https://doi.org/10.2352/EI.2022.34.3.MOBMU-387

Evaluation of AI-based use cases for enhancing the cyber security defense of small and medium-sized companies (SMEs)

Daniel Kant, Andreas Johannsen

Technische Hochschule Brandenburg, Department of Business and Management, Magdeburger Str. 50. D-14770 Brandenburg, Germany

daniel.kant@th-brandenburg.de, andreas.johannsen@th-brandenburg.de

Abstract

Companies are increasingly facing the challenges of a persistent cyber threat landscape. By means of AI, cyber attacks can be efficiently conducted more successful through offensive AI. As for cyber defense, AI can be also utilized against cyber threats (defensive AI). Due to limited resources, especially in small and medium-sized companies (SMEs), there is a need to deploy more effective defensive cyber security solutions. Precisely, the adaptation of AI-based resilient defenses must be driven forward. Therefore, the aim of this paper is to identify and evaluate AI-related use cases with a high impact potential on the cyber security level, while being applicable to SMEs at the same time. In order to reach the research goal, an extensive literature review of several online catalogs, surveys and online platforms was conducted. In conclusion, seven crucial AI-based security features were outlined that are providing a high impact potential to the security level for SMEs. Afterwards, the results are discussed and set into a broader context. Even though AI-based security solutions are providing a large range of advantages, certain challenges and barriers using AI-related security applications are addressed in the paper as well. A high need for usable state of the art AI based cyber security solution for SMEs was identified.

Keywords

Cyber defense, cyber security, AI, artificial intelligence, defensive AI, cyber security applications, cyber security use cases, security use cases, AI-based security applications, SME

Introduction

Artificial Intelligence (*abbrev.*: AI) is enormously pushing economic as well as social developments [29]. It has also become one of the key technologies of digitalization, enabling opportunities as well as risks. According to a Gartner survey [4], 37% of organizations have already implemented AI in some form. In the domain of information and cyber security in particular, AI is considered as a "dual-use potential", meaning AI can be used to enhance cyber attacks and - vice versa - to strengthen the cyber defense [16].

In a positive sense, AI can be utilized for the defense against cyber threats - or protection in general (*defensive AI*) [22]. By means of AI, malware, spam and phishing emails can be detected more accurately. This can significantly increase the level of IT protection. At the same time, AI can make cyber attacks much more efficient and also more scalable. The usage of AI as a disruptive force is often referred to as *offensive AI* [17]. Thus, new possibilities for bypassing authentication procedures are evolving, so are new approaches to cryptanalysis. In conjunction with AI, attacks on IT systems in offices and production can be conducted in a significantly more sophisticated manner [16]. Today, attacks can already be purchased conveniently via the darknet (*malware-as-a-service*) i.e. even expert knowledge is not necessarily required to successfully launch an attack. Hackers are actually using AI for cyber attacks [31]. Therefore, it is absolutely critical for enterprises to deal with the new threats rising through AI. [7].

Conventional rule-based systems are reaching their limits in terms of IT and cyber security, both in terms of detection and defense against attacks: IT security systems that do not use or integrate AI, cannot be persistently sustained at the same level of security and protection. [23]. Research, development and innovation is often initially applied in larger companies having more financial, human and technological resources than small and medium-sized companies. Due to the limited resources, small companies in particular are struggling to introduce and integrate these new emerging technologies. This paper aims to figure out AI-related defensive cyber security features with a high potential use case applicable for SMEs.

AI capabilities for cyber defense

The foundation of today's widespread AI-utilization was especially set in the 20th century establishing Artificial Intelligence as a unique research domain [24]. The rapid development in the last decade is specifically explained by the advances made in *Machine Learning* - and especially in *Deep Learning* [29]. Further reasons for the increasing utilization of AI technologies are the enhanced performance of IT systems, significantly increased data quantity and quality, growing AI experience, more efficient AI algorithms [23] as well as the increased data availability [3]. When AI is used in a positive sense for defense against cyber threats, it is also referred as *defensive AI* [17]. The goal of cyber defense in general, is to withstand attacks from the internet and thus protecting the availability, integrity and confidentiality of companies IT network and infrastructure. Classical security systems work on the basis of rules or signatures without checking the content or context behavior, for instance of data packages. Concerning malware protection, traditional signature-based security systems do detect only 75% to 95% of untargeted mass malware attacks and just 27% of targeted malware cyber attacks [22]. The detection rates of IT systems that do not use any form of AI cannot be sus-

tained at the same level of security and protection when attackers are also using AI methods to attack IT systems [22]. When effectively deployed, AI can make a decisive contribution to the cyber defense domain due to its properties and capabilities. AI methods with an added value against cyber threats are Support-Vector-Machines (SVM), Random Forest (RF), Linear Regression (LR), k-Means, k-Nearest-Neighbor (kNN) and Convolutional Neural Networks (CNN) [23]. These methods are having advantages and disadvantages depending on the data quality and also differ in accuracy [14]. The following abilities make AI a valuable technology in cyber defense and for information security in general, because of:

- efficient evaluation of large data volumes (e.g. log files),
- pattern analysis and recognition,
- anomaly detection (e.g. 10,000 login attempts per second i.e. possible cyber attack detected),
- pattern prediction and forecast (e.g. server shutdown imminent) and
- clustering and categorization (e.g. malware, phishing or spam email).

Objectives and research design

Research question

The paper aims to figure out, which AI-related cyber security use cases can bring added value by increasing the cyber security protection level of small and medium-sized enterprises (SMEs). A first topic overview unveiled, that there are already AI-based cyber security solutions on the market. As for the next step, the added value of AI-related use cases for SMEs had to be figured out. A high added value is given when AI-based features can be implemented with moderate (or less) effort and when the features are of high potential for cyber security in companies. The summarized research question is:

- What are the AI-related use cases having a high impact potential for small and medium-sized enterprises (SMEs) to increase the cyber security and protection level to be implemented or utilized with only moderate effort?

Literature review

The intersection of AI and cyber security has been the scope of various research papers. Our research is mainly based on a literature review. The primary aim was to get a picture about AI-based cyber security use cases. At the same time, we searched for companies experiences concerning AI-based cyber security solutions in published scientific papers. With regard to the academic literature, we reviewed a wide range of online catalogs, namely IEEE Xplore, SpringerLink, ACM Digital Library and ResearchGate. Furthermore, we surveyed non-academic sources including vendor websites, technical blogs, online forums, discussion boards, comparison sites and support platforms. Additionally, we evaluated consulting surveys and studies from Gartner, PwC and IDC.

The main purpose of our search query was to find articles that combine work in three fields. Precisely, the search query contained three parts: (1) AI-related terms, (2) cyber security-related terms and (3) SME-related terms.

Results

The *Capgemini Research Institute* classified twenty different AI-related use cases for cyber security with regard to the three dimensions: *Information Technology (IT)*, *Operational Technology (OT)* and *Internet of Things (IoT)*. Furthermore, all uses cases were "*ranked [...] according to their implementation complexity and resultant benefits (in terms of time reduction)*" [31] (see Figure 1). We initially focused on this study to evaluate suitable use cases in the domain of cyber security for SMEs. Precisely, we reevaluated all use cases from Figure 1 and reallocated them according to their benefit and required adaptability in SMEs on a scale of 1 to 10. Summarizing the results, we figured out the following seven use-cases, in which AI can provide a high added value for SMEs:

- Malware Detection,
- Anti-Exploit Technology,
- Intrusion Detection,
- Endpoint Protection and Response (EDR),
- User/Machine Behavioural Analysis,
- Scoring Risk in a network and
- Security Information and Event Management (SIEM).

In Table 1 on the last page of this paper, each AI-based added value of the seven figured out uses cases is explained in detail. The outlined seven high potential use cases (see Figure 2) scored above 5 in the benefit dimension (high benefits) and are having at least a moderate adaption complexity (score 4 and above). The resulting use cases deviated from the ranking of *Capgemini* [31] in certain use cases with regard to the needs of SMEs. The deviations and differences of our figured out use cases in comparison to the Capgemini study are explained in the following.

In contrast to Capgemini, for the purpose of simplification, no differentiation was made with regard to *IT*, *OT* and *IoT*; the technologies in SMEs are used more equivalent compared to larger companies. Concerning the use case *Endpoint protection*, we added the extended use case *Endpoint Protection and Response (EDR)*, since response abilities of AI can bring an added value here i.e. we consider it also to be a high use case for SMEs. EDR can detect security related incidents on end-devices, which can directly stop an initial cyber threat from spreading among the company's IT network. Also in comparison to the Capgemini study, we have added a further use case: *Security Information and Event Management (SIEM)*. Based on our research, especially for SMEs with less resources, SIEM is considered to be of very high AI-based added value since it has interfaces to a variety of other security features and can be seen as a centralized bundle point, where all security related information come together. Thus, a company can get a brief overview about its cyber security state. *Scoring Risk in a network* is furthermore classified as a high potential use case: in particular SMEs lack of understanding their individual risk profile [13]. *User/Machine Behavioral Analysis* is another use case, AI is considered to bring a added value, mainly by means of anomaly detection. Additionally, AI-based *Anti-Exploit Technology* can provide a benefit, since the exploitation of vulnerabilities is an entry point for attackers to compromise the corporate IT network. Even though, the integration of AI-based *Anti-Exploit Technology* does require at least a moderate adaption effort.

Multiple uses cases were not evaluated as a high potential use case. For instance, *data protection and compliance* can be seen more suitable for larger companies. Although data protection and compliance is also relevant for SMEs (e.g. GDPR), it can be regarded as highly complex due to the required adaption effort. According to *Capgemini*, the use case *Fraud detection* is mainly targeted to reduce financial damage to companies - *PayPal* benefits from this AI-based feature in a particular extent [31][20]. In conclusion, we consider *Fraud detection* also being a use case more suitable for large companies. *Security Orchestration, Automation and Response* (SOAR) is providing a high benefit for companies, but at the same time require a high integration and adaption effort [6]. The use case *Behavioural Analysis to prevent Bot Spam* is also not considered - similar to *Campgemini* - to bring a high added value.

Evaluation and Discussion

Companies lack of understanding AI-related high-potential use cases [31]. The goal of our research was to evaluate AI-related cyber security use cases with a high potential, which are furthermore applicable for SMEs. Available academic resources have shown, that AI techniques already have numerous applications in the cyber security domain and that they are actual utilized by companies - in particular for detecting security related incidents [31].

According to the study from the *Capgemini Research Institute*, 51% of the companies (n=*850*) are using AI already for detection purposes, though the study contains mainly large companies. The same study outlines a 34% utilization of AI within the companies for prediction purposes and barely 18% for response purposes. In another study of the the *German Mittelstand-Digital Program* only 37% of the companies see very high potential in the utilization of AI for IT security (n=35) [15]. Summarizing, it can be estimated that AI is presently utilized unproportionally less in SMEs than compared to larger companies. The concrete cyber threats for SMEs can be very different: besides the classical office IT, adversaries are also focusing on industrial control systems ([11]) - also referred as *Operational Technology (OT)* - and inadequately secured IoT devices [12]).

The utilization of AI-based cyber security features can be highly recommended with regard to the added value resulting in higher detection rates of threads or incidents, and subsequently leading to increased cyber security defense abilities.

AI-related cyber security use cases differ in benefit and complexity. There are security features like *Security Orchestration, Automation and Response* (SOAR) or *Extended Endpoint Detection & Response* (XDR) that provide a high benefit for companies, but at the same time require a high integration and adaption effort [6]. According to *Gartner* (2021) [6], various security features are in different stages of development (from "innovation trigger" to "plateau of productivity"). Therefore, features differ in maturity level. "*Vulnerability Assessment*" is the only security feature according to *Gartner*, that has already reached the highest maturity stage. All security features outlined by *Gartner* are already used or integrated by global vendors. Based on our analysis, we recommend seven use cases having a high potential for SMEs. It can be admitted that there are intersections between uses cases. Similarities of cyber security features (e.g. XDR, EDR, SIEM or SOAR) from namely vendors are perceptible.

It is also still noticeable that there are hardly any technologies in the AI-based security environment that can be introduced with fairly simple effort and complexity, and that have low potential (bottom right quadrant on Figure 2). The related security features should be integrated into the companies infrastructure with high priority to meet the threat landscape [6]. One problem that occurs in evaluating AI-based products is to disclose the concrete benefits of AI functionalities in applications since comparability is not always possible, due to different AI methods or training data being used. The vendors also do not disclose functionalities of certain products or solutions due to market competition reasons (i.e. they can be regarded as a black box). Furthermore, the individual products are using different interfaces - some work exclusively in the cloud, others require a local web server in their own data center.

Another barrier is the architectural complexity in corporate infrastructure that can be seen as a vast challenge [6]. The added value of a concrete AI-based use case can vary since each company is unique and has a individual network infrastructure as well. Therefore, it can be challenging to identify and implement the best fitting product-vendor-combination. In this case, it is advisable to implement "AI-as-a-Service", to utilize resources more efficient. SMEs also lack of required knowledge, but they need to utilize AI methods to stay competitive [9]. The involvement of AI experts is associated with costs for the companies. Especially when integrating AI functionalities into the cyber security environment, expertise in two domains is needed for deploying AI-based security software: within the cyber-security and AI domain.

Another obstacle besides expertise are the high demands on performance and infrastructure: Training an AI model normally requires high computational power in addition to a large database. Security-related historical data, as well as the current state of the systems are furthermore required in order make "intelligent decisions" [14]. In contrast, some SMEs do not have an own IT department.

An additional challenge in practice is the integration of AI solutions into legacy security solutions. Existing IT security solutions are already highly complex. This can be regarded as extremely challenging, especially if when companies are using multiple security solutions at the same time. A study from IDC states, that 26% of the companies are using between 11 to 20 different security solutions at the same time [10].

A further challenge is the degree of autonomy and automatic response abilities of an AI system. Today's security systems still require that security-related events must also be manually observed by human expertise ([21]). Whether an IT security expert is involved in the decision or the cyber security system does this automatically is an important aspect of the effectiveness and cost of the system [23]. With the advent of AI-based systems, decisions could be autonomously made by AI: *Gartner* underlines "*AI's increasing role in augmenting human decision*" [7]. A vast challenge also with regard to autonomy is the comprehensibility of AI's decisions, for instance: "*Why the AI system has blocked certain ip addresses or TCP/UDP ports?*". In the meantime, *Explainable Artificial Intelligence (XAI)* has become a distinct research field of AI [1] [30]. Concerning classification, it is also crucial to consider, that even if an AI system has an accuracy of 99%: in a data set consisting of 1 million entries, an amount of 1000 cases will not be correctly classified. In other words: there will

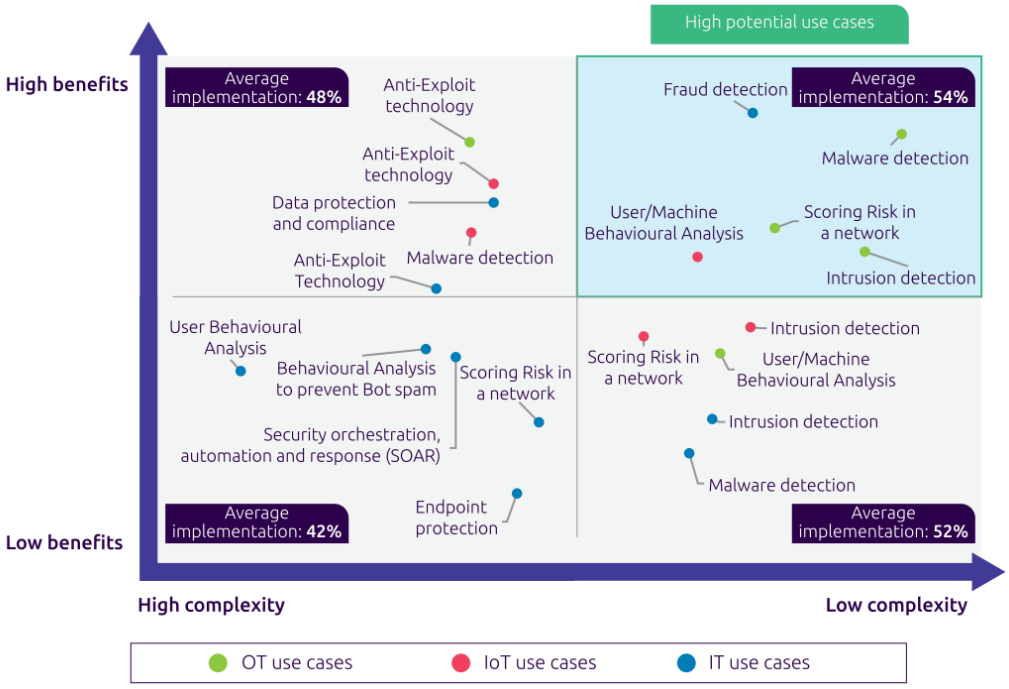

Figure 1. *Potential cyber security uses cases figured out by Capgemini (Source: Capgemini Research Institute [31]*

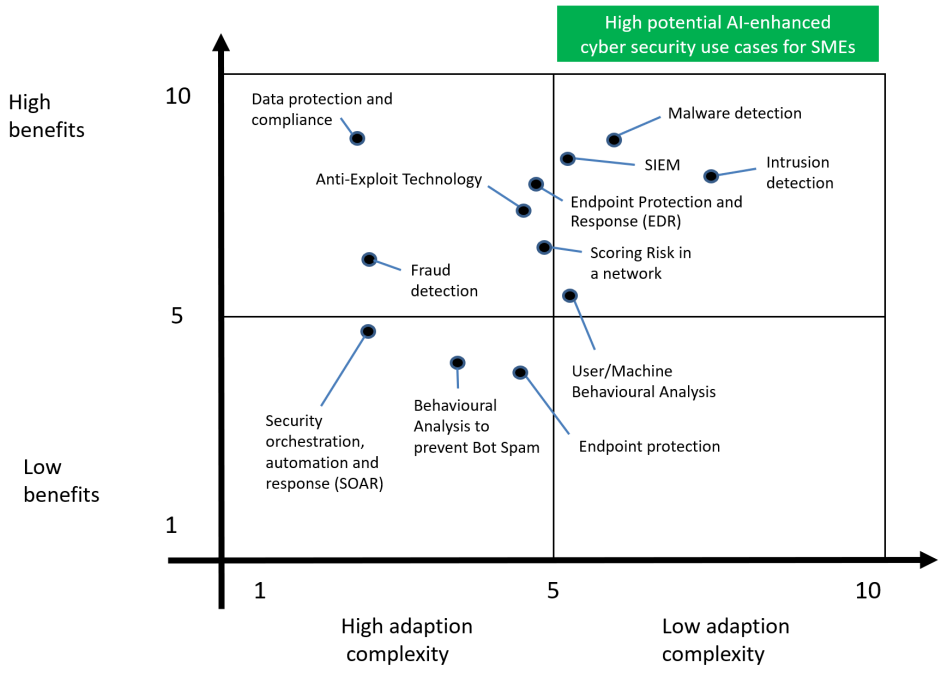

Figure 2. *Recommended AI-enhanced cyber security use cases for SMEs (representation based on [31])*

always be successful cyber attacks or undetected malware bypassing even sophisticated AI-based security mechanisms. A breach should always be regarded as the default state. Thus, technologies like *zero trust* are highly recommended to deploy. Furthermore, Concerning the training process, wrong or malicious training sets can be also deliberately trained. Machine Learning in particular works "*according to the predefined specific features which means that features which are not predefined will escape detection and cannot be discovered*" [14]. This flaw related to *zero-day exploits* and *Advanced Persistent Threats (APT)* - although the detection

of APT attacks via AI is already in the scope of scientific research [32].

Further research

With regard to future work, we recommend the following further research to be conducted by the scientific community. We suggest to conduct a case study with several SMEs that are keen to implement AI-based security solutions. This should be done in order to empirically identify the specific challenges and barriers in detail, that SMEs are facing while implementing AI-based security solutions. Based on these results, we recommend to develop a prototype awareness tool, which specifically sensitizes companies for the risks and barriers of AI integration, in order to cope with the challenges. As for further scientific research, we outline the following research questions with regard to SMEs:

- What are the main challenges and barriers that SMEs are facing when implementing AI-based security solutions?
- What parameters enable SMEs to overcome these challenges and barriers implementing AI-based security solutions?
- How could a concrete (perhaps prototype) solution look like that minimizes the challenges for SMEs in successfully implementing AI-based security solutions?
- What prerequisites are needed to integrate AI-based security solutions into the existing infrastructure, legacy systems or security applications?

Summary and conclusion

The goal of this research was to identify and evaluate AI-related use cases with a high potential impact to the cyber security level, that are at the same time applicable to small and medium-sized companies (SMEs). Throughout the literature review several use cases were identified from which seven could be assigned to provide a high potential The outlined high cases are providing an increased detection rate in general and allow to discover deviating behavior compared to common cyber security solutions. In addition, AI can make a decisive contribution in the prevention of cyber threats. By means of AI, cyber security solutions can achieve a higher protection and security level. In particular, potential correlations can be found in large amounts of data (e.g. in network log files). Besides the benefits concerning cyber security, utilizing AI can also spare personnel expenses in the long term. For instance, in common security systems, incidents must be identified by human expertise while AI can provide an autonomous evaluation and response to the incident.

Our research has also shown that the usage of AI-based cyber security provides not only advantages. There are challenges, particularly when utilizing or integrating AI for the cyber security domain. The deployment of AI security systems require a vast initial investment of personnel time as well as a high level of human expertise because machine learning methods have to be adapted exactly to the respective environment. Furthermore, the implementation of AI-based solutions need high demands on performance and infrastructure because the training of an AI-model requires high computational power and literally a large database. Security-related historical data, as well as the current state of the systems are also required, in order to adequately respond in a smart manner. Concerning classification, it is also crucial to consider, that even if an AI system has an accuracy of 99%, there will always be successful cyber attacks or undetected malware bypassing even sophisticated AI-based security mechanisms. This should be taken into account for the overall risk management. Therefore, architectures like *zero trust* should be applied. Another issue is related to the decision making process: inexplainability can be regarded as a major flaw, when a decision of the AI cannot be comprehended by the user or employee.

Especially SMEs are inadequately positioned with regard to cyber and IT security, because the implementation obstacles can be high as well as time consuming. As an outlook, a combination of AI and human interaction, both in terms of attack and defense, can be assumed. Detection rates of IT systems that do not use AI cannot be persistently be sustained at the same level of security and protection when attackers are also using AI methods to attack IT systems [23]. The research results indicate that on the long term perspective, the usage of defensive AI-based security solutions will be necessary in order to successfully face the challenge of *offensive AI*. Nevertheless, even though well known vendors have initially integrated AI in their security solutions, there is still a need to develop more suitable, usable and state of the art AI-based cyber security solutions especially for small and medium-sized companies, that can be implemented with adequate effort.

Disclaimer

For the information offered in this paper, there is no claim to completeness, quality, accuracy, relevance and correctness. No liability will be assumed for claims built on the confidence or use of this paper.

References

[1] A. B. Arrieta et al. (2019) Explainable Artificial Intelligence (XAI): Concepts, Taxonomies, Opportunities and Challenges toward Responsible AI. URL: `https://arxiv.org/abs/1910.10045` (accessed: 5 Jan 2021)

[2] Artificial Intelligence and Cybersecurity Technology, Governance and Policy Challenges, in: Centre for European Policy Studies (CEPS) Brussels URL: `https://www.ceps.eu/wp-content/uploads/2021/05/CEPS-TFR-Artificial-Intelligence-and-Cybersecurity.pdf` (accessed: 17 Dec 2021)

[3] M. Christen et al. (2020) When algorithms decide for us: Opportunities and risks of artificial intelligence (*transl. from german*) URL: `https://www.researchgate.net/publication/340720749_Wenn_Algorithmen_fur_uns_entscheiden_Chancen_und_Risiken_der_kunstlichen_Intelligenz` (accessed: 24 Nov 2021), p. 55

[4] K. Costello (2019) Gartner Survey Shows 37 Percent of Organizations Have Implemented AI in Some Form. Gartner. Press Releases. `https://www.gartner.com/en/newsroom/press-releases/2019-01-21-gartner-survey-shows-37-percent-of-organizations-have` (accessed: 13 Dec 2021)

[5] S. Dilek et al. (2015) Applications of artificial intelligence techniques to combating cyber crimes: A review. International Journal of Artificial Intelligence & Applications, 6(1), 21–39. URL: `https://aircconline.com/ijaia/V6N1/6115ijaia02.pdf` (accessed: 9 Dec 2021)

[6] P. Shoard and S. Handa (2021) Cycle for Security Operations, Gartner, 2021 URL: https://www.gartner.com/doc/reprints?id=1-27JN2ORV&ct=210928&st=sb#cppdip.748538 (accessed: 7 Dec 2021)

[7] Top 10 Strategic Technology Trends for 2020: AI Security. URL: https://www.gartner.com/en/documents/3981944/top-10-strategic-technology-trends-for-2020-ai-security (accessed: 21 Dec 2021)

[8] K. Gaßner (2019) Machine learning for IT security (*transl. from german*). IN:ARTIFICIAL INTELLIGENCE. Technology application society. Springer Vieweg. Editor: V. Wittpahl. URL: https://link.springer.com/book/10.1007/978-3-662-58042-4 (accesssed: 15 Dec 2021)

[9] E. B. Hannsen and S. Bøgh (2021) Artificial intelligence and internet of things in small and medium-sized enterprises: A survey. URL: https://www.sciencedirect.com/science/article/abs/pii/S0278612520301424 (accessed: 23 Dec 2021)

[10] A. Rüdiger (2021) Too many and complex security systems overwhelm administrators (t*ransl. from german*). heise Verlag. URL: https://www.heise.de/news/Zu-viele-und-komplexe-Security-Systeme-ueberfordern-Administratoren-6237566.html (accessed: 20 Dec 2021)

[11] D. Kant, R. Creutzburg and A. Johannsen (2020) Investigation of risks for critical infrastructures due to the exposure of SCADA systems and industrial controls on the Internet based on the search engine Shodan. In: IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2020. Society for Imaging Science and Technology, USA. URL: https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-253 (accessed: 23 Dec 2021)

[12] D. Kant, R. Creutzburg and A. Johannsen (2021) Analysis of IoT Security Risks based on the exposure of the MQTT Protocol. In: IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia: Enabling Technologies, Algorithms, and Applications 2021. Society for Imaging Science and Technology, USA. URL: https://doi.org/10.2352/ISSN.2470-1173.2021.3.MOBMU-096 (accessed: 23 Dec 2021)

[13] C. Köhler et al. (2021) IT Service Providers as Actors for Strengthening IT Security among SMEs in Germany - Study commissioned by the German Federal Ministry for Economic Affairs and Energy. Publisher: NKMG mbH & BIGS gGmbH. URL: https://www.bmwi.de/Redaktion/DE/Publikationen/Studien/it-dienstleister-als-akteure-zur-staerkung-der-it-sicherheit-bei-kmu-in-deutschland.pdf?__blob=publicationFile&v=10 (accessed: 28 Nov 2021)

[14] J. LI (2018) Cyber security meets artificial intelligence: a survey. Frontiers of Information Technology & Electronic Engineering. Shanghai Jiao Tong University, Shanghai. URL: https://doi.org/10.1631/FITEE.1800573 (accessed: 2 Dec 2021)

[15] Artificial Intelligence in medium-sized businesses: relevance, applications, transfer (*transl. from german*). URL: https://www.mittelstand-digital.de/MD/Redaktion/DE/Publikationen/kuenstliche-intelligenz-im-mittelstand.pdf (accessed: 21 Dec 2021) p. 8

[16] J. Müller-Quade et al. (2019) Artificial Intelligence and IT Security - Stocktaking and Solution Approaches, Publisher: Learning Systems - The Platform for Artificial Intelligence. https://www.plattform-lernende-systeme.de/files/Downloads/Publikationen/2019043_Whitepaper_AG3_final.pdf (accessed: 28 Nov 2021)

[17] Y. Mirsky et al. (2021) The Threat of Offensive AI to Organizations. URL: https://arxiv.org/abs/2106.15764 (accessed: 4 Jan 2022)

[18] R. Pal et al. (2019) On Robust Estimates of Correlated Risk in Cyber-Insured IT Firms: A First Look at Optimal AI-Based Estimates under "Small" Data. URL: https://dl.acm.org/doi/pdf/10.1145/3351158 (accessed: 17 Dec 2021)

[19] T. G. Palla and S. Tayeb (2021) Intelligent Mirai Malware Detection for IoT Nodes. Department of Electrical and Computer Engineering, California State University. URL: https://www.mdpi.com/2079-9292/10/11/1241 (accessed: 14 Dec 2021)

[20] PayPal Inc. (2021) The power of data: How PayPal leverages machine learning to tackle fraud. URL: https://www.paypal.com/us/brc/article/enterprise-solutions-paypal-machine-learning-stop-fraud (accessed: 19 Dec 2021)

[21] N. Pohlmann (2018) Artificial intelligence and cyber security - A basis for discussion (*transl. from german*). URL: https://norbert-pohlmann.com/wp-content/uploads/2019/02/K%C3%BCnstliche-Intelligenz-und-Cybersicherheit-Diskussionsgrundlage-f%C3%BCr-den-Digitalgipfel-2018-Prof.-Norbert-Pohlmann.pdf (accessed: 21 Dec 2021)

[22] N. Pohlmann (2019) Cyber Security. The textbook for concepts, principles, mechanisms, architectures and properties of cyber security systems in digitalization (*transl. from german*). Doi: https://doi.org/10.1007/978-3-658-25398-1_15 (accessed: 26 Aug 2021) URL: https://link.springer.com/chapter/10.1007/978-3-658-25398-1_15 (accessed: 26 Aug 2021).

[23] N. Pohlmann (2019) Artificial Intelligence and Cyber Security - immature but necessary (*transl. from german*). In: T-Sicherheit – Fachmagazin für Informationssicherheit und Compliance. Publisher: DATAKONTEXT-Fachverlag. URL: https://norbert-pohlmann.com/wp-content/uploads/2019/04/393-K%C3%BCnstliche-Intelligenz-und-Cybersicherheit-Unausgegoren-aber-notwendig-Prof.-Norbert-Pohlmann.pdf (accessed: 26 Nov 2021), p. 523-524.

[24] S. Russell and P. Norvig (2009) Artificial Intelligence: A Modern Approach. 3rd Edition. Publisher: Pearson.

[25] Granadillo, Gustavo & González-Zarzosa, Susana & Diaz, Rodrigo. (2021). Security Information and Event Management (SIEM): Analysis, Trends, and Usage in Critical Infrastructures. Sensors. 21. 4759. 10.3390/s21144759. URL: https://www.researchgate.net/publication/

353214895_Security_Information_and_Event_Management_SIEM_Analysis_Trends_and_Usage_in_Critical_Infrastructures (accessed: 23 Dec 2021)

[26] Siemens AG (2018) Siemens heightens industrial cyber security by detecting anomalies. Press release. URL: https://press.siemens.com/global/en/pressrelease/siemens-heightens-industrial-cyber-security-detecting-anomalies (accessed: 7 Jan 2021)

[27] B. Sharma et al. (2020) User Behavior Analytics for Anomaly Detection Using LSTM Autoencoder - Insider Threat Detection. In: IAIT2020: Proceedings of the 11th International Conference on Advances in Information Technology. URL: https://dl.acm.org/doi/pdf/10.1145/3406601.3406610 (accessed: 17 Dec 2021)

[28] B. Soewito and C. E. Andhika (2019) Next Generation Firewall for Improving Security in Company and IoT Network. URL: https://ieeexplore.ieee.org/abstract/document/8937145 (accessed: 2 Dec 2021). Jakarta, 2019

[29] M. Tegmark (2017) Life 3.0: Being Human in the Age of Artificial Intelligence. 1st Edition. Publisher: Allen Lane, London 2017

[30] E. Tjoa and C. Guan (2021) A Survey on Explainable Artificial Intelligence (XAI): towards Medical XAI. In: IEEE Transactions on Neural Networks and Learning Systems Vol. 32. URL: https://ieeexplore.ieee.org/document/9233366 (accessed: 5 Jan 2022)

[31] R. Tolido et al. (2019) Reinventing Cybersecurity with Artificial Intelligence - The new frontier in digital security. Capgemini Research Institute. https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf (accessed: 11 Nov 2021)

[32] X. Yuan (2017) Deep Learning-Based Real-Time Malware Detection with Multi-Stage Analysis. In: 2017 IEEE International Conference on Smart Computing (SMARTCOMP). URL: https://ieeexplore.ieee.org/document/7946997 (accessed: 6 Dec 2021)

[33] B. Yüksel, K. Schwarz and R. Creutzburg (2020) AI-based anomaly detection for cyberattacks on Windows systems - Creation of a prototype for automated monitoring of the process environment. In: IS&T International Symposium on Electronic Imaging 2020 Mobile Devices and Multimedia. Society for Imaging Science and Technology, USA. URL: https://doi.org/10.2352/ISSN.2470-1173.2020.3.MOBMU-331 (accessed: 6 Jan 2022)

[34] N. Ziems; S. Wu (2021) Security Vulnerability Detection Using Deep Learning Natural Language Processing, in: Cornell University. URL: https://arxiv.org/abs/2105.02388 (accessed: 15 Dec 2021)

Cyber security use case (mainly based on [31])	AI-based added value	Description / Example
Malware Detection	higher malware detection rate	AI-based malware detection is superior in detecting malware compared to signature-based approaches [31] [33]. Cyber security solutions based on AI are already used by namely vendors for malware detection within conventional IT infrastructure [8]. Concerning IoT environments, due to AI a protection enhancement can be attested through more accurate detection of malware with also reduced false negatives rate [19].
Anti-Exploit Technology	hinder or prevent vulnerability exploitation	Suspicious data should only be analyzed and executed in sandboxing environments. It is absolutely critical to prevent an attacker as good as possible from exploiting a vulnerability. This can prevent an initial attack or at least diminish the damage extent. Conventional methods have shown to work inefficient [34]. By means of *Deep Learning*, significantly higher results in detecting and classifying software vulnerabilities can be achieved [34]. According to *Gartner*, vulnerability assessment has a high market maturity already [6].
Intrusion Detection	increased detection rate of cyber attacks	There are a variety of AI techniques (e.g. adaptability to the environment [2]) that have major advantages for intrusion detection and prevention [5]. Especially for *Operational Technology* (OT) there is seen a high potential use case for intrusion detection to defend against cyber attacks in real-time [31]. *Deep Learning* can detect nonlinear correlations hidden in the data and detect unknown attacks, which is an "attractive advantage in cyber security defense" [14]. AI-based intrusion detection can also significantly reduce the time, cyber attacks remain undiscovered in the network [2]. Furthermore, AI-based Intrusion Detection is already used by namely vendors [8] as well as by industrial companies [26].
Endpoint Protection and Response (EDR)	higher detection of security incidents	EDR is a category of tools and techniques used to protect computer hardware (e.g. desktop computer, laptops or IoT devices). They detect potentially malicious activity on clients and servers in a network by continuously monitoring all connected endpoints. This ability is crucial to rapidly respond in real time and stop incidents from spreading and extending [6].
User (/Machine) Behavioural Analysis	detection of abnormal behavior of systems or users	With the help of *Deep Learning*, a deviation from a "normal use" can be detected. This relates to machines as well as human users. One major weakness of conventional firewalls is that they are not check the content of packages [28]. Next Generation Firewalls are able to check the behavior and content of a data packet, and they also perform significantly better against threats from the internet [28]. Especially within IoT environments, the behavior-based technology allows detecting and blocking cyber-attacks more accurate [31]. AI can also improve the detection rate based on user behavior: with regard to human users, compromised accounts can be detected due to suspicious behavior [31]. A study showed an insider threat detection rate of approx. 90% [27].
Scoring Risk in a network	classify and prioritize risks (extent, urgency etc.)	The risk score provides a comprehensive overview of the IT risks. AI can help to identify and prioritize security related risks [31]. AI-based approaches do already exist to assess cyber-risks in IT firms [18]. A major advantage: less personnel (e.g. IT specialists) would be required for evaluating risks.
Security Information and Event Management (SIEM)	centralized detection, classification and evaluation of security incidents and alerts	A SIEM combines security-information-management and event-management for real-time analysis of security alerts from software and network components. Recognizing the cyber security threat situation can significantly provide better management of incidents [23]. Traditionally, alerts and events from IT security systems have required additional human analysis. AI can be a great added value, for example to bundle security-relevant information in real time, evaluate and prepare it in a way that is understandable for everyone (even without technical background). An AI-based SIEM can decide whether human intervention is required concerning an incident (partial autonomy) [25]. This can release additional resources.

Table 1. **AI-related cyber security use cases (based on [31]) with an added value for SMEs**