Universiteit Leiden
Campus Den Haag

MASTER THESIS
ARTIFICIAL INTELLIGENCE SUPPORTING SECURITY OPERATIONS CENTERS

THESIS SUPERVISORS:
ASSISTANT PROFESSOR DR. FRANCIEN DECHESNE, LEIDEN UNIVERSITY
DR.IR. JAN VAN DER LUBBE, TECHNICAL UNIVERSITY DELFT

Author: Alex Kooistra

Version: 1.0 Final version

Date: December 26, 2019

Abstract

Security operations centers prevent, detect, and respond to security alerts and incidents. The ongoing digitalization and expansion of digital information pose a serious concern for security operations centers. This concern is whether or not security operations centers can process and analyze the multiple information from systems and devices to prevent and detect security alerts of incidents. This paper analyses using artificial intelligence within a security operations center to overcome this concern. In the analyses, the challenges of using artificial intelligence within an organization are taken into account. The theoretical possibilities, including the challenges, are compared against the current situation of Dutch governmental organizations. This results in a gap analysis that can support the organizations to identify the next steps to address the above-mentioned concern.

Acknowledgements

I would like to thank the Cyber Security Academy (CSA) for their multi-disciplinary view of cybersecurity. The integral approach of technical, legal and social scientific aspects has raised my understanding of cybersecurity and broadened my horizon. Where there was once chaos, there is now order. Many thanks to my lecturers and students for their thoughts, discussions, and insights.

It was a privilege to have both Francien Dechesne and Jan van der Lubbe as supervisors for my paper. The combination of Francien focusing on the structure & process and Jan providing valuable technical insight have contributed to the quality and finishing of the paper on time.

The paper would not have been possible without the support of the interviewees of Dutch governmental organizations. Thank you for contribution, openness, and insights into your organizations. I would also like to thank UWV for making it possible to pursue my quest for knowledge on cybersecurity and participating in this study.

Special thanks to fellow students of “42”. You know why. Finally, I would like to thank my family, my wife, and my kids. Your continuous support and faith, especially in my darkest hours, kept me going and brought me to where I am today.

Index

Table of Figures

1. Introduction

"Data is the new gold". This quote was made by Neelie Kroes at the press conference in Brussel on open data strategy in 2011 (Kroes, 2011). With the evolution of the digital era and the emerging fourth industrial revolution (Schwab, 2017), data is growing exponentially and is becoming more important. Based on the seventh edition of Data Never Sleeps (Domo, 2019), around 56.1% of the world population is connected to the internet with 40 times more bytes than there are stars in the observable universe. On average, every minute of the day there are 188 million email sent, 231.840 skype calls made, 18,1 million text messages sent, 511.200 twitter feeds, 277.777 Instagram posts, and 162.037 user transactions. This data is all shared, processed, and stored digitally. The organizations who are responsible for processing, sharing, and storing of digital information have a responsibility towards their clients to adequately secure and disclose the information. Sensitive information, like personal, political, or medical information, in the wrong hands can lead to serious concern for the individuals but also to the organizations. Criminal organizations, that steal sensitive information through hacking of systems, sell this sensitive information on the dark web for considerable money (Trend Micro, 2015). Securing the data and keeping the data private is a continuous process that requires situational awareness of the changing security landscape.

Security operations centers play an important role in respect to securing data within an organization. The main focus of a security operations center is to prevent, detect and respond to security alerts and incidents. Security operations centers rely on internal and external information sources to carry out their tasks. The information is processed and analyzed by the security operations center to make correct decisions. Analyzing the information sources can be time-consuming given the complexity of the information source, however correlation between different information sources is an even bigger challenge. Analyzing the combined information sources requires capabilities that are beyond the capabilities of a human being. Applications are available to support basic functionality concerning analyzing information sources however, given the amount and complexity of data sources new technologies such as machine learning and artificial intelligence open new opportunities.

With the rise of artificial intelligence, it is important to understand the impact of artificial intelligence on an organization and specifically the security operations center from multiple lenses. It is important to understand the pros and cons when using new technologies such as artificial intelligence.

1.1 Problem statement

The security operations center relies on information to prevent, detect, and respond to security alerts. The digital information including the metadata of the information is expanding rapidly given the digitalization, internet of things, and bring your own device. Specifically, the devices that are not controlled and maintained by the organization pose an additional security challenge. Additional measures like onboarding is required to avoid potential malware from the individual devices. More and more digital data is available for a security operations center to digest. For humans, it is almost impossible to handle all the information and make sense of it. Computers can analyze large amounts of information based on predetermined use cases. These predetermined use cases are configured by humans and processed by machines. Examples of use cases are three failed user log-on attempts, downloading a large number of documents within a certain time window or malicious traffic outside office hours. Computers can carry out these tasks faster, more efficient, and effective than humans. Combining different information sources adds to the complexity and as a result, it is almost impossible to comprehend from a human perspective.

1.2 Conceptual context / Scope

Commercial organizations have an incentive to secure their environment and protect their intellectual property. Failure to secure their environment of protect their intellectual property will affect the stock price or the organization's reputation. Government organizations do not have such an incentive. Most of these government organizations have a monopoly and have different incentives. Also, the budgets are determined centrally by the Dutch government and priorities need to be made given the workload of the Dutch governmental organization. Given the monopoly Dutch citizens rely on these Dutch governmental organizations to carry out their tasks adequately as there is no alternative.
In the selection of governmental organizations for this paper the following aspects are taken into consideration: size of the organization, in-house security operations center, centrally organized, and relevance towards the Dutch citizens. Based on the selection the Dutch tax administration, UWV, Sociale VerzekeringsBank, Rijkswaterstaat, and Department of Justice and Security are interviewed.

1.3 Research questions

Given the problem statement that security operations center need to process and analyze a large number of information sources, the main research question of this thesis is:

To what extent can artificial intelligence take over human activities in a security operation center?

To answer the main question a better understanding is required of the concept of artificial intelligence and security operations center models. Based on the capabilities of artificial intelligence a mapping can be made on the tasks and activities of a security operations center. Also important is to have an understanding of the side effects when implementing artificial intelligence in a security operations center.

The sub-questions that need to be addressed to answer the main question are:

1) What is a Security Operations Center?
2) What is Artificial Intelligence?
3) How can artificial intelligence support security operations centers in carrying out their tasks and activities more efficient and effective?
    a) What are the considerations, both from a technical and organization perspective, of artificial intelligence applied in security operations centers?
        i) What are the limitations?
        ii) How can we overcome them?
4) Dutch governmental organizations; its security operations center and position on artificial intelligence.
5) Gap analysis. Possibilities of artificial intelligence applied in security operations center at Dutch governmental organizations

1.4 Research approach & methods

In this paper, the concepts security operations center and artificial intelligence is analyzed using existing literature. Analyzing the concepts security operations center and artificial intelligence lead to the answering the first two sub-questions of this paper. Based on the literature of these concepts the sub-questions 3 and 4 can be answered. This analysis of whether or not artificial intelligence can support security operations center activities is based on qualitative analyses. By inductive reasoning based on literature possibilities, the extent of artificial intelligence supporting security operations center is answered. These results will be

challenged by interviews that are held at Dutch governmental organizations. The results of the interviews will be interpreted by the author and compared with the theoretical analyses to indicate the gap between what is possible based on a literature study and what is applied. The data used for this thesis is primarily a literature study and multiple interviews with Dutch governmental organizations

The outline of the paper follows the method described above. In the next two chapters, the concepts security operations center and artificial intelligence are discussed. Based on existing literature the purpose of a security operations center, its responsibility and goals are presented. In the second chapter artificial intelligence is analyzed keeping the context of a security operations center in mind. There are many perceptions of artificial intelligence so there is no single truth. By pealing down its capabilities this provides insight into how artificial intelligence can perform certain security operations center activities. In the third chapter, the gap analysis is performed to understand to what extent artificial intelligence can support security operations center. This gap analysis is done through literature analysis. The fourth chapter describes the current situation of the security operations center and the position of artificial intelligence from the Dutch governmental organization. The fifth chapter compares the theoretical possibilities of artificial intelligence with the actual situation of the Dutch governmental organization. This gap analysis provides insight for the Dutch governmental organizations how they become more efficient and effective using artificial intelligence.

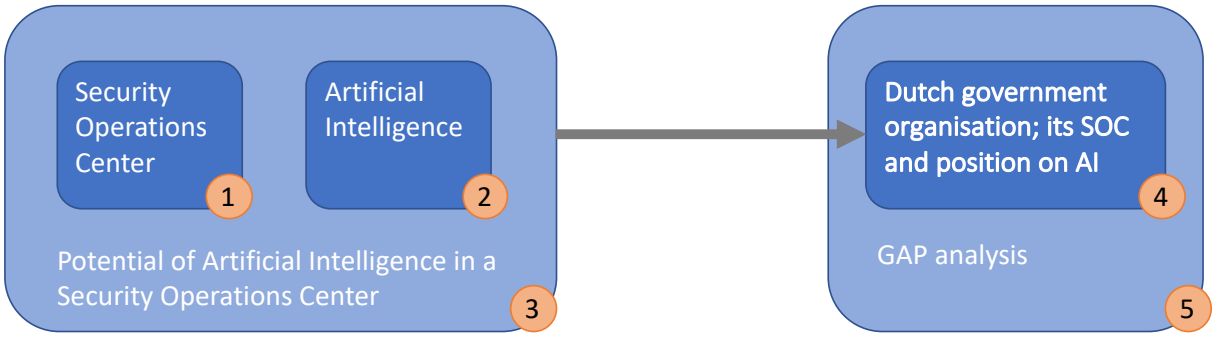

Figure 1. Conceptual model

2 Security operations Center

Data is growing exponentially (Domo, 2019; Hewlett Packard Enterprise, 2017) and is becoming more important. As stated in the introduction the amount of data in the digital domain every minute of the day is enormous. Data can be anything from a message of Facebook, personal health information, social security or financial information, to membership information. Securing this data is of utmost importance. A posting on Facebook or Instagram might not be so interesting due to the limited amount of sensitive information shared, however health, financial or social security information is. Exposing this sensitive information broadly could lead to serious negative effects on individuals. In case of health information, a person could be rejected for a life insurance policy of pay a higher premium due to his known condition. Criminals have made a business model to steal personal information and resell this personal information on black markets (Trend Micro, 2015). Depending on the sort of personal data this can vary between a few euros for address details and hundreds of euros for sensitive information like passports or electronic health records. Given the importance of data is it not uncommon for organizations to be hacked or breached. Major security breaches are reported from the early 2000s and include respectable organizations like AOL, Yahoo, Sony, and Target Marriott International (Hosting Tribunal, 2019). Most of the breaches, however, have taken place within the last few years according to the report. In the Netherlands, the number of data breaches have doubled every year since 2016 (Autoriteit Persoonsgegevens, n.d.). The doubling of breaches every year is closely related to new legislation that mandates by law, wet meldplicht datalekken (Ministerie van Veiligheid en Justitie, 2015) and the general data protection regulation (Europees Parlement, Raad van de Europese Unie, 2016), that organizations have to report data breaches to the authorities.

The security operations centers play a crucial role for managing these security risks and incidents. Its primary goal is to prevent, detect and responds to security alerts and incidents.

In the following paragraphs, a closer look is taken at the security operations center. This starts with a literature review on the history and background of a security operations center. What led to the introduction of a security operations center and which steps have been taken since? The following paragraph looks at the goals of a security operations center followed by the functional domains within a security operations center. In the last paragraph, the challenges of a security operations center are discussed.

2.1 Literature review

The first-generation security operation centers date back from the early days of the internet. The first security components were antivirus and firewall. The security operation center, typically a single person back in those days was responsible for monitoring these components and in case of possible threats or incidents act accordingly. Over the years the security operation centers have evolved to what is currently known as the fifth-generation with a focus on analysis on large data sets. Including in this focus is the business context to understand enterprise risks (Hewlett Packard, 2013).

The report by Hewlett Packard (2013) provides valuable information on the focus of a Security operation center however it does not provide insight into how security operation centers should be organized. Security vendors like IBM (Meenan & Laurens, 2015), HP (Hoffmann, 2014) and Ernst & Young (2014) have published presentations and whitepapers with respect to best practices for designing and implementing security operation centers. These publications are to a certain extent subjective because of self-promoting of products

and services. This conclusion is also stated by Van Os (Van Os, 2016) is his research paper with respect to measuring capability maturity in security operations centers.

Research papers on security operations centers are limited in numbers and depending on the author from a different perspective. The research paper written by Michail (2015) provides a broad overview of the goals and functional domain for a security operations center. The functional domains listed in the research paper are also discussed in the paper by Schinagl, Schoon, & Paans (2015) and Jacobs e.a. (2013) and described in more detail in the next paragraph. The research paper by Kelly & Moritz (2006) discusses the best practices of a security operations center and are to a large extent similar to the goals mentioned in the paper by Michail (2015).

An interesting observation by Hoffman (2014, p. 5) is with respect to the scope of the security operations center. In the beginning, the focus of a security operations center is on securing the perimeter, over time the focus of a security operations center shifted towards securing the applications and finally into securing the business.

In the following paragraphs, the goals and functional domains are described in more detail.

2.2 Main goals of a SOC.

The main goals of a security operations center mentioned in the research papers by Kelly & Moritz (2006) and Michail (2015) are:

2.2.1.1 Situational Awareness

Organizations require real-time visibility on the status of their infrastructure. By aggregation and correlating data logs from the network devices, the security operations center is aware of what is and when it is happening to determine whether or not this is normal behavior. Analysis done by the security operations center lead to predictions that support the security operations center to make the rights decisions at the right time.

2.2.1.2 Risk & downtime reduction

Security is all about risks. Managing these cyber security risks is an essential task for a security operations center. Risks can manifest itself into security incidents if the security risk in not addressed in time. A simple example is patch management. Should an organization fall behind in patching its systems this poses a risk on the organization. In case weaknesses as a result of not patching systems are exploited, this leads to security incident, if not it remains a security risk. Security incident should be avoided or in case it does happen should be restored instantly. To avoid security risks, an organization should have a risk management process in place that balances the security risk against the risk appetite of the organization. Should a security incident manifest itself it is important to have an incident response team and business continuity plans. Business continuity plan should include playbooks for major security incidents and a governance structure with roles & responsibilities

2.2.1.3 Threat control and/or prevention

The threat landscape is constantly changing and depending on the actual state of the landscape certain threats need to be contained or prevented. Organizations like European Agency for Cybersecurity and Nationaal Cyber Security Centrum provide yearly reports on the threat level landscape (ENISA, 2019; Nationaal Cyber Security Centrum, 2019). The earlier the threat can be identified by means of the “kill-chain” model the less impact the threat actually has on an organization (Hutchins, Cloppert, & Amin, 2011).

2.2.1.4 Diminishing administrative overhead

The amount of data collected by the security operations center is enormous. This data needs to be analyzed and correlated before it has actual meaning to the organization. Visualization of meaningful data helps for security operations center employees to make the right decisions. Important is that the right information is available at the right time to minimize administrative overhead.

2.2.1.5 Forensic capabilities

When threats manifest itself into security incidents, it is important to understand how this security incident could have happened and even more important how this can be prevented in the future. This forensic investigation, through digesting log files of infected systems, leads to the root cause of the threat or security incident. By understanding the root cause preventive measures can be taken to avoid similar threats or security incidents in the future.

2.2.1.6 Audit & Compliance support

Organizations have an obligation either by law or local government to be compliant with regulatory standards. Dutch Government organizations have to comply with regulatory standards like the Baseline Informatiebeveiliging Rijksoverheid, Baseline Informatiebeveiliging Overheid, DigiD, and Structuur Uitvoering Werk en Inkomen. The security operations center helps to provide security information to prove that organizations are compliant with the regulatory standards.

2.3 Functional domains of a security operations center

In the literature of Michail (2015), Schinagl, Schoon, & Paans (2015) and Jacobs e.a. (2013) the responsibilities of a security operations center are clustered by domain. These main focus areas are called functional domains. Depending on how an organization is organized different responsibilities and activities are part of the security operations center.

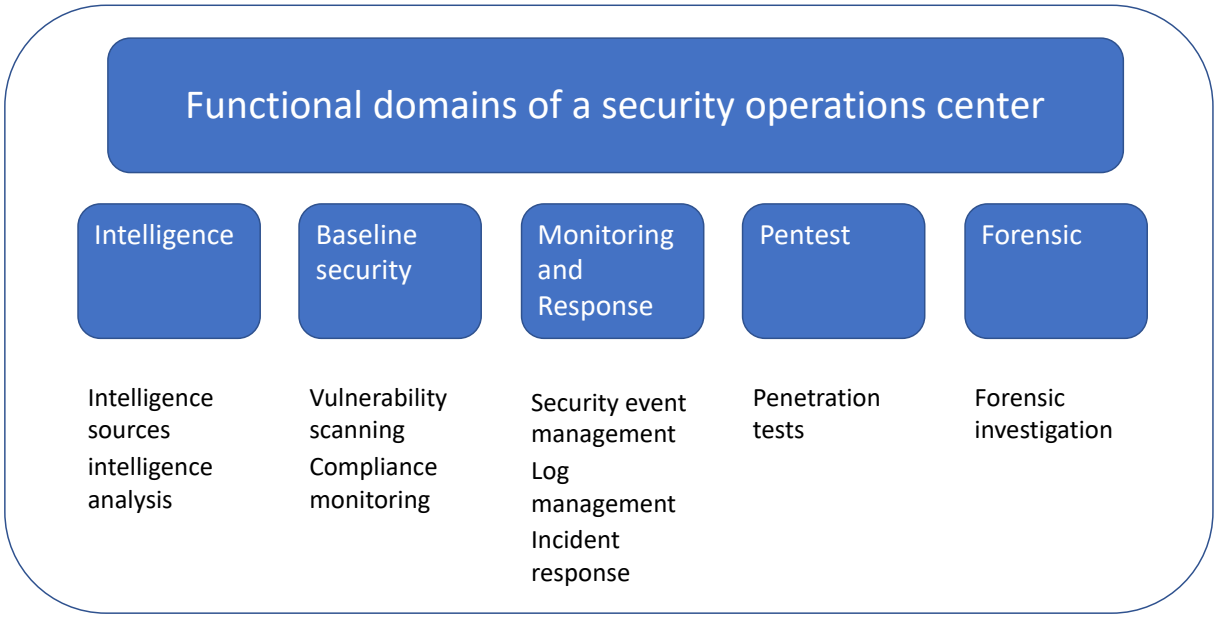

Figure 2. Functional domains of a security operations center based on literature by Michail (2015) and Schinagl et al (2015)

2.3.1.1 Intelligence function

The intelligence function is at the core of the security operations center. In this domain, the decisions are made on how to proceed given any threat or security incident. The intelligence domain is dependent on the security information it receives from either internal monitoring

feeds, baseline reports or external threat reports. Analyses of threats and security incidents are performed in this domain.

2.3.1.2 Baseline security

Compliance and vulnerability checks are essential to avoid security incidents. Awareness of the security deciations based on compliance and vulnerability checks of your ICT landscape is essential. Deviancies are reported for further action by the intelligence team.

2.3.1.3 Monitoring and response

Monitoring your ICT landscape provide insights into the traffic patterns inside your network. By understanding the traffic flows and the system behaviors within your network anomalies can easily be detected and potential threats can be eliminated early in the process. Organizations use Security Incident & Event Management tooling to collect all the traffic patterns and log data from ICT systems.

2.3.1.4 Pentest

Penetration testing is often used in an organization to understand the security vulnerabilities within a given system. Penetration testing is done as part of the development process to avoid security vulnerabilities in live systems, however, live systems are also tested as new threats and vulnerabilities emerge.

2.3.1.5 Forensic investigation

Forensic investigation is done in cases where there has been a major security incident that requires detailed investigation into the root cause and the threat actor. Forensic evidence should be secured properly should this information be shared with local authorities. These investigators support the local authorities by providing them evidence such as log files, hashed hard drives, etc.

2.4 People, process, and technology perspective

Achieving the goals of a security operations center given the functional domains requires people, processes, and technology. This model has similarities with the 3 layer model of Jan van der Berg (2018) in which these layers are describes as the technical, social-technical, and governance layer. In the next paragraphs, these perspectives are discussed in more detail.

2.4.1.1 People

It is often claimed that people make a difference in a security operations center (Kuiper et al., 2017). The human is able provide to context to decision making when reacting on alerts or incidents. Depending on the responsibilities of a security operations center the number of employees differs, however, most security operations center have security analysts and a security operations center manager. Depending on the tasks and activities carried out by the security analyst the level of expertise is different. (Exabeam, 2019; Torres, 2015).

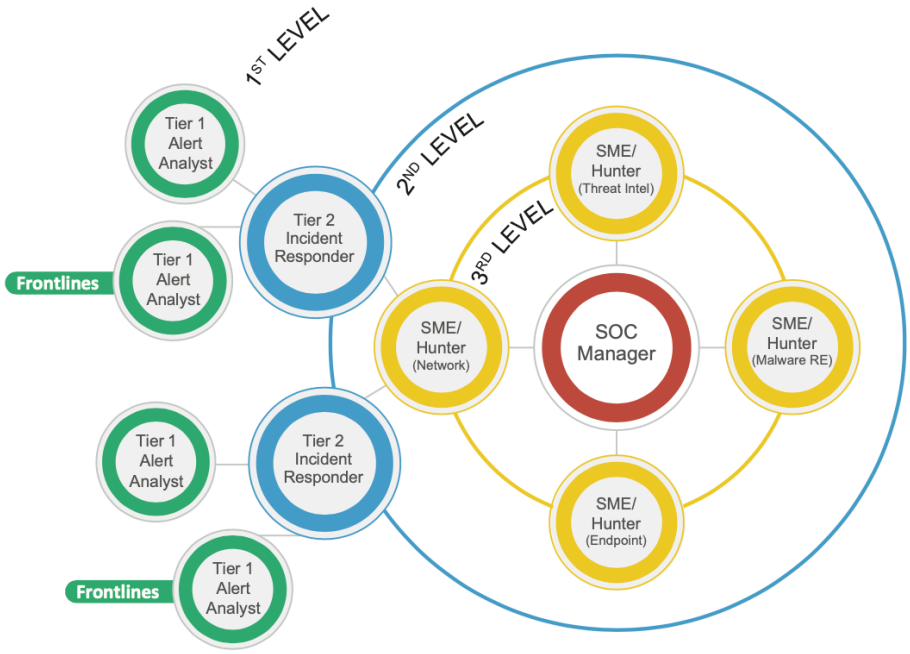

Figure 3. Functions in a security operations center (adapted from ((Torres, 2015, p. 5)):

Security operations center manager. The security operations center manager is ultimately responsible for the security operations center and manages the employees in his team. He/she is also the linking pin to higher management.

Level of security analysts:
Security analyst level 1. The security analyst level 1 is responsible for monitoring the infrastructure and systems of an organization. Reacting to alerts, carrying out triages on the alerts and providing the security analyst level 2 with the relevant security information to further investigate.
Security analyst level 2. The security analyst level 2 is responsible for analyzing incidents based on the various security feeds. Correlating the information and taking action accordingly to remediate or potentially avoid any further impact to the organization.
Security analyst level 3. The security analyst level 3 is also known as the subject matter expert. This person has deep knowledge on a specific focus area, such as threat intelligence or malware. Its primary goal is to prevent incidents by pro-actively taking action. Also, the security analyst level 3 provides expert support to a security level 2 analyst upon request.

2.4.1.2 Process

In the literature, there are many different views on the processes of a security operations center. According to a white paper by Escal Institute of Advanced Technologies (Torres, 2015), the processes within a security operations center are focused on the incident response process models of the Computer Incident Advisory Capability of the Department of Energy and the NIST SP800-61 Revision 2, “Computer Security Incident Handling Guide” (Cichonski, Millar, Scarfone, & Grance, 2013). Other publications go beyond the incident processes and include other processes like compliance, metrics, and on-boarding of applications and/or systems (ArcSight, 2010; Hoffmann, 2014). The processes on top of the security incident response processes are at the discretion of the organization and depending on the responsibilities.

2.4.1.3 Technology

Effective security operations centers have at the core of their operation a monitoring solution. This monitoring solution is capable of collecting, detecting, aggregating, and analyzing log data from the various systems. This includes but not limited to systems like network devices, firewalls, mail filters, antivirus, intrusion detection systems, intrusion prevention systems, proxy services, and business applications. The monitoring system used by most security operations center is called a Security Information & Event Management system (Swift, 2007).

2.5 Challenges of a security operations center

Security operations centers are under constant pressure to secure their organizations and prevent security incidents. This is not an easy task given that any weakness within an organization can lead to security incidents. The main challenges (Crowley & Pescatore, 2019; Help Net Security, 2018; Tillyard, 2018) that security operations center face nowadays are:

1) Handling the Increasing volumes of security alerts. With the expansion of new systems and devices within an organization, the volumes of (log) information that require analysis, triage, and follow up is growing constantly. Are security analysts able to keep up with the growing number of security alerts and more important are they focusing on the real security alerts and threat.
2) Different technology. The security operations centers have a broad responsibility as described as part of the functional domains. All these domains have their own systems and tools. These systems and tools help to automate tasks and become more productive however also require the security operations center to maintain, train for, and work with multiple different systems and tooling.
3) People. In the security industry, there is a shortage of skilled personnel. The demand for educated people is higher than there are people available. Also, it is more difficult to get educated in the security domain. This requires years of education, training, and experience.
4) Budgets. How much is an organization willing to spent on security? There is no such thing as 100% secure, therefore the question remains how much risk is organization willing to take. What is the risk posture?

The challenges of a security operations center have a direct relation with the people, process, and technology perspectives described in the previous sub-chapter.

2.6 Summary

Literature on security operations centers is limited. Over the last decade only a limited amount of papers has been produced on security operations centers. Most of the information available on security operations centers is based on best practices and security vendor blogs & presentations. Research papers on security operations center are limited. Based on the information available the overview in the figure below provides the reader with an overview of the security operations center goals, its functional domains, and the related people, processes, and technology.

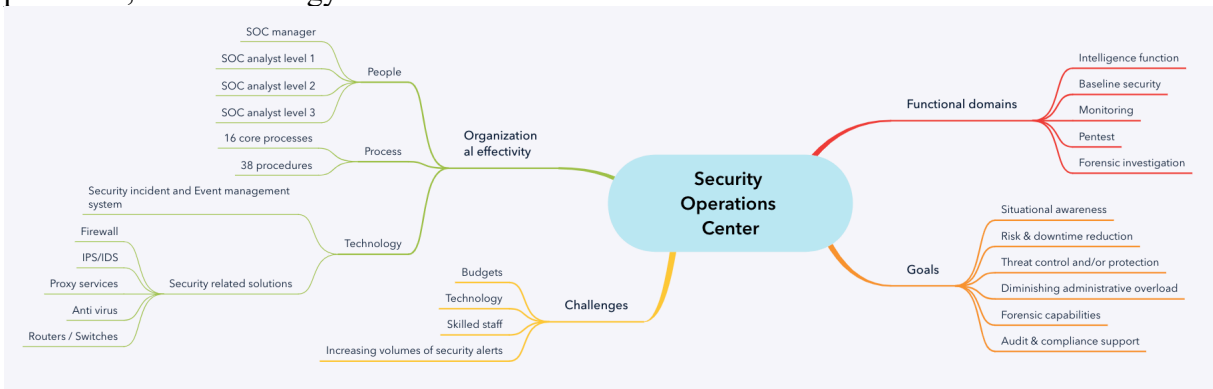

Figure 4. Security operations center overview

The challenges for skilled staff and the increasing volumes of security alerts endorse the main question of this paper. Is artificial intelligence able to contribute and support security operations center to perform their tasks more effectively and efficiently? The functional domains of a security operations center provide a good overview of the responsibilities of a security operations center for further analyses with respect to artificial intelligence. In the next chapter artificial intelligence is discussed in more detail.

3 Artificial intelligence

This chapter describes the topic of artificial intelligence. Through literature study, the sub-question "what is artificial intelligence" in respect to this paper is given. Many articles are written and much research is performed on the subject of artificial intelligence. The authors each have their own perception and definition on artificial intelligence. The most common used general definitions of artificial intelligence are: 1) the definition by the US government in the report Preparing for the Future of Artificial Intelligence (Felton, 2016): *"Artificial intelligence is a computerised system that exhibits behaviour that is commonly thought of as requiring intelligence."*, 2) the definition in the book The Thinking computer: Mind inside matter by Bertram Raphael (1976): *"Artificial Intelligence is the science of making machines do things that would require intelligence if done by man."*, and 3) the definition of the founding father of artificial intelligence Alan Turing (2004): *"Artificial Intelligence is the science of making machines do things that would require intelligence if done by man."*

In the first paragraph is a literature study on artificial intelligence. This includes the history of artificial intelligence and its capabilities. How is artificial intelligence classified and what types of artificial intelligence are available. The next paragraph discusses the limitations of artificial intelligence and concluded with a summary.

3.1 Literature background

Artificial intelligence is capable of performing human tasks more effective and faster. Tradition problems like planning, learning, perception, logic decision making, communicating, and acting that previously were only performed by humans are now also performed by artificial intelligence (Russell & Norvig, 2002). The capabilities, perceiving, learning, abstracting and reasoning of artificial intelligence have increased over the years as the technology of artificial intelligence has grown from solving narrowly defined problems, via nuanced classifications & predictions, to learning, reasoning & adapting to new situations (Kaplan & Haenlein, 2019; Prabhakar, 2017).

Artificial intelligence systems are characterized by databases, rulesets, and a control system according to Nilsson (2014). The database is the central data structure, the ruleset is the database instructions and the control system instructs the system to apply a ruleset on the database. The example used by Nilsson is the "8-Puzzle". Artificial intelligence is able to solve the puzzle using the four elements; 1) initial state, 2) state space, 3) a goal test, and 4) a path cost (Chopra, 2012).

3.1.1 History of artificial intelligence

The notion of artificial intelligence was first introduced middle of last century with the idea that a machine could be as intelligent as a human being. John McCarthy and Alan Turing are considered the founding fathers of artificial intelligence. Following this idea of artificial intelligence, much research is conducted on the concept of artificial intelligence. With the rise of computers in the 70ties, "Natural Language Processing" became of on the branches of artificial intelligence. Shortly after other branches of artificial intelligence like deep learning techniques and neural networks were introduced. The pace in which artificial intelligence is developing has an impact on the society and the possibilities for humans.

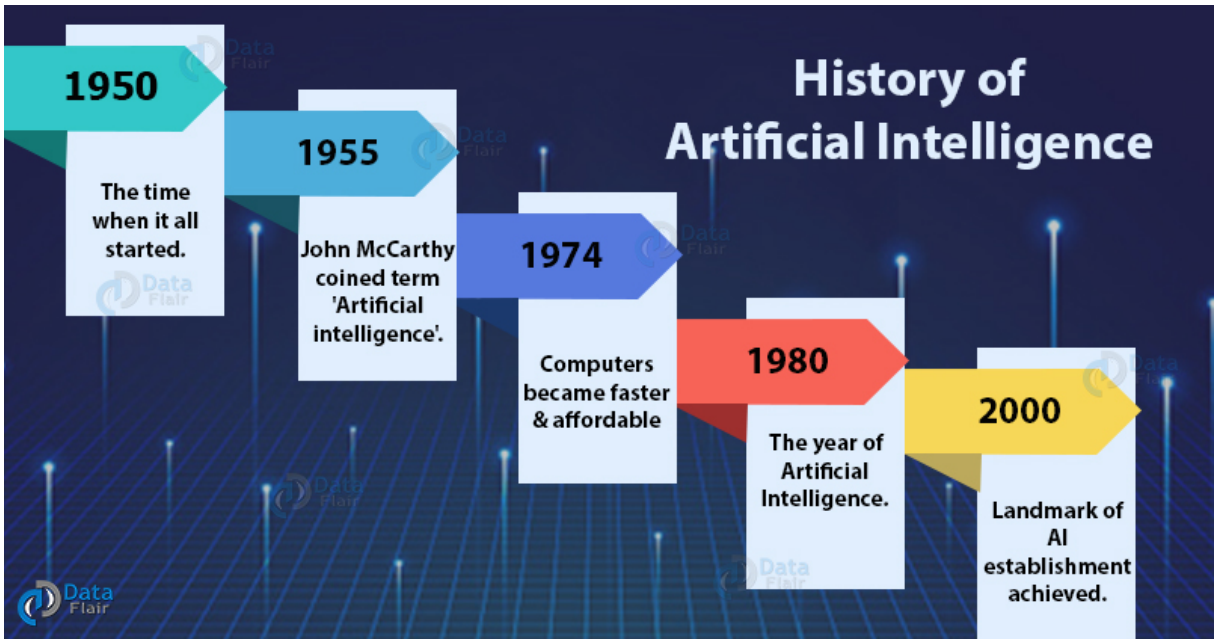

Figure 5. History of artificial intelligence (adapted from (Dataflair team, 2019)

3.1.2 Phases of artificial intelligence

In the very beginning, it started with a simple ruleset based algorithm to nowadays self-learning algorithms capable of understanding, learning and adapting. The three distinguished phases are according to Prabhakar (2017) are:

Handcraft knowledge.

The first capabilities of artificial intelligence were to represent knowledge based on a rule set in well-defined domains. Artificial intelligence was all about perceiving information and reasoning, decision making. Artificial intelligence at this stage was not able to learn or create context based on the information received. Typical examples are planning tools, automated response forms, and early monitoring tools for cybersecurity.

Statistical learning

The second phase of artificial intelligence is based on statistical learning. Artificial intelligence is able to perceive information and learn from the information however is only partially able to create context based on the information and make decisions accordingly. Examples are virtual assistants, text analyses software, image recognition and AlphaGo.

Contextual adaption

The third phase of artificial intelligence is based on contextual adaption. Artificial intelligence is able to perceive and learn from the information presented and make decisions accordingly. Artificial intelligence is also, to a certain extent, able to include context and therefore able to incorporate new tasks and situations. The challenge remains how artificial intelligence communicates between machines and people. Examples of this third wave artificial intelligence are autonomous robots and self-driving cars.

3.1.3 Classification of artificial intelligence systems

Artificial intelligence systems can be classified into three different groups depending on their characteristics according to Kaplan & Hainlein (2019). The most commonly known is the analytical artificial intelligence that generates a cognitive representation based on past experience to predict the future. Typical examples of such artificial intelligence systems are fraud detection, anomaly detection, image recognition, and self-driving cars. The second is human inspired artificial intelligence that includes next to the cognitive intelligence also emotional intelligence. By understanding human emotions, artificial intelligence systems are

able to better predict and make adequate decisions. These types of artificial intelligence systems are used by the HR department when recruiting new employees. An example of human-inspired artificial intelligence is the robot Kismet (Breazeal, n.d.) The third type of artificial intelligence system is humanized artificial intelligence. Humanized artificial intelligence includes not only cognitive and emotional intelligence but also social intelligence like empathy, teamwork and leadership. This would make the artificial intelligence system self-conscious and self-aware. To this date, there are no known examples of a humanized artificial intelligence system.

3.1.4 Focus areas of artificial intelligence

Artificial intelligence can be applied broadly depending on the field of expertise. Today artificial intelligence is mostly applied in one or more areas, combining all of the areas and including the capabilities of self-conscious and self-aware is perhaps the ultimate goal. The overview of the focus areas of artificial intelligence is discussed in many articles and blogs (Granage, 2019; Kumar, 2018; Mellett, 2017).

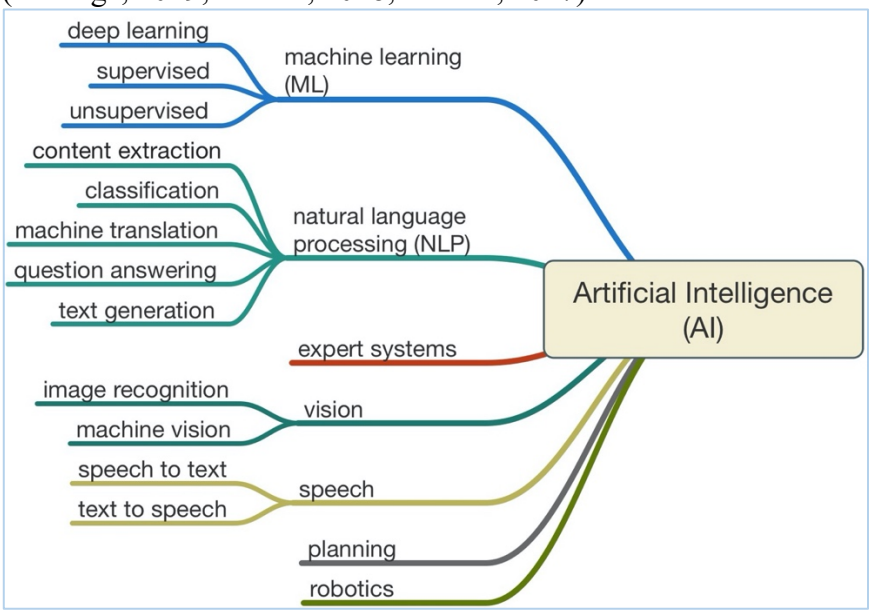

Figure 6. Focus areas of artificial intelligence (adapted from (Kumar, 2018))

An important factor of artificial intelligence is its learning capabilities. There are three main learning processes: 1) supervised learning, 2) unsupervised learning, and 3) reinforcement learning. All these learning processes are part of machine learning and build a mathematical model based on sampling data.

3.1.4.1 Supervised learning

Supervised learning is characterized as learning using a large data set that contains both the desired input and output. By labeling the training data set with the desired outcome, the system is able to differentiate between a correct and incorrect sample. The larger the data set the better the algorithm. This type of learning is task-driven and focusses on regression & classification. Supervised machine learning is considered time-, cost-, and resource consuming. (Litjens et al., 2017). Examples of supervised learning are image classification and email spam filters.

3.1.4.2 Unsupervised learning

Unsupervised learning is unlike supervised learning only characterized by the input data set and not the output. The algorithm, therefore, does not have any reference material to compare the input to the output and therefore the outcome is derived from the algorithm itself. Given the outcome is based on the algorithm it is not possible to check if the output is correct and users become more dependent on the reliability of the algorithm. This type of learning is used to find structure in data by clustering data points. By discovering patterns in the data, the algorithm is able to group the input data set into categories. This type of learning is used for speech or face recognition.

3.1.4.3 Reinforcement learning

Reinforcement learning is characterized as a goal-oriented algorithm. This type of learning interacts with the environment and takes decisions accordingly. This feedback loop, reward, is called the reinforcement signal. The algorithm learns based on the reinforcement signal to maximize his objective or goal. Unlike supervised learning, the outcome is not always correct and the outcome of the algorithm is based on its own experience of the environment. This type of learning is used for autonomous vehicles.

3.2 Considerations when using artificial intelligence

In this sub-chapter, the considerations are discussed for artificial intelligence. The considerations are divided into two categories. The first category is related to the technology of artificial intelligence and the second category is related to the organizational implications.

3.2.1 Artificial intelligence technology considerations

In the subparagraphs below the technology considerations for artificial intelligence are discussed. The technology considerations are:

3.2.1.1 Data set

Artificial intelligence systems are trained using sampling data. The saying “Garbage in is garbage out” (“GIGO (Garbage In, Garbage Out) Definition,” n.d.) is true when working with artificial intelligence systems. Picking the right sampling data set is essential for artificial intelligence systems to function properly. In general, it is stated that a larger data sampling set leads to better learning performances of the artificial intelligence algorithm. Smaller sampling sets are more prone to overfitting than large sampling sets (Jabbar & Khan, 2014). In case of overfitting too many parameters are taken into account which leads to noise within the training sampling set. Underfitting, in contrast to overfitting, occurs when the underlying parameters and structure of the training data set are not captured properly. Data poisoning is an example where malicious actors deliberately feed the learning model with malicious data to corrupt artificial intelligence systems (Steinhardt, Koh, & Liang, 2017).

3.2.1.2 Bias

Bias is disproportionate weight in favor of or against an idea or thing (“Bias,” 2019). Bias is typically associated with biased training data, however, there are other aspects that can also lead to bias of artificial intelligence systems. Framing the problem requires the scientist to decide what they would like to achieve. This goal needs to be translated into language artificial intelligence systems understand. This translation, if not done correctly, can lead to a slightly different goal, therefore, creating a bias artificial intelligence system. Another aspect that can lead to bias of artificial intelligence systems is a wrongly prepared data set. This is related to the attribution of data sets that the artificial intelligence algorithm needs to consider.

Although artificial intelligence systems are not configured to be biased, in practice some artificial intelligence systems do experience bias behavior. Based on an article from AI Business (Smolaks, 2019) there are three historical cases in which artificial intelligence systems led to biased behavior. These cases are 1) Compas, 2) Any NLP model pre-trained naïvely on Common Crawl, Google News, or any other corpus, since Word2Vec, and 3) Allegheny Family Screening Tool.

3.2.1.3 Specific task

Artificial intelligence systems are designed for a specific task. Different tasks require different artificial intelligence systems. Within this specific task, the artificial intelligence system is capable of self-learning, however, this self-learning does not transcend its primary task. To this date, there is no knowledge of self-learning artificial intelligence systems like a human being with capabilities such as self-conscious and self-aware.

3.2.1.4 Context

Artificial intelligence systems have difficulties factoring in contextual information. As indicated artificial intelligence is designed for a specific task and therefore cannot take into account the environment. The business context is difficult to factor into the algorithm.

3.2.2 Organizational artificial intelligence considerations

In the previous subparagraph, the technology considerations of artificial intelligence are discussed. Adopting and integrating artificial intelligence into an organization also requires additional considerations. These considerations are:

3.2.2.1 Trust in artificial intelligence systems

Understanding the logic of artificial intelligence systems and its algorithms are difficult and depending on the complexity sometimes impossible. The artificial intelligence system itself is considered a black box as it is nearly impossible to explain the outcome of the black box given the input variables, particularly in combination with self-learning.
Trusting an artificial intelligence system is related to three aspects: 1) predictability, 2) dependability, and 3) faith (Rempel, Holmes, & Zanna, 1985). Gaining and maintaining trust in artificial intelligence systems requires time and patience. Above mentioned criteria play an important role in gaining and maintaining trust. Losing trust in artificial intelligence systems however is far easier as the negative impact is more visible and draws more attention than building a sustainable trust level over time (Slovic, 1993).

3.2.2.2 Accountability

Artificial intelligence is a new phenomenon with endless possibilities. Social media platforms already integrated artificial intelligence into the core of their systems and applications. Integrating artificial intelligence into the core of the systems and application does raise the questions who is accountable when artificial intelligence cause harm. The accountability gap needs to be addressed, specifically because our legal system is built on human actors and not artificial intelligence actors. Important factors to take into account with accountability are causality, justice, and compensation.
The UK government recently published a white paper called online harms (Department for Digital, Culture, Media & Sport, 2019). In this paper, the UK government addresses the accountability gap from a global perspective with plans on how to address accountability and oversights for tech organizations in the social media industry. Similar to in the social media industry other industries, like the car and medical industry, are raising similar concerns.

This accountability gap is addressed in the general data protection regulation (Europees Parlement, Raad van de Europese Unie, 2016) under article 22 "Automated individual decision making, including profiling". Art 22 states "The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her."

3.2.2.3 Strategy and policies

A corporate strategy on artificial intelligence is essential for an organization. Corporate strategies are guidelines for an organization on how goals can be achieved. This includes aspects related to resources and solutions. The corporate strategy should be translated into a clear roadmap and policies for the organization.
Corporate strategies are derived from the governmental rules, regulations, and guidelines on artificial intelligence. The Dutch government recently published its action plan with respect to artificial intelligence (Ministerie van Algemene Zaken, 2019). The Netherlands is not an early adaptor of artificial intelligence given the position other of European countries. Based on the publication by the European Union (Craglia et al., 2018) the front runners on artificial intelligence are United Kingdom, France, and Finland.

3.2.2.4 Strategic human resources plan

Artificial intelligence is a relatively new technology. To fully understand the potential of artificial intelligence constant education and training required. Organizations embracing artificial intelligence need to re-educate their employees on how to work with artificial intelligence. In a report by Gartner, it is stated that employee skills are the number one challenge to overcome. Employees simply mimicking the results of the artificial intelligence system is not sufficient. Employees should understand the basics of artificial intelligence to reproduce how artificial intelligence systems reached the results. The basics include an understanding of the data set, algorithm, and ruleset used.
Next to the employees that require additional education, it is also important that the people who are affected by the outcome of the artificial intelligence systems are educated or at least informed. This is closely related to the topic of trust, people affected by the results of the artificial intelligence system are more likely to accept results if the transparency of the artificial intelligence system is given.

3.3 Summary

Artificial intelligence has been around some time now. The early discussions on artificial intelligence date back to mid-1900. Not until early 2000, the first applications of artificial intelligence came into play. One of the first real examples of artificial intelligence is the deep blue computer. This computer was able to beat the grandmaster in a game of chess. Nowadays the number of areas where artificial intelligence could potentially play a significant role has grown exponentially. Recent applications being self-driving cars and human-like robots. The upcoming challenge for artificial intelligence is to include emotional and social intelligence into the systems, so it becomes self-aware and self-conscious.

The focus areas and its learning capabilities are used as a reference to determine to what extent artificial intelligence can take over human activities in a security operations center. In the next chapter, this is analyzed and discussed.

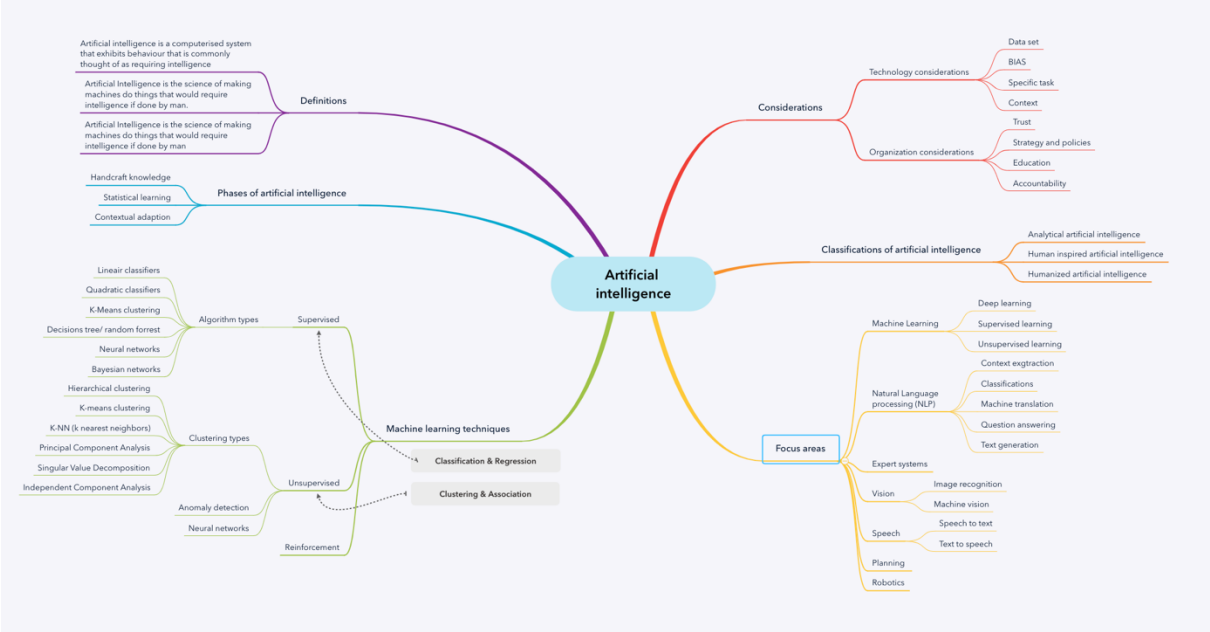

Figure 7. Artificial intelligence overview

4 Artificial intelligence applied to Security operations centers

This chapter analyses to what extent the capabilities of artificial intelligence can be applied in a security operations center. The first paragraph describes the approach of how the capabilities of artificial intelligence can be applied to a security operations center. The second paragraph analyses the capabilities from a literature perspective, in which functional domains of a security operations center can benefit from the capabilities of artificial intelligence. In the third paragraph, broader considerations are analyzed. These broader considerations are not specifically related to a functional domain of a security operations center but related to organization's aspects. The final paragraph is an overview of the results and how artificial intelligence can help the security operations center be more efficient and effective.

4.1 Approach

The approach to identify the capabilities of artificial intelligence in security operations centers is performed by mapping functional domains against the focus areas of artificial intelligence. The starting point is the functional domains of the security operations center, which are: 1) Intelligence function, 2) Baseline security, 3) Monitoring, 4) Pentesting, and 5) Forensics investigation. For each of the functional domains of the security operations center, an analysis is performed on how the focus areas of artificial intelligence can contribute. This analysis is performed through three lenses, which are people, process, technology. This model has similarities with the 3 layer model of Jan van der Berg (2018) in which these layers are describes as the technical, social-technical, and governance layer.
The technology lens focusses on the current artificial intelligence technology available and to what extent this can contribute to the functional domain. The people lens focusses on the potential of automating human activities within a security operations center given the artificial intelligence technology available. The process lens focusses on the implementation and considerations of applying artificial intelligence within a functional domain.

After identifying the capabilities of artificial intelligence, both from a people, process and technology perspective, in a security operations center, the general considerations for and organizations are analyzed in more detail. In the final paragraph, insight is given in the effectiveness of artificial intelligence in a security operations center. What is the benefit of the security operations center in terms of resources and effectiveness?

4.2 Capabilities analysis based on the literature study

The functional domains of the security operations center are analyzed in the following subparagraphs. For each functional domain, the technical possibilities of artificial intelligence are presented. Based on the technical possibilities an analysis is performed to what extent this has an effect on the human activities in a security operations center.

4.2.1 Intelligence function

The intelligence function is essential for an effective security operations center. Most organizations nowadays close monitor their internal landscape with respect to security but do not fully include information that is publicly available. Understanding the external landscape can benefit security operations centers by addressing alerts and incidents more effectively. Also, by understanding the external threats and whether these threats have an impact on your organization can help to take pre-emptive actions.
Open Source INTelligent (OSINT) tools are used by security operations center employees to actively "scan" the open internet for possible threats to their organization. OSINT tools are not new, the concept is been around quite some time, but has only gained interest as a result

of the emerging digitalization of the information and the rise of the internet (Glassman & Kang, 2012; Schaurer & Störger, 2013). External information can be integrated into the monitoring tooling directly to help prioritize alerts, helps to perform triages of an alert or incident, and validate events to decide follow up actions (FireEye, 2019). Example of threat intelligence feeds are suspicious domains, IP banned list, and malware hashes. A more complete overview of open intelligence feeds can be found on Github (Slatman, 2015/2019). Artificial intelligence has the potential to digest and analyze the OSINT information in real time to make adequate and swift decisions (Carroll, 2005; Glassman & Kang, 2012). Applying artificial intelligence supports security operations centers to focus on the things that matter and take the right actions. Activities performed by the security operations center analyst level 1 can be taken over by artificial intelligence. This includes the basic monitoring of the open intelligence feeds and correlating information from the various open intelligence feeds. Further activities performed by security operations center analyst levels 2 and 3, such as follow up on the monitoring alerts and actual threat hunting, are not easily performed by artificial intelligence as this requires in-depth knowledge and contextual information. Implementing artificial intelligence for domain intelligence function is hard due to the many open sources. All these open sources need to pre-formatted before the data can be processed by the artificial intelligence algorithm. Learning is an important aspect that includes weighting information to improve the outcome.

4.2.2 Baseline security

Understanding the security status of the organization's infrastructure through vulnerability testing is essential to keep the organization and its data protected. Included in the infrastructure are the routers, switches, servers, and end-user devices. Identifying and mitigating security weaknesses in an early stage contribute to the continuity of the environment, avoiding downtime as a result of a disruption of the infrastructure.

Security vulnerability assessment is carried out in four distinct stages (Khan & Parkinson, 2018). These stages are: 1) identify and prioritize resources, 2) determine threats to each resource, 3) analyze and mitigate identified threats, 4) define policies to prevent future attacks.

Vulnerability assessment can be done manually, assistive, and fully automated. Manually performing security vulnerability assessments requires that all activities related to the four stages are carried out manually. Specifically, the time and effort associated with stage 2 are extremely high and labor-intensive not to mention it requires skilled knowledge to carry out this activity. Depending on the size of the infrastructure this an enormous challenge, specifically, because vulnerability assessment is a continuous cycle.
Assistive vulnerability testing includes the use of scanning tools (Kali Tools, n.d.). Utilizing these tools significantly reduces the time associated with carrying out the activities in stage 2. At the same time, the intelligence required to carry out these activities is partly taken over by the tooling, therefore requiring less skilled personnel.
Taking this a step further would include the support of artificial intelligence in vulnerability assessment making this process fully automated. The three forms of artificial intelligence that can be applied in security vulnerability assessments are 1) machine learning, 2) expert systems and 3) automated planning (Khan & Parkinson, 2018).
Machine learning is used to build predictive models for vulnerability classification, clustering, and ranking. Using these predictive models reduces false positives and goes beyond the traditional tooling by discovering new and unknown vulnerabilities. The expert systems aid the decision-making process that otherwise would include human intervention. By automatic

decision making the reaction time to mitigate the vulnerability is significantly reduced. Another benefit is less overhead due to automated decision making. Automated Planning is a process of selecting and organizing purposeful actions in achieving expected outcomes (Ghallab, Nau, & Traverso, 2016). Generating attack plans to assess vulnerabilities reduces complexity, increases the quality of the plans and requires less skilled personnel.

Vulnerability assessments are carried out by security analyst level 1 and security analyst level 2. The activities of a security analyst level 1 are mainly planning, logistics and reporting. By applying automated planning the activities of a security analyst level 1 would be reduced. The activities of the security analyst level 2 are related to analyzing the outcome of the vulnerability scans, given the threat landscape, and take further action. By implementing artificial intelligence capabilities like machine learning and expert systems this would have an impact on the daily activities of the security analyst level 2 employee.

Vulnerability assessments are not the same as penetration testing. Penetration testing will be discussed in the next subparagraph. The main difference is that vulnerability testing is to explore, find and prioritize vulnerabilities and mitigate them. Penetration testing is aimed to exploit vulnerabilities. (Shah & Mehtre, 2015)

4.2.3 Monitoring

Monitoring the organization's infrastructure is of vital importance. Real-time or near real-time insight into your infrastructure helps to pro-actively respond to anomalies in the environment and prevent security incidents from happening. Handing all the log data from the various component in the environment is done through a Security Incident and Event Management System (SIEM). The SIEM collects and aggregates the log data of the infrastructure components. Individual log data from a single component helps to determine if the component itself functioning normally however combining individual log data from different components helps to create patterns and detect anomalies. Typical log sources that are monitored by a SIEM are operating servers, database servers, application services, employee end-user devices, domain controllers, routers, switches, antivirus, firewall, and intrusion detection/protection systems. Next to the log sources from the organization's infrastructure, threat intelligence feeds and vulnerability scans are taken into account by the SIEM systems. By using the cyber kill chain (Hutchins et al., 2011) framework it helps the security operations center to assess the alerts and act accordingly. Security incidents are avoided if indicators of comprise are detected in an early stage. The alerts generated by the SIEM are followed up by security analyst level 1 and depending on the severity also security analyst level 2.

In market reports by security vendors (Dalzoppo, 2018, p. 3) it is stated that security operations centers struggle with the amount of data, unaddressed threats and shortages of skills. By implementing artificial intelligence into the SIEM system, it helps to address the struggles mentioned above. Specifically, the simpler tasks, incident analysis and intelligent investigation, performed by security analyst's level 1 can be done more effectively by support from artificial intelligence. In a study performed by Suarez-Tangil, Polar, Ribagordo, & Sanz (2015) supervised learning is used to train SIEM system based on contextual learning & enhanced event correlation. By using artificial intelligence capabilities, the effectiveness goes up and requires less (skilled) security operations center personnel. According to a white paper by Vectra (2019) a workload reduction of 32 can be achieved for security analyst level 1.

Most of the current applications of artificial intelligence in cybersecurity are based on rule and signature-based solutions. New technologies are currently being developed based on the human immune system (Darktrace, 2019). These solutions are not based on rules nor signatures but rather on behavior and anomalies. These systems are self-learning, like an immune system, and do not require a reference data set. These systems do require a learning period to digest the unstructured information in order to differentiate between normal activities and malicious activities.

4.2.4 Pentesting

The objective of penetration testing is to find security flaws in the system and/or application. (Braden, 2002; Nationaal Cyber Security Centrum, 2010). To understand how artificial intelligence can support penetration testing a breakdown of the different stages of penetration testing is required. Much is written about the stages of penetration testing (Ami & Hasan, 2012) but for the purpose of this thesis 5 stages are relevant. These stages are: reconnaissance, scanning, exploitation, maintaining access, and reporting. Penetration testing is performed by the subject matter experts who have in-depth knowledge on this topic. The benefits of using artificial intelligence have a direct impact on the effectiveness of security analyst level 3 in a security operations center. In the following subparagraphs, the possibility of artificial intelligence supporting each stage of penetration testing is further examined.

4.2.4.1 Reconnaissance

In the reconnaissance stage, the object is to gather intelligence of the surrounding landscape and understand how the systems and/or application works and what is potential weaknesses are. This reconnaissance stage is depending on the surrounding landscape and is different for every application, therefore artificial intelligence is not beneficial.

4.2.4.2 Scanning

In the scanning stage, the code of the applications is inspected. This can be done statically by reviewing the source code or dynamically by real-time interacting with the application. Static code analysis can be supported by artificial intelligence with the focus area of natural language processing (Mokhov, Paquet, & Debbabi, 2014). With the use of supervised learning, artificial intelligence is able to predict if the source code is valid or not (Gupta & Sundaresan, 2018). Dynamic code analyses, done through interacting with the application, is typically done using reinforcement learning (Schwartz & Kurniawati, 2019). By applying reinforcement learning the algorithm learns from his last series of actions, to be more effective in reaching his goal.

4.2.4.3 Gaining access

Gaining access to an application requires detailed security knowledge. Depending on the outcome of a certain action a follow-up action is taken. This requires that the outcome is interpreted by the penetration tester and based on his analysis further steps are taken. For standard vulnerabilities in the system, automated scripts are available. Artificial intelligence can add to the automated scripts however this will not lead to substantial benefits.

4.2.4.4 Maintaining access

Similar to gaining access, maintaining access requires detailed security knowledge. There are tools currently available (Kali Tools, n.d.) that can support the penetration tester. Artificial intelligence can add to the automated scripts however this will not lead to substantial benefits

4.2.4.5 Reporting

Reporting on penetration tests and providing insight into the security status of an application is essential. The penetration tester interprets the information and based on the context suggestions are done to mitigate security risks. Given the contextual information that is required, artificial intelligence is less interesting.

4.2.5 Forensics investigation

Forensics investigation is performed for various reasons, ranging from a data breach, malware, fraud investigation to internal investigations. Forensics investigation preserves the original data's integrity when collecting and analyzing the data. By preserving the data's integrity and creating a chain of evidence the findings of the forensic investigation can be used in a formal process.
The possibility of using artificial intelligence in forensics investigation is limited. The main reason is the ability to explain the reasoning process of artificial intelligence. Although artificial intelligence is able to support individual parts of the forensics investigation, there is no overall solution. It is stated by Spencer (2018) and Irons & Lallie (2014) that artificial intelligence contributing to forensics investigations is still in its early stage.

4.3 Results

The results of the literature study on artificial intelligence that can be applied in security operations center are positive. There are multiple possibilities in which artificial intelligence can support a security operations center becoming more effective and efficient. In the figure below a high-level overview of the possibilities is given.

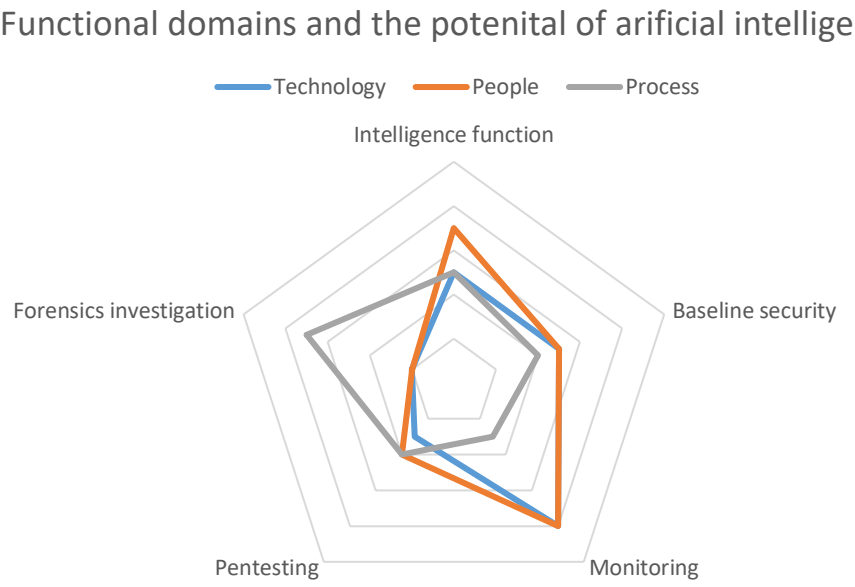

Figure 8. Overview of artificial intelligence possibilities in a security operations center

All functional domains, with the exception of forensics investigation, benefit when artificial intelligence is used. Depending on the functional domain this is more/less interesting. The biggest potential for artificial intelligence is in the function domain monitoring. The ability to automate activities in these domains by using artificial intelligence to perform security operations center analysts' level 1 and 2 activities is the largest and there making the security operations center more effective and efficient. The artificial intelligence technology is

available for these functional domains and the ability to adapt these artificial intelligence technologies is relatively easy.

The benefits of the functional domain monitoring, if artificial intelligence is applied, are the ability to process more logging information faster and more accurate. The ability to do more with less significantly helps to coop with the enormous amount of information the security operations center analyses on a daily basis. One of the main challenges also discussed as part of the problem statement, is that the security operations centers are overwhelmed with logging information. This results in not being able to process all relevant logging information but also adequately analyze the information that is analyzed. By using artificial intelligence more logging information can be analyzed and only the relevant cases are handled by the SOC analyst for further actions. The fact that many logging information is available helps to create a reliable artificial intelligence system.

For the functional domains intelligence function, baseline security, and pentesting the potential of artificial intelligence is not as big as with the functional domain monitoring. The functional domain intelligence function is perhaps the 2nd most interesting domain to apply artificial intelligence. The benefits in terms of automating the simple task performed by security operations center analyst level 1 & 2 are rather big, however, the technology is in its early stages and the ability to adopt this artificial intelligence technology is rather difficult. On specific aspects within the functional domains baseline security and pentesting there are possibilities to implement artificial intelligence but the overall effect on a functional domain is limited. Within the pentest domain, the possibility of dynamic code analysis using artificial intelligence is a specific aspect in which artificial intelligence is beneficial. The same applies to assistive vulnerability scanning within the baseline security domain. On this specific topic, artificial intelligence can be applied but again the overall impact on the functional domain is limited.

Given the complexity of forensic investigation combined with the early stage of artificial intelligence in this functional domain, the possibilities are limited. Over time with more experience in the field of forensic investigation and artificial intelligence in this domain, this becomes more interesting.

5 Dutch government organization; its security operations center and position on artificial intelligence

The previous chapter gave an overview of the possibilities of artificial intelligence and of how artificial intelligence can support security operations centers. It is clear from the literature that in certain functional domains of the security operations center benefit from artificial intelligence capabilities. This chapter describes the actual situation of governmental organizations with respect to the security operations center, its position on artificial intelligence, and to what extent the Dutch governmental organizations have experience with artificial intelligence, particularly in their security operations center. Based on the conceptual model in Figure 1 this chapter provides insight into step 4. In the first two paragraphs, the interview plan used for gaining the information from the Dutch governmental organization and the interviewees who participated in the interviews are discussed. The next three paragraphs are related to the interview questions and the responses from the interviewees. The three major topics, that reflect the research question on Dutch governmental organizations; its security operations center and position on artificial intelligence, are 1) How is the security operations center organized, 2) Position on artificial intelligence, and 3) Examples of artificial intelligence applied within the organization. The last paragraph provides a broad overview and summary of the Dutch governmental organizations, its security operations center and position on artificial intelligence.

5.1 Interview plan

The interview plan used for the interviews is attached in Appendix a: Interview plan. The interview plan consists of three main parts. The first is related to general information of the interviewee, his/her position, background, expertise and experience in the security environment. The second part is related to the security operations center, what is a security operations center, what are the main responsibilities, how is the security operations center positioned in the organization, challenges of security operations centers. The third part is about artificial intelligence. What is the interviewee's perspective on artificial intelligence, strategy on artificial intelligence within the organizations and specifically the security operations center, is artificial intelligence already applied within the organization, what are the opportunities and constraints of artificial intelligence?

Reports have been made of all conducted interviews. The reports were validated and approved by the interviewees. The reports are available upon request. The reports are used in the next few paragraphs to describe the actual situation of the respective security operations centers and position on artificial intelligence.

5.2 Interviewed governmental organizations

The interviewees for this thesis are representatives of Dutch governmental organizations. These Dutch governmental organizations have a public task and are funded by tax payer's money. Most if not all Dutch citizens are in the administration of these organizations with the exception of Rijkswaterstaat. The Dutch Tax Administration has a responsibility for raising taxes and paying out surcharges. UWV is responsible for implementing employee insurances and provide labor market and data services, work and income for all working Dutch citizens. The department of Justice and Security is responsible for maintaining the rule of law in the Netherlands so that people can live together in freedom, regardless of their lifestyle or views is responsible for the enforcement of the sentence or custodial measure taken by the Dutch court and the Sociale Verzekeringsbank is responsible for the implementation national insurance schemes in the Netherlands.

Rijkswaterstaat is responsible for the design, construction, management, and maintenance of the main infrastructure facilities in the Netherlands. Rijkswaterstaat is part of the vital infrastructure in the Netherlands. Infrastructure is considered vital if disruptions to this infrastructure lead to disruptions to society or threat to national security.

5.3 Interview results

In this paragraph, the results of the interviews are presented with respect to the security operations center and the position on artificial intelligence. Based on the conceptual model in Figure 1. Conceptual model this relates to step 4. The first paragraph is the feedback on the security operations center. The second paragraph is on artificial intelligence and the third paragraph is on artificial intelligence applied in security operations center.
The people interviewed for this thesis all have a multiple years of experience in the security field and have direct involvement with security operations centers. Further details of the interviewees can be found in the reports.

5.3.1 Security operations center

All governmental organizations interviewed for this thesis have a form of security operations center. Some governmental organizations have a security operations center with broader responsibility and size than others. In the following subparagraphs, per organization, the main questions of the research based on the interview plan will be analyzed in more detail.

5.3.1.1 Dutch tax administration

The security operations center of the Dutch tax administration was founded in 2010. Founding the security operations center was a logical next step given the developments with respect to cybersecurity and the rising threat landscape. The security operations center currently holds 10 employees excluding a team lead who reports into the manager of the Security Competence Center. The Security Competence Center is also responsible for digital fraud, physical data center security, information security, business continuity management, and certificates.
The security operations center is based on the model “Best Practices Joint Security Operations Center”. This proprietary model is a joint effort by the Dutch tax administration, Rijkswaterstaat, SSC-ICT and National Cyber Security Center. This model includes differentiation between employees in the security operations center. The different levels of the security analyst function mentioned in the propriety model is consistent with the literature analyses in chapter 2. They are team lead, level 3 security analyst, level 2 security analyst, and level 1 security analyst.
The responsibilities of the security operations center at the Dutch tax administration are:

- Intelligence function
  - Threat intelligence
  - Computer Emergency Response Team (CERT)
  - Security Incident Handling
- Baseline security
  - Intel-based vulnerability handling
  - Vulnerability scanning
  - Configuration monitoring
- Monitoring
- Pentesting
- Forensic investigation
- Certificates

With the exception of certificates, the responsibilities are in line with the functional domains from the literature study. The responsibilities for pentesting and forensic investigation performed using internal resources and depending on scale and complexity with support of external resources.

The Dutch tax administration has an open and progressive mindset on artificial intelligence. They participate or have participated in many market initiatives like the "Best Practices Joint Security Operations Center" together with the National Cyber Security Center, innovation projects to evaluate technologies and security solutions with TNO ("TNO - innovation for life," n.d.), and working with academic universities in researching security topics. Although artificial intelligence is not yet implemented in the security operations center there are possibilities for machine learning and expert systems in the areas of threat intelligence and monitoring

5.3.1.2 Department of Justice and Security

The security operations center at the Department of Justice and Security consists of a central security operations center that is responsible for the shared infrastructure and services and a more specific security operations center per sub-department. The focus is on the central security operations center and its responsibilities. The security operations center was founded in 2013 as a result of various large security incidents. These large security incidents, described by Wikipedia, are ("Blaster (computer worm)," n.d.; "DigiNotar," n.d.; "Nimda," n.d.; "SQL Slammer," n.d.). These larger security incidents help raise the topic of cybersecurity to the agenda of the board members and consequently to the implementation of the security operations center.
The central security operations center is positioned under the CIO office that falls directly under the secretary of Justice and Security. The sub-department security operations centers have a focus on the local processes and services and report into the CTO.
The security operations center is based on the security model by professor Paans (Schinagl et al., 2015, fig. 3) and the proprietary model "Best Practices Joint Security Operations Center".
The main security operations center consists of 6 employees including the manager. Next to the manager, the security operations center also has 1 senior analyst, 2 medior analysts, and 2 junior analysts.
The responsibilities of the central security operations center at the department for Justice and Security are:

- Baseline security
  - Vulnerability scans
  - Configuration management
- Monitoring
- Responsible disclosure
- Identity & access management

On top of the responsibilities mentioned above, there are additional responsibilities that fall within the specific security operations center at the sub-department. These responsibilities are not taken into account in this paper. The department of Justice and Security is able to keep up with new technologies and market developments. Important is to signal these opportunities early given the rapid changes in the security environment. Although artificial intelligence is not yet implemented in the security operations center, machine learning and expert systems are interesting in respect to the monitoring domain.

5.3.1.3 UWV

The security operations center at UWV was founded in 2012 based on an internal report from the internal accountant's departments and an external report from a consultancy firm. The security operations center is part of the ICT department that falls under the responsibility of the CIO. The number of employees operating within the security operations center is 12 with potential growth to 15 employees. On top of regular employees operating in the security operations center, there are 4 employees working on projects related to the security operations center. These projects are Information Security Management System (ISMS) and loghost. The security operations center is based on the proprietary model "Best Practices Joint Security Operations Center".
The responsibilities of the central security operations center at the department for UWV are:

- Intelligence function
  - Threat intelligence
  - Computer Emergency Response Team (CERT)
  - Security Incident Handling
- Baseline security
  - Intel-based vulnerability handling
  - Vulnerability scanning
  - Configuration monitoring
- Monitoring
- Pentesting
- Forensic investigation

The responsibilities are in line with the literature study. The main challenge at UWV is gaining maturity within the security operations center. The basics with respect to the services are in place but need to grow in terms of efficiency. UWV has integrated new technologies and services over the last few years. The challenge, however, is about the same as it was 5 to 10 years ago. This is related to extracting metadata from systems, makes sense of the data, correlating the data into useful use cases. Given the new technologies and expertise, improvements have been made but remains an area of concern. The human remains crucial for an effective security operations center. Especially understanding the surroundings and acting accordingly is critical. This contextual information is key.

5.3.1.4 Sociale Verzekeringsbank (SVB)

The security operations center at the Sociale Verzekeringsbank was founded in 2015. The main reason is the consolidated focus on security-related topics. The security operations center is part of the security & continuity department that resides under the management services department. Currently, there are 6 employees, including the team lead, operational in the security operations center. All employees have the same function however based on their expertise do perform different tasks. The Sociale Verzekeringsbank did not use a specific model to implement the security operations center. That said different documents by both Gartner (Gartner, 2018) and MITRE corporation (Strom, 2018) are used to implement the security operations center.
The responsibilities of the central security operations center at the Sociale Verzekeringsbank are:

- Executing its responsibilities according to the security policy Sociale Verzekeringsbank
- IT risk management
  - Offering resilience against digital threats from inside or outside the organization
  - Execute and analyze vulnerability scans on the IT infrastructure
  - Executing threat analysis
  - Executing security assessments

- Security monitoring
  - Set up of security use cases
  - Executing (near) real-time log analyses and correlations on components and systems within the Sociale Verzekeringsbank IT landscape
  - Creating security events and incidents
- Security incident response/handling
  - Executing security incidents according to the incident management process
  - Support toward the CSIRT process through the collection of intelligence, analyzing the indicators of compromise (IoC), and providing advice to the CSIRT team
- Reporting
  - Delivering periodic (steering) reports
  - Delivering periodic compliance reports

The Sociale Verzekeringsbank has chosen to outsource the threat intelligence, pentest, and forensics analysis. The challenges of the security operations center are related to the maturity level of the security operations center and the discussion on 24x7 continuous service based on a hybrid security operations center. Other areas of concern, not necessarily challenges, are cloud services and Internet of Things (IoT).
New technologies and market developments are hard to integrate into the services of the security operations center. This is partly because of the current workload and maturity level requires time and resources, but also because the existing contracts do not provide the flexibility to adopt new services and security solutions. Strategy and guidelines from board level are missing to pro-actively anticipate on new developments or technologies.
Many of the activities in a security operations center can be automated however human interaction and intelligence remain important. Machines do not have soft skills nor are they able to include contextual information.

5.3.1.5 Rijkswaterstaat

The security operations center at Rijkswaterstaat was founded in 2012 followed by a report from the Audit Rijksdienst. Based on the report from the Audit Rijksdienst Rijkswaterstaat started a 3-year program that included the implementation of the security operations center. During the implementation of the security operations center, there were plans to outsource the security operations center but after internal discussions, it was decided to insource the security operations center. The security operations center is positioned under the Security center which is part of the ICT department of Rijkswaterstaat. The security operations center was initially based on best practices and common knowledge available at the time. Rijkswaterstaat joint forces with the Dutch tax administration and SSC-ICT (Ministerie van Binnenlandse Zaken en Koningsrelaties, 2016) and together founded the model “Best Practices Joint Security Operations Center”.
The security operations center of Rijkswaterstaat currently employs 22 employees. These 22 employees are divided into a team lead, multiple level 3 security analysts, multiple level 2 security analysts, and multiple level 1 security analysts.
The responsibilities of the central security operations center at Rijkswaterstaat are:

- Intelligence. Collecting threat intelligence and vulnerabilities information
- Baseline security. Surveillance on BIR compliance including risk analysis
- Monitoring and response. Monitoring of vital infrastructure and critical infrastructure
- Forensic investigations. Collecting and analyzing evidence
- Pentesting. Security testing on critical infrastructure. Upon request or initiated by the security department

The scope of the responsibility of the security operations center includes both the IT and OT environment. OT environment includes water management, roads, and bridges.

Rijkswaterstaat monitors its IT and OT environment 24x7. During working hours this is done at the security operations center and after working hours the monitoring and response are taken over the network operations center. Rijkswaterstaat has an open mind with respect to new technologies and market developments. It is the experience of Rijkswaterstaat that new technologies and services offered by security vendors are simplified during proof of concepts and pilots. In reality, these new technologies and/or market developments are more complex. The role of the employee is essential to the success of a security operations center. Most information within the security operations center is technical related and does not include any contextual information or relevance. This is typically done by the security operations center employee.

5.3.2 Position on artificial intelligence

This paragraph will analyze the response of the interviewee with respect to artificial intelligence. The analyses are done based on the outline of the questions of the interview plan with the exception of one question that is related to current artificial intelligence developments, this question will be analyzed in the next paragraph. In the following subparagraphs, the responses from de Dutch governmental organization are given.

5.3.2.1 Dutch tax administration

The Dutch tax administration has an open and progressive mindset with respect to artificial intelligence in general. In the past, the Dutch tax administration has worked with academic institutions and TNO to explore new artificial intelligence possibilities. The innovation department within the Dutch tax administration experiments with new technologies such as artificial intelligence. In case these new technologies are successful the Dutch tax administration is considering applying the technology broader within the organization.
This progressive mindset has led to artificial intelligence being applied at the Dutch tax administration. Not directly within the security operations center but in other areas.
The Dutch tax administration does not have a corporate strategy with respect to artificial intelligence. Policies and frameworks related to artificial intelligence are being developed in conjunction with the innovation process.
The main reason for adopting artificial intelligence within the Dutch tax administration is to carry out their public tasks more effectively and efficiently. The large data sets analyzed by the security operations center are impossible to digest manually. More automated tools, including the possibility of artificial intelligence, support the security operations center to prioritize the workload and focus on the security alerts and incidents that matter. When applying artificial intelligence, it is imperative that the data sampling set is accurate. Incorrect data sampling set has a major impact on the results of the artificial intelligence and therefore on the business and potentially the clients of the Dutch tax administration. Another aspect to consider is the impact of the artificial intelligence systems on the business of the Dutch tax administration. Is the business capable of understanding the results of the artificial intelligence system and vice versa is the artificial intelligence system able to include the context of the business? Both the business and the security operations center employees need to understand how to interpret the artificial intelligence results. A user-friendly interface helps the organization to interpret the result.
Designing and building an artificial intelligence algorithm is a specific and difficult task. This requires skilled people with specific knowledge of data science and artificial intelligence. This goes beyond the expertise of a security operations center analyst. The security operations center analyst should be able to interpret the results of the artificial intelligence including a basic understanding of the artificial intelligence algorithm.

Artificial intelligence is able to support security operations center to be more effective and efficient, however, it is not able to fully take over human activities. Specifically adding contextual information is something an artificial intelligence system is not capable of. Information without context is plain data.

5.3.2.2 Department of Justice and Security

The department of Justice and Security have an open mindset with respect to artificial intelligence. Artificial intelligence is able to support the organization being more effective. The department of Justice and Security does have a corporate strategy on artificial intelligence however not tailored for the security operations center. When artificial intelligence will be applied in the security operations center the strategy and policies will be developed. The main reason for the department of Justice and Security to adopt artificial intelligence in their security operations center is to best make use of the employee skills and experience. Bulk work currently handled by the security operations center employees can be further automated using artificial intelligence leaving more time for the security operations center employees to focus on the important topics. This also adds to the employee's satisfaction as his skills and expertise is being challenged. The constraints for the department of Justice and Security in actively using artificial intelligence are trust and contextual information. Are the results from an artificial intelligence system trustworthy for further actions, even with legal consequences, by the organization. What defines trustworthy and how is this validated? The other concern is related to dependencies in the organization and whether or not artificial intelligence is able to factor in all these dependencies in the results. This contextual information is not only IT-related but also business-related. Prerequisites for using artificial intelligence in security operations center are well documented standard operating procedures including mandates. With the introduction of artificial intelligence in the organization and particularly in the security operations center it requires employees to gradually learn and understand artificial intelligence. This is a slow process but until now have not led to a knowledge gap. Products like SOAR (Security Orchestration, Automation and Response) are integrated into the services of the security operations center and anticipate potential future artificial intelligence solutions. Artificial intelligence can definitely support the security operations center, that said the human perspective remains important mainly because an artificial intelligence system is not capable of comprehending emotions, understand business dependencies, act according to emergencies or understand the impact.

5.3.2.3 UWV

UWV is reluctant towards artificial intelligence hence UWV have not yet implemented artificial intelligence into their business nor in their security operations center. The possibilities of artificial intelligence are endless, however, artificial intelligence is still in its infancies. Artificial intelligence applications such as robotics and Watson ("Watson," 2019) are good examples of the potential of artificial intelligence in the near future. The real potential of artificial intelligence is when these systems become self-aware and self-consciousness. Over time artificial intelligence will be integrated into the security operations center and be part of the daily operations, this is inevitable. UWV does not have a strategy on artificial intelligence on a corporate level. Within the security operations center, discussions are taken place how artificial intelligence is able to further improve the security monitoring, specifically with used cases. The structured data is further analyzed by artificial intelligence to reduce the volumes of information and the false positives from security alerts. The motto is to start simple, learn and gradually explore more complex forms of artificial intelligence. UWV is currently exploring the potential of artificial intelligence to support decision making from a client's perspective. These initiatives are not related to the security operations center

but to the primary business processes. Within the security operations center, the discussion on artificial intelligence is focused on the detection of security anomalies and not on automatic remediation or restore. Given the enormous amount of data that is processed on a daily basis by the security operations center, it is inevitable that artificial intelligence will be used in the near future. Artificial intelligence is capable of performing analyses more quickly and efficiently than humans.
An artificial intelligence roadmap is essential for security operations centers. Start simple and add complexity as you grow. This also applies to the security operations center employees who are working with artificial intelligence systems, they too must grow skills and expertise over time. This is an ongoing process and needs constant attention.
The constraints working with artificial intelligence is the substantial data set for training the artificial intelligence algorithm. In case the data set is not complete or includes malicious data, this has an effect on the artificial intelligence system and its outcome when used in practice. Security operations center employees should understand the artificial intelligence algorithm and be able to reproduce the result of the artificial intelligence system.
Furthermore, the security operations center employee should provide further analysis and include contextual information.
Overtime when artificial intelligence systems become self-aware and self-consciousness it might take over all activities currently carried out humans. In the foreseeable future, the human interaction is still essential in a security operations center.

5.3.2.4 Sociale Verzekeringsbank (SVB)

The Sociale Verzekeringsbank has an open mindset with respect to artificial intelligence. Artificial intelligence will become more important in the near future as more logging information is processed by the security operations center daily. The example of Watson ("Watson," 2019) is a good illustration of the capabilities and features of artificial intelligence. Given the fact that artificial intelligence will become a commodity over time, it is important that the artificial intelligence systems can be trusted. In other market areas, there has been proof that the artificial intelligence systems have been biased and the results have been incorrect.
The Sociale Verzekeringsbank does not have a corporate strategy on artificial intelligence. Within the security operations center, the main focus is on the maturity of the security operations center, discussions on artificial intelligence will follow once the desired maturity level is reached. Most like it will take another year or two to reach the desired maturity level. The Sociale Verzekeringsbank does have an innovation lab where new technologies and services are piloted. The focus of the innovation lab is on the business and client-side, not on infrastructure or security. The main reason for adopting artificial intelligence within the security operations center is to be more efficient and effective. More logging information can be processed and analyzed in a shorter period of time. Also, the shortage of trained and experienced security operations center employees is a reason to implement artificial intelligence for automating standard tasks.
One of the important constraints when using artificial intelligence in the security operations center is the correct training of the artificial intelligence algorithm. A good sampling data set is required. When self-learning is applied it is essential that the system is not biased as in the case with the US court that used a risk assessment tool, based on artificial intelligence, to assess whether parolees are likely to break the law again. It turns out this system was biased towards black prisoners. Another concern when using artificial intelligence is that the security operations center employees should be able to understand the algorithm and able to interpret the results correctly.

For the Sociale Verzekeringsbank to adopt artificial intelligence it is necessary to have a clear strategy including policies and standards on artificial intelligence. This helps the security operations center to implement artificial intelligence systems according to the company's guidelines. Failure to provide these guidelines could lead to many different forms of artificial intelligence systems each with its own challenges that need to be overcome by the security operations center.
The security operations center employees should embrace new technologies and educate themselves accordingly. This is a logical next step and mandatory given the changing responsibilities and tasks in a security operations center.

5.3.2.5 Rijkswaterstaat

Rijkswaterstaat has an open and positive mindset with respect to artificial intelligence. Artificial intelligence is considered a buzz word, the definition of artificial intelligence is very broad. This varies from a single algorithm to complete neural networks. A more precise definition of artificial intelligence, of what is not artificial intelligence, is helpful for common understanding. Rijkswaterstaat has a digital strategy that includes technologies like artificial intelligence but also blockchain. New initiatives and technologies are piloted and if successfully implemented in the broader organization. This innovative mindset is partly driven by the report from the minister of Infrastructure en Waterschap that states that governmental organizations should lead in ICT.
The main reason for Rijkswaterstaat to adopt artificial intelligence is to make decision more accurately. This results in carrying out her tasks more effectively and thereby reducing operational costs.
The major constrain for Rijkswaterstaat to adopt artificial intelligence was clear legislation. Rijkswaterstaat uses endpoint software called EnCase ("EnCase," 2019) on their laptops. This end point software is broadly used within Europe but could potentially lead to legal issues, specifically with countries like China. What is legal in one country is not necessarily legal in another country.
A good plan with clear objectives and a roadmap is essential for organizations prior to using artificial intelligence within their security operations center. Budgets are equally important. At Rijkswaterstaat it is the experience that the money will naturally follow when a good plan is presented. National and international collaboration with similar organizations is beneficial to avoid re-inventing the wheel over and over.
Security operations center employees, in general, are capable of interpreting the outcome of artificial intelligence, given the user interface is similar. In the example of measuring the water level, Rijkswaterstaat automated the process using artificial intelligence systems and therefore eliminating activities that were previously performed by humans. The example is related to the Operational Technology (OT) and not Information Technology (IT). By using artificial intelligence systems in the OT environment, Rijkswaterstaat initiated a strategic personnel plan to re-educate the employees that are affected.
Artificial intelligence systems are capable of learning new things, however, within the scope it was designed for. This can help support activities previously performed by employees but not the broader aspect related to the employees' function.

5.3.3 Applied artificial intelligence in security operations centers

All Dutch organizations have some experience with artificial intelligence, whether this is based on innovation projects or actual applications. Most of the discussion on artificial intelligence is related to the business side or OT side of the organization. Within the ICT and more specifically in the security operations center artificial intelligence is still in the early stages. Over time it is the contention of the Dutch governmental organizations that artificial

intelligence will be integrated into the daily operations and become a commodity. In the interview with the Sociale Verzekeringsbank it was mentioned that current security services like “mail/spam filtering” use some form of algorithms however as such should not be considered as artificial intelligence.
The examples given by the Dutch governmental organizations of artificial intelligence within their organizations, however not in the security operations center, are:

Dutch tax administration; Digital fraud
Within the digital fraud department artificial intelligence is used to investigate possible digital fraud. Over more than 4.000 attributes within the administration of the Dutch tax administration are analyzed by artificial intelligence to assess the likeliness of digital fraud. Based on the outcome of the artificial intelligence system further investigations by employees are performed to determine whether or not it is indeed digital fraud.

Department of Justice and Security; Child protection services
An example is child protection services where artificial intelligence is used to advise agents on how to detect possible abused children. Based on artificial intelligence patterns that often occur with child abuse are found in the files. Agents are warned on possible abuse patterns in the files they themselves wouldn’t have seen. The first results are promising. Agents feel supported by artificial intelligence and successes have been seen.

Rijkswaterstaat; Traffic management
Artificial intelligence is used to analyze different data sources to determine how, when and where to deploy resources. By allocating resources based on artificial intelligence, both in personnel and in material, Rijkswaterstaat is more effective and reducing inconvenience for their customers

Rijkswaterstaat; Bridges and locks
Bridges and locks are nowadays equipped with sensors that feed information into the artificial intelligence system. By correlating this information Rijkswaterstaat was able to save 10% on the energy bill. The artificial intelligence also provided Rijkswaterstaat with information on the status of the bridge or sluice to effectively perform maintenance.

Rijkswaterstaat; Maastkantkering
The maaskantkering is operated automatically by artificial intelligence. Depending on the level of the water measured by various sensors the locks automatically closes of opens. There is a manual override button but only in case of malfunction or emergencies.

5.3.4 General observations

The persons interviewed for this thesis were all enthusiastic to corporate. Depending on the interviewee the level of detail specifically on artificial intelligence was different. All interviewees had a good understanding of the security operations center and its responsibilities. With respect to artificial intelligence, there were some differences in the responses. The more security and technically skilled interviewees had detailed knowledge of artificial intelligence, its capabilities, its constraints, and how this could benefit the security operations center. That said these interviewees, with the exception of the interviewee of Rijkswaterstaat, did have little understanding on artificial intelligence within the broader organization. What is the corporate strategy, what are the current pilots and application with respect to artificial intelligence? The managers interviewed had a good overview of the

broader organization but did not have the full technical and security insights. In the interviews, both types of people were interviewed to get a more holistic view.

5.4 Summary

The summary from the interviews is presented in the overview below. In this overview, the most relevant aspects of the security operations center and artificial intelligence are taken into account.

Topic \ Organisation			Dutch Tax Adminisatration	Department of Justice and Security	UWV	Sociale VerzekeringsBank	Rijkswaterstaat
Security Operations Cener							
	General						
		Compelling event for SOC	Natural evolution	Diginotar and similar cyber incidents	Internal accounting report & External report	Natural evolution	Governmental accounting resport (ADR)
		SOC origin date	2010	2013	2012	2015	2012
		Size of SOC	11	6	12 with a budget for 15	6	22
		Model	Best practices JSOC	Best practices JSOC & SOC model by proffesor Paans	Best practices JSOC	MITTRE and Gartner	Best practices JSOC
	Functional domain						
		Intelligence function	Yes	No	Yes	No, Outsourced	Yes
		Baseline security	Yes	Yes	Yes	Yes	Yes
		Monitoring	Yes	Yes	Yes	Yes	Yes
		Pentest	Yes	No	Yes	No, Outsourced	Yes
		Forensic inventigation	Yes	No	Yes	No, Outsourced	Yes
		Other responsibilities	Certificates	Identity & Access Management Responsible disclosure	Not applicable	Compliance reporting	OT Physical objects
	Other						
		adaptability to new market technogolies	Open minset, restraints are internal approval and budgets	Open mindset, certainly possible but needs constant attention	Yes in terms of new technologies, no in terms of functionality	Hard. Focus is on maturity	Possitive outlook. RWS controls and operates their own infrastructure.
		Sourcing strategy	Insourced	outsourced	outsourced	Outsourced	Insourced
		24x7	fail over to central facilities after working hours	No	fail over to central facilities after working hours	No	fail over to central facilities after working hours to NOC
Artificial Intelligence							
		Mindset on artificial intelligence	Open and progresive mindset	Open mindset	Reluctant mindset	Open mindset	Open and progresive mindset
		Strategy	Agile approach in combinanation with innovation	Corpertate strategy yes, SOC specific strategy no	No corporate strategy; discussions at soc level	No corportate strategy	Digital strategy that includes AI and blockchain
		Reason for adopting Artificial intelligence	Efficency en effectively	Automate "bulk" work so security analist can focus on the important stuff	Amount of Information that needs to be processed. Support decision making	Shortage of skilled and experienced staff	More accurate decisison. Lead to more effectiveness and lower costs
		Constraint	Accurate data set. Contex information	Trust & Contextual inforamtion	accurate data set	Correct training including data set, skill set of soc employee	Clear legislation
		Prerequisite	No specific prerequisite were mentioned by the Dutch tax administration	Standard operation procedures with correct mandates.	Roadmap, skills and expertise	strategy including policies and standards on artificial intelligence	A good plan with clear objectives and a roadmap
		SOC employees knowledgeable	Data science. SOC should be able to interpret the outcome and understand the algorithm	Slowly learning. comprehending emotions, understand business dependencies, act according to emergencies or understand the impact	Mandatory until artificial intelligence is self consiousness and self aware	Embrace new technologies, constant education	re-education is required
		Aritifical Intelligence examples	Digital fraud	Child protection services			Traffic management, Bridges and Locks, and Maaskantkering

Figure 9. Overview results interviews

Over the last decade all the Dutch governmental organizations have implemented a security operations center. With the exception of the Sociale Verzekeringsbank all Dutch governmental organizations have the responsible for the functional domain's intelligence function, baseline security, monitoring, pentest, and forensic investigation. This is in line with the theoretical model by Michail (2015) and Schinagl et al (2015). The security operations center of Rijkswaterstaat is by far the largest in terms of employees. This is partly because the security operations center of Rijkswaterstaat is also responsible for the security monitoring of physical objects, like road, bridges, and locks.
The Dutch governmental organizations all agree that keeping track on the latest technologies and market developments within a security operations center is a challenge, however, the restraints are more related to the organizational aspects like budgets and internal approval

than related to the ability to integrate these new technologies and market development into the daily operations from a security perspective.

Artificial intelligence is adopted by the Dutch tax administration and Rijkswaterstaat. They have an open and progressive mindset with respect to adopting artificial intelligence. Both organizations have a form of corporate strategy. The Dutch tax administration has developed their strategy based on an agile approach whereas Rijkswaterstaat does have a corporate digital strategy including both artificial intelligence and blockchain. The department of Security and Justice also have a corporate strategy but have a more open mindset towards artificial intelligence. Both UWV and Sociale Verzekeringsbank do not have a corporate strategy on artificial intelligence. Discussions are taken place within the organizations however they have not yet led to a corporate strategy. All Dutch governmental organizations do believe that over time artificial intelligence will be integrated into the daily operations of the security operations center. The reasons for integrating artificial intelligence into the daily operations of a security operations center slightly differ per organization. That said the general conclusion was that with applying artificial intelligence more can be achieved with fewer people and decisions are more effective.
The organizations that have insourced their environment are more prone to experiment with artificial intelligence. Both the Dutch tax administration and Rijkswaterstaat have already artificial intelligence applications integrated into their business processes.
With respect to the constraints of artificial intelligence, the responses from the interviewed organizations are roughly in line. The most important constraint is an accurate data set to train the artificial intelligence algorithm. The second important constraint, mentioned by two of the organizations, is contextual information. Other constraints that are mentioned were trust, the skill set of security operations center employees, and legislation.
All organizations agree that the employees working in the security operations center require further education when artificial intelligence is integrated into the daily operations of a security operations center. The Dutch tax administration believes that next to re-educating the security operations center employees you need a data scientist when working with more complex forms of artificial intelligence. All organizations do believe that the role of the employees remains trivial because of the soft skills and contextual information.

6 Gap analysis: possibilities of artificial intelligence applied in security operations center at Dutch governmental organizations

In the previous chapters the literature study on security operations center as well as artificial intelligence is researched. Based on the literature research the potential for artificial intelligence within security operations centers is presented. Understand the position of the Dutch governmental organization with respect to their security operations center and artificial intelligence leads to a potential gap. This gap is analyzed in the paragraphs below. The first paragraph combines the results from the literature study with the current situation of the Dutch governmental organizations. The second paragraph analyses the consideration of artificial intelligence and to what extent these considerations are taken into account by the Dutch governmental organization. By closing the potential gap the Dutch governmental organization is able to carry out their work more effective and efficient. Based on the conceptual model in Figure 1 this chapter provides insight into step 5

6.1 Possibilities of artificial intelligence. Literature and business combined.

The possibilities of artificial intelligence based on the literature study are enormous. With the exception of the forensic investigation, all other functional domains have possibilities to apply artificial intelligence. An overview is presented in Figure 8. Overview of artificial intelligence possibilities in a security operations center. The most interesting domain to apply artificial intelligence is the monitoring domain followed by the intelligence function domain. Applying artificial intelligence solutions in these domains significantly reduces the activities carried out by SOC analysts' level 1 & 2.
The functional domains pentesting and intelligence function are more complex domains and require more skills and expertise. Also, the contextual information is more relevant in these domains compared to the functional domains baseline security and monitoring.

All Dutch governmental organizations have in their responsibilities the functional monitoring. Within this domain, efforts have been made to automate process however no artificial intelligence is used within this domain, or in any of the other domains related to the security operations center. Automation is done using standard type tooling. In the functional domain monitoring SIEM tooling is used to automate security monitoring and within the functional domain baseline security vulnerability tooling is to automate scanning. These types of tooling help to automate activities however is not considered artificial intelligence.
The functional domains intelligence function and pentesting are not included in all the security operations center at the Dutch governmental organization. Only the Dutch tax administration, UWV, and Rijkswaterstaat have these functional domains included in their security operations center. The Sociale Verzekeringsbank has outsourced these responsibilities and the department of Justice and Security does not have these responsibilities included in their security operations center.

The Dutch tax administration, department of Justice and Security, and Rijkswaterstaat all have artificial intelligence solutions in place, however not within the security operations center.

The potential for Dutch governmental organizations to be more efficient and effective, taking into account artificial intelligence is not yet used, is enormous. Specifically, in the domain monitoring closely followed by the domain intelligence function.

6.2 Considerations

Most of the Dutch governmental organizations have experience with artificial intelligence however not in the field of security operations centers. Whether the experience is based on innovation projects or actual applications, it is on the radar of the organizations.
The considerations mentioned in the chapter "Artificial Intelligence" need to be addressed when organizations start using artificial intelligence. The considerations with respect to the organization can be addressed regardless of any implementation of artificial intelligence. The technology related considerations are relevant upon implementation of artificial intelligence.

6.2.1 Organization considerations

The organization considerations mentioned in the chapter "Artificial Intelligence" are trust, strategy, strategic HR plan, and accountability. In the picture below an overview is given of the Dutch governmental organizations with respect to the organization considerations. Based on the interviews held, the information given by the Dutch governmental organizations is analyzed and processed. The axes in the figure below are relative and based on the qualitive interpretation of the interviews held at the Dutch governmental organizations.

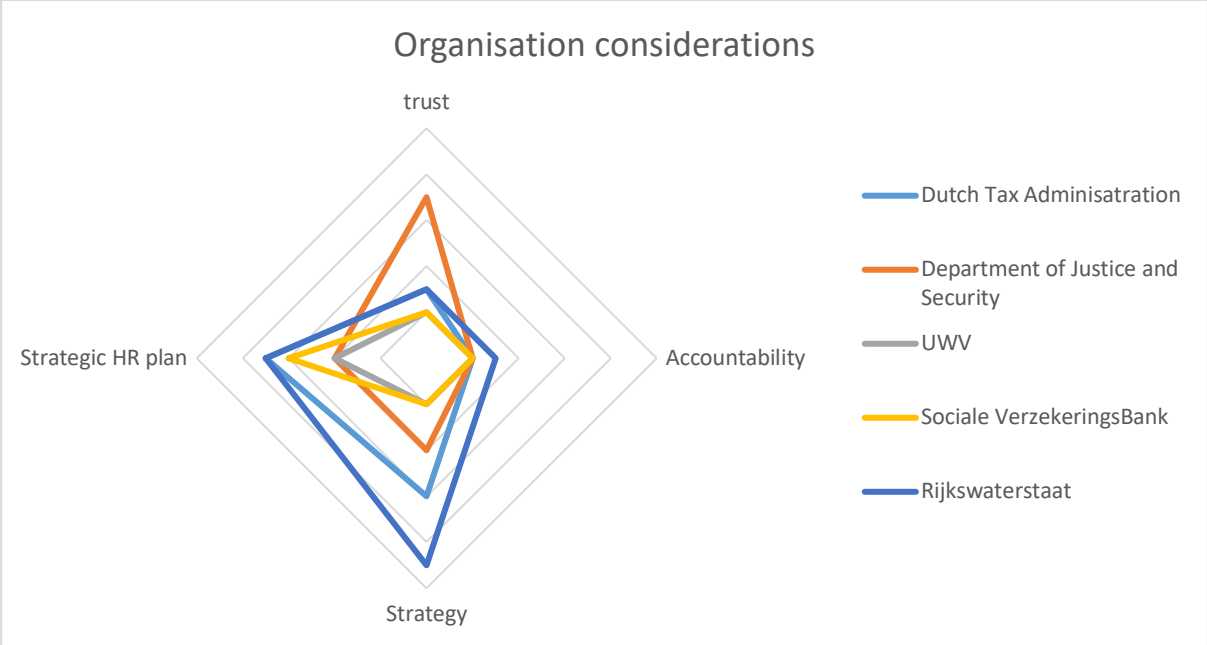

Figure 10. Organization considerations by Dutch governmental organization

It is clear from the analyses that the considerations strategy and strategic HR plan are on the radar of most organizations. The considerations of trust and strategy are topics that require attention and focus. In the interviews conducted these aspects are hardly mentioned as topics that need to be addressed. The organization considerations are discussed in more detail in the next few paragraphs.

6.2.1.1 Strategy

Rijkswaterstaat is one of the few Dutch governmental organizations with a clear digital strategy. This digital strategy includes new technologies like blockchain and artificial intelligence and is established on a corporate level. The Dutch tax administration has an agile approach with respect to the corporate strategy on artificial intelligence. Based on new developments and lessons learned the corporate strategy on artificial intelligence is renewed. The department of Justice and Security are in the process of developing a corporate strategy on artificial intelligence however do have local guidelines for the artificial intelligence

initiatives already in place. UWV and Sociale Vezekeringsbank do not have a corporate strategy yet.

6.2.1.2 Strategic HR plan

All Dutch governmental organizations acknowledge that by integrating artificial intelligence into the business and security operations center processes this possesses a challenge on from an education perspective. Both Rijkswaterstaat and the Dutch tax administration have started strategic HR plans on a corporate level to address this challenge. The other Dutch governmental organizations have local initiatives to address this challenge however do not yet have a holistic view.

6.2.1.3 Trust

The department of Justice and Security is one of the few Dutch governmental organizations that explicitly mentioned this topic as an important consideration. The reason being that the artificial intelligence solution has a direct impact on its clients and their families. Rijkswaterstaat has multiple artificial intelligence solutions in place however these do not directly impact clients directly as the artificial intelligence solutions are mainly used in the OT environment. That said, it is under constant discussion at Rijkswaterstaat. The other Dutch governmental organizations did not mention this consideration explicitly, the main focus of these organizations is on a strategy and building experience.

6.2.1.4 Accountability

The artificial intelligence solutions currently in place at the Dutch Governmental organizations help organizations to make more effective and efficient decisions. The actual decisions are still made by the employees of the organizations. The accountability is therefore not yet a consideration of concern. In time with automatic decisions making this becomes more important.

6.2.2 Technical considerations

The technical considerations mentioned in the chapter “Artificial Intelligence” are test data set, context, bias, and specific task. In the picture below an overview is given of the Dutch governmental organizations with respect to the technical considerations. Based on the interviews held, the information given by the Dutch governmental organizations is analyzed and processed. The axes in the figure are relative and based on the qualitive interpretation of the interviews held at the Dutch governmental organizations.

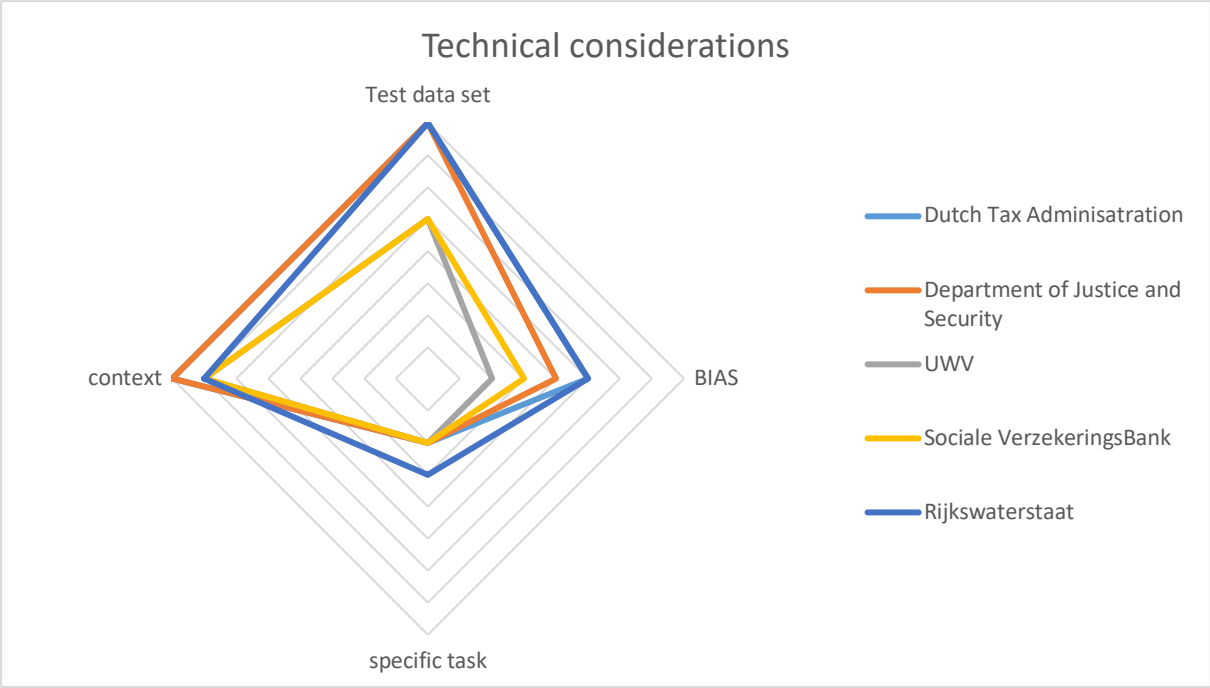

Figure 11. Technical considerations by Dutch governmental organization

It is clear from the analyses that the considerations test data set and context are high on the radar of most organizations. The technical considerations bias has a bigger impact on the Dutch governmental organizations that have experience in artificial intelligence. In the interviews conducted these aspects are hardly mentioned as topics that need to be addressed. The technical considerations are discussed in more detail in the next few paragraphs.

6.2.2.1 Test data set

All Dutch governmental organizations have mentioned that having an accurate and complete test set is essential when applying artificial intelligence solutions. The Dutch governmental organizations that have actual experience with artificial intelligence find it even more important. The overall feedback is that if the artificial intelligence algorithm is not trained properly this has a direct impact on the results.

6.2.2.2 Context

Contextual information is important for all Dutch governmental organizations. Artificial intelligence systems are able to process information more effective and efficient than humans but are not capable of including contextual information. Including the bigger picture and weighing these factors accordingly is more difficult for artificial intelligence systems.

6.2.2.3 Bias

All Dutch governmental organizations do believe that bias is a consideration that needs to be addressed. The Dutch governmental organizations with the most experience do tend to actively deal with the bias aspect as this is a real concern. For the other Dutch governmental organizations this is a consideration to be looked at more specifically.

6.2.2.4 Specific task

Although this consideration is applicable to artificial intelligence many of the Dutch governmental organizations have not mentioned this consideration as a concern.

6.3 Result

The result of the gap analyses performed is that currently no Dutch governmental organization has applied artificial intelligence applications in their security operations center. The potential is enormous, specifically in the functional domains monitoring and threat intelligence. That said, Rijkswaterstaat closely followed by the Dutch tax administration and the department of Justice and Security are the organizations that have experience on a corporate level with artificial intelligence. Given the experience on a corporate level, these Dutch governmental organizations also have experience with the organization and technical consideration with respect to artificial intelligence. In the figure below, the position of the Dutch governmental organizations with respect to the considerations is presented. The axes in the figure below are relative and based on the qualitive interpretation of the interviews held at the Dutch governmental organizations.

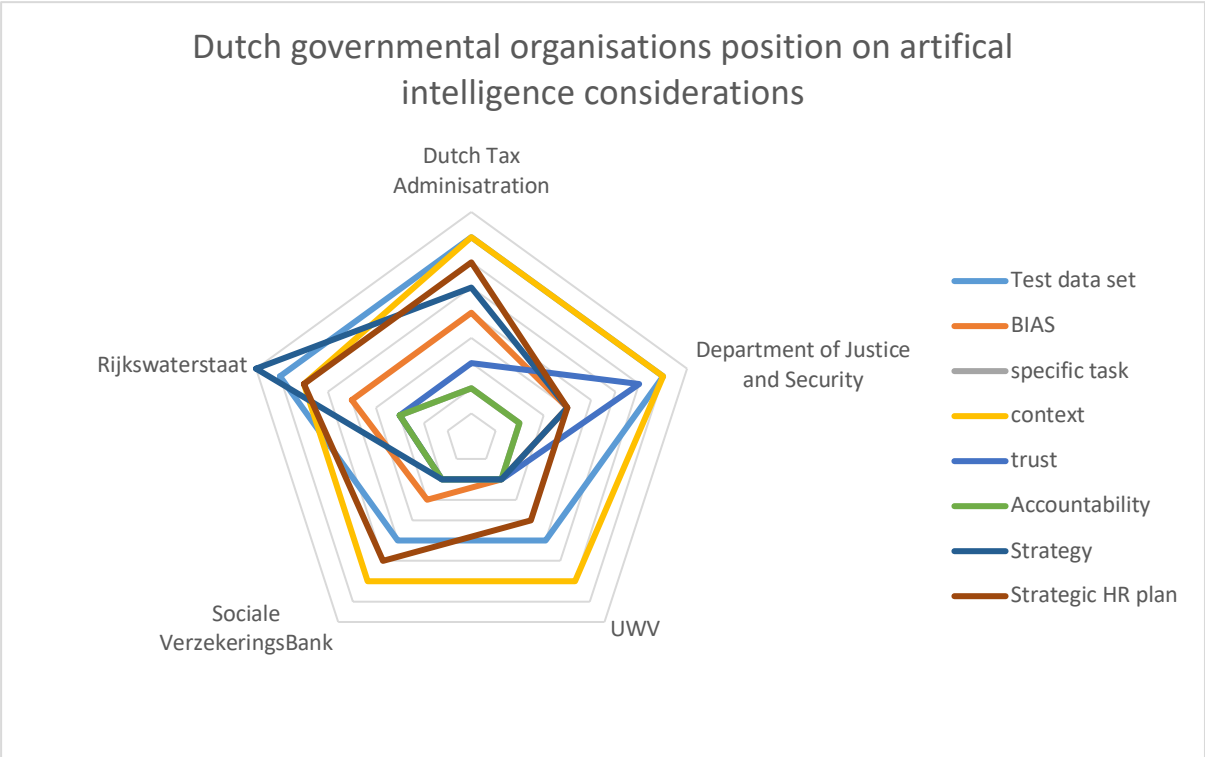

Figure 12. Dutch governmental organization position on artifical intelligence considerations

The considerations context, test data set, and strategic HR plan is on the radar of all Dutch governmental organizations. These topics have visibility in the organizations and activities are taken to address these considerations. Rijkswaterstaat and the Dutch tax administrations have taken steps already, where others are planning and discussing steps to address these considerations.

The considerations specific task and accountability with respect to artificial intelligence are not subject of discussion within the Dutch governmental organizations. Based on the interviews conducted these considerations were not explicitly mentioned.
The responses by the Dutch governmental organizations on the artificial intelligence considerations bias, trust, and strategy are very different. Rijkswaterstaat and the Dutch tax administration both have a corporate strategy whereas UWV and the Sociale Verzekeringsbank are at the early stages of developing a corporate strategy.

The considerations accountability and trust are topics that need further discussions, not only on a corporate level but also on a governmental level. The Dutch government has an important position to educate the people of the Netherlands with respect to artificial intelligence in general and specifically on the aspect's accountability and trust.

7 Conclusions and recommendations

The challenges for the security operations center to keep organizations secure remains difficult, especially with the digital data that is growing year over year. Security analysts are unable to keep up. Integrating artificial intelligence in security solutions supports security operations center to carry out their tasks more effective and efficient.

Although the literature on security operations centers is limited, there is a common view of the goals and functional domains of a security operations center. These functional domains are 1) Intelligence function, 2) Baseline security, 3) Monitoring, 4) Pentesting, and 5) Forensic investigation. Within a security operations center there are 3 levels of security analysts active. The level 1 security analysts are the generalist, mainly responsible for monitoring and responding to security alerts. The level 2 security analyst have a deeper understanding of processes and technology and responsible for analyzing incidents, correlating information and determining follow up actions. The level 3 security analysts are considered the experts, they focus on specific areas such as forensic and malware but also support the level 2 security analyst in complex and major security incidents.

Artificial intelligence, however, is a buzz word. In this paper, the focus was on the type of artificial intelligence is beneficial to use in the security operations center. The main focus areas interesting for security operations center based on the literature study are machine learning, natural language processing (NLP), expert systems, and planning. Other focus areas based on the literature are vision, speech, and robotics. During the analysis these topics are found less interesting in respect supporting security operations centers.

According to the analyses done in chapter 4, that is based on the literature study performed in chapters 2 (security operations center) and 3 (artificial intelligence) the potential of artificial intelligence supporting security operations center activities is enormous. Specifically, the tasks that are performed by SOC analysts' level 1 and potential level 2 can be performed or supported by artificial intelligence. Based on the literature study performed, the results indicate that artificial intelligence can perform these tasks faster and more accurate reducing the workload of SOC analysts' level 1 and level 2. Being able to do more with less affirms the research question that artificial intelligence is able to support human activities within a security operations center. For artificial intelligence to perform human activities completely requires additional aspects like contextual information, self-awareness, and self-consciousness. The primary functional domains for effectively using artificial intelligence, specifically machine learning and expert systems, are in the monitoring and threat intelligence domains.

The Dutch governmental organizations that were interviewed as part of this paper are at the beginning of using artificial intelligence. Some Dutch governmental organizations already have experience with artificial intelligence however not in the security operations center environment. Important when considering artificial intelligence are the organization and technical considerations. These considerations are important to address for artificial intelligence to be effective. The technical considerations discussed in this paper are data set, context, bias, specific task. The organization's considerations are trust, strategy, strategic HR plan, and accountability. The Dutch tax administration, department of Justice and Security, and Rijkswaterstaat have addressed at a corporate level the consideration mentioned above, with the exception of accountability. UWV and the Sociale VerzekeringsBank are discussing the artificial intelligence at a corporate level however have not addressed these considerations.

The organization considerations accountability and trust in respect to artificial intelligence are important from a company's perspective but also require attention on a government level. This is closely related to the position of the Dutch government with respect to artificial intelligence. Embracing artificial intelligence on a government level with a clear strategy and roadmap will help organizations and individuals to adopt artificial intelligence more easily.

Given the benefits of artificial intelligence it is recommended that the Dutch governmental organizations take actions accordingly to integrate artificial intelligence into security operations centers. At a corporate level the recommendations are: 1) define an artificial intelligence strategy and roadmap. This help security operations center to align their initiatives accordingly. This includes ethical and legal aspect; and 2) Develop a corporate HR plan that anticipates the adoption of artificial intelligence.

From a security operations center perspective, the recommendations to adopt artificial intelligence are: 1) Transparency towards security operations center employees. The adoption of artificial intelligence into the security operations center have an effect on the employees. Commitment from the employees is therefore essential for successfully adopting artificial intelligence; 2) Align the security operations center according to the framework of Torres (2015, p. 5). Clear distinction between roles in the security operations center helps to anticipate on further implementations of artificial intelligence. It also provides insight into the areas of constraints for the security operations center; 3) Start with a small artificial intelligence initiative, learn and gradually explore more complex artificial intelligence solutions. All the Dutch governmental organizations actively monitor the environment for security alert using security information & event management (SIEM) tooling. The outcome of SIEM tooling could be used to start a proof of concept using supervised machine learning. Based on the lessons learned further steps can be taken like unsupervised machine learning. Similar in the intelligence domain the outcome of open source intelligent (OSINT) can be used for supervised machine learning.

References

Ami, P., & Hasan, A. (2012). Seven Phrase Penetration Testing Model. *International Journal of Computer Applications, 59*(5), 16–20.

ArcSight. (2010, September 17). ArcSight SOC Process Framework.jpg. Retrieved October 14, 2019, from Micro Focus Community website: https://community.microfocus.com/t5/Archive-Discussion-Board/ArcSight-SOC-Process-Framework-jpg/m-p/1598246#M34155

Autoriteit Persoonsgegevens. (n.d.). Cijfers datalekken 2018. Retrieved June 21, 2019, from https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken/overzichten-datalekken/cijfers-datalekken-2018

Bias. (2019). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Bias&oldid=923919575

Blaster (computer worm). (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Blaster_(computer_worm)&oldid=915621800

Braden, J. (2002). *Penetration Testing—Is it right for you?* SANS Institute.

Breazeal, C. (n.d.). Kismet, the robot. Retrieved October 12, 2019, from http://www.ai.mit.edu/projects/humanoid-robotics-group/kismet/kismet.html

Carroll, J. M. (2005). OSINT Analysis using Adaptive Resonance Theory for Conterterrorism Warnings. *Artificial Intelligence and Applications*, 756–760.

Chopra, R. (2012). *Artificial Intelligence*. S. Chand Publishing.

Cichonski, P. R., Millar, T., Scarfone, K. A., & Grance, T. (2013). Computer Security Incident Handling Guide. *International Journal of Computer Research*, *20*(4), 459.

Craglia, M., Annoni, A., Benczúr, P., Bertoldi, P., Delipetrev, B., De Prato, G., … Vesnić Alujević, L. (2018). *Artificial Intelligence: A European Perspective*. https://doi.org/10.2760/11251

Crowley, C., & Pescatore, J. (2019, July). *Common and Best Practices for Security Operations Centers: Results of the 2019 SOC Survey*. SANS Institute.

Dalzoppo, L. (2018, March). *QRadar Advisor with Watson*. Powerpoint. Retrieved from https://edist.it/wp-content/uploads/2018/05/QRadar-Advisor-with-Watson-Luca-Dalzoppo.pdf

Darktrace. (2019). *Machine Learning in the Age of Cyber AI*. Retrieved from https://www.darktrace.com/en/resources/wp-machine-learning.pdf

Dataflair team. (2019, October 11). History of AI. Retrieved December 14, 2019, from History of Artificial Intelligence – AI of the past, present and the future! website: https://data-flair.training/blogs/history-of-artificial-intelligence/

Department for Digital, Culture, Media & Sport. *Online harms white paper*. , (2019).

DigiNotar. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=DigiNotar&oldid=928251661

Domo. (2019). Data Never Sleeps 7.0. Retrieved December 20, 2019, from https://www.domo.com/learn/data-never-sleeps-7

EnCase. (2019). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=EnCase&oldid=909868900

ENISA. (2019, January 28). *ENISA Threat Landscape Report 2018*. Retrieved from https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2018

Europees Parlement, Raad van de Europese Unie. *General Data Protection Regulation*. , Pub. L. No. 2016/679 (2016).

Exabeam. (2019). SOC, SecOps and SIEM: How They Work Together. Retrieved December 13, 2019, from Exabeam website: https://www.exabeam.com/siem-guide/the-soc-secops-and-siem/

EY. (2014, October). *Security Operations Centers—Helping you get ahead of cybercrime*. Retrieved from https://www.ey.com/Publication/vwLUAssets/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime/$FILE/EY-security-operations-centers-helping-you-get-ahead-of-cybercrime.pdf

Felton, E. (2016, May 3). Preparing for the Future of Artificial Intelligence [Blog]. Retrieved October 14, 2019, from https://obamawhitehouse.archives.gov/blog/2016/05/03/preparing-future-artificial-intelligence

FireEye. (2019). *Threat Intelligence Use Case Series*. Retrieved from https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/sb-soc-analyst-profile.pdf

Gartner. (2018, September 6). How to Plan, Design, Operate and Evolve a SOC. Retrieved November 19, 2019, from Gartner website: https://www.gartner.com/en/documents/3889122/how-to-plan-design-operate-and-evolve-a-soc

Ghallab, M., Nau, D., & Traverso, P. (2016). *Automated Planning and Acting*. Cambridge University Press.

GIGO (Garbage In, Garbage Out) Definition. (n.d.). Retrieved November 15, 2019, from https://techterms.com/definition/gigo

Glassman, M., & Kang, M. J. (2012). Intelligence in the internet age: The emergence and evolution of Open Source Intelligence (OSINT). *Computers in Human Behavior*, *28*(2), 673–682. https://doi.org/10.1016/j.chb.2011.11.014

Granage, A. (2019, March 4). Getting smart about artificial intelligence. Retrieved October 14, 2019, from Wellcome Sanger Institute Blog website: https://sangerinstitute.blog/2019/03/04/getting-smart-about-artificial-intelligence/

Gupta, A., & Sundaresan, N. (2018). *Intelligent code reviews using deep learning*.

Help Net Security. (2018, June 6). Key challenges and frustrations of SOC workers. Retrieved December 13, 2019, from Help Net Security website: https://www.helpnetsecurity.com/2018/06/06/challenges-soc-workers/

Hewlett Packard. (2013, May). *5G/SOC: SOC Generations -HP ESP Security Intelligence and Operations Consulting Services—Business white paper*. Retrieved from http://www.cnmeonline.com/myresources/hpe/docs/HP_ArcSight_WhitePapers_5GSOC_SOC_Generations.PDF

Hewlett Packard Enterprise. (2017, February 16). *The Exponential Growth of Data—Business white paper*. Retrieved from https://insidebigdata.com/2017/02/16/the-exponential-growth-of-data/

Hoffmann, M. (2014, September). *How to build a successful SOC*. Presentation presented at the Protect 2014, Washington, D.C. Retrieved from https://h41382.www4.hpe.com/gfs-shared/downloads-312.pdf

Hosting Tribunal. (2019, May 6). 15 Biggest Data Breaches in The Last 15 Years (Infographic). Retrieved September 16, 2019, from Hosting Tribunal website: https://hostingtribunal.com/blog/biggest-data-breach-statistics/

Hutchins, E. M., Cloppert, M. J., & Amin, R. M. (2011). Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. *Leading Issues in Information Warfare & Security Research*, *1*(1), 80.

Irons, A., & Lallie, H. S. (2014). Digital Forensics to Intelligent Forensics. *Future Internet*, *6*(3), 584–596. https://doi.org/10.3390/fi6030584

Jabbar, H. K., & Khan, R. Z. (2014). Methods to Avoid Over-Fitting and Under-Fitting in Supervised Machine Learning (Comparative Study). *Computer Science, Communication and Instrumentation Devices*, 163–172. https://doi.org/10.3850/978-981-09-5247-1_017

Jacobs, P., Arnab, A., & Irwin, B. (2013). Classification of security operation centers. *2013 Information Security for South Africa*, 1–7. IEEE.

Kali Tools. (n.d.). Kali Linux Penetration Testing Tools. Retrieved October 17, 2019, from https://tools.kali.org/tools-listing

Kaplan, A., & Haenlein, M. (2019). Siri, Siri, in my hand: Who's the fairest in the land? On the interpretations, illustrations, and implications of artificial intelligence. *Business Horizons*, *62*(1), 15–25. https://doi.org/10.1016/j.bushor.2018.08.004

Kelley, D., & Moritz, R. (2006). Best Practices for Building a Security Operations Center. *Information Systems Security*, *14*(6), 27–32. https://doi.org/10.1201/1086.1065898X/45782.14.6.20060101/91856.6

Khan, S., & Parkinson, S. (2018). Review into State of the Art of Vulnerability Assessment using Artificial Intelligence. In S. Parkinson, A. Crampton, & R. Hill (Eds.), *Guide to Vulnerability Analysis for Computer Networks and Systems: An Artificial Intelligence Approach* (pp. 3–32). https://doi.org/10.1007/978-3-319-92624-7_1

Kroes, N. (2011). Data is the new gold. *Opening Remarks, Press Conference on Open Data Strategy Brussels, 12th December*. Presented at the Open Data Strategy, Brussels.

Kuiper, R., Kagie, S., Rorive, K., Rugers, C., Smulders, A., Ben van Zuijlen, & van Os, R. (2017). *An Agile SOC Requires People's Effort* (No. ISSN 1872-4876, volume 12-No. 2). Platform voor InformatieBeveiliging.

Kumar, C. (2018, August 31). Artificial Intelligence: Definition, Types, Examples, Technologies. Retrieved October 14, 2019, from https://medium.com/@chethankumargn/artificial-intelligence-definition-types-examples-technologies-962ea75c7b9b

Litjens, G., Kooi, T., Bejnordi, B. E., Setio, A. A. A., Ciompi, F., Ghafoorian, M., … Sánchez, C. I. (2017). A survey on deep learning in medical image analysis. *Medical Image Analysis*, *42*, 60–88. https://doi.org/10.1016/j.media.2017.07.005

Meenan, C., & Laurens, V. (2015, February). *Building a Next-Generation Security Operation Center Based on IBM QRadar and Security Intelligence Concepts*. Presentation presented at the InterConnect 2015, Las Vegas. Retrieved from https://www.slideshare.net/ibmsecurity/building-a-nextgeneration-security-operation-center-based-on-ibm-qradar-and-security-intelligence-concepts

Mellett, A. (2017, November 17). Legal A.I. – High on artificial, low on intelligence. Retrieved October 14, 2019, from Plexus website: https://www.plexus.co/legal-a-i-high-on-artificial-low-on-intelligence/

Michail, A. (2015). *Security operations centers: A business perspective* (Master's Thesis).

Ministerie van Algemene Zaken. (2019, October 9). *Strategic Action Plan for Artificial Intelligence—Report*. https://www.government.nl/documents/reports/2019/10/09/strategic-action-plan-for-artificial-intelligence

Ministerie van Binnenlandse Zaken en Koningsrelaties. (2016, October 13). *Samenwerking SSC-ICT en Belastingdienst*. Retrieved from https://www.ssc-ict.nl/actueel/nieuws/2016/samenwerking-ssc-ict-en-belastingdienst.aspx

Ministerie van Veiligheid en Justitie. Meldplicht datalekken Wet bescherming

persoonsgegevens. , Pub. L. No. BWBR0036695, Staatsblad van het Koninkrijk der Nederlanden (2015).

Mokhov, S. A., Paquet, J., & Debbabi, M. (2014). The Use of NLP Techniques in Static Code Analysis to Detect Weaknesses and Vulnerabilities. In M. Sokolova & P. van Beek (Eds.), *Advances in Artificial Intelligence* (pp. 326–332). https://doi.org/10.1007/978-3-319-06483-3_33

Nationaal Cyber Security Centrum. (2010, September 20). Pen-testen doe je zo [Whitepaper]. Retrieved October 16, 2019, from https://www.ncsc.nl/documenten/publicaties/2019/mei/01/pentesten-doe-je-zo

Nationaal Cyber Security Centrum. (2019). *CSBN 2019: Ontwrichting van de maatschappij ligt op de loer* (Rapport No. CSBN 2019). Retrieved from https://www.ncsc.nl/documenten/publicaties/2019/juni/12/cybersecuritybeeld-nederland-2019

Nilsson, N. J. (2014). *Principles of Artificial Intelligence*. Morgan Kaufmann.

Nimda. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=Nimda&oldid=908472190

Prabhakar, A. (2017, January). *Powerful but limited: A DARPA persepctive on ai*. Presentation. Retrieved from https://sites.nationalacademies.org/cs/groups/pgasite/documents/webpage/pga_177035.pdf

Raphael, B. (1976). *The thinking computer: Mind inside matter*. Citeseer.

Rempel, J. K., Holmes, J. G., & Zanna, M. P. (1985). Trust in close relationships. *Journal of Personality and Social Psychology*, *49*(1), 95–112. https://doi.org/10.1037/0022-3514.49.1.95

Russell, S. J., & Norvig, P. (2002). *A modern approach*. Prentice Hall.

Schaurer, F., & Störger, J. (2013). The Evolution of Open Source Intelligence (OSINT). *Journal of U.S. Intelligence Studies*, *19*(3), 4.

Schinagl, S., Schoon, K., & Paans, R. (2015). A Framework for Designing a Security Operations Centre (SOC). *2015 48th Hawaii International Conference on System Sciences*, 2253–2262. https://doi.org/10.1109/HICSS.2015.270

Schwab, K. (2017). *The fourth industrial revolution*. Currency.

Schwartz, J., & Kurniawati, H. (2019). Autonomous Penetration Testing using Reinforcement Learning. *ArXiv:1905.05965*.

Shah, S., & Mehtre, B. M. (2015). An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, *11*(1), 27–49. https://doi.org/10.1007/s11416-014-0231-x

Slatman, H. (2019). *A curated list of Awesome Threat Intelligence resources*. Retrieved from https://github.com/hslatman/awesome-threat-intelligence (Original work published 2015)

Slovic, P. (1993). Perceived Risk, Trust, and Democracy. *Risk Analysis*, *13*(6), 675–682. https://doi.org/10.1111/j.1539-6924.1993.tb01329.x

Smolaks, M. (2019, October 14). Three notable examples of AI bias [Blog]. Retrieved November 10, 2019, from The World's Number One Portal for Artificial Intelligence in Business website: https://aibusiness.com/three-notable-examples-of-ai-bias/

Spencer, F. (2018). *Digital Forensics with Artificial Intelligence Internet of Things*. https://doi.org/10.13140/RG.2.2.36612.17280

SQL Slammer. (n.d.). In *Wikipedia*. Retrieved from https://en.wikipedia.org/w/index.php?title=SQL_Slammer&oldid=927744382

Steinhardt, J., Koh, P. W. W., & Liang, P. S. (2017). Certified Defenses for Data Poisoning Attacks. In *Advances in Neural Information Processing Systems* (pp. 3517–3529). Curran

Associates, Inc.

Strom, B. (2018, September 21). Adversarial Tactics, Techniques, and Common Knowledge. Retrieved November 19, 2019, from ATT&CK 101 website: https://attack.mitre.org/

Suarez-Tangil, G., Palomar, E., Ribagorda, A., & Sanz, I. (2015). Providing SIEM systems with self-adaptation. *Information Fusion*, *21*, 145–158. https://doi.org/10.1016/j.inffus.2013.04.009

Swift, D. (2007). *A Practical Application of SIM/SEM/SIEM Automating Threat Identification*. Retrieved from https://www.sans.org/reading-room/whitepapers/logging/practical-application-sim-sem-siem-automating-threat-identification-1781

Tillyard, J. (2018, March 21). The Top 5 Challenges Faced by Security Operations Centers. Retrieved December 13, 2019, from Blog website: https://www.dflabs.com/blog/the-top-5-challenges-faced-by-security-operations-centers/

TNO - innovation for life. (n.d.). Retrieved November 19, 2019, from TNO website: https://www.tno.nl/nl/

Torres, A. (2015). *Building a World-Class Security Operations Center: A Roadmap* (Paper No. Building a World-Class Security Operations Center: A Roadmap).

Trend Micro. (2015). A Global Black Market for Stolen Personal Data. Retrieved December 15, 2019, from https://www.trendmicro.com/vinfo/us/security/special-report/cybercriminal-underground-economy-series/global-black-market-for-stolen-data/

Turing, A. (2004). *The essential Turing: Seminal writings in computing, logic, philosophy, artificial intelligence, and artificial life plus the secrets of Enigma*. Oxford [etc.]: Clarendon Press.

van den Berg, J. (2018). Cybersecurity for Everyone. In *Cybersecurity Best Practices* (pp. 571–583). Springer.

Van Os, R. (2016). *SOC-CMM: Designing and Evaluating a Tool for Measurement of Capability Maturity in Security Operations Centers*.

Vectra. (2019). *How to augment security operations centers with artificial intelligence* [White paper].

Watson. (2019, November 7). Retrieved November 20, 2019, from IBM website: https://www.ibm.com/watson

Appendix a: Interview plan

Interview plan: Artificial Intelligence and Security operation center
Author: Alex Kooistra

Background information
Artificial Intelligence (AI) has made a significant upswing in the recent years. Organizations are integrating AI in their primary and secondary business processes to become more efficient and maximize their operations. The interview is focussed on organizations within the Dutch government with an inhouse Security Operations Center (SOC). The purpose of the interview is to get to understanding on the organizations position on Artificial Intelligence and to what extend Artificial Intelligence can support or take over human activities within a Security operation center.
The interview is conducted in the scope of the executive master's programme in Cyber Security of Leiden University. The main research question of the thesis is: *to what extent can AI take over human activities in a SOC.* The aim of the interview is to understand how the Security operation center is organised and to what extend AI can take over or support human activities within a Security Operations Center.
The outcome and results of the interview will be incorporated in the thesis and compared with the outcome of the literature study on AI and SOCs.

Interview Structure
The duration of the interview is about 60 to 90 minutes. The preferred language is English but upon request of the interviewee the interview can be can be conducted in Dutch. With consent of the interviewee an audio recording will be made. A written interview report, in English, will be shared with the interviewee for comments and corrections. After consent from the interviewee the results of the interview will be incorporated into the theses. The audio recording will subsequently be deleted.
The interview is divided into four sections, which are described below.

Personal information
- Name, gender
- Organization / Department / Function
- Which role best describes you
- Previous functions/ roles in the Security operation center domain
- What is your relation to the Security operation center
- What is your working experience in the Security operation center domain

Security Operations Center
- How would you best describe a SOC
- What was the compelling event that lead to the implementation of the SOC
- How is the SOC positioned within the organization
- Is the SOC based on a specific model and if so, could you elaborate
- What is the size of the SOC, including functions, roles and tasks
- Which services fall under the responsibility of the SOC
- In your opinion, what is the role of the human within the SOC.
- In your opinion, is a SOC capable of keeping up with technologies, market developments and the rapid changing threat landscape.

Artificial Intelligence

- How would you best describe AI
- What is your position on Artificial Intelligence? Specifically, with respect to the different kind of AI.
- Does the organization have a strategy on AI and if so could you elaborate on the strategy.
- What current AI developments are conducted within the company? Are these initiatives related to the primary or secondary business process.
- What are the main reasons to adopt (or not adopt) AI in general and specifically for the SOC.
- In your opinion, what are the main constrains in using AI.
- In your opinion, what are the prerequisites for using AI within the SOC.
- In your opinion, are SOC employees knowledgeable on AI and capable of interpreting and explaining the outcome of AI information
- In your opinion, is AI capable of taking over human activities and if so, could you elaborate.

Concluding remarks

- Any further comments or remarks?

Recording consent form
I, ..., consent to the interview being recorded and this recording being used within the research team in order to facilitate the analysis of the interview. I understand that recordings will be deleted after I have agreed with the transcript made of the recording.
Signature..... Date.....