Expertise
and insight
for the future

Otto Lindström

Next Generation Security Operations Center

Metropolia University of Applied Sciences

Bachelor of Engineering

Information and Communications Technology

Bachelor's Thesis

5 November 2018

Author	Otto Lindström
Title	Next Generation Security Operations Center
Number of Pages	47 pages
Date	5 November 2018
Degree	Bachelor of Engineering
Degree Programme	Information and Communications Technology
Professional Major	IoT and Cloud Computing
Instructors	Kari Salmela, Chief Information Security Officer Marko Uusitalo, Senior Lecturer

The goal of this thesis was to research how a security operations center can be improved. A security operations center is an essential part of modern cyber defense, as it establishes and maintains the cyber security situational picture. This thesis highlights problems of current security operations centers and proposes improvements.

The thesis is based on researches and studies about security operations centers and other relevant topics. Security operations centers do not have a standardized form and therefore the thesis combines multiple sources.

According to the results of this thesis, today's security operations centers are struggling with overwhelming amounts of data while cyber attacks are becoming more sophisticated and challenging to detect. Modern tools and technologies such as machine learning and artificial intelligence can be utilized to automate the processing of recurring threats. Furthermore, a security operations center can collect and analyze cyber threat intelligence, to become more aware of current threat trends. Security operations center units must be able to streamline their processes, so that the unit can execute its mission in an agile manner, while adapting to their environment.

The results of this thesis can be utilized while planning and implementing a modern security operations center. In addition, existing security operations centers can use the results of this thesis to gain information about modern implementations.

Keywords	Cyber security, Security Operations Center, SOC, cyber security situational picture.

Tekijä Otsikko Sivumäärä Aika	Otto Lindström Uuden sukupolven tietoturvahallintakeskus 47 sivua 5.11.2018
Tutkinto	insinööri (AMK)
Tutkinto-ohjelma	Tieto- ja viestintätekniikka
Ammatillinen pääaine	IoT and Cloud Computing
Ohjaajat	Chief Information Security Officer Kari Salmela Lehtori Marko Uusitalo

Insinöörityön tavoitteena oli selvittää tietoturvahallintakeskuksen kehittämismahdollisuuksia. Tietoturvahallintakeskus on oleellinen osa organisaatioiden nykyaikaista kyberpuolustusta, sillä se rakentaa ja ylläpitää kyberturvallisuuden tilannekuvaa. Tietoturvahallintakeskus koostuu ihmisistä, prosesseista ja teknologioista, jotka kaikki on otettu huomioon insinöörityössä. Insinöörityössä pohditaan nykyisten tietoturvahallintakeskuksien ongelmia ja esitetään niihin parannusehdotuksia. Insinöörityössä pohditaan tietoturvahallintakeskuksen kehittämistä lisäksi tietoturvapalveluntarjoajan näkökulmasta.

Insinöörityön pohjana käytettiin alan kirjallisuutta ja tutkimuksia. Tietoturvahallintakeskuksilla ei ole standardisoitua muotoa tai toimintatapaa, jonka takia insinöörityössä on yhdistetty tietoa useista eri lähteistä. Insinöörityön muoto on tutkimuspohjainen, sillä tilaajayritys halusi selvittää tietoturvahallintakeskuksen kehitysmahdollisuuksia.

Insinöörityön tuloksena päädyttiin siihen, että nykyiset tietoturvahallintakeskukset kamppailevat kasvavan datamäärän kanssa samalla, kun tietoturvaloukkaukset ovat entistä monimutkaisempia ja vaikeampia havaita. Tietoturvahallintakeskukset voivat hyödyntää nykyaikaisia teknologioita ja työkaluja, kuten koneoppimista ja tekoälyä automatisoidakseen toistuvien tietoturvauhkien käsittelyn. Lisäksi tietoturvahallintakeskukset voivat hyödyntää olemassa olevaa uhkatietoa parantaakseen tietoturvariskien havainnointia. Tietoturvahallintakeskuksen tulee pyrkiä virtaviivaistamaan prosessinsa, jotta yksikkö voi toimia mahdollisimman ketterästi mukautumalla ympäristöönsä.

Insinöörityötä voidaan käyttää avuksi tietoturvahallintakeskusten suunnittelu- ja toteutusvaiheissa. Tämän lisäksi jo olemassa olevat tietoturvahallintakeskukset voivat hyödyntää insinöörityön tuloksia kehittyäkseen. Insinöörityön ansioista tilaajayritys pystyy kehittämään jo olemassa olevaan tietoturvahallintakeskustaan parantaakseen sen tuomaa tietoturvanäkyvyyttä ja kehittääkseen sen reagoimiskykyä tietoturvauhkiin.

Avainsanat	Tietoturva, Tietoturvahallintakeskus, SOC, kybertilannekuva

Contents

List of Abbreviations

AI	Artificial Intelligence. A machine that can perform tasks that mimics human's cognitive functions like learning.
APT	Advanced persistent threat. A term used to explain determined and skillful attackers that target private organizations and nation states. APT commonly refers to a group of attackers or even a nation state sponsored attacker.
AV	Antivirus. A computer program that prevents, identifies and removes malicious programs.
BYOD	Bring Your Own Device. A policy that permits employees to bring their personal devices to the workplace and use those devices in their work tasks.
C2	Command and Control. An attacker influencing a compromised computer system. C2 is also used explain the techniques used by the attacker to control the compromised system
CEF	Common Event Format. An open standard for text-based format for transporting and storing event messages developed for Micro Focus' ArcSight SIEM.
CTI	Cyber Threat Intelligence. CTI is a concept of collecting information regarding current trends in cyber security threats.
CVE	Common Vulnerabilities and Exposures. Provides a reference-method for known vulnerabilities and exposures in computing devices and programs.
CVSS	Common Vulnerability Scoring System. A standard for determining the severity of a computer security vulnerability.
DDoS	Distributed denial of service attack. A variation of DoS. In a DDoS attacker the harmful incoming traffic is coming from multiple sources. DDoS attacks can be more powerful and more difficult to mitigate than DoS attacks because the traffic originates from multiple sources.

DFIR	Digital forensics and incident response. Incident response aims to minimize the impact of a security incident. Digital forensics consists of analyzing an already occurred incident to gain information of it.
DNS	Domain Name System. A naming system and a protocol that translates domain names into IP addresses and vice versa.
DoS	Denial of Service. An attack in which the attacker disrupts the service temporary making it unavailable for the intended users.
EPS	Events Per Second. Used to measure the number of events that a device, for example SIEM system, is receiving, sending or processing.
GDPR	General Data Protection Regulation. A regulation on data protection and privacy that became enforceable on 25.5.2018.
HTTP	Hypertext Transfer Protocol. A protocol used for serving web-content from a server to a client.
HTTPS	Hypertext Transfer Protocol Secure. Extension of HTTP that uses SSL or TLS to encrypt the communication.
IDS	Intrusion detection system. A hardware or software product that analyzes information from a computer or a computer network to identify possible security breaches.
IoC	Indicator of compromise. A sign on a network or an operating system that indicates a computer intrusion. An IoC can be for example a cryptographical hash of a malicious software.
IoT	Internet of things. A network of physical devices, like home appliances and censors that communicate and exchange data.
IP	Internet Protocol. A network protocol that divides traffic into packets. Devices are identified using IP addresses.

IPS	Intrusion prevention system. Similar to an IDS, but an IPS is also capable of stopping the identified security breach, by for example blocking the malicious network connection.
IT	Information Technology. Using computers to transmit, store, manipulate and retrieve data.
LAN	Local Area Network. A computer network that connects devices capable of networking within a limited area such as a residence or a school.
MitM	Man in the Middle attack. An attack where the attacker secretly positions between two or more parties that are communicating. The attacker may try to alter the communications or collect data.
MSSP	Managed security service provider. An organization that offers information security services to other organizations.
NTP	Network Time Protocol. A networking protocol used for synchronizing clocks across different devices.
OSI	Open Systems Interconnection model. A theoretical model that explains how computing systems communicate regardless of the underlaying system. OSI model divides the communication model into seven layers.
OSINT	Open Source Intelligence. Collecting data from publicly available sources for intelligence purposes.
SEM	Security event management. System that is capable of real-time monitoring, event correlation and alerting. A part of SIEM.
SIEM	Security information and event management. A software or a device that is capable of analyzing and correlating great amounts of security events in near real-time. Mature SIEM products are also capable of generating alerts and visualizing security related data.

SIM	Security information management. System that provides long-term storage, analysis and manipulation of security logs. SIMs are also capable of producing reports. A part of SIEM.
SLA	Service Level Agreement. An agreement that defines quality, availability and responsibilities between a service provider and a client.
SMB	Server Message Block. A protocol for sharing printers, and files between computers connected to a network.
SOC	Security operations center. A centralized unit in an organization that establishes and maintains cyber security situational picture.
STIX	Structured Threat Information eXpression. A collaboration to standardize a structured language for cyber threat information sharing.
TAXII	Trusted Automated eXchange of Indicator Information. A transport mechanism for cyber threat information represented in STIX format.
TLS	Transport Layer Security. TLS is a cryptographic protocol that provides encryption for communications between two parties.
TTP	Tactics, Techniques and Processes. TTP is used to describe certain attacker's behavior.
UEBA	User and Entity Behavior Analytics. System that can perform analysis on human behavior to detect breaches and misuse.
UTM	Unified threat management. An approach where a single hardware or software product provides multiple security functions. For example, a device that simultaneously functions as a firewall and a IPS.

1 Introduction

The fast pace of the cyber security industry forces security operations center (SOC) units to evolve, so that the SOC units can defend the organizations from the current and upcoming threats. Reactive defending is not sufficient on its own anymore, as the cyber threat landscape has become increasingly diverse and complicated. A SOC unit's main mission is to establish and maintain the cyber security situational picture for an organization.

The goal of this thesis is to analyze problems of current security operations center units and to propose improvements, so that they can meet the high demands of the cyber security field. The thesis evaluates improvements in all SOC unit's building blocks: people, processes and technologies. This thesis includes proposals for improvements on technical aspects as well as on processes. In both cases, the thesis aims to provide multiple suggestions, because all SOC units are different and same tools and processes may not work for different SOC units.

The topic was chosen by a company that offers SOC services for clients. This research evaluates how SOC units can be further improved, to increase their value for the customers. Customers gain value from the situational picture and the reactive defending capability that a SOC unit can provide. However, as cyber threats have become more dangerous, an external SOC units must be able to provide proactive defending methods.

The thesis is based on researches and studies about security operations centers and other relevant topics. Security operations centers do not have a standardized form and therefore the thesis combines multiple sources.

The thesis is divided into four main sections. Chapter two is an introduction to a SOC unit. It describes the needs for a SOC and presents its main components. The third chapter analyses the challenges that current SOC units are facing. The fourth chapter expresses the improvements that are needed to build a mature, next generation SOC. The fifth chapter concentrates on implementing, and thus building the next generation SOC unit. The sixth chapter concludes this thesis.

2 Centralized Information Security Management

A Security Operation Center (SOC) is a centralized unit consisting of people, processes and technologies that provides cyber security situational awareness to a company or an organization. A SOC unit's goal is to prevent and analyze information security incidents. A SOC unit accomplishes this by analyzing security related data collected from the organization's technical environment.

2.1 The purpose of a Security Operations Center

Cyber attacks and data breaches have become more common than ever before. Cyber security affects everyone from large enterprises to small companies and individuals. Almost all data including personal information is stored and controlled by computer systems. As cyber attacks get more sophisticated, it is important to react quickly to security incidents, before the attackers gain access to even more crucial systems or gain a foothold into the network. The purpose of a SOC is to establish and maintain a situational picture of the organization's security, while reacting rapidly to possible changes in it. Computer controlled systems are everywhere, and without sufficient security measures, they pose a risk of being breached. As the society relies increasingly on the functionality of these systems, the stakes are high. The cyber security field is changing constantly, and the attacks are more complicated and diverse than ever.

On December 23, 2015 three Ukrainian power companies were attacked by hackers who managed to disrupt the energy distribution in central facilities. The attack left approximately 225,000 customers without electricity for 1 to 6 hours in the middle of winter. The hackers used a malicious software (malware) called BlackEnergy to infect and gain control of the computers managing the power grids. The distribution method of the malware remains unknown to date. Prior to the attack, the hackers performed lengthy reconnaissance on the targets to learn about their environments. All three attacks took place within 30 minutes. [1]. This attack indicates how fast a security incident can happen, and how it can affect thousands of individuals. Cyber security threats must be detected and prevented rapidly, which is why SOC units exist.

Traditionally, there have been relatively few tools used for protecting information networks. When the number of tools was lower, the management and monitoring was relatively straightforward. Firewalls, intrusion detection systems (IDS) and antivirus software (AV) have each separate vendor-specific user interfaces for configuration, management and monitoring purposes. [2, 35-36]. A network firewall is a device that filters traffic according to configured rules. A network IDS (NIDS) analyzes traffic to detect security breaches. AV software is usually installed on the host's operating systems and analyzes the device for malware. However, the increasingly complicated attacks have created a demand for tools like intrusion prevention systems (IPS) and improved firewalls, that are often marketed as next-generation firewalls. IPSes are similar to IDSes, but capable of attempting to block the detected intrusions unlike IDSes.

Centralized management becomes more complex when the number of security devices increases. Usually software and hardware vendors have tools that aim to unify the management between different devices. However, using products solely from a single vendor may not always be possible or effective, as the vendors commonly specialize on a few products. The multi-vendor market creates gaps in the visibility and complicates the process of creating and maintaining a situational picture. A SOC unit's function is to centralize the management of security across the organization, so that the organization can respond to threats before they turn into security incidents.

Unified Threat Management (UTM) is an approach where a single security device or software performs multiple security functions, that may include firewall, IDS and IPS. However, this approach has its own disadvantages. A modern defense consists of multiple layers of protection, while UTM combines the features of multiple security devices. If the attacker manages to bypass the UTM device, they are more likely to remain unnoticed as opposed to having multiple layers of defense. In addition, an UTM device creates a single point of failure into the network. However, UTM devices can be helpful because they provide a of the broad security coverage. UTM devices should be deployed in a layered manner to prevent single points of failure.

Information networks are becoming increasingly complicated. As new technologies are emerging constantly, and the number of devices connected to an organization's networks is greater than ever before. Trends like Bring Your Own Device (BYOD) complicate the process of asset management. BYOD means that organizations permit employees to

bring their personal devices like smartphones to the workplace, which can be connected to the wireless networks. Devices not managed by the organization can harm security, because the devices are out of reach of the organization's security policies. An employee's malware infected smartphone poses a risk to the whole organization. As a result, the organizations are forced to monitor their networks for threats more actively.

On May 25, 2018 a new European Union regulation General Data Protection Regulation (EU) 2016/679 (GDPR) came into effect. GDPR affects how companies must treat individuals' personal data. The regulation also defines that in an event of a data breach, a company may have to pay fines up to 20 million euros or up to 4% of their annual turnover. Article 33 specifies that if personal data is breached, an organization has 72 hours to notify the authorities after discovering the breach. [3]. The time it takes for the SOC to respond to breaches is usually measured using two metrics, mean time to identify (MTTI) and mean time to contain (MTTC). Multiple metrics are needed to measure a SOC unit's capability. For example, MTTC on its own does not measure the time it took to identify the breach. The attacker could have had access to the organization's internal systems for weeks or even months before the attacker was noticed.

SANS's 2017 incident response survey reported that 50% of the organizations detect security compromises in less than 24 hours, which improved from previous year by 10%. This still means that it took more than a day for the half of the organizations to detect an incident. [4, 8]. However, it is important to note that SANS is a non-profit company that specializes in information security. The individuals who participated in this survey are security professionals or otherwise interested in information security. All the organizations that entered the survey have invested in security and have ongoing security programs to detect and stop threats. If this survey was conducted on all organizations, whether they had a security program or not, the security incident detection times would probably be significantly longer. Figure 1 presents the survey's results on how long it takes to detect security compromises on average. The results indicate that generally MTTC is shorter than MTTI, which emphasizes the need for faster detection.

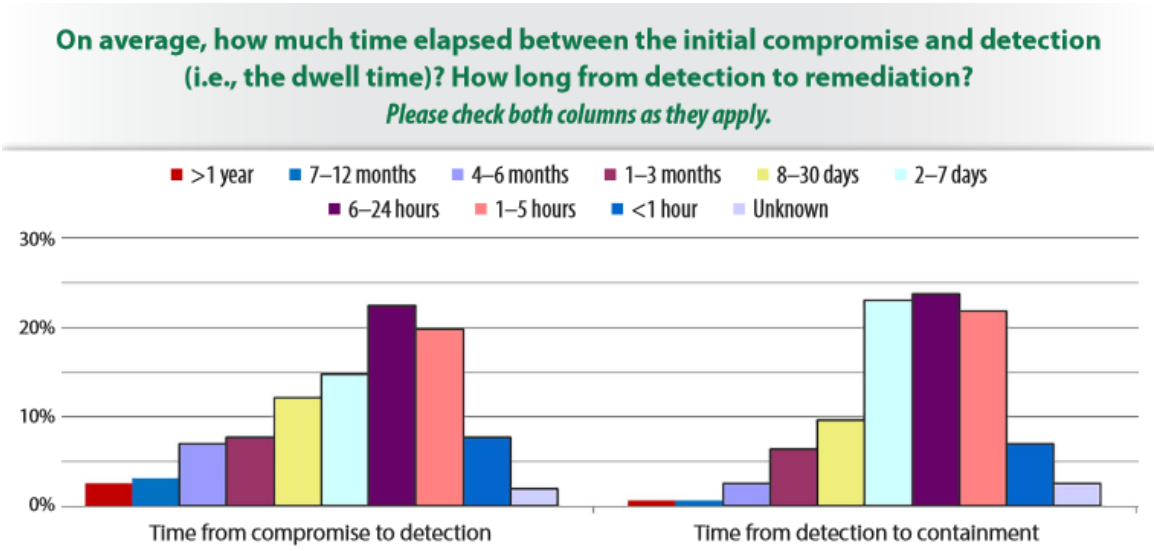

Figure 1. Detection and containment times of security compromises [4, 8].

A SOC differs notably from other operational units in an organization even though their objective is the same – to provide continuity to the organization. For instance, network operations centers focus on maintaining and operating the network devices, whereas a SOC concentrates on defending the organization from cyber attacks. A SOC should be recognized as a distinct and separate unit, so that it can focus purely on its objective. [5, 13].

2.2 Security Threats for an Organization

In January 2018, European Union Agency for Network and Information Security (ENISA) released a report of the threat trends of 2017. Malware (malicious software) is the greatest individual security threat. Malware is a hypernym for a large variety of harmful software. For example, ransomware is a type of malware that encrypts the victim's files and requires a payment for decrypting the files. Spyware on the other hand gathers information about the victim and sends it to a third-party without knowledge of the victim. Main attack vectors for malware are typically phishing and exploiting known vulnerabilities. [6, 25]. Phishing means that a malicious party attempts to obtain sensitive information from a target by sending an email or a message that mimics a legitimate service like a website [6, 40]. Web-based attacks are the second largest risk for organizations. This mainly concerns organizations that host web applications that are accessible from the Internet. Web application attacks are mostly used by attackers to gain confidential

information like customer data or to leverage their access into the internal networks. Web application attacks can be for example adversaries exploiting vulnerabilities in web server applications. [6, 31-36]. Other significant threats include Denial of Service (DoS) attacks and insider threats. DoS attacks aim to render the target unavailable for the intended users. Distributed Denial of Services (DDoS) is a variation of this disruptive attack, where the traffic comes from multiple sources. Attackers can compromise poorly secured devices to create botnets that can be used to launch massive DDoS attacks [6, 60]. An insider threat means that a human or a group within the organization wittingly or unwittingly harms the organization's security. Insider threats range from leaking company's private data to the public to intentionally causing damage like disrupting critical services. [6, 64]. Figure 2 lists the top 15 cybersecurity threats in 2016 and 2017. A mature SOC is capable of detecting all threats in the figure apart from physical manipulation/damage/theft/loss.

Top Threats 2016	Assessed Trends 2016	Top Threats 2017	Assessed Trends 2017	Change in ranking
1. Malware	↑	1. Malware	→	→
2. Web based attacks	↑	2. Web based attacks	↑	→
3. Web application attacks	↑	3. Web application attacks	↑	→
4. Denial of service	↑	4. Phishing	↑	↑
5. Botnets	↑	5. Spam	↑	↑
6. Phishing	→	6. Denial of service	↑	↓
7. Spam	↓	7. Ransomware	↑	↑
8. Ransomware	→	8. Botnets	↑	↓
9. Insider threat	→	9. Insider threat	→	→
10. Physical manipulation/damage/ theft/loss	↑	10. Physical manipulation/damage/ theft/loss	→	→
11. Exploit kits	↑	11. Data breaches	↑	↑
12. Data breaches	↑	12. Identity theft	↑	↑
13. Identity theft	↓	13. Information leakage	↑	↑
14. Information leakage	↑	14. Exploit kits	↓	↓
15. Cyber espionage	↓	15. Cyber espionage	↑	→

Legend: Trends: ↓ Declining, → Stable, ↑ Increasing
Ranking: ↑ Going up, → Same, ↓ Going down

Figure 2. Comparing the top 15 cyber threats in 2016 and 2017 side-by-side [6, 9].

2.3 Situational Awareness

Situational awareness means that the organization knows what events take place on their information technology (IT) property, who performed the actions and when. IT property includes all devices that are capable of transmitting, storing, manipulating and retrieving data. To provide situational awareness, a SOC must understand the environment it is working in. Building the situational awareness can be divided into three main components: gathering information, analyzing it and visualizing the analyzed information. Information can be for instance log data from different devices, threat intelligence or known vulnerabilities in the devices or services. Humans are not good at handling massive amounts of individual pieces of data, so the information is further analyzed after it has been collected. Analyzing the data is done automatically or partly automatically, using computer aided analytics tools. Humans tend to become overwhelmed when handling substantial amount of written information, so it is important to visualize the data. A SOC analyst can use the visualized information to quickly build up an overview of the security. [5, 26]. In addition, visualization helps in trend analysis.

Situational awareness is essential to a SOC unit because it makes reacting quickly possible, when the SOC unit discovers new threats. The IT environments that SOC units are monitoring are continuously changing and maintaining situational awareness helps to adapt to these changes. In addition, situational awareness helps SOC units to follow observe, orient, decide and act loop (OODA loop). OODA loop can be used to explain SOC unit's processes in a simplified way. First the analysts observe the network environment for changes, orienting the observations by using previous experience. Decision making happens based on knowledge gained form observing and orienting. After the analysts have made the decisions, they act accordingly. [5, 26].

Situational awareness can be split into three equally important sections: network, mission and threat. All three sections must be considered by the SOC. The network section concerns all devices that are connected and thus form the networks. A SOC should be aware of the quantity, type and location of all IT assets that are connected to the organization's networks. In addition, a SOC should be aware of the network topologies, including physical and logical, and the possible vulnerabilities in the devices. The mission is defined by the line of business and how the organization interacts with other parties. The threat section includes the primary adversaries, their capabilities and skillsets. It is also

necessary to emphasize the importance of being aware of the attacker's motivation and primary intents, as it makes a notable difference, whether an organization is defending against so-called script kiddies or state-sponsored attackers. [5, 26-28]. A script kiddie is an attacker with relatively low skill level, but who can download exploiting software developed by other hackers, to attack organizations [5, 324]. Script kiddies are not usually motivated or capable to perform sophisticated cyber attacks, as usually their motivation is entertainment and to gain respect among their peers.

2.4 SOC tools – SIEM

Security Incident and Event Management (SIEM) system is one the most valuable and important tools for a SOC for establishing and maintaining a situational picture. SIEM systems differ from traditional log management systems by adding several security related features, such as event correlation and analyzing capabilities. SIEM combines two concepts, Security Event Management (SEM) and Security Information Management (SIM). SIM systems collect security related data from multiple different sources on the network and stores the data in a single, centralized location. In addition to collecting data, SIM systems are capable of generating reports and performing historical analysis. SEM systems on the other hand, provide real-time monitoring capabilities that are used to monitor the data collected from different sources by the SIM component. SEM systems are efficient in real time analysis and event correlation. In addition SEM systems are responsible for alerting the analysts whenever a rule is triggered. [7, 1]. SIEM system's high-level architecture that combines SIM and SEM system's capabilities is presented in Figure 3.

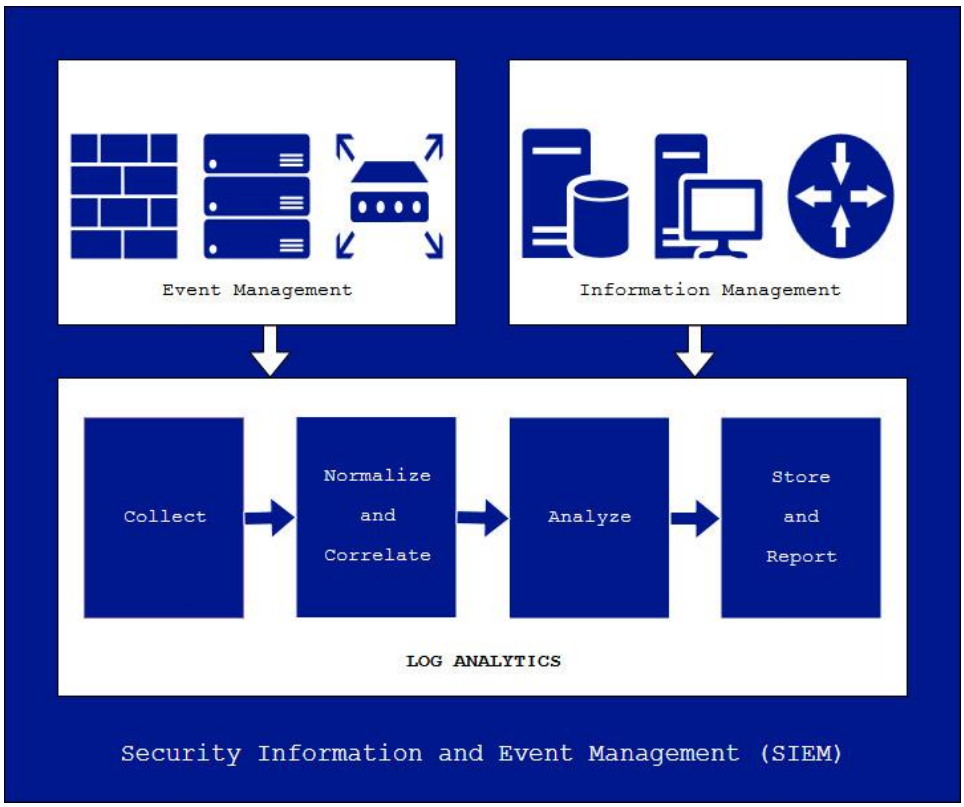

Figure 3. Unifying SEM and SIM into SIEM for centralized management [7, 1].

2.4.1 Collecting Log Data

SIEM systems can collect log data from various sources which include, but are not limited to workstations, servers, network devices like routers and switches, firewalls, IDS and IPS. Generally, any device that produces or processes security related data can forward it's logs into the SIEM. SIEM systems use log collectors to forward the security data into the main centralized unit. Log collectors can be either software or hardware appliances, depending on the product and the vendor. [8, 717-718]. Usually the log collectors can be installed centrally, so that the receive the data using for example syslog protocol. Syslog is a standardized protocol for transporting event logs. Syslog provides a standardized format for log messages. The protocol is defined in the RFC 5424 document. [9]. An organization may for example have multiple log collectors that simultaneously act as syslog servers. Therefore, the organization does not have to install hundreds or even thousands of software log collectors on end-point devices.

2.4.2 Normalization

Data normalization is essential when working with log data because it turns all data into a consistent format. Different vendors and products use various log formats in their log messages. Data normalization is crucial to SIEM systems, because the SIEM must be able to do correlation analytics in a multi-product environment. The networks may contain hundreds or even thousands of different log sources. Many SIEM products can process general log formats by default. According to Micro Focus, their SIEM product ArcSight can normalize data from over 500 different devices. In addition, users can write custom parsers that normalize the log messages to a certain form. [10, 1]. The data normalization format varies between vendors. The main goal of message normalization is to turn data from different vendors and devices into a homogeneous form. For example, ArcSight uses Common Event Format (CEF) in their SIEM. Some of the formats like CEF can be customized to include certain information that would not be normally included in the message. CEF includes a syslog prefix that consists of a timestamp and the hostname of the device that generated the log. After the prefix, a CEF message includes information about CEF version used, vendor, device product, device version, signature ID, name, severity and extensions fields. An example of a CEF message from the CEF standard document is presented in the Figure 4. A security device called threatmanager successfully stopped a worm malware and the severity of the event 10. The message also includes three extensions: source IP address (src), destination IP address (dst) and the source port (spt). [11, 5].

```
Sep 19 08:26:10 host CEF:0|security|threatmanager|1.0|100|worm
successfully stopped|10|src=10.0.0.1 dst=2.1.2.2 spt=1232
```

Figure 4. An example of CEF message [11, 5].

The accuracy of time and date data in log messages is crucial. SIEM systems cannot properly perform correlation and analytics if the logs have incorrect timestamps. Organizations commonly use centralized Network Time Protocol (NTP) servers, to synchronize the clocks between all devices. Using a NTP server is practically mandatory when collecting and analyzing log data. Large organizations can have log sources in different time zones. In the normalization phase, the timestamps are usually parsed and converted to a certain time zone, like Coordinated Universal Time (UTC). Events coming from different time zones can be analyzed centrally if the time data is normalized. In addition, the

analysts need to know exactly when certain events happened, so that they can search for additional information.

2.4.3 Rule Sets and Event Correlation

Detecting intrusions using only one log source can be difficult but when the information is combined with logs from other sources, even the stealthier attacks can be detected. Correlation means that security data is connected and compared between different devices and even device types. SIEM systems usually have pre-made correlation rules by default, but they are usually insufficient one their own. According to Crawley an example of a correlation rule could be that the SIEM system raises an alert if five login attempts using different usernames are performed from the same IP address within fifteen minutes, followed by a successful login occurring from the same source IP address to any machine in the network [12]. This example rule would be used to detect a brute-force attacks against login services.

SIEM system's correlation engines can be split into three categories. Similarity-based engines work by comparing events while trying to find similarities in them. The algorithms attempt to cluster events into groups by similarities. Similarity-based correlation engines do not need precise information about the different types of attack, as they solely find similarities. Knowledge-based correlation compares events to sets of rules. Knowledge-based engines depend on highly accurate rule-sets that must be constantly updated to stay relevant. Usually the rule-sets must be created per attack. For example, the same rules do not detect brute-force attacks and attackers trying to execute their own code on the organization's Internet facing web server. Statistical correlation engines try to find similarities with old and new events. [8, 720]. Statistical correlation algorithms use normally some forms of machine learning to build an understanding of normal activity on the network.

Developing rules for a SIEM requires high precision and expertise because too detailed rules are likely to be too narrow to raise any alerts, while too general rules cause numerous false positives that reduce SOC's efficiency. Creating SIEM rules is a time-consuming task because the rules must be tested thoroughly, so that it can be assured that the rules do not cause too many false positives or false negatives. Furthermore, the rules must be constantly updated to match the current threat trends. SIEM system's rules must

be customized for each environment which means that the same rules that work in an environment may not work in another one [12].

2.4.4 Monitoring and Reporting

SIEM systems are managed from a web-based user interface or a locally installed console program that connects to the SIEM. These user interfaces are used for configuring and monitoring the SIEM as well as analyzing the security events. SIEM systems usually include visualizing features that can be used to quickly form a situational picture of the environment. In addition, the SOC analysts can use search queries to find additional data. Because of the normalization, the same search function work across different source devices and services.

All major SIEM systems, including IBM's QRadar, Micro Focus' ArcSight, Splunk and Log Rhythm support reporting [8, 719]. Reporting is useful because a SOC must be able to prove its value to the organization. SIEM systems can be configured to automatically generate and send reports on a constant interval. For example, the SOC unit's manager may want to receive a daily report containing information of the last 24 hours. The manager may be interested in the number of alerts generated by the SIEM and the time it took by the analysts to respond to the alerts. [5, 171]. A trend report, on the other hand can be used to identify emerging trends in the alerts and security threats.

2.4.5 Alerting

Time is crucial in cyber security and the SOC unit must be able to react quickly when they notice a threat. SIEM systems are configured to raise alerts when certain conditions are met. The alerts can usually be configured in multiple ways. For example, the alerts can be raised into the SIEM system's console or the alerts can be sent via email or text messages. Some SIEM systems are also capable of pushing the alerts straight into ticketing systems or custom applications using application programming interfaces (API). APIs ease the process of integrating the SIEM system with existing infrastructure. For example, many IT companies use ticketing systems to organize the work tasks. Integrating the ticketing system with SIEM may be useful, if otherwise the analysts would have to create the tickets manually. A SIEM system's main functions are shown in Figure 5.

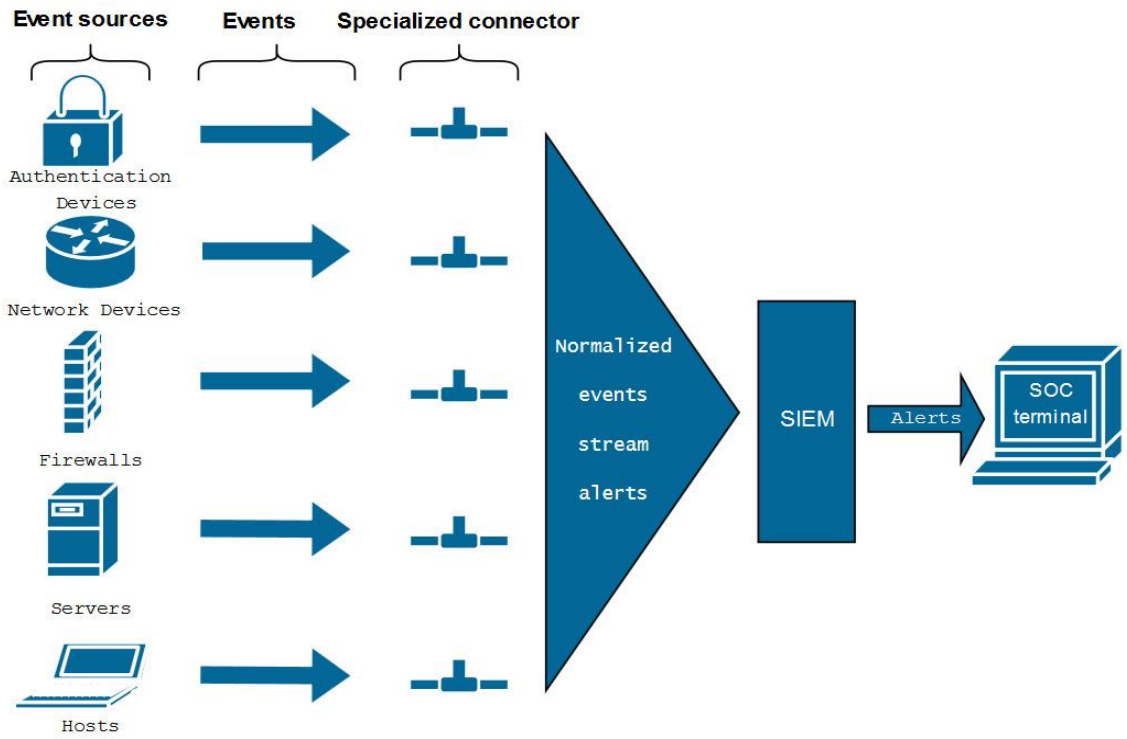

Figure 5. The main functions of a SIEM system. [2, 36].

2.5 Structure of a SOC – People

Enterprise SOC units are arranged around a SIEM system. SOC analysts monitor the SIEM systems for suspicious activities and events. Like many other IT units, SOC units often consist of multiple levels of analysts who have different responsibilities. Usually the higher-level analysts are more experienced and specialize in investigating complex events. The lowest level analysts, usually referred as tier 1, monitor the SIEM systems for alerts. When an alert is raised, the tier 1 analysts decide whether the alert is a true positive or a false positive. The suspected true positives are then escalated to higher level analysts, who perform deeper investigation to understand what caused the alert. Higher level analyst may have broader access to the security systems and tools for further investigation. [2, 37].

Multiple false positives from the same rule may imply that the rule needs further configuration. A senior analyst, or a separate SOC engineer, is in charge of modifying the rules so that it does not cause as many false positives. In addition, SOC engineers develop

and maintain the SOC unit's infrastructure so that the analysts can focus on finding the threats. [2, 37]. SOC units that have less resources usually have one or two layers of analysts. This means that a single analyst may be responsible for the whole lifecycle of a threat from the initial detection to the final eradication. In a small SOC unit, it is important that the analysts are experienced and competent. The lower number of analyst tiers increases the responsibility for a single analyst.

In addition to building and maintaining a situational picture, some SOC units perform digital forensics and incident response (DFIR). DFIR is needed when an incident has already occurred. Incident response concentrates on normalizing the situation after an incident so that the organization can continue with their day-to-day business. If an attacker has successfully breached the network, an incident responder's main task is to clean the systems and ensure that all the possible backdoors created by the attacker are removed. Backdoors are usually software that create a persistent connection back to the attacker so that they can access the breached systems afterwards and transfer data back and forth. Digital forensics is used to collect as much information about the incident as possible. The gathered information is usually used as legal evidence against the attacker. In case of a data breach, digital forensics is used to form an understanding of what data the attacker was able to obtain. In addition, digital forensics may be used if there are reasons to suspect an insider threat. For example, a digital forensics team could investigate if a former employee has stolen any sensitive data.

2.6 The Increasing Amount of Data

The amount of security related data that is generated daily by computing devices is only increasing. Almost all actions performed on computing devices generate log data. For example, loading a web page on an end-point device like a laptop produces multiple logs across many devices. Firewalls, for example decide if the packet should be forwarded or dropped depending on the active rules. In addition, the laptop and the AV running on it produces multiple logs. These log messages are sent into a SIEM that correlates and analyses them. The number of events that are being passed to a SIEM system is usually measured in EPS (events per seconds). SIEM systems can process a great number of events in a short period of time. For instance, Micro Focus's SIEM, ArcSight Enterprise Security Manager (ESM) is capable of processing up to 100,000 EPS in real time [10, 1].

Analyzing vast amounts of data is time-consuming. According to Zimmerman, a large SOC may collect, analyze and store tens or hundreds of millions of security-related events per day [5, 10]. Most of the events in the networks are always benign, so a SOC must isolate and prioritize the events that are indicating a security threat. Finding the real threats can be almost like searching for a needle in a haystack. SOC units must try to keep the volume of noise as small as possible to maintain focus on the real threats. Using sensitive and precise tools is necessary, as without them the analysts would be overwhelmed by the number of events.

Not all data is necessarily equally important. In cyber security, information has multiple parameters that must be assessed. Correctness of the data is important because the automated tools and the human analysts may perform wrong actions if the available data is incorrect. Similarly, events have different urgencies. While some events in the networks require immediate actions, the others may not. For example, a quickly spreading malware requires that the analysts act fast to minimize the damages. Detecting a port scan on the organization's Internet-facing services, like a web server may not require as fast action because port scanning happens regularly on the Internet. Of course, in both cases the analysts must investigate the alerts to assess the risks.

In a security operations center environment, the correctness of an alert can be described with negativity or positivity. Misinterpretation of information can have great consequences. For example, if a SOC analyst decides that an alert is a false positive due to insufficient or incorrect information, while the alert truly was a true positive, the misinterpretation could lead to a security breach. False negatives are a problem for SOC units, but false positives pose a greater threat.

When analyzing security related data, the amount of ingested data must be considered, as too little data affects the accuracy of the analysis, while too much data overwhelms the human analysts and their tools. Anomaly-based tools characterize a baseline for normal activity. Building the baseline is difficult if there is not enough data to analyze. [5, 36]. Figure 6 further explains the reasons why the amount of ingested data must be evaluated, so that the amount and the value of data are balanced.

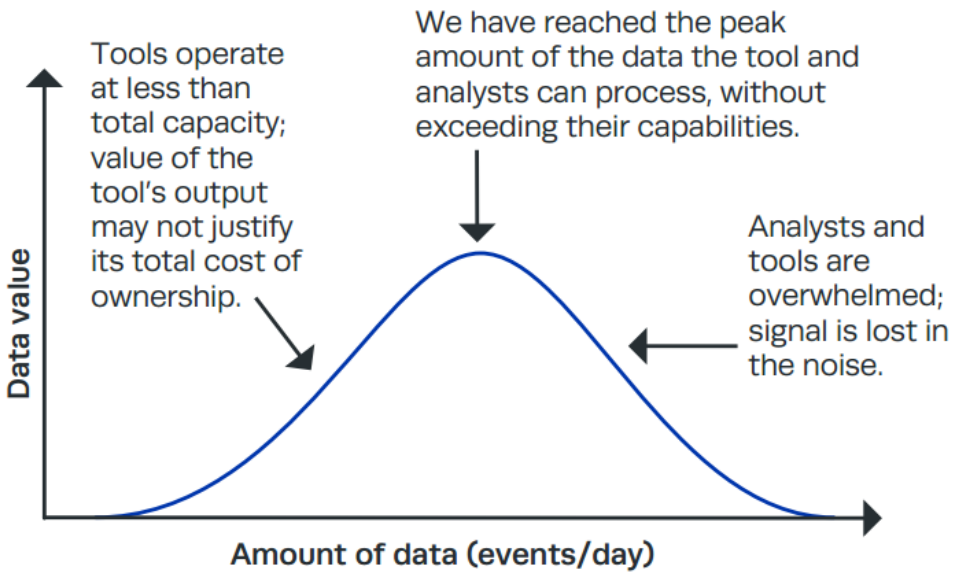

Figure 6. Balancing the amount of data with the its value [5, 38].

SOC units do not necessarily benefit from inspecting full packet captures on a daily basis. A full packet capture is a recording of all traffic. The amount of data in a full packet capture across the network can be overwhelming for real time analysis. However, a full packet capture may become extremely useful in post-incident analysis. By collecting packet captures, the SOC analysts can gain a more solid understanding on how the event occurred. A packet capture can be utilized to replay the events that happened before and during the attack. However, a full packet capture needs a lot of storage and analysis capabilities, as the size of the packet capture files increases quickly. [5, 131]. For instance, if an organization has a 1 gigabit per seconds (Gb/s) network connection and on average half of the bandwidth is utilized, the amount of data collected in a 24-hour period is 5.4TB. The calculation is illustrated below:

$$1000\frac{megabit}{seconds} * 60\ seconds * 60\ \text{minuntes} * 24\ hours * \frac{0.5\ utilization}{8\ bits\ per\ bytes} = 5.4TB \qquad (1)$$

The organization is probably capable of storing and processing 5.4TB of data, but for post-incident analysis 24 hours is not enough. To perform historical analysis the SOC needs at least a month's worth of data, which significantly increases the storage size requirements.

$$5.4TB * 30\ days = 162TB \qquad (2)$$

While collecting full packet captures can be extremely useful for post-incident analysis, it may not be possible for all organization to collect and analyze the vast amount of data it generates. The example used above covered only one 1 Gb/s connection. Commonly large organizations have multiple networks and possibly multiple offices with redundant connections. In this case the size of the packet captures increases significantly. An organization must assess the pros and cons of a full packet capture, as it requires a great number of resources to analyze and store the data.

NetFlow is a technology developed by Cisco Systems that as opposed to a full packet capture only records the summary of a network connection. NetFlow records do not include the content of the network packets, but rather the information that the connection happened in the first place. Usually NetFlow records contain the start and the end time, destination and source IP address and the port used, bytes sent and received and the OSI layer 4 protocol used for example, whether it was TCP, UDP or ICMP. [5, 127]. NetFlow thrives at summarizing the network activity and the simplicity of it can in some cases be a feature rather than a defect. The sub-OSI layer 4 information can be utilized to detect anomalies. For example, it is suspicious if a server constantly connects to a host using abnormal protocols. However, NetFlow is insufficient at its own, because it does not capture the packet's content. TCP port 80 is normally used in Hypertext Transfer Protocol (HTTP) connections. However, NetFlow does not capture any information above layer 4 so it cannot ensure that the connection is legitimate HTTP traffic. HTTP is most commonly used in serving web-content.

2.7 Internal and external Security Operations Centers

When an organization considers a SOC they must evaluate whether they build an internal SOC or buy it as a service from a managed security service provider (MSSP) [5, 15]. Commonly only large organizations have internal SOCs, because building and maintaining a SOC is expensive. It is also important to keep in mind that it can take a long time before a SOC is running at the desired efficiency, as it is an evolving unit that requires time to mature.

An internal SOC benefits from having a direct access to the monitored environment and the teams managing the infrastructure. However as mentioned before, SIEM systems

alone are often expensive, and operating a SOC is much more than just a SIEM. The whole process of building and operating a SOC requires lots of investments.

MSSP's vary in their services, as some provide SOC only for security monitoring. This means that the MSSP's SOC unit informs the customer if they discover threats in the customer's networks. After the customer has been informed of the threats, the customer is responsible for any actions to prevent an incident from happening. Some MSSPs offer services for the entire life cycle of an attack, which means that the MSSP handles the attack from detection all the way to the containment, eradication and recovery.

MSSPs and their customers make contracts that defines the service level agreements (SLA). The SLA obliges the MSSP to act within the time defined in the contract. This obligation benefits the customer because the contract forces the MSSP's SOC to react in the time frame that is defined in the contract. In addition, the SLA defines the MSSP's SOC unit's authority over the customer's network. [5, 75].

2.8 Collaboration with Other Organizations

A SOC unit acts as an individual unit inside an organization, but the SOC must be able to continuously collaborate with other units and organizations. When the SOC notices a weakness in the organization's defense, the SOC should notify other units dealing with the security about the weakness so that it can be fixed. Otherwise, the flaw can be exploited by an attacker. In addition to internal cooperation, security operations centers collaborate with other organizations, such as local law enforcements. National Cyber Security Center Finland (NSCS-FI) and Computer Emergency Response Team (CERT-FI) maintain a national situational picture of cybersecurity. The organizations release information about current threats, vulnerabilities and security breaches. In addition, CERT-FI advices in dealing with security breaches on a general as well as technical level. [13]. In a wide spread malware outbreak SOC units from different organizations can spread information with national security agencies that distribute the information further. Detection and prevention methods are just a few examples of the information that can be shared in a situation described above.

SOC units from different organizations can share cyber threat intelligence (CTI) on community driven platforms. Collaborating with other SOCs that share similarities like geolocation and industry can be extremely beneficial for both parties. [5, 222]. In addition, SOC units can work closely with security researchers [5, 316]. Security research is a broad term as some researchers try to find vulnerabilities in existing products before the adversaries while others may study malware and large botnets.

3 Problems with Traditional Security Operations Centers

The IT field is constantly changing, as new innovations are released on an almost constant phase. Cyber security units and organizations must keep evolving together with the new trends, so that they can defend from the new threats. For a long time, security operations centers relied solely on SIEM system monitoring device logs. However, as the cyber security field has changed greatly, the same tactics that used to work five to ten years ago do not necessarily work anymore.

3.1 Manual Labor and Unmanageable Workloads

A SOC must evolve in unison with the current threats and trends in the information security field. SIEM rule sets must be maintained and fine-tuned constantly, so that the SOC can detect security offenses. This requires that SOC personnel are aware of the new trends. Collecting CTI is a challenging because the amount of available data is overwhelming [6, 17].

When a SOC receives an alert, the analysts must manually search the SIEM for additional information, so that they can decide whether the alert was a false or a true positive and act accordingly. Manually querying the SIEM and other security related systems is time consuming and prolongs the time it takes to notice the real threats.

Humans tend to become tired and lose concentration when they do repetitive tasks. If the bulk of alerts are false positives, it may be difficult for the analyst to prioritize and remain accurate. Many of the repetitive tasks can be automated, so that the security analysts can focus on real threats. Automation also helps to reduce the time-to-response. [14]. Automation is further discussed in chapter 4.2

3.2 Scalability and Modularity

Due to the ever-changing manner of cyber security, a SOC should be built modularly, so that it can adapt new security technologies and processes. Security technologies and tools are developing constantly, and a SOC must be able to keep up with the technical and non-technical advancements, so that it can identify new threats. In addition, a SOC

unit must be able to adopt new processes because the defensive side of cyber security is always running behind, trying to catch up with the adversaries constantly developing new methods to attack organizations.

There is not a single, universal technology or a tool that is solely capable of defending and monitoring the network on its own. Security vendors specialize in developing different tools that may or may not communicate natively with each other. This can easily build silos of security information that complicates the process of maintaining a situational picture. [15, 1]. For example, some vendors specialize in developing complicated machine learning algorithms for security tools, while others develop firewalls or SIEM systems.

3.3 False Positives

False positives are one of the greatest challenges for SOC units, as there is not a simple way to suppress the number of them. SIEM systems produce numerous false positives if they are not properly configured and maintained. Without sufficient tuning, the number of daily alerts can be in the thousands in a large enterprise's environment. No matter how large the SOC is, thousands of daily alerts is way more than the analysts can investigate profoundly. As a result, a SOC may have to reduce the number of events that are fed into the SIEM by excluding lower priority alerts. However, this can lead to potentially missing threats, because highly skilled adversaries can perform attacks without generating lots of noise. To reduce the number of false positives the SIEM's rules must be adjusted and tuned constantly, which requires a lot of time and knowledge. Furthermore, it is important to note that a SOC must be able to focus on the present, as attacks or violations may happen at any given time. False positives slow down the whole security operations and can create a growing queue of alerts that need to be examined. The main mission of a SOC is to provide real-time situational awareness. False positives cause distractions that slow down the detection of the real threats.

3.4 Unnecessarily Complex Processes

A SOC must be able to react quickly to new alerts and indicators because attacks can happen in minutes or even seconds. In May 2017 a ransomware called WannaCry spread around the world infecting 400,000 computers [6, 28]. WannaCry targeted

vulnerable versions of Server Message Block (SMB) service that is used for local network file sharing and network printing. [16]. For example, the ransomware affected U.K.'s National Health Service (NHS) operations significantly, as the ransomware rendered their devices unusable including computers and magnetic resonance imaging scanners. The ransomware outbreak affected their day-to-day operations and could have caused casualties. [17]. In October 2018, the English Department of Health and Social Care reported that the estimated financial cost of the 2017's ransomware outbreak is £92 million. The same report states that NHS will be investing in a SOC to enhance their ability to detect and respond to cyber attacks. [18]. A SOC must be agile because threats can escalate into incidents rapidly. A SOC unit may not be able to react swiftly if they are restricted by strict processes.

Classically only large organizations have had the resources to operate an inhouse SOC. However, large enterprises are not usually especially agile because the authority is spread between numerous units and executives. A SOC unit's reactive nature forces the analysts to perform quick actions. Insufficient authority lengthens the response time, because the analysts may have to request permissions to perform the preventive actions. The SOC unit's level of authority can be divided into three main levels: no authority, shared authority and full authority. A SOC without authority can only suggest actions to take. For example, A MSSP SOC can have no authority over the customer's networks and therefore they can only give suggestions. Shared authority means that the SOC performs decision-making together with the organization's executives. Therefore, the SOC unit's opinion has some weight, but it cannot perform actions on the organization's assets independently. A SOC with full authority can directly instruct other units to perform actions to organization's assets. With full authority, the SOC does not have to request approval from higher level executives or units. [5, 17]. The scope of the SOC unit's authority must be defined carefully so that the SOC and all the other parties are aware of it. When the level of authority is clear, the SOC can focus on performing the right actions.

3.5 Poor Visibility into the Networks

To extend a SOC to its fullest capabilities the unit should have an extensive vision in to the managed networks. The SOC's vision consists primarily of the quality and quantity of the monitored devices and services. If the SOC only has limited visibility, some of its

capabilities like SIEM system's efficient usage deteriorates. In addition, the possible incident response and other reactive measures become much more complicated as the analysts must make decisions while not having enough information. For instance, a MSSP SOC monitoring numerous customer networks, could only receive events from the customer's edge firewall that is located in between the Internet and the customer's local area network (LAN). In this case, the analysts have very little information to use as a base for the decision-making. If an attacker has successfully evaded the Internet edge's security appliance, the attack can remain unnoticed.

Nowadays, it is a trend to encrypt all data, both in transition and "at rest" in storage. Encrypting data in transition prevents man in the middle attacks (MitM), where an attacker places themselves between the source and receiver of the connection and examines the IP packets for sensitive information. If the traffic is not encrypted, all data, including passwords and other secrets, is transitioned in plain text. Encrypting all traffic using a strong algorithm makes it extremely challenging and time consuming for the attacker to decrypt the data. While encrypting data is sensible, it may worsen the visibility for security tools.

Network Intrusion detection systems (NIDS) and network intrusion prevention systems (NIPS) analyze data that is transmitted in the network, and they may therefore be unable to inspect encrypted packets. [19, 222]. Some NIDS and NIPS systems can perform packet inspection on TLS (Transport Layer Security) encrypted data. TLS is used for example in HTTPS (Hypertext Transfer Protocol Secure). Practically, security systems that can perform packet inspection on encrypted data, are performing MitM attacks. However, the security system's performance decreases significantly when they are configured to perform encrypted packet inspection. The significantly lower throughput can make it impossible to use this feature in a high-traffic environment.

3.6 Evolving Threats

Advanced persistent threat (APT) is used to describe highly skilled and motivated attackers that have the resources to perform extensive and sophisticated attacks. APT's are usually part of large criminal organizations or like some of them, backed by nation states. An APT focuses on a single target for an extended period of time and continually adapts

to the defender's tactics to maintain a foothold to the network. [5, 319]. APT's may for example use a staged approach, like the cyber kill chain which is a framework developed by Lockheed Martin. The cyber kill chain consists of seven steps, that are used by attackers to gain access to their main objective. The adversary's object can for example be a remote access to the target organization's customer database. [20]. Traditional defensive methods may be insufficient to detect and stop APTs. Static approaches such as signature-based IDS and IPS and firewalls are not enough on their own to defend from skilled and determined attackers who may use custom built malware. The different steps of the cyber kill chain are illustrated in Figure 7.

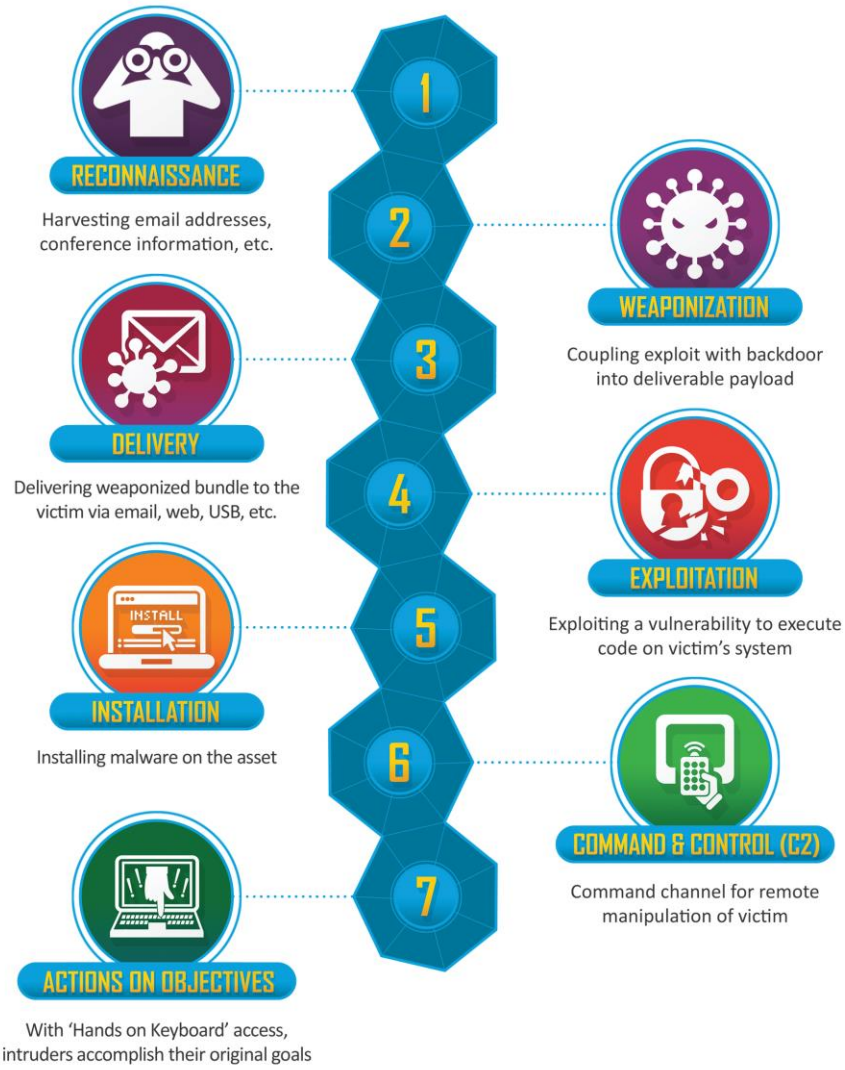

Figure 7. The Cyber Kill Chain framework that divides a cyber attack to seven phases [20].

Current SOC units tend to focus on short-term alerts, and do not necessarily asses the long-term situation. This is due to the historically reactive nature of a SOC. Highly skilled and determined attackers like APTs can exploit this trend by performing slowly advancing and stealthy attacks, which can be nearly impossible to detect in a short amount of time. [2, 39]. In the reconnaissance phase the attackers would study the organization for an extended period. This includes gathering as much information as possible about services running on the organization's premises, as well as external cloud platforms. In addition, the reconnaissance phase involves investigating the target organization's employees to find possible targets for the delivery phase. After the adversary has found a weakness in the target's Internet facing services, or selected a group of employees to target, the attacker will begin the weaponization phase.

Weaponization consists of developing an exploit for an Internet facing service or constructing a custom phishing campaign that targets individuals or a certain target group. A targeted attack can be almost impossible to notice in the first two phases because the adversaries try to minimize the digital fingerprints that they are leaving. Attackers utilizing open source intelligence (OSINT) may not even directly visit the target's website before the delivery phase. OSINT includes gathering data from publicly available sources like social media and online publications. [6, 23]. The payload can be delivered by directly exploiting a web server, or by sending email that contains malicious code to the targeted employees. The exploitation occurs when the adversaries run their own software on the target machine. The software creates a backdoor for the attacker. The attackers use a command and control (C2) servers to remotely manipulate the target machines. After the attackers can control a machine inside the target organization's network, they continue advancing towards their goal.

Hackers are using and developing highly automated programs to scan the Internet for vulnerable applications and servers. These kinds of attacks generate a lot of noise which can distract the analysts. In addition, hackers are creating complex and sophisticated tools for scanning the Internet and exploiting vulnerable systems. Shodan is a website that acts as a search engine for Internet-connected systems. Unlike normal search engines like Google, that only crawl websites, Shodan crawls the Internet to find running services. [21]. Vulnerability exploiting tools like Metasploit are used by penetration testers, as well as malicious hackers [22]. AutoSploit is a tool that combines Shodan's search engine functions and Metasploit's exploiting capabilities to automatically exploit

vulnerable services found on the Internet. The tools itself is not completely unique, but it raised debate in the cyber security community, whether releasing these kinds of automatic mass exploitation tools is morally right, because they do not require any skill and the consequences can be severe. [23]. Tools like AutoSploit are mainly used by script kiddies. These kinds of tools are not generally used by sophisticated attackers, because they create a lot of noise in to the network which causes SIEM to raise alarms. However, it is important that analysts know that these kinds of tools exist.

3.7 Lack of Modern Tools and Attackers Bypassing the Defenses

SOC relies on highly precise tools that are capable of detecting and stopping attacks. Security devices and software have improved notably in the past years. However, static defense mechanics are insufficient on their own, because skilled attackers may be able to bypass these defenses. Attackers may use techniques like obfuscation, fragmentation and encryption. Obfuscation means that the attacker manipulates the packets so that the signature changes, while maintaining the payloads integrity, so that the receiving device interprets the packet normally [24, 4]. If the IPS and the antivirus systems are configured to block certain signatures, the obfuscated packets may bypass the defenses. Fragmentation means that a packet is split into multiple smaller packets. Packet fragmentation is normal in networks and networking capable devices can usually handle this well. A TCP packet's headers contain information about the right order, so the fragmented packets are reconstructed when received. Some security devices do not assemble the fragmented packets, which can lead to malicious packets passing unnoticed. Attackers can encrypt the messages so that the security device cannot read the malicious content from the packets. [24, 5].

Signature-based tools, including IDSes, IPSes and AVs must be equipped with the latest signatures so that they can defend the organization from attackers exploiting the latest known vulnerabilities. Signatures should be updated regularly, preferably on a daily basis. WannaCry infected computers that were running Windows operating systems. The ransomware used a vulnerability that was fixed in an update released almost two months prior to the WannaCry outbreak. [25]. Open-source IDS/IPS Snort released signatures for the vulnerability MS17-010, that WannaCry was using on 14.3.2017 [26]. The security updates and IDS/IPS signatures were released almost immediately after the vulnerability

was found. Still, WannaCry was highly successful, considering the number of infected computers. The threat could have been mitigated by installing the security updates and detection signatures.

4 Next Generation Security Operations Center

A mature, next generation SOC has the same mission as its predecessor - to defend the organizations network from unauthorized activity, while providing situational awareness. However, the fast pace of the cyber security industry has forced SOC units to evolve. The traditional tools and processes worked for quite a while, but new threats have emerged in the last couple years. Many of the challenges are due to the increasing amount of data and the new tactics used by adversaries. The number of alerts has become exhausting and investigating all of them is beyond the capability of human analysts. Computers are much more efficient at processing and executing repetitive tasks. However, not everything can or should be automated, as automating security tasks can cause problems [27, 3]. Automating SOCs functionality is further is discussed in chapter 4.2.

4.1 From Reactive to Proactive

SOC units have historically been mainly reactive units that respond to threats as they are discovered. However, as the number of threats grow, and they have become more dangerous to the organizations, SOC units must evolve towards proactive incident prevention. Cyber attacks can happen in minutes which may be too fast for a SOC to react in time. This means that in addition to reacting to security threats, a SOC must take measures before an incident occurs. To become proactive a SOC unit must develop processes for constant threat analysis to maintain a situational awareness. For example, proactiveness can be improved by actively scanning the networks and host system for known vulnerabilities, so that the necessary updates or other precautions can be deployed before an attacker can exploit the vulnerabilities. [5, 10].

4.2 Automating the Defenses

New tactics, techniques and processes (TTPs) used by advanced attackers have weakened the effectiveness of static defense methods like signatures-based IDS/IPS. Nonetheless, static methods are still relevant, as they stop and detect automated tools and basic attacks. However, detecting targeted attacks requires effort and precisely configured defensive systems. Machine learning and artificial intelligence has become

increasingly popular in cyber defense products. For instance, Darktrace's Enterprise Immune System uses machine learning to build up an understanding of normal activities on the network. The self-learning algorithm adapts to changes in the network, while improving its accuracy over time. [28, 1]. Traditional static intrusion detection systems, cannot normally detect zero-day malware, because they use signature-based detection engines. Zero-day malware uses previously unknown vulnerabilities to exploit or infect target systems. Signatures do not exist for zero-day malware, as no one has encountered them before. Anomaly-based tools do not require any signatures, which makes them effective against previously unknown threats. However, machine learning-based systems tend to generate a lot of false positives and false negatives. Machine learning-based tools work best when combined with static tools, because of the high false positive rate. [29, 171].

Artificial Intelligence (AI), which is a hypernym for techniques like machine learning, can be utilized to support the human's decision-making progress. Machines lack skills that humans have naturally. Computers are not as good as humans at understanding social behavior that is natural to human. For example, a SIEM system's security analytics engines and AI lack common sense and moral. Even though cyber security is technical in many cases, utilizing human expertise is necessary. The advances of human and machine collaboration in cyber security is presented in Figure 8.

Figure 8. Bridging the gap between the analysts and their tools using artificial intelligence [30].

Machine learning based tools can be especially helpful for MSSP's SOC units. Building the definition of normal activity in the customer's network can be almost impossible without the use self-learning tools. Even if the customers provided the SOC with enough information about the network environment, the MSSP may not be aware of the customer's internal changes. Typically, the customer may provide a limited view to the network. For example, the SOC could only receive security events from the edge firewall that is placed between the customer's private network and the Internet. However, this does not provide enough information for the SOC, as the SOC can only see the traffic between the Internet and the LAN. A machine learning IDS/IPS inside the customer's network will provide a more comprehensive view to the customer's network.

Some AI powered intrusion prevention systems can perform autonomous threat response. For example, Darktrace's Antigena can be configured to disrupt malicious connections. Antigena does this by sending TCP RST (reset) packets to the networking devices to interrupt the transfer of malicious data. [31]. Automating repetitive tasks using machine learning and artificial intelligence is important, but automation has also its downsides. The weaknesses of automation are mainly due to the fact that machine learning systems in general produce a notable number of false positives. For instance, if a machine learning based IPS system has capabilities to shut down and block connections due to malicious activity, it can cause a denial of service. An accidental DoS attack can have destructive consequences if it is performed on critical components. For example, the system could disrupt medical devices in a hospital or air traffic control devices in an airport. [27, 2]. In both cases, the cybersecurity incidents can easily reflect into the physical world. When evaluating such options, it is important to be aware of the environment so that the risks can be assessed.

4.3 Automated Threat Intelligence

Being aware of the newest threats helps a SOC units to lean towards proactive defensing. As discussed earlier in chapter 3.3, collecting relevant threat intelligence is demanding, because the amount of available data is massive. Numerous new threats are discovered daily, and it is important to assess only those that are meaningful to the organization. Threat intelligence is beneficial, but it is important not to saturate the list of collected threat intelligence with insignificant information. Good threat intelligence is up-

to-date, relevant to the organization and clearly describes the threat. [5, 244]. Numerous CTI sources exist, and their content may overlap, which makes finding relevant threat intelligence difficult. However, there are many commercial and free threat intelligence platforms available that gather information from multiple sources. For example, IBM's X-Force Exchange is a community-driven threat intelligence sharing platform where security professionals and researchers can discuss and share their newest discoveries [32].

Threat intelligence platforms are also used to share indicators of compromise (IoC). IoCs are signs on a computer or a network that indicate an intrusion. IoCs can be for example cryptographic hashes like MD5 or SHA1 of a malware sample or a known malicious IP addresses that have been affiliated with a recent cyber attack. [5, 247]. IoCs can be added to the SIEM, so that an alert is raised when a known IoC is identified. Figure 9 presents an infrastructure built around CTI. The data is collected from multiple sources, that include free and commercial threat intelligence feeds and platforms. Afterwards, the data is analyzed centrally using automated tools and correlation engines. The processed information is forwarded to the desired destinations. For example, IoCs are sent to the SIEM, virus signatures to the endpoint AVs, and IDS/IPS signatures are sent to the network IDS/IPS. The SOC analysts and other security personnel have access to the threat intelligence platforms, where they can find further information about the threats.

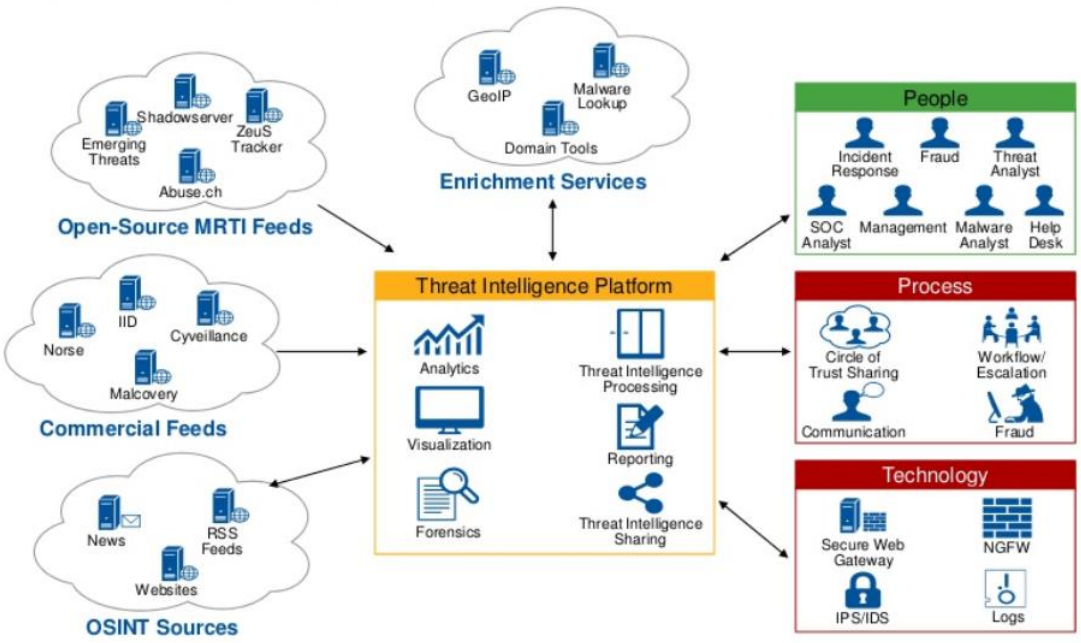

Figure 9. Centralized threat intelligence [33, 23]

Trusted Automated Exchange of Indicator Information (TAXII) and Structured Threat Information Expression (STIX) are open and free specifications for automated threat intelligence sharing. TAXII is an application layer protocol for sharing CTI over encrypted HTTPS connections, while STIX is a structured language for standardized communication. Many CTI sources like IBM's X-Force Exchange and AlienVault's OTX can act as STIX/TAXII servers, providing easier integration with other product used by SOC units. [34]. STIX/TAXII servers can be used to automatically send the normalized threat intelligence to the internal CTI platform. The platform processes and distributes the CTI to desired destinations. This reduces the number of different tools that SOC analysts use daily.

Externally obtained CTI is useful because it contains information about current threat trends. However, it contains a lot of unnecessary data that may not be relevant for the organization. To acquire personalized CTI for the environment, an organization can deploy honeypots. A honeypot is an isolated system emulating a real server or a service. Honeypots do not contain any real information that could benefit an attacker. Honeypots are usually configured to be less secure than the systems they are emulating, so that they attract the attackers. [7, 3]. The honeypots are thoroughly monitored, and any action performed on them raises an alert. For example, honeypots are usually configured so, that they do not receive or send any data in a situation. Because of this, even a port scan performed by an attacker raises an alert and reveals the attacker. However, skilled attackers may be able to detect the honeypots, and therefore avoid being caught. Honeypots can be placed inside the organization's LAN or the Internet's edge, depending on the purpose. Honeypots inside a LAN are used to detect intruders that have managed to bypass the edge's security devices. Contrarily, honeypots placed on the Internet's edge gather much more data that can be used as CTI. The honeypots may collect IoCs such as malware hashes and malicious IP's.

4.4 New Trends – IoT and Cloud Computing

Internet of Things (IoT) devices have gained popularity in the last few years. IoT devices range from home automation equipment all the way to industrial appliances that are connected to the Internet. These devices are used for monitoring and operative functions.

Gartner has predicted that by the end of the year 2020 there are more than 20 billion IoT units, of which 7.5 billion units are used by businesses across different fields [35].

Some IoT devices have had security issues, partly due to their usually low processing capabilities along with restricted management features. These restrictions may mean that using traditional protective and cryptographical mechanisms is not possible. IoT devices themselves may not process highly sensitive data. Therefore, they are not usually the attacker's main target. However, poorly secured IoT devices that are directly connected to the Internet can be used as stepping stones to gain access to the network that the device is connected to. In addition, botnets of infected IoT devices have been used in DDoS attacks. A botnet is a network of infected computing systems that are controlled by a single malicious party. In October 2015, DNS service provider, DYN was attacked by botnet that launched a massive DDoS attack against the company's infrastructure. The botnet was built using a malware called Mirai and consisted of up to 100,000 nodes, of which most were poorly secured IoT devices and home routers. [36;37]. Many major websites like Twitter, Reddit and Spotify that used Dyn's services became unavailable for hours [37].

IoT devices are getting constantly more popular, because more applications for these low-resource computing systems are being developed. It is inevitable that these devices are becoming a part of a normal network. The sheer amount of IoT devices in the near future will generate a lot of data. This must be considered by SOC units because in the near future SOCs must be able to process the data generated by IoT devices. Otherwise, the SOC cannot maintain a situational picture of the security.

Another challenge that SOC units are facing, is the increasing usage of cloud computing. Cloud computing means highly available, on demand computing resources that in some cases are rented from service providers. Private cloud means that the organization owns the hardware servers that are used to power the cloud but, in this chapter, the focus will on the public cloud, because of the challenges it creates. Public cloud providers like Amazon's AWS (Amazon Web Services) and Microsoft's Azure rent pools of computing resources that can be accessed from anywhere. Moving resources from a local network to the public cloud on the internet, causes new challenges for the SOC. While using public cloud, the organizations have limited authority over the cloud provider's networks. This means that the organization's may be unable to see what happens in the cloud's

network environment. However, many of the modern SIEM systems can be integrated with cloud resources by deploying a log collecting software into the cloud. The log collector forwards the parsed event messages to the SIEM locating on the organization's premises. Alternatively, the log collector may be physically on the organization's premises. In this case, the services in the cloud like are configured to send the log data to the log connector over the Internet. In addition, it is possible to deploy a SIEM system into the cloud [38, 403]. However, this is usually worthwhile only if the organization utilizes the cloud extensively, rather than hosting services locally.

5 Building a Scalable and Adapting Security Operations Center

Building a scalable and adaptive SOC unit can be complicated because certain aspects must be planned in advance. Before building a SOC, the organization must assess their existing security program, that consists of tools and processes. The organization should have thorough log collection and management programs in place, because the amount of available data directly defines the SOC unit's performance. A SOC is not a magical unit that can protect an entire organization on its own. When basic security measures are in place, a SOC unit can provide additional cyber security situational awareness, that no other unit or technology can.

5.1 The Visibility into the Networks

It is important to assess the suitable visibility into the customer's network, when building a MSSP SOC. As discussed earlier, a SOC unit's effectiveness threats detection is directly proportional to the visibility they have into the network. However, this can lead to alert exhaustion if SIEM rules are not configured properly. The number of devices that are feeding alerts into the SIEM play an important role in the extensiveness of a SOC's visibility into the network. Critical alerts from firewalls alone are not enough for a SOC to be able to perform correlation and proactive defense. In addition to the received number of events, SOC units benefit from having access to network topology maps, that describes how the different devices are connected [5, 111].

As discussed earlier, NIDS and NIPS are not enough on their own, because most the of traffic is being end-to-end encrypted. Some products are capable of decrypting TLS traffic, but this lowers the throughput speed. TLS decryption is usually used to block end-user's access to harmful or otherwise forbidden sites from the organization's network. This upstream decryption is only capable of decrypting the data that is originating from the organization's own network. Host intrusion detection systems (HIDS) and host intrusion prevention systems (HIPS) are installed on the endpoints. HIDS/HIPS systems do not necessarily need to decrypt the traffic because they monitor the end-point device's services and logs. The software can also help to identify insider threats and potentially dangerous misuse. [5, 121].

When building a security operations center, the organization should already have a mature security policy, that they are executing. A SOC is only as good as the existing security program. If the overall security is insufficient, a SOC may not be able to improve it significantly. SOC units depend on the existing technologies to block the routine threats and provide the data for further analysis. The organization should have both network and host security systems. The network defense may consist of firewalls and NIPS/NIDS devices deployed on all network segments. The end-points should be protected with AV and HIDS/HIPS software. The logs should be collected from all devices and forwarded to the SIEM. In addition, the host operating system's security and audit logs should be collected and analyzed as they contain important data. However, this is only the bare minimum that a SOC unit needs to perform their operation.

5.2 Asset and Vulnerability Management

To act proactively, a SOC should be aware of the organization's assets. An asset in computer security is any device, software or a piece of data that should be protected. Physical assets include for example, servers and networking devices. Software assets on the other hand may be even more important for a SOC, as the unit focuses on maintaining a situational picture of the organization's cyber premises. In addition to maintaining an understanding of the assets, a SOC should be aware of other information regarding the assets like software versions used on a web server. Having information about the assets helps to proactively identify threats as new vulnerabilities are found. A great part of information security is keeping devices and software up to date. Updates are extremely important in security as adversaries may try to exploit known vulnerabilities to gain their goal, whether it is access to sensitive information or access to the target organization's internal systems. However, installing an update on a business-critical service can be a complicated process and sometimes the new updates can be incompatible with other components. When SOC analysts know the vulnerabilities, they can look for certain IoCs that are linked to the vulnerabilities.

Assets have multiple parameters in information security. An asset has technical properties like for example, software version and an IP and a MAC address. However, an asset also has a certain value for the organization. This value can consist of a financial benefit created be asset. On the other hand, the asset's value might not be financially significant,

but it is necessary for the organization's day-to-day operations. Both properties should be assessed in asset and vulnerability management. Severe vulnerabilities, that are easy to exploit, in critical assets must be fixed immediately. On the other hand, minor vulnerabilities in internal systems may not need as fast attention.

Vulnerabilities could also be detected by regularly scanning the network with vulnerability scanners. Vulnerability scanners are programs designed to search networks, devices and applications for known weaknesses. One of the most popular vulnerability scanners is Tenable's commercial Nessus [39] but many open source and other proprietary scanners exist as well. MITRE maintains a list of known vulnerabilities, Common Vulnerabilities and Exposures (CVE). CVE aims to provide a standardized list for each vulnerability or exposure. CVE's contains CVE ID number for example CVE-2018-1312 (Vulnerability in Apache HTTP Server), brief description of the vulnerability and references like advisories or reports. Vulnerabilities are scored using Common Vulnerability Scoring System (CVSS). Current version is CVSSv3 (released in June 2015) and it scores the vulnerabilities from 0 to 10, with 10 being to most critical. [40]. Asset and vulnerability management is especially complex in a MSSP environment. However, being aware of the assets helps a SOC to execute its mission proactively. For example, if a SOC detects a new critical vulnerability through CTI for a certain version of Apache HTTP server, they can proactively notify the parties that are running that version of Apache to update the service. If upgrading is not possible in a short period of time, the SOC can focus on identifying certain IoCs that are associated with the vulnerability.

5.3 Utilizing Technologies and Tools

The amount of available data is forcing SOC units to make use of computer-based analysis tools. User and Entity Behavior Analytics (UEBA) systems use machine learning algorithms and statistical analysis to find abnormalities in actions performed by humans. UEBA systems can detect for example insider threats and user accounts controlled by attackers. [41]. If compared to a SIEM system that looks for anomalies in the network, an UEBA system analyzes human behavior to detect abnormalities. However, products that combine these two exists. Rapid7's InsightIDR is a SIEM that is capable of analyzing user and entity behavior [42]. Combining SIEM and UEBA systems can be helpful, because it centralizes the management.

As the amount of data increases, the SIEM systems must be able to ingest and process large amounts of data. The vast amount of data is usually called big data [8, 717]. Many big data analytics implementations use distributed computing frameworks, like Apache Hadoop. Hadoop distributes the computing tasks to multiple machines simultaneously, which makes the mathematical calculations notably faster, compared to single machine computing. [43]. While the amount of data is increasing, searching the security events must still be fast.

5.4 Processes

SOC processes should be agile and evolve constantly with the current threats. Processes should be streamlined, so that the SOC can handle incidents within a short amount of time. AlienVault suggests dividing the processes into four stages – event classification & triage, prioritization & analysis, remediation & recovery and assessment & audit. The first level, event classification and triage mean that the analysts monitor the latest events and alerts starting from the most critical ones. If the analyst verify that an event requires deeper investigation, they will escalate the issue to a higher-level analyst. It is important to note that if the SOC team is small and does not have multiple levels of analysts the same analyst may perform the further investigation. [44, 9] The next is prioritization and analysis, where SOC staff prioritize their actions, so that the most significant events are analyzed first [44, 11]. For instance, an IoC should have a higher priority than a detected port scan. If the analyst discovers an incident the analyst starts the remediation and recovery stage, where the damage caused by the incident is minimized and similar attacks are prevented. The SOC should collaborate with the rest of the IT department in the remediation phase. [44, 13]. A modern SOC is evolving constantly. To support the improvement, the SOC should assess itself regularly. Processes for self-assessment should be clear and could include metrics like mean time to resolution by incident level, incident by classification and percent of false positives [44, 14]. In addition, the collected metrics can be used to evaluate the current trends and the sufficiency of configurations.

Measuring the capabilities of a SOC can be a complicated task because of the varying nature of the mission. Conventional metrics, like measuring the number of resolved tickets in a certain timeframe can be difficult or even impossible to apply to a SOC. It is

important to remember that a SOC is only a part in an organization's defensive toolkit. If the overall security is insufficient, a SOC may receive numerous of alerts which leads to a high number of resolved alerts. However, this may not mean that the SOC is particularly good. The meaning of a SOC is not to replace other security processes and tools, but rather to complement these by filling the gaps and providing a higher-level visibility across the whole environment.

A SOC unit should not concentrate solely on events that are blocked by other defenses, like firewalls. When creating reports for executives, the SOC should try to minimize the emphasis on the Internet's background noise like port scans. Reporting the number of firewall blocks is unnecessary, because it does not measure the SOC unit's efficiency or usefulness. SOC units should primarily focus on complicated events that cannot be detected and prevented by classical defenses. A SOC unit's mission is not to be a substitute for a firewall or an IDS/IPS. Firewall and IDS/IPS technologies excel at their tasks which is to detect and prevent individual threats. However, they only see traffic passing, and therefore cannot build an overview of the threat.

In an ideal situation, the automated systems eliminate the simple threats, so that the SOC unit can focus on the more complicated tasks. In reference to the last paragraph, if the overall security is good in an organization, the SOC does not receive as many alerts as opposed to an organization that does not have as good security measures deployed. It is likely that the SOC unit that receives less alerts, is more effective when it comes to detecting and mitigating complicated threats because it can focus on the threats that would not be detected by conventional defenses.

Self-assessment is not enough on its own. To truly test a SOC unit's capabilities the organization should consider hiring a red team. A red team is a group of people authorized to simulate a fullfledged cyber attack. A red team assessment is like a penetration test but more extensive and covers all the attack vectors. The purpose of a penetration test is to find as many vulnerabilities in the IT environment as possible, whereas a red team assessment tests the organizations capabilities of detecting and responding to attacks. [45]. A red team assessment can be used to find weaknesses in all building blocks of a SOC unit – people, processes and technologies. A red team assessment may in addition cover physical security. If so, the testers may for example use social engineering on the target's staff to get into critical areas like server rooms. Thorough testing helps to

mature a SOC unit. For example, defending an organization from an APT can be extremely difficult if the organization hasn't been targeted by an APT before. A skilled red team can simulate an advanced adversary and therefore train the analysts to detect these kinds of attacks.

A SOC should consider building a playbook, as it guides the SOC analysts to perform the right actions from the beginning of detection. A playbook consists of solutions and steps to solving certain kinds of alerts. Building a playbook can reduce the SOC unit's response time, as SOC analysts use it as a guide. [46]. It is important to note that a playbook can become obsolete quickly if it is not updated regularly with the current threats and solving steps. A playbook can be constructed in several ways, depending on the organization and the skill level of SOC employees. For example, a playbook can be a collection of flow charts that are categorized by the type of attack like DDoS, data theft or malware outbreak. After the type of the attack has been defined, the analysts follow the flowchart that supports quick decision-making based on the threat's type. The playbook can be built on an open platform, which allows everyone in the SOC unit to involve in building it. Internal collaboration is vital to a SOC, and therefore the unit should have an easily accessible collaboration platform, like a private real-time chat room [5, 303]. Collaboration helps to spread knowledge and skills between the analysts.

A SOC unit should have clear processes for escalation as well as disaster-like situations, where for example a zero-day malware spreads widely inside an organization's network. A SOC's purpose after all is to ensure continuity of the organization's normal day-to-day operations. For a non-cybersecurity company, a SOC is not a productive unit – it's function is to keep the organization out of the newspaper's front page that reports a new data breach. Whether an organization has an internal SOC or it buys SOC as a service from a MSSP, the organization must have a working disaster recovery plan. WannaCry ransomware outbreak in mid-2017 was a great example of the importance of a working disaster recovery plan. The organization must be able continue with their day-to-day operations even if half of their endpoints are rendered useless by a ransomware that encrypted the endpoints hard drives.

5.5 People

While many tools help SOC units to react quicker and achieve better visibility, the people are still by far the most important part of a SOC. Automating the repetitive tasks does not reduce the importance of human analysts. AI and human analysts support and complement each other. However, finding talented employees to a SOC can be difficult. The work tasks of a lower tier analysts can be quite repetitive, which may lead to a high turnover rate amongst the lower tier analysts if they feel that they cannot advance in their careers. Cyber security is one of the fastest growing industries and it is predicted that there will be a shortage of approximately two million professional worldwide by 2019 [47]. In addition to having good technical skills, a SOC analyst should be curious by nature and have a analytical mind-set [5, 88]. The cyber security field is constantly changing, so being curious and interested about the field is crucial.

A skilled SOC analyst must have a broad theoretical and practical knowledge of general IT infrastructure, that includes networking and security devices and protocols, servers and common operating systems like Microsoft's Windows, and Linux. In addition, the analysts should have knowledge of SIEM and log management systems, but this can also be trained. It is an advance, if a SOC analyst knowns the TTPs of the adversaries. These skills can be learned from penetration testing and red teaming.

Availability is extremely important in cybersecurity, as hackers and other adversaries do not solely work during business hours. If a SOC operates only on an 8/5 schedule (09:00 to 17:00 on Monday to Friday), being proactive is almost impossible. In this case actively defending the network can easily turn into incident response. Data breaches and cyber attacks can happen within minutes or hours, which makes it reasonable to consider running the SOC around the clock. Multinational organizations may run the using "follow the sun" model. In this model three security operations centers that are approximately 8 time-zones apart work during local business hours. [5, 65]. However, this type of model is not possible for smaller national organizations. In addition, a non-24/7 SOC unit must catch up with alerts from last night, which further increases the reaction times. A small SOC may resort to an automated response system, like Darktrace to fill in the gap during the night and the weekends. In addition, they can utilize an on-call SOC analyst that receives an automated alert when an urgent alert is raised.

5.6 Marathon Rather Than a Sprint

Building an effective and mature SOC takes time. SOC units consist of people, processes and technology and every single one of the components takes time to evolve. It is important to remember that every building block is equally important and should be considered from the very beginning. In a large organization with enough employees and funding the technical part is the fastest to implement. Training a SOC unit's worth of new employees takes a long time, as they must learn the underlaying technologies and processes. Even if the new employees are experienced in working in a SOC they must adapt the new tools. In many cases the tools contribute in building and shaping the processes. [5, 172]. For example, if the SIEM and UEBA are integrated, it decreases the number of different platforms that the SOC analysts must use while investigating an alert.

A SOC unit's main responsibility is to provide situational awareness of the security to the constituencies whether they are the same organization or third-party customers. Therefore, a SOC must be able to constantly mature which means that all three aspects people, processes and technology are always developing. A mature SOC does not necessarily mean that it is able to stop every single known adversary and threat. A mature SOC is capable of developing and adapting to changes.

6 Conclusion

The goal of this thesis was to research current security operations centers and to analyze how they can be further developed to meet the demands of the cyber security field. Reactive cyber defense is not sufficient anymore because the threats have become more sophisticated and can escalate into large-scale breaches in a short amount of time. This has forced SOC units to become more agile and proactive. At the same time, the SOC units are struggling with overwhelming amounts of data and unmanageable workloads. The transition from reactive to proactive defense requires changes in a SOC unit's technologies and processes.

To improve, SOC units must utilize new technologies such as machine learning and artificial intelligence to minimize the number of recurring events that must be analyzed manually. Some reactive defenses can be automated, but the organization should be aware of the risks. To become more proactive, SOC units collect and analyze cyber threat intelligence so that they can be aware of the current threat. The intelligence is analyzed using computer aided analytics engines, that distributes the analyzed information to different destinations. A modern SOC is agile and can adapt quickly to changes. The processes support a SOC unit's decision making rather than slows it down.

A SOC unit is a broad term and the implementations vary. This thesis did not include thorough analysis of products used by SOC units. The research can be continued by comparing products that are used by a modern SOC. For example, a research conducted on automated cyber threat intelligence systems and products would be highly beneficial. Research topics on SOC units are almost infinite, because the SOC units are continuously adapting new processes and technologies to improve their performance.

The results of this thesis can be used when designing and implementing a SOC unit. In addition, the information provided in this thesis can be used to further improve an existing SOC unit. The company that requested this thesis can use the results to improve their SOC unit's efficiency and detection capabilities. However, they will still need to compare the different products that are going to be used in the implementation. This thesis did not contain a separate product comparison because the results of the comparison can quickly become obsolete due to the technology's fast advancement.

References

1 ICS-CERT: Alert (IR-ALERT-H-16-056-01) - Cyber-Attack Against Ukrainian Critical Infrastructure: February 25, 2016. URL: https://ics-cert.us-cert.gov/alerts/IR-ALERT-H-16-056-01 Accessed 18.6.2018

2 Sandeep Bhatt, Pratyusa K. Manadhata, Loai Zomlot 2015: The Operational Role of Security Information and Event Management Systems. IEEE Security & Privacy (Volume: 12, Issue: 5, Sept.-Oct. 2014), p. 35-41

3 REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation): 4.5.2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679 Accessed 4.7.2018

4 Bromiley Matt 2017: The Show Must Go On! The 2017 SANS Incident Response Survey: 6.2017. URL: https://www.sans.org/reading-room/whitepapers/incident/show-on-2017-incident-response-survey-37815 Accessed 17.7.2018

5 Zimmerman, Carson 2014: Ten Strategies of a World-Class Cybersecurity Operations Center: 1.7.2014. MITRE Corporation

6 European Union Agency for Network and Information Security 2017: ENISA Threat Landscape Report 2017: 15.1.2018. ENISA

7 Sornalakshimi K. 2017: Detection of DoS attack and zero-day threat with SIEM. 2017 International Conference on Intelligent Computing and Control Systems (ICICCS), p. 1-7

8 Sekharan S. Sandeep, Kansasamy Kamalanathan 2017: Profiling SIEM Tools and Correlation Engines for Security Analytics. 2017 International Conference on Wireless Communications, Signal Processing and Networking (WiSPNET), p. 717-721

9 Gerhards R 2009: The Syslog Protocol: March 2009. IETF.

10 Micro Focus: ArcSight Enterprise Security Manager: 18.4.2018. URL: https://www.microfocus.com/media/flyer/arcsight_enterprise_security_manager_ds.pdf Accessed 3.7.2018

11 Bonilla Daniela 2017: Micro Focus Security ArcSight Common Event Format – Implementing ArcSight common Event Format (CEF) Version 25: 28.9.2017

12 Crawley Kim 2018: How SIEM Correlation Rules Work: 20.2.2018. URL: https://www.alienvault.com/blogs/security-essentials/how-siem-correlation-rules-work Accessed 24.7.2018 AlienVault

13 Viestintävirasto: Cyber security. URL: https://www.viestintavirasto.fi/en/cybersecurity.html Accessed 23.7.2018

14 Rapid7 LLC 2016: SOC Series: How to Make A Security Operations Center More Efficient: 6.12.2016. URL: https://blog.rapid7.com/2016/12/06/how-to-make-your-security-operations-center-more-efficient/ Accessed 25.7.2018

15 Palo Alto Networks 2017: Build A Next-Generation SOC: 13.3.2017

16 Krebs Brian 2017: U.K. Hospitals Hit in Widespread Ransomware Attack: May 12, 2017. Updated 13.5.2017. URL: https://krebsonsecurity.com/2017/05/u-k-hospitals-hit-in-widespread-ransomware-attack/ Accesses 19.7.2018

17 Thomas-Ungoed Jon, Henry Robin, Gadher Dipesh: Cyber-attack Guides Promoted on YouTube: 14.5.2017. URL: https://www.thetimes.co.uk/article/cyber-attack-guides-promoted-on-youtube-972s0hh2c Accessed 19.7.2018

18 Cyber Security Policy: Securing cyber resilience in health and care: Progress update October 2018: 11.10.2018. URL: https://www.gov.uk/government/publications/securing-cyber-resilience-in-health-and-care-october-2018-update Accessed 17.10.2018

19 Brotherston Lee, Berlin Amanda 2017: Defensive Security Handbook: Best Practises for Securing Infrastructure: 4.2017. O'Reilly Media

20 Lockheed Martin: The Cyber Kill Chain. URL: https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html Accessed 07.07.2018.

21 Shodan 2018: What is Shodan?: 28.5.2018. URL: https://help.shodan.io/the-basics/what-is-shodan Accessed 3.7.2018.

22 Rapid7 LLC: Metasploit Basics. URL: https://metasploit.help.rapid7.com/docs/getting-started Accessed 3.7.2018.

23 Gallagher Sean 2018: Threat or menace? "Autosploit" tool sparks fear of empowered "script kiddies": 1.2.2018. URL: https://arstechnica.com/information-technology/2018/02/threat-or-menace-autosploit-tool-sparks-fears-of-empowered-script-kiddies/ Accessed 3.7.2018

24 Del Carlo Corbin 2003: Intrusion Detection Evasion: How Attackers Get Past the Burglar Alarm: 25.9.2003. SANS Institute.

25 Brewster Thomas 2017: An NSA Cyber Weapon Might Be Behind A Massive Global Ransomware Outbreak: 12.5.2017. URL: https://www.forbes.com/sites/thomasbrewster/2017/05/12/nsa-exploit-used-by-wannacry-ransomware-in-global-explosion/#18cc790ae599 Accessed 1.11.2018

26 Talos Advisories: Talos Rules 2017-03-14 – Talos is aware of vulnerabilities affecting products from Microsoft Corporation: 14.3.2017. URL: https://www.snort.org/advisories/talos-rules-2017-03-14.html Accessed 3.11.2018

27 Cole Eric 2017: SOC Automation – Deliverance or Disaster: 12.2017. SANS Institute.

28 Darktrace: Darktrace Enterprise: Product Overview. URL: https://www.darktrace.com/resources/ds-core-and-tv.pdf Accessed 20.7.2018

29 Gandotra Ekta, Bansal Divya, Sofat Sanjeev 2016: Zero-Day Malware Detection: 15.12.2016. 2016 Sixth International Symposium on Embedded Computing and System Design (ISED), p. 171-175

30 Pathak Parag 2018: 5 Reasons AI is the Pillar of the Next-Gen SOC. 20.9.2018. Webinar.

31 Darktrace 2017: Darktrace Antigena Network – Autonomous Response to Cyber Threats – PRODUCT OVERVIEW. 2017

32 IBM: Frequently Asked Questiong – What is XFE? URL: https://exchange.xforce.ibmcloud.com/faq#what_is_xfe Accessed 1.11.2018

33 Carsten Casper 2016: Gartner Essentials: Top Cybersecurity Trends for 2016-2017: 28.4.2016. URL: https://www.slideshare.net/SBAResearch/gartner-essentials-top-cybersecuritytrends-for-20162017 Accessed 19.7.2018

34 MITRE corporation: STIX/TAXII Supporters List (Archive). URL: https://stixproject.github.io/supporters/ Accessed 13.8.2018

35 Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016: 7.2.2017. URL: https://www.gartner.com/newsroom/id/3598917 Accessed 12.6.2018.

36 Hilton Scott 2016: Dyn Analysis Summary Of Friday October 21 Attack: 27.10.2016. URL: https://dyn.com/blog/dyn-analyasis-summary-of-friday-october-21-attack/ Accessed 24.10.2018

37 Krebs Brian 2016: DDoS on Dyn Impacts Twitter, Spotify, Reddit: 21.10.2016. URL: https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/ Accessed 1.11.2018

38 Holik Filip, Horalek Josef, Marik Ondrej, Neradova Sona, Zitta Stanislav 2015: The deployment of Security Information and Event Management in cloud infrastructure. 2015 25th International Conference Radioelektronika (RADIOELEKTRONIKA), p. 399-404

39 Tenable Network Security: Nessus. URL: https://www.tenable.com/products/nessus/nessus-professional Accessed 20.7.2018

40 Forum of Incident Response and Security Teams (FIRST): Common Vulnerability Scoring System v.3.0: Specification Document. URL: https://www.first.org/cvss/specification-document Accessed 20.7.2018

41 Bussa Toby, Litan Avivah, Phillips Tricia 2016: Market Guide for User and Entity Behavior Analytics: 8.12.2016. URL: https://www.gartner.com/doc/reprints?id=1-3NLF0R6&ct=161209&st=sb Accessed 4.7.2018

42 Rapid7: InsightIDR – Detect stealthy behavior behind breaches. Get up and running in no time. URL: https://www.rapid7.com/products/insightidr/ Accessed 3.11.2018

43 Apache Hadoop 2018: What is Apache Hadoop? 13.6.2018. URL: https://hadoop.apache.org/ Accessed 30.7.2018

44 AlienVault 2017: How to Build a Security Operations Center (On a Budget). 6.11.2017. AlienVault

45 Hayes Kirk 2016: Penetration Test vs. Red Team Assessment: The Age Old Debate of Pirates vs. Ninjas Continues: 23.6.2016. URL: https://blog.rapid7.com/2016/06/23/penetration-testing-vs-red-teaming-the-age-old-debate-of-pirates-vs-ninja-continues/ Accessed 1.8.2018.

46 Zurus Kacy 2018: Does Your SOC Have a Security Playbook?: 8.10.2018. URL: https://securityintelligence.com/does-your-soc-have-a-security-playbook/ Accessed 3.11.2018

47 Kauflin Jeff 2017: The Fast-Growing Job with a Huge Skills Gap: Cyber Security: 16.3.2017. URL: https://www.forbes.com/sites/jeffkauflin/2017/03/16/the-fast-growing-job-with-a-huge-skills-gap-cyber-security/ Accessed 25.7.2018