Artificial intelligence in the cyber security environment

Petri Vähäkainu, Martti Lehto
University of Jyväskylä, Jyväskylä, Finland
petri.vahakainu@jyu.fi
martti.j.lehto@jyu.fi

Abstract
Artificial Intelligence (AI) is intelligence exhibited by machines. Any system that perceives its environment and takes actions that maximize its chance of success at some goal may be defined as AI. The family of AI research is rich and varied. For example, cognitive computing is a comprehensive set of capabilities based on technologies such as deep learning, machine learning, natural language processing, reasoning and decision technologies, speech and vision technologies, human interface technologies, semantic technology, dialog and narrative generation, among other technologies. Artificial intelligence and robotics have steadily growing roles in our lives and have the potential to transform vital functions of the society. Organizations benefit from the ability of cognitive systems to improve their expertise quickly and from sharing it to all those who need it. The know-how of top experts is quickly made available to all, when their subject matter expertise is taught to a cognitive system. Through repeated use, the system will provide increasingly accurate responses, eventually eclipsing the accuracy of human experts. With artificial intelligence, comprehension can be outsourced. As the intelligence of machines improve, they will use deep learning to understand the collective information of humankind. With the use of digital sensor data, equipment based on artificial intelligence can used to develop smart advisors, teachers or assistants. As artificial intelligence technology is helping society to advance, there are risks associated with its use, found in the operating systems, hardware, algorithms, system management, ethics and liability, and privacy. The study focuses on artificial intelligence threats and risks and how AI may help to solve cyber security problems. This study uses taxonomy classification principle to classify 12 the most crucial areas of cyber security. Research method of this study was to gather 11 AI solutions that were divided into seven different categories of the crucial areas of cyber security represented in introduction chapter. AI solutions gathered uses artificial intelligence in detecting and predicting information security threats and anomalies and blocking them. The purpose of this study is to classify AI-based cyber security solutions gathered and provide information what they can offer in solving problems in the field of cyber security.

Keywords: anomaly, artificial intelligence, cognitive abilities, cyber security, supervised machine learning, unsupervised machine learning

1. Introduction

Originally, Artificial Intelligence (AI) was introduced as a concept to mimic the human brain, and to investigate the real-world problems with a holistic human approach. AI has become widely known from creative cinematic and literary works. AI makes it possible to store large amounts of data, and to process that data intelligently. This processing enables the creation of functional tools. AI has been used to provide intelligent applications in various areas, such as defense or space exploration. These areas have rich histories of varied problem-solving approaches. Later, AI has seen application in the healthcare sector. It has been used for such things as diagnoses, treatment recommendations, and surgery treatments. (Kannan 2017) New areas of application for AI include structural health management (SHM), where AI can provide forecasts. This, in turn, translates to savings in repair costs.

Artificial intelligence can be defined as artificially formed intelligence that provides tools for solving complex and demanding problems, on a computer or machine. Artificial intelligence is a combination of information technology and physiological intelligence, which can be computationally used to reach goals. Intelligence is an ability to think by creating memories and understanding, recognizing patterns, making adaptive choices and learning from experiences. AI can make machines behave like humans, but they can be faster and more humane. (Lehto, 2015, 3 - 29.)

The word “cyber” is generally believed to originate from the Greek verb κυβερεω (kybereo) – to steer, to guide, to control. At the end of the 1940s, Norbert Wiener (1894–1964), an American mathematician, began to use the word cybernetics to describe computerized control systems. According to Wiener, cybernetics deals with sciences that address the control of machines and living organisms through communication and feedback. In accordance with the cybernetic paradigm, information sharing, and manipulation are used in controlling biological, physical and chemical systems. (Lehto, 2015, 3 - 29.)

According to Lord (2017) cyber security refers to technologies, processes and practices, which are designed to protect networks, devices, programs and data from attack, damage or unauthorized access. Cyber security may also be referred to as information technology security. Kaspersky Lab (2018) claims that cyber security is a practice to protect computers and servers, mobile devices, electronic systems, networks and data from unauthorized malicious attacks. The concept of cyber security is broad, and it includes everything from information security of personal computers, recovery from various catastrophes, to end-user training. Artificial intelligence has a strong relationship with cyber security. The Finnish cyber security strategy (2013) defines cyber security as a "safe and reliable operating environment and critical infrastructure resilience". Cyber security builds on people's activities, organization processes and information technology.

Organizations are starting to utilize artificial intelligence in cyber security to provide better information security against increasingly skilled attackers. Artificial intelligence assists in automating complex and complicated processes to identify attacks, and to react to information systems breaches. These kinds of applications are developing and becoming more advanced and comprehensive by taking an advantage of artificial intelligence. Machine learning is a core area of artificial intelligence. It refers to technologies that provide a means to teach computers to learn and adapt through experience. This technological component stimulates human cognition, such as learning from experience and patterns instead of reasoning (i.e., cause and effect).

There are many cybersecurity frameworks such as NIST, ISO 27001/27002/27017, Cloud Security Alliance CCM, NERC CIP, HIPAA, ISC2. Most of these security standards groups control the security domains. A classification principle used in this study can be understood as taxonomy. It describes the most crucial areas of cyber security discussed in this study. The following cyber security areas discussed are:

- Infrastructure security
- Endpoint security
- Application security
- IoT-security
- Web-security
- Security operations and incident response
- Threat intelligence
- Mobile security
- Cloud security
- Identity and access management
- Network security
- Human security

This study discusses applications that utilize artificial intelligence from different manufacturers. Applications studied make use of artificial intelligence to predict recognize and prevent information security threats and anomalies. The discussion of applications is intended to give an overview of what kind of cybersecurity solutions that use artificial intelligence exist, and what they can offer to solve problems in that area.

2. Artificial Intelligence

Artificial intelligence can be thought of as an umbrella term. Its purpose is to enable computers to mimic human thinking, to simulate human activities and to solve problems faster and more efficiently than people can solve them. Various tasks, such as creative, planning, moving, speaking, object and sound recognition, social and business transactions can be executed by exploiting AI. To perform tasks, different methods, such as evidence-based methods, natural language processing (NLP), text mining, predictive and prescriptive analytics, recommendation systems, machine and deep learning can be utilized. Methods mentioned above may also be used to solve problems in cyber security. (Buczkowski, 2017.)

Evidence-based thinking refers to a concept or a strategy based on objective evidence. Evidence-based thinking depends on real world experiments or tests, which prove that strategy or a concept has a likelihood to succeed. The information obtained leads the decision-maker in choosing the best way to act. Decision-makers believe that the way of acting should solve a specific problem and lead to a desired result. An evidence-based approach asks a key question: "has such a course of action been proven to be effective for others in similar situations?" Evidence-based decision-making has been, among other things, successfully utilized in medicine. The probability to find correct treatment based on evidence has eliminated uncertainties, as a result, doctors have been able to determine the correct and solid treatment. (Spencer & Lumen Learning.)

Artificial Intelligence also includes Natural Language Generation (NLG), which refers to text information generation from data. NLG is a process in which data is to be interpreted appropriately. NLG works by parsing textual data and presenting the results in the form of natural language. These kinds of tools are used when processing large structured and unstructured datasets. The result of NLG processing is natural language text, which is generated from a combination of gathered data and user-generated input. Natural language processing is the inverse process of natural language understanding (NLU).During NLU, the system reasons how to verbalize the input data, while NLP generates data from a natural language input. (GeeksforGeeks)

3. Cyber Security

Cyber security measures are associated with managing risks, patching vulnerabilities and improving system resilience. Key research subjects include techniques associated with detecting different network behavior anomalies and malware, and IT questions related to IT security. In short, cyber security can be defined as a range of actions taken in defense against cyber-attacks and their consequences and includes implementing the required countermeasures. Cyber security is built on the threat analysis of an organization or institution. The structure and elements of an organization's cyber security strategy and its implementation program is based on the estimated threats and risk analyses. In many cases it becomes necessary to prepare several targeted cyber security strategies and guidelines for an organization. (Lehto, 2015, 3 - 29.)

The important aspect is that necessary preparations against threats will be made, and sufficient protection towardnegative effects of threats will be attempted to be implemented. Preparations against cyber threats can be best carried out by improving the basics of cyber security, increasing everyone's knowledge of threats, improving operational capability and maintaining security. The core issueis to identify the challenges of cyber security and be able torespond appropriately. An important part of cyber security is being able to maintain the ability to function under a cyber-attack, be able to rapidly end the attack and restore the organization's functions to the previous normal state before the incident. Proper legislation and relevant, deeper discourse are needed to solve these issues. Potential countermeasures against cyberattacks have been widely discussed. (Limnéll, Majewski & Salminen, 2014, 107.)

Threats to society's vital functions directly or indirectly targets national systems or citizens, from within or outside the national borders. The threat landscape is a list of threats containing information about threat agents and attack vectors. By exploiting weaknesses or vulnerabilities, threats lead to a loss or takeover of assets. (Lehto, 2015. 3 - 29.)

Threat, vulnerability and risk form an intertwined entity in the cyber world. The underlying system isa valuable physical object, competence or some other immaterial right, which needs protection and safeguarding. A threat is a harmful cyber event, which may occur. The numeric value of the threat represents its degree of probability. Vulnerability is the inherent weakness in the system, which increases the probability of an occurrence or exacerbates its consequences. Vulnerabilities can be divided into those that exist in human action, processes or technologies. Risk is the value of the expected damage. Risk equals probability times the loss. It can be assessed from the viewpoint of its economic consequences or loss of loss at face value. Risk management consists of the following factors: risk assumption, risk alleviation, risk avoidance, risk limitation, risk planning and risk transference. Countermeasures can be grouped into the three following categories: regulation, organisational solutions (i.e. management, security processes, methods, procedures, and security culture) and security technology solutions. (Lehto, 2015, 3 - 29.)

4. Artificial intelligence and cyber security solutions

Artificial intelligence not only includes threats and risk factors, but it can also act as a problem solver. Artificial intelligence and cognitive data processing are used to detect, defend against and examine cyber-attacks.
Modern information security solutions are either man- or machine-made. So-called analytical solutions are based on the rules created by IT security experts, which ignoreattacks that do not match the established rules. Machine-learning-based approaches rely on identifying anomalies that can identify false positive results, creating a sense of mistrust toward the system and thus require human-effort to investigate cases.(Dale, 1995, 6.)

4.1 Security operations and incident response

4.1.1 AI2

MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and PatternEx have developed an artificial intelligence AI2 platform to predict cyber-attacks. According to Conner-Simons (2016), the AI2 platformwas able to reach 86 % accuracy in detecting cyber-attacks, which is approximately three times better than results of previous studies. Tests were conducted with 3.6 billion data components (log lines), which were generated by millions of users in a three-month research period. To prevent attacks, AI2 identifies suspicious activity by applying clustering algorithms to the input data by utilizing unsupervised machine learning algorithms. Hence, the results will be presented to analysts, who confirm which incidents are real attacks. Analysts also incorporate the outcome into platform models (supervised learning) for the next set of data, which enables further learning. The system is also capable of continuously generating new models within hours, which can significantly improve the speed of its detection ability of cyber-attacks. (Conner-Simmons, 2016.)

4.1.2 CylanceProtect

CylanceProtect (Cylance, 2018) is an integrated information security threat prevention tool, which combines the benefits of artificial intelligence with information security controls to prevent malware infections. Information security controls are used to protect against script-based, memory targeted attacks or attacks exploiting external devices. Unlike traditional security tools based on the analysis of signatures and user behavior in identifying security threats in the environment, CylanceProtect:

- Utilizes artificial intelligence (not signatures) to identify and prevent known and unknown malicious software run on terminal devices
- Prevents known and unknown zero-day attacks
- Protects devices without disturbing the end-user

4.1.3 Darktrace

Darktrace is an information security solution, which can help detect and recognize emerging cyber threats that are able to circumvent traditional information security protections. Darktrace uses the Enterprise Immune System technology (EIS) and utilizes machine learning algorithms and mathematical principles in order to detect anomalies within an organization's information network. EIS uses mathematical approaches, which implies it does not need to take an advantage of signatures or rules, and it can identify unknown cyber security attacks that have not been experienced before. EIS has capabilities to identify and respond to most of the proficiently implemented cyber threats, including the insider's threats hidden in the information networks. By utilizing machine learning and mathematics, the EIS can adapt and automatically learn how each user, device and information network behave, in order to identify behaviors that reflect real cyber threats. Darktrace's self-learning technology provides companies with a comprehensive visibility of the information network and allows them to respond proactively to threats and reduce risk. (Darktrace, 2018.)

Instead of defining "bad" behavioral models beforehand and relying on earlier attack methods, Darktrace's machine learning, along with Bayesian probability theory, can automatically model and combine data dynamically and rapidly. Darktrace monitors raw data, such as cloud service interactions, transferred on a network in real time, without disturbing, for example, business operations and transactions. It also provides a direct view to all digital activities by reporting ongoing attacks or anomalies. (Darktrace, 2018.)

Darktrace's core consists of four mathematical engines, which utilize several mathematical approaches, such as recursive Bayesian estimation. The first of three models produce behavioral models for individual people and the devices they use, and for organizations as a whole. When detecting unusual behavior, one or more of these engines sends a message to the threat classifier, whose task is to classify false positive cases and report actual anomalies that can be accurately analyzed. A combination of Bayesian approaches that is correlated and measured by threat classifier enables accurate identification of anomalies within an organizational scale. Darktrace also uses an integrated module (model editor) to monitor and supervise operating principles. This supports the definition of other regulatory policies and models that can be tailored to specific customer identification requirements (e.g., no Dropbox access, no travelling with sensitive information technology to specific countries) (Darktrace, 2018.)

4.2 Web-security

4.2.1 Cyberlytic profiler

Cyberlytic Profiler is a tool developed to detect threats to web sites. The profiler uses artificial intelligence to identify and prioritize cyber-attacks based on the magnitude of the risk to the data. The profiler analyzes all HTTP-based web traffic by analyzing web server requests and responses and generating a comprehensive risk assessment in real time. This assessment can be examined through dashboard user interface. Reports

such as threat analysis, hosts targeted by cyber-attacks, time-based risk distribution, and timeline of the attack, provide an image of exposure to the risk. The profiler prioritizes the workload by informing the user when a high-risk threat has been identified and IT teams responsible for correcting the problem are able to intervene. (Cyberlytic.)

Cyberlytic Profiler utilizes novel types of strategies in analyzing abnormalities from web traffic in order to reduce incidents caused by conventional signatures and rule-based technologies. These methods help to identify the ever-growing and sophisticated cyber threats by reducing the need for human interventions or interactions. Profiler uses a web application and unsupervised machine learning to analyze data streams. Autonomous self-learning algorithms profile normal web traffic behavior by making decisions by themselves. Indicators available are unique to a web server and include trends and seasonal models. Field features include length and distribution of the character sequence. (Cyberlytic.)

By profiling web applications, Profiler is able to determine whether sent requests originate from the normal distribution of an application in a specific web application area. This approach determines how “normal” looks like for a specific organization. As a result, conclusions can be drawn to find a reason, which induces anomalous traffic. By identifying anomalies, highly probable interference can be emphasized; anomalies can be risk-assessed. Profiler uses a patented classifier approach to determine characteristics of attacks for the following types of attacks: SQL injection, cross-site scripting (XSS) and Bash. (Cyberlytic.)

4.2.2 Amazon Macie

Amazon Macie is an information security service that utilizes machine learning. Artificial intelligence provides tools for Macie to find, classify and protect sensitive data on Amazon Web Services (AWS). Macie recognizes sensitive data such as personal information or copyrights. In addition, it is able to monitor how copyrighted material, such as documents, are copied, moved or viewed. Macie has a dashboard view, which helps to conclude how the data has been used or where it has been moved. The service continuously monitors data usage and anomalies and provides detailed alerts if the data is subject to unauthorized usage or unintentional data leakage. Macie can also automatically detect the risk to business data, if the data has been distributed outside the organization without an authorization, or if the data has otherwise been unintentionally accessed. (Amazon Web Services, Inc, 2018.)

Amazon Macie explores data and searches for keyword file formats such as Microsoft Word, Excel, .txt files. Macie compares file format extensions to evaluate data security levels. For example, Macie places .pemfiles in a higher risk category than an ordinary txt-files. In addition, Macie examines information related to files and S3objects when issuing security classification. Macie also utilizes the Amazon CloudTrail service, which logs almost all API requests, and uses these log files when exploring object level S3 API activities. It also gathers data on users and their roles. (Stonefly, 2018.)

4.3 End point security

4.3.1 Deep Instinct

Deep Instinct’s software is designed to protect organization’s mobile devices and services against known and unknown malicious attacks in real time. The software is based on the exploitation of artificial neural networks. With artificial intelligence, Deep Instinct is able to identify malicious software on mobile devices, services and workstations. Using appropriate deep learning algorithms, the software is able to anticipate unrecognized cyber attacks.

Deep Instinct's developers utilized deep learning algorithms in their implementation of the application, which made it possible to identify structures used in malicious software. Deep Instinct is capable of detecting and preventing the execution of malicious software at all levels of the organization. By utilizing deep learning algorithms, Deep Instinct's developers built an extensive neural network in laboratory conditions and taught it with a large set of malicious code samples. Databases with tens of millions of harmful and harmless files were used to teach these neural networks. The result was a prediction model, which could be sent to a device to be protected to provide real time detection and to prevent malicious software. (Selden, 2016.)

The idea is to teach the software to identify combinations of requests and operations referring to malicious software. Deep Instinct’s learning method slices the malicious software code samples into very small snippets, so that the malicious software can be surveyed.

The method is similar to genomic sequencing, since it also consists of tens of thousands of smaller sequences. These sampled pieces are imported into neural networks to teach the network for identification purposes. This kind of a network performs very complex computations, and a GPU cluster has been implemented to help with these computations. A GPU cluster's capability to compute is considerably faster than the CPU's. The result is a fast and statistical neural network that requires little computing power, and which can be utilized in detecting malicious software. (Selden, 2016)

The University of Göttingen conducted a malicious software identification test, which explored up to 16 000 malicious software samples gathered by Siemens CERT, Bit-Defender, McAfee, AVG, Kaspersky, Sophos, among others.". The above-mentioned companies have their own antivirus software, which can reach up to a 61 % average malicious software detection rate, compared with Deep Instinct's average detection rate of 98.86 %. Some of the malicious software samples were already mutated, but in a way that did not permanently affect the behavior of those malicious software. Deep Instinct could identify up to 99.7 % of harmful PDF files and 99.2 % of harmful executable files.". Deep Instinct's application was taught with 8000 malicious samples." (Selden, 2016.)

4.3.2 SparkCognition DeepArmor

SparkCognition DeepArmor is able to detect and prevent the threat of malware, viruses, worms, Trojans and ransomware programs, using mathematical methods such as machine learning and natural language processing. The DeepArmor architecture consists of a small endpoint agent integrated into a cloud-based cognitive engine, as well as a platform exploring threats. The terminal agent identifies and prevents malicious programs and other more advanced threats, regardless of signatures. The agent is designed to protect the client, server, mobile and IoT devices, and to protect integrated information security for an organization. An agent can also be configured to work autonomously without a user interface, providing a security solution for IoT devices. (SparkCognition, 2018.)

The cloud-based cognitive engine of the DeepArmor solution uses a multi-layer filtering process to identify threats. The first layer of protection performs file analysis, as well as application and risk control to quickly identify known malicious or abnormal files. After filtering the detected files, DeepArmor uses cognitive algorithms to scan unknown files and forms threat scores for each file. At the next step and after identifying the threat, the cloud-based management console provides a natural language processing (NLP) tool. Deep NLP not only looks for evidence on the Internet, but also understands the context around threats. DeepArmor is able to distinguish precisely what is harmful based on abnormal cases. (SparkCognition, 2018.)

SparkCognition's Deep NLP technology functions in a way that thousands of pages of relevant information concerning various threats are taken as the base input for SparkCognition's Deep NLP technology. This data is also used to contextualize the threats themselves. NLP technology also explores the Internet for possible evidence of threats, from which an evidentiary summary will be produced. Risk assessment scoring will also be computed based on the known risks. Finally, a threat analysis summary can be produced from the generated information that can be used to form policy strategies and tackle the most relevant issues. (SparkCognition, 2018.)

4.3.3 Vectra Networks Cognito

Vectra Networks Cognito uses artificial intelligence to generate a detailed real time image of current cyber-attacks to react to them. Cognito combines sophisticated machine learning technologies, such as deep learning and neural networks, with continuous learning conceptual models, in order to quickly and efficiently locate hidden and unknown attackers before they cause damage. Cognito also eliminates so-called "blind spots" by analyzing all the information security and authentication systems and SaaS 'applications' network traffic and log files. This provides a comprehensive snapshot of the situation for users and IoT devices concerning running processes on cloud and data centers, preventing attackers from hiding. (Palmer, 2017, 1.) Vectra Cognito uses sophisticated supervised and unsupervised machine learning technologies, such as deep learning and neural networks, in combating cyber-attacks and identifying them. Traditional information security systems attempt to identify cyber-attacks by searching already known signatures and exploits. A cyber attacker can use this information against the system. Cognito learns from the network activity for a long time period, such as days, weeks, or months. Cognito identifies attacker's online behavior at every step of the cyber-attack chain. An attacker's identified behaviour is categorized and compared to ordinary user behavior, using servers that are already risk-assessed. Those who are part of an individual coordinated cyber-attack campaign are identified as exhibiting an attacker's behavior. In this case, the administrators can concentrate on directing their resources to the attacks that pose the greatest business risk. (Palmer, 2017, 1.)

The classification feature and threat presentation provided by Cognito offer the first stage classification feature for information system administrators. By utilizing the relevant information, administrators are quickly able to get a snapshot of attacked servers, without having to examine thousands of different kinds of alerts that would occur in traditional information security systems. (Palmer, 2017, 1.)

4.4 Mobile security

IBM MaaS360 is a mobile device management application developed by IBM that enables all of an organization's personal mobile devices, applications, content management and cyber security. The MaaS360 provides a secure environment that keeps prospective organizations files consisting of commercial secrets distinct from applications installed on a mobile device. This enables employees on organizations to work without endangering both data and device information security. The solution simplifies IT management, as it only needs to monitor the environment controlling an application and not the entire device. (FinancesOnline, 2018.)

Using MaaS360, organizations are able to manage applications through an interactive list, through which they can encourage users to use selected apps, share them with users and update them when needed. In addition, the MaaS360 ensures that corporate data is encrypted and is kept separate from other applications installed on mobile devices. With MaaS360, organizations can also limit employees' data access rights, and only allow heightened access rights for specific duties in a very controlled manner. The environment also provides a calendar for scheduling appointments, as well as a real time chat feature. (FinancesOnline, 2018.)

MaaS360 includes a certain kind of data container built for data management and storage. The container helps to ensure that data is stored on a mobile device rather than on servers, which makes it accessible for service provider personnel. The container also provides tools to ensure that the rights to data processing are regulated on-demand-based basis. The data is encrypted using the AES-256 CTR encryption algorithm, CommonCrypto FIPS 140-2 compliant algorithm (Apple devices) or the SQLCipher + OpenSSL (AES-256) encryption algorithm on Android devices. The software is compliant with General Data Protection Regulation (GDPR) requirements. (IDG Connect Ltd.)

The core of MaaS360 Advisor lays an effective cognitive engine that provides information on relevant alerts regarding emerging security threats. This information is based on both structured and unstructured data and is specific to the organization's industry, size and mobile environment. The Advisor helps organizations to find best practices for employee productivity, recommendations for optimizing IT services and information concerning potential information security risks. (IDG Connect Ltd.)

4.5 Threat Intelligence

IBM QRadar Advisor with Watson applies IBM Watson's cognitive abilities (i.e., artificial intelligence) QRadar Security Platform, a platform designed for information security analysis, to reveal hidden threats and automate the authentication process of threats. The system automatically examines hazardous indicators, utilizes cognitive applies its cognitive abilities for gaining critical insights and ultimately accelerates the reaction cycle to security threats. QRadar Advisor with Watson also uses the features of Watson for Cyber Security to investigate and respond to information security threats. (IBM QRadar Advisor with Watson.)

QRadar Advisor with Watson works through the following steps:

- When the QRadar Security Intelligence platform detects an information security threat, an information security analyst can transfer it to QRadar Advisor with Watson for more precise investigation. The Advisor initiates a wider scanning of information security threats by mining data from local QRadar software. The software will then use Watson for Cyber Security to perform a more thorough analysis of the threat.
- Watson for Cyber Security compiles data from various sources, such as web sites, information security forums and news bulletins, into a human-readable format. On completion, the software searches for additional information-security-related information concerning harmful files and suspicious IP addresses.
- Finally, QRadar Advisor with Watson processes the information it receives from Watson for Cyber Security, seeking for key factors related to information security threats.

The key features of IBM QRadar with Watson are automated threat investigations, usage of Artificial Intelligence and detecting high-level risks. QRadar implements local data mining of information security attacks

by collecting relevant network data. The application investigates whether one or some of the information security threats have passed layered defenses, or if they blocked. By taking and advantage of lists and certain suitable indicators, the inspection can be automated. Cognitive reasoning can identify the most liable threats and connect threats to original events, such as malicious files and suspicious IP addresses, to draw connections between them. QRadar automatically uses Watson for Cyber Security to exploit external unstructured data such as web pages, forums and threat intelligence. IBM QRadar also reveals the criticality of events, like whether a malware code has been executed or not, enabling more efficient time management, in order to examine higher priority risks. (IBM QRadar Advisor with Watson.)

4.6 Human security

User Behavior Analytics (UBA) has been receiving widespread attention in the domain of information security. While developing an organization's protection against external threats, organizations must also protect themselves against threats that may arise from inside an organization. Threats can be caused, for instance, by an employee or an external actor, capable of causing damage in some capacity due to negligent behavior. Such threats are challenging to identity, and may cause significant damage to an organization's property, weakening its intangible assets and consumer confidence and harming an organization's brand or reputation. (Patel, 2017.)

Machine learning algorithms can be applied to understand accustomed end-user behavior and to detect relevant deviations. Such algorithms have been included in IBM's QRadar UBA application for detecting suspicious and anomalous end-user behavior. These machine learning algorithms are able to identify consecutive and time series anomalies. To identify deviations, user's activities are monitored. Based on monitoring results, the norms of behavior, resources and networking utilization operating models are created. These models can be used to determine when the end-user will begin acting abnormally. These algorithms are able to identify and report anomalous behavior and trigger the UBA application, whose user's risk scores are increased on demand. (Patel, 2017.)

By monitoring end-user activity of each organization's information system, the tool is able to identify roles users have in the organization. This implies users can be allocated to role-based peer groups, users can be allocated to role-based peer groups. Unique behavior deviating from these roles can also be identified. Such behavior can be an early indicator of harmful intent. The tool's algorithms function independently and monitor user activity from a variety of points of view, so that the number of false positive results may decrease. (Patel, 2017.) The UBA application runs along with the QRadar system, collecting data from users on the organization's network. The graphical user interface of the UBA application presents data from the Docker container (with a SQLite database). Collectible data include user aliases, latest risk scores, system points, alerts, and trends. The user interface also presents information from the QRadar system. The data provided by the QRadar system is information, status and sources related to the attack. In addition, the QRadar system's ARIEL database provides generic data and user activity records, for instance. The latter corresponds to activities performed with aliases. The UBA application sends information to the QRadarsystem concerning ongoing attacks for more detailed investigation.

Using a predefined ruleset, the application looks for issues that would cause end-users a "sense event", which UBAapplication would then register. The application policies require that events have performed username, and other, tests. At the next phase, UBA reads the senseValue and user ID values from the "sense event", and then increases the user's risk score by senseValue. When the user risk scores exceed the threshold set in the UBAapplication settings, the application sends an event triggering the "UBA: Create Offence" rule in the UBAapplication, creating a policy violation for the specified user.

5. Conclusion

The study was conducted by using a classification principle (taxonomy) to classify the 12 most crucial areas of cyber security discussed in this study. When conducting the study, information on 11 artificial intelligence solutions were gathered. These solutions were divided into following areas: infrastructure security, endpoint security, web security, security operations and incident response, threat Intelligence, mobile security and human security. The solutions studied have extensive coverage of cyber security threats.

At present, several cyber security solutions and tools are available for organization's needs. The challenge is the fragmentation of solutions and tools, as well as the problems of the implementation and maintenance of new systems, which cause management difficulties and increase complexity within the whole system. The

complexity of systems requires the development of integrated systems that identify both external and internal threats, and which have comprehensive, built-in cyber security systems. The system under development must include intelligent analytic solutions within the entire organization's IT infrastructure. The system must be able to perceive both the organization's internal processes, as well as external ones. The IT infrastructure must contain the necessary information security capabilities.

The system should detect and quickly react to symptoms of a network attack, such as an abnormal login to a server containing valuable data, or suspicious usage of cloud services. Novel ways to detect threats are needed, as an organization may face up to 200 000 information security events per day. Investigating events by using human information security specialists is expensive and is time-consuming.

Integrated and holistic solutions provide the required visibility for all levels of the ICT system, which means protection and preventing of cyber-attacks can be implemented as a whole rather than as individual procedures. Artificial intelligence provides great utility in conducting early-stage analysis and observations and detect anomalies. Artificial intelligence is able to process hundreds of thousands of documents and data sources instantly. At present, nearly 8000 articles concerning information security are published each day, whose processing and application requires the use of an intelligent machine and sophisticated tools, such as natural language processing (NLP).

An attacker takes an advantage of siloed organizational solutions that have been compromised, but which have an impact on the organization's entire ICT system. Traditional perimeter old-fashioned information security solutions do not respond to today's sophisticated threats, both within the organization, and outside of it. Within an integrated security system, a strong network information security protection, terminal management and security, active monitoring of data streams, creation of detection capability and preventing attack vectors is created. The system requires the ability to understand the ever-changing field of attacks and novel attack vectors. An intelligent cyber security forms a platform that provides a broad ecosystem of integrated information security solutions. The platform solution enables an effective co-operation between cyber security specialists and an artificial-intelligence-based solution in which the artificial intelligence componentacts as an expert assistant by executing necessary operations, and at the same time produces processed information as a basis for decision-making.

References

Amazon Web Services, Inc. 2018. Amazon Macie FAQ. Amazon. Retrieved to 17.10.2018 https://aws.amazon.com/macie/faq

Buczkowski, A. 2017. What's the Difference Between Artificial Intelligence, Machine Learning and Deep Learning? GEO. Retrieved to 31.5.2017 http://geoawesomeness.com/whats-difference-artificial-intelligence-machine-learning-deep-learning

Conner-Simons. A. 2016. System Predicts 85 Percent of Cyber-Attacks Using Input from Human Experts.Science X network.Retrieved to https://phys.org/news/2016-04-percent-cyber-attacks-human-experts.html

Cyberlytic. The Profiler – AI for Web Security Technical Data Sheet. Cyberlytic. Retrieved to 17.10.2018 https://www.cyberlytic.com/uploads/resources/Technical-Data-Sheet-Final.pdf

Cylance. Continuous Threat Prevention Powered by Artificial Intelligence.CylancePROTEC. Retrieved to 16.10.2018 https://www.cylance.com/content/dam/cylance-web/en-us/resources/knowledge-center/resource-library/data-sheets/CylancePROTECT.pdf

Dale. R. 1995. An Introduction to Natural Language Generation. *ESSLI*.

Darktrace. 2018. Darktrace Enterprise - Detects and classifies cyber-threats across your entire enterprise. Darktrace. Retrieved to 17.10.2018 https://www.darktrace.com/en/products

FinancesOnline. 2018. Financesonline IBM MaaS360 Review. Retrieved to 22.10.2018 https://reviews.financesonline.com/p/ibm-maas360

GeeksforGeeks. Artificial Intelligence | Natural Language Generation. A Computer Science Portal for Geeks. Retrieved to 30.3.2018 https://www.geeksforgeeks.org/artificial-intelligence-natural-language-generation

IBM QRadar Advisor with Watson. What can Artificial Intelligence Do for Security Analysis? IBM QRadar Advisor with Watson.Retrieved to 20.10.2018 https://www.ibm.com/us-en/marketplace/cognitive-security-analytics

IDG Connect Ltd. Preparing for GDPR Compliance with Endpoint and Mobile. IDG Connect Ltd. Retrieved to 22.10.2018 https://reviews.financesonline.com/p/ibm-maas360

Kannan, P. V. 2017 Artificial Intelligence – Applications in Healthcare. Asian Hospital & Healthcare Management.Retrieved to30.5.2017 https://www.asianhhm.com/technology-equipment/artificial-intelligence

Kasperskylab. 2018. What is Cyber-Security?AO Kaspersky Lab. Retrieved to 8.1.2018 https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Lehto,M. 2015. Phenomena in the Cyber World.M. Lehto & P. Neittaanmäki (Edit.) Cyber Security: Analytics, Technology and Automation. Berlin: Springer.

Limnéll, J., Majewski, K. & Salminen, M. 2014. Kyberturvallisuus. Saarijärvi: Docendo.

Lord, N. 2017. What is Cyber Security? Data Insider. Retrieved to 8.1.2018 https://digitalguardian.com/blog/what-cyber-security

Palmer, T. 2017. Vectra Cognito – Automating Security Operations with AI. ESG Lab Review. Retrieved to 21.10.2018 https://info.vectra.ai/hs-fs/hub/388196/file-1918923738.pdf

Patel, M. 2017. QRadar UBA App Adds Machine Learning and Peer Group Analyses to Detect Anomalies in User's Activities. IBM. Retrieved to 23.10.2018 https://securityintelligence.com/qradar-uba-app-adds-machine-learning-and-peer-group-analyses-to-detect-anomalies-in-users-activities

Selden, H. 2016. Deep Instinct: A New Way to Prevent Malware, with Deep Learning. Tom's hardware. Retrieved to 18.10.2018 https://www.tomshardware.com/news/deep-instinct-deep-learning-malware-detection,31079.html

SparkCognition. 2018. A Cognitive Approach to System Protection. SparkCognition. Retrieved to 18.10.2018 https://www.sparkcognition.com/deep-armor-cognitive-anti-malware

Spencer, A. &Lumen Learning. Evidence-Based Decision Making. Principles of Management. Lumen. Retrieved to 9.5.2018 https://courses.lumenlearning.com/wm-principlesofmanagement/chapter/evidence-based-decision-making

Stonefly. 2018. Amazon Macie: Artificial Intelligence for Efficient Data Security. StoneFly. Retrieved to 18.10.2018 https://stonefly.com/blog/amazon-macie-artificial-intelligence-efficient-data-security