The Interface Between Technology and People in Cybersecurity: Technological Solutions Supporting Humans in Organizational Protection

Jukka Ylitalo

2025 Laurea

Laurea University of Applied Sciences

Technology and People in Cybersecurity: Tech Solutions Supporting Organizational Protection

Jukka Ylitalo
Business Information Technology
Thesis
May 2025

Laurea University of Applied Sciences **Abstract**

Business Information Technology

Bachelor's Degree

Jukka Ylitalo

The Interface Between Technology and People in Cybersecurity: Technological Solutions Supporting Humans in Organizational Protection

Year 2025 Pages 44

The thesis aims to explore the synergy between technology and human and the interaction between them in order to enhance cybersecurity within organizations. Commissioned by the Information Technology (IT) department of one of the leading construction companies in Finland, the study focuses on user-centered security, behavior analytics, real-time threat management and technology-supported training with the goal to minimize vulnerabilities and improve organizational overall security posture.

The thesis is made as a development task and it aims to provide ways to gain benefits on interfaces that facilitate detection automation, implementing behavior analytics powered by artificial intelligence and machine learning and how to deploy comprehensive training modules to prepare employees against cyber threats. These goals aim to reduce the potential for human errors in daily security processes and improve the efficiency of threat detection and response.

The theoretical framework is built upon a review of academic literature, cybersecurity standards, industry reports and case studies from reputable sources such as the European Union Agency for Cybersecurity (ENISA). This foundation supports the exploration of user-centric security design principles, behavioral analytics methodologies, automation capabilities and effective training strategies. The thesis employs a qualitative approach for analyses and data collection involves interviews with the client's cybersecurity personnel. With these methodologies a well-rounded understanding of real life challenges that organizations usually face will be achived.

The key findings of the thesis show that AI-driven behavior analytics can significantly improve detection capabilities by identifying anomalies from normal user behavior patterns. Automation tools can effectively reduce the manual workload that is associated with maintaining cybersecurity defenses, therefore allowing for more efficient allocation of resources. Real-time threat management systems can provide important insights through data analytics for the information that is used by human when making rapid decisions during threat scenarios. Interactive training exercises are proven to be in a key role when increasing employee awareness and preparedness against emerging cyber threats. The analysis of the results obtained by this thesis indicate, that with integrating advanced technologies alongside with human factors can improve organizational cybersecurity significantly by enabling rapid threat detection and automated proactive response mechanisms. The need for careful consideration of privacy concerns, legal constraints and ethical implications associated with surveillance technologies is also highlighted in the findings. The thesis concludes with recommendations on how to balance the benefits of different technological innovations and also introduces the potential risks alongside it. It suggests adopting adaptive learning systems that evolve alongside emerging threats and emphasizes the importance of continuous user education as a vital component in battling social engineering attacks.

In this report, organization's internal Generative AI tool has been used to edit and improve the language and fluency of the text.

Keywords: Cybersecurity, Training solutions, Technology-Human interaction, Behavior analytics, Real-time threat management

Table of contents

1 Abbrevations

- AD – Active Directory
- AI – Artificial Intelligence
- AR – Augmented Reality
- BU – Business Unit
- CASB – Cloud Access Security Broker
- CIA – Confidentiality, Integrity, Availability
- EDR – Endpoint Detection & Response
- ENISA – European Union Agency for Cybersecurity
- EU – European Union
- GDPR - General Data Protection Regulation
- IP – Internet Protocol
- ISO – International Organization for Standardization
- IT – Information Technology
- LDAP – Lightweight Directory Access Protocol
- Malware – Malicious Software
- MDCA – Microsoft Defender for Cloud Applications
- ML – Machine Learning
- NIST - National Institute of Standards and Technology
- OCI – Oracle Cloud Infrastructure
- OTP – One-Time Password
- PCI DSS - Payment Card Industry Data Security Standard
- PHI - Protected Health Information

- PII - Personally Identifiable Information
- PPP – Public-Private-Partnership
- Shadow IT – Use of IT-related hardware or software unknown to IT department
- SIEM - Security Information and Event Management
- SOAR – Security Orchestration, Automation and Response
- SOC – Security Operations Center
- SSO – Single Sign-On
- UBA – User Behavior Analytics
- UEBA – User and Entity Behavior Analytics
- VR – Virtual Reality
- XDR – Extended Detection and Response

2 Introduction

This chapter introduces the client company, background of the thesis and used research methodologies. It also sheds light on the problems that the thesis aims to solve and aims to give a clear picture of the starting point for the research.

2.1 Client introduction

The client of the thesis will remain anonymous due to the sensitivity of the thesis. Client is a leading global project developer and construction company, that has deep expertise in constructing infrastructure, commercial property development, residential developments and undertaking Public-Private-Partnerships (PPPs). It has established operations throughout the Nordic region, Europe and North America since its establishment. The client's portfolio is varied and includes developing intricate infrastructure projects like tunnels, roads and bridges. In commercial property development, they lead in developing and building office buildings and retail outlets that enhance urban areas. In Finland, the client company is one of the market leaders in construction.

The client's IT management plays a significant role in facilitating the global construction and project development operations of the company. The IT services include infrastructure services, application development, cybersecurity and end-user services. The IT department wishes to maximize the potential of technology by realizing efficiency, collaboration and innovation. Operations are supported by a strong IT infrastructure that includes data centers, cloud computing, network management systems and hardware provisioning. Cybersecurity is a top priority for the client company. The IT department is strict in protecting data and systems from any potential threats. There is 24/7 cybersecurity user support available through a dedicated service desk that assists the employees with cyber-related issues and incidents.

In Finland, the IT administration of the client follows their global strategy but also addresses local requirements. These consist of locally tailored infrastructures following national standards, software adapted for use scenarios in a local context, adherence to data protection regulations such as General Data Protection Regulation (GDPR) and Finnish-specific cyber security policies. Finnish support services guarantee effective co-operation among personnel. By utilizing the latest technologies and following global and local best practices, their goal is to outperform their rivals in providing first-class results to customers.

2.2 Thesis' background

As cyberattacks keep growing in sophistication, organizations are realizing the need to protect their information and resources with all the latest solutions (Splunk 2024a, 4). This thesis explores the best practical ways to achieve this using technology as an enabler rather than

autonomous system, that only overlooks the processes. Faster deployment of technology in business has great advantages but on the other hand it gives more exposure to cyberattacks. Most organizations across the globe find cybersecurity a constant challenge. The intersection of human and technology poses serious implications for companies across all sectors, which is the subject of this thesis. The study contributes to the existing knowledge on the subject by investigating how technological solutions can aid humans in cybersecurity.

The thesis will analyze and essentially discuss multiple technological solutions that can help in assisting users' daily complex security processes, especially the ones where the potential for human errors is high. This includes developing user-friendly interfaces and building automated features that can reportedly detect security threats and minimize user-created threats. Behavior analytics is an integral part, as its function is to locate any abnormalities that may be present within an organization's infrastructure. Through the eyes of artificial intelligence and behavior analysis software, one can apply unusual events such as mass deletions or unauthorized access attempts that are automatically classified as flagged events that must be reviewed for further potential threats and dealt with before they evolve into real incidents. The interaction between human and technology is the key to threat management. A better insight can be provided by analyzing real-time data in order to make an informed decision in threat scenarios. Gaining access to all the threat intelligence enhances decision making regarding the mitigation of potential security threats and therefore enabling quick and effective action.

2.3 Research methodology

To ensure a well-rounded understanding, the research methodology was structured using qualitative approach. This included literature review, interviews and document analysis to fully explore the role and possibilities of technology in cybersecurity, and to establish the theoretical framework for the thesis.

2.3.1 Data collection

A comprehensive collection and analysis of data from various sources will be carried out for this thesis. To examine the correlations between technology and human in cybersecurity, it is important to draw upon multiple types of data that provide both theoretical insights and practical examples. The primary sources of data for this thesis include academic journals and publications, whitepapers, vendor and industry reports, cybersecurity news and blogs, interviews and reports. Academic publications and journals are an important resource when acquiring information on the latest theories, models and empirical findings regarding cybersecurity. Peer-reviewed articles provide intel on analysis done by experts in the cybersecurity field and therefore make a good foundation for the theoretical framework.

Official reports and whitepapers by institutions like the National Institute of Standards and Technology (NIST), European Union Agency for Cybersecurity (ENISA), and International Organization for Standardization (ISO) are recognized as authoritative sources of best practices in cybersecurity. These reports usually offer holistic frameworks, standards and protocols that organizations should implement into their processes. Reports published by leading cybersecurity vendors such as Verizon and IBM Security Services provide insight into current emerging threat trends, statistics and technological advancements within industry. These reports often include case studies with expert opinions which can help contextualize findings. Conducting interviews within the client's cybersecurity branch helps collect data directly from the practitioner, which is essential for understanding real life challenges and experiences the organization has faced. They also provide a clear understanding of the client organization's current situation. By integrating insights from these different sources, this thesis will present a comprehensive and balanced analysis of the intersection of technology and humans in organizational defense. The aim is not only to enlighten the theoretical discussion around the topic, but also implement these practices in real-world situations, making the recommendations feasible and actionable.

2.3.2 Data Analysis

Methods based on qualitative analyses will be employed, since the aim is to gain knowledge about concepts, but also to share information as to whether and how these solutions work to boost cybersecurity practices at organizations. This will involve in-depth examination of various sources of information related to user-centered security design, behavior analytics, automation tools, real-time threat management and training solutions. The key questions to be answered in this thesis are:

1. How can technological solutions be designed to support users' daily activities while minimizing human errors?
2. How can AI-driven behavior analytics detect anomalies from normal behavior?
3. What role do automation tools play in reducing the manual workload associated with maintaining cybersecurity defenses?
4. How does real-time data and analytics provided by technology enhance decision making in threat management?
5. How do interactive security exercises prepare staff members to defend against cyber threats?

3 Theory base

This theory base will introduce what the term and practice of cybersecurity is. It will also cover the theory behind behavioral analytics, real-time data, digital tools in training and

legislation and ethical perspectives. These are concepts that require some level of understanding in order to fully understand what the thesis explores and what the recommendations and conclusion offers.

3.1 Basic concepts of cybersecurity

Cybersecurity is a term used to describe the actions done to protect systems, networks and programs against computer attacks. These cyberattacks are typically made to steal, alter or delete confidential data, extort money or create havoc on the usual operation of businesses. As the world becomes increasingly digital every day, cybersecurity becomes even more important. One basic element of cybersecurity is realizing that there are two kinds of companies: those that know they are hacked and those that do not. There are reports of companies, whether big or small being hacked almost daily (Ozkaya 2019, 109). This is the reality which highlights the need for strong cybersecurity practices.

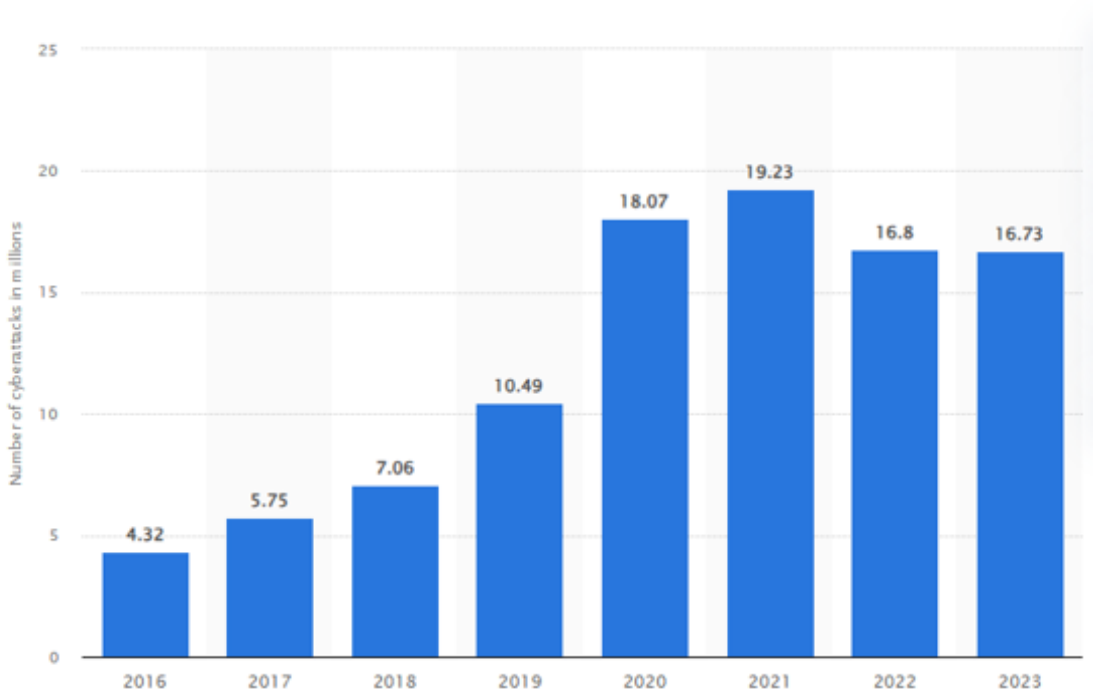

Figure 1: Annual number of attacks (Statista 2025)

Cybersecurity is vital because it protects all forms of data from theft and sabotage. Such forms of data are usually sensitive in nature, and they can consist of Personally Identifiable Information (PII), Protected Health Information (PHI), intellectual property or government and industry information systems. No organization can protect themselves against data breaches without a comprehensive cybersecurity strategy, and the lack of it can make them a simple target for cybercriminals. The need for new cybersecurity professionals is real and education programs have identified this. In his "Cybersecurity: The Beginner's Guide," Erdal

Ozkaya (2019) highlights the reality that anyone who desires to remake themselves as a cybersecurity master should observe that cybersecurity is required. Ozkaya summarizes the justifications for the establishment of the field with the way that progress in machine learning and artificial intelligence is colliding with existing security software as base pillars. Cybersecurity is a dynamic field that requires continuous learning and adaptation to understand new threats and technologies. Through networking, mentorship and studies individuals can gain the skills and knowledge needed to properly assist in protecting virtual spaces from cyberattacks. (Ozkaya, 2019, 202.) Experts in cyber protection must be aware of the attackers' mindset and this calls for research on their behavior and thinking, to understand what encourages hackers and how they approach things (Ozkaya 2019, 83). Cybersecurity is a domain that demands ongoing learning and updating based on the emerging threats and technology. This includes knowledge of the countermeasures as well as the attack methodologies used by the attackers. The practitioners can acquire the knowledge and skills necessary to excel in safeguarding digital platforms against cyber-attacks through mentorship and networking.

3.2 Behavioral analytics in cybersecurity

Behavioral analytics represent a proactive shift in the way that it aims to detect threats by identifying deviations from normal behavior in user and system activities (Kosinski 2024). The main idea is that even well-camouflaged malicious actions can stand out as statistically anomalous, given that baseline behaviors are well understood (Wickramasinghe 2023). The first step in behavioral analytics is to create a behavioral baseline. This works as an understanding of what constitutes as normal for the user, device or application. Behavioral baseline is developed by continuous monitoring and historic data analysis, enabling systems to establish individualized behavior profiles. Once these baselines are established, behavioral analytics tools detect anomalies that deviate from these norms. Traditional behavior monitoring can be expanded with User and Entity Behavior Analytics (UEBA) to not only include individual users but also entities such as servers, endpoints or applications. UEBA uses various sources for data and applies machine learning to model and analyze behavior (Securonix 2024). UEBA brings a broader scope for behavioral analytics and improves the detection of low-and-slow attacks and lateral movement, which often are missed by signature-based systems.

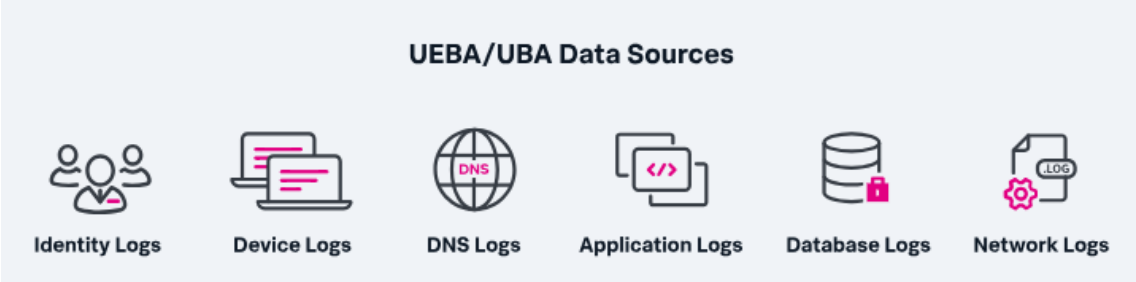

Figure 2: UEBA/UBA Data Sources (Wickramasinghe 2023)

There are technologies that enable us to perform behavior analytics. Key enablers are Artificial Intelligence (AI) and Machine Learning (ML). With these two, automated learning can be facilitated from vast amounts of behavioral data to detect even subtle anomalies (Wickramasinghe 2023). These models can be trained to classify behavior as harmful or risky or even predict potential threats before they happen, giving major advantage over rule-based detection (Sharma, Thakur & Tiwari 2024, 21). Real-time analysis is usually integrated with behavioral analytics, and this allows organizations to respond to threats as they happen, therefore minimizing the exposure window and allowing for faster containment procedures (ENISA 2022).

Even though behavioral analysis is a great tool for organizations to increase their security readiness, it also comes with its challenges. False positives, where an event or behavior is incorrectly flagged as malicious can often lead to alert fatigue, where analysts receive massive amounts of alerts, which are not real. Monitoring must also comply with privacy laws such as GDPR to ensure anonymization and transparency in policies (ENISA 2022). The deployment of effective behavioral analytics also requires significant computational thinking and a vast data infrastructure, which is not only expensive, but also takes its toll on the planet.

3.3 Real-time data in decision-making

Real-time data is something that allows organizations to detect and act on threats as they unfold and therefore minimize damage and response time. This capability also addresses one of the most critical cybersecurity vulnerability, which is human error. Time is a critical factor when it comes to cybersecurity and real-time data helps organizations to mitigate threats at machine speed, rather than human speed. With the real-time data collected organizations have a continuous visibility of their security posture. Without such data they are forced to work in the dark relying only on possibly outdated or incomplete information.

Figure 3: Real-time Data Benefits (Watts 2023)

The ability to make rapid decisions doesn't depend solely on data availability, but also on contextual understanding. Real-time information is enriched with user identity, asset criticality, historical baselines and threat intelligence, creating the context required for confident decision-making (Tounsi, Rais 2018). Technologies like Microsoft Sentinel and Defender for Endpoint leverage behavioral analytics to score risks as they unfold. For example, if a user logs in from a new country, accesses SharePoint and downloads an unusual number of files, the system can automatically flag and restrict access based on predefined sets of rules (Microsoft 2024h). With this technology, real-time data doesn't just inform about events, but it also enables a decision to be executed instantly, often also without human intervention.

Fast decisions are not always accurate or right ones, especially if made with haste and under pressure. One of the key advantages of real-time data systems brings some relief to this. Their ability to reduce the cognitive loads on people analyzing the data allows them to act faster and with more confidence (Edwards, Fox, Hamby, Makinson & Snyder 2013, 7). Instead of manually correlating the logs and hunting for context, they receive enriched alerts and visual clues. It is also important to realize that security concerns should not be isolated in their own categories, since they affect other aspects of business, such as business continuity, customer trust and compliance. With real-time data this information trade-off can be made more seamless. For example, Data Driven Business Continuity where if a real-time alert of ransomware behavior triggers, it immediately starts containment protocols while simultaneously alerts the business continuity teams to shift operations (CLDigital 2024).

A concrete example of real-time decision support is found in Microsoft Sentinel's fusion detection rules. These rules automatically correlate information from different sources, like Azure Active Directory (Azure AD) sign-ins, Defender alerts and third-party threat intel, to create a coherent picture of multi-stage attacks (Microsoft 2024i). These correlated incidents are prioritized and sent directly to analysts, cutting through noise and reducing decision time from hours to minutes. Microsoft Defender for Cloud Apps analyzes live session data to block downloads or prompt for reauthentication when anomalous behavior is detected during an active user session (Microsoft 2024c). These are decisions made in the background, taken in milliseconds which are based entirely on real-time input.

3.4 Digital tools in cybersecurity training

Cybersecurity training is essential for strengthening organizational resilience against cyber threats, given that human error remains a major factor in security breaches. Digital training tools enhance employees' ability to recognize and respond properly to threats such as phishing, social engineering and malware attacks (McDonough 2023, 182). It also helps foster a culture of security awareness which is critical for continuous organizational protection. An example of an awareness campaign can be a simulation phishing training sent directly to users'

email. Effective training incorporates psychological principles such as motivation, feedback loops and cognitive load management to enhance learning outcomes.

There are four key dimensions when planning an effective technology supported training program: accessibility, engagement, personalization and integration (Teachflow 2023). Accessibility is that users are able to enter these training regardless of what time of the day it is or where they are positioned. Engagement is one of the key components for getting the workforce to onboard awareness trainings. One way to increase engagement is to give immediate feedback during digital exercises to encourage positive security behaviors on users. Personalization is important for getting the most out of these exercises. One shoe does not fit all, and people come from different starting points. Some users need more advanced trainings to keep them motivated and some might lose interest if the topic is too hard to understand. These systems need to be integrated with others, for example Outlook. Users are more prone to flag an email as harmful, if the report button is integrated to the software already.

3.5 Legislation and ethical perspectives

Cyber law contains a broad scope of legal matters closely related to the use of technology including but not limited to intellectual property and privacy and even data protection. Property laws deal with assets which an individual or corporation gets as a consequence of creative labor. Protection of intellectual property is becoming more and more important when it comes to cybersecurity, as the consequences of a cyberattack may be unlawful appropriation or even theft of highly sensitive proprietary information (Brathwraite 2019, 5-7).

GDPR is perhaps the most well-known cyber-related law. It is one of if not most contributing laws that define our modern-day notion of cybersecurity. In the implementation of this European Union provided law, all entities within the scope of European Union or handling data of EU citizens are legally bound to adhere. Privacy and data protection are a priority area for Europe. The policy of the EU is based upon the premise that human beings are the actual proprietors of their data. The GDPR does this by putting the individual into the driver's seat with their data and putting strong obligations upon the organizations for protecting the data. They vary from the need for transparency through accountability and data protection against hacking into one's data. (Sharma 2020, 45-48.) Ensuring you are only capturing what is required is a key factor and another is the environment. One could end up with vast datastores of data that you don't need and that also may have an impact on the planet. (Interview 1 2025.)

Ethics have a critical function within cybersecurity as they work as guidelines on what is wrong and what is right. Ethical principles include Confidentiality, data Integrity, and data Availability (CIA) and also protection of privacy rights and protection of stakeholders' trust. Ethical principles promoting cybersecurity’s best practices are centered around protection against misuse and abuse of sensitive data. Bulk data surveillance involves monitoring bulk

amounts of data with the intention of identifying potential breaches. This practice may raise the level of protection of an individual by identifying abnormal patterns early enough, but it also has some inherent questions regarding confidentiality and privacy. One of the mechanisms that are employed against the consequences brought about by such problems is the use of encryption. It means intercepted data while surveillance is ongoing will not be useful unless a decryption key is made available. (Bossomaier & Miller 2024, 86-87.) Organizations should monitor only what they must and nothing more, also what is monitored and reasons for monitoring are to be made clear through company policy and understood by employees (Interview 1 2025). Cybersecurity regulations ensure organizations adopt enough data protection with respect for individual privacy rights. Moral obligations compel organizations towards accountability while dealing with sensitive data. Knowledge about the regulatory context such as the GDPR and following the ethical guidelines helps organizations navigate the challenging environment of cybersecurity.

4 Utilizing technology on behavioral analytics

Behavioral analytics in cybersecurity is an expansive field with which organizations attempt to increase their level of security. It focuses on the monitoring, understanding and predicting human activities by utilizing advanced technologies such as Artificial Intelligence (AI) and Machine Learning (ML), which have greatly impacted the use of behavioral analytics. These technologies add effectiveness to the detection of anomalies, automating the response and handling threats. (Ashton 2024, 46-47). Ensuring compliance with regulations such as GDPR while leveraging the capabilities of behavioral analysis is one of the major challenges to overcome (Interview 1 2025).

Behavioral analytics can be implemented as an extra security layer. A good example of this implementation was done by Visa, who faced significant challenges in securing online transactions against advanced fraud techniques (Digitaldefynd 2025). Social engineering attacks were used to exploit human psychology in order to deceive individuals into revealing confidential information, while credential snuffing was involved to steal credentials to gain unauthorized access. These methods are often sophisticated enough to bypass traditional authentication systems and therefore put users and their transactions at risk. Visa implemented a real-time behavioral biometrics system that scrutinizes user behavior patterns such as typing speed, mouse movements and device interactions. (Digitaldefynd 2025.) This technology enhances security by verifying users' identities based on their unique behavioral traits. By integrating this with an already existing security framework, the system adds a layer of protection for online transactions. With these integrations in place, behavioral biometrics start to operate by continuously monitoring user interactions with their devices during transaction processes. Machine learning algorithms then analyze this data to create detailed profiles of normal user

behavior. When a transaction happens, the system compares the current behavior on the transaction to the established user profile and any deviations from the normal are flagged as potential fraud attempts, triggering additional verification steps or blocking the transaction altogether. (Digitaldefynd 2025.)

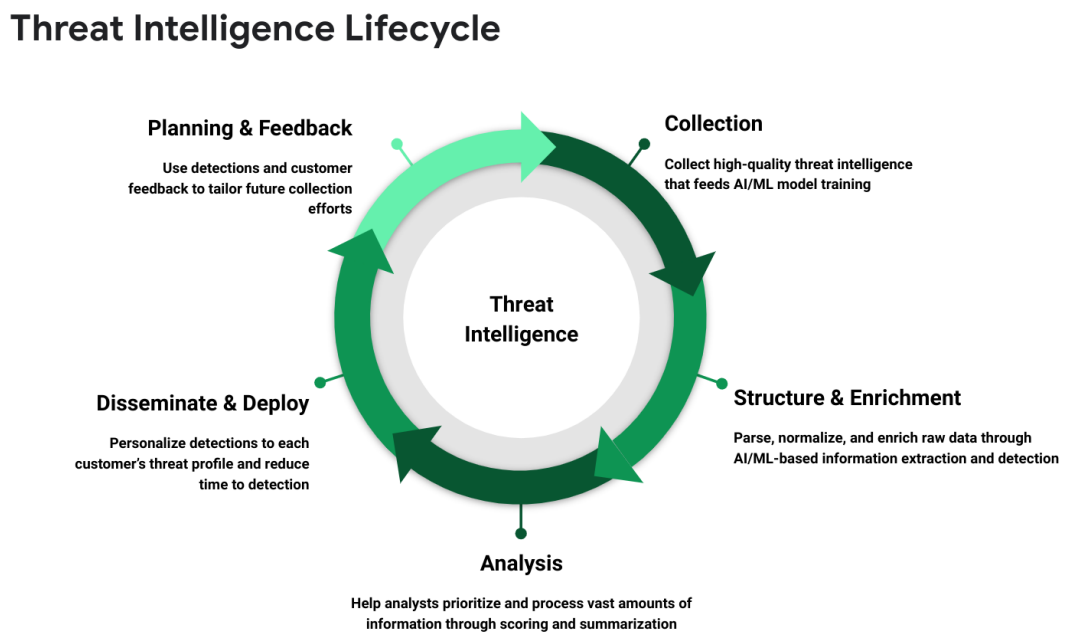

Figure 4: AI-driven Threat Intelligence Lifecycle (Cybersecurity News Everyday 2023)

4.1 Artificial Intelligence and Machine Learning

Artificial intelligence and machine learning are at the center of advancement in cybersecurity behavioral analytics. AI is used to refer to the simulation of human intelligence by machines and specifically computer programs (Manda 2021, 7). Machine learning on the other hand is a branch of AI that allows for the learning and improvement capabilities for systems through experience. This can happen with or without the need for explicit programming. Both technologies do play an important role when it comes to cybersecurity due to their ability for enabling the automation of detection processes, the capacity to analyze large sets of information and the possibility to identify unusual patterns that can indicate potential security breaches. (Manda 2021, 15.)

AI-based detection systems can handle vast amounts of information at speeds greater than human analysts can accomplish, therefore making it possible to analyze and react to it in real-time (Bertino 2023, 79). This will speed up data-led threat and risk assessment (Interview 1 2025). For example, deep learning-based algorithms are used to analyze network traffic information to identify anomalies which flags as an attempt of intrusion (Ashton 2024, 40).

Machine learning-based models are trained in historical information to identify patterns with malicious activity. It is possible for such models to continue learning new information, therefore improving by themselves with each passing moment (Bertino 2023, 18).

Anomaly detection is one of the main uses of AI and ML in the field of cybersecurity behavioral analytics. By constantly monitoring user activities and system performance, anomaly detection systems can discover deviations from known patterns that could indicate unauthorized access or other security breaches. Anomaly detection systems use statistical methods in combination with machine learning algorithms to separate normal behaviors from unusual behaviors, thereby enabling early intervention before any possible damage occurs. (Ashton 2024 46-47.) Artificial intelligence has the ability to upgrade the automation of recurring processes like patching and monitoring vulnerabilities. Automated programs reduce the burden for IT professionals by having computer programs patched for security, therefore removing the ongoing need for human involvement (Bertino 2023, 79). This not only makes processes more efficient, but it also reduces the potential for human error that often contributes to cybersecurity breaches.

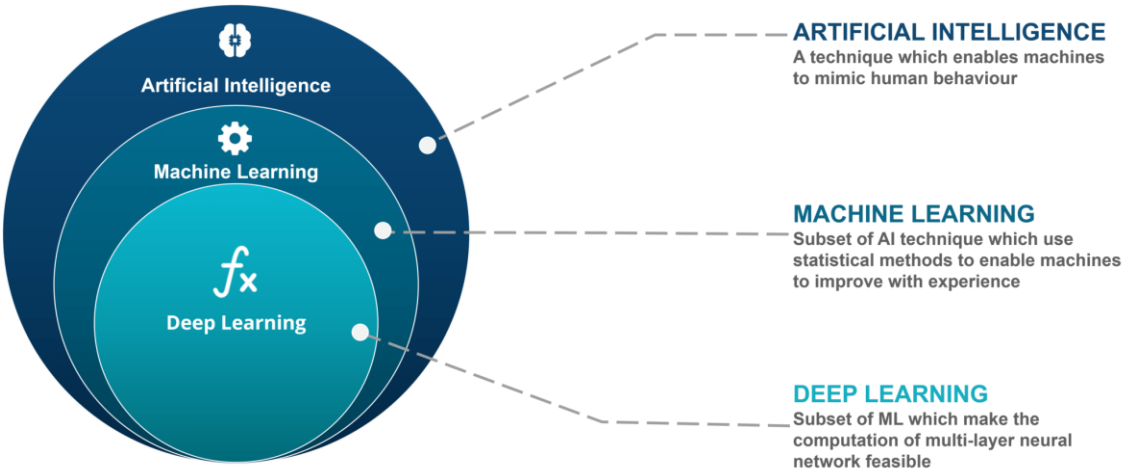

Figure 5: AI vs ML vs Deep Learning (Edureka 2025)

4.2 Mass deletions and transfers

Mass deletion and mass transfers refer to massive efforts to delete or transfer information in an organization's network. Example cases where these can happen:

- Insider threats
    - Employees with administrative rights initiate a mass wipeout or transfer of critical data repositories
- Account compromise
    - Threat actor gains access to privileged account and begins exporting or erasing sensitive data

- Ransomware or malware
    - Malicious code deletes or encrypts masses of data, often targeting backups and archives
- Wrong automation
    - Poorly scripted automation accidentally overwrites or removes large volumes of data
- Accidental deletion
    - An employee accidentally deletes large volumes of data
- Unauthorized downloading of data
    - An employee is leaving the company and takes large sets of data with them

Such actions can be signals for security breaches, especially if they are unexpected or unrelated to legitimate activities. Behavior analytics, if founded on artificial intelligence and machine learning can hold the potential to pick up on such anomalies through the observation of information flow patterns and the identification of unusual activities (Ashton 2024, 55). For example, machine learning programs have the potential to be trained to recognize normal patterns of information transmission within an organization. Any unusual information transfers or delete activities that deviate from the normal patterns can produce alarms for closer investigation. Such programs can predict potential security weaknesses even before they are triggered through the monitoring of past records related to mass transfers and deletion. (Ashton 2024, 56.)

AI-based behavioral analytic tools have the ability to auto-classify identified events, including mass deletions or attempted unauthorized accesses (Ashton 2024, 55). This feature allows security teams to prioritize response activities in proportion to the level of risk presented by the threat. Automated processes can be used to implement instant actions like quarantining compromised machines or reverting unauthorized changes, to minimize potential harm (Binnar, Bhirud & Kazi 2024). The use of real-time threat management tools greatly enhances the processes used to make decisions during security breaches. They provide large amounts of information about what is occurring in the network at any specific moment, making it easier to identify and counter the attacks (Sarker, 2022, 16). Being able to identify the deletion or transfer quickly reduces the amount of time the attacker has to perform these actions.

Figure 6: How Threat Intelligence Tools Enhance Security Measures (SecureLayer7 2024)

The integration of technology in behavioral analytics greatly improves an organization's ability to identify and respond to security breaches. Artificial intelligence and machine learning play a central role in automating the process of threat discovery, user behavior analysis and routine cybersecurity operations (Sarker 2022, 18). By using advanced algorithms to track large data deletions and transfers, organizations can identify potential breaches at their initial stages and take proactive steps to protect their networks (Sarker 2022, 3). The continuous evolution of these technologies guarantee that cybersecurity defense systems continue to work effectively despite the constantly changing threat actors.

4.3 Utilizing Security Information and Event Management (SIEM)

There are tools which can be used for detection and response to mass deletions and transfers. Microsoft Sentinel has a machine learning engine which detects the subtle and not-so subtle indicators of mass data operations. By leveraging information from Microsoft 365, Azure services and other possible hybrid sources, Sentinel can provide early warning signs and automate defensive actions (Microsoft 2024a). One program that integrates natively with Microsoft Sentinel’s SIEM platform is Microsoft Defender for Cloud Applications (MDCA). It provides visibility, analytics and control across sanctioned and unsanctioned cloud services, while enabling organizations to discover shadow IT usage, monitor user behavior across apps like Microsoft 365, Google Workspace, Box, Dropbox, and Salesforce and apply real-time controls to govern risky activity. It functions as a Cloud Access Security Broker (CASB) to detect risky application behavior and anomalous data exfiltration. MDCA is designed to enforce security policies on data traversing the cloud while addressing regulatory and compliance mandates (Microsoft 2024b).

One of MDCA's major strengths is its ability to detect abnormal user behavior and mass activity patterns such as when a user downloads thousands of files within a short period of time or uploads sensitive content to personal cloud storage. These patterns are often early indicators of data exfiltration, insider threat or misuse of credentials following a compromise. At the core of MDCA is UEBA, which uses machine learning to establish activity baselines for every user. These baselines are derived from typical login times, geographies, device types and data interaction patterns. Once a baseline is established, MDCA can detect anomalies that deviate significantly from expected user behavior. For example, if a user typically accesses fewer than 50 files per day and suddenly downloads 2000 files from OneDrive outside working hours using a previously unseen Internet Protocol (IP) address, MDCA generates a high-severity alert. (Microsoft, 2024c.) MDCA also uses anomaly detection policies that identify risky behavior without requiring administrators to define thresholds for them manually. These AI-driven policies detect threats such as impossible travel for example if a login from Finland and Japan happens within five minutes apart for the same user or an unusual administrator activity or abnormal sharing patterns is detected. MDCA can trigger an alert in these cases and optionally even block a transfer in real time using Conditional Access App Control for example if a user attempts to upload sensitive data to an unsanctioned or high-risk app, such as personal Dropbox. This is a functionality that is particularly handy in industries subject to strict data sovereignty and compliance requirements. (Microsoft 2024d.) MDCA can also be integrated with firewall logs and endpoint telemetry to discover shadow IT applications and assess their security posture over known risk criteria.

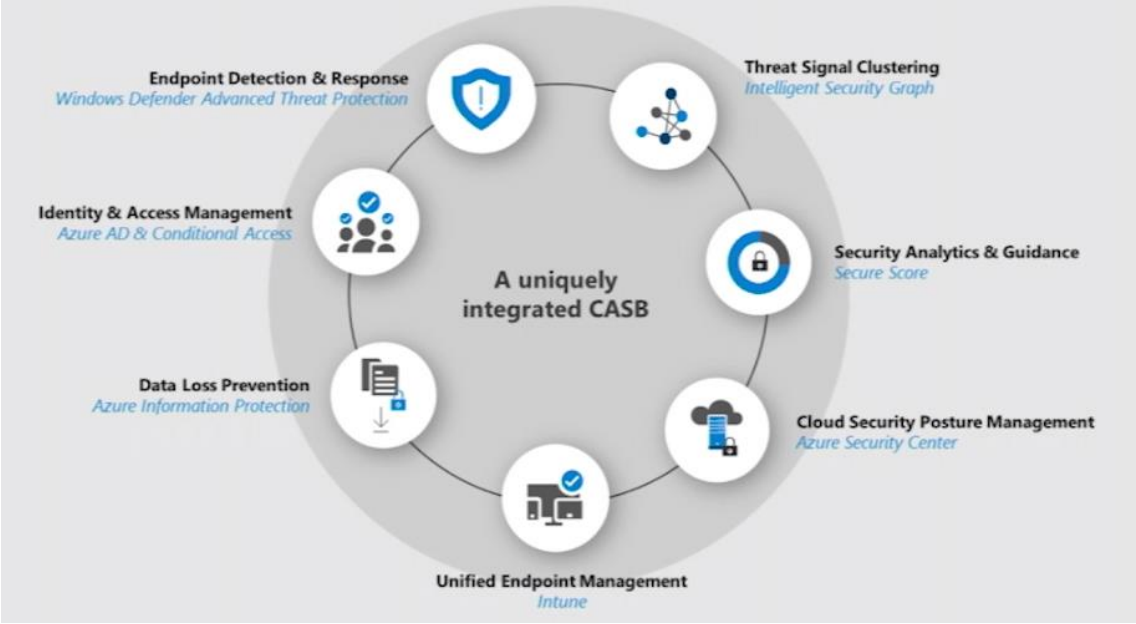

Figure 7: CASB integration figure (Prokopets n.d.)

5 Utilizing real-time data in decision making

Throughout its history, cybersecurity has mostly been reactive by relying on periodic assessments, incident responses after breach detections and retrospective data analysis (ENISA 2022, 89). With the threat landscape evolving all the time in its complexity and speed, real-time data utilization has become a cornerstone for proactive cybersecurity decision-making. By leveraging technology to process real-time information, organizations can not only enhance their threat detection and response but also significantly alleviate human error, which unfortunately remains to be one of the most persistent and damaging vulnerability in cybersecurity (Truitte 2019).

Real-time data in cybersecurity refers to the continuous collection and analysis of information from various sources. According to Proofpoint 2025, These sources can be:

- Network traffic
    - The flow of data packets across a computer network, encompassing all communications between devices, systems and services
- User activity
    - The recorded actions or behaviors of users interacting with systems, such as logins, file access or command executions
- Endpoint telemetry
    - Data collected from end-user devices (laptops, servers, mobile phones) that provides insight into system health, configurations and security-related events
- Cloud applications
    - Software services hosted in the cloud (Microsoft 365, Salesforce etc.) that users access over the internet
- Threat intelligence feeds
    - Continuously updated streams of data containing indicators of compromise, tactics and techniques used by cyber threat actors

Organizations can gain the ability to detect anomalies, misconfigurations, breaches and insider threats with minimal delay by analyzing this data as it is generated (Wilson 2025). Many modern platforms such as SIEM, Extended Detection and Response (XDR) and UEBA already utilize real-time processing to dynamically assess risks and automate decision making, therefore creating a continuously updating security posture. By combining conditional access policies in Azure AD with Defender technologies, real-time decisions based on live conditions such as device health, location, user risk score and app behavior can be efficiently reinforced (Microsoft 2024e). So, if a user attempts to access sensitive data from an unknown device, access can be automatically blocked or require additional authentication.

Figure 8: Why Prefer UEBA (Sharma, Thakur & Tiwari 2024)

5.1 Humane errors and alleviation benefits

Despite the many advances in cybersecurity technologies, human errors remain one of the leading causes of cyber breaches. The 2024 Cost of a Data Breach report by IBM shows that human errors were the cause of about 22% of the breaches examined (IBM 2024). These errors can range from simple mistakes made, such as clicking on phishing links to even more complex issues like misconfiguration of security settings. Real-time data and analytics have a critical role in mitigating these errors by providing timely and actionable insights into what is happening, where it is happening and why. Real-time data provides organizations with the capacity to detect threats and anomalies almost in real time. SIEM system collects and analyzes log data from various sources in real-time and flags abnormal behaviors such as mass file downloads, unusual logins or privilege escalation attempts. This feature allows the security team to identify threats and act instantaneously. This rapid detection reduces the window of opportunity for attackers and also minimizes the impact of human errors. (Dahj 2022, 368-369.) Instead of relying on human vigilance and manual interventions, the system automatically identifies and alerts suspicious activities to the attention of the security team in real times or even automatically blocks these actions (Microsoft 2024c). Machine learning algorithms are also able to scrutinize user behavioral patterns to identify deviations that indicate malicious activities. Predictive models are able to provide proactive notifications to the security team about impending threats, which allows them to act ahead of an occurrence leading to an error and therefore act preventatively. Through ongoing data analysis, these systems become increasingly accurate with the passage of time and reduce the likelihood of incidences of human errors (Bellis & Roytman 2023, 38).

Using orchestration tools like Microsoft Sentinel's Logic Apps, organizations can trigger automated workflows when specific alerts are detected. For example, if real-time data indicates that a user’s credentials were leaked, a playbook can automatically:

- Disable the user account
- Invalidate sessions
- Notify the security team
- Launch a password reset workflow

This proactive real-time response is powerful in alleviating the risk that human administrator may overlook, especially under pressure or outside normal office hours. (Microsoft 2024f.) Implementing real-time data utilization technologies to address human errors has several significant benefits. Some of these benefits are:

- Faster detection and response
    - Real-time analysis shrinks the time to detect and contain incidents from days or even weeks, to minutes or hours

- Reduced operational stress
    - Automating decision-making reduces cognitive overload on security teams, allowing them to focus on strategic initiatives rather than chasing alerts manually
- Consistency and objectivity
    - Machines apply policies and detection rules just as instructed, avoiding subjective human judgment errors under stress or fatigue
- Stronger compliance
    - Real-time monitoring and enforcement help maintain continuous compliance with standards like ISO 27001, GDPR and PCI DSS
- Improved security culture
    - By embedding security controls into workflows, users are protected by design, rather than relying solely on training and voluntary adherence

While real-time technologies do offer us some clear advantages, they also require careful planning. There are scenarios that must be taken into consideration. False positives can overwhelm security teams if detection rules are too sensitive, over automation can cause legitimate actions to be blocked and privacy concerns arise when monitoring employee behavior extensively. Policies require transparency and ethical governance and the best way to successfully implement a real-time cybersecurity strategy is balance automation with human supervision (CyberRiskInsight 2025).

5.2 Information created by data analytics on threat mitigation

Data analytics provide valuable information to organizations that can be utilized when enhancing threat mitigation strategies. By processing massive amounts of data from various different sources, these analytic tools can uncover hidden patterns and correlations that might not be apparent when looked at through manual analysis. By integrating relevant cyber threat intelligence into other business operations, organizations are able to gain understanding to a much wider context of threats they might be facing. This integration enables companies to perform prioritization of threats based on their potential impact on business, allocate and diverse resources effectively and to develop precise targeted mitigation strategies. (Dahj 2022, 366-367). Real-time data analytics is also very useful in facilitating proactive threat modeling (Dahj 2022, 368). By simulating various different attack scenarios and analyzing their potential impact, organizations can prepare for multiple different types of cyber incidents. Threat modeling helps organizations in identifying their critical assets, understanding different vulnerabilities and implementing appropriate countermeasures for them. This proactive modeling has the capacity to significantly enhance an organization’s readiness and tolerance when it comes to handling threats. One practical use of this approach can be seen in predictive vulnerability management. Predictive models assess the likelihood of most known vulnerabilities

based on historical data collected and current threat intelligence. With these predictions security teams are able to prioritize patching efforts and more effectively focus on vulnerabilities that pose the greatest risk on business (Bellis & Roytman 2023, 38).

SIEM systems are great tools when it comes to real-time incident response and digital forensics. They serve as central monitoring platforms that gather information across networks to identify threats and security incidents. Traditionally, SIEM has been acting passively, but modern applications and changing threat landscape demand that these systems take an active role. This is achieved by integrating SIEM with digital forensic platforms to provide richer tactical information in real-time. This integration can enhance the speed and accuracy of threat detection and response by automating the collection of digital evidence at critical moments, and therefore essentially transforming SIEM into a proactive tool in cybersecurity defense. (Ozkaya 2019, 120-121.) In the interview 1 (2025) clients' head of cybersecurity engineering and operations confirmed this by saying that the SIEM tooling helps to analyze significant volumes of data, which in turn helps to identify and prioritize security events that humans need to investigate further. The interviewee also pointed out that it would be ideal to remove human interaction until it is absolutely required. Automation should be introduced where tasks are repetitive and where humans are most likely to induce error. Anywhere where human interaction exists there is a possibility for a humane error. Sometimes volume of work, alert fatigue or other distractions can lead to errors. (Interview 1, 2025.)

Security Orchestration, Automation and Response (SOAR) platforms complement SIEM by automating and orchestrating different security operations. The automation aspect of it reduces human intervention in routine tasks, therefore allowing cybersecurity teams to shift their focus to more complex decision-making processes (Splunk 2024b, 3-4). SOAR can increase efficiency when handling threats through its automated workflows. SOAR's ability to integrate various security tools and automate responses to different incidents enables organizations to respond more swiftly and accurately to cyber threats while at all times maintaining a high level of collaboration among security teams (Ozkaya 2019, 121). Incorporating these technologies into the organizational framework not only enhances operational efficiency but also supports strategic decision making through detailed threat intelligence reports. Endpoint Detection and Response (EDR) technology provides both proactive and reactive actions and this is deeply integrated with the SIEM and SOAR capabilities. Much of these workloads are already automated leaving the human analyst to focus on more specialist items. (Interview 1 2025.) These technologies provide a more collaborative environment where human interaction is enhanced by technology-driven information and therefore allowing for more informed decisions to be made and proactive threat mitigation strategies to be developed.

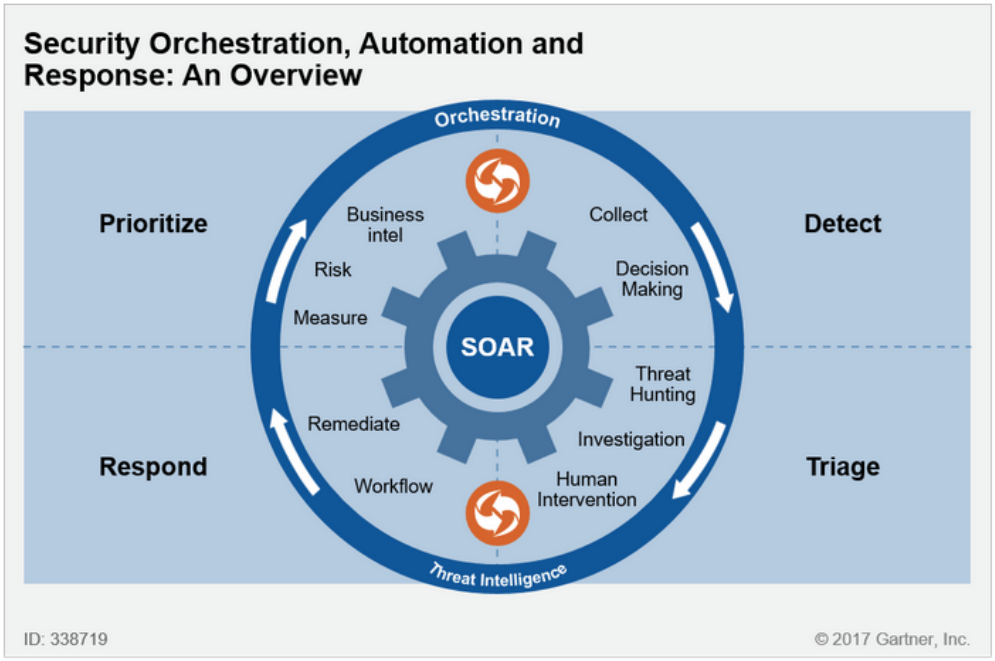

Figure 9: What is SOAR (Softprom 2021)

5.3 Case examples of rapid decisions in threat situations

An alleged breach involving Oracle recently came into light and was fully catalogued by many cybersecurity forums, such as Cloudsek. Initial reports suggested that a threat actor using the alias "rose87168" claimed to have accessed Oracle's legacy cloud infrastructure, specifically targeting Single-Sign-On (SSO) and Lightweight Directory Access Protocol (LDAP) systems. This breach reportedly started in January 2025 but was publicly acknowledged around March and April 2025. The initial entry point to the systems appeared to have been through two obsolete servers that were no longer part of Oracle's cloud infrastructure. There have been claims circulating that about six million Oracle customer records have been up for sale on Breach-Forums. Oracle has dismissed these allegations with a statement that its Oracle Cloud systems were not compromised, and the incident did not affect customer data or cloud services. Oracle has emphasized that their current cloud infrastructure OCI did not experience any security breach. (Cloudsek 2025.) This case was also noticed in the client company and interviewee used it as an example of real-time monitoring successfully mitigating threats. Real-time intelligence provided us with insight and allowed us to make a decision around what action we needed to take as a precaution weeks before Oracle had even acknowledged a breach (Interview 1 2025).

Digitaldefynd has collected multiple case examples of security breaches and best-case practices on their site and one of them is about Palo Alto Networks. They struggled to manage the massive amounts of security data generated by their clients' networks and therefore traditional security methods, which relied heavily on manual analysis and signature-based

detection started to prove inadequate against the advanced persistent threats and sophisticated malware that circulate through networks nowadays. These outdated methods used were very time and resource consuming and often also failed to detect subtle indicators of compromise due to human errors, leaving some networks vulnerable to attacks. The sheer volume of data alone made it difficult for security teams to identify and respond to threats in a timely manner. (Digitadefynd 2025.) To address these challenges, Palo Alto Networks introduced an AI-powered security platform that uses machine learning algorithms to analyze their extensive network data. This advanced system has the ability to automate threat detection by identifying patterns that show indications of cyber threats. These machine learning models which are trained in handling large datasets allow the recognition of anomalies and even prediction of potential attacks with fairly high accuracy. The AI-powered platform continuously monitors network traffic and automatically flags suspicious activities for further investigation to be done by human analysts. By automating the detection process itself, the system reduces the time that is required to identify and eventually respond to threats. This enhances the overall efficiency of security operations and with the platform evolving over time and learning from new data to adapt to new emerging threats, it remains effective against the continuously changing cyber threat landscape. (Digitadefynd 2025.)

Traditional Security Operations Centers (SOC) often find themselves struggling to manage risks effectively. One example of this case was made by Sony who, with its different business units in various industries such as electronics, entertainment and financial services, faced significant security challenges. The huge amount of digital assets and technology infrastructure they have requires robust protection against a wide range of cyber threats. Traditional SOCs, which relied heavily on manual processes and reactive measures, were insufficient to manage the complexity and scale of these risks. (Digitaldefynd 2025.) The need for a more effective approach became clear as cyber threats continued to evolve and grow in sophistication and complexity. Sony enhanced its security operations by implementing an AI-driven SOC. This leverages machine learning and artificial intelligence to monitor, analyze and handle threats in real-time. The AI-driven SOC automatically detects patterns with indications of cyber threats and initiates responses to potential security incidents without human intervention. The implementation involves continuous monitoring of network traffic, user behavior and system activities across Sony's digital landscape. Machine learning algorithms then analyze this data to identify anomalies and predict possible potential attacks. If a threat is detected, the system can automatically trigger predefined response protocols, such as isolating affected systems, blocking malicious traffic or alerting security personnel for further investigation. (Digitaldefynd 2025.)

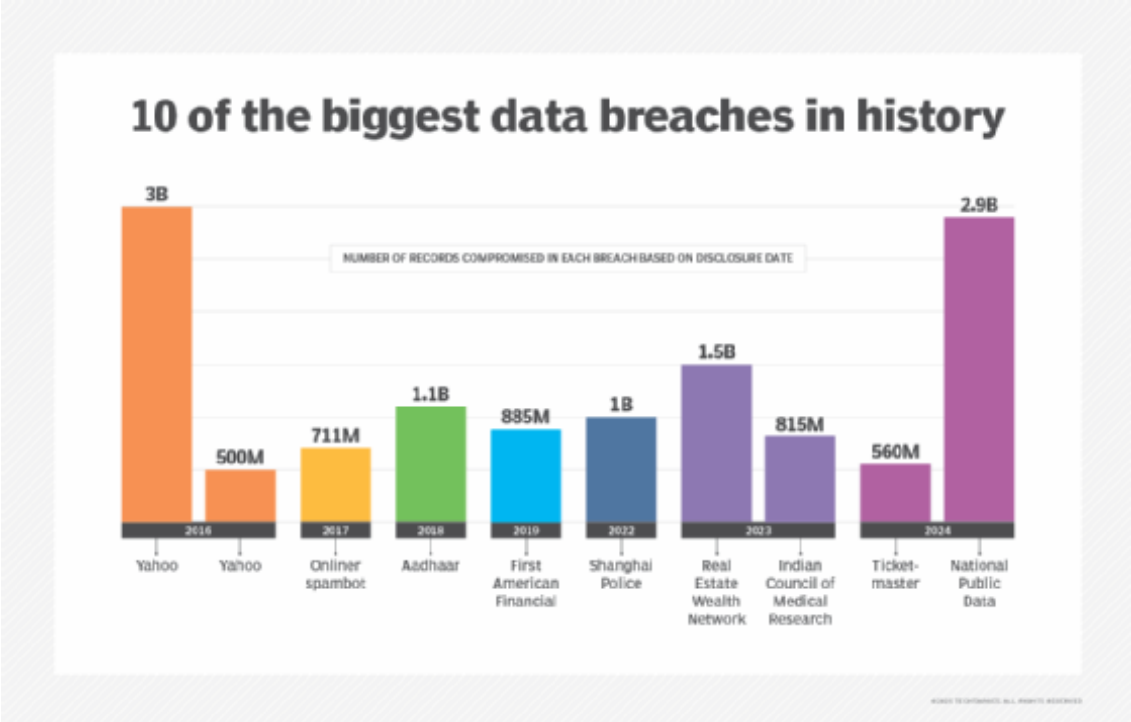

Figure 10: 10 of the Biggest Data Breaches in History (Kerner 2025)

6 Technology supported training solutions

The world is now at the peak of the digitalization age and cybersecurity is becoming a pressing issue for even more organizations worldwide. Technology-enhanced training solutions and awareness programs are starting to become standardized for many organizations. On average companies spend 3.5 million dollars annually on cybersecurity programs, which is a massive 20% increase when compared to the year 2020 (Security Innovation 2023). Organization leadership plays a crucial role in shaping their culture of cybersecurity awareness. By leading by example and emphasizing the importance of cybersecurity as a shared responsibility, leaders can foster a culture of open dialogue and information sharing among the workforce (Abrahams, Farayola, Kaggwa, Uwaoma, Hassan & Dawodu 2024, 107). There are many advantages to technology-enabled training solutions compared to traditional education, which usually consists of outdated or irrelevant information. These advantages include, but are not limited to scalability, accessibility and efficiency that training solutions can gain. With the support of technology, training can be spread across the whole workforce, ensuring all employees possess the knowledge and skills required to identify cyber threats. Interactive and engaging training has the capacity to improve levels of learning in the actual environment, which ultimately leads to strengthening the security overall posture of the whole organization (McDonaugh 2023 182).

As cyber threats grow in complexity, employee awareness and readiness have become essential layers of defense. Human factors, such as lack of awareness, poor security practices and tendency to social engineering contribute to a significant portion, roughly 60% of cybersecurity incidents (Verizon 2025). Traditional training methods such as annual e-learning courses are no longer sufficient on their own. In order to address this gap in knowledge, organizations are increasingly leveraging technology-supported training solutions for their dynamic, scalable and interactive education methods.

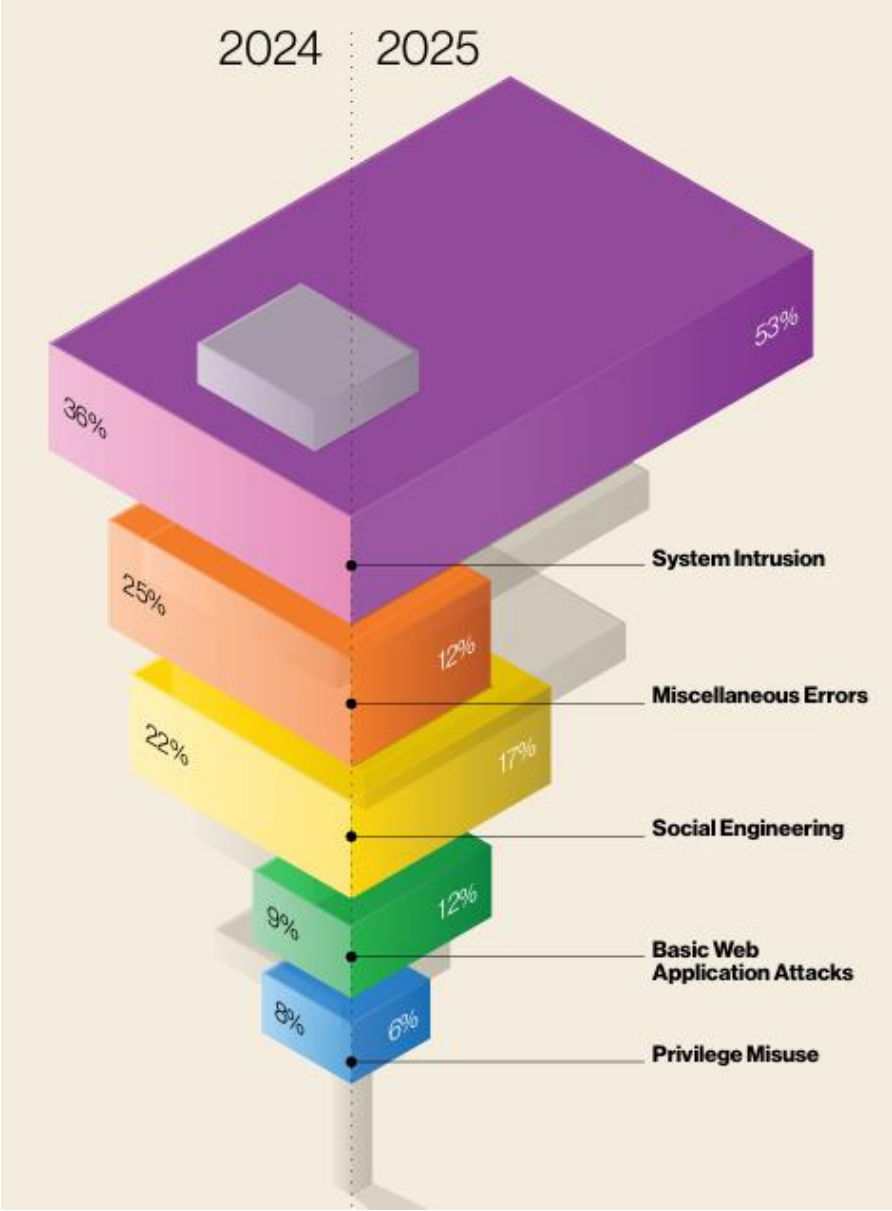

Figure 11: Report of breaches 2024 vs 2025 (Verizon 2025, 2)

6.1 Employee awareness opportunities on a big scale

One of the key aspects of technology-supported training solutions is its ability to raise cybersecurity awareness on a large scale. Employee awareness programs are critical in fostering a culture of security within an organization. By using digital platforms, companies can efficiently distribute information and training materials to a large audience. One of the primary challenges of cybersecurity training is to ensure consistent awareness without over exhausting internal resources. Digital transformation has paved the way for advanced training tools that can reach employees regardless of their geographical location or work schedule. Online courses, recorded webinars and e-learning modules offer flexible learning opportunities that can be accessed at any time and place, making it easier for employees to fit training into their schedules. Cyber threats are constantly evolving and as the client company's head of cyber engineering and operations said in the interview, updating content is required to help users understand how threats may be present, and how to respond to these threats (Interview 1 2025).

Employee engagement goes beyond just participation as it involves cultivating a mindset of vigilance and proactive involvement in cybersecurity efforts. Understanding psychological aspects such as motivation and behavioral triggers is important in tailoring programs that resonate with diverse workforce demographics (Abrahams etc. 2024, 103). These tools also make use of multimedia capabilities such as videos, animations and interactive quizzes to make the lessons more understandable and enhance the learning (McDonough 2023, 182). Gamification in cybersecurity is a good case point of utilizing the technology that is already available. Gamified modules make learning an engaging process, where employees receive points, badges and rewards for completing exercises and challenges in cybersecurity. This not only makes the method fun but also promotes ongoing participation and improvement. (Gao, Islam, Khando & Salman 2021, 10.) These technologies also support individualized learning experiences with adaptive learning systems that have the capability to customize training content in accordance with a person's job role in the company, past knowledge and experience and test scores. One size does not fit to all, and therefore different approaches are needed (Interview 1 2025). With data analysis, organizations can measure and track the success of their awareness programs. This happens through the monitoring of course completion percentages, quiz scores and participation levels. Businesses are able to determine the areas where further training is necessary and make the required changes to their programs.

6.2 Interactive cybersecurity exercises

Interactive cybersecurity exercises are an essential part of technology-supported training solutions. These exercises provide employees with hands-on experience in dealing with cyber threats, therefore allowing them to apply theoretical knowledge in practical scenarios.

Sessions promote a deeper understanding of cybersecurity principles and enhance the learning of critical information (Abrahams etc. 2024, 106). One effective method is the use of simulated cyberattacks. Simulation exercises create realistic scenarios where employees must identify and respond to various types of cyber threats such as phishing attacks, malware infections or network breaches (Nizich 2023, 139). These simulations help build confidence and competence among the workforce in handling real-world incidents. Another innovative and not so used approach is the integration of AR and VR in cybersecurity training. These are not so commonly used, due to the costs and difficult build-up. AR and VR technologies immerse users in lifelike environments where they can interact with digital elements as if they were real. (Yildirim 2025, 11-12). For example, a VR headsets can simulate a SOC environment, allowing trainees to experience the dynamic nature of threat monitoring and incident handling response firsthand.

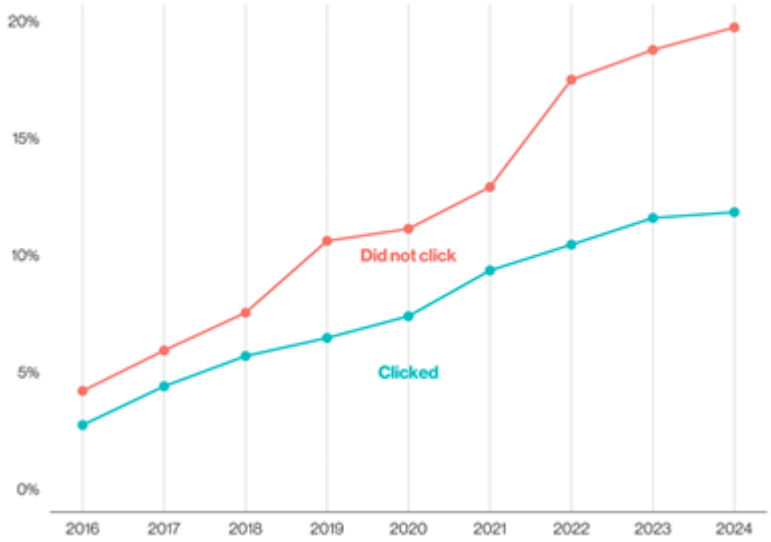

Figure 12: Trend of Phishing simulation report rate (Verizon 2025, 49)

Collaborative exercises encourage teamwork and communication among employees from different departments. Cybersecurity is not solely the responsibility of IT personnel, but it requires a collective effort from all organization members. Collaborative exercises simulate scenarios where cross-functional teams must work together to resolve security issues. (McDonough 2023, 134.) To maximize the benefits of interactive exercises, organizations should ensure that training activities are regularly updated to reflect the current threat landscapes. Many companies use known real threat actors that have happened to them or other organizations. It is important to establish metrics to assess and monitor the effectiveness and impact of cybersecurity awareness program, for example through reduced phishing click rates or increased incident reporting. Continuous improvement can be facilitated by gathering feedback from participants through periodic surveys, focus group discussions and analysis of

incident reports. (Abrahams etc. 2024, 109). Improvements made based on feedback from participants can enhance the relevance and effectiveness of these exercises (Doucet, Giamos & Léger 2024, 195). Recognizing the dynamic nature of the cybersecurity landscape requires adjusting training content and methodologies to address new and evolving cyber threats (Abrahams etc. 2024, 107). For instance, Microsoft Defender for Office 365 integrates phishing simulation capabilities, allowing security teams to create realistic attack scenarios to test employee behavior under pressure. After participation, employees receive immediate feedback explaining what they missed, reinforcing learning through experience. (Microsoft 2024g).

6.3 Case study: Hoxhunt and Metacompliance

Softwares like Hoxhunt and Metacompliance have significantly advanced training solution initiatives by integrating various educational methodologies tailored to engage employees effectively and foster a cybersecurity-conscious culture. The client of the thesis uses these training tools to enhance their employees cybersecurity skills and preparedness. Hoxhunt is an interactive training program that focuses specifically on recognizing and reporting phishing attacks. At the client's organization the primary purpose of Hoxhunt is to improve its employees ability to identify and respond appropriately to phishing attempts, which are common organizational cyber threats. One of the key features of Hoxhunt is its simulated phishing attacks, where employees regularly receive simulated phishing emails that mimic real-world threats (Hoxhunt 2024a). This helps them to practice safe responses and learn to identify suspicious messages. Each successful identification is rewarded with points and prizes that aim to increase motivation and engagement for the users in the training process. Hoxhunt also offers personalized training modules tailored to the employee's role within the organization (Hoxhunt 2024a). For example, IT department employees receive more in-depth simulations on technical security measures, while other staff are targeted with more general practices. This personalized approach ensures that each employee receives relevant and necessary training. Hoxhunt was taken into use in the Finnish Business Unit (BU) of the client company in March 2022. It was after one particular cyberattack that had effects on the clients' operations as well. Even though the attack was targeted to a geographically wide area and progressed rapidly the client company was able to shut it down in their end quickly. Their years-long global cybersecurity collaboration bore fruit, allowing them to work with other client business units to identify the threats promptly and prevent their spread effectively. (Client 2022). Over forty client employees worldwide worked for more than a week to prevent the spread of damage and repair the damage done, which was significant, but also an educational experience. They had a unique opportunity to test their cybersecurity readiness level and management measures in practice. We can be pleased that the cybersecurity protections we have built over several years served their purpose and provided us with the right kind of protection (Client 2022).

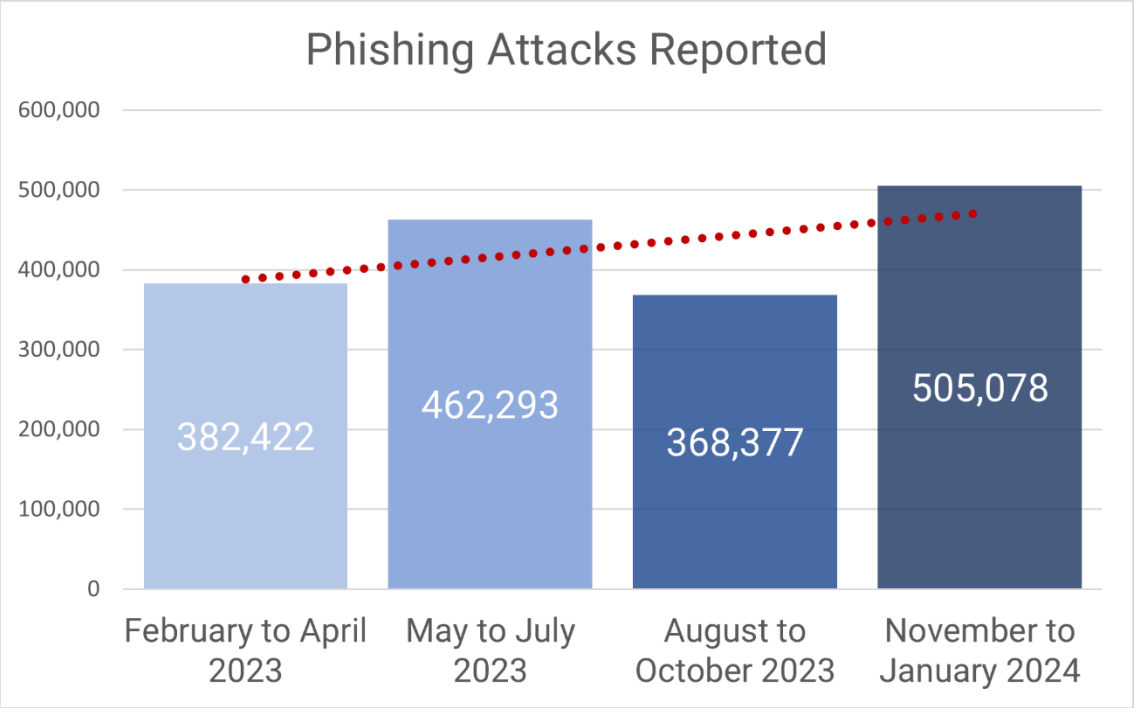

Figure 13: Phishing attack reported (Cybercrime Information Center 2024)

Metacompliance is another essential virtual training tool that is used by the client organization. It focuses more broadly on organizational security culture and compliance matters. Metacompliance provides a comprehensive range of training materials and interactive courses covering topics such as GDPR compliance, security policies and risk management. At the client's organization, Metacompliance is used on phishing trainings that is sent wider than just one Business Unit (BU). Training programs include interactive modules where employees can test their knowledge and receive immediate feedback on their performance. Videos, practical exercises and quizzes are part of this diverse training process. Metacompliance also supports internal communication between teams and individuals regarding security issues within the organization. It offers tools for creating awareness campaigns that can spread information about best security practices throughout the organization. These campaigns can effectively inform employees about new emerging threats, upcoming updates and best-known practices. (Metacompliance 2024). Metacompliance also allows data integration to be done to PowerBI, so that the management and IT department can view the results in simpler form and plan the next steps accordingly.

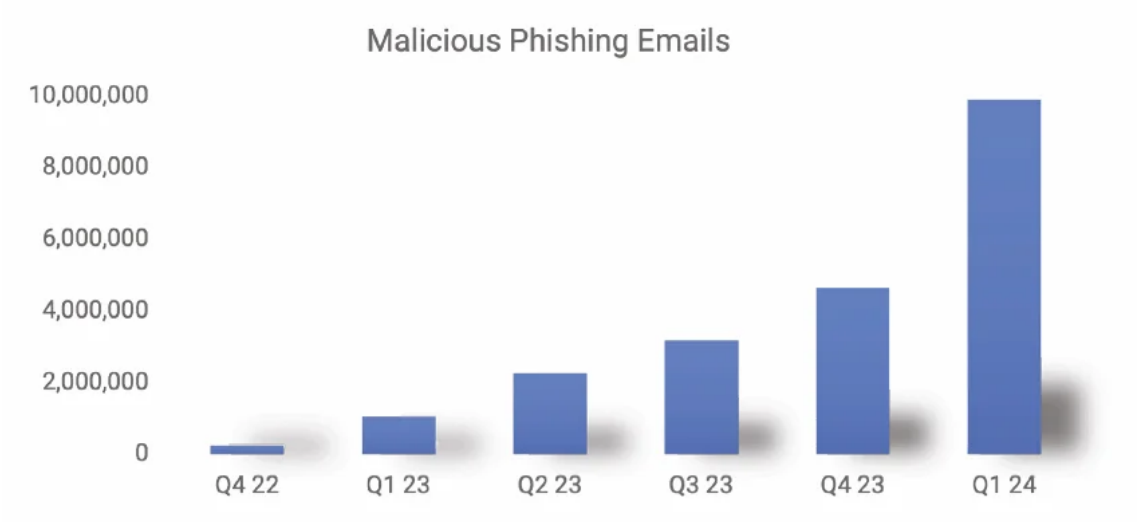

Figure 14: Phishing email trend after OpenAI introduced (SOCRadar 2024)

Virtual training tools such as Hoxhunt and Metacompliance have been deeply integrated into the client's cybersecurity strategy. These tools provide the client with the means to educate employees on recognizing cyber threats, adhering to security standards and how to operate safely in a digital environment. Through these tools, the client has the ability to enhance their employees' readiness to face cyber threats and maintain a high level of security throughout the organization. Virtual training tools should not be viewed only as mere technical aids but also as a strategic investments in the overall security of the company. Their usage promotes continuous learning and adaptability in an ever-changing cybersecurity landscape.

7 Results

The goal was to investigate the co-operation between technology and human, and their roles in organizational cybersecurity, with the focus on how technological solutions can support and enhance human efforts to protect digital assets. The research was conducted as an improvement study for a leading global construction firm’s cybersecurity department. Data for the study was gathered through interviews, academic literature, industry blogs and reports. The key findings highlight the critical roles played by AI-driven behavior analytics, automation via SIEM and SOAR platforms, real-time data utilization and technology-enhanced training in strengthening cybersecurity defenses while addressing associated challenges and proposing mitigations.

7.1 Key findings on behavioral analysis

One of the most significant findings of the thesis is the efficiency of AI-powered behavior analytics in detecting anomalies that deviate from established behavior baselines. This study

shows that the most powerful way for this is to leverage machine learning algorithm systems like User and Entity Behavior Analytics (UEBA) to monitor suspicious patterns such as mass deletions or unauthorized access attempts and other user activities continuously across multiple environments, which would include cloud services, endpoints and network traffic. The AI-driven models do not only detect known threat signatures but also uncover other threats by learning normal behavioral profiles and flagging deviations in near real-time. The integration of AI into behavior analytics would reduce the likelihood of human error in identifying threats and relieves security analysts from shifting through large volumes of benign alerts and enables prioritization of high-risk incidents for faster investigation and remediation. Challenges such as false positives require ongoing calibration and contextual awareness to maintain trust in automated detections. Nonetheless, this technology has the ability to significantly enhance situational awareness, for example within Security Operations Centers (SOCs) empowering human analysts with actionable intelligence.

Automation tools embedded within Security information and Event Management (SIEM) systems and Security Orchestration, Automation and Response (SOAR) platforms play a crucial role in alleviating the manual workload traditionally done by security teams. Technologies such as Microsoft Sentinel can enable orchestration of security workflows where alerts generated by SIEM are automatically triaged, correlated and responded by predefined workflows. It also has the capacity to trigger actions like account disabling, password resets or blocking malicious IP addresses without immediate human intervention. This automation facilitates faster incident response times and more logic in enforcing security policies. By automating repetitive tasks, these tools allow time and focus for human experts on complex threat hunting and strategic security planning. SOAR platforms promote collaboration by integrating diverse security tools into unified dashboards and this can also enhance operational efficiency. Maintaining an appropriate balance between automated responses and human oversight is crucial to avoid unintended consequences or overlooking nuanced threats.

7.2 Key findings on utilizing real-time data

There is a clear importance found in real-time data analytics in supporting effective decision-making during security incidents. Modern cybersecurity platforms are able to draw information from endpoints, network devices, cloud applications and external threat intelligence feeds to provide a comprehensive view of the threat landscape. This continuous data stream of information provided can enable rapid identification of different attack vectors and support proactive defense strategies. Technologies such as Microsoft Sentinel’s advanced fusion detection rules can scan through diverse data points to detect attacks that might otherwise evade monitoring. The enriched contextual information it can produce has the ability to reduce cognitive load on security teams by surfacing only prioritized alerts with detailed

insights. Real-time analytics can empower organizations to make data-driven decisions quickly, while minimizing potential damage from breaches or disruptions.

7.3 Key findings on technology driven cybersecurity training

Technology incorporated training solutions have proven essential in preparing employees to recognize and respond to cyber threats effectively. Interactive platforms like Hoxhunt and Metacompliance provide engaging training experiences through simulated phishing campaigns, gamified learning modules and personalized content tailored to different roles within the organization. The use of adaptive learning technologies can ensure that training remains relevant by evolving alongside emerging threat scenarios. Such training initiatives not only raise awareness but also build resilience against social engineering attacks which are one of the leading causes of cybersecurity breaches. Feedback mechanisms embedded within these platforms facilitate continuous improvement by tracking user progress and identifying areas that require more education. Technology enhanced training fosters a security-conscious culture that supports overall organizational protection.

7.4 Suggested mitigations

The research was conducted as an improvement study and mitigations work as suggestions for best use practices for medium and large organizations. To create a well-balanced and resilient defense against evolving cyber threats and to harness advanced technology while preserving ethical standards and empowering human operators, there are several steps for organizations to take. First is to establish clear governance and privacy frameworks. Organizations should develop comprehensive governance policies that define the scope and purpose of cybersecurity monitoring, and this should be done with as much transparency as possible. These developed policies must comply with data privacy laws such as GDPR, in order to ensure that only necessary data is collected and monitored. These policies and what is being monitored and why should also be clearly communicated to employees to build trust and maintain ethical standards. Incorporating ethical principles such as confidentiality, data integrity and availability into organizational culture is essential for this. Regular audits and accountability mechanisms should be introduced within the framework to ensure compliance and ethical data handling.

Deploying AI and ML based behavior analytics can significantly enhance anomaly detection by establishing dynamic behavioral baselines tailored to individual users, devices and systems. These models do require constant refinement and improvement to reduce false positives that cause alert fatigue through feedback and analyst inputs. Organizations should combine automated detection with human oversight to validate suspicious activities before escalating them. Investment in sufficient computational infrastructure is necessary to support the high demands of continuous real-time behavioral analytics.

Automation tools such as SIEM and SOAR platforms should be carefully integrated into existing cybersecurity ecosystems through phased deployment plans that prioritize interoperability and minimal disruption. Automated workflows can handle routine tasks like disabling compromised accounts or invalidate sessions based on predefined triggers, thereby accelerating response times and reducing manual errors. Organizations must avoid over-automation by designing systems that allow human intervention when complex judgment or contextual understanding is required. The establishment of clear escalation workflows ensures that critical incidents receive the appropriate level of expert attention, while routine alerts are efficiently managed. While automation increases efficiency, it cannot fully replace human expertise in cybersecurity decision-making. Organizations should foster a collaborative environment where cybersecurity personnel work alongside automated systems, receiving enriched alerts with contextual insights that aid faster and more confident decisions. Ongoing training programs must equip staff with skills to interpret AI-driven analytics and understand automation limits. Organizations should also implement protocols for regular review of automated actions to detect potential errors or gaps in coverage, maintaining a safety net through human judgment.

Cybersecurity awareness programs should leverage technology-enabled platforms that offer interactive, engaging training tailored to different employee roles and skill levels. Solutions like simulated phishing campaigns create realistic scenarios allowing employees to practice threat recognition safely, while gamification elements increase motivation and retention of knowledge. To remain relevant and effective, training content must be continually updated based on emerging threats, incident reports and participant feedback. Leadership endorsement is crucial to reinforce the importance of cybersecurity practices organization wide. Metrics such as reduced phishing click rates and improved reporting of suspicious activity help measure program success and inform ongoing improvements.

8 Conclusion

The results of the thesis highlight that by combining advanced technological solutions alongside with human factors, organizations can improve their overall cybersecurity posture. AI-driven behavior analytics can add anomaly detection capabilities and automation via SIEM/SOAR platforms have the ability to reduce manual workloads and accelerate response times. Real-time data analytics can give more insight into informed decision-making and technology-supported awareness training has the capability to elevate staff readiness against cyber threats. It should be noted that the implementation of these measures must be carefully balanced against issues such as privacy concerns, legal constraints, system complexity and the need for human expertise.

Without this balance in place these actions may have the potential to do more harm than good. Organizations that embrace this synergy between technology and human may achieve more effective defense mechanisms that are capable of adapting to dynamic cyber threat environments.

Technological solutions that are designed for supporting users' daily activities should be made with user-centric designs that focus on simplicity, usability and automation. By creating intuitive interfaces for the users and integrating automated threat detection and response features in them, these solutions will reduce the cognitive load that will be presented on users and therefore help to prevent them from making mistakes such as misconfigurations or acting unsafe. Automation tools embedded in platforms like Microsoft Sentinel can automate routine security tasks such as alert triage and account management and this will minimize human intervention and errors related to it. Supportive training modules that educate users about common threats and safer practices would further help reduce errors.

In order for AI-driven behavior analytics to be able to detect anomalies, a behavioral baseline for users, devices or applications must be established. This can be done by continuous monitoring and historical data analysis. After the baseline is established machine learning models then analyze current behavior against these to identify deviations that indicate of potential threats. Technologies such as User and Entity Behavior Analytics (UEBA) can extend this by withdrawing data from multiple sources such as users, servers and endpoints and by applying sophisticated algorithms to detect subtle or rare anomalies like lateral movement or low-and-slow attacks that traditional signature-based systems might miss. With real-time behavioral analysis organizations can respond to detected anomalies quickly and minimize the exposure windows.

Manual workload can be significantly reduced by automating repetitive tasks within cybersecurity orchestration workflows. SIEM and SOAR platforms do this by automatically creating and handling alerts, correlating incidents across multiple data sources and executing predefined workflows such as disabling accounts or resetting passwords. With these tools this can be without requiring constant human intervention, which on the other hand reduces alert fatigue among analysts and frees them to focus on more complex investigations and strategy development. Automation also can streamline incident response time and ensure consistent enforcement of different security policies.

The integration of real-time data and analytics can empower organizations to respond more faster and more accurately to emerging cyber threats. This is achieved with the systems delivering constant, up-to-date visibility into organization’s security environment. Real-time data and analytics collect information from several sources such as network flows, endpoint activities, cloud usage and external threat intelligence. With this data security systems can

construct a detailed, contextual picture of ongoing incidents. Advanced detection mechanisms like Microsoft Sentinel's fusion rules have the ability to synthesize this data to uncover even sophisticated multi-phase attacks quickly. The insight given by real-time data does not only accelerate the identification of critical threats but also gives support to security teams by filtering out the extra noise, thereby enabling them to focus on high-priority issues and make better informed mitigation decisions that limit potential harm.

Interactive security exercises serve as practical training tools that can engage employees in different simulated cyberattack scenarios, therefore allowing them to actively apply their own prior knowledge in detecting and responding to threats. Phishing simulations, game-like challenges and role-specific adaptive learning modules offered through platforms like Hoxhunt and Metacompliance help implement a critical view on cyber-related matters in an engaging manner. These programs can provide immediate feedback on users performance and help participants recognize vulnerabilities in their own understanding or internet behavior. This approach on awareness education cultivates heightened awareness and proactive security habits among the workforce, which in exchange bolsters the organization's cyber defense by reducing the risk posed by human-related vulnerabilities.

References

Abrahams, T., Farayola, O., Kaggwa, S., Uwaoma, P., Hassan, A., Dawodu, S. 2024. Cybersecurity Awareness and Education Programs: A Review of Employee Engagement and Accountability. Computer Science & IT Research Journal, 5(1). https://doi.org/10.51594/csitrj.v5i1.708

Ashton, D. The Digital Shield: AI in Cyber Defense. 2024. Ebookit.com

Bellis, E., Roytman, M. 2023. Modern Vulnerability Management: Predictive Cybersecurity. Artech House.

Bertino, E. Machine Learning Techniques for Cybersecurity. 2023. Springer International Publishing.

Binnar, P., Bhirud, S., Kazi, F. Security Analysis of Cyber Physical System Using Digital Forensic Incident Response. 2024. https://www.sciencedirect.com/science/article/pii/S2772918423000218

Bossomaier, T. & Miller S. Cybersecurity Ethics and Collective Responsibility. 2024. Oxford University Press. United States of America

Brathwaite, S. Cybersecurity Law: Protect Yourself and Your Customers. 2019. Business Expert Press. Unites States of America

CLDigital. 2024. Data-Driven Business Continuity Plan: The Role of Technology in Building Resilient Enterprises. Accessed 30.4.2025. https://cldigital.com/blog/data-driven-business-continuity-plan-the-role-of-technology-in-building-resilient-enterprises/

Cloudsek. The Biggest Supply Chain Hack Of 2025: 6M Records Exfiltrated from Oracle Cloud affecting over 140k Tenants. Accessed 20.4.2025. https://www.cloudsek.com/blog/the-biggest-supply-chain-hack-of-2025-6m-records-for-sale-exfiltrated-from-oracle-cloud-affecting-over-140k-tenants

CyberRiskInsight. 2025. Cybersecurity Automation: Balancing Efficiency and Human Oversight for Robust Security. Accessed 30.4.2025. https://www.cyberriskinsight.com/operations/cybersecurity-automation-balancing-efficiency-human/

Cybercrime Information Center. 2024. Phishing Trends: November 2023 - January 2024. Accessed 1.5.2025. https://www.cybercrimeinfocenter.org/phishing-trends-november-january-2024

Cybersecurity News Everyday. 2023. AI and the Five Phases of the Threat Intelligence Lifecycle. Accessed 29.3.2025. https://www.hendryadrian.com/ai-and-the-five-phases-of-the-threat-intelligence-lifecycle-mandiant/

Dahj, J. 2022. Mastering Cyber Intelligence: Gain Comprehensive Knowledge and Skills to Conduct Threat Intelligence for Effective System Defense. Packt Publishing Limited.

Digitaldefynd. Top 40 Cybersecurity Case Studies. Accessed 14.4.2025. https://digitaldefynd.com/IQ/cybersecurity-case-studies/

Doucet, O., Giamos, D., Léger, P. 2024. Continuous Performance Feedback: Investigating the Effects of Feedback Content and Feedback Sources on Performance, Motivation to Improve Performance and Task Engagement, Journal of Organizational Behavior Management, 44:3, 194-213. https://www.tandfonline.com/doi/epdf/10.1080/01608061.2023.2238029?needAccess=true

Edureka. 2025. AI vs Machine Learning vs Deep Learning. Accessed 29.2.2025. https://www.edureka.co/blog/ai-vs-machine-learning-vs-deep-learning/

ENISA. 2022. ENISA Threat Landscape 2022. Accessed 26.4.2025. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Fox, P., Edwards, J., Snyder, F., Makinson, K., Hamby, D. 2013. The Effect of Cognitive Load on Decision Making with Graphically Displayed Uncertainty Information. Risk analysis: an official publication of the Society for Risk Analysis. https://www.researchgate.net/publication/259393290_The_Effect_of_Cognitive_Load_on_Decision_Making_with_Graphically_Displayed_Uncertainty_Information

Hoxhunt 2024a. Automate Phishing Training, Your Way. Accessed 11.4.2025. https://hoxhunt.com/product/phishing-training

IBM Corporation. 2024. Cost of a Data Breach Report 2024. Accessed 27.4.2025. https://www.ibm.com/reports/data-breach

Kerner, S. 2025. 35 cybersecurity statistics to lose sleep over in 2025. TechTarget. Accessed 18.4.2025. https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020

Kosinski, M. 2024. What is user behavior analytics (UBA)?. IBM. Accessed 29.4.2025. https://www.ibm.com/think/topics/user-behavior-analytics

Manda, K. Cybersecurity Automation in Telecom: Implementing Automation Tools and Technologies to Enhance Cybersecurity Incident Response and Threat Detection in Telecom Operations. 2021. https://acadexpinnara.com/index.php/acs/article/view/370

McDonough, B. Cyber Guardians: Empowering Board Members for Effective Cybersecurity. 2023. Wiley & Sons. United States of America

Metacompliance. Advanced Cyber Security Training for Employees: Engaging, Multilingual eLearning Solutions. Accessed 11.4.2025. https://www.metacompliance.com/cyber-security-training-for-employees?_gl=1*zxil1n*_up*MQ..*_gs*MQ..&gclid=EAIaIQobChMIr-L0yrnQjAMVMheiAx3KtAYwEAAYAiAAEgK7NvD_BwE

Microsoft 2024a. Anomalies detected by the Microsoft Sentinel machine learning engine. Accessed 25.4.2025. https://learn.microsoft.com/en-us/azure/sentinel/anomalies-reference#anomalous-data-destruction

Microsoft 2024b. Microsoft Defender for Cloud Apps overview. Accessed 25.4.2025. https://learn.microsoft.com/en-us/defender-cloud-apps/what-is-defender-for-cloud-apps

Microsoft 2024c. Create Defender for Cloud Apps anomaly detection policies. Accessed 25.4.2025. https://learn.microsoft.com/en-us/defender-cloud-apps/anomaly-detection-policy

Microsoft 2024d. Conditional Access app control in Microsoft Defender for Cloud Apps. Accessed 26.4.2025. https://learn.microsoft.com/en-us/defender-cloud-apps/proxy-intro-aad

Microsoft 2024e. What is Conditional Access?. Accessed 28.4.2025. https://learn.microsoft.com/en-us/entra/identity/conditional-access/overview

Microsoft 2024f. Azure Logic Apps for Microsoft Sentinel playbooks. Accessed 28.4.2025. https://learn.microsoft.com/en-us/azure/sentinel/automation/logic-apps-playbooks

Microsoft 2024g. Simulate a phishing attack with Attack simulation training. Accessed 18.4.2025. https://learn.microsoft.com/en-us/defender-office-365/attack-simulation-training-simulations

Microsoft 2024h. Advanced threat detection with User and Entity Behavior Analytics (UEBA) in Microsoft Sentinel. Accessed 30.4.2025. https://learn.microsoft.com/en-us/azure/sentinel/identify-threats-with-entity-behavior-analytics

Microsoft 2024i. 2024. Configure multistage attack detection (Fusion) rules in Microsoft Sentinel. Accessed 30.4.2025. https://learn.microsoft.com/en-us/azure/sentinel/configure-fusion-rules

Nizich M. The Cybersecurity Workforce of Tomorrow. 2023. Emerald Publishing Limited

Ozkaya, E. Cybersecurity: The Beginner's Guide. 2019. Packt Publishing Ltd. United Kingdom

Prokopets, M. N.D. What is Microsoft Cloud App Security? Is it Any Good? Nira Blog. Accessed 1.4.2025. https://nira.com/microsoft-cloud-app-security/

Proofpoint. 2025. What is Telemetry? Accessed 4.5.2025. https://www.proofpoint.com/br/node/131601

Sarker, I. Machine Learning for Intelligent Data Analysis and Automation in Cybersecurity: Current and Future Prospects. 2022. Annals of Data Science. https://link.springer.com/article/10.1007/s40745-022-00444-2

SecureLayer7. 2024. A Guide to the Top 10 Threat Intelligence Tools. Accessed 10.4.2025. https://blog.securelayer7.net/threat-intelligence-tools/

Security Innovation. 2023. Ponemon Cybersecurity Training Study Finds Significant Shifts In Cybersecurity Training Over Past Two Years with 24% Higher Use of Simulated Environments. Accessed 18.4.2025. https://www.securityinnovation.com/ponemon-cybersecurity-training-study-finds-significant-shifts-in-cybersecurity-training-over-past-two-years-with-24-higher-use-of-simulated-environments/

Securonix. 2024. Behavioral Analytics in Cybersecurity. Accessed 29.4.2025. https://www.securonix.com/blog/behavioral-analytics-in-cybersecurity/

Sharma, S. Data Privacy and GDPR Handbook. 2020. Wiley & Sons. United States of America

Sharma, G., Thakur, A., & Tiwari, C. 2024. Developing a Comprehensive Framework for User and Entity Behavior Analytics (UEBA). https://research-reels.com/wp-content/uploads/2024/08/Developing-a-Comprehensive-Framework-for-User-and-Entity-Behavior-Analytics-UEBA.pdf

SOCRadar. 2024. Phishing in 2024: 4,151% Increase Since Launch of ChatGPT; AI Mitigation Methods. Accessed 29.4.2025. https://socradar.io/phishing-in-2024-4151-increase-since-chatgpt/

Softprom. 2021. What is SOAR? Accessed 27.3.2025. https://softprom.com/how-to-increase-the-productivity-of-security-centers-by-an-order-of-magnitude-and-another-2-times

Son, J., Chinedum, I., Fitzgibbons, P. 2012. Virtual Lab for Online Cyber Security Education, Communications of the IIMA: Vol. 12: Iss. 4, Article 5. https://scholarworks.lib.csusb.edu/ciima/vol12/iss4/5?utm_source=scholarworks.lib.csusb.edu%2Fciima%2Fvol12%2Fiss4%2F5&utm_medium=PDF&utm_campaign=PDFCoverPages

Splunk. 2024a. State of Security – The Race to Harness AI.

Splunk. 2024b. The Essential Guide to SOAR.

Statista. 2025. Annual number of cyberattacks worldwide from 2016 to 2023. Accessed 10.4.2025. https://www.statista.com/forecasts/1485031/cyberattacks-annual-worldwide

Teachflow. 2023. The Role of Technology in Personalized Learning. Accessed 31.4.2025. https://teachflow.ai/the-role-of-technology-in-personalized-learning/

Tounsi, W., Rais, H. 2018. Technical threat intelligence in sophisticated attacks. Computers & Security, 72, 212–233. https://www.sciencedirect.com/science/article/pii/S0167404817301839

Truitte, K. 2019. An Unpatchable Exploit: The Human Vulnerability in Cybersecurity. Georgetown Security Studies Review. Accessed 19.04.2025. https://georgetownsecuritystudiesreview.org/2019/08/23/an-unpatchable-exploit-the-human-vulnerability-in-cybersecurity/

Verizon. 2025. 2025 Data Breach Investigations Report. Accessed 28.4.2025.

https://www.verizon.com/business/resources/reports/dbir/

Watts, S. 2023. Real-Time Data: An Overview and Introduction. Accessed 14.4.2025.

https://www.splunk.com/en_us/blog/learn/real-time-data.html

Wickramasinghe, S. 2023. Behavioral Analytics in Cybersecurity. Splunk. Accessed 29.4.2025.

https://www.splunk.com/en_us/blog/learn/behavioral-analytics.html

Wilson, A. 2025. Data Threat Analytics: How Real-Time Insights Enhance Cybersecurity. IMS Cloud Services. Accessed 22.4.2025. https://www.imscloudservices.com/knowledge-base/security-articles/data-threat-analytics-how-real-time-insights-enhance-cybersecurity/

Yildirim, E. 2025. Exploring Realities: XR, VR, AR, MR, AV and Beyond in Architecture. All Sciences Academy. https://www.researchgate.net/profile/Erdem-Yildirim-6/publication/389913211_Exploring_Realities_XR_VR_AR_MR_AV_and_Beyond_in_Architecture/links/67d888f735f7044c9231b459/Exploring-Realities-XR-VR-AR-MR-AV-and-Beyond-in-Architecture.pdf

The language and style of this text have been improved using organizations' internal Generative AI tool.

Unpublished references

Client 2022. At XX, Safety is taken seriously – including cybersecurity. Intranet posting.

Interview 1. 2025. Head of Cybersecurity and Operations. 10.4.2025. The client company.

Figures