Cyber Threat Analytics in Data Science: Intrusion Detection And Prevention Systems

Özgür TONKAL

Samsun University

To Cite This Chapter

Tonkal, O. (2024). Cyber Threat Analytics in Data Science: Intrusion Detection And Prevention Systems. In M. H. Calp & R. Bütüner (Eds.), *Current Studies in Data Science and Analytics* (pp. 97–108). ISRES Publishing.

Introduction

In recent years, the enormous increase in the volume of data in the digital world has necessitated the development of new approaches and solutions in the field of cyber security. Traditional security methods are insufficient against dynamic and constantly changing threats. At this point, data science comes into play with its powerful analyzing capabilities. By using machine learning, big data analytics and artificial intelligence techniques, it has become possible to not only detect but also predict attacks. This strong relationship between data science and cybersecurity plays a critical role in creating a more effective and proactive defence mechanism.

Data science is used to detect cyber attacks and learn the patterns of these attacks by analysing large amounts of structured and unstructured data. The data used in cyber security spans a wide range of areas such as user activities, network traffic and system logs. Analyses made on this data enable earlier detection of attacks and faster response to threats. Thus, data science techniques play a critical role in managing cyber security threats more effectively and making security solutions more flexible.

Nowadays, cyber-attacks are becoming more sophisticated and harder to detect. Traditional signature-based security systems are weak against unknown or newly derived attacks, as they can only protect against previously identified threats. Therefore, modern cyber security solutions need to be more proactive and predictive. Cyber threat analytics helps detect and prevent attacks by bringing data science into play to fulfil this need (Agbadoku, 2024).

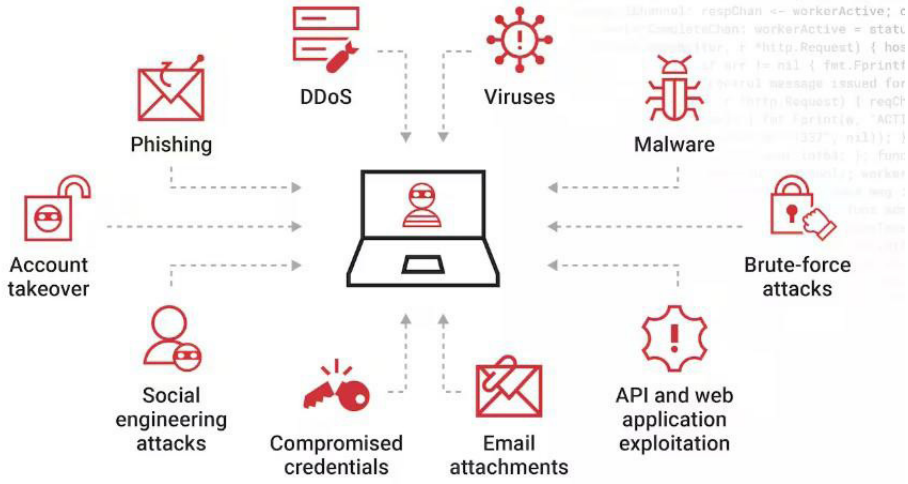
Data science offers a powerful analytical tool for identifying threat patterns and predicting potential attacks based on historical data of cyber security incidents (Babu et al., 2018). Machine learning and deep learning algorithms, in particular, can detect anomalous behaviour, go beyond known threats to recognise new types of attacks and provide real-time intervention. This enables organisations to minimise security risks and make better strategic decisions. This section will focus on how data science is used in cyber threat analytics. Firstly, data science techniques used for the detection and prevention of cyber threats will be analysed in detail. In particular, how data science approaches are integrated into critical security structures such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) will be emphasised. In this context, important techniques such as machine learning, big data analytics and anomaly detection methods will be elaborated. The aim of the chapter is to understand the critical role of data science techniques in cyber security and to illustrate how these techniques are applied in practice. It also aims to provide readers with an understanding of the current state of cyber security

analytics and a glimpse of where the field may evolve in the future.

Cyber Threats and Their Categories

Cyber threats are constantly evolving and diversifying. More complex attack techniques emerge every day and new ways are discovered to bypass organizations' cybersecurity systems. Figure 1 shows cyber attack vectors. While attack vectors are increasing day by day, the main types of cyber threats are as follows: (Chakraborty et al., 2023)(Kashif et al., 2018)

Figure 1
Cyber Attack Vectors



Distributed Denial of Service Attacks (DDoS):

DDoS attacks aim to render the system unserviceable by sending excessive amounts of traffic to a specific target. This type of attack can be detected, especially with big data analytics techniques. Abnormal increases in network traffic can be analyzed by machine learning algorithms to quickly determine whether there is a DDoS attack (Tonkal et al., 2021).

Malicious Software (Malware):

Malware includes types of software that aim to cause damage by gaining unauthorized access to systems. Data science techniques, especially big data and anomaly detection methods, can detect unusual activities in file and network traffic. In this way, unknown malware can be uncovered more effectively.

Phishing:

Phishing attacks force users to share sensitive information via deceptive emails or websites. By analyzing such attacks, data science can detect recurrent patterns in the email content. Natural language processing (NLP) techniques are commonly used in the automatic classification of phishing emails (Alhogail & Alsabih, 2021).

Zero-day Attacks:

Zero-day attacks are attacks carried out before software vulnerabilities are discovered. While such attacks are extremely difficult to detect, machine learning algorithms can identify potential zero-day attacks by analyzing anomalies in network traffic.

Insider Threats:

These are threats carried out by malicious employees or those at risk of data leakage.

Behavioral analytics and anomaly detection techniques used in data science have the potential to detect these threats in advance.

In addition to the above, there are many other types of cyber threats such as SQL injection, advanced persistent threats, etc. (Figure 1). Addressing these diverse and dynamic threats requires a proactive cybersecurity approach, and data science plays a crucial role in this approach. Each type of threat offers a rich source of data that can be analyzed with data science. These data sources include a wide range of information such as system logs, user behavior, and network traffic, and can provide effective results when the right algorithms are used (Ávila et al., 2021).

Cyber Threat Analytics in Data Science

Data science plays a key role in cyber threat analytics emerging in the process of earlier detection and prevention of attacks. Machine learning, big data analytics, and other data science approaches are used to detect attacks and prevent threats proactively. Thanks to these methods, attacks that cannot be detected by traditional methods can be recognized and security strategies can be made more proactive.

Machine Learning: In cybersecurity, machine learning is one of the most critical tools used to detect threats quickly and effectively. Machine learning algorithms predict future threats and detect anomalies by learning from historical data. In particular, supervised, unsupervised, and reinforcement learning models are used to detect anomalies in network traffic and user behavior (Martínez et al., 2019).

- ***Supervised Learning***: Learning from large data sets in which attack types are labeled. For example, to identify phishing emails, models can be built that classify spam and secure emails.

- ***Unsupervised Learning***: Especially effective at detecting previously unseen threats, such as zero-day attacks. Studies unusual behavior in network traffic to detect anomalies.

- ***Reinforcement Learning:*** It is a powerful artificial intelligence method that enables systems to react faster and proactively against threats in areas such as attack detection, malware classification, and the development of dynamic defense strategies in cyber security.

Big Data Analytics: Large amounts of data need to be analyzed to detect cyber security threats. Data from sources such as network traffic, user activities, and system logs are processed and analyzed with big data tools. Big data analytics plays a critical role in understanding large-scale threats, especially DDoS attacks (Alani, 2021).

Anomaly Detection: Anomaly detection is one of the most important applications of data science techniques. Identifying deviations from normal is important for the early detection of threats. For example, a user's unusual login to the system or unusual network traffic may be a sign of a potential attack. Anomaly detection algorithms can automatically recognize these deviations and alert the system(Kaur et al., 2013).

Deep Learning: Deep learning algorithms play an important role, especially in detecting more complex attacks and analyzing data in greater depth. In particular, deep learning techniques are used effectively in advanced malware detection and the identification of anomalous network traffic patterns(Kimanzi et al., 2024).

Intrusion Detection Systems (IDS)

Intrusion Detection Systems are critical cyber security systems that monitor network and system traffic to detect potential security breaches or attacks. **Figure 2** shows the placement of IDS in the network structure. Advanced data science techniques, especially machine learning and big data analytics have become essential components of modern intrusion detection systems. IDSs are generally based on two basic approaches: signature-based and anomaly-based detection systems.

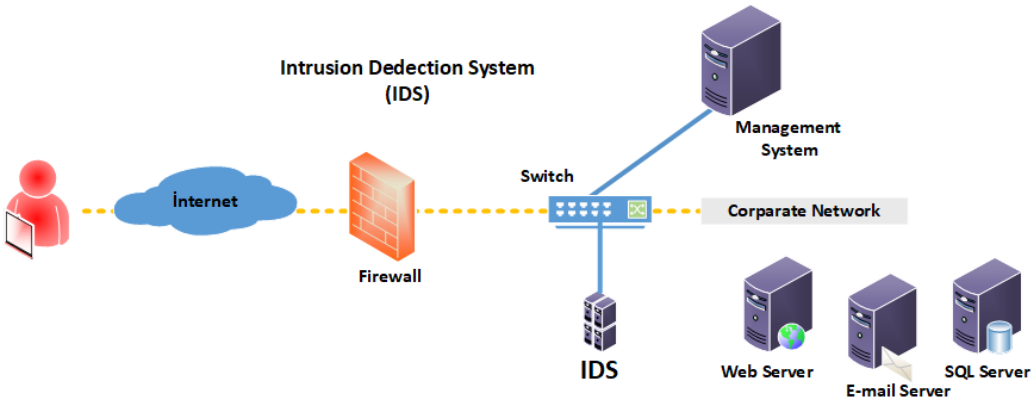
Signature-based IDS: These systems use signatures (pre-defined attack patterns) of known threats to detect threats. For example, if a particular piece of malware is infecting the system, the signature that contains the characteristics of this software will be detected by the IDS and an alert will be issued. However, signature-based systems cannot detect new threats, such as zero-day attacks, because they can only detect previously identified threats.

Anomaly-based IDS: An anomaly-based IDS learns the normal patterns of behavior of the system and issues an alert when there is a deviation from that normal behavior. Because these systems assume that any anomaly can potentially be a threat, they are more effective at detecting unknown threats.

IDS systems are generally divided into two categories: Network-based IDS (NIDS) and Host-based IDS (HIDS). **NIDS** detects threats by analyzing network traffic and **HIDS** analyses events on a specific device or system.

Figure 2

IDS Network Placement



Machine Learning Based IDSs

While classical IDS systems use specific rules and signatures to detect threats, machine learning-based IDS systems learn attack patterns by analyzing data and detecting threats accordingly. The advantages offered by machine learning-based IDSs are as follows:(Suthishni & Kumar, 2022)

- ***Detect New Attacks:*** Machine learning-based IDSs can even recognize previously unseen attacks by using the information they learn from data sets. This is the biggest advantage over signature-based systems. Unsupervised learning techniques enable these systems to detect known threats as well as zero-day attacks.
- ***Higher Accuracy Rate:*** Machine learning algorithms can analyze very large data sets and identify anomalies more accurately. By better understanding attack patterns and continuously updating the system, false positive and false negative rates are reduced.
- ***Dynamic and Adaptable Systems:*** While traditional IDSs are based on static rules, machine-learning-based systems are constantly updated with new data. This allows systems to adapt to new types of threats over time. In addition, such

systems can be continuously trained and become more effective over time.

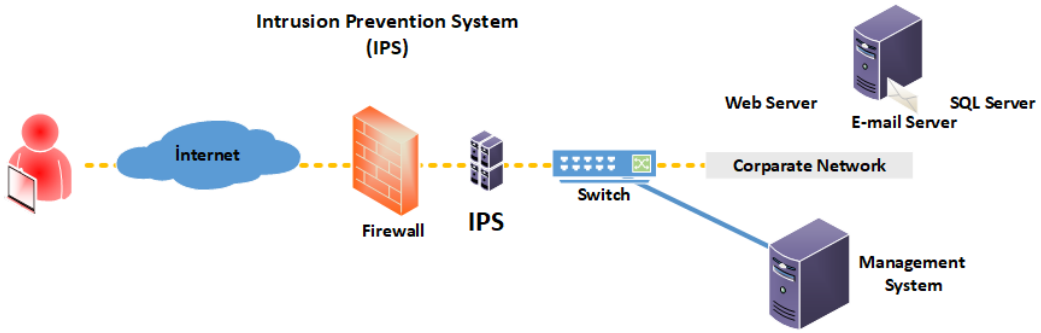
- ***Real-Time Analysis:*** IDSs powered by machine learning can quickly process large amounts of data and detect threats in real time. This provides a critical advantage, especially against fast-moving threats such as DDoS attacks.

Machine learning-based IDSs protect systems against threats using both supervised and unsupervised learning techniques. While supervised learning creates datasets for known threats, unsupervised learning attempts to find previously undetected threats through anomaly detection.

Intrusion Prevention Systems (IPS)

Intrusion Prevention Systems (IPS) not only detect threats by monitoring network traffic and system activity but also actively respond to these threats. **Figure 3** shows the placement of IPS in the network structure. When IPS identifies a potential attack, it takes steps such as stopping, blocking, or limiting harmful activity. IPSs go one step beyond IDS systems and automatically respond after detecting threats (Jayalaxmi et al., 2022). These systems can work as network-based (NIPS) and host-based (HIPS).

Figure 3
IPS Network Placement



Data Science and Proactive Defence

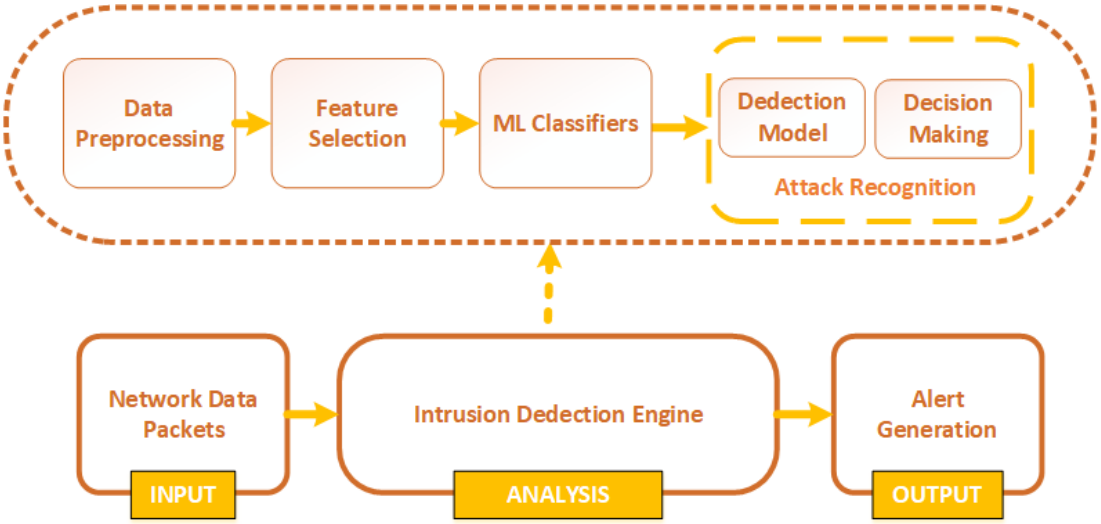
Data science tools enable attack prevention systems to be more proactive. Using machine learning, big data analytics, and anomaly detection algorithms, potential threats can be predicted before they occur. This allows systems to take faster and more accurate steps to prevent attacks. Predictive analyses and learning models, especially those used in data science, help to identify future threats in advance and close security gaps. Thus, IPS systems are not only reactive but also proactive defense mechanisms.

IPS and Deep Learning

Deep learning enables IPS systems to become more sensitive and comprehensive. Deep learning algorithms, especially working on large data sets, better analyze anomalies and are highly effective in identifying complex attack patterns. Deep learning-based IPS systems achieve significant success in detecting unknown threats and responding quickly to advanced attacks. These techniques enable systems to continuously improve themselves and create stronger defenses against new types of threats (Jayalaxmi et al., 2022).

Figure 4

Threat Analysis Process with Data Science



Explanatory Note: Figure 4 shows a model showing the application steps of these methods. The process that starts with the collection of network traffic continues with the processing of data and the training of different learning models.

The trained model can detect/block unauthorized access and inform the network administrator. The stages in the model are explained below:

Data Collection

Collecting data from different sources like network traffic, user activities, and system logs into a data lake. The main data sources are:

- ***Network Traffic:*** Packet logs and network activity provide critical data for the detection of network-based attacks.
- ***System Logs:*** User activity, transaction logs, and file access information are used to identify system threats.
- ***User Behaviour:*** Data used to detect abnormal user behavior, helping to understand insider threats.
- ***Security Incidents:*** Incident data from security incident management (SIEM) systems is an important source for threat analysis.

Data Pre-processing and Cleaning

In order to make effective analyses in threat detection, pre-processing of raw data is required. Data pre-processing stages include the following:

- ***Data Cleaning:*** Cleaning erroneous, incomplete, or duplicate data helps to achieve more accurate results.
- ***Data Transformation:*** The transformation of data into a form that can be analyzed. Especially for network traffic data, it is important to normalize the different protocols.
- ***Feature Selection:*** Selecting meaningful features from data critical to threat detection improves the performance of algorithms.

Modelling and Algorithms

Data science algorithms for threat detection and prevention work effectively on large data sets to detect attack patterns. These algorithms are used both in dealing with known threats and in detecting new and unknown attacks. Here are the three main algorithms commonly used in threat analytics and their details in cyber security applications:

Decision Trees

- Decision trees are a branching data modeling technique that reveals how to reach a conclusion based on various conditions. These algorithms create branching

points by using features in the data set and terminate the final classification at a leaf node. They are one of the most widely utilized methods for intrusion detection for the following reasons:

- ***Easy Interpretability:*** Decision trees are highly transparent in explaining how attacks are identified. By analyzing the branching points in the decision tree, security analysts can discern which decisions lead to specific conclusions.
- ***Minimal Data Preparation:*** Decision trees can operate with limited data preprocessing requirements, which is advantageous when working with large and diverse data sets.
- ***Efficiency and Speed:*** Decision trees run quickly and can effectively process extensive data sets. Moreover, they enable the instant detection of attacks by providing rapid results.
- ***Applications Areas****:* Decision trees are widely used, especially in the detection of DDoS attacks, malware classification, and phishing attacks

Support Vector Machines (SVM)

- Support Vector Machines (SVM) is an algorithm that shows high success in classification problems. SVM finds the hyperplane that provides the widest range between data points in order to classify them. Important advantages of SVM in cyber threat detection are as follows:
  - ***High Accuracy****:* SVM is very successful in large data sets containing many features thanks to its ability to work with complex data structures. It offers high accuracy, especially in problems such as network anomaly detection.
  - ***Efficiency on Small and Large Datasets****:* SVM can operate efficiently on both small and large data sets. This feature is especially advantageous in security projects with limited data sets.
  - ***Overfitting Robustness****:* SVM, when properly optimized, reduces the risk of overfitting and provides more general solutions. This is an important factor in the ever-changing nature of cybersecurity threats.
  - ***Applications Areas****:* SVM is widely used in anomaly detection, spam email detection, malware detection, and network traffic analyses.

Neural Networks

- **Neuronal networks** are a technique that works by modeling neurons in the human brain and are particularly used in deep learning algorithms. Applications of neural networks in cyber security perform better, especially on large and complex datasets:
  - ***High Performance with Deep Learning****:* Neural networks have the ability to learn more complex attack patterns with deep learning methods. It provides great success, especially in the detection of zero-day attacks. Deep learning can detect hidden patterns of attacks using multilayer neural networks.
  - ***Compatibility with Big Data****:* Neural networks work well with large and complex data sets. In systems with continuous data flow, such as cyber security, deep learning methods can constantly update themselves by learning from this data flow.
  - ***Feature Engineering****:* Neural networks, unlike other algorithms, reduce the need for feature engineering. That is, the model can learn by automatically discovering features. This eliminates the hassle of manually selecting features in big data.
  - ***Application Areas****:* Neural networks are widely used in malware detection, intrusion prevention systems, network anomaly analysis, and phishing attack detection.

All of these algorithms are used to more effectively detect and prevent cyber security threats. The advantages and weaknesses of each algorithm can be optimized for particular use cases. For example, neural networks are effective for large data sets and complex patterns, while decision trees provide more explainable and faster results. Support vector machines, on the other hand, provide accurate and robust results in complex classification tasks.

Real-World Applications and Case Studies

The success of data science techniques in detecting and preventing cyber threats has been demonstrated in many sectors and different security scenarios. Here are some examples of successful applications using these techniques (Opara et al., 2022):

Google's Security Solutions: Google uses advanced machine learning techniques to protect its users' data. In particular, machine learning-based algorithms have achieved great success in spam filtering, detecting phishing attacks, and monitoring abnormal account activity. Billions of emails are analyzed every day and advanced models are applied to protect users from fake or malicious content (Google Cloud security solutions, 2024).

Darktrace: Darktrace, an artificial intelligence and machine learning-based cybersecurity company, focuses on preventing cyberattacks by monitoring network traffic and performing anomaly detection. The company uses self-learning algorithms to detect threats from both inside and outside. Darktrace has helped protect many large companies from cyber attacks (Darktrace Security Solutions, 2024).

IBM Watson for Cyber Security: IBM is using its Watson AI system to analyze cybersecurity threats. By examining large amounts of structured and unstructured data, Watson can make fast and accurate analyses to identify threats. It is especially successful in detecting phishing attacks and ransomware. Watson analyses cyber threat intelligence data and provides recommendations to security analysts (Artificial intelligence (AI) cybersecurity, 2024).

Machine learning and anomaly detection algorithms are among the critical tools for detecting and stopping such attacks in the early stages. Table 1 lists the recent cyber security attacks and the measures taken.

Table 1
Cyber Security Attacks and The Measures Taken

Attack	The Effect	Data Science Method
WannaCry Ransomware Attack (2017) (The WannaCry ransomware attack, 2017).	It is a major ransomware attack that affected more than 200,000 systems all over the world in 2017. It targeted Microsoft Windows operating systems using a security vulnerability called EternalBlue.	**Early Detection with Machine Learning:** Machine learning-based IDS systems have been able to detect threats in the early stages of an attack by detecting unusual activities in the network. In particular, abnormal file movements and system behavior have been successfully detected by neural network algorithms. **Malware Analysis with Data Analytics:** WannaCry's propagation process was analyzed by data mining with malware analysis tools.

Target Data Breach (2013) (Pigni et al., 2017).	Target, one of the largest retail chains in the US, suffered a data breach in 2013 in which the credit card information of 40 million customers was stolen as a result of a cyber-attack.	**Anomaly Detection:** If anomaly detection systems had been able to detect abnormal data movements in the network during the attack, it may have been possible to stop the breach at an early stage. Analyses conducted after the breach revealed the importance of data anomaly monitoring techniques during the attack process. **ML to Prevent Credit Card Fraud:** In the aftermath of the attack, many financial institutions have made machine learning-based fraud detection systems more effective to prevent the misuse of stolen credit cards. These systems stopped fraudulent activity by analyzing unusual shopping activity.
SolarWinds Attack (2020) (Kruti et al., 2023).	It is a supply chain attack that took place in 2020 and affected many US government departments and large private companies. Attackers were able to infiltrate networks by placing a malicious update to SolarWinds' Orion software.	**Anomalous Behaviour Detection:** Abnormal network activity on systems using SolarWinds software was detected by data science-based anomaly detection algorithms. **Attack Pattern Recognition:** Deep learning algorithms have enabled a clearer understanding of the size of the attack by recognizing the patterns that attackers follow in networks. Especially due to the sophisticated nature of the attack, early detection of attacks has been possible with big data analyses
Colonial Pipeline Attack (2021) (Beerman et al., 2023)	It is one of the largest pipelines supplying fuel to the east coast of the USA and was attacked by ransomware in 2021. This attack, carried out by a cybercrime group called DarkSide, caused large-scale fuel disruptions in the US.	**Ransomware Detection**: Machine learning and big data analysis were used to detect ransomware infiltrating the Colonial Pipeline system. In particular, the detection of ransomware activity was based on unusual changes in system behavior during the attack. **Early Warning with Anomaly Detection**: Post-attack analysis has shown that systems can be better protected by detecting abnormal behavior on the network using big data and machine learning techniques. **Forensic Analysis After the Event**: After the attack, big data analytics was used to understand how the attack was carried out. Analyzing log data from the systems and the paths taken by the attackers revealed how the attack took place in the supply chain and which vulnerabilities were exploited.

These real-world examples illustrate how data science techniques are being used effectively to combat cyber threats. Machine learning, big data analytics, and anomaly detection techniques play a vital role in the detection and prevention of modern attacks.

Conclusion and Future Trends

This chapter provides an in-depth overview of the intersection between data science and cyber security, including cyber threat analytics, intrusion detection, and prevention systems. Firstly, the role and importance of data science in cyber security is discussed. Cyber threat analytics stands out as a critical tool to deal with modern threats; machine learning, big data, and analytical approaches offer great advantages in attack detection and prevention.

Applications such as intrusion detection systems (IDS) and intrusion prevention systems (IPS) enable the integration of data science methods. In particular, the advantages of machine learning-based systems over traditional methods, combined with anomaly detection and proactive defense mechanisms, increase the security level. Data collection, pre-processing, modeling, and algorithms are considered critical components of the threat analysis process. Real-world applications demonstrate how data science is effectively used to combat cyber threats, while case studies reveal the measures taken and solutions developed against significant attacks.

However, there are also challenges that data science faces in cyber threat analytics. Technical challenges such as big data management, data quality, and real-time processing can limit the ability of security experts to work effectively. Future directions have the potential to offer significant innovations in machine learning and artificial intelligence, autonomous security systems, and data privacy. Future studies in the field of data science and cyber security may focus on the following areas:

1. **New Machine Learning Models**: It is important to develop more advanced machine learning models to deal with new threats in cyber security. In particular, research should be conducted on how techniques such as deep learning and transfer learning can be used more effectively in anomaly detection and attack classification.

2. **Data Privacy and Ethical Approaches**: Addressing ethical issues related to user data protection and data privacy should be an important part of future work. In this area, it is recommended to develop more transparent and reliable data collection and analysis methods.

3. **Cyber Threat Intelligence and Cooperation**: Research should be carried out on increasing inter-agency cyber threat intelligence sharing and co-operation. This could enable joint defense strategies and faster response to threats.

4. **Autonomous Security Systems**: The development and implementation of autonomous systems will be an important step in the detection and prevention of cyber threats. The focus should be on increasing the ability of these systems to operate without the need for human intervention.

5. **Real-Time Analysis Methods**: Real-time data processing and analytical methods will increase the ability to respond quickly to cyber security. The development of more effective algorithms in this area can enable security analysts to be more proactive against threats.

In conclusion, this study in the field of data science and cybersecurity emphasizes the importance of cyber threat analytics and innovations in this field and prepares an important basis for future research. Cybersecurity requires the effective use of data science methods in the ever-changing threat environment and the development of innovative solutions in this field has become a great need.

References

Agbadoku, E E. (2024, January 1). The Application of Data Analytics in the Investigation of Cyberattacks: Scope and Impact. RELX Group (Netherlands). https://doi.org/10.2139/ssrn.4738358

Alani, M M. (2021, January 6). Big data in cybersecurity: a survey of applications and future trends. Springer Science+Business Media, 7(2), 85-114. https://doi.org/10.1007/s40860-020-00120-3

Alhogail, A., & Alsabih, A. (2021, July 22). Applying machine learning and natural language processing to detect phishing email. Elsevier BV, 110, 102414-102414. https://doi.org/10.1016/j.cose.2021.102414

Artificial intelligence (AI) cybersecurity. (2024, October 25). , undefined(undefined). https://www.ibm.com/ai-cybersecurit

Ávila, R L F D., Khoury, R., Khoury, R., & Petrillo, F. (2021, March 11). Use of Security Logs for Data Leak Detection: A Systematic Literature Review. Hindawi Publishing Corporation, 2021, 1-29. https://doi.org/10.1155/2021/6615899

Babu, F., Sebastian, K., & Sebastian, K. (2018, August 29). A Review on Cybersecurity Threats and Statistical Models. IOP Publishing, 396, 012029-012029. https://doi.org/10.1088/1757-899x/396/1/012029

Beerman, J T., Berent, D., Falter, Z., & Bhunia, S. (2023, May 1). A Review of Colonial Pipeline Ransomware Attack. , undefined(undefined). https://doi.org/10.1109/ccgridw59191.2023.00017

Chakraborty, A., Biswas, A., & Khan, A K. (2023, January 1). Artificial Intelligence for Cybersecurity: Threats, Attacks and Mitigation. Springer Nature, 3-25. https://doi.org/10.1007/978-3-031-12419-8_1

Darktrace Security Solutions. (2024, October 25). , https://darktrace.com/platform

Google Cloud security solutions. (2024, October 25). ,https://cloud.google.com/solutions/security

Jayalaxmi, P L S., Saha, R., Kumar, G., Conti, M., & Kim, T. (2022, January 1). Machine and Deep Learning Solutions for Intrusion Detection and Prevention in IoTs: A Survey. Institute of Electrical and Electronics Engineers, 10(undefined), 121173-121192. https://doi.org/10.1109/access.2022.3220622

Kashif, M., Arshad, S., Tahir, M., Umair, M., & Waqas, P. (2018, January 1). A Systematic Review of Cyber Security and Classification of Attacks in Networks. Science and Information Organization, 9(6). https://doi.org/10.14569/ijacsa.2018.090629

Kaur, H., Singh, G., & Minhas, J. (2013, March 10). A Review of Machine Learning based Anomaly Detection Techniques. , 2(2), 185-187. https://doi.org/10.7753/ijcatr0202.1020

Kimanzi, R., Kimanga, P., Cherori, D., & Gikunda, P K. (2024, February 26). Deep Learning Algorithms Used in Intrusion Detection Systems -- A Review. Cornell University. https://doi.org/10.48550/arXiv.2402.

Kruti, A., Butt, U J., & Sulaiman, R B. (2023, January 1). A review of SolarWinds attack on Orion platform using persistent threat agents and techniques for gaining unauthorized access. Cornell University. https://doi.org/10.48550/arxiv.2308.10294

Martínez, J M., Comesaña, C I., & Nieto, P G. (2019, January 4). Review: machine learning techniques applied to cybersecurity. Springer Science+Business Media, 10(10), 2823-2836. https://doi.org/10.1007/s13042-018-00906-1

Opara, E C., Wimmer, H., & Rebman, C. (2022, July 20). Auto-ML Cyber Security Data

Analysis Using Google, Azure and IBM Cloud Platforms. , undefined(undefined). https://doi.org/10.1109/icecet55527.2022.9872782

Pigni, F., Bartosiak, M., Piccoli, G., & Ives, B. (2017, November 16). Targeting Target with a 100 million dollar data breach. SAGE Publishing, 8(1), 9-23. https://doi.org/10.1057/s41266-017-0028-0

Suthishni, D N P., & Kumar, K S. (2022, March 23). A Review on Machine Learning based Security Approaches in Intrusion Detection System. , undefined(undefined). https://doi.org/10.23919/indiacom54597.2022.9763261

The WannaCry ransomware attack. (2017, April 21). Taylor & Francis, 23(4), vii-ix. https://doi.org/10.1080/13567888.2017.1335101

Tonkal, Ö., Polat, H., Başaran, E., Cömert, Z., & Kocaoğlu, R. (2021, May 21). Machine Learning Approach Equipped with Neighbourhood Component Analysis for DDoS Attack Detection in Software-Defined Networking. Multidisciplinary Digital Publishing Institute, 10(11), 1227-1227. https://doi.org/10.3390/electronics10111227

About The Author

Özgür TONKAL received his PhD from Gazi University, Department of Computer Engineering, one of the most prestigious universities in Türkiye. He works as an Assistant Professor in the Software Engineering Department of Samsun University. His research interests include Software Defined Networks (SDN), Computer Networks, Machine Learnings, Cyber Security.

E-mail: ozgur.tonkal@samsun.edu.tr, **ORCID:** 0000-0001-7219-9053

Similarity Index

The similarity index obtained from the plagiarism software for this book chapter is 7%.