jamk.fi

Utilizing Cyber Security Kill Chain model to improve SIEM capabilities

Petri Toropainen

Master's thesis
May 2020
School of Technology
Degree Programme in Information Technology, Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Toropainen, Petri	Master's thesis	May 2020
		Language of publication: English
	Number of pages: 50	Permission for web publication: x

Title of publication

Utilizing Cyber Security Kill Chain model to improve SIEM capabilities

Degree programme

Degree Programme in Information Technology, Cyber Security

Supervisor(s)

Samir Puuska, Sampo Kotikoski

Assigned by

Istekki Oy

Abstract

In the current cyber threat situation, it is vital for an organization to be able to keep up to date cyber situational awareness (cyber SA) and detect the intrusion attempts. The everchanging cyber security threat situation forces organizations to deploy and utilize new tools and techniques to detect and react to events taking place in their environment. Security Information & Event Management (SIEM) is one of these systems that can be used to produce the cyber SA and detect those adversary events.

Cyber SA and Cyber Security Kill Chains were studied from the standpoint of developing SIEM system capabilities. One of the most important concepts was the SIEM use case used to describe the added value of the SIEM use case and its technical details. The objective was to create a novel construct that could be utilized in developing and managing SIEM use cases throughout its lifecycle and to help in directing the development efforts towards to the most needed sections of the environment.

Constructive research approach was utilized while researching problems arising from work life and trying to produce a novel construct to solve these problems. The produced construct was implemented, and the achieved results were analyzed with qualitative means. A set of interviews was held with the involved parties to get a wider view of the achieved results.

By utilizing the SIEM use case concepts and with the proposed construct, answers to the research questions were received, and it was discovered that the proposed construct provides the desired structure and methods to create and maintain SIEM use cases.

Keywords/tags (subjects)

SIEM, cyber security, cyber SA

Miscellaneous

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Toropainen, Petri	Opinnäytetyö, ylempi AMK	Toukokuu 2020
		Julkaisun kieli Englanti
	Sivumäärä 50	Verkkojulkaisulupa myönnetty: x

Työn nimi

Utilizing Cyber Security Kill Chain model to improve SIEM capabilities

Tutkinto-ohjelma

Degree Programme in Information Technology, Cyber Security

Työn ohjaaja(t)

Samir Puuska, Sampo Kotikoski

Toimeksiantaja(t)

Istekki Oy

Tiivistelmä

Vallitsevassa kyberturvallisuuden uhkatilanteessa organisaatioille on tärkeää ylläpitää reaaliaikaista kybertilannekuvaa, kyetäkseen havaitsemaan heidän ympäristöönsä kohdistuvat uhkat ja hyökkäysyritykset. Jatkuvat muutokset kyberturvallisuuden uhkatilanteessa pakottaa organisaatiot ottamaan käyttöön uusia työkaluja ja tekniikoita tapahtumien havainnointiin ja niihin reagoimiseen. SIEM (Security Information & Event Management) on yksi näistä järjestelmistä, jota voidaan hyödyntää kybertilannekuvan tuottamisessa ja tapahtumien havainnoimisessa.

Kybertilannekuvaa ja kyberturvallisuuden tappoketjuja tutkittiin SIEM-järjestelmän kyvykkyyksien kehittämisen näkökulmasta. Yksi tärkeimmistä käsitteistä oli SIEM-käyttötapaus, joka kuvaa SIEM-järjestelmän avulla tuotettavaa lisäarvoa ja sen tarvitsemia teknisiä yksityiskohtia. Tavoitteena oli muodostaa konstruktio ja menetelmiä SIEM-käyttötapausten elinkaaren hallintaan ja SIEM-käyttötapausten kohdentamiseen ympäristön eri osa-alueisiin.

Tutkimus toteutettiin konstruktiivisen tutkimusotteen avulla tutkien käytännön työelämästä noussutta ongelmaa. Ongelman ratkaisemiseksi muodostettiin konstruktio SIEM-käyttötapausten elinkaaresta ja hallinnasta. Ehdotettu ratkaisu toteutettiin käytännössä ja saavutettuja tuloksia arvioitiin laadullisesti. Haastattelujen avulla kerättiin kokemuksia ehdotetun konstruktion toteutukseen ja jalkautukseen osallistuneilta henkilöiltä, sekä saavutettiin tulosten arviointi laajemmasta näkökulmasta.

SIEM-käyttötapausten konseptin ja muodostetun konstruktion avulla saatiin vastauksia asetettuihin tutkimuskysymyksiin, sekä todettiin kuvatun konstruktion tuovan kaivattua rakennetta ja menetelmiä SIEM-käyttötapausten muodostamiseen ja hallintaan.

Avainsanat (asiasanat)

SIEM, kyberturvallisuus, kybertilannekuva

Muut tiedot

Contents

Figures

Tables

Glossary

MSSP	Managed Security Services Provider
NCSC-FI	National Cyber Security Center Finland
SOC	Security Operations Center
SA	Situational Awareness
APT	Advanced Persistent Threat
CKC	Cyber Security Kill Chain
IR	Incident Response
Zero-Day exploit	Previously undisclosed exploit with no fix or update available
UKC	The Unified Kill Chain
MO	Modus Operandi

1 Introduction

In the modern IT threat landscape the ability to produce up to date and relevant cyber security situational awareness (SA) is crucial for organizations in order for them to be able to detect and respond to the ever-growing amount of threat actors and ill activities taking place in their environments and this way to ensure their business continuity. Continuous development of cyber security threat landscape forces organizations to implement new tools and techniques constantly to detect and mitigate ongoing cyber events and security incidents.

In their 2019 Internet Security Threat Report Symantec stated that cyber criminals use living of the land technique and supply chain attacks more often while conducting attacks. Symantec has also seen a rise in targeted attacks utilizing above techniques and therefore these types of attacks pose a serious risk to organizations. Living of the land technique means utilizing built-in features of operating systems and off-the-shelf tools, and in supply chain attacks third-party services and software are exploited to gain access to a final target. According to Symantec, these types of attacks need advanced detection methods such as analytics and machine learning. (Symantec 2019, 17-18)

As many organizations outsource their IT infrastructure management, some organizations also outsource parts of the situational awareness creation to managed security services provider (MSSP) and to their security operations center (SOC). This makes forming and creating situational awareness of the cyber security events in the customer environments crucial for MSSP SOC services.

Cyber SA is typically formed by an SOC analyst by utilizing the output of multiple technical systems and external sources, e.g. NCSC-FI information sharing communities. Security information and event management (SIEM) system is one of these systems that aims to help SOC analysts in creating situational awareness. SIEM technology has been around for a substantially long time and as it is closing on the 20 years mark it is also closing the Plateau of Productivity stage on Gartners “Hype Cycle for Threat-Facing Technologies, 2018” (Shoard 2018).

The understanding of how attacks take place in the modern ICT environments makes it possible to detect the attacks and defend against them (Pols 2017, 9). An SOC analyst can utilize cyber security kill chain (CKC) models while forming cyber SA to be able to better comprehend the chain of actions taken place previously and to project the possible future actions taken by adversaries. Events presented in CKC phases can also be utilized when presenting this information to associated personnel, e.g. for a customer representative responsible for decision making.

This thesis is assigned by Istekki Oy. Istekki is an ICMT company providing ICT and medical technology services for its customers which are also its owners. As a part of these services there are Cybersecurity consultant and situational awareness services.

2 Research

2.1 Research objectives and framework

In this thesis, the creation of cyber security situational awareness and cyber security kill chains are studied from the perspective of SIEM system and SIEM use cases.

For every organization it is important to have the ability to detect and respond to cyber security incidents. Therefore, each organization needs to have cyber security situational awareness (SA), and SIEM system is an essential system in creating this cyber SA. While forming SA, the SOC analyst receives and processes SIEM system outputs. Each SIEM system output for the SOC analyst is based on specific reasons why that output was provided and what kind of threat that output could indicate. These reasons form the SIEM use case. After an SOC analyst has formed SA and detected the incident, it is possible to start cyber security incident management processes.

In this thesis the SIEM use case is the main concept. The SIEM use case includes the description of the threat that it responds to and the specific technology components and logic used to accomplish that objective, including the needed information requirements. The SIEM use case describes how the information is used to create and maintain cyber SA. As an output the SIEM use case can use alerts, reports or dashboards depending on the use case objective and operation logic. SIEM use case

is more specific than the general cyber security business use case or the goals set for security monitoring. Many SIEM vendor documents and other publicly available documents only describe the general security monitoring use case's which needs to be further refined into a SIEM use case.

The objective of this thesis is to form and propose a construct that is used for developing new SIEM use cases and to manage SIEM use cases throughout their lifecycle. This proposed construct should help security specialists in developing SIEM use cases that are relevant to the customer organizations' threat and risk management objectives and provide actionable and relevant output that help to create the cyber SA and a way to manage these SIEM use cases throughout their life cycle. In order to target SIEM use case development to the most important areas, a way to visualize and assess the capabilities provided by the SIEM system and a way to detect potential blind spots in detection capability is needed.

This thesis research does not seek to build new SIEM use cases, but to find and create ways to help develop and manage them and to assess the visibility those SIEM use cases provide, i.e. how the SIEM use case aims to improve cyber SA. Additionally, this thesis does not seek to find out initial reasons and justification for SIEM deployment or how to choose the right SIEM system platform.

2.2 Research methodology

It is typical for constructive research approach that the researcher's empirical intervention is explicit and strong, and the ideal outcome of constructive research is that a real-life problem is solved with a new implemented construction (Lukka 2001).

The main elements of the constructive research approach are practical relevance, practical functioning, theory connection and theoretical contribution. Figure 1. presents the four core elements of constructive research approach (Hyötyläinen, Häkkinen & Uusitalo 2014, 4; Lukka 2001). The constructive research approach starts by acquiring an in depth understanding of the research object both in theory and practice. The theoretical research is what differentiates constructive research from a consulting project. (Lukka 2001)

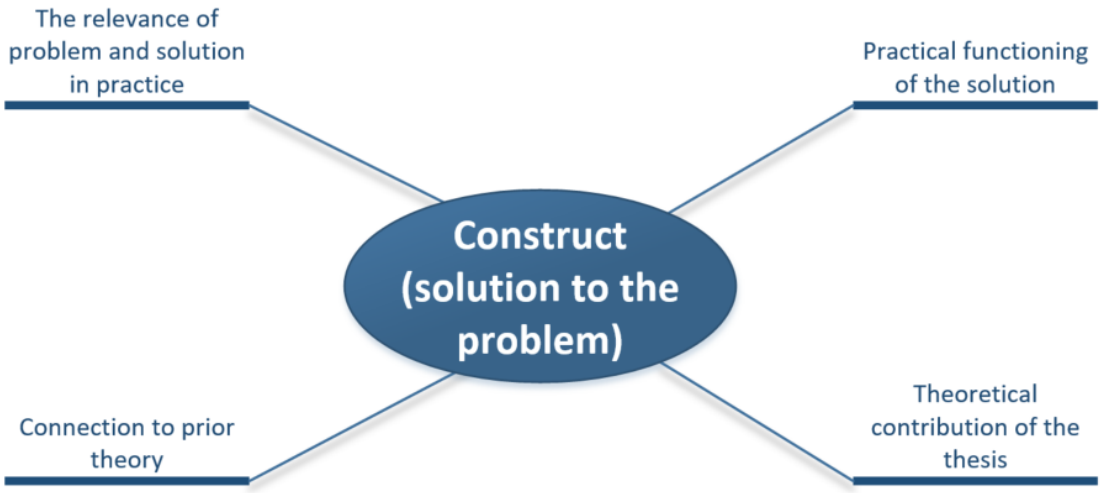

Figure 1. Constructive research approach

This research starts by defining the problem at hand and acquiring research papers and other theoretical information related to the subject and studying available methods and constructs used for solving similar kind of problems, e.g. cyber security kill chain and SIEM use case development methods. Figure 2. provides a schematic overview of the research approach and thesis process.

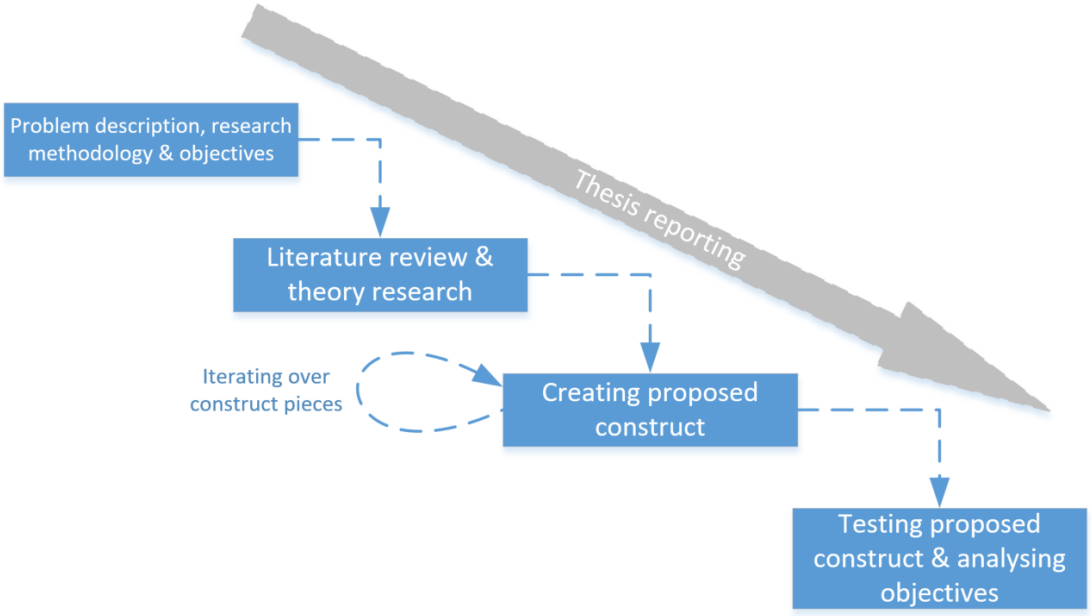

Figure 2. Schematic overview of the thesis process

The initial version of the proposed construct is created by combining the acquired theory knowledge and experience gathered through previous work experience and SIEM deployments. The proposed construct is further developed by iterating and

developing its pieces while creating SIEM use cases and developing SIEM capabilities with the team responsible for managing and developing the SIEM system.

After the proposed construct is finished, it is utilized and tested by creating SIEM use cases to customer environments and measuring its success by analyzing it against the objectives set for this thesis.

This analysis is carried out by interviewing people related to the SIEM and situational awareness by using theme interview method. Qualitative evaluation is conducted for the results of the interviews and researchers' personal experiences to assess the proposed solution and compare the acquired results with the objectives set for the thesis. In the theme interview the researcher discusses with the interviewee about beforehand defined topics or themes (Puustinen 2013, 5).

The theory connection and theoretical contribution are discussed in the theoretical part and the results section when analyzing the results. The practical relevance is demonstrated in chapters 3 & 4 and practical functioning in chapter 5.

The problem to be solved in this thesis emerges from the work life tribulations of creating SIEM use cases that provide effective situational awareness; hence, constructive research approach was chosen to be used in this thesis research.

Lukka (2001) describes that the risks included in the use of constructive research approach are research subjects and the high relevance of the findings to the employer's business, which could be too delicate to be published. Additionally, there is a risk that the research subject organization's commitment will not hold (Lukka 2001). These risks are recognized and accounted in the thesis process by concentrating more on the general problem than on the environments and processes of the employers and customers.

2.3 Research questions

Multiple studies and research articles can be found on cyber security kill chain, cyber security situational awareness and SIEM systems; however; only limited information could be found describing the ways to utilize these models and concepts together in practice, while trying to achieve better situational awareness and visibility into cyber security events by utilizing SIEM use cases from technical and practical standpoint.

To assist in defining the thesis contents and constraints and to structure this thesis, the following main research questions were set.

- How could the available frameworks, methods and tools be utilized to improve SIEM capabilities?
- How can cyber security kill chain models be used to create SIEM use cases?

Additionally, the following three sub research questions were set to further guide the process:

- How can organizations' risk and threat management information be used to guide in technical SIEM use case development?
- What are the most important requirements for creating new SIEM use cases?
- How could the visibility provided by the SIEM use cases be analyzed to recognize potential blind spots and assess the need for development of new use cases?

3 SIEM system as basis for situational awareness

3.1 Cyber security situational awareness

Situational awareness (SA) has been studied extensively in many applications, and it is also getting more popular in cyber security domain, where it is called cyber situational awareness (cyber SA) (Onwubiko 2016, 2).

An operator's SA is crucial to decision making, and as the complexity and dynamics of the environments increase, acquiring and maintaining SA becomes more difficult. Endsley (1995, 34) states that "S*ituation awareness, as such, incorporates an operator's understanding of the situation as a whole, forming a basis for decision making"*.

In the original SA model proposed by Endsley, SA consists of three aspects which are Perception, Comprehension and Projection. Perception aspect of the SA means awareness of the current situation with respect to time. Comprehension means understanding of the current situation, consequences, impact, changes in the situations over time, and possibly what could have caused it. Final SA aspect projection means estimation of the changes in the current state, and what could become of the impending situation if not controlled in time, and prediction of possible evolution of the current to impending situation. (Endsley 1995, 36-37)

A simple example of SA is a car driver who wants to know about obstacles in the way and to take these observations in to consideration to avoid colliding into them. To help the driver in forming SA, many modern cars have sensors to track the proximity of objects around the car.

Cyber security environments are very complex and contain many aspects with challenging and dynamic states. Therefore, up to date SA is needed for informed decision making. Cyber SA is similar to applications of SA in air traffic control or ground military operations. (Onwubiko 2016, 5)

Onwubiko (2016, 6) summarizes Cyber SA as follows:

> *In summary, Cyber SA encompasses people (operator/team), process and technology required to gain awareness of historic,current and impending (future) situations in cyber, the comprehension of such situations, and using those understandings to estimate how current situations may change, and through those predict future situations and the resolution of the current situation, and the enablement of controls to protect the systems from future projected incidents.*

Endsley originally described three levels (L1-L3) of SA, and McGuinness and Foy extended this to include resolution as the level four (L4). In relation to Cyber SA, Onwubiko states that perception (Level 1) is related to evidence gathering of cyber situations. Comprehension (Level 2) is related to understanding the situation by analysing the evidence gathered and the events observed in cyber situation combined with threat and risk level and identification of attack types. Projection (Level 3) means forecasting the future situations or states by understanding the ways current state could escalate. Resolution (Level 4) is related to controls that could be used to repair, recover, remedy and resolve the conceived situation. Figure 3 represents these SA levels. (Onwubiko 2016, 7-9).

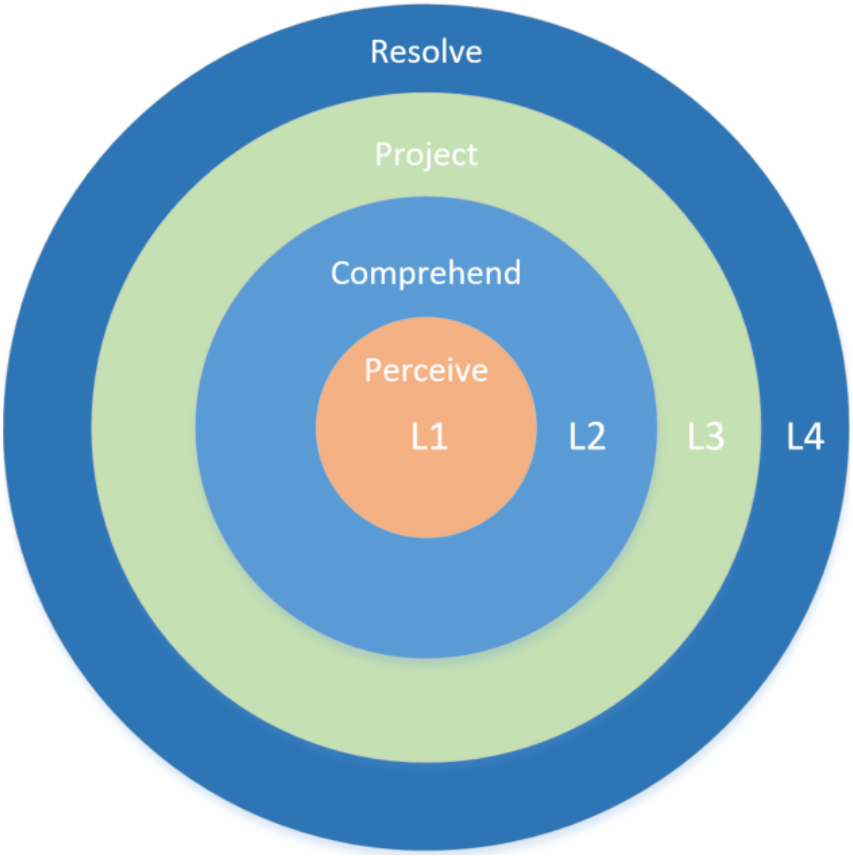

Figure 3. Cyber SA levels

While Cyber SA exists on different levels, these levels depend on the underlying layer; Level 2 could not be acquired without level 1, i.e. the current and future situation could not be projected if the situation is not perceived (logs of events received) and comprehended (operator analysis done by aggregating and correlating events) (Onwubiko 2016, 10-11).

In his paper "Understanding Cyber Situation Awareness", Onwubiko proposed a Cyber SA Instantiation Model which is an overlay of the modified Endsley's process model. It enables the use of situation awareness process model when building new Cyber SA applications or assessing existing implementations. This model is shown in Figure 4. (Onwubiko 2016, 12).

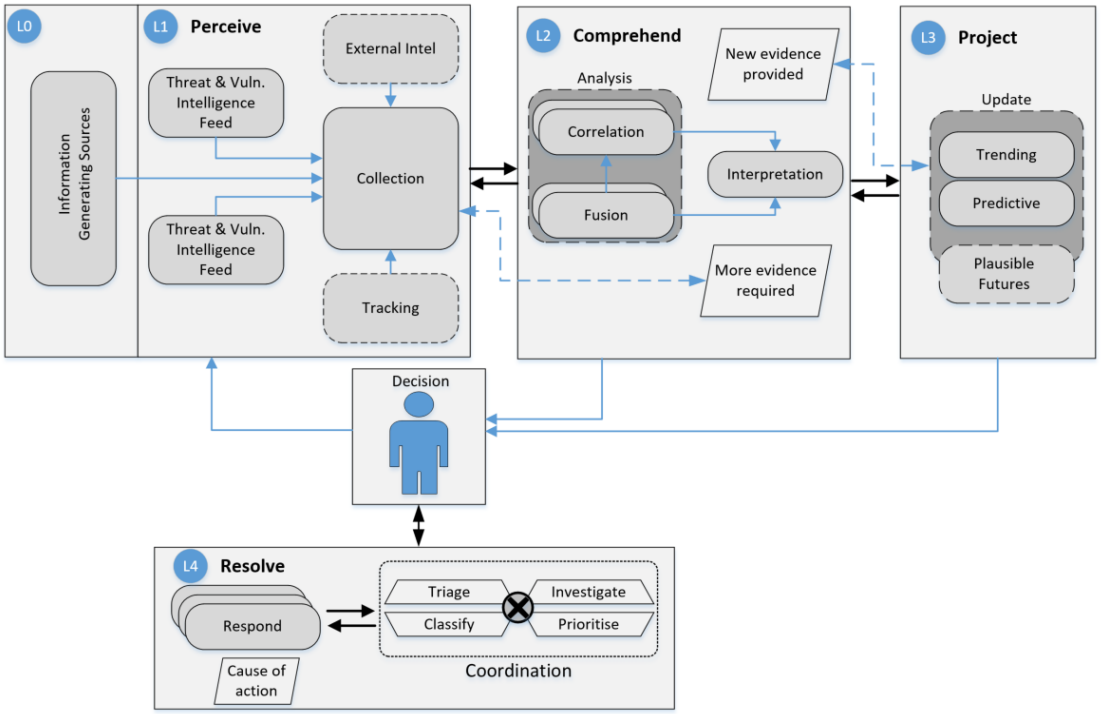

Figure 4. Cyber SA instantiation model

In Cyber SA instantiation model, there are five broad sources that provide information for SA creation. The first sources are classified as information generating sources and classified as L0. These are systems that provide logs of their operation and are targets of an attack, compromise or exploitation. These systems are not able to detect an attack by themselves unless there is some other mechanism built into them, e.g. Windows desktop computer with antivirus system installed. The logs provided by these information generating sources could contain pieces of evidence of an attack. (Onwubiko 2016, 12-13)

On L1 there are four sources that provide information for SA. These sources are protection enforcing sources, vulnerability and threat intelligence gathering sources, tracking and external intel. These L0 and L1 information sources feed information to a collection mechanism that is used to make this information available to L2 Comprehend stage, where different information is used to fully understand the situation. To help form level 2 SA, information could be fused and correlated to help understand and process it and therefore provide enhanced SA. The analysis of information collected should be continuous real-time process and even possibly automated. The collected information could be conflicting, or some parts could be missing; therefore, the analysis techniques must be such that they can take this into

account. Onwubiko (2016, 13-15) states that *"Finally, analysis is meaningless if its outcome cannot be interpreted and well understood".*

On Projection (L3) level, understanding of the current situation created in L2 is used to form possible outcomes and what can be done to influence to the outcome. Resolution (L4) focuses on steps needed to remedy, recover and resolve the situations and achieving this resolution includes processes and functions to triage, classify, prioritize and investigate situations. (Onwubiko 2016, 16)

Human factors affect the quality and performance of the formed SA. Attributes that affect this are skills, experience, abilities and training. Additionally, enviromental, workload and stress factors affect the individual's performance. (Onwubiko 2016, 8)

Studies show that when team members understand that SA is lacking information, they perform better than the teams thinking they have all needed information (Endsley 1995, 39-40).

3.2 Security Information and Event Management - SIEM

Security Information and Event management (SIEM) systems have been used for a long time in IT, and as the technology has evolved into more mature it is ready to be implemented by more and more organizations (Shoard 2018; Miller, Harris, Harper, Vandyke & Blask 2011). SIEM system is a collection of technologies designed to provide insight into events taking place in cyber security environment. SIEM system combines the Security Information Management (SIM) and Security Event Management (SEM) systems. (Miller et al. 2011, Introduction)

SIEM systems are designed to be used by security professionals and analysts to monitor security posture of IT environments and respond to security events. SIEM system uses alerts, dashboards and reports to deliver information for the SIEM users. It can detect security events by correlating events from different sources. Reduction of false positives is one important objective for SIEM systems, which is accomplished by correlating events. Correlating means to relate events to each other, e.g. correlating IDS alert information with Windows AD login events to detect user behind these actions. (Miller et al. 2011, Introduction)

Miller et al. (2011, Regulatory Compliance) state that for successful SIEM system deployment an organization needs to recognize its assets and consider the organization's risk and threat management information. SIEM can help the organization to protect all aspects of Confidentiality, Integrity and Availability, which is also known as CIA triangle (Frye 2010, 15)

To successfully be able to tie SIEM system usage to current threat landscape SIEM use cases need to be defined. These use cases define in what kind of events SIEM system is used to detect and what is the logic behind them. The risk and threat management processes of an organizations should be used to guide the selection of SIEM use cases to ensure efficient resource usage of SIEM systems (personnel and compute/storage). (Miller et al. 2011, Threat Models; Frye 2010, 8;) SIEM use case can be used to describe SIEM correlation alerts, monitoring dashboards and reports.

In his blog post Andre Hohner (2019) states the following about importance of SIEM use cases:

> *Without tangible use cases, the data in any SIEM would only be stored in a structured manner, enabling ex-post investigation if necessary – but near real-time monitoring of security-relevant parameters is a long way off.*

Generally, a SIEM system consists of collection layer, parsing and normalization layer, correlation and rule engine, log/data storage, information presentation layer and event management. The main building blocks of a SIEM system are presented in Figure 5. (Miller et al. 2011, chapter 5)

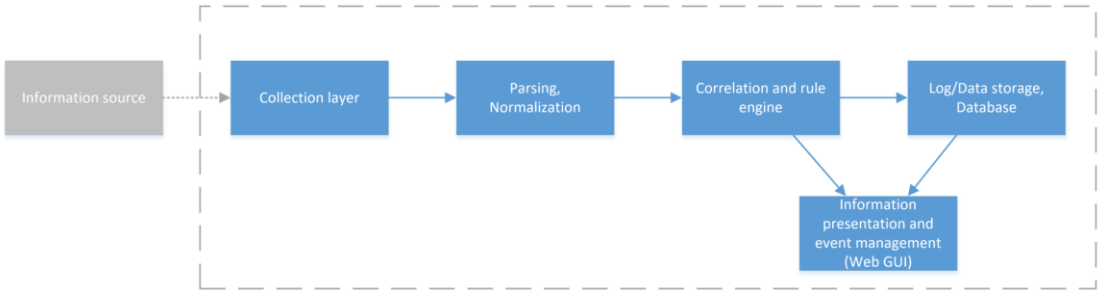

Figure 5. SIEM system building blocks

SIEM systems can utilize many different sources of information including Windows and Linux workstations and servers' events, firewall logs, IDS/IPS device alerts, network flow data and databases (Miller et al. 2011, The Anatomy of a SIEM). The information collected using different means is then parsed and normalized before indexing and storing into the database for searching and long-term storage. Rule and correlation engine go through the information with predefined rules to find the security events and then alerts the user. A SIEM user can also search through the information to perform additional searches by using graphical user interface, which is typically a web interface. (Logpoint Administrator training 2018)

3.3 SIEM as information source for Cyber SA

As stated in the previous chapter, a SIEM system collects information from different sources, combines, correlates, and enriches it for the analyst to consume and to understand. From this information and based on the previous paragraphs it can be deduced that a SIEM system works mainly in the Cyber SA levels 1-2 (perceive and comprehend) but it also could be developed to provide guidance and understanding on level 3 (projection) by tying events and alerts to predefined threat scenarios. This should be one of the guiding principles in the SIEM system design and use case development.

Lötjönen (2017, 37) stated in his thesis that *"cyber security and its situational awareness is much more than just a technical issue"*. This means that not one technical system could solve the creation of SA; however, technology and automation can help the persons responsible for creating cyber SA perform more efficiently and make decisions in more timely manner.

Information needs for different roles in Cyber security management differ as they are needed in order to make decisions on different level (Lötjönen 2017, 37), e.g. in MSSP SOC and a hospital customer case, the SOC analyst consumes information received from different technical systems to detect possible cyber security events, predicts possible outcomes and potential remedy steps and therefore forms personal and SOC team cyber SA. This information is then presented to the customers' personnel responsible for their IT environment decision making. With this received

information and with the current situation in the hospital environment, the customer representative forms their own cyber SA.

Based on the author's own experience, the conclusion from this is that the SIEM system and SIEM use case outputs should be mainly targeted towards the SOC analyst and people responsible for the maintenance of technical systems. In addition, SOC analysts should understand the chain of events behind the SIEM use case to be able to form a better SA. Importantly SOC analyst should understand and be aware of the potential blind spots in detection capabilities.

When working with and developing SIEM system use cases security specialists and analysts can benefit from the knowledge of Cyber SA and the different levels of it.

3.4 SIEM system use case creation models

As established in previous chapters, well planned SIEM use cases make the basis for SIEM system usage and provide benefits from the system in creating Cyber SA. In previous research and publications found on the topic, few different models were found describing the methods to be used in SIEM deployment and in developing SIEM use cases.

Initial SIEM use cases should be valuable and yet achievable in order to get the SIEM work started and prove SIEM system's effectiveness early on. SIEM use cases that provide the best value for organization depend on the organization's risk management, threats and business priorities; hence, they need to be defined independently for each organization and environment although many similarities may exist between organizations. (Chuvakin et al. 2018, 20)

In a SANS Institute publication "Effective Use Case Modeling for Security Information & Event Management" by Daniel Frye (2010, 9-15), the author suggests a Top-Down Bottom-Up Middle-Out (TDBUMO) design process to be used in developing SIEM use cases.

The Top-Down part of the method describes how the data will flow in to the SIEM system by grouping the data sources based on different categories e.g. operating system version and log collection method (Frye 2010, 9-15).

The Bottom-Up part of the model describes methods to find out which data points each log type includes. These data points are used to recognize correlations between the log sources and how the characteristics of each log source should be catalogued.

The Middle Out phase describes how to tie data points gathered in Bottom Up phase to SIEM use cases across the different systems found in the environment. Frye (2010, 9-15) suggests that the starting point of SIEM use case development should be asking the question *"What is important to maintain a profitable business model and to reduce the risk to that model?"* Frye (ibid.) also proposes to categorize all use cases with the CIA triad (Confidentiality, Integrity and Availability), as all of these could cause significant business risk.

Frye (2010, 7-8) also highlight the importance of understanding the difference between a business use case and a SIEM system use case. Business use case describes a general business requirement and SIEM use case describes the actual technology used in the SIEM system to achieve the requirements set in the business use case e.g. "Identify failed logins" is a business use case that needs to be defined more precisely to form a SIEM use case.

Chuvakin et al. (2018, 31-32) describe the Output driven SIEM method to be used in SIEM system design and operation. This model is based on the concept that logs can be collected only after log information usage in SIEM system has been defined, i.e. SIEM use cases are defined before the log collection is configured. The output driven SIEM method is illustrated in Figure 6. (Chuvaking et al. 2018); this pre-planned SIEM use case can include reports, visualization, alerts, dashboards or profiling algorithm. By using this approach, the SIEM system analyses only the data that is utilized and thus avoids the common problem of having masses of data in a SIEM system without any insight gained from it. Using this model makes a distinction between a SIEM system and broad-scope log management which is used just to collect the logs and not to provide security insights from it.

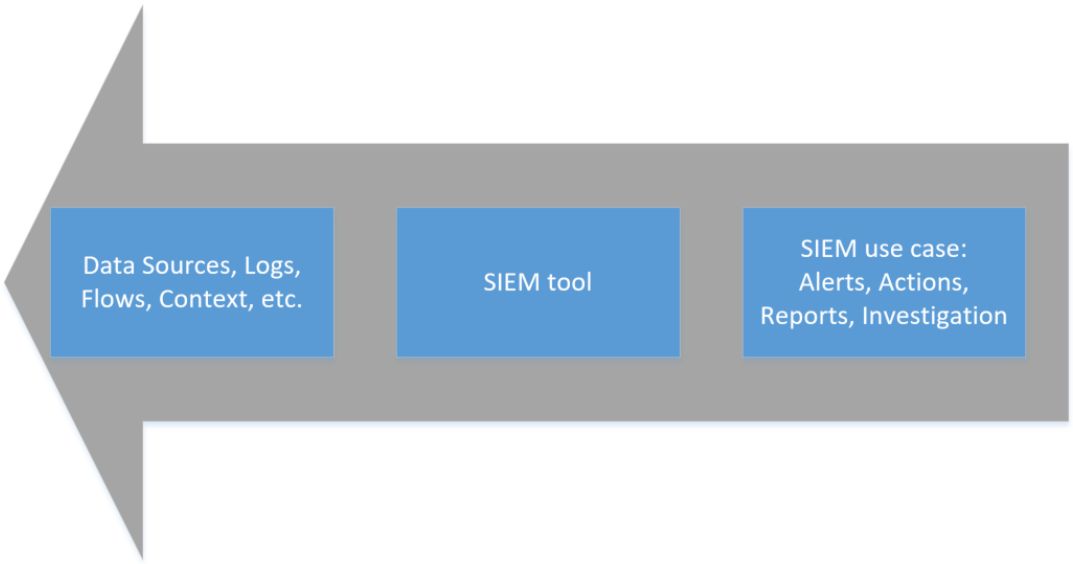

Figure 6. Output driven SIEM

Chuvaking et al. (2018, 32) raised the concern that if output driven SIEM deployment is not followed and "*just collect it for now and figure out what to do with it later*" method is used, the SIEM deployment could be stuck in this stage for years without providing any real value for the organization.

3.5 SIEM use case creation and deployment issues

Many sources have stated and recognized problems in SIEM system deployment, use case creation, implementation and continuous development. Hohner (2019) stated that many SIEM projects face challenges because they do not have clear focus on project goals, no structure during use case creation and no control over involved stakeholders.

As a remediation Hohner (2019) stated that SIEM project should initially focus on aiming at quick wins, use risk-based approach and include business requirements at decision making. To make use cases more effective stakeholders should be involved in SIEM use case creation, e.g. application owners who understand how the application or information system operates and how it affects organization's business goals can be stakeholders.

Chuvakin, Belak and Barros (2018) state that SIEM implementations fail to deliver full value because of broken practices in use case scoping, readiness and design. They also stated the following:

> *Technical professionals are often surprised that simply acquiring and installing a SIEM product does not automatically improve the organization's threat detection and security posture.*

This statement by Chuvakin et al. (2018) also supports the author's experiences with the topic, as the real work to provide value starts after finishing the initial deployment, and the ability to start monitoring the environment with the means of logs is achieved.

Chuvakin et al. (2018) suggest that SIEM deployment should be implemented in small continuous deployment steps to deliver value sooner and with less risk of getting stuck in technical and organizational prerequisites.

According to Vasudevan (n.d. 3), most organizations rely on the SIEM vendor provided default rules, although it is unclear that this approach provides monitoring for the specific risks the organization is facing and should be watching for. He also summarizes that security monitoring is primarily dependent on the quality of the use cases (Vasudevan n.d. 14).

According to Frye (2010, 14), underfunding SIEM deployment is detrimental and to avoid this he proposes to create a strong partnership with the individual business units as it is their information that is being protected with the SIEM system.

Because of the complex problem to be solved, many sources state on the importance of starting from small and useful SIEM use cases to deliver results quickly and to let the organization learn as the work goes on. This applies to both the security specialist and customer organizations' IT management. Additionally, ensuring stakeholders and business units dedication and involvement in to the SIEM deployment seem to be highly recognized concern.

4 Cyber security kill chain models and frameworks

4.1 Cyber security Kill Chain & APT

As the information technology and computer systems have developed, also threats and threat actors being directed to them have evolved. Particularly capable threat actors are referred to as Advanced Persistent Threats (APTs). These APTs have substantial resources with the intent to compromise data for economic or military advancement. Typically, they are backed up by nation-states and normally, attacks by APTs include exploiting multiple systems and vulnerabilities along the attack path starting from the internet facing systems and advancing towards the target system and asset. As APTs have substantial resources, they try to develop their operations and perform intrusion after intrusion to reach their objective. (Pols 2017, 8-9; Hutchins, Cloppert &Amin 2010, 2-3)

The term kill chain has been used in a military context before it was introduced in the realm of cyber security by computer scientists at Lockheed Martin in 2010. Cyber security kill chain aims to describe the structure of the intrusion by APT actor, and it can be used by the defender to develop mitigations against intruders and prioritize investments in technology and processes. (Hutchins et al. 2010, 2)

In the original cyber security kill chain paper published by Lockheed Martin, the authors proposed an intelligence-driven and threat-focused risk management strategy, where analyzing intrusions from the attacker's point of view, the defensive steps and countermeasures could be determined and deployed faster than the adversaries could evolve their operation. In this model the assumption is that just one mitigation is enough to break an attackers' chain of actions and prevent the adversary from reaching their objective. (Pols 2017, 18; Hutchins et al. 2010, 3)

The kill chain model is based on the concept of indicators, i.e. information that objectively describes an intrusion. These indicators can be divided into three subtypes which are Atomic, Computed and Behavioral. Atomic indicators are the smallest forms of indicators and they cannot be broken down into smaller parts, e.g. IP addresses, email addresses and vulnerability information. Computed indicators most commonly include hash values that are computed from incident data, e.g.

malware executable file hash. Behavioral indicators combine other indicators together, e.g. IP address of the destination server where a user has downloaded a malicious file combined with hash of that file and timestamp of this event. Attention should be paid to processing and tracking indicators throughout their life cycle so that the analysts do not find themselves applying these techniques to threat actors for which they were not designed. This indicator life cycle and its states are presented in Figure 7. (Hutchins et al. 2010, 3-4).

SIEM system is used to find out these indicators of compromises (IOC) from the masses of data gathered from the information sources.

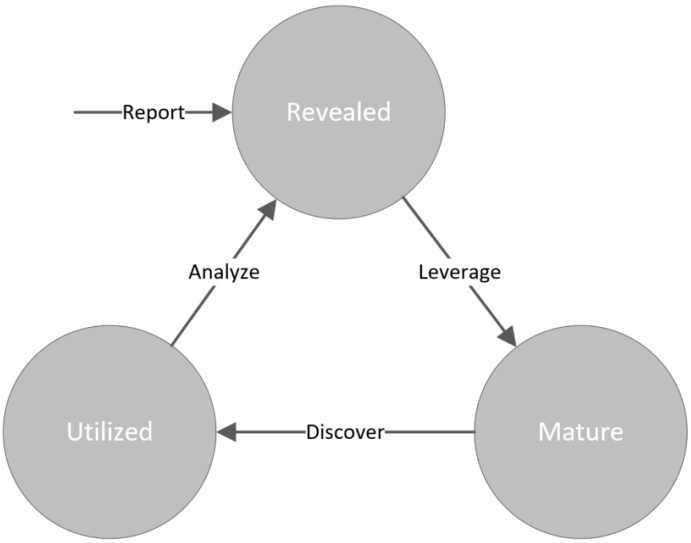

Figure 7. Indicator life cycle

Original Cyber security kill chain consists of seven (7) phases representing attacker objectives for computer network attack to be successful. Computer scientists at Lockheed Martin described the phases of the computer network attack kill chain as follows (Hutchins et al. 2010, 4-5):

1. ***Reconnaissance*** *- Research, identification and selection of targets, often represented as crawling Internet websites such as conference proceedings and mailing lists for email addresses, social relationships, or information on specific technologies.*

2. ***Weaponization*** *- Coupling a remote access trojan with an exploit into a deliverable payload, typically by means of an automated tool*

(weaponizer). Increasingly, client application data files such as Adobe Portable Document Format (PDF) or Microsoft Office documents serve as the weaponized deliverable.

3. ***Delivery*** *- Transmission of the weapon to the targeted environment. The three most prevalent delivery vectors for weaponized payloads by APT actors, as observed by the Lockheed Martin Computer Incident Response Team (LM-CIRT) for the years 2004-2010, are email attachments, websites, and USB removable media.*

4. ***Exploitation*** *- After the weapon is delivered to victim host, exploitation triggers intruders' code. Most often, exploitation targets an application or operating system vulnerability, but it could also more simply exploit the users themselves or leverage an operating system feature that auto-executes code.*

5. ***Installation*** *- Installation of a remote access trojan or backdoor on the victim system allows the adversary to maintain persistence inside the environment.*

6. ***Command and Control (C2)*** *- Typically, compromised hosts must beacon outbound to an Internet controller server to establish a C2 channel. APT malware especially requires manual interaction rather than conduct activity automatically. Once the C2 channel establishes, intruders have hands on the keyboard" access inside the target environment.*

7. ***Actions on Objectives*** *- Only now, after progressing through the first six phases, can intruders take actions to achieve their original objectives. Typically, this objective is data exfiltration which involves collecting, encrypting and extracting information from the victim environment; violations of data integrity or availability are potential objectives as well. Alternatively, the intruders may only desire access to the initial victim box for use as a hop point to compromise additional systems and move laterally inside the network.*

For the defender to fully benefit from utilizing the methods depicted in the cyber security kill chain paper, the defender should utilize intrusion reconstruction and campaign analysis to find out the adversary's previous steps after determining that an intrusion has taken place. After this it is possible to develop new detection methods that can be used to detect and mitigate future intrusions in earlier phases of CKC. Equally important is to do analysis on the unsuccessful and mitigated attacks and this way try to gain insight into what the adversary's objectives are and what might have happened if this attack could have been successful. (Hutchins et al. 2010, 6-7)

Detection techniques described previously can be SIEM use cases, which are used to detect the known indicators acquired by intrusion reconstruction methods. This way it is possible to try to defend also against zero-day threats by detecting indicators of adversary actions around the vulnerable software component or system.

4.2 Additional cyber security kill chain models and adaptation

4.2.1 Bryant kill chain

In their paper Bryant and Saiedian (2017) introduced a novel kill chain model named Bryant kill chain that is based on the original CKC by Lockheed Martin. In the Bryant kill chain some phases were omitted; the sequence was changed, and two new phases were introduced and a model with seven (7) phases was defined as presented in Figure 8. (Pols 2017, 22; Bryant & Saiedian 2017, 199-200)

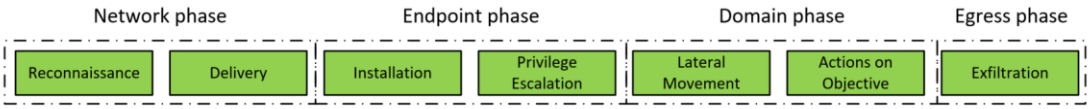

Figure 8. Bryant kill chain

In Bryant's kill chain paper (Bryant et.al. 2017, 201-205), the methods and procedures were introduced to apply the Bryant's kill chain model to network forensics and SIEM system data correlation and aggregation. By leveraging the Bryant kill chain model to lessons learned analysis of security breach, the analyst provided more through data compared to their peers implementing investigations using ad-hoc analytical methods. This paper provided indications that a kill chain model could

be utilized as an intermediate tool to communicate between the SOC analysts and security specialists to help further develop SIEM use cases.

4.2.2 Unified kill chain

In Paul Pols's (2017, 67-72) thesis The Unified Kill Chain (UKC) he analyzed the original CKC, multiple CKC variants and Mitre ATT&CK patterns as a literature study, performed analysis of multiple red team case studies and analysis on one APT group tactics to form the UKC model. This UKC model consists of 18 phases and therefore it expands on the granularity offered, compared to the many other CKC models consisting of 7 phases.

Pols (2017, 79) proposed that the UKC could prove useful in raising the resilience of organizations against other APT cyber attacks such as modern ransomware worms e.g. WannaCry, NotPetya and BadRabbit. The tactics implemented by these ransomware worms have been previously seen in targeted attacks and the tactics such as pivoting, privilege escalation and lateral movement, which among others were also identified in the attacks conducted by APT28 group.

4.2.3 Problems and limitations in cyber security kill chain models

In the Unified kill chain paper by Paul Pols (2017, 8; 79) the author states that the original CKC by Lockheed Martin relies on untested assumptions in describing the modus operandi (M.O.) of APTs. Original CKC guides to focus the defenders' efforts to disrupting and detecting the APT attacks at the earliest phase. Furthermore, the proposition that APT attack can be stopped by disrupting one of the phases in this chain of events was discovered to be false as attack phases can be bypassed. By bypassing the attack phase, the attacker may also bypass the security control or monitoring applying specifically to that phase.

Patrick Reidy (2013) stated that *"The Intrusion Kill Chain is excellent for attacks, but doesn't exactly work for insider threats".* This suggest that CKC cannot be used to defend against every types of threats.

Pols (2017, 79) suggests that realigning the defense strategy to the phases occurring more frequently or to the phases that are vital for the attack path to be successful.

Preventing the compromise of every single internet connected system in a large network is challenging, and it may be more effective to choose a strategy that focuses on defending the limited amount of critical supporting assets.

4.2.4 Cyber security kill chain usage with SIEM use cases

By assigning a CKC phase to each SIEM use case the whole intrusion can be understood better by the SOC analyst and this way improve the perceived cyber SA, and the SOC analyst can project the possible outcomes more precisely and faster. This CKC phase can be utilized when reviewing the overall visibility achieved with the implemented SIEM use cases and when planning for next steps in the SIEM use case roadmap.

5 SIEM use case management model

5.1 Target environment and description of observed problems

This chapter describes the environment where SIEM systems are deployed, the end customer organizations and the problems recognized while providing the SIEM system service and during the previous SIEM system deployments. The problems recognized and described here are based on the author's personal observations and free form interviews with the security specialists working with SIEM systems.

As part of the Managed Security Services Provider (MSSP) security services portfolio is a technical situational awareness service. This service is aiming to create and maintain cyber SA by monitoring the customers' environments with the means of different technical systems, different internal and external information sources and threat intelligence sources. SIEM system is an integral tool to be used in the creation of this cyber SA.

Typical customers of this technical situational awareness service are Finnish hospital districts, cities and public sector organization's. Each customer has their own multivendor IT environment including workstations, servers and networks. Each customer has multiple information systems specific to their environment, e.g. hospital patient information system or work scheduling system for city employees.

A SIEM system receives information and events in multiple formats from multiple systems and by the means of alerts, dashboards and reports the SIEM system helps SOC security analysts in forming the different levels of cyber SA for each of the customer's environments. For the security analyst it is impossible to know all the differences and potential weaknesses in detection capabilities or security architecture of each customer environment. Therefore, the outputs of the SIEM system (alerts, dashboards and reports) should provide the necessary information needed in cyber SA creation and integration to business goals and risks.

The SIEM use case acts as a tool in describing these information requirements, the outputs it provides, and how it is meant to contribute to the cyber SA. During this thesis process the term SIEM use case has been introduced to the workflow and conversations. This adoption was started by the security specialists working directly with SIEM system development, and then it started slowly to spread into use of other security specialists, sales personnel and customer IT management.

During previous SIEM deployments the problems observed included inaccurate project scope definition regarding the value provided by the SIEM system. This has been recognized to be mainly caused by the focus being on the log source selection and log management function instead of the initial SIEM use case selection and definition; e.g. SIEM projects have had log sources defined without predetermined usage for each log source, which has led to inefficient SIEM resource usage in compute and personnel areas.

Another important observation is that customer IT threat and risk management has not been fully matured to provide adequate feedback and guidance for SIEM deployments and SIEM use case creation and selection. This means that customer IT management is not fully aware of the threats that pose the greatest risk for the organizations' IT environment. This leads to the problem of not knowing where security monitoring should be targeted and what the most important information systems are to focus on. Customer IT management involvement in SIEM deployment has proven to be difficult due to an unconstructed and log source focused deployment strategy.

These realizations are the most important drivers for this thesis and call for a more structured way of choosing, managing and developing SIEM use cases for these customer environments.

5.2 Description of the proposed construct

The following SIEM use case management model was developed for this thesis. It consists of a SIEM use case lifecycle combined with a process flow describing the actions taking place in each phase of the lifecycle and supporting SIEM use case management tools to be used as a use case library and in creating novel SIEM use cases. This proposed management model aims to raise the maturity level of SIEM system utilization and implementation.

As stated in multiple literature references concerning utilization of SIEM use cases in designing and managing the SIEM deployment, they allow efficient use of compute and personnel resources. This approach also helps to deliver results quicker; hence, a use case-based method to develop the SIEM system is chosen. Utilizing SIEM use cases allows to focus security monitoring on those key target areas set by the business threat and risk management processes. Output driven SIEM method was chosen to be utilized as a guiding principle in connecting SIEM information sources. This requires that the SIEM use case must be defined before the log source can start sending logs to the SIEM system. Output driven SIEM incorporated with applicable methods from TDBUMO method is utilized to help in developing and choosing the SIEM use cases.

When an organization's threat and risk management information is not available or it is lacking in detail, the security specialists must use their own expertise and knowledge about the threats and the environment to direct the SIEM use case development. This approach has the risk of the SIEM system focus to be guided in a direction that does not align with the customer expectations. With the introduction of the SIEM use case concept and the proposed SIEM use case management model, communication with the customer's IT management is expected to be improved.

In the proposed construct the Bryant kill chain was chosen to be utilized in categorizing the SIEM use cases. With the modifications in the Bryant kill chain, it provides better categorization of the indicators provided by the SIEM system than

the original CKC model. The 18 phases included in the UKC model were deemed to be too granular for the intended usage, and the UKC would make the visualization creation and usage cumbersome, although the UKC provided a way to abstract the attacks further and more accurately.

5.2.1 SIEM use case lifecycle

To make the management of multiple SIEM use cases by multiple security specialists more efficient, a SIEM use case lifecycle was defined. This lifecycle includes 7 phases and each SIEM use case is in one of these phases throughout its lifespan. Each lifecycle phase has its own functions and defined tasks that are presented in the following chapter.

By utilizing SIEM use case lifecycle security specialists can manage a larger amount of use cases and it allows to utilize applicable use cases in multiple customer environments. When presenting SIEM system capabilities with the means of SIEM use cases, the lifecycle status can be used as a filtering item.

To track and manage a SIEM use case throughout its lifecycle the following seven (7) phases were defined:

1. Review needed
2. Idea Refinement
3. Development
4. Testing
5. Production
6. Maintenance needed
7. Discarded

Lifecycle phase functions and tasks are presented in the following chapter together with the detailed SIEM use case management process.

5.2.2 SIEM use case management process

SIEM use case management process defines the detailed actions and decision points inside each lifecycle phase. These actions and decision points are presented in detail in this chapter.

In the review needed phase, a new SIEM use case idea is recorded and an initial feasibility review is made. New SIEM use case ideas can be suggested by any

personnel related to the environments' cyber security monitoring on MSSP or customer side regardless of their role. Review needed (1.) phase is presented in Figure 9 together with idea refinement (2.) phase.

The methods to collect new SIEM use case ideas can vary from post-it notes on a whiteboard to an Excel spreadsheet to a ticketing system depending on tools otherwise utilized by the team responsible for SIEM development. To get the customer involved in the SIEM use case selection and development, a regular review of the SIEM use case library with the customer's IT management is recommended.

Initial use case feasibility should be reviewed by multiple professionals to ensure a review from multiple viewpoints and thus enhance prioritization and resource usage in the later phases. If a use case is deemed implausible for any reason, it can be discarded at this phase.

In the idea refinement phase, each use case idea is worked on by the security specialists to include the necessary information for use case review and scoring during this phase. After this phase the SIEM use case must include at least the following preliminary information: use case name and description, kill-chain phase, information needs (log source or other information sources) and operation mode (alert, dashboard or report). The description needs to be accurate enough for the security specialist to be able to form an initial draft of the use case operation logic, and information needs are needed for estimating the work effort needed to have that information available in SIEM system, e.g. when the log format is supported by the SIEM system and the normalization is readily available, the work effort is much smaller than if it is necessary to write one's own normalization policy.

In use case review & scoring step each SIEM use case is reviewed for implementation feasibility and effort needed to develop (later referred as Effort) and potential gains expected (later referred as Benefit) when use case is working. In this step effort and benefit get values assigned ranging from 1 to 5, and these values are multiplied together to get the priority value. For effort value 1 means that the information needed for the use case is not readily available in SIEM system and the operation logic needs plenty of work, value 5 means that information is readily available in SIEM system and operation logic uses simple search operations. For benefit value 1

means that the use case is producing only statistical value or anticipated false positive rate is high and value 5 means that the use case will produce output that can be acted upon immediately and it has low false positive rate. SIEM use case prioritization can be used to guide work resource usage during development stage. SIEM use case can be discarded at this phase.

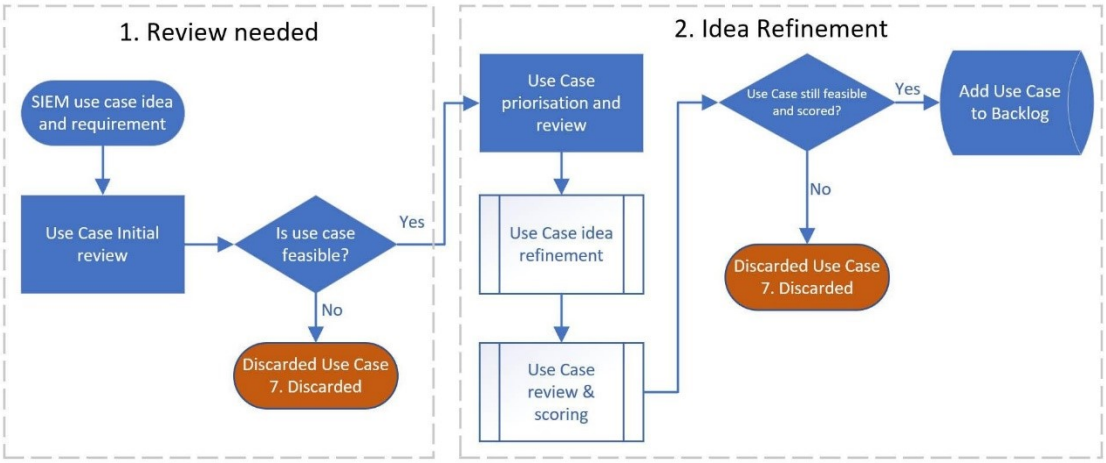

Figure 9. Development of SIEM use case phases 1 and 2

The development phase includes the main development effort of SIEM use case. It starts by selecting the use case from the prioritized backlog and then planning and defining the SIEM use case objective, the threat it responds to, the stakeholders related to the use case and information requirements. The next step is to define how the use case operation logic is formed, i.e. use case operation logic defines if it is displaying its output as alert, dashboard or report or any combination of these and what kind of search queries and other techniques are needed to provide the desired output. These definitions form the basis on how SIEM use case relates to cyber SA and how its output can be used to provide enhanced perception, comprehension and projection (SA levels 1-3).

Based on the previous steps, a prototype of the use case is created, and it is evaluated whether it is ready for the testing phase. If not, then another development round is needed. This creates the main development cycle and the use case iterates in it until it is ready for production testing. Figure 10 presents the steps and actions in the development (3.) and testing (4.) phases.

In the testing phase SIEM use case is run in the production environment to see how it operates and whether the generated output is adequate, and the use case responds to the threat defined in earlier steps. In “Use Case false positive & alert rate review period” step the SIEM use case is run in the production or test environment to find out how many indications it produces and what the amount of false positive indications is. In “Use case threshold tuning” step search query and alert thresholds are tuned according to the observations made in the previous step.

The final step before the use case is ready to be deployed in production is the playbook creation. In this step a playbook is created that aims to define the procedures for the SOC analyst to follow when a SIEM use case is triggered in production, e.g. a playbook could define the steps that SOC analyst can take to exclude false positive findings and the first steps to do to start mitigating the threat. This SIEM use case specific playbook should be linked to the SOC documentation and to other SOC processes, e.g. incident management process. Dependencies to other teams should be recognized and described at this stage. One of the most important objectives for the SIEM use cases is to provide actionable outputs that help in creating the cyber SA and to provide good starting information for incident management process.

Actions and techniques used during the testing phase depend on the type of use case logic and output (Alert, Report or Dashboard). When these steps are completed, the SIEM use case is ready for production usage and its phase is changed to production (5.).

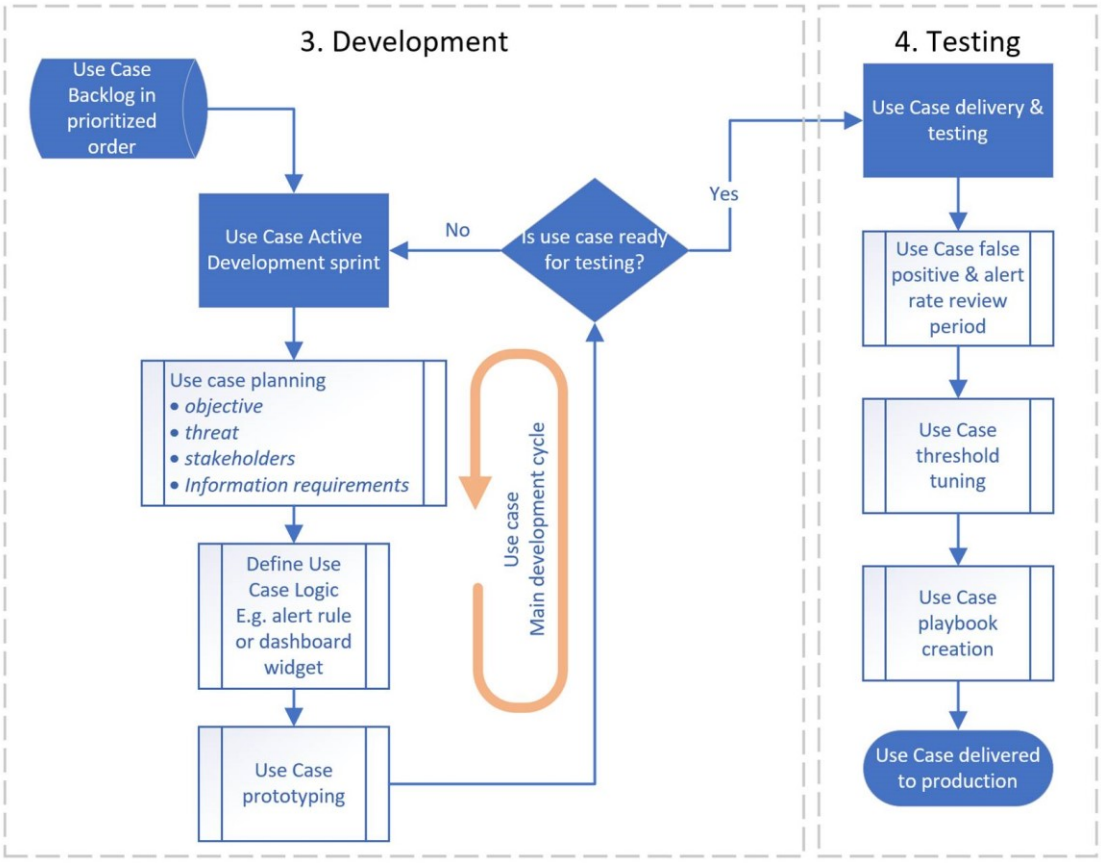

Figure 10. Development of SIEM use case phases 3 and 4

When the SIEM use case is in the production (5.) phase and a need for a change arises, the change need is reviewed by the SOC analysts and security specialists to determine if it is a matter of threshold tuning or if there is need for a major change. In the case of tuning needed, the adjustments to the thresholds or small tuning to the operation logic can be made to provide a better output. These tuning operations can be made during the production phase. Figure 11 presents the steps in Production (5.) and Maintenance (6.) needed phases.

In the case of a more major change need, the phase of SIEM use case is changed to “Maintenance needed” (6.). In this phase the SIEM use case is reviewed if it still is relevant, if it responds to the threat described in the SIEM use case and if it provides the desired output. The SIEM use case can be discarded at this stage if it is deemed irrelevant or outdated. If the SIEM use case change need recognized is something deemed fixable, the SIEM use case is prioritized and put back into the development backlog, e.g. the log format of the log source utilized in the SIEM use case has changed and therefore operation logic needs to be revised to take this change into account.

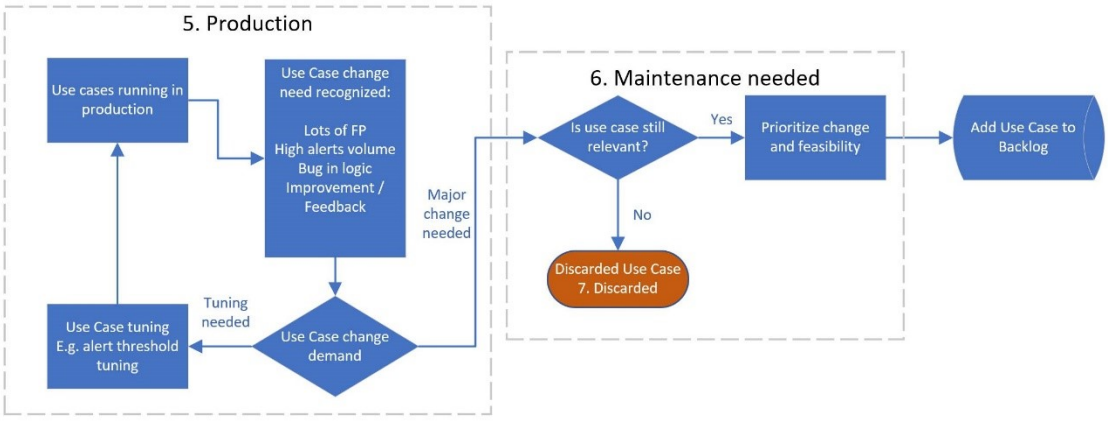

Figure 11. Development of SIEM use case phases 5 and 6

If the SIEM use case is discarded, its status is changed to discarded but it is kept in the use case library, so it can be found and referenced later.

New use case ideas could be handled during a weekly use case review meeting, where new ideas, prioritization of use cases and task selection for the next development cycle is done.

5.2.3 SIEM use case information fields and use case library

During their lifecycle SIEM use cases are organized by utilizing the structure presented in Table 1 including a short explanation of each data field. Together these form a use case library used to document each use case. This SIEM use case library helps in utilizing use cases with different customer environments and in forming other use case ideas. A use case library in its simplest form can be an Excel spreadsheet with use case information fields as column headers and use cases as rows as shown in Appendix 1, data in Appendix 1. SIEM use case library is created for illustration purposes.

Table 1. Use Case structure

Use Case Name	Short descriptive name, ties use cases to alerts, dashboards and reports
Description	Longer description about the use case and its objectives
Bryant kill chain phase	Bryant kill chain phase associated with use case. <selection of fields described below>
Bryant kill chain sub phase	Bryant kill chain sub phase associated with use case. <selection of fields described below>
Priority	This value is used to prioritize use cases in development stage within each customer (multiplication of benefit and effort)
Benefit of the use case	Numeral estimate of the potential use case benefit. (1 minimal benefit – 5 straight and actionable indication of anomaly)
Effort needed to develop	Numeral estimate of the effort needed to develop use case logic and getting the logs. (1= Development estimated to be hard and needs plenty of work, or log source is hard to connect to SIEM – 5= log data already in SIEM system and logic easy to develop)
Customer	List of customers utilizing the use case
Lifecycle phase	Use case lifecycle phase is used to manage use cases in different stages. <selection of fields described in SIEM use case lifecycle chapter>
Technologies involved	List of technologies involved to be used in visual or textual representation of use case library
Log sources	list of log source needs used to aid in log source management

Following values can be selected in Bryant kill chain phases and sub phases; these are the same fields as described in chapter 4.2.1 Bryant kill chain.

Bryan kill chain phases are as follows:

- Network phase (Pre hack)
- Endpoint phase (Hack)
- Domain phase (Compromise)
- Egress phase (Theft)
- Other

Bryant kill chain sub phases are listed below:

- Reconnaissance
- Delivery
- Installation
- Privilege escalation
- Lateral Movement
- Actions on Objective
- Exfiltration
- Other

5.2.4 Methods for SIEM use case creation

Previous research found during the information acquisition for this thesis provided only little information on the methods and tools to be used in the SIEM use case creation and few sources stated broader models describing the overall SIEM deployment.

To allow new SIEM use case ideas to be found and developed in a more structured way, a few different types of SIEM use case workshops were recognized. These workshop types are overall monitoring capability review, system specific attack workshop and system specific threat and risk management workshop. In these workshops the customer IT management and stakeholders need to be present as increasing the understanding of the SIEM system capabilities and tying it to organizations threat and risk management are major objectives in addition to creating new SIEM use cases. Further details of the contents and structure for these workshops are outside of the scope for this thesis.

As presented in the original CKC paper, intrusion reconstruction can help in determining what indicators are available for detecting adversary actions and to find

out more information related to intrusion. Based on the intrusion reconstruction new SIEM use case ideas can be worked on to further improve the SIEM system detection capabilities. By using the same Bryant kill chain phases in intrusion reconstruction, it helps to form better understanding of the threat actor and its objective.

In the Bottom Up phase of the TDBUMO model, log source data points are mapped to find out potential collisions and therefore correlation possibilities. This method helps the security specialists to get familiar with the contents of the logs and provides faster SIEM use case development as well as improves the quality of the indications by correlating information from multiple sources together. This process is conflicting with the Output driven SIEM method as SIEM use cases and their information needs should be defined before this analysis can be done; nevertheless, it can be a valuable task to perform when building more advanced SIEM use cases that utilize information correlation between information sources. Bryant suggested a similar process to map the information provided by the log sources to the applicable Bryant kill chain phase and to find out potential data pairings for correlation (Bryant & Saiedian 2017, 201-205). These methods can be utilized by the security specialists' when developing new SIEM use cases or improving existing SIEM use cases.

A set of basic SIEM use cases needs to be defined to help in the SIEM system deployment and to ease the communication with customer's IT management personnel who necessarily do not have enough knowledge to give input to the SIEM use case development before the SIEM system deployment starts. During the deployment stage great care must be taken to ensure the customer involvement in the security monitoring planning. Continuous development process must be in place to ensure that SIEM capability development continues after the initial deployment project is finished.

5.2.5 Visualisation methods

As described previously, each SIEM use case has the Bryant kill chain phase assigned to it. This is done to assist in visualizing the SIEM monitoring capabilities provided by the SIEM use cases and to improve the SOC analyst's understanding of the impending situation indicated by the SIEM use case. The SIEM use cases applied to each customer can be presented under the Bryant kill chain phases to provide an overall

view of the monitoring capabilities in the customer environments as presented in Figure 12. This figure shows example SIEM use cases and their kill chain phases, from the figure it can be deducted that privilege escalation phase does not have any SIEM use cases, and therefore no adversary actions can be detected at this phase. For example, creation of this visualization can be achieved automatically by utilizing a PowerBI application presenting a high-level view of the SIEM use case information retrieved from the SIEM use case library.

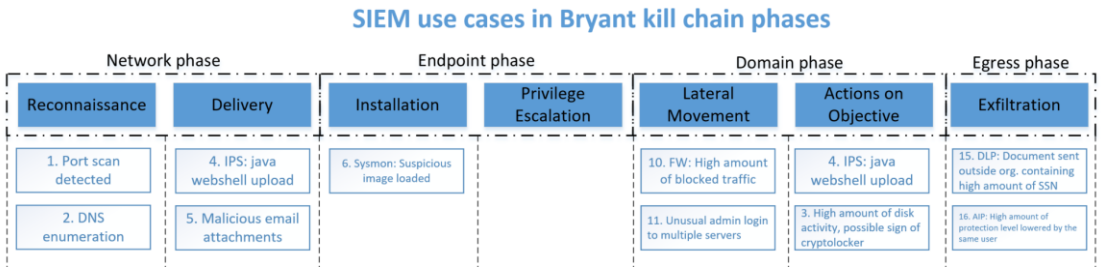

Figure 12. Example SIEM use cases presented in Bryant kill chain phases

The Bryant kill chain can be utilized in the communication of cyber SA to the customer IT management and stakeholders, as it helps to provide uniform understanding of the impending situation. The security analysts can use the format presented in Figure 13 to display the IOC and other information related to the incident. It can be utilized during the active incident management or after the lessons learned and intrusion reconstruction has been done. In the figure each adversary action is mapped to the applicable Bryant kill chain phase.

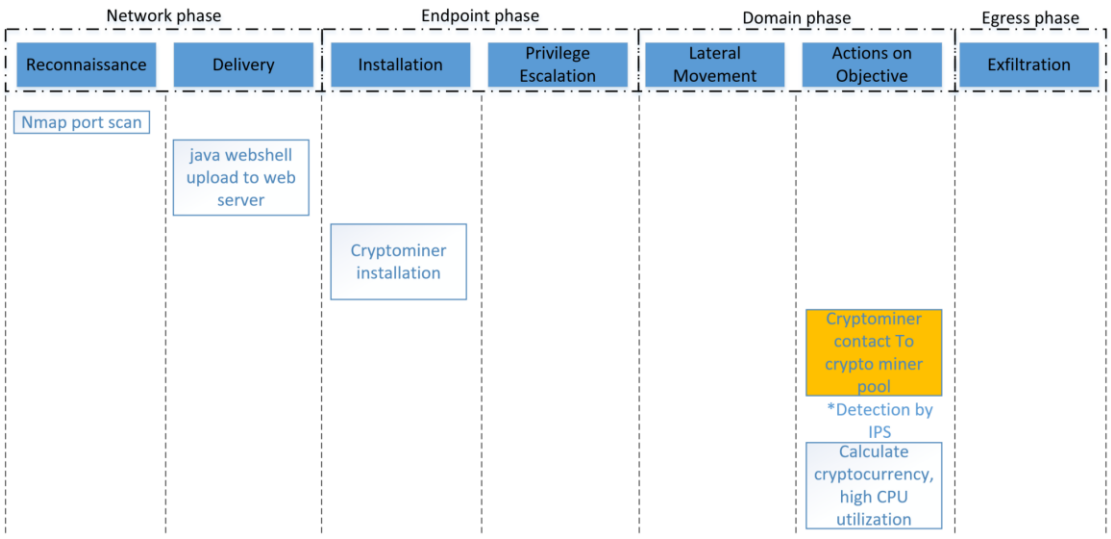

Figure 13. Example of intrusion events presented on the Bryant kill chain

6 Implementation and research results

6.1 Construct implementation in practice

During the iterative process of creating the proposed construct, the principles have been utilized in practice among the team of security specialists working with SIEM system development. This has provided feedback of the construct throughout the process. Multiple SIEM use cases have been defined and developed by the team members, and use cases are currently in the production phase of SIEM use case lifecycle. Supporting tools and practices to help manage the SIEM use case library and provide visualizations have been implemented within the team of security specialists responsible for SIEM system development.

Initial deployment to include customer IT management has started for one customer, providing feedback and confirmation of proposed constructs suitability for communication between the security specialists and customer IT management.

6.2 Interview execution

To further understand the results achieved with the proposed construct, a set of interviews was held. The interviews were conducted by using theme interviews. Each of the interviewees had familiarized themselves with this thesis and the proposed construct from their own standpoint as each had their own role in the security monitoring. In total two interviews were held, and the results of the interviews are summarized and presented in the following chapter.

Both interviews followed a similar theme, and the structure of the interview was based on the structure of this thesis report as the purpose was to verify the suitability of the proposed construct and receive feedback on the findings. The first interviewee was the author's colleague working closely with SIEM systems and who has been working closely with the proposed construct during its development and the other was a security specialist from a customer organization working in the security services unit.

The total duration of both interviews was approximately one hour.

6.3 Interview results

Both interviewees told that Cyber SA theory was not previously familiar, and that the thesis provided an understandable description of the concepts. According to one interviewee, it was closely related to the topic and it can be utilized to further enhance the understanding of the SIEM system position related to the cyber SA creation.

During the interviews it became apparent that the theory section regarding the SIEM systems was accurate and gave the basic understanding of the SIEM system. The other interviewee mentioned that the description of the difference between a business case and a SIEM use case was important thing to bring out as it is often mixed up in the vendor white papers.

When asked about the accuracy of the SIEM deployment problem description, both interviewees agreed that the problems are accurate and can be identifiable.

The other interviewee told that in his opinion the techniques presented in the CKC papers can be utilized while working with threats not coming from APT actor and the seven phases of the Bryan kill chain are a suitable method for presenting the SIEM use cases and the intrusions.

Both interviewees agreed that the proposed construct provides structure for developing SIEM use cases and the SIEM use cases can be propagated to other environments more easily. The other interviewee told that while reading the construct it felt that this is how it should have always been done, and it made him think why this has not been done like this way before.

Coupling the threat and risk management to SIEM deployments was thought out to be an important way to improve SIEM capabilities as then the resources can be better directed to the areas important for the organization. By using the visualization methods described in the proposed construct the SIEM system capabilities can be reviewed and potential blind spots can be identified.

As a problem one interviewee identified the large amount of work required to transform the currently utilized SIEM alerts, dashboard and reports to include SIEM use case description as these previously have been implemented by the individual

security specialists without all the documentation steps and concepts introduced in the proposed construct.

One interviewee pointed out that to ensure that the SOC analysts understand the SIEM use case outputs correctly, the necessary documentation of the monitored environment must be available even though the SIEM use case output must be as informative as possible. The other interviewee pointed out that it is important for the SIEM use cases to be thought out with the specific environment in mind and this way improve the SIEM use case outputs and reduce the load on SOC analyst.

As a summary of the answers given by the interviewees, this thesis subject was justified, and the thesis responded to a real problem in the deployment of the SIEM systems and provided new knowledge that can be applied to the described field of problems.

6.4 Research results

This chapter describes how the results achieved with the proposed construct meet the requirements set for this thesis and how the research questions were answered.

The decision to handle SIEM system alerts, dashboards and reports as SIEM use cases has improved the efficiency of the SIEM systems development, and it was the first step in utilizing the concept of “Output-driven SIEM”. This decision has helped to change the mindset from log source first mentality to value-based thinking: how to detect adversary actions in the systems and how to provide value by improving the cyber SA.

Initial experiences support the assumption that by transferring the focus from the log sources to the SIEM use case selection and development during the SIEM deployment, the customer IT management and stakeholders get a better and more realistic understanding of the capabilities provided by the SIEM system. Initial experiences gathered from the usage of the visualizing techniques presented in the proposed construct provided better understanding of the SIEM system capabilities. As the deployment of the proposed construct to the customer side was brief, no conclusion can be made for the long-term impacts of the proposed constructs usability.

Based on the experiences during construct development and the interview, it was noted that the burden of developing new SIEM use cases can be overwhelming. Therefore, the process must be as light as possible; however, it must provide the necessary information to form new and effective SIEM use cases. The structure provided by the proposed construct enables multiple security specialists to share and document their work and this way improve the efficiency of teamwork. Properly documented SIEM use cases can be transferred to other customer environments with smaller time investment. SIEM use case lifecycle and the process described in the proposed construct have provided the means to address this burden and the proposed construct seems like a good fit for the employer organization.

Understanding of the cyber SA in theory will help to develop better SIEM use cases as the security specialists can take into account the humane aspects of the SOC analysts, i.e. SIEM use case output should indicate clear events and be easily interpreted by the SOC analyst consuming the information to form the cyber SA and to take actions based on it without overwhelming the SOC analyst with a flood of information. During the SOC analysts' introduction to the SIEM use cases attention must be paid to the way the SIEM use case logic is formed and what the outputs of the use cases mean. In this way the SOC analyst can weigh the reliability of the observation.

The methods described in the cyber kill chain documents refer to the fact that adversaries are APT actors with major resources, and therefore the suggested actions are justified. From the standpoint of a Finnish organization or company, the majority of cyber security incidents is not caused by APT actors but rather threat actors looking for a quick way to monetize the attack and gather user accounts or personal information. Regardless of this, techniques such as intrusion reconstruction can be beneficial and provide value in creation of SIEM use case to detect similar attacks in the future; however, care must be taken to evaluate the effort invested in each of the cases.

During the thesis process it became apparent that the threat and risk management information in the organizations has not been the guiding factor in developing the SIEM capabilities. It was recognized that the threat and risk management information should provide general guidelines for choosing SIEM use cases, and the SIEM use

case could be used as a risk mitigation factor by lowering either the probability or impact of the risk event. Ensuring the customer IT management, and the stakeholders' commitment and involvement in SIEM use case selection and development is vital for successful SIEM deployment.

Lukka (2001) stated that an inevitable stage in constructive research is that the researcher must recognize the theoretical contribution accomplished in the research. In this thesis the theoretical contribution is achieved by creating a novel construction that utilizes the previously presented methods such as SIEM use case and CKC.

The proposed construct and the thesis provide methods and tools to use in the SIEM capability development, and cyber security kill chain models are utilized as part of the solution. This way it can be concluded that the answers to the main research questions set in the beginning of the thesis process have been achieved.

Based on the interview answers and the author's personal experiences the proposed construct meets the requirements set for this thesis by providing the needed structure and tools for the SIEM system capability development. The interviews provided feedback on the validity and generalization of the thesis subject.

The risks mentioned in the chapter on research methods have not been actualized, and the employer organization has withstood the commitment to this thesis.

7 Discussion

This thesis process started with the idea of how to utilize CKC model in the SIEM system development and how to make the development work more structured. The paper on Bryant kill chain by Bryant & Saiedian (2017) was inspiring in the topic selection and provided reassurance that these methods should be investigated more deeply.

During the theory research phase of this thesis it became obvious that the previously published research does not cover the SIEM system deployment and the SIEM use case management in detail. This realization strengthened the need for this research, and more future research remains to be conducted on this subject.

Many of the issues faced in this thesis could be solved by automation, data fusion and anomaly detection; yet, the human understanding of the cyber SA is vital and necessary to present it forward for other levels of decision making, e.g. a hospital's cyber SA affects greatly to the treatment of the patients.

Based on the author's understanding it can be said that the most important intellectual capital for a MSSP are the contents of the SIEM use case library, and a great deal of work should be done to develop SIEM use cases to provide added value.

Understanding of the problem at hand matured during the thesis, and the objective to provide more structure to the SIEM development work was kept in mind throughout the thesis process. This thesis supports the work done towards implementing and deploying SIEM systems by providing a more structured way of managing and developing the SIEM capabilities. A challenging aspect in the chosen research topic was the difficulty to separate the general SIEM system development tasks of the author's work role and the thesis objectives. Some ideas and constructs were developed and utilized at work; they were, however, left out of this thesis report as they were out of the thesis scope. In the end it can be said that these two roles supported each other.

The selected constructive research approach worked well in this thesis and provided guidelines on how to proceed with the thesis research process and avoid the potential pitfalls. It provided the guidance to the scientific way of reporting and was a good fit for problems arising from the working life difficulties. During the thesis process the proposed construct was improved in steps while building on the knowledge acquired in the theory research conducted for the thesis.

During the thesis process and with the implementation of the SIEM use case concept and the proposed construct, the overall maturity of the SIEM deployments was increased; however, without a way to measure the maturity progress of the SIEM capability it was impossible to weigh. As a further research objective, a SIEM system maturity measurement model would be needed, and it would greatly benefit organizations running SIEM systems in choosing the right development activities and in achieving more up-to date and relevant SA by utilizing the SIEM system.

In the future it would be beneficial to study how one should modify the framework in this thesis to best suit the different phases and maturity levels of SIEM customer projects and the organization's environments. As presented in the thesis construct, workshops are an integral part of developing new SIEM use cases; therefore, further research needs to be conducted to find out how these workshops should be carried out and how available threat modelling techniques could be used to improve SIEM use case development.

Thorough testing and wide deployment of the proposed construct to the customer environments were not possible during the thesis project due to limited resources and timeframe, although initial feedback was received indicating positive results from the customer organization. It would have improved the reliability of the results and provided a better understanding of the suitability of the proposed construct for it be used in other organizations. Further research should be conducted with a wider implementation scope and longer observation period.

While conducting and analyzing the interviews, the author noticed that his own experiences and opinions could easily affect the opinions and answers of the interviewees. A small number of interviewees was a choice forced by the timeframe of the thesis. As the researcher conducting the interview has also created the proposed construct, it created a biased setting for the interview situation. These observations lower the reliability of the interview results. Regardless of these observations, the interviews provided a wider perspective of the results achieved with the proposed construct and thesis.

This thesis and the assigned topic were interesting to the author as they are closely related to the work role and the proposed construct affects the author's daily work. Personally, this thesis has provided plenty of insights into the SIEM systems and the pitfalls related to them. The theory connection presented in this thesis combined to the years of work experience in the cyber security field and experiences gathered during the implementation phase greatly improve the author's professional skills and at the same time they showed that there are still plenty of aspects to study regarding the security monitoring and SIEM systems.

References

Bryant, B., & Saiedian H. 2017. A novel kill-chain framework for remote security log analysis with SIEM software. *Computers & Security,* 67, 198-210.

Chuvakin, A., 2012. On "Output-driven" SIEM. Blog-post. Accessed 17 October 2019. Retrieved from https://blogs.gartner.com/anton-chuvakin/2012/09/24/on-output-driven-siem/

Chuvakin, A., Belak, A., & Barros, A. 2018. How to Architect and Deploy a SIEM Solution. Gartner Technical Professional Advice. Gartner ID: G00366351.

Endsley, M.R. 1995. Toward a Theory of Situation Awareness in Dynamic Systems. *Human Factors*, 37(1), 32-64.

Frye, D. 2010. Effective Use Case Modeling for Security Information & Event Management. SANS reading room whitepaper. Accessed 16 October 2019. Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/effective-case-modeling-security-information-event-management-33319

Hohner, A. 2019. Use cases are a key component of every SIEM. Blog-post. Accessed 17 October 2019. Retrieved from https://www.capgemini.com/2019/05/how-to-define-complex-use-cases-and-implement-them-in-your-siem-soc-project/

Hutchins, E., Cloppert, M., & Amin, R. 2010. Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains. Lockheed Martin Corporation. Accessed 10 of August 2019. Retrieved from https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf

Hyötyläinen, R., Häkkinen, K., & Uusitalo, K. 2014. The constructive approach as a link between scientific research and the needs of industry. Accessed 8 of December 2019. Retrieved from https://www.researchgate.net/publication/279183260

Lukka, K. 2001. Konstruktiivinen tutkimusote [*Constructive scientific researchapproach*]. www.metodix.com. Referred from https://metodix.fi/2014/05/19/lukka-konstruktiivinen-tutkimusote/

Logpoint. 2018. Logpoint administrator training material. Powerpoint presentation.

Lötjönen, J. 2017. Requirement specification for cyber security situational awareness: Defender's approach in cyber security exercises. Master's thesis. JAMK University of Applied Sciences, School of Technology, Master's Degree Programme in Information Technology. Accessed 12 October 2019. Retrieved from http://urn.fi/URN:NBN:fi:amk-2017121320954

Miller, D., Harris, S., Harper, A., Vandyke, S., & Blask, C. 2011. Security Information and Event Management (SIEM) Implementation. McGraw-Hill/Osborne.

Onwubiko, C. 2016. Understanding Cyber Situation Awareness. International Journal on Cyber Situational Awareness, Vol. 1, No. 1, 11-30.

Pols, P. 2017. The Unified Kill Chain: Designing a Unified Kill Chain for analyzing, comparing and defending against cyber attacks. Cyber Security Academy. Accessed on 15 October 2019. Retrieved from https://www.csacademy.nl/images/scripties/2018/Paul-Pols---The-Unified-Kill-Chain.pdf

Puustinen, S. 2013. Qualitative research and theme interview as a method of collecting data. Aalto University. Accessed on 21 March 2020. Retrieved from https://mycourses.aalto.fi/pluginfile.php/195681/mod_resource/content/1/qualitative%20research%202013-10-28_handout.pdf

Reidy, P. 2013. Combating the Insider Threat at the FBI. Presentation at Black Hat USA 2013. Accessed on 10 December 2019. Retrieved from https://media.blackhat.com/us-13/US-13-Reidy-Combating-the-Insider-Threat-At-The-FBI-Slides.pdf.

Shoard, P. 2018. Hype Cycle for Threat-Facing Technologies, 2018. Gartner. Accessed on 13 September 2019. Retrieved from https://www.gartner.com/en/documents/3882466/hype-cycle-for-threat-facing-technologies-2018.

Symantec. 2019. Internet Security Threat Report 2019. Accessed on 11 December 2019. Retrieved from https://www.symantec.com/security-center/threat-report

Vasudevan, V. n.d. A Framework for Business Aligned Security Monitoring Use Cases. Whitepaper. Accessed on 19 October 2019. Retrieved from https://www.paladion.net/hubfs/Whitepaper%20PDF/A_Framework_for_Business_Aligned_Security_Monitoring_Use_Cases.pdf

Appendices

Appendix 1. Example of SIEM use library and use cases.

#	Use Case	Description (Objective)	Lifecycle phase	Sub-phase	Prio	Benefit	Effort	Cust.	Log sources, technology
1	Crypto locker activity detected in network share	Detect and alert when suspicious amount of writes and reads are performed.	5.	Actions on Objective	12	4	3	Cust 1.	file server
2	New vulnerability found in critical server	Compare and alert when new vulnerabilities have beend found in critical services	4.		10	2	5	Cust 1.	Nessus
3	Malware detected in server	Alert when AV detected new malware infection in server.	3.	Installation	16	4	4	Cust 1. & cust 2	Fsecure policy manager
4	Malware detected in workstation	Alert when AV detected new malware infection in workstation.	3.	Installation	16	4	4	Cust 1. & Cust 2	Fsecure policy manager