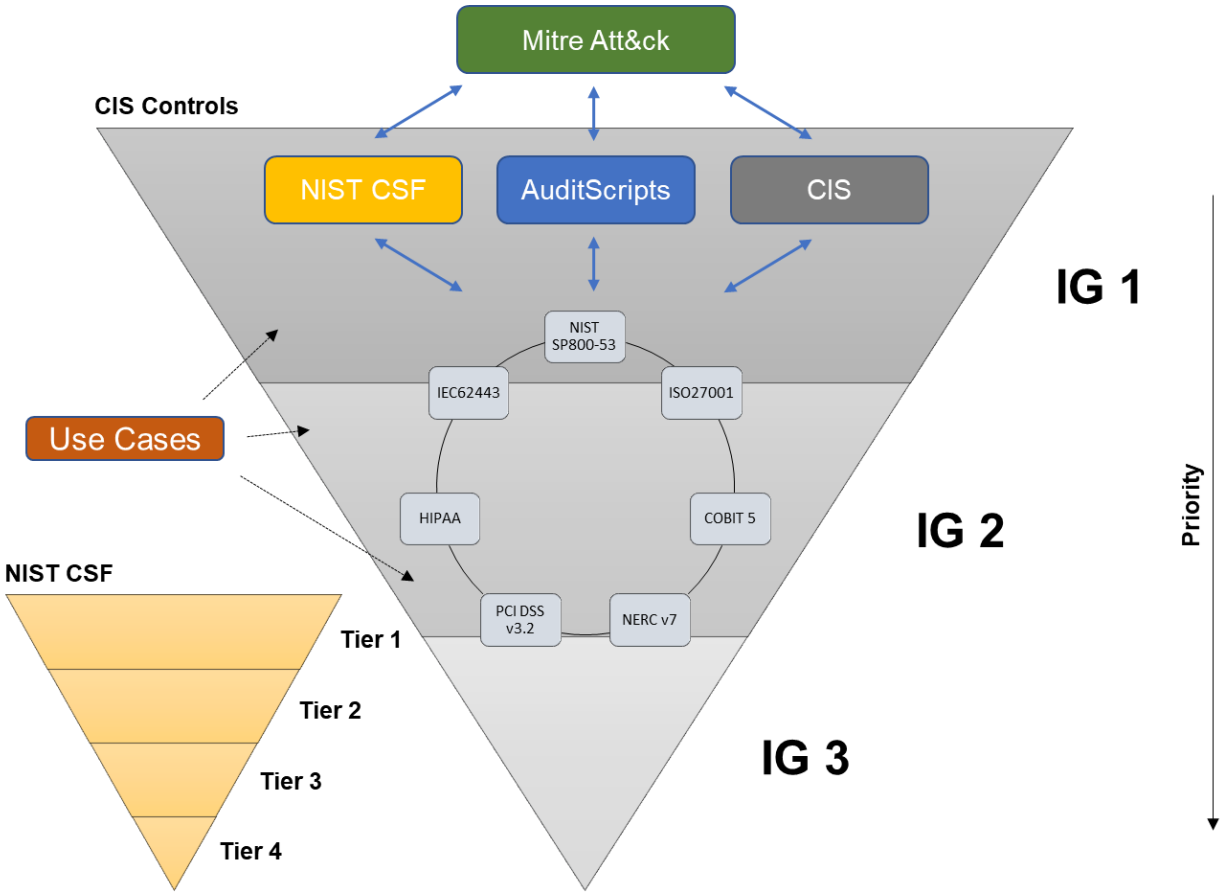


Figure 26: Proposed solution

Source: Compiled and graphed by the author

The previous picture shows the two reverse pyramid shapes. The bigger reverse pyramid is showing the three Implementation Groups of the CIS controls and the smaller reverse pyramid the tiers of the NIST CSF. The idea behind the utilization of these prioritisation categories is to apply these priorities also to the implementation of the SIEM Use Cases. Any number of identified SIEM Use Cases will have implementation priorities assigned due to the association with the CIS controls or the NIST CSF categories.

The result of applying this technique is a roadmap of the SIEM Use Cases to implement according to prioritisation as shown in the next graph.

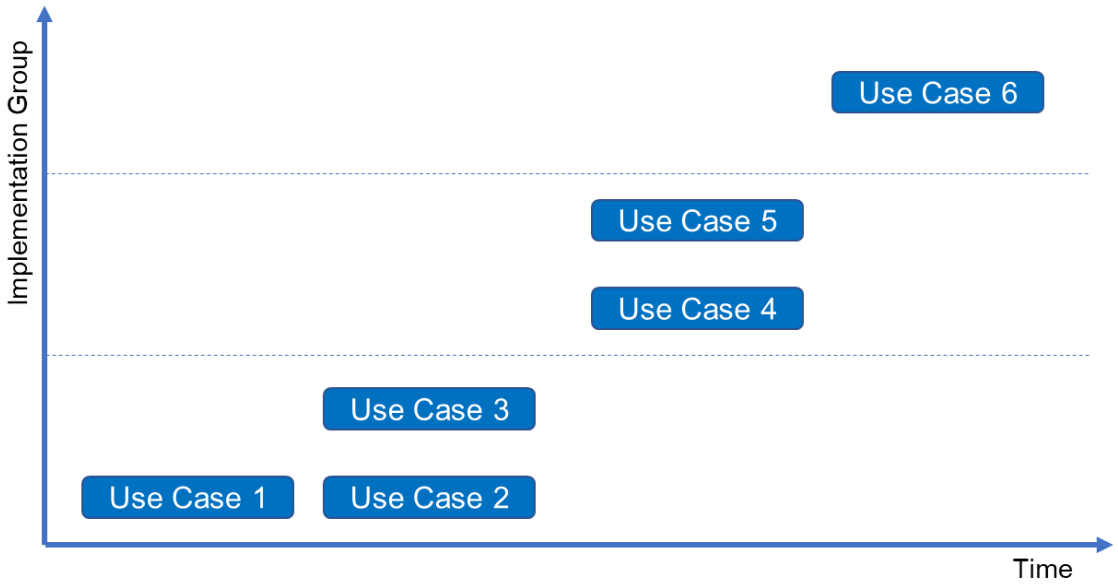


Figure 27: Prioritisation based on framework categorisation of the CIS controls

Source: Compiled and graphed by the author

The application of the framework categorisation allows to plan the implementation of the SIEM Use Cases and as such guides as outlined in the problem statement. However, it is not possible to have prioritisation within an implementation group or a tier. The prioritisation inside an implementation group or a tier can be defined within the project based on the availability of resources and implementation time. This model does not provide further guidance to break down prioritisation further.

The logical next step is to transport the initial mapping idea into a working model. At the centre is the Att&ck Framework. Chapter 2.2.2.4 holds a short introduction on the framework and about the data available. The focus now resides on the log sources, techniques, kill-chain, groups and the industries. Apart from the industries references the framework provides these data points in a normalised form (Mitre, 2019) and can be extracted as described in chapter 3.5.2.

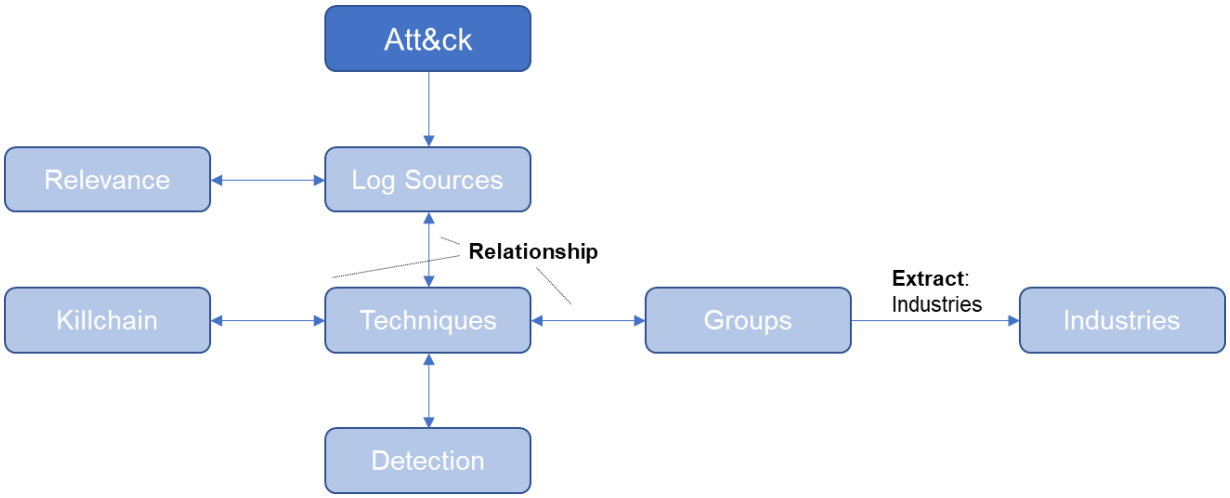


Figure 28: Att&ck data relevant for the mapping

Source: Compiled and graphed by the author

As shown in the above graph, the log sources have a bi-directional link to the techniques and the relevance. The relevance stands for the SMEs and indicates the log sources with the most detection capabilities. The techniques, on the other hand, connect to the detection, kill-chain and the groups bidirectionally. The industry information is extracted manually from the Att&ck group information and for that reason are only directly linked to the groups.

The central component of the final mapping solution is the glue between the Att&ck Framework and CIS. The mentioned glue is a mapping file listing all Att&ck log sources and entries of all matching CIS sub-controls as described in chapter 4.5.2.

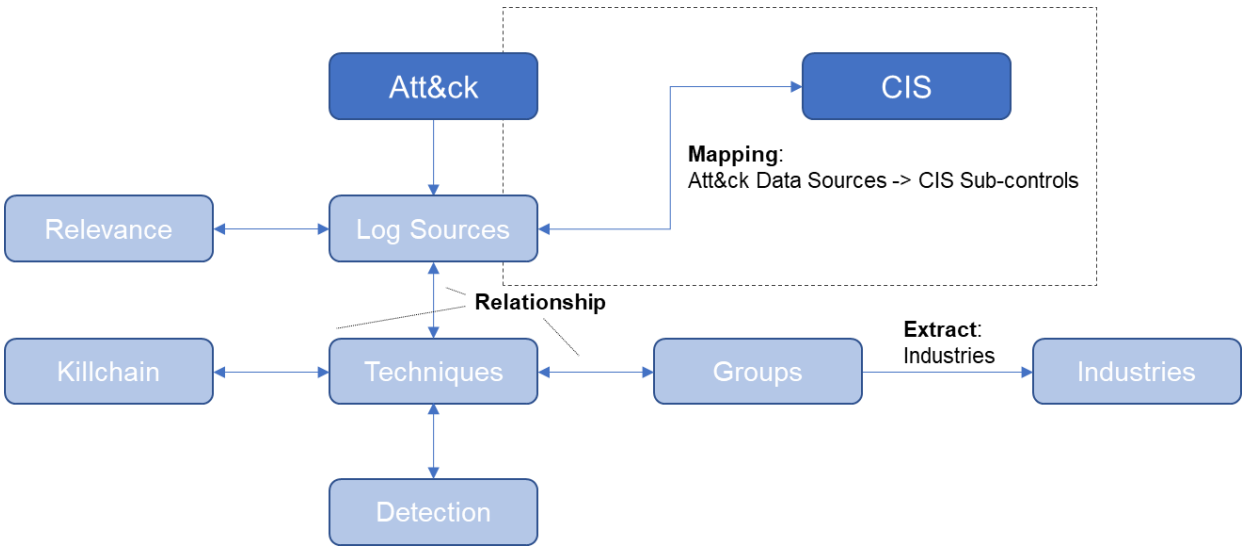


Figure 29: Mapping between Att&ck log sources and CIS sub-controls

Source: Compiled and graphed by the author

After having established the connection between the Att&ck Framework and the CIS controls it is possible to connect the three mapping files from CIS, NIST CSF and AuditScripts. Each of the three mapping files contains entries with matching CIS controls.

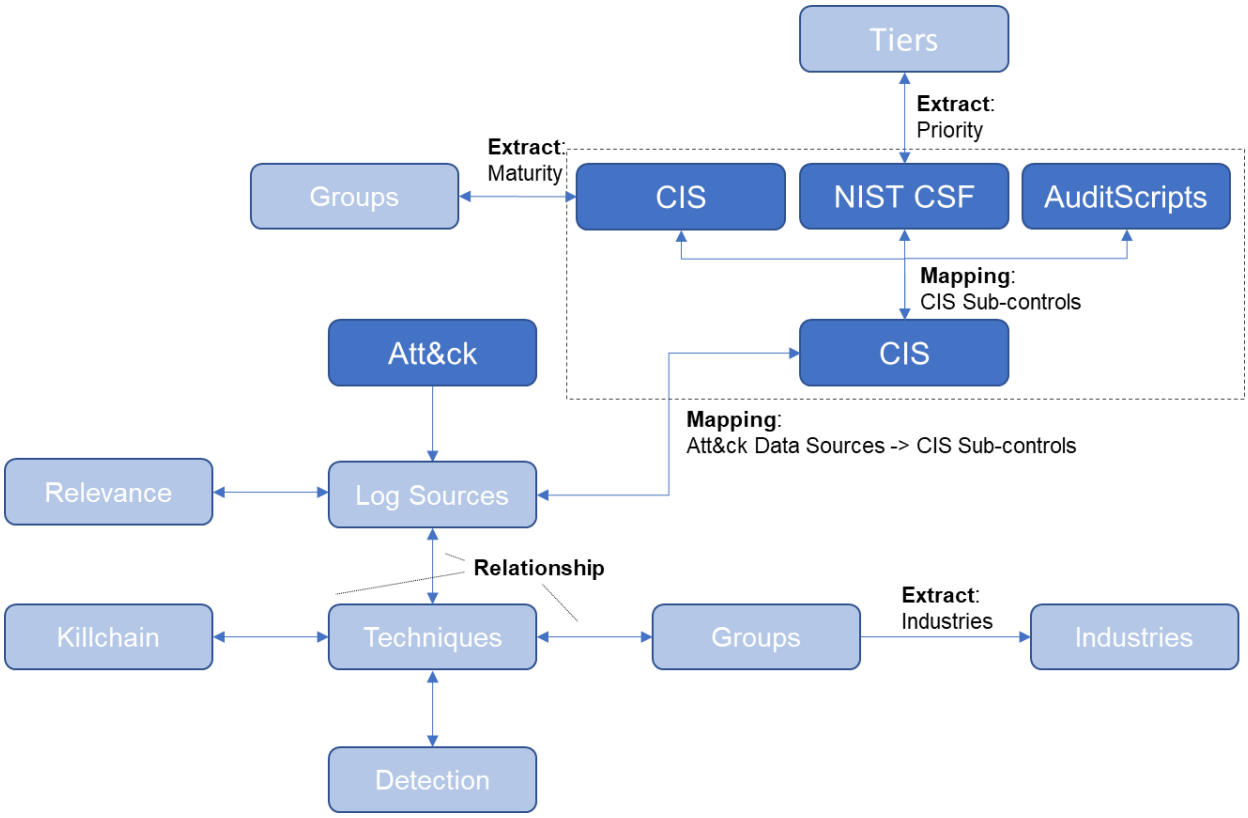


Figure 30: Mapping of CIS sub-controls to the individual mapping files

Source: Compiled and graphed by the author

The above graph also shows the prioritisation categories for the implementation groups provided by CIS and the Tiers as provided by NIST CSF.

The last step is the inclusion of the content of the mapping files. The CIS mapping file will provide a mapping to the NIST CSF. The NIST CSF mapping file will provide mappings to Cobit 5, IEC 62443, ISO 27001 and NIST SP800-53. Lastly, the AuditScript mapping file provides mappings to NIST CSF, Nerc v7, PCI DSS v3.2, Cobit 5, IEC 62443, ISO 27001 and NIST SP800-53.

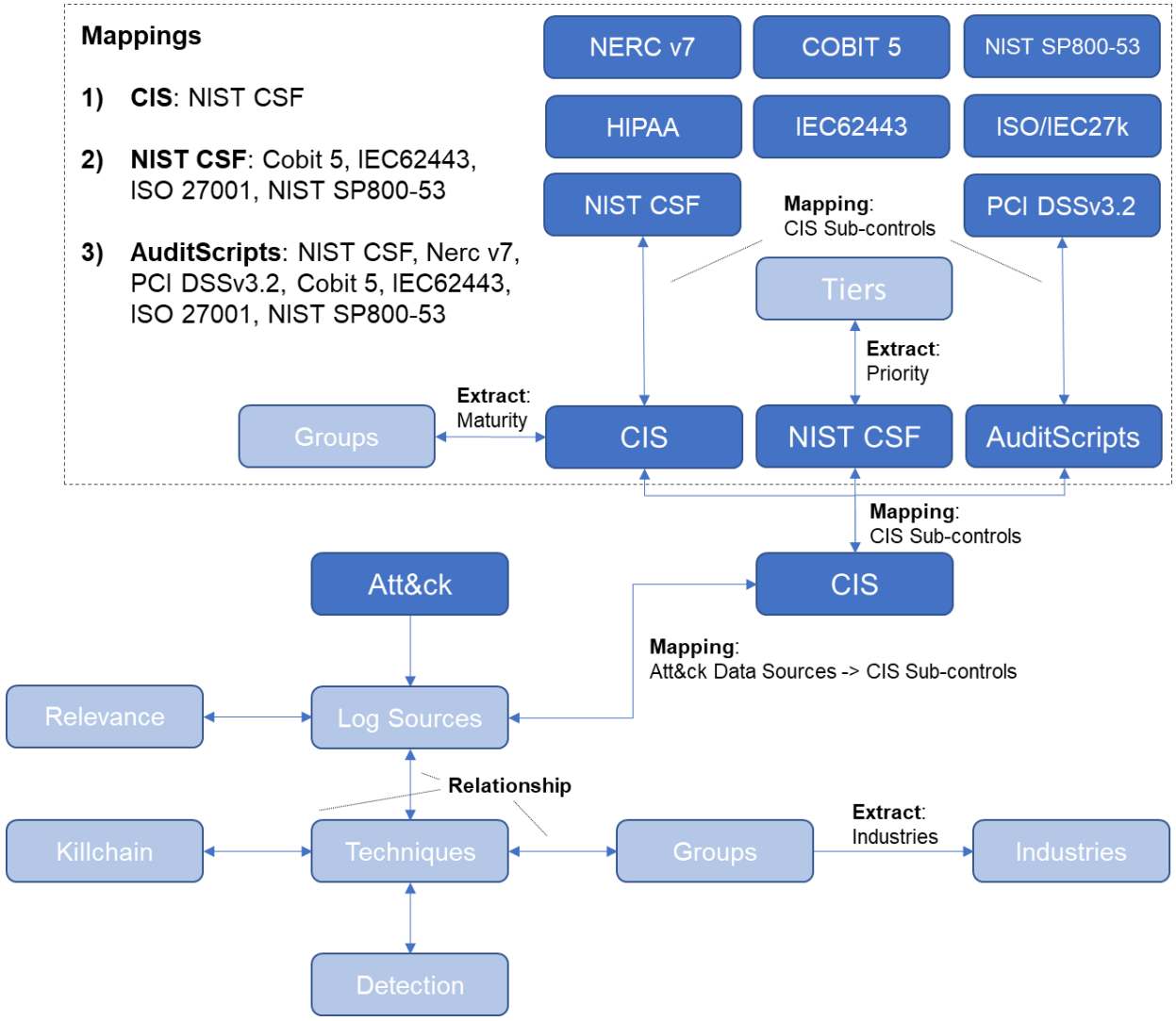


Figure 31: mapping overview of all datasets

Source: Compiled and graphed by the author

The data produced by combining the Att&ck Framework and all the standards is an extensive list of detections. We have established in chapter 3.8 that detections are referred to as SIEM Use Cases. What is missing is a method of assistance to make the extensive list of Use Cases selectable via the focus areas discussed in chapter 4.2.2. The bi-directional links as shown are providing these filters and selectors. The following picture contains possible selectors and filters.

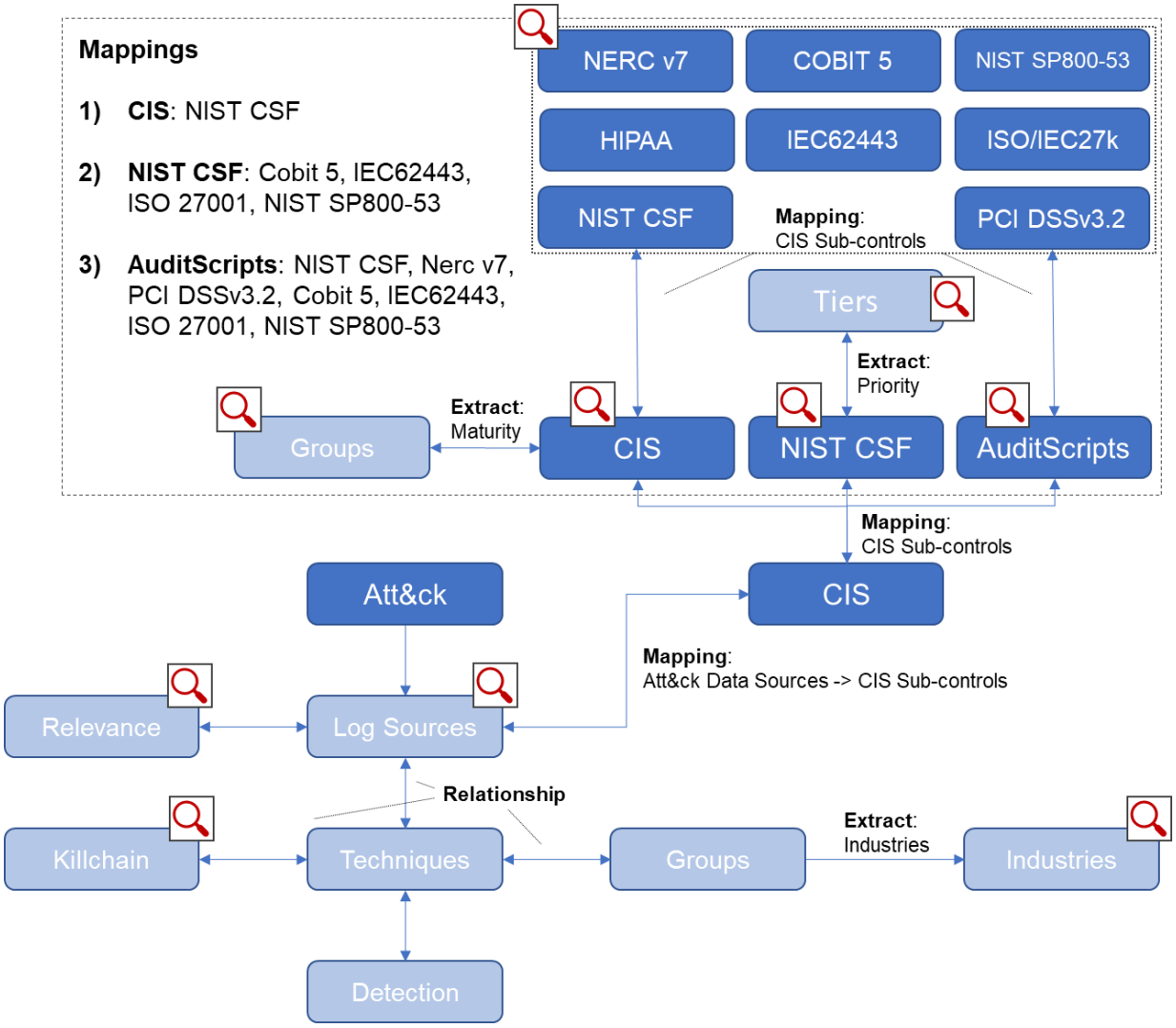


Figure 32: Data filters and selectors

Source: Compiled and graphed by the author

The meaning of filters in this context is to provide drill-down capabilities. Selectors, on the other hand, can be used to build up a meaningful SIEM Use Case selection.

As previously discussed, the method can easily be extended depending on the specific requirements. The next picture is highlighting the objects and places where the extension can occur. If for example the mapping between Att&ck and CIS (1) needs small adjustments or need to be changed due to new data, then that mapping file can be replaced. The same is valid also for the mapping standards (2). If a standard is not included, then a mapping file including that standard is included. Lastly, organisations might have very distinct detection needs (3) not covered in the Att&ck Framework. These can be added by mapping them to the relevant log sources or techniques.

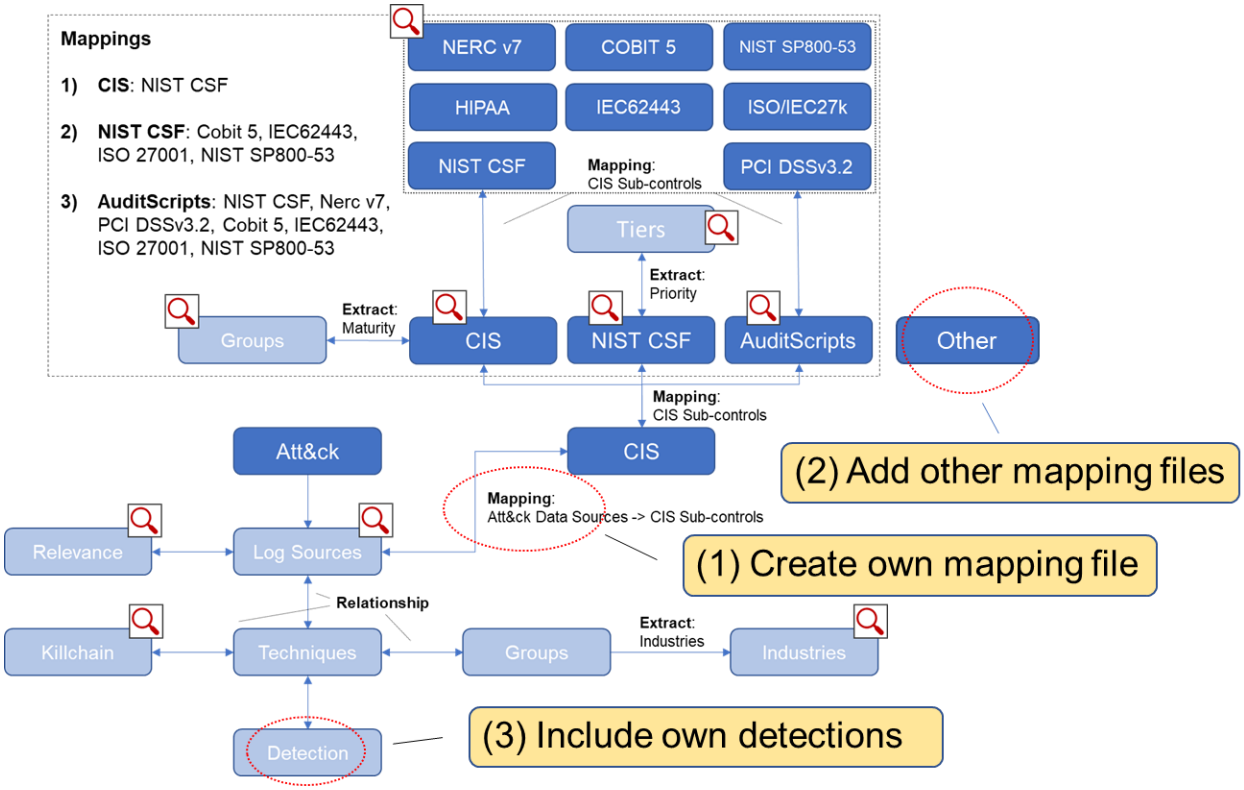


Figure 33: Ease of adjustment of the method

Source: Compiled and graphed by the author

4.6.3 Application

The possibility to map the threat and detection database to several standards allows for an automated approach in the form of an application. As part of this research, the author would like to produce a proof of value (POC) application to reflect on the findings and to evaluate an example. As basis serves the established Att&ck and CIS mappings detailed in chapter 4.6.2.

The application produced allows answering basic questions when addressing the SIEM Use Case selection process. Following questions were considered during the conception phase of the application.

- We have log sources X, Y and Z. What kind of protection can these log sources provide?"
- We must follow the standard X, what are the SIEM Use Cases we should implement?
    - Can we prioritise the implementation of the Use Cases?
- We are a medium-sized company in the industry X, which SIEM Use Cases should we implement?
- We have done a risk assessment and have found several findings. What are the Use Cases protecting us?
- Tell us the top 5 Use Cases relevant to our industry?

However, due to the time constraint, only the features are implemented to answer the first question listed above. With more effort, the features to answer the rest of the questions are added according to the research of this thesis.

Proof of value web application:

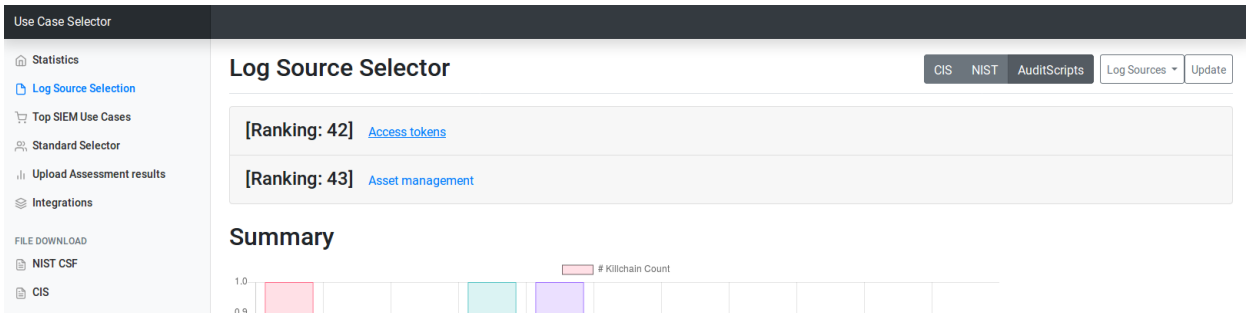


Figure 34: Application overview

Source: Screenshot from the application, taken by the author

The application (Source code: 7.2.3) can be demonstrated by answering the first question. If for example, the question is: We have log sources X, Y and Z. What kind of protection can these log sources provide?

Assuming that the log sources are “Asset Management” and “Access Tokens”, then the answer can be stepped through with the application by first selecting the log source types, selecting the preferred mapping standard and the by performing the search. The results are displayed as shown in the following picture.

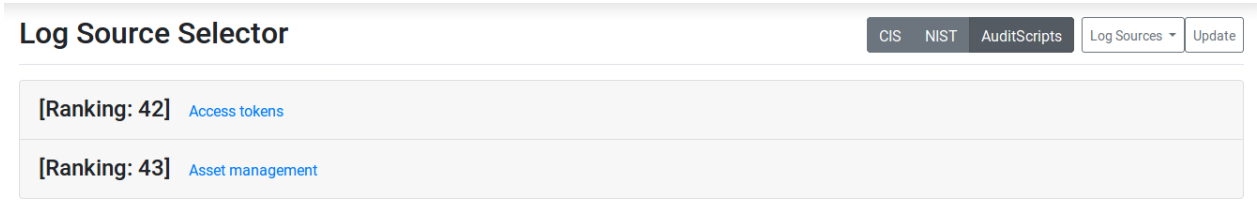


Figure 35: Log source collector and mapping selector

Source: Screenshot from the application, taken by the author

The log sources are listed and also have been given a number in the brackets. That included number is the log source ranking from the Att&ck Framework and is an indicator of how relevant the log source is to an organisation. The lower the number, the more detection methods are available and the more likely it is that the log source can help to identify an attacker.

By tapping on a log source, there is an instant view of the detection method. It also provides an inside on which kill-chains the attack is contributing to. Below the detection method is a list of all NIST CSF sub-categories, which are associated with the log source as defined by the selected mapping standard.

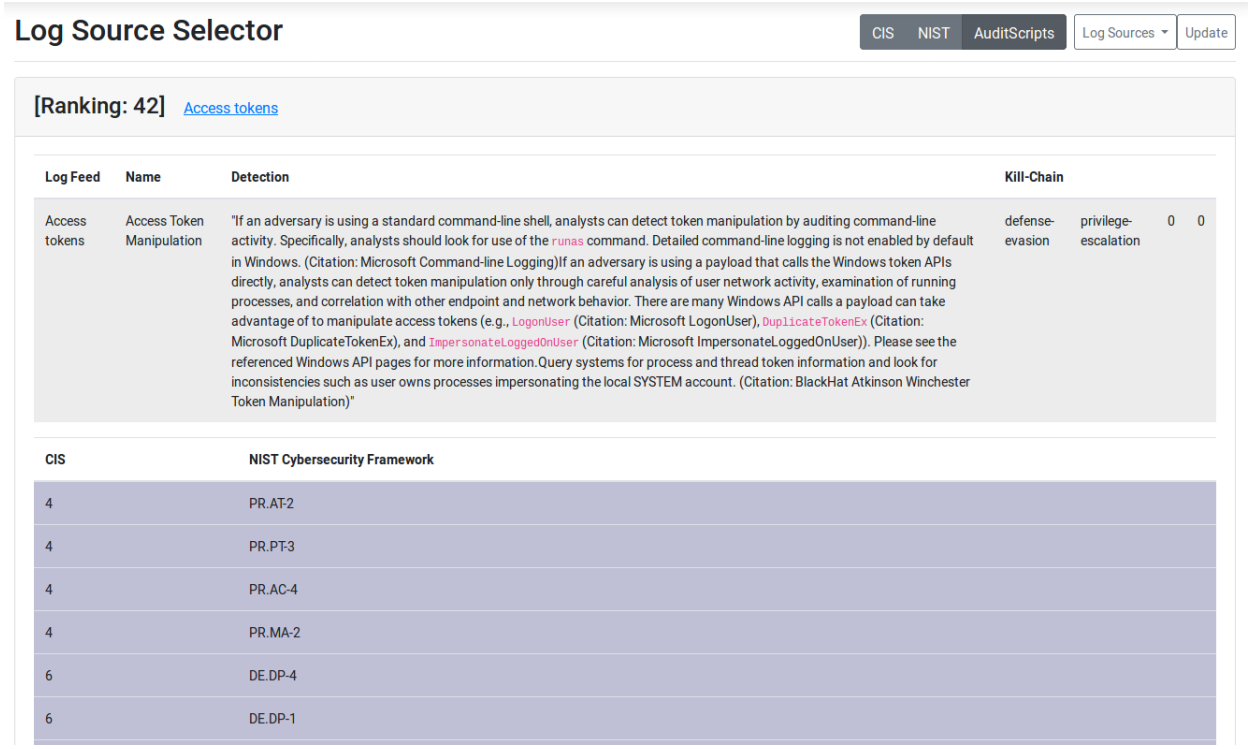


Figure 36: Detection method and associated NIST CSF sub-controls

Source: Screenshot from the application, taken by the author

Lastly, the viewer can see a statistical overview of the log sources selected. There are four types of statistics. The first bar chart graph shows the number of kill-chain tactics which cover the selection of these log sources.

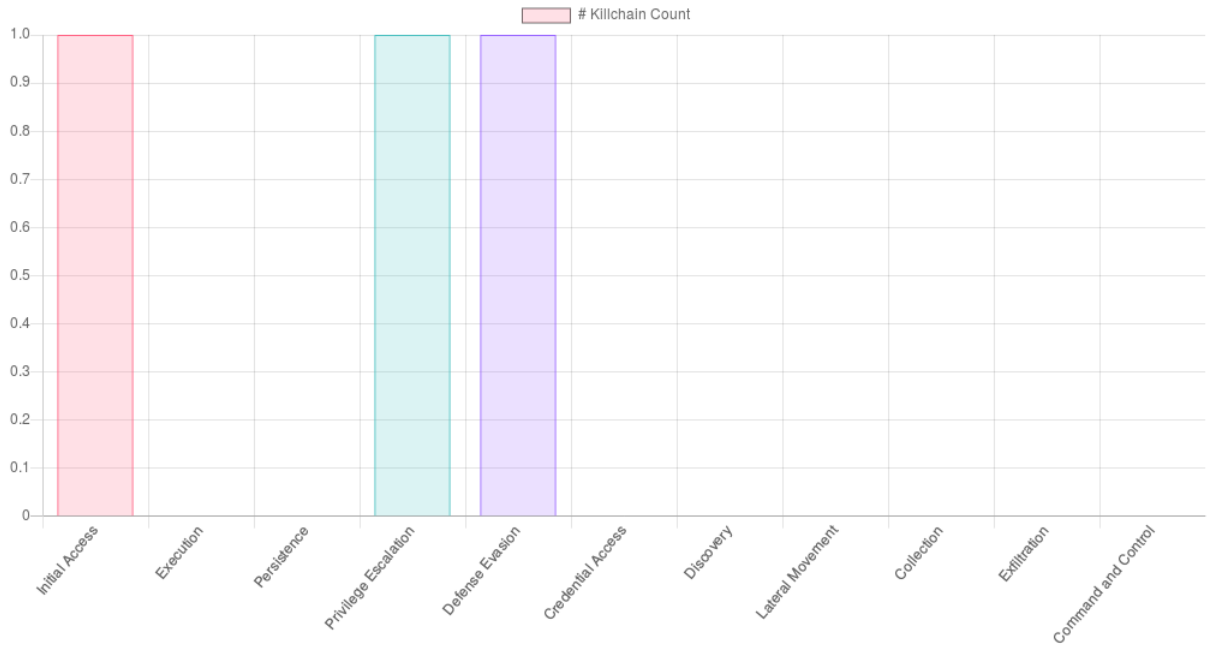


Figure 37: Kill-chain graph of the selected log sources

Source: Screenshot from the application, taken by the author

The second graph is a radar graph showing the same data in a different format.

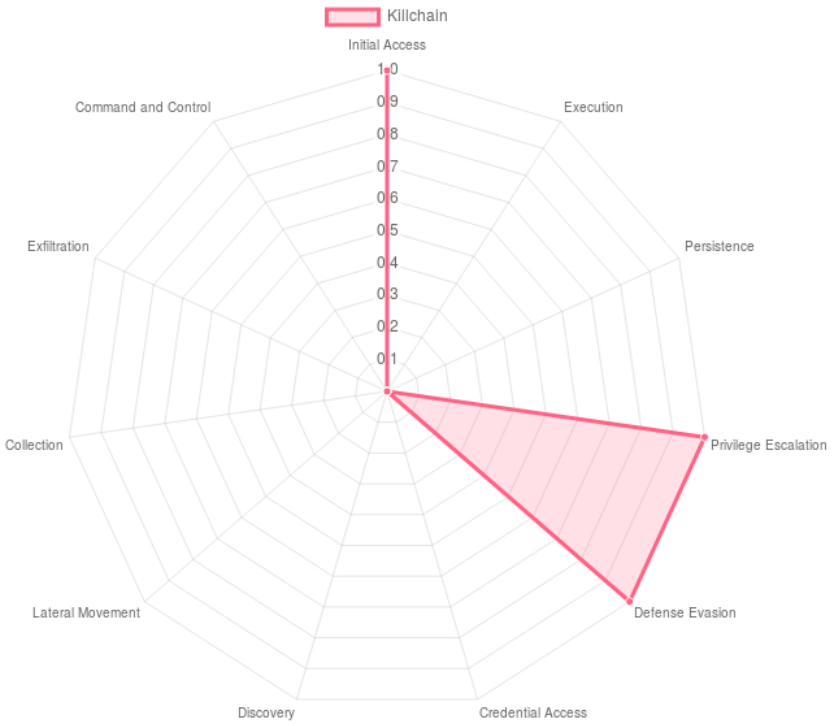


Figure 38: Kill-chain radar graph of the selected log sources

Source: Screenshot from the application, taken by the author

A different format was selected because it can highlight better the overall kill-chain coverage. The second bar chart shows the NIST CSF functions.

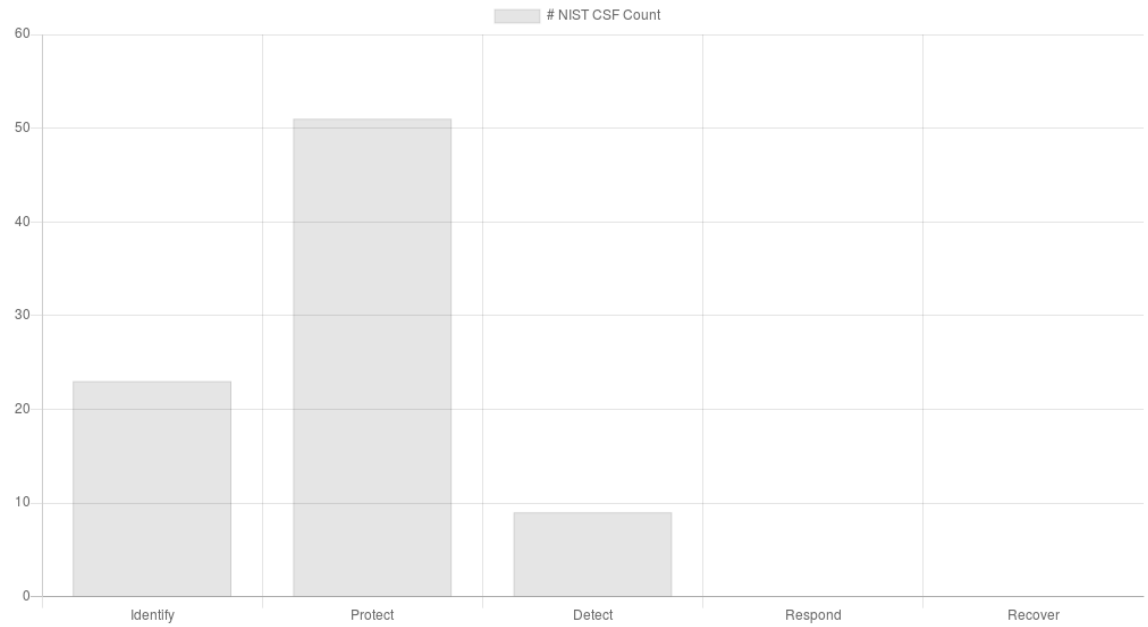


Figure 39: NIST CSF controls count

Source: Screenshot from the application, taken by the author

Lastly, there is a pie chart graph showing the coverage regarding the CIS Controls.

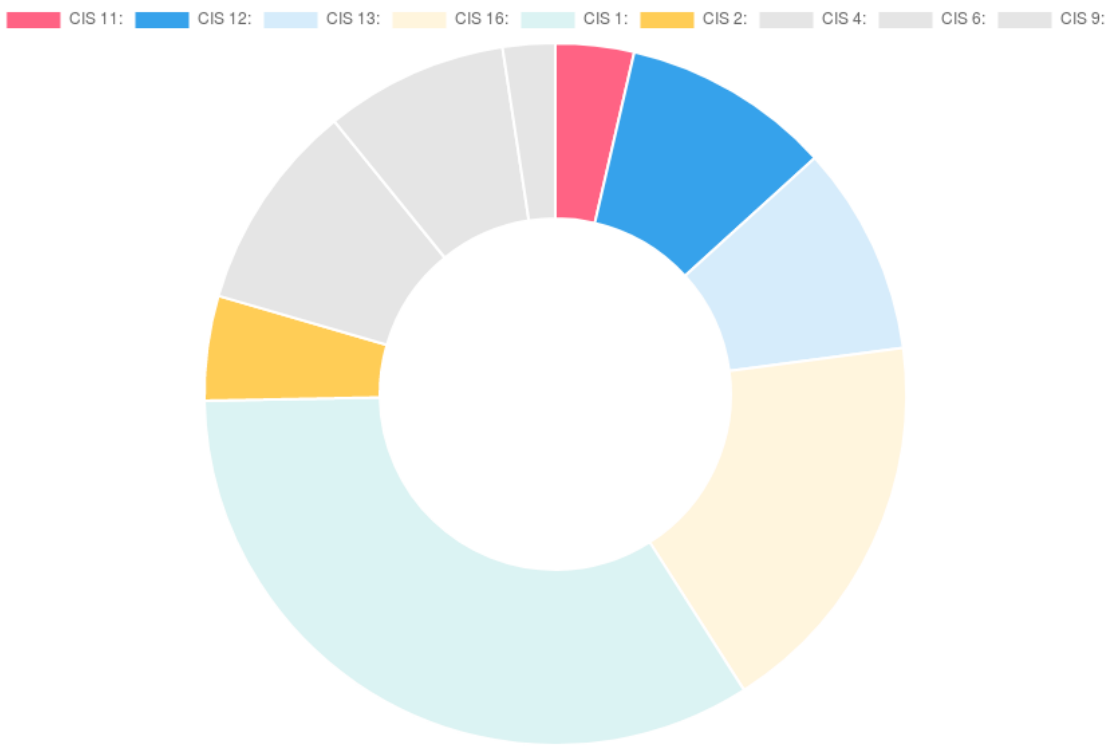


Figure 40: CIS control doughnut chart

Source: Screenshot from the application, taken by the author

4.7 Summary

This chapter was discussing the creation of a mapping file (4.6.1) between the log sources from the Mitre Att&ck Framework and the CIS sub-controls. The resulting mapping file is controlling the resulting link between the Att&ck Framework and the individual standard mappings. It is not the claim of this research that the produced Att&ck and CIS mapping is without errors. That is not necessary. It was to show that with a mapping file there is a possible methodology for a best practises approach for the SIEM Use Case selection process.

5. Analysis and Synthesis

5.1 Introduction

In this chapter, we will discuss the results of the sub- and the central questions of this research to interpret and analyse the findings.

5.2 Discussion

5.2.1 Sub-question: SIEM Use Case selection

The research in chapter 4.2.2 has identified the focus areas of the SIEM Use Case selection process. The identification of the focus areas is a combined approach between academic and vendor approaches to describe a method for the selection process of SIEM Use Cases. In combining both, the academic and vendor recommendations, we were able to produce a decision galaxy for SIEM Use Cases in chapter 4.2.2. The identified focus areas were: Threats, detection capabilities, organisation, risk management, regulations, SMEs and threats.

The decision galaxy is a qualitative measure for the SIEM Use Case selection process, and the focus areas cover a vast expanse on influencing parameters. To counter this effect, the chapter was also addressing simplification methods. **The argument was to find quantitative replacements for the focus areas able to formulate a methodology on how SIEM Use Cases can be selected. The results thereof are direct relationships between the focus areas and standards and frameworks. With this approach, we can select Use Cases based on frameworks and standards.**

The organisation (4.2.3) can be covered by the NIST CSF Tiers and the CIS CSC Implementation Groups. The standards handle the regulations (4.2.4). The detection capability (4.2.5) can be found in the Mitre Att&ck Framework. Risk Management (4.2.6) can be handled with the NIST CSF. Subject Matter Experts (4.2.7) can be matched with the huge threat and detection information of the Att&ck Framework. Finally, the threats (4.2.8) themselves are also covered extensively in the Att&ck Framework.

5.2.2 Sub-question: Threats & Detection

The research in chapters 2.2.2 has shown that the Mitre Att&ck Framework has proven to be the most effective dataset available. By studying the most prolific and advanced cybersecurity attacks, it was possible to create a database not only with the names of the groups and software used, but also techniques on how to detect these attacks by supplying a rule recommendation and the required log sources for the log events to be recorded in. By selecting specific log sources, an organisation can leverage the various detection capabilities the log source allows to implement. In doing so, the organisation can gain a much steeper maturity increase then by adding traditional log sources (Roe, 2019) (Exabeam, 2019). Mainstream cybersecurity vendors are still holding on to traditional log sources (Exabeam, 2019). The real attack data presented by the Mitre Att&ck Framework leads to the conclusion that by focusing on their mentioned data sources, an organisation is more likely to be able to identify an attacker.

There is still a distinctive gap between the Mitre Att&ck Framework and the business side of organisations. The Framework is mainly addressing the technical experts in the field of cybersecurity. However, it does not address a vital audience relevant to the decision-making process for cybersecurity programs. The Framework is not addressing the industry related business requirements and providing decision makers with a link to existing established processes and frameworks. The reference goes to the various industry standards, frameworks or government requirements such as NIST CSF, ISO/ICE 2700x and COBIT 5. Organisations have invested a

significant capita on implementation of these standards and are required to project cybersecurity risks against their relevant framework. The author sees here a great potential to close that gap and to include the decision makers in the Mitre Att&ck Framework.

5.2.3 Sub-question: Standards

The initial aim by analysing the mapping files was to either select one of these files as the best mapping resource or to prove that either of these mapping files could be used congruently. The result of that study was that neither the best of the mapping files nor proof that all were equal could be provided. The data has shown that there are some matching values between these mapping files, but these were not decisive enough to provide an answer to the aim initially set forward.

Even though from a quantitative standpoint it was not possible to draw a conclusion supporting the aim set forward, the research has provided positive findings.

The data demonstrate that the results are not allowing a limited selection of a mapping file. However, it became apparent during the analytics that this is not relevant. **If there is a declaration of which mapping file is used, then any of the mapping files can be used**. It is the same approach as if an organisation defines a standard for their organisation to follow.

It was a successful exercise to discover that mapping files exist and that the mapped data might not be congruent but that the data shared a more significant portion of its mappings. Possibly useful when developing a method to allow the combination of standards with detection capabilities.

The author would have liked to include the Minimal ICT standard. Unfortunately, the Minimal ICT standard was excluded from further research as the standard was the only one which was referencing to NIST CSF v1.0. The mapping file also contained several typographical errors not allowing a clear conclusion for several entries (4.4.3).

5.2.4 Sub-question: Selection

A selection of SIEM Use Cases becomes possible if a mapping between the Att&ck data and the CIS controls Framework exists. **It has been shown in chapter 4.5.2 that such a mapping can be created. The mapping of Att&ck and CIS is done by matching the content of each source logically by terminology. For the remainder with ambiguity or with no direct linkage to sensor technology, the whole framework description and the attack data set had to be compared against each other.**

A mapping file has been created. An important fact is that the Att&ck Framework has frequent releases and new data is being added about tactics, techniques, groups and software. The data becomes more relevant as new essential facts are being added and can be used to protect any organization susceptible to the attack method added or changed. Working with the Att&ck Framework and with mapping files to other standards requires a lifecycle process. It must be ensured that the data is continuously synced, implemented sources and detection rules are verified and updated, and most importantly, new threats must be countered by adding new detection methodologies.

Any change can also impact the standard used, and possibly a new control needs to be referenced to. On the other hand, there are also changes to the used standards, infrastructure or processes, requiring a review of the implemented controls. These also can impact the mapping or the needed and required log sources.

5.2.5 Main research question

This chapter was discussing the creation of a mapping file (4.6.1) between the log sources from the Mitre Att&ck Framework and the CIS sub-controls. The resulting mapping file is controlling the resulting link between the Att&ck Framework and the individual standard mappings. By adding that missing link, it is now possible to create a methodology to support the SIEM Use Case selection process as envisioned in the problem statement of this thesis.

The statement of purpose mentions that the author is driven by the personal objective to mitigate the impact of cyber-attacks. **This research has shown that it is possible to have a unified approach in using SIEM Use Case focus areas necessary for their selection and combine them with the relevant cybersecurity standards and frameworks. The result is a flexible best practises solution allowing for various parameters to be configured to receive a list of applicable SIEM Use Cases.**

All that is required to build this methodology is the Mitre Att&ck Framework, the mapping file created in chapter 4.6.1 and the standard mapping files mentioned in chapter 0. Combining these files allows anyone to use the methodology and select SIEM Use Cases based on the decision galaxy discussed in chapter 4.2.2.

The data produced by combining the Att&ck Framework and all the standards is an extensive list of detections. We have established in chapter 3.8 that detections are referred to as SIEM Use Cases. What is missing is a method of assistance to make the extensive list of Use Cases selectable via the focus areas discussed in chapter 4.2.2. The bi-directional links as shown are providing these filters and selectors. The meaning of filters in this context is to provide drill-down capabilities. Selectors, on the other hand, can be used to build up a meaningful SIEM Use Case selection.

This methodology can easily be extended, either by editing the mapping between Att&ck and CIS, adding new standard mapping (0) or by adding new detections.

It is not the claim of this research that the produced Att&ck and CIS mapping is without errors. That is not necessary, and it was to show that with a mapping file there is a possible methodology for a best practises approach for the SIEM Use Case selection process.

6. Conclusions and Recommendations

The research has shown that it is possible to have a unified approach in using SIEM Use Case focus areas necessary for their selection and combine them with the relevant cybersecurity standards and frameworks. The result is a flexible methodology allowing for various parameters to be configured to receive a list of applicable SIEM Use Cases.

With moving the detection capability of an organisation back into the focus, we can break down the goals based on the data gathered.

None of the existing parameters was subdued or marginalised with this approach, and it still can be added if required. At the centre is still a robust cybersecurity program driving the organisational needs, but it will be supported with qualified data from a relevant threat source able to assist in formulating a roadmap of rolling out detection capabilities. It answers the questions of what is needed to be able to detect the threats against the organisation.

6.1 Potential impact

Exposing the methods on how attackers are being detected can be used to evade detection. Therefore, it is crucial that the SIEM Use Case selection and implementation process is enclosed within a lifecycle process. It needs to be ensured that new attacks are evaluated continuously and if relevant added to the Use Case portfolio.

6.2 Flexibility of model

The model is highly flexible as shown in chapter 4.6.1. Not only does the method provide a workable solution on how to select SIEM Use Cases according to existing focus areas but it also is possible to that the mapping files are interchangeable.

The bi-directional links as introduced in chapter 4.6.1 are providing filters and selectors. The meaning of filters in this context is to provide drill-down capabilities. Selectors, on the other hand, can be used to build up a meaningful SIEM Use Case selection.

As previously mentioned, the method can easily be extended depending on the specific requirements. The extensions can be done on the primary mapping between Att&ck and CIS, on the mapping standards and the detection capability.

6.3 Further research

The author sees potential in pursuing further research in the areas of:

- Incorporation of other SIEM Use Case resources such as SIGMA or SOCPrime. A guide could be provided also to include self-developed SIEM Use Cases and how to map them to the Att&ck Framework.
- Further development of the application to upload risk assessment results of one of the supported frameworks and then provide an overview of which SIEM Use cases to deploy in which prioritisation, the required log sources, the association to the other standards and the statistical overview of CIS, kill-chain and NIST CSF functions.
- Reach out to Mitre for a suggestion to include business-relevant information such as discussed in chapter 4.3. Increasing the reach of the Framework in order to protect organisations must be a goal of every cybersecurity practitioner.

- Reach out to Mitre to suggest the mapping to CIS. The impact of a precise mapping is much more significant than done by an individual. If the mapping can help to drive the adoption rate, then it is a win for all.

7. Appendix

7.1 Mitre Att@ck

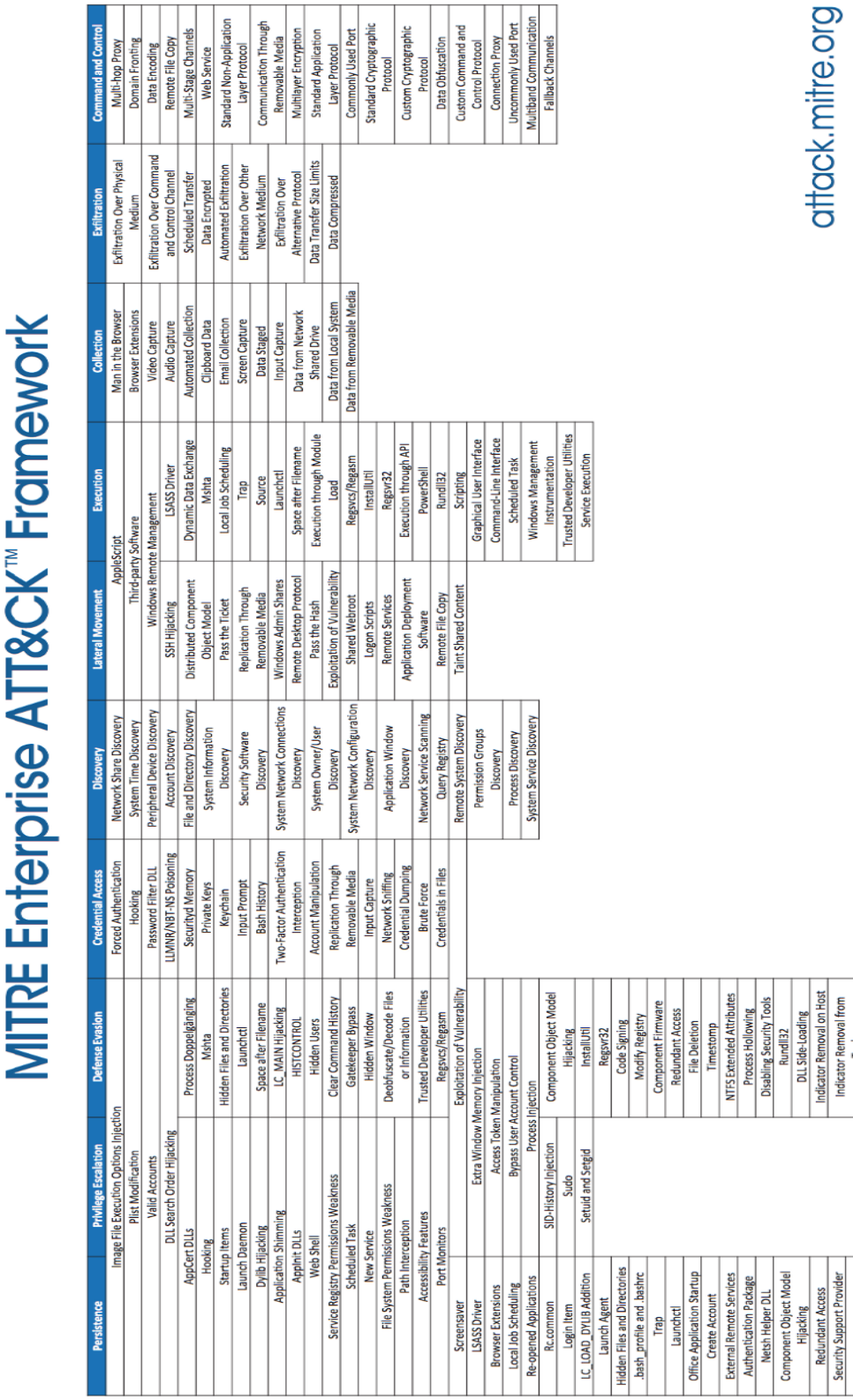


Figure 41: Mitre Attack Framework

Source: Forensic detection of MITRE Att&ck Techniques (Forensic Labs, 2019)

7.2 Source code

7.2.1 convert_attack_excel_export.pl

```
#!/usr/bin/perl
#
# Author: Pascal Imthurn
# Date: 2019
#
# This is a basic form generator for SIEM Use Case data
#

use strict;
use warnings;

my $line;  # Holds the concatenated data

my $ATTACK_DATA_FILE = "/usr/lib/cgi-bin/attack.csv";
my $ATTACK_DATA_EXPORT = "/usr/lib/cgi-bin/attack_export.csv";
open(EXPORT,">$ATTACK_DATA_EXPORT") || die "Cannot open file $ATTACK_DATA_EXPORT $!\n";
open(DATA,"<$ATTACK_DATA_FILE") || die "Cannot open file $ATTACK_DATA_FILE $!\n";
while(<DATA>) {
   # The file exported by Excel contains carriage returns within the data. A new line is
marked with "\015\012"
   # We merge now these lines to re-create the data-set
   my $tmp_line = $_;
   if ($tmp_line !~ m/\015\012/) {
      $tmp_line =~ s/\R//;              # Remove the carriage returns
      $line .= $tmp_line;
   }
   elsif ($tmp_line =~ m/\015\012/) {
      $tmp_line =~ s/\015\012//;  # Remove the proper return
      $line .= $tmp_line;
      print EXPORT $line,"\n";               # Record the whole line
      $line = '';                            # Reset the line variable
   }
   else {
      # Should never hit
   }
}
close DATA;
close EXPORT;
```

7.2.2 relationship.pl

```
#!/usr/bin/perl
#
# Author: Pascal Imthurn
# Date: 2019
#
# Extract the relationship information from the attack framework
# for Group and Techniques
#

use strict;
use warnings;

my $ATTACK_DATA_FILE = "/usr/lib/cgi-bin/convertcsv_export.csv";
my $RELATIONSHIP = "/usr/lib/cgi-bin/relationship.csv";
my %GROUP;
my %TARGET;
```

```
my %DATA;

&read_attack_data('init');
&read_attack_data('targets');
&read_attack_data('find');
&print_data();

# [0] id (intrusion-set--)
# [2] name (group name)
# [4] external_reference (G0001)
# [21] type (V)
# [126] target_ref (DW)
# [129-137] aliases

sub read_attack_data {
   my ($step) = @_;
   open(DATA,"<$ATTACK_DATA_FILE") || die "Cannot open file $ATTACK_DATA_FILE $!\n";
   while(<DATA>) {
      my $tmp_line = $_;
      chomp($tmp_line);

      if ($step eq 'init') {
         # Get the group information
         if ($tmp_line =~ m/\|intrusion-set\|/) {
            my @line_data = split('\|',$tmp_line);
            $GROUP{$line_data[0]}{$line_data[4]}{$line_data[2]}=[];
            for (my $i=129;$i<138;$i++) {
               push(@{$GROUP{$line_data[0]}{$line_data[4]}{$line_data[2]}}, $line_data[$i]);
            }
         }
      }
      elsif ($step eq 'targets') {
         # Get the target_ref (the references to the actual data)
         foreach my $intrusionset (keys %GROUP) {
            if ($tmp_line =~ m/$intrusionset/) {
               my @line_data = split('\|',$tmp_line);
               if ($line_data[21] eq 'relationship') {
                  $TARGET{$line_data[126]}{$intrusionset}="1";  # target_ref [DW]
               }
            }
         }
      }
      elsif ($step eq 'find') {
         # Find the actual target data (techniques, software(
         foreach my $target (keys %TARGET) {
         if ($tmp_line =~ m/^$target/) {                # Do not match the entries other than
the first column
            my @line_data = split('\|',$tmp_line);
            $DATA{$target}{$line_data[4]}="1";
         }
         }
      }
   }
   close DATA;

} # end sub

sub print_data {
   open(FILE,">$RELATIONSHIP") || die "Cannot open file: $!\n";
   foreach my $intrusion (sort keys %GROUP) {
      foreach my $group_id (keys $GROUP{$intrusion}) {
         foreach my $groupname (keys $GROUP{$intrusion}{$group_id}) {
               my $aliases;
```

```
               foreach (@{$GROUP{$intrusion}{$group_id}{$groupname}}) {
                  $aliases .= ",";
                  if ($_) { $aliases .= $_; }
               }
               # Do TARGET handling
                        # Print group details
                        print FILE "$group_id,$groupname";
                        # Print alias details
                        print FILE $aliases;
               foreach my $reference (keys %TARGET) {
                  if (exists($TARGET{$reference}{$intrusion})) {
                     foreach my $result (keys $DATA{$reference}) {
                        # Print result details (software, technique)
                        print FILE ",", $result;
                     }
                  }
               }
            print FILE "\n";
         }
      }
   }
   close FILE;
} # end sub
```

7.2.3 Proof of concept web application code

```
#!/usr/bin/perl
#
# Author: Pascal Imthurn
# Date: 2019
#
# This is a basic form generator for SIEM Use Case data
#

use strict;
use warnings;

use Data::Dumper;
use CGI;
use CGI::Session;
my $session = CGI::Session->new();
my $CGISESSID = $session->id();
my $query = new CGI;

my %LOG_SOURCES_DROPDOWN;                                    # All log source entries
my @LOG_SOURCES_DROPDOWN_SELECTED;                           # All selected log sources
my $LOG_SELECT_NAME = "log_sources_dropdown";                # Name of the log source drop
dowm
my $FRAMEWORK_SELECT_NAME = "framework_sources_dropdown";    # Name of the framework
source drop dowm

my $IMPLEMENTATION_GROUPS="CIS_Implementation_Groups.csv";   # Group mapping for CIS Sub-
controls
my $CIS_MAPPING_ALL="Mapping-CIS-ALL-AuditScripts.csv";      # CIS Mapping by Au-
ditScripts, CIS;Mapping;Framework
my %CIS_MAPPING_ALL_DATA;                                    # Holds all mapping info from
AuditScripts
my $NIST_MAPPING_ALL="Mapping-NIST-ALL.csv";                 # NIST CSF Mapping by NIST,
CIS;Mapping;Framework
my %NIST_MAPPING_ALL_DATA;                                   # Holds all mapping info from
NIST
```

```
my $MENU="menu";                                                    # Menu variable
my $MENU_SELECTED="0";                                              # The selected menu item
my $FRAMEWORK_DROPDOWN_SELECTED="0";                                # The selected framework
my $ATTACK_DATA_FILE = "/usr/lib/cgi-bin/attack_export.csv";
my $ATTACK_MAPPING = "/usr/lib/cgi-bin/mapping.csv";
my $CIS_MAPPING = "/usr/lib/cgi-bin/cis_mapping.csv";
my @COLOR = (1..20);                                                # Used for CSS to set table
colors
my @FRAMEWORKS = ('CIS','NIST','AuditScripts');
my $GROUP_SELECT_NAME = "group_dropdown";
my @GROUPS = ('','Implementation Group 1','Implementation Group 2','Implementation Group 3');
my $GROUP_DROPDOWN_SELECTED="0";                                    # The selected group
my %ATTACK_LOG_RATING;                                              # Rating of attack log
sources
my %ATTACK_LOG_COUNT;                                               # Count of attack log sources
my %IMPLEMENTATION_GROUP;                                           # Group data
my $PRIORITY_SELECT_NAME="priority_selection";
my $PRIORITY_CHECKBOX_SELECTED;
my $PRIO_SELECT_NAME="prio_dropdown";
my @PRIO_SELECTION_OPTION=('','Implementation Groups','Log Importance');
my $PRIO_DROPDOWN_SELECTED="0";
my @NISTCSF = ('Identify','Protect','Detect','Respond','Recover');
my %NISTCSF_HELP = (
        'ID' => 'Identify',
        'PR' => 'Protect',
        'DE' => 'Detect',
        'RS' => 'Respond',
        'RC' => 'Recover',
);
my @KILLCHAIN = ('Initial Access','Execution','Persistence','Privilege Escalation','Defense
Evasion','Credential Access','Discovery','Lateral Move-
ment','Collection','Exfiltration','Command and Control');
my @KILLCHAIN_HELP = ('initial-access','execution','persistence','privilege-
escalation','defense-evasion','credential-access','discovery','lateral-
movement','collection','exfiltration','command-and-control');
my %CONTENT = (
        '0' => 'Statistics',
        '1' => 'Log Source Selector',
        '2' => 'Top SIEM Use Cases',
        '3' => 'Select Standard',
);

# Data prep
&read_attack_data();

# Print HTML Header
print $query->header;

# Process form data
my %FORM_VALUES = process_form_data();

# HTML Body
&print_html_header();
&print_html_body_tag();
&print_top_navigation_bar();
print "<FORM name='ucb' form action='/cgi-bin/ucb' enctype='multipart/form-data' meth-
od='post' target='_self'>\n";
&print_left_navigation_bar_header();
&print_left_navigation_bar_main($MENU_SELECTED);
&print_left_navigation_bar_end();
&print_right_result_content($CONTENT{$MENU_SELECTED});
&print_left_navigation_bar_footer();
print "</FORM>\n";
```

```
&print_html_footer();


# - MENU -------------------------------------
#&print_groups_drop_down();
#&print_priority();
#&print_prio_selection();

#&read_nist_mapping_all();
#print Dumper(%NIST_MAPPING_ALL_DATA);
#&read_cis_mapping_all();
#print Dumper(%CIS_MAPPING_ALL_DATA);


exit;


# --- Subroutines ------------------------------------------------------------------------
--------

sub process_form_data {

   my @values = $query->param();
   my %value_hash;      # Having the data makes it easier for handling
   foreach(@values) {
      $value_hash{$_}="1";
      # Read values from drop down
      if ($_ eq $LOG_SELECT_NAME) {
         @LOG_SOURCES_DROPDOWN_SELECTED = $query->multi_param($_);
      }
      elsif ($_ eq $FRAMEWORK_SELECT_NAME) {
         $FRAMEWORK_DROPDOWN_SELECTED = $query->param($_);
      }
      elsif ($_ eq $GROUP_SELECT_NAME) {
         $GROUP_DROPDOWN_SELECTED = $query->param($_);
      }
      elsif ($_ eq $PRIORITY_SELECT_NAME) {
         $PRIORITY_CHECKBOX_SELECTED = $query->param($_);
      }
      elsif ($_ eq $PRIO_SELECT_NAME) {
         $PRIO_DROPDOWN_SELECTED = $query->param($_);
      }
      elsif ($_ eq $MENU) {
         $MENU_SELECTED = $query->param($_);
      }
   }
   return(%value_hash);

} # end sub


sub read_attack_data {

   open(DATA,"<$ATTACK_DATA_FILE") || die "Cannot open file $ATTACK_DATA_FILE $!\n";
   while(<DATA>) {
      my $tmp_line = $_;
      chomp($tmp_line);
      my @line_data = split('\|',$tmp_line);

      # Logsource hash
      for (my $i=0;$i<12;$i++) {
         next if $line_data[$i] =~ m/x_mitre_data_sources/ || !$line_data[$i];  # Ignore the
headers and empty fields
```

```
         # Log source index
         $line_data[$i] =~ s/^\s+//;
         $line_data[$i] =~ s/\s+$//;
         $LOG_SOURCES_DROPDOWN{$line_data[$i]}="1";
         # Log source rating
         $ATTACK_LOG_COUNT{$line_data[$i]}+=1;
      }
   }
   close DATA;
   &rate_attack_log();

} # end sub

sub rate_attack_log {

   my @unsorted;
   foreach my $log (keys %ATTACK_LOG_COUNT) {
      push @unsorted, [$log,$ATTACK_LOG_COUNT{$log}];
   }
   my @sorted = sort { $b->[1] <=> $a->[1] } @unsorted;
   # Translate the arraz position to a rank
   for(my $i=0;$i<=$#sorted;$i++) {
      $ATTACK_LOG_RATING{$sorted[$i][0]}=$i;
   }

} # end sub


sub print_log_drop_down {

   print "            <div class='btn-toolbar mb-2 mb-md-0'>\n";
   print "              <div class='btn-group mr-2'>\n";
   &print_framework_drop_down();
   print "              </div>\n";
   print "              <button type='button' id='$LOG_SELECT_NAME' class='btn btn-sm btn-
outline-secondary dropdown-toggle' data-toggle='dropdown' aria-haspopup='true' aria-
expanded='false'>\n";
   print "                <span data-feather='calendar'></span>\n";
   print "                Log Sources\n";
   print "              </button>\n";
   print "              <div class='dropdown-menu' aria-labelledby='$LOG_SELECT_NAME'>\n";
   print "              <select id='$LOG_SELECT_NAME' name='$LOG_SELECT_NAME' class='form-
control' multiple='multiple' size='10'>\n";
   if (@LOG_SOURCES_DROPDOWN_SELECTED) {
      foreach my $keys (sort keys %LOG_SOURCES_DROPDOWN) {
         my $matched = "0";     # Marker that a line is not printed twice
         foreach(@LOG_SOURCES_DROPDOWN_SELECTED) {
            if ($_ eq $keys) {
                print "                  <option selected value='$keys'>$keys</option>\n";
               $matched="1";
               next;
            }
         }
         next if $matched;              # Ignore if we had a 'selected' event
          print "                  <option value='$keys'>$keys</option>\n";
      }
   }
   else {
      foreach my $keys (sort keys %LOG_SOURCES_DROPDOWN) {
          print "                  <option value='$keys'>$keys</option>\n";
      }
   }
   print "              </select>\n";
```

```
   print "              </div>\n";
   print "              <button type='submit' class='btn btn-sm btn-outline-
secondary'>Update</button>\n";
   print "            </div>\n";
   print "            <input type='hidden' name='$MENU' value='1'>\n";

} # end sub


sub print_framework_drop_down {

   print "<div class='btn-group btn-group-toggle' data-toggle='buttons'>\n";
   # I already use as default CIS but its nice to show this also in the form
   if (!$FRAMEWORK_DROPDOWN_SELECTED) { $FRAMEWORK_DROPDOWN_SELECTED='CIS'; }
   foreach(@FRAMEWORKS) {
      if ($FRAMEWORK_DROPDOWN_SELECTED eq $_) {
         print "  <label class='btn btn-secondary active'>\n";
         print "    <input type='radio' name='$FRAMEWORK_SELECT_NAME' value='$_' autocom-
plete='off' checked>$_\n";
         print "  </label>\n";
      }
      else {
         print "  <label class='btn btn-secondary'>\n";
         print "    <input type='radio' name='$FRAMEWORK_SELECT_NAME' value='$_' autocom-
plete='off' checked>$_\n";
         print "  </label>\n";
      }
   }
   print "</div>\n";

} # end sub

sub print_groups_drop_down {

   print "<SELECT name='$GROUP_SELECT_NAME' size='1'>\n";
   foreach(@GROUPS) {
      if ($GROUP_DROPDOWN_SELECTED eq $_) {
         print "\t<OPTION value='$_' selected>$_</OPTION>\n";
      }
      else {
         print "\t<OPTION value='$_'>$_</OPTION>\n";
      }
   }
   print "</SELECT>\n";
   print "<BR>\n";

} # end sub


sub print_priority {

   if ($PRIORITY_CHECKBOX_SELECTED) {
      print "Show prioritised approach: <INPUT type='checkbox' name='$PRIORITY_SELECT_NAME'
checked>\n<br>\n";
   }
   else {
      print "Show prioritised approach: <INPUT type='checkbox'
name='$PRIORITY_SELECT_NAME'>\n<br>\n";
   }

} # end sub
```

```
sub print_prio_selection {

   print "<SELECT name='$PRIO_SELECT_NAME' size='1'>\n";
   foreach(@PRIO_SELECTION_OPTION) {
      if ($PRIO_DROPDOWN_SELECTED eq $_) {
         print "\t<OPTION value='$_' selected>$_</OPTION>\n";
      }
      else {
         print "\t<OPTION value='$_'>$_</OPTION>\n";
      }
   }
   print "</SELECT>\n";
   print "<BR>\n";

} # end sub

sub print_attack_data {

   my (@logs) = @_;
   my %attack_data = get_attack_data(@LOG_SOURCES_DROPDOWN_SELECTED);
   # Change color for every log feed
   my $col_num = "-1";
   my $color;

   # Ppreparing the mapping data
   my %map_data = read_attack_mapping(@logs);
   # Load the CIS mapping file
   my %cis_map = read_cis_mapping($FRAMEWORK_DROPDOWN_SELECTED,%map_data);

   print "<div class='accordion' id='cisAccordion'>";

   foreach my $log_source (sort keys %attack_data) {

      # Print the collapseable
      my $htmp = $log_source; $htmp =~ s/\s//g; # The spaced values do not work well with the
html
      my $head = "heading" . $htmp;     # The class id
      my $cola = "collapse" . $htmp;    # The button id
      print "<div class='card'>\n";
      print "    <div class='card-header' id='$head'>\n";
      print "      <h4 class='mb-0'>\n";
      print "        <a href='#' class='text-reset'>[Ranking: $AT-
TACK_LOG_RATING{$log_source}]</a>\n";
      print "        <button class='btn btn-link collapsed' type='button' data-
toggle='collapse' data-target='#$cola' aria-expanded='false' aria-controls='$cola'>\n";
      print "          $log_source\n";
      #print "          <a href='#' class='text-reset'>[Log ranking: $AT-
TACK_LOG_RATING{$log_source}]</a> $log_source\n";
      print "        </button>\n";
      print "      </h4>\n";
      print "    </div>\n";

      print "    <div id='$cola' class='collapse' aria-labelledby='$head' data-
parent='#cisAccordion'>\n";
      print "      <div class='card-body'>\n";

      # Print the table
      print "<table class='table table-hover'>\n";
      print "\t<thead>\n\t<tr>\n\t\t<th scope='col' style='white-space: nowrap;'>Log
Feed</th>\n\t\t<th scope='col'>Name</th>\n\t\t<th scope='col'>Detection</th>\n\t\t<th col-
span='4'>Kill-Chain</th>\n\t</tr></thead>\n";
      print "\t<tbody>\n";
      $col_num = change_colour($col_num);
```

```
      $color = "log" . $COLOR[$col_num];        # Set table color (CSS class)
      foreach my $name (sort keys %{$attack_data{$log_source}}) {
         foreach my $detection (keys %{$attack_data{$log_source}{$name}}) {
            # Since every entry has between 1 and four killchain entries, I need to test and
build the html code
            my $att_table;      # Contains HTML td code
            my $cnt = "0";      # I need to track 4 values
            for (my $t=0; $t<=4; $t++) {
               next if not exists($attack_data{$log_source}{$name}{$detection}->[$t]);
               if ($attack_data{$log_source}{$name}{$detection}->[$t] ne '0' && ex-
ists($attack_data{$log_source}{$name}{$detection}->[$t])) {
                  $att_table .= "<td>$attack_data{$log_source}{$name}{$detection}-
>[$t]</td>";
                  ++$cnt;
               }
            }
            # Pad the leftover
            if ($cnt != '4') {
               for (my $j=0; $j<(4-$cnt); $j++) {
                  $att_table .= "<td>0</td>\n\t\t";
               }
            }
            print "\t<tr
class='$color'>\n\t\t<td>$log_source</td>\n\t\t<td>$name</td>\n\t\t<td>$detection</td>\n\t\t$
att_table</tr>\n";
            #print "\t<tr bgcolor='$color' opaci-
ty='0.5'>\n\t\t<td>$log_source</td>\n\t\t<td>$name</td>\n\t\t<td>$detection</td>\n\t\t$att_ta
ble</tr>\n";
         }
      }
      print "\t<tbody>\n</TABLE>\n";

      # Print the CIS data
      &print_cis($log_source, %cis_map);

      # Print graphs
      #my $log_id = $log_source; $log_id =~ s/\s+//g;
      #print "<div>\n";
      #print "<canvas id='$log_id' style='height:20vh; width:20vw'></canvas>\n";
      #print "<canvas id='myChart5' style='height:20vh; width:20vw'></canvas>\n";
      #print "<td><canvas id='myChart2' style='height:20vh; width:20vw'></canvas></td>\n";
      #print "</div>\n";

      #print print_bar_chart($log_id,$log_source,%cis_map);
      #print print_radar_chart('myChart5');
      #print print_pie_chart('myChart2');

      print "      </div>\n";
      print "    </div>\n";
      print "  </div>\n";
   }
   print "</div>";

} # end sub


sub change_colour {

   my ($pos) = @_;
   if (++$pos >= scalar @COLOR) {
      return(0);
   }
   else {
```

```
      return(++$pos);
   }

} # end sub


sub get_attack_data {

   my (@log_data) = @_; # Contains all log sources
   my %log_hash;        # Simpler to handle data
   my %result;          # Holds the retrieved data
   # Transform into hash
   foreach(@log_data) {
      $log_hash{$_}="1";
   }

   open(DATA,"<$ATTACK_DATA_FILE") || die "Cannot open file $ATTACK_DATA_FILE $!\n";
   while(<DATA>) {
      my $tmp_line = $_;
      chomp($tmp_line);

      my @line_data = (split('\|',$tmp_line))[0,1,2,3,4,5,6,7,8,9,10,11,12,15,24,26,28,30];
      for (my $i=0;$i<12;$i++) {
         next if $line_data[$i] =~ m/x_mitre_data_sources/ || !$line_data[$i];  # Ignore the
headers and empty fields
         if ($log_hash{$line_data[$i]}) {
            # Entry matches selected log file
            # {log_file}{name}{detection}[0,1,2,3]
            if (!$line_data[$i]) { $line_data[$i] = "0"; }
            if (!$line_data[12]) { $line_data[13] = "0"; }
            if (!$line_data[13]) { $line_data[13] = "0"; }
            if (!$line_data[14]) { $line_data[14] = "0"; }
            if (!$line_data[15]) { $line_data[15] = "0"; }
            if (!$line_data[16]) { $line_data[16] = "0"; }
            if (!$line_data[17]) { $line_data[17] = "0"; }
            $re-
sult{$line_data[$i]}{$line_data[12]}{$line_data[13]}=[$line_data[14],$line_data[15],$line_dat
a[16],$line_data[17]];
         }
      }
   }
   close DATA;
   return(%result);

} # end sub

sub read_attack_mapping {

   my (@log_data) = @_; # Contains all log sources
   my %log_hash;        # Simpler to handle data
   my %mapping;         # Holds the retrieved data, {}{}{}
   # Transform into hash
   foreach(@log_data) {
      $log_hash{$_}="1";
   }
   open(DATA,"<$ATTACK_MAPPING") || die "Cannot open file $ATTACK_MAPPING $!\n";
   # {log source}{cis subcontrol}
   while(<DATA>) {
      my $tmp_line = $_;
      chomp($tmp_line);
      my @line_data = split('\;',$tmp_line);
      # Fix empty entries
      if (!$line_data[1]) { $line_data[1]="0"; }
```

```
      # Get only the relevant entries from the drop down selector
      if ($log_hash{$line_data[0]}) {
         # Create an hash of hashes
         if ($mapping{$line_data[0]}) {
            $mapping{$line_data[0]}{$line_data[1]}="1";
         }
         else {
            $mapping{$line_data[0]}{$line_data[1]}="1";
         }
      }
   }
   close DATA;
   return(%mapping);

} # end sub


sub read_cis_mapping {

   # Incoming % contains: Log Source:CIS Subcontrol
   my ($framework,%data) = @_;
   # We expand the hash with the mapping information
   my %data2;

   # CIS CSC; NIST CSF; Framework
   open(DATA,"<$CIS_MAPPING") || die "Cannot open file $CIS_MAPPING $!\n";
   while(<DATA>) {
      chomp($_);
      my @line = split('\;',$_);
      # Remove whitespace
      $line[2] =~ s/\R//;
      # Select only thee correct framework data
      if ($line[2] eq $framework) {
         foreach my $log_source (keys %data) {
            foreach my $cis (keys %{$data{$log_source}}) {
               # Need the integer of the saved CIS Subcontrol value
               my $cis_sub = int($cis);
               # Match only the correct CIS values
               if ($cis_sub eq $line[0]) {
                  # We could replace the second entry '{$cis}'
                  $data2{$log_source}{$cis}{$line[1]}="1";
               }
            }
         }
      }
   }
   close DATA;
   return(%data2);

} # end sub

sub print_cis {

   # Hash: {log source}{cis}{nist csf}
   my ($log,%cis_data) = @_;
   # Change color for every log feed
   my $col_num = "-1";
   my $color;
   foreach my $log_source (sort keys %cis_data) {
      next if $log_source ne $log;                      # Only print the log source relevant
mappings
      print "<table class='table table-hover'>\n";
```

```
      print "<thead>\n\t<th scope='col'>CIS</th>\n\t<th scope='col'>NIST Cybersecurity Frame-
work</th>\n";
      $col_num = change_colour($col_num);
      $color = "log" . $COLOR[$col_num];        # Set table color (CSS class)
      foreach my $cis (sort {$a<=>$b} keys %{$cis_data{$log_source}}) {
         my $cis_int = int($cis);
         foreach my $nist (keys %{$cis_data{$log_source}{$cis}}) {
            print "\t<tr
class='$color'>\n\t\t<td>$cis_int</td>\n\t\t<td>$nist</td>\n\t</tr>\n";
         }
      }
      print "\t<tbody>\n</TABLE>";
   }

} # end sub


sub read_implementation_group {

   # CIS;Subcontrols;Group1;Group2;Group3
   open(DATA,"<$IMPLEMENTATION_GROUPS") || die "Cannot open file $IMPLEMENTATION_GROUPS
$!\n";
   while(<DATA>) {
      chomp($_);
      my @line = split('\;',$_);
      $IMPLEMENTATION_GROUP{$line[0]}{$line[1]}{'Implementation Group 1'}=$line[2];
      $IMPLEMENTATION_GROUP{$line[0]}{$line[1]}{'Implementation Group 2'}=$line[3];
      $IMPLEMENTATION_GROUP{$line[0]}{$line[1]}{'Implementation Group 3'}=$line[4];
   }
   close DATA;

} # end sub


sub read_cis_mapping_all {
   # $CIS_MAPPING_ALL   # CIS Mapping by AuditScripts, CIS;Mapping;Framework
   # %CIS_MAPPING_ALL_DATA
   open(DATA,"<$CIS_MAPPING_ALL") || die "Cannot open file $CIS_MAPPING_ALL $!\n";
   while(<DATA>) {
      chomp($_);
      my @line = split('\;',$_);
      $CIS_MAPPING_ALL_DATA{$line[0]}{$line[1]}{$line[2]}="1";
   }
} # end sub


sub read_nist_mapping_all {
   # $NIST_MAPPING_ALL  # NIST CSF Mapping by NIST, CIS;Mapping;Framework
   # %NIST_MAPPING_ALL_DATA
   open(DATA,"<$NIST_MAPPING_ALL") || die "Cannot open file $NIST_MAPPING_ALL $!\n";
   while(<DATA>) {
      chomp($_);
      my @line = split('\;',$_);
      $NIST_MAPPING_ALL_DATA{$line[0]}{$line[1]}{$line[2]}="1";
   }
} # end sub

sub print_html_header {

   print "<!doctype html>\n";
   print "<html lang='en'>\n";
   print " <head>\n";
   print "  <!-- Required meta tags -->\n";
```

```
   print "  <meta charset=\"utf-8\">\n";
   print "  <meta name='viewport' content='width=device-width, initial-scale=1, shrink-to-
fit=no'>\n";

   print "  <!-- Bootstrap CSS -->\n";
   print "  <link rel='stylesheet' href='/css/bootstrap.min.css' integrity='sha384-
ggOyR0iXCbMQv3Xipma34MD+dH/1fQ784/j6cY/iJTQUOhcWr7x9JvoRxT2MZw1T' cros-
sorigin='anonymous'>\n";

   print "  <title>Use Case Selector</title>\n";

   print "  <style>\n";
   print "    .bd-placeholder-img {\n";
   print "      font-size: 1.125rem;\n";
   print "      text-anchor: middle;\n";
   print "      -webkit-user-select: none;\n";
   print "      -moz-user-select: none;\n";
   print "      -ms-user-select: none;\n";
   print "      user-select: none;\n";
   print "    }\n";

   print "    \@media (min-width: 768px) {\n";
   print "      .bd-placeholder-img-lg {\n";
   print "        font-size: 3.5rem;\n";
   print "      }\n";
   print "    }\n";
   print "  </style>\n";
   print "  <!-- Custom styles for this template -->\n";
   print "  <link href='/css/dashboard.css' rel='stylesheet'>\n";

   print "  <script src='/js/node_modules/chart.js/dist/Chart.js'></script>\n";

   # Favicon
   print "<link rel='apple-touch-icon' sizes='180x180' href='/apple-touch-icon.png'>\n";
   print "<link rel='icon' type='image/png' sizes='32x32' href='/favicon-32x32.png'>\n";
   print "<link rel='icon' type='image/png' sizes='16x16' href='/favicon-16x16.png'>\n";
   print "<link rel='manifest' href='/site.webmanifest'>\n";
   print "<link rel='mask-icon' href='/safari-pinned-tab.svg' color='#5bbad5'>\n";
   print "<meta name='msapplication-TileColor' content='#2d89ef'>\n";
   print "<meta name='theme-color' content='#ffffff'>\n";

   print " </head>\n";

} # end sub


sub print_html_body_tag {

   print " <body>\n";

} # end sub


sub print_top_navigation_bar {

   print "  <nav class='navbar navbar-dark fixed-top bg-dark flex-md-nowrap p-0 shadow'>\n";
   print "   <a class='navbar-brand col-sm-3 col-md-2 mr-0' href='ucb'>Use Case Selec-
tor</a>\n";
   print "   <ul class='navbar-nav px-3'>\n";
   print "      <li class='nav-item text-nowrap'>\n";
   print "      </li>\n";
   print "   </ul>\n";
   print "  </nav>\n";
```

```
} # end sub


sub print_left_navigation_bar_header {

   print "  <div class='container-fluid'>\n";
   print "    <div class='row'>\n";
   print "      <nav class='col-md-2 d-none d-md-block bg-light sidebar'>\n";
   print "        <div class='sidebar-sticky'>\n";

} # end sub

sub print_left_navigation_bar_main {

   my ($active_menu) = @_;
   my $activate_menu="nav-link active";
   my $normal_menu="nav-link";
   my $link = $normal_menu;
   print "          <ul class='nav flex-column'>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '0') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=0'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-home'><path d='M3 9l9-7 9
7v11a2 2 0 0 1-2 2H5a2 2 0 0 1-2-2z'></path><polyline points='9 22 9 12 15 12 15
22'></polyline></svg>\n";
   print "                        Statistics<span class='sr-only'>(current)</span>\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '1') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=1'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-file'><path d='M13 2H6a2 2 0 0
0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V9z'></path><polyline points='13 2 13 9 20
9'></polyline></svg>\n";
   print "                        Log Source Selection\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '2') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=2'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-shopping-cart'><circle cx='9'
cy='21' r='1'></circle><circle cx='20' cy='21' r='1'></circle><path d='M1 1h4l2.68 13.39a2 2
0 0 0 2 1.61h9.72a2 2 0 0 0 2-1.61L23 6H6'></path></svg>\n";
   print "                        Top SIEM Use Cases\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '3') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=3'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-users'><path d='M17 21v-2a4 4
0 0 0-4-4H5a4 4 0 0 0-4 4v2'></path><circle cx='9' cy='7' r='4'></circle><path d='M23 21v-2a4
4 0 0 0-3-3.87'></path><path d='M16 3.13a4 4 0 0 1 0 7.75'></path></svg>\n";
   print "                        Standard Selector\n";
   print "                      </a>\n";
```

```
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '4') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=4'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-bar-chart-2'><line x1='18'
y1='20' x2='18' y2='10'></line><line x1='12' y1='20' x2='12' y2='4'></line><line x1='6'
y1='20' x2='6' y2='14'></line></svg>\n";
   print "                        Upload Assessment results\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   if ($active_menu == '5') { $link = $activate_menu; } else { $link = $normal_menu; }
   print "                      <a class='$link' href='ucb?$MENU=5'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-layers'><polygon points='12 2
2 7 12 12 22 7 12 2'></polygon><polyline points='2 17 12 22 22 17'></polyline><polyline
points='2 12 12 17 22 12'></polyline></svg>\n";
   print "                        Integrations\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                  </ul>\n";


   print "                  <h6 class='sidebar-heading d-flex justify-content-between align-
items-center px-3 mt-4 mb-1 text-muted'>\n";
   print "                    <span>File download</span>\n";
   print "                    <a class='d-flex align-items-center text-muted' href='#'>\n";
   print "                      <span data-feather='plus-circle'></span>\n";
   print "                    </a>\n";
   print "                  </h6>\n";

   print "          <ul class='nav flex-column mb-2'>\n";
   print "                    <li class='nav-item'>\n";
   print "                      <a class='nav-link' href='#'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-file-text'><path d='M14 2H6a2
2 0 0 0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V8z'></path><polyline points='14 2 14 8 20
8'></polyline><line x1='16' y1='13' x2='8' y2='13'></line><line x1='16' y1='17' x2='8'
y2='17'></line><polyline points='10 9 9 9 8 9'></polyline></svg>\n";
   print "                        NIST CSF\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   print "                      <a class='nav-link' href='#'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-file-text'><path d='M14 2H6a2
2 0 0 0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V8z'></path><polyline points='14 2 14 8 20
8'></polyline><line x1='16' y1='13' x2='8' y2='13'></line><line x1='16' y1='17' x2='8'
y2='17'></line><polyline points='10 9 9 9 8 9'></polyline></svg>\n";
   print "                        CIS\n";
   print "                      </a>\n";
   print "                    </li>\n";
   print "                    <li class='nav-item'>\n";
   print "                      <a class='nav-link' href='#'>\n";
   print "                        <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-file-text'><path d='M14 2H6a2
2 0 0 0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V8z'></path><polyline points='14 2 14 8 20
```

```
8'></polyline><line x1='16' y1='13' x2='8' y2='13'></line><line x1='16' y1='17' x2='8'
y2='17'></line><polyline points='10 9 9 9 8 9'></polyline></svg>\n";
   print "                          Social engagement\n";
   print "                        </a>\n";
   print "                      </li>\n";
   print "                      <li class='nav-item'>\n";
   print "                        <a class='nav-link' href='#'>\n";
   print "                          <svg xmlns='http://www.w3.org/2000/svg' width='24'
height='24' viewBox='0 0 24 24' fill='none' stroke='currentColor' stroke-width='2' stroke-
linecap='round' stroke-linejoin='round' class='feather feather-file-text'><path d='M14 2H6a2
2 0 0 0-2 2v16a2 2 0 0 0 2 2h12a2 2 0 0 0 2-2V8z'></path><polyline points='14 2 14 8 20
8'></polyline><line x1='16' y1='13' x2='8' y2='13'></line><line x1='16' y1='17' x2='8'
y2='17'></line><polyline points='10 9 9 9 8 9'></polyline></svg>\n";
   print "                          Year-end sale\n";
   print "                        </a>\n";
   print "                      </li>\n";
   print "                    </ul>\n";

} # end sub



sub print_left_navigation_bar_end {

   print "        </div>\n";
   print "      </nav>\n";

} # end sub

sub print_right_result_content {

   my ($content_title) = @_;
   print "        <main role='main' class='col-md-9 ml-sm-auto col-lg-10 px-4'>\n";
   print "          <div class='d-flex justify-content-between flex-wrap flex-md-nowrap
align-items-center pt-3 pb-2 mb-3 border-bottom'>\n";
   print "            <h1 class='h2'>$content_title</h1>\n";

   # Create the log source dropdown
   if ($MENU_SELECTED == '1') {
      &print_log_drop_down();
   }
   print "          </div>\n";

   # Show the Attack data based on the log selection
   if ($MENU_SELECTED && $FORM_VALUES{$LOG_SELECT_NAME}) {
      # Attack data prep
      my %attack = get_attack_data(@LOG_SOURCES_DROPDOWN_SELECTED);
      # Print Attack data
      &print_attack_data(@LOG_SOURCES_DROPDOWN_SELECTED,%attack);

      # NIST data prep
      # Ppreparing the mapping data
      my %graph_map_data = read_attack_mapping(@LOG_SOURCES_DROPDOWN_SELECTED);
      # Load the CIS mapping file
      my %graphcis = read_cis_mapping($FRAMEWORK_DROPDOWN_SELECTED,%graph_map_data);

      # Print the Summary part of the page
      print "<div>\n";
      print "          <br><h2 class='h2'>Summary</h2>\n";
      print "<table>\n";
      print "<tr>\n";
      print "<td><canvas id='sum_killchain' style='height:40vh;
width:40vw'></canvas></td>\n";
```

```
      print "<td><canvas id='spider_killchain' style='height:40vh;
width:40vw'></canvas></td>\n";
      print "</tr>\n";
      print "<tr>\n";
      print "<td><canvas id='sum_nist' style='height:40vh; width:40vw'></canvas></td>\n";
      print "<td><canvas id='sum_cis' style='height:40vh; width:40vw'></canvas></td>\n";
      print "<td></td>\n";
      print "</tr>\n";
      print "</table>\n";
      print "</div>\n";

      print print_bar_chart('sum_killchain','killchain',%attack);
      print print_radar_chart('spider_killchain','killchain',%attack);
      print print_bar_chart('sum_nist','nist',%graphcis);
      print print_pie_chart('sum_cis','cis',%graphcis);
   }

   print "        </main>\n";

} # end sub



sub print_left_navigation_bar_footer {

   print "    </div>\n";
   print "  </div>\n";

} # end sub


sub print_html_footer {

   print "  <!-- Optional JavaScript -->\n";
   print "  <!-- jQuery first, then Popper.js, then Bootstrap JS -->\n";
   print "  <script src='https://code.jquery.com/jquery-3.3.1.slim.min.js' integrity='sha384-
q8i/X+965DzO0rT7abK41JStQIAqVgRVzpbzo5smXKp4YfRvH+8abtTE1Pi6jizo' cros-
sorigin='anonymous'></script>\n";
   print "  <script
src='https://cdnjs.cloudflare.com/ajax/libs/popper.js/1.14.7/umd/popper.min.js' integri-
ty='sha384-UO2eT0CpHqdSJQ6hJty5KVphtPhzWj9WO1clHTMGa3JDZwrnQq4sF86dIHNDz0W1' cros-
sorigin='anonymous'></script>\n";
   print "  <script
src='https://stackpath.bootstrapcdn.com/bootstrap/4.3.1/js/bootstrap.min.js' integri-
ty='sha384-JjSmVgyd0p3pXB1rRibZUAYoIIy6OrQ6VrjIEaFf/nJGzIxFDsf4x0xIM+B07jRM' cros-
sorigin='anonymous'></script>\n";

   print " </body>\n";
   print "</html>\n";

} # end sub

sub prepare_killchain_graph_data {

   my (%attackdata) = @_;
   my %count;
   foreach my $alog (keys %attackdata) {
      foreach my $aname (keys %{$attackdata{$alog}}) {
         foreach my $adetect (keys %{$attackdata{$alog}{$aname}}) {
            my $att_table;      # Contains HTML td code
            my $cnt = "0";      # I need to track 4 values
            for (my $t=0; $t<=4; $t++) {
               next if not exists($attackdata{$alog}{$aname}{$adetect}->[$t]);
```

```
               if ($attackdata{$alog}{$aname}{$adetect}->[$t] ne '0' && ex-
ists($attackdata{$alog}{$aname}{$adetect}->[$t])) {
                  $count{$attackdata{$alog}{$aname}{$adetect}->[$t]}+=1;
                  ++$cnt;
               }
            }
         }
      }
   }
   # Build data string
   # Issue is, the saved data has different upper and lower case usage. Need to use a helper
hash
   my $data_str="data: [";
   for(my $z=0; $z<11; $z++) {
      if (exists($count{$KILLCHAIN_HELP[$z]})) {
         $data_str.=$count{$KILLCHAIN_HELP[$z]};
      }
      else {
         $data_str.="0";
      }
      #
      if ($z != '10') { $data_str.=", "; }
   }
   $data_str.="],";
   return($data_str);

} # end sub


sub prepare_nist_graph_data {

   my (%nistdata) = @_;
   my %count;
   foreach my $alog (keys %nistdata) {
      foreach my $acis (keys %{$nistdata{$alog}}) {
         foreach my $anist (keys %{$nistdata{$alog}{$acis}}) {
            # The entries are in the form of DE.DP-1, we only need the beginning
            my @atmp = split('\.',$anist);
            $count{$NISTCSF_HELP{$atmp[0]}}+=1;
         }
      }
   }
   # Build data string
   my $data_str="data: [";
   for(my $z=0; $z<5; $z++) {
      if (exists($count{$NISTCSF[$z]})) {
         $data_str.=$count{$NISTCSF[$z]};
      }
      else {
         $data_str.="0";
      }
      #
      if ($z != '10') { $data_str.=", "; }
   }
   $data_str.="],";
   return($data_str);

} # end sub

sub prepare_cis_graph_data {

   my (%cisdata) = @_;
   my %count;
```

```
   foreach my $alog (keys %cisdata) {
      foreach my $acis (keys %{$cisdata{$alog}}) {
         my $tmp_cis = "CIS " . int($acis) . ":";
         foreach my $anist (keys %{$cisdata{$alog}{$acis}}) {
            $count{$tmp_cis}+=1;
         }
      }
   }
   # Build data string
   my $data_str="data: [";
   my $labels_str="'labels':[";
   # 'labels':['Red','Blue','Yellow'],
   foreach my $gcis (sort keys %count) {
      $data_str.=$count{$gcis} . ",";
      $labels_str.="'$gcis',";
   }
   # Remove the last comma
   $data_str =~ s/\,$//;
   $labels_str =~ s/\,$//;
   $data_str.="],";
   $labels_str.="],";
   return($data_str,$labels_str);

} # end sub

sub print_bar_chart {

   my ($chartid,$data_type,%rawdata) = @_;

   my $data_string;                    # All mighty data string used for the graph
   my $labels_string;                  # Labels string (X axis)
   my $label;                          # Label above the graph
   if ($data_type eq 'killchain') {
      # We must have: Y=Count of entries, Y=Killchain
      # We have {log_file}{name}{detection}[0,1,2,3]
      $labels_string = "labels: ['Initial Access','Execution','Persistence','Privilege Esca-
lation','Defense Evasion','Credential Access','Discovery','Lateral Move-
ment','Collection','Exfiltration','Command and Control'],";
      $label="label: '# Killchain Count',";
      $data_string=prepare_killchain_graph_data(%rawdata);
   }
   elsif ($data_type eq 'nist') {
      # We must have: Y=Count of entries, Y=NIST
      # We have {log_file}{name}{detection}[0,1,2,3]
      $labels_string = "labels: ['Identify','Protect','Detect','Respond','Recover'],";
      $label="label: '# NIST CSF Count',";
      $data_string=prepare_nist_graph_data(%rawdata);
   }

   print "<script>\n";
   print "var ctx = document.getElementById('$chartid');\n";
   print "var myChart = new Chart(ctx, {\n";
   print "    type: 'bar',\n";
   print "    data: {\n";
   print "        $labels_string\n";
   print "        datasets: [{\n";
   print "             $label\n";
   print "             $data_string\n";
   if ($data_type eq 'killchain') {
      print "            backgroundColor: [\n";
      print "                'rgba(255, 99, 132, 0.2)',\n";
      print "                'rgba(54, 162, 235, 0.2)',\n";
      print "                'rgba(255, 206, 86, 0.2)',\n";
```

```
      print "                'rgba(75, 192, 192, 0.2)',\n";
      print "                'rgba(153, 102, 255, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)',\n";
      print "                'rgba(255, 159, 64, 0.2)'\n";
      print "            ],\n";
      print "            borderColor: [\n";
      print "                'rgba(255, 99, 132, 1)',\n";
      print "                'rgba(54, 162, 235, 1)',\n";
      print "                'rgba(255, 206, 86, 1)',\n";
      print "                'rgba(75, 192, 192, 1)',\n";
      print "                'rgba(153, 102, 255, 1)',\n";
      print "                'rgba(255, 159, 64, 1)',\n";
      print "                'rgba(255, 159, 64, 1)',\n";
      print "                'rgba(255, 159, 64, 1)',\n";
      print "                'rgba(255, 159, 64, 1)',\n";
      print "                'rgba(255, 159, 64, 1)',\n";
      print "                'rgba(255, 159, 64, 1)'\n";
      print "            ],\n";
   }
   if ($data_type eq 'NIST') {
      print "            backgroundColor: [\n";
      print "                'rgba(255, 99, 132, 0.2)',\n";
      print "                'rgba(54, 162, 235, 0.2)',\n";
      print "                'rgba(255, 206, 86, 0.2)',\n";
      print "                'rgba(75, 192, 192, 0.2)',\n";
      print "                'rgba(153, 102, 255, 0.2)'\n";
      print "            ],\n";
      print "            borderColor: [\n";
      print "                'rgba(255, 99, 132, 1)',\n";
      print "                'rgba(54, 162, 235, 1)',\n";
      print "                'rgba(255, 206, 86, 1)',\n";
      print "                'rgba(75, 192, 192, 1)',\n";
      print "                'rgba(153, 102, 255, 1)'\n";
      print "            ],\n";
   }
   print "            borderWidth: 1\n";
   print "        }]\n";
   print "    },\n";
   print "    options: {\n";
   # Remove the label
   #print "        legend: {\n";
   #print "          display: false\n";
   #print "        },\n";

   print "        scales: {\n";
   print "            yAxes: [{\n";
   print "                ticks: {\n";
   print "                    beginAtZero: true\n";
   print "                }\n";
   print "            }]\n";
   print "        }\n";
   print "    }\n";
   print "});\n";
   print "</script>\n";

} # end sub


sub print_radar_chart {
```

```
   my ($chartid,$data_type,%rawdata) = @_;

   my $data_string;                    # All mighty data string used for the graph
   if ($data_type eq 'killchain') {
      # We must have: Y=Count of entries, Y=Killchain
      # We have {log_file}{name}{detection}[0,1,2,3]
      $data_string=prepare_killchain_graph_data(%rawdata);
   }

   print "<script>\n";
   print "new Chart(document.getElementById('$chartid'),{\n";
   print "    'type':'radar',\n";
   print "    'data':{\n";
   print "         'labels':['Initial Access','Execution','Persistence','Privilege Escala-
tion','Defense Evasion','Credential Access','Discovery','Lateral Move-
ment','Collection','Exfiltration','Command and Control'],\n";
   print "         'datasets':[{\n";
   print "                 'label':'Killchain',\n";
   print "                 $data_string\n";
   print "                 'fill':true,\n";
   print "                 'backgroundColor':'rgba(255, 99, 132, 0.2)',\n";
   print "                 'borderColor':'rgb(255, 99, 132)',\n";
   print "                 'pointBackgroundColor':'rgb(255, 99, 132)',\n";
   print "                 'pointBorderColor':'#fff',\n";
   print "                 'pointHoverBackgroundColor':'#fff',\n";
   print "                 'pointHoverBorderColor':'rgb(255, 99, 132)'\n";
   print "              },\n";
   print "
]},'options':{'elements':{'line':{'tension':0,'borderWidth':3}}}});</script>\n";

} # end sub

sub print_pie_chart {

   my ($chartid,$data_type,%rawdata) = @_;

   my $data_string;                    # All mighty data string used for the graph
   my $labels_string;                  # Labels string (X axis)
   my $label;                          # Label above the graph
   # Figure out how many CIS controls are included and then print labels, data and back-
groundColor
   if ($data_type eq 'cis') {
      # We must have: Data=Count of entries, labels=CIS controls
      # We have {log_file}{cis}{nist}
      ($data_string,$labels_string)=prepare_cis_graph_data(%rawdata);
   }

   print "<script>\n";
   print "new Chart(document.getElementById('$chartid'),{\n";
   print "    'type':'doughnut',\n";
   print "    'data':{\n";
   print "          $labels_string\n";
   print "         'datasets':[{\n";
   print "                 'label':'CIS Coverage',\n";
   print "                  $data_string\n";
   print "                 'backgroundColor':[\n";
   print "                      'rgb(255, 99, 132)',\n";
   print "                      'rgb(54, 162, 235)',\n";
   print "                      'rgba(54, 162, 235, 0.2)',\n";
   print "                      'rgba(255, 206, 86, 0.2)',\n";
   print "                      'rgba(75, 192, 192, 0.2)',\n";
   print "                      'rgb(255, 205, 86)'\n";
```

```
   print "                  ]\n";
   print "          }]\n";
   print "    }\n";
   print "});\n";
   print "</script>\n";

} # end sub
```

7.3 Bibliography

AuditScripts. (2019, 04 10). *AuditScripts Critical Security Control Manual Assessment Tool – v7.0a.* Retrieved from https://www.auditscripts.com/?attachment_id=3816

AuditScripts. (2019, 02 25). *Critical Security Controls.* Retrieved from https://www.auditscripts.com/free-resources/critical-security-controls/

BAE Systems. (2019, 02 23). *Looking Back to Spring Forward BAE Systems 2019 Cyber Threat Predictions.* Retrieved from https://www.baesystems.com/en/cybersecurity/feature/five-cyber-security-predictions-for-2019

Bodeau , D., & Graubart , R. (2019, 02 28). *Characterizing Effects on the Cyber Adversary .* Retrieved from https://www.mitre.org/sites/default/files/publications/characterizing-effects-cyber-adversary-13-4173.pdf

Bootstrap. (2019, 04 02). *Bootstrap*. Retrieved from https://getbootstrap.com/

Borboën, Yan; PwC Switzerland. (2019, 03 04). *IT and cyber risk management – where do you stand?* Retrieved from https://www.pwc.ch/en/insights/it-and-cyber-risk-management-english.html

BSI. (2019, 02 25). *BSI-Standards*. Retrieved from https://www.bsi.bund.de/EN/Publications/BSIStandards/BSIStandards_node.html

Carbon Black. (2019, 03 02). *Carbon Black Delivers MITRE ATT&CK™ Coverage with Zero Delayed Detections & Zero Tainted Detections*. Retrieved from https://www.carbonblack.com/company/news/press-releases/carbon-black-delivers-mitre-attck-coverage-with-zero-delayed-detections-zero-tainted-detections/

CFR. (2019, 02 23). *Cyber Operations Tracker*. Retrieved from https://www.cfr.org/interactive/cyber-operations

Chart.js. (2019, 04 02). *Chart.js*. Retrieved from Simple yet flexible JavaScript charting for designers & developers

Checkpoint. (2019, 02 23). *Cyber Attack Trends Analysis.* Retrieved from https://pages.checkpoint.com/cyber-security-report-2019-trends.html

Chuvakin, Anton; Barros, Augusto;. (2019, 02 22). *How to Develop and Maintain Security Monitoring Use Cases.* Retrieved from https://www.gartner.com/doc/3844970

Chuvakin, D. A. (2019, 02 21). *The complete guide to Log and Event Management.* Retrieved from https://www.microfocus.com/media/white-paper/the_complete_guide_to_log_and_event_management_wp.pdf

CIS. (2019, 02 22). *CIS Controls*. Retrieved from https://www.cisecurity.org/controls/

CIS. (2019, 04 2019). *CIS Controls V7.1 Mapping to Implementation Groups.* Retrieved from https://www.cisecurity.org/white-papers/cis-controls-v-7-1-mapping-to-implementation-groups/

CIS. (2019, 04 10). *CIS Controls V7.1 Mapping to NIST CSF*. Retrieved from https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/

CIS. (2019, 04 10). *CIS Controls V7.1 Mapping to NIST CSF.* Retrieved from https://www.cisecurity.org/white-papers/cis-controls-v7-1-mapping-to-nist-csf/

CIS. (2019, 02 21). *CIS Critical Security Controls Mapping Poster.* Retrieved from https://www.cisecurity.org/wp-content/uploads/2017/03/Poster_Winter2016_CSCs.pdf

CIS. (2019, 04 10). *CIS Mapping and Compliance*. Retrieved from https://www.cisecurity.org/cybersecurity-tools/mapping-compliance/

Cisco. (2019, 02 23). *Defending against today's critical threats.* Retrieved from https://www.cisco.com/c/en/us/products/security/security-reports.html

COBIT. (2019, 02 22). *COBIT.* Retrieved from https://en.wikipedia.org/wiki/COBIT

CSIS. (2019, 02 23). *Significant Cyber Incidents Since 2006.* Retrieved from https://csis-prod.s3.amazonaws.com/s3fs-public/190211_Significant_Cyber_Events_List.pdf

Dorigo, S. (2012). *Security Information and Event Management, Master Thesis on the methodology, implementation challenges, security issues and privacy implications concerning SIEM environments.* Nijmegen: Radboud University Nijmegen.

Dr. Hugh, T., & Steve, T. (2019, 02 23). *Cyber Security Predictions: 2019 and Beyond.* Retrieved from https://www.symantec.com/blogs/feature-stories/cyber-security-predictions-2019-and-beyond

Exabeam. (2019, 02 19). *10 SIEM Use Cases in a Modern Threat Landscape*. Retrieved from https://www.exabeam.com/siem-guide/siem-use-cases/

Exabeam. (2019, 03 14). *SIEM Logging Sources*. Retrieved from https://www.exabeam.com/siem-guide/siem-architecture/

Faircloth, R. (2016, 02 24). A Framework For Developing And OperaIonalizing Security Use Cases. *Splunk .conf2016* (p. 34). Los Angeles: Splunk. Retrieved from https://conf.splunk.com/files/2016/slides/a-framework-for-developing-and-operationalizing-security-use-cases.pdf

Federal Office for National Economic Supply FONES. (2018). Minimum standard for improving ICT resilience. Bern, Bern, Switzerland.

FireEye. (2019, 02 23). *FACING FORWARD Cyber Security in 2019 and Beyond.* Retrieved from https://content.fireeye.com/predictions/rpt-security-predictions-2019

Forcepoint. (2019, 02 23). *2019 Forcepoint Cybersecurity Predictions Report.* Retrieved from https://www.forcepoint.com/sites/default/files/resources/files/report-2019-cybersecurity-predictions-en.pdf

Forensic Labs. (2019, 02 22). *Forensic detection of MITRE ATT&CK Techniques*. Retrieved from https://medium.com/@cloudyforensics/forensic-detection-of-mitre-att-ck-techniques-83940f3b86ec

Froud, D. (2019, 02 22). *PCI-DSS and ISO 27001 mapping.* Retrieved from http://www.davidfroud.com/wp-content/uploads/2013/06/PCI-DSS-v3.2-vs-ISO-27001-2013_160729.xlsx

Glick, A. (2019, 04 07). *Why MITRE ATT&CK Matters.* Retrieved from https://www.symantec.com/blogs/expert-perspectives/why-mitre-attck-matters

Google Scholar. (2019, 02 24). *Google Scholar*. Retrieved from https://scholar.google.com

Hackmageddon. (2019, 02 23). *Hackmageddon 2018 Master Table.* Retrieved from https://www.hackmageddon.com/2018-master-table/

IBM. (2019, 02 23). *IBM X-Force Threat Intelligence Index 2018.* Retrieved from https://www.ibm.com/downloads/cas/MKJOL3DG

ISA. (2019, 02 22). *ANSI/ISA-62443-3-3 (99.03.03) Security for industrial automation and control systems Part 3-3: System security requirements and security levels*. Retrieved from https://www.isa.org/store/ansi/isa-62443-3-3-990303-2013-security-for-industrial-

automation-and-control-systems-part-3-3-system-security-requirements-and-security-levels/116785

ISA. (2019, 02 24). *ISA/IEC 62443 (ISA-99)*. Retrieved from http://isaeurope.com/isa99/

ISA. (2019, 02 22). *ISA–62443-2-1–2009 Security for Industrial Automation and Control Systems: Establishing an Industrial Automation and Control Systems Security Program*. Retrieved from https://www.isa.org/store/ansi/isa%E2%80%9362443-2-1-990201%E2%80%932009-security-for-industrial-automation-and-control-systems-establishing-an-industrial-automation-and-control-systems-security-program-/116731

ISACA. (2019, 02 22). *COBIT.* Retrieved from http://www.isaca.org/cobit/pages/default.aspx

ISACA. (2019, 02 22). *Information Systems Audit and Control Association.* Retrieved from https://www.isaca.org/pages/default.aspx

ISO. (2019, 02 25). *Information technology -- Security techniques -- Information security management guidelines based on ISO/IEC 27002 for process control systems specific to the energy utility industry.* Retrieved from https://www.iso.org/standard/43759.html

ISO. (2019, 02 22). *ISO/ICE 27001.* Retrieved from https://www.iso.org/isoiec-27001-information-security.html

ISO 27001. (2019, 02 22). *GDPR-ISO27k mapping.* Retrieved from http://www.iso27001security.com/ISO27k_GDPR_mapping_release_1.docx

it, p. (2019, 03 02). *How to add a module to Metasploit from Exploit-DB*. Retrieved from https://medium.com/@pentest_it/how-to-add-a-module-to-metasploit-from-exploit-db-d389c2a33f6d

Kane, M. (2019, 02 22). *GDPR – ISO 27001 Mapping Tool.* Retrieved from https://www.certificationeurope.com/insights/gdpr-iso-27001-mapping-tool-now-available/

Kaspersky. (2019, 02 23). *Cyberthreats to financial institutions 2019: Overview and Predictions.* Retrieved from https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/11/27083106/Financial-cyber-threat-predictions-for-2019.pdf

Lockheed Martin. (2019, 02 22). *Cyber Kill Chain.* Retrieved from https://lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html

Logpoint. (2019, 02 22). *Top 10 SIEM Use Cases.* Retrieved from http://www.config.ma/wp-content/uploads/sites/15/2016/12/Top-10-SIEM-cases-with-screen-dumps.pdf

Malware Wiki. (2019, 02 24). *Malware Wiki - Petya*. Retrieved from http://malware.wikia.com/wiki/Petya

Malware Wiki. (2019, 02 24). *Malware Wiki - WannaCry*. Retrieved from http://malware.wikia.com/wiki/WannaCry

Man, J. (2019, 04 15). *How to talk about cybersecurity in your organization*. Retrieved from https://blog.apnic.net/2018/12/14/how-to-talk-about-cybersecurity-in-your-organization/

Metasploit. (2019, 03 02). Retrieved from Rapid7: https://www.metasploit.com/

Microsoft. (2019, 02 23). *Microsoft Security Intelligence Report.* Retrieved from https://info.microsoft.com/ww-landing-Security-Intelligence-Report-Vol-23-Landing-Page-eBook.html

Minimal ICT Standard. (2019, 02 21). Retrieved from https://www.bwl.admin.ch/bwl/de/home/themen/ikt/ikt_minimalstandard.html

Mitre. (2019, 03 12). *CVE*. Retrieved from https://cve.mitre.org/

Mitre. (2019, 02 22). *Mitre Att&ck Data.* Retrieved from https://github.com/mitre/cti/tree/master/enterprise-attack

Mitre. (2019, 02 18). *Mitre Att@ck Framework*. Retrieved from https://attack.mitre.org/

Mitre. (2019, 03 23). *Mitre Philosophy behind Att@ck.* Retrieved from https://www.mitre.org/sites/default/files/publications/pr-18-0944-11-mitre-attack-design-and-philosophy.pdf

Mitre Att&ck. (2019, 04 18). *APT18*. Retrieved from https://attack.mitre.org/groups/G0026/

National Institute of Standards and Technology. (2019, 02 19). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework/framework

NERC. (2019, 02 25). *NERC Standard*. Retrieved from https://www.nerc.com/pa/Stand/Pages/default.aspx

NERC. (2019, 02 25). *NERC-CIP*. Retrieved from https://www.nerc.com/pa/Stand/pages/cipstandards.aspx

Nicole, P., Amie, T., & Adam, S. (2019, 02 23). *Marriott Hacking Exposes Data of Up to 500 Million Guests*. Retrieved from https://www.nytimes.com/2018/11/30/business/marriott-data-breach.html

NIST. (2019, 02 22). *Framework for Improving Critical Infrastructure Cybersecurity.* Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

NIST. (2019, 02 21). *Framework Improving Critical Infrastructure Cybersecurity version 11.* Retrieved from https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity-version-11

NIST. (2019, 04 16). *NIST Cybersecurity Framework*. Retrieved from https://www.nist.gov/cyberframework

NIST. (2019, 04 10). *SP 800-53 Rev. 4 - Security and Privacy Controls for Federal Information Systems and Organizations.* Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

Obermeier, S., Schneider, J., & Schlegel, R. (2019, 02 25). *Assessing the Security of IEC 62351.* Retrieved from https://www.researchgate.net/publication/300343725_Assessing_the_Security_of_IEC_62351

Offensive Security. (2019, 02 23). *About Exploit-DB*. Retrieved from https://www.exploit-db.com/

Offensive Security. (2019, 02 23). *The Exploit Database Git Repository*. Retrieved from https://github.com/offensive-security/exploitdb

Outpost 24. (2019, 02 23). *TOP 10 of the world's largest cyberattacks*. Retrieved from https://outpost24.com/blog/top-10-of-the-world-biggest-cyberattacks

Özkan, S. (2019, 03 12). *CVE Details.* Retrieved from https://www.cvedetails.com/top-50-product-cvssscore-distribution.php

Perniola, A., & Gray, D. (2019, 02 21). *Targeted SOC Use Cases for Effective.* Retrieved from https://digital-forensics.sans.org/media/Targeted-SOC-Use-Cases-for-effective-Incident-Detection-and-Response-Angelo-Perniola-David-Gray.pdf

Roe, S. (2019, 02 21). *4 SIEM Use Cases That Will Dramatically Improve Your Enterprise Security*. Retrieved from https://www.alienvault.com/blogs/security-essentials/4-siem-use-cases-that-will-dramatically-improve-your-enterprise-security

Security Event Management. (2019, 02 18). Retrieved from https://en.wikipedia.org/wiki/Security_event_manager

Security information and event management. (2019, 02 18). Retrieved from https://en.wikipedia.org/wiki/Security_information_and_event_management

Security information management. (2019, 02 18). Retrieved from https://en.wikipedia.org/wiki/Security_information_management

Security Operation Center. (2019, 02 22). Retrieved from https://en.wikipedia.org/wiki/Information_security_operations_center

Semantic Scholar. (2019, 02 24). *Semantic Scholar*. Retrieved from https://www.semanticscholar.org/

Smith, T. (2019, 03 01). *The MITRE ATT&CK Framework: What You Need to Know*. Retrieved from https://securityboulevard.com/2018/07/the-mitre-attck-framework-what-you-need-to-know/

Smith, Travis; Tripwire. (2019, 02 22). *Mapping the ATT&CK Framework to CIS Controls.* Retrieved from https://www.tripwire.com/state-of-security/security-data-protection/security-controls/mapping-the-attck-framework-to-cis-controls/

Stein, L. (2019, 04 01). *CGI*. Retrieved from https://perldoc.perl.org/CGI.html

Stoner, J. (2019, 03 01). *ATT&CK-ing the Adversary: Episode 3 – Operationalizing ATT&CK with Splunk*. Retrieved from https://www.splunk.com/blog/2019/02/08/att-ck-ing-the-adversary-episode-3-operationalizing-att-ck-with-splunk.html

Switch. (2019, 02 22). *SWITCH-CERT for Banks.* Retrieved from SWITCH-CERT for Banks

The Council on Foreign Relations. (2019, 02 23). *Cyber Operations Tracker*. Retrieved from https://www.cfr.org/interactive/cyber-operations

The Pennsylvania State University. (2019, 02 24). *SiteSeerX*. Retrieved from http://citeseerx.ist.psu.edu

Tripwire. (2019, 02 22). *MITRE ATT&CK Matrix with CIS Controls and Tripwire Mapping.* Retrieved from https://www.tripwire.com/solutions/configure-and-harden-your-systems/mitre-attck-matrix-with-cis-controls-and-tripwire-mapping-register/

University of Trier. (2019, 02 24). *DBLP*. Retrieved from https://dblp.org/

US Department of Health & Human Services. (2019, 02 22). *Health Information Privacy.* Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

van de Moosdijk, J., & Wagenaar, D. (2015). *Addressing SIEM - Determining focus areas and their coverage within IT risk frameworks.* Amsterdam: University Amsterdam.

VDA. (2019, 02 22). *VDA-ISA EN v4 TISAX.* Retrieved from https://www.vda.de/dam/vda/publications/2015/information-security-assessment-isa-en/VDA-ISA_EN_4.xlsx

Vindu, G., & Nicole, P. (2019, 02 23). *Yahoo Says 1 Billion User Accounts Were Hacked*. Retrieved from https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html

Wikipedia. (2019, 02 23). *Sony Pictures hack*. Retrieved from https://en.wikipedia.org/wiki/Sony_Pictures_hack

Zeinali, D. S. (2016). *Analysis of Security Information and Event Management (SIEM) Evasion and Detection Methods.* Tallinn: Tallinn University of Technology.

Statement of Authorship

I hereby declare that I have written the present work or the service I have indicated independently, without the assistance of third parties and only with the use of the sources indicated.

If this declaration subsequently proves to be untruthful, the Master's thesis shall be deemed not to have been passed.

Place, Date: Rotkreuz, 13.05.2019

Imthurn Pascal: ……