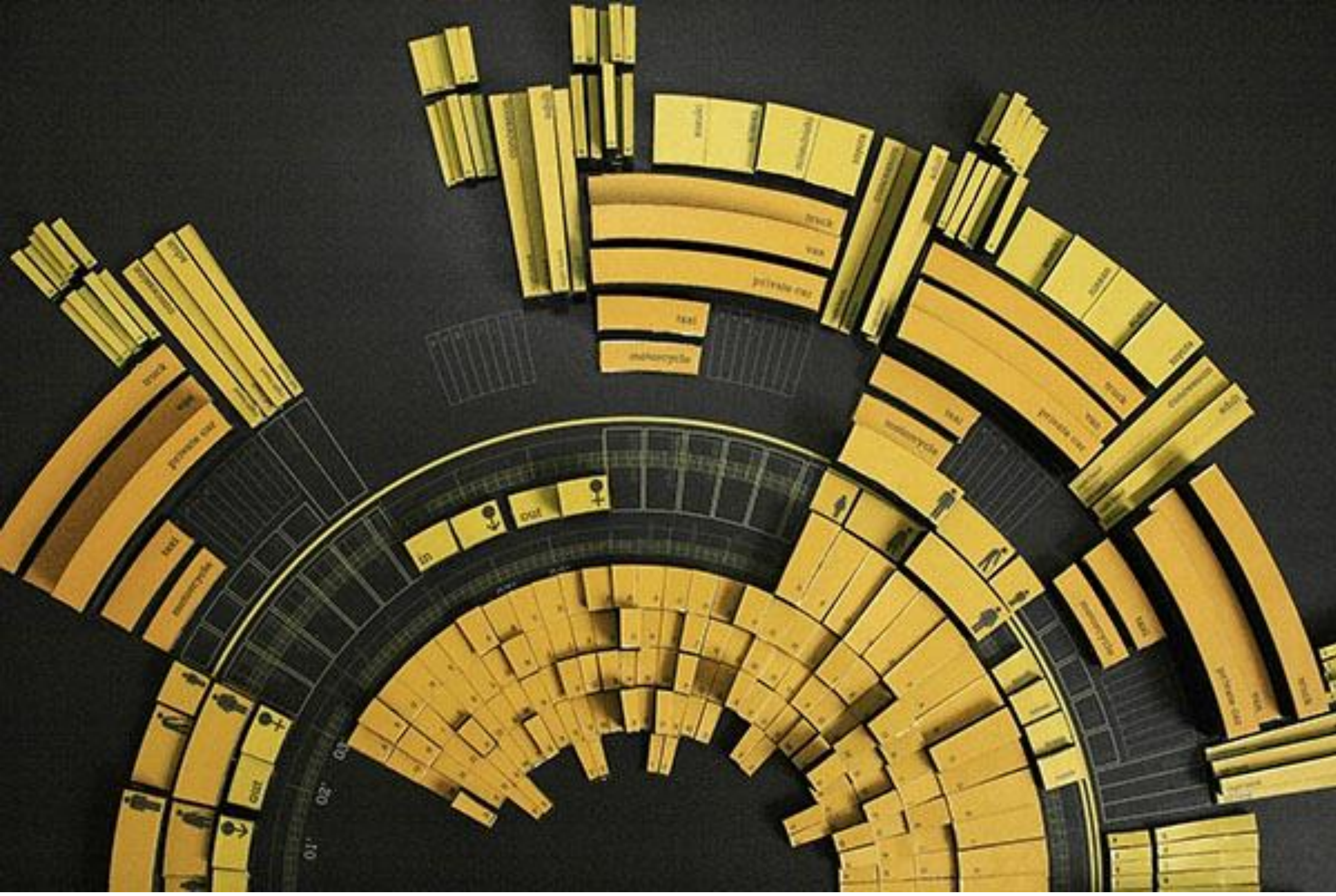

SGRP 1337 2019

Abstract of the master thesis “Methodology to select Security Information and Event Management (SIEM) Use Cases”

Author Pascal Imthurn

Submitted 08th of February 2020

Lucerne University of Applied Sciences and Arts

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.

The author is planning to publish a SIEM Use Case selection tool based on this research in the first quarter of 2020.

All references in this abstract are referenced in the thesis work "Methodology to select Security Information and Event Management (SIEM) Use Cases" (Imthurn, 2019).

What is the innovation of the master thesis?

The uniqueness of this research is to highlight the possibility to have a streamlined SIEM Use Case selection process for any company. Existing standard, frameworks and methodologies were used but linked in a unique way to optimise usage within the enterprise environment. The argument consists of the fact that individual domains such as cybersecurity frameworks, standards, threat databases exist, but no overarching answer to provide a solution to the SIEM Use Case selection issue.

The thesis follows a four phased approach:

The first step aims at the identification of the focus areas of the SIEM Use Case selection process. In combining both, the academic and vendor recommendations, we were able to produce a decision galaxy for SIEM Use Cases. 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.

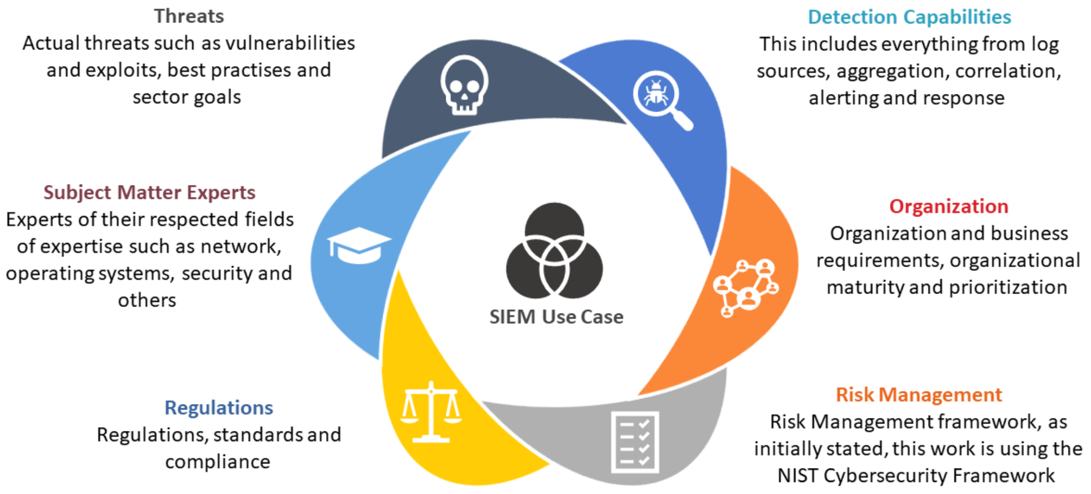
Threats
Actual threats such as vulnerabilities and exploits, best practises and sector goals
Detection Capabilities
This includes everything from log sources, aggregation, correlation, alerting and response
Subject Matter Experts
Experts of their respected fields of expertise such as network, operating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

Figure 1: Use Case Selection Galaxy

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.

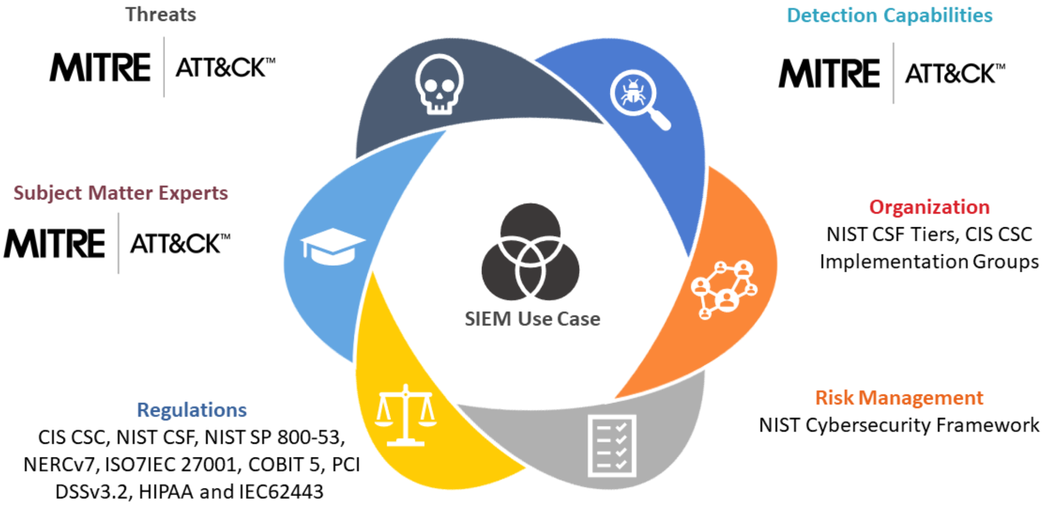
Threats
MITRE | ATT&CK™
Detection Capabilities
MITRE | ATT&CK™
Subject Matter Experts
MITRE | ATT&CK™
Organization
NIST CSF Tiers, CIS CSC Implementation Groups
SIEM Use Case
Risk Management
NIST Cybersecurity Framework
Regulations
CIS CSC, NIST CSF, NIST SP 800-53, NERCv7, ISO7IEC 27001, COBIT 5, PCI DSSv3.2, HIPAA and IEC62443

Figure 2: Simplified Use Case Selection Galaxy

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

The second step focuses on the identification of a threats & detection database. The research shows that the Mitre Att&ck Framework has proven to be the most effective dataset available. Achieved 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.

The goal of **the third step** is to identify an existing cybersecurity standard or framework, which can be mapped to threats and detection capabilities. The result indicates that several organisations produces datasets to allow for such a relationship model. The thesis selected the CIS, NIST and AuditScripts associations.

The fourth step is to analyse how organisations can select suitable detection methods for implementation considering cybersecurity threats and requirements defined in standards and frameworks. A selection of SIEM Use Cases becomes possible if a mapping between the Att&ck data and the CIS controls Framework exists. 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. The author notes that an even better mapping is achieved between single techniques and the CIS controls Framework.

And **finally**, the combination of all the previously discussed steps into a combined approach to select SIEM Use Cases.

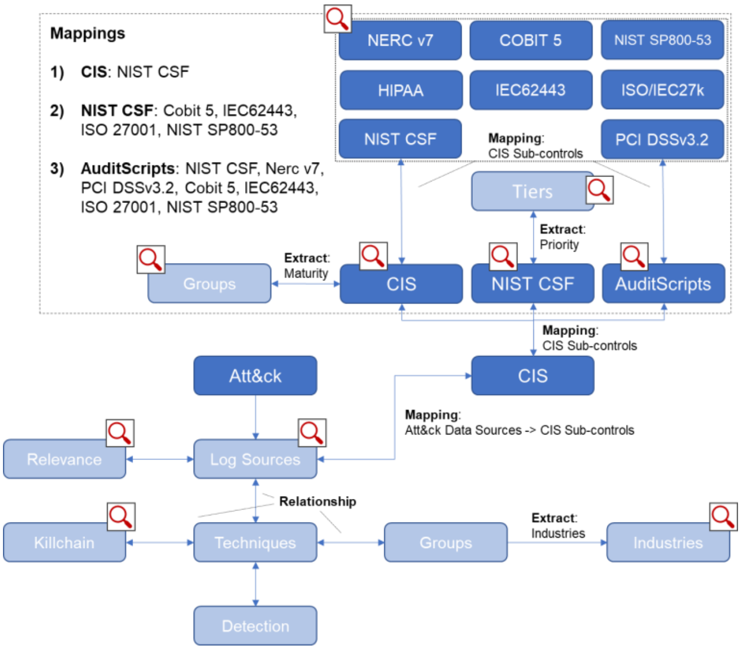

Figure 3: SIEM Use Case Selection Methodology

By combining the Mitre Att&ck Framework with the CIS Sub-controls, we can map individual standards to the detection techniques.

What was the motivation for the thesis?

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.

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.

What are the findings and main conclusions?

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 (e.g. Adding SME input or specific organisational requirements). 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.

This research provides the structure to create a tool (e.g. Excel Dashboard) for a guided SIEM Use Case selection process.

Flexibility of model

The model is highly flexible. 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. This results in, that anyone can create a valid mapping file.

The bi-directional links 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.

Who is the target group of the thesis?

The target group for this research are security professionals supporting, and companies of all sizes investing in a security detection program. This methodology allows for a structured selection process and raises the maturity of the cyber defence program. Data produced can also assist in improving overall return of investment (ROI) of such programs.

In combination of a NIST CSF driven SOC-CMM (SOC Capability Maturity Model) assessment, any company can start implementing a cyber security roadmap. The strength in combining the Security Operations Centre maturity with a comprehensible SIEM Use Case selection methodology provides any CISO or security professional a planning tool for their cyber defence strategy.