jamk

Enhancing Cybersecurity Resilience: Proactive Strategies Utilizing Microsoft Defender XDR Tools

Fatih Gulusen

Master's thesis
May 2025
Degree Programme in Information Technology
Cyber Security

jamk | Jyväskylän ammattikorkeakoulu
University of Applied Sciences

jamk

Description

Gulusen, Fatih

Master's Degree Programme in Information Technology, Cyber Security

Jyväskylä: Jamk University of Applied Sciences, May 2025, 60 pages

Master's Degree Programme in Information Technology, Cyber Security

Permission for open access publication: Yes

Language of publication: English

Abstract

The continuous change and development of the cyber landscape and the technologies used necessitate the development of different approaches against increasing threats. Organizations cannot protect themselves against these complicated attacks and remain vulnerable to attacks when traditional approaches and technologies are not sufficient. Integrating proactive strategies into defense processes provides organization great advantages in cyber defense. Microsoft Defender XDR provides various tools to the organizations. These tools and technologies can be utilized to implement proactive strategies into processes and eliminate threats before they occur. Strategies that will increase organizations' cyber resilience using these tools offered by Microsoft Defender XDR are discussed with sample case studies. Technologies and tools like Exposure management, Attack path analysis, security posture management and attack simulation training are discussed, and best practices are explained and implemented to the processes. In this thesis, a framework has been tried to be presented. Organizations can use all these tools and technologies, or they can use some of them due to reasons such as license limitations or they can create their own models. As a result, the findings show that there are different and effective models for organizations to utilize Microsoft Defender XDR tools proactively.

Keywords/tags (subjects)

Cybersecurity, Proactive security, Defender, XDR

Miscellaneous (Confidential information)

Work is public. Information is anonymized and it does not contain any confidential information

Contents

Figures

Tables

1 Introduction

This thesis was assigned by a Finnish IT-Services provider company to develop and improve Microsoft security services and make contributions to the literature.

The absence of research in this area highlights the importance of the research. Additionally, the research emphasizes theoretical exposition, practical use, and implementation of modern approaches in real-world environments. This research aims to provide a practical, real-world framework for adopting proactive cybersecurity using Microsoft Native Tools in Microsoft-based environments. While there are studies on cyber threats and their mitigation, there are no studies discussing the transition from reactive defense and monitoring approaches to proactive approaches supported by Microsoft Defender XDR. The best practices of Microsoft and cyber industry are used in configuring and using the tools. This research addresses modern tools and threats theoretically and focuses on technical implementation and testing of Microsoft Defender XDR solutions practically.

Reactive cybersecurity models no longer suffice, as digital transformation continues. Organizations must adopt a proactive security posture that not only responds to threats but anticipates them to remain resilient. This thesis examines how proactive cybersecurity strategies help organizations to enhance their ability to prevent, detect, and respond to advanced threats in real time, by using Microsoft Defender XDR tools

Foundational understanding in cyber security is discussed in the first part, by examining key cybersecurity concepts and the current cyber threat landscape theoretically. Essential terminology, key concepts, attack types, and the organizational impact of cyber incidents, including financial losses, reputational harm, operational disruption, and legal consequences are discussed (Edwards, J., 2024). Understanding these impacts is critical to appreciating why proactive measures are not only

beneficial, but necessary. Following this, the study delves into detection and response technologies, offering a comparative look at Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR). Each tool is examined in terms of its capabilities, limitations, and role in the evolving cybersecurity ecosystem. Special attention is given to XDR technologies, and how Microsoft Defender XDR expands traditional detection tools by unifying signals across endpoints, identities, applications, and networks to provide contextual, cross-domain visibility.

One of the most important parts of the study is proactive and reactive security, since it is crucial to understand these concepts. The thesis contrasts reactive and proactive approaches to cybersecurity. What are the differences, limitations and effects of these approaches and how they help organizations in their defense strategies. Reactive strategies focus on responding to incidents after compromise, often with high cost and limited control. In contrast, proactive approaches emphasize prevention, early detection, continuous monitoring, and training from a passive stance to a dynamic, anticipatory posture.

Key proactive capabilities such as exposure management, attack path analysis, security posture management and user awareness training, are discussed in depth. These tools and strategies are assessed for their practical effectiveness, ease of implementation, and contribution to overall security resilience. Microsoft Secure Score and other native metrics are used to measure improvements in the organization's threat readiness.

Proactive security is a very trendy topic and approach in the security world as most of the vendors develop exposure management tools. It is important to research the use cases of these tools/approach in practice in real world. I think it will make significant contributions to literature and proactive security concepts. The goal of the thesis:

- To explore the proactive development of cybersecurity posture using Microsoft Defender XDR tools based on exposure management.
- To evaluate the effectiveness of Microsoft Defender XDR tools in proactively developing and maintaining a strong cybersecurity posture and security awareness.
- To develop an effective proactive cyber security strategy model for organizations

2 Research methodology

2.1 Research Questions

The research questions on this thesis are:

a. How do organizations benefit from implementing Microsoft Defender XDR in their cybersecurity strategy?

b. How can Microsoft Defender XDR tools be utilized to proactively enhance cybersecurity posture?

c. What are the key features of Microsoft Defender XDR that contribute to exposure management, security posture and threat detection and security awareness?

2.2 Research methods

This thesis aims to provide intermediate information about proactive cybersecurity, Microsoft Defender XDR tools and their implementation and use in practice in a specific context. Constructive case studies are used to implement proactive strategies in the real world with the construction of how to enhance cyber resilience by using proactive strategies. Semi quantitative analysis is used to evaluate and compare security posture by using secure score changes.

2.3 Research Ethics

The research is conducted in accordance with accepted ethical standards and guidelines. All the software and tools used in the research have been licensed appropriately.

The research process has been implemented in a way that allows for ethical integrity, and nothing has been done that could lead to harm to individuals or groups. Privacy and autonomy were never violated, and all practical exercise was carried out in an anonymized context.

Academic honesty is a guiding principle of this work. Plagiarism in which another person's ideas or results are presented as one's own is eschewed under all circumstances. Sources of information, texts, resources, and ideas have been properly acknowledged and accurately cited in the thesis.

Furthermore, due care has been taken to verify the validity and reliability of the materials used. This involves assessing authors' expertise, publication or platform credibility, and the information's relevance and precision given. The work is solidly grounded on sound theories and models in the field of cybersecurity, thus ensuring academic as well as real-world rigor.

3 Cybersecurity and Current Cyber Threats

In today's digital world, cybersecurity has become more critical and complex than ever. Organizations, institutions, governments, even individuals inevitably rely on technology. As a result of this, risk continues to grow. Cybercriminals use sophisticated attack techniques with different motivations. At that point, organizations must adopt robust and holistic defense strategies and use modern approaches in both administrative and technical side.

In this chapter we introduce and discuss general terms of cybersecurity. What is the general definition of cybersecurity, the concepts of cybersecurity, types of threats and the impact of these threats on organizations.

3.1 Definition and Key concepts

When we are talking about cybersecurity, it is important to understand what we are trying to protect and how we ensure security. Cybersecurity is the practice of protecting networks, devices, and data from unauthorized access, damage, or malicious activities. Its main goal is to ensure confidentiality, integrity, and availability of information, so that data remains secure and is used appropriately (Cisa, 2021.). Confidentiality, Integrity and Availability concepts should be described to understand the scope of cybersecurity in real life. These core principles are called CIA triad.

C is Confidentiality. Confidentiality means that only authorized individuals have access to sensitive information and resources, helping to protect data from being exposed to unauthorized users (Chapple, M., 2024). Various measures are used to provide confidentiality and ensure that only the authorized individuals have access to resources and sensitive data. These are, encryption, access controls, Multi Factor Authentication (MFA), security tokens etc. (Outsource accelerator ,2024.).

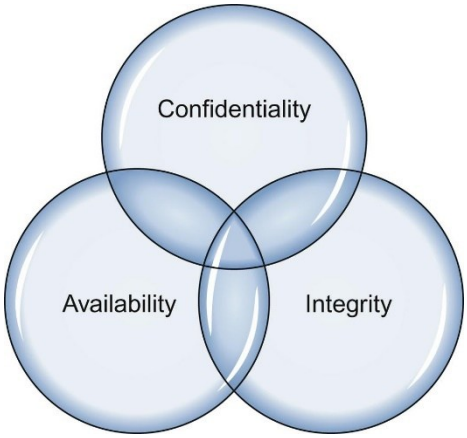


Figure 1 CIA Triad

Integrity means making sure that data remains accurate and unaltered by anyone who isn't authorized to change it. It's important that information is verified and kept consistent, and organizations need to be able to detect and undo any unauthorized modifications. Maintaining data integrity is a vital part of cybersecurity, and there are various tools and techniques used to protect it — such as encryption, hashing, digital signatures, Data Loss Prevention (DLP) systems, and digital certificates (Andress, J., 2014).

A, stands for Availability. Availability means making sure that data and resources are always accessible to authorized users whenever they need them. This is essential for keeping information systems reliable and fully functional (Fruhlinger, J., 2020). Enhanced network security, DDoS prevention, disaster recovery plans etc. are examples of security measures, which are used to provide availability.

3.2 Types of Cyber Threats

In the rapidly evolving digital landscape, understanding the various types of cyber threats is crucial for developing effective security measures. This section discusses common cyber threats.

Common Types of Cyber Threats

1- Malware

Malware or malicious software is a script, piece of code or software designed to gain unauthorized access to systems. Viruses, worms, ransomware, keyloggers are specific examples of malware. Attackers can gain unauthorized access to systems, access sensitive data or affect the operation of systems. They pose one of the most fundamental challenges for cybersecurity (Gharibi, 2011). Websites, emails, SMS messages and nowadays QR codes are commonly used to spread malware.

2- Phishing

Phishing is an attack that uses different tools and methods to help attackers gain access to systems by presenting themselves as a trusted source to users. Attackers design systems where users can reveal sensitive content such as passwords and financial information. They aim to exploit the weaknesses of human psychology (UC Berkeley, 2024).

3- Social engineering

Social engineering is a cyber-attack that uses people's trust to gain information or access. It targets people, rather than technical vulnerabilities. For example, an attacker may attempt to obtain passwords, private information, or system access by posing as an authorized person. Social engineering attacks are typically conducted over the phone, email, or in-person and are designed to trick people into trusting them (IBM, 2024).

Emerging Threats and Trends

In today’s complicated digital world, it is crucial to understand advanced and emerging threats for organizations, institutions and individuals to act against them.

1- Advanced Persistent Threats (APTs)

APT is a type of cyber-attack carried out with long-term and covert means against the targeted organization. These attacks attempt to remain unnoticed for a long time after infiltrating an institution or individual, to collect information or to cause harm. APT attacks are usually very complex, planned and multi-stage; attackers aim to gain permanent access to systems and access the data they want (Daksh et al., 2023).

2- Artificial Intelligence (AI)-Driven Cyber Attacks

AI-powered cyber-attack is when attackers use artificial intelligence (AI) and machine learning technologies to carry out more complex, faster and more effective cyber-attacks. It is used in target selection and reconnaissance, social engineering, automation or vulnerability discovery phases (Guembe et al., 2022).

3- Internet of Things (IoT) Vulnerabilities

IoT (Internet of Things) vulnerabilities are weaknesses found in devices and systems connected to the Internet like printers and smart TVs. These weaknesses can allow attackers to gain unauthorized access to devices, steal data, or misuse devices. These vulnerabilities are usually missing updates, use of vulnerable protocols, no standardization etc. (NIST, 2021).

4- Insider Threats

Insider threats are security risks created intentionally or unintentionally by employees, managers or authorized people within an organization. These people can damage the system, steal or disclose confidential information due to their access rights (Mason, J and Amelia, O., 2024).

5- Ransomware Evolution

Ransomware attacks can be described as attacks where attackers gain access to systems, often by exploiting vulnerabilities such as a user's credentials, misconfigurations, or weak encryption, and encrypting sensitive data by using sophisticated encryption techniques. Studies show that ransoms and damages are in millions of dollars (Wasif, S, Shabir, G., 2024).

Addressing these evolving and emerging threats, developing a culture of awareness, and conducting continuous research and collaboration is crucial.

3.3 Impact of Cyber Threats on Organizations

Increasing cybersecurity issues and threats are causing financial, operational, or reputational damage. The impacts of cyber threats on organizations are discussed in this section.

1- Financial Implications

Current data shows that cyberattacks cause significant financial losses to organizations. This can be caused by legal liability, direct ransoms, or regulatory penalties from governments. A cyber incident that results in the theft of customer or user information can cause significant financial losses and reputational damage (Agrafiotis et al, 2018).

2- Operational Disruptions

Business operations can be disrupted because of cyber threats. For example, DDoS attacks or ransomware attacks can bring business operations to a standstill because systems are rendered inoperable (Kala, E., 2023).

3- Legal and Regulatory Consequences

Organizations must adhere to various legal and regulatory requirements to protect the data they collect and use. As cyber-attacks become more complex every day, it is important for organizations to constantly follow changing regulations to avoid these legal issues. Regulations such as GDPR, NIS2, PCI-DSS are examples of these regulations (Liu, C., Babar, M. A., 2024).

4 Detection and Response Technologies

The world of cybersecurity is changing rapidly. Organizations use different tools to identify, analyze, and respond to evolving threats. The main types of these tools include Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR). Knowing the differences between these tools, how they work, and their strengths

and weaknesses is important for creating a strong security plan. In the dynamic world of cybersecurity, attack vectors have also increased with the proliferation of cloud services, the use of Internet of Things (IoT) devices, and remote working. Newly implemented technologies bring new security problems and new challenges to overcome. Additionally, cybercriminals are constantly evolving their techniques, tactics and processes, forcing organizations to find more proactive and innovative solutions to threat. At that point, evet the solutions like antivirus software or firewalls still have an important place in protecting the assets, modern strategies need to go beyond traditional solutions. Organizations need more holistic approaches and modern tools to identify, investigate and mitigate threats that threaten different layers of the IT infrastructure. Early detection and effective response to malicious attacks reduces potential damage and ensures business continuity. As a result, organizations increasingly need tools that integrate with real-time monitoring, AI-powered tools, automated responses and threat intelligence. The three main categories of these tools are Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR), and Extended Detection and Response (XDR). These technologies are core components of many security architectures that provide the capabilities needed to detect, analyze, and respond to a variety of cyber threats. Understanding their functions, differences, and benefits is vital for organizations to build strong and comprehensive cybersecurity frameworks.

4.1 Security Information and Event Management (SIEM)

SIEM systems collect log data from sources owned by the organization, including servers, network devices, applications, and cloud systems, through pre-configured configurations. By correlating these events, they provide real-time monitoring of potential security incidents. Automation provides the opportunity for rapid and automated responses to specific threats. They are also crucial for providing the necessary log source for security reporting and post-incident forensic investigations (Paloaltonetworks, 2024). SIEM solutions monitor environments reactively and if there is a suspicious activity it alerts the security team.

Benefits of using SIEM systems

Using SIEM systems offers several key benefits for organizations:

1- **Improved Threat Detection**: SIEM systems collect data from various sources in real time. The data is correlated and parsed to improve the detection capabilities and identify threats effectively.

2- **Efficient Incident Response:** Monitoring alerts and security incidents from a single view and the ability to use automation enables faster and more efficient responses.

3- **Enhanced Compliance Management:** SIEM systems help organizations fulfill their legal and compliance requirements and responsibilities by using reporting and advanced auditing capabilities.

4- **Centralized Security Data Management:** SIEM systems collect the data from various sources and correlate them to provide easier management.

5- **Reduced Security Management Costs:** SIEM systems help to reduce overall costs by increasing security operations efficiency and using automation (Sentinelone, IBM, n.d.).

4.2 Endpoint Detection and Response (EDR)

EDR solutions are designed to monitor and protect endpoint devices. Unlike traditional products, they collect and analyze data collected from devices, enabling rapid response. They use user and device behavior algorithms, as well as automatic orchestration features, to perform incident and threat analysis based on these patterns (Crowdstrike n.d.).

Benefits of Using Endpoint Detection and Response (EDR)

Endpoint detection and response (EDR) solutions use advanced techniques such as automated responses, behavioral algorithms, and advanced threat detection to continuously monitor endpoints such as end-user computers, servers, and mobile devices, enabling security professionals to effectively combat complex and sophisticated threats.

1. **Real-Time Threat Detection and Monitoring**: EDR solutions help security professionals respond to advanced and complicated threats like zero-day threats, ransomware, or advanced persistent

threats (APTs). EDR solutions use advanced techniques like behavioral analytics, machine learning, and threat intelligence to analyze these unexpected activities (Gartner, 2019).

2. Faster Incident Response and Mitigation: Security professionals can use automations in some incident response actions by using EDR solutions. These are:

1. Compromised device isolation from the network.
2. Terminating malicious process termination and detailed analysis.
3. Blocking or auditing known indicators of compromise (IoCs) in real time **(**Microsoft Learn, n.d).

3. Improved Threat Hunting Capabilities: EDR solutions provide enhanced tools to analyze past events through advanced logging. Security professionals can review these events and proactively analyze the environment (MITRE, n.d.).

4. Integration with Other Security Tools: Modern EDR platforms can be a part of a security eco-system and work with other solutions in the background. These are:

- SIEM (Security Information and Event Management) for centralized log management.
- XDR (Extended Detection and Response) to provide a broader view of security by including diverse systems.
- Threat intelligence platforms for more affective threat detection.

This seamless integration makes it possible to enrich security monitoring by merging the endpoint data with cloud, network or modern work systems (IBM, n.d.).

4.3 Extended Detection and Response (XDR)

Extended Detection and Response (XDR) is designed to provide effective and automated threat detection and response across different security components like endpoints, collaboration tools, cloud systems etc. EDR solutions focus only on endpoint security, however XDR additionally brings various security layers together to enhance the overall security posture of the organizations (Gartner, 2024).

Operational Mechanism of Extended Detection and Response (XDR)

XDR collects and analyzes telemetry data from various security tools, applies AI-driven analytics, and enables automated or manual response actions.

1- Data Collection and Correlation

XDR aggregates real-time security data from multiple sources, including:

- Endpoints (laptops, desktops, mobile devices)
- Networks (firewalls, intrusion detection/prevention systems)
- Cloud applications (SaaS, IaaS, PaaS)
- Identity and access management (IAM) solutions
- XDR (Extended Detection and Response) identifies complex, multi-step attacks by analyzing and linking security data, which might otherwise be missed by standalone security systems (MITRE, 2024).

2- Threat Detection Using AI & Behavioral Analytics

XDR leverages machine learning (ML) and behavioral analytics to detect:

- Advanced Persistent Threats (APTs)
- Zero-day malware
- Phishing and email threats
- Insider threats (Microsoft, n.d.).

3- Automated and Manual Incident Response:

XDR enables automated remediation actions, such as:

- Isolating compromised endpoints
- Blocking malicious IPs and domains
- Quarantining suspicious emails
- Enforcing identity protection measures

Security analysts can also perform manual investigation and threat hunting via a centralized XDR dashboard (Palo Alto Network, n.d.).

Comparing XDR with Other Security Solutions

Table 1 provides a comparative overview of the features offered by XDR and other security solutions.

FEATURE	EDR (ENDPOINT DETECTION & RESPONSE)	SIEM (SECURITY INFORMATION & EVENT MANAGEMENT)	XDR (EXTENDED DETECTION & RESPONSE)
SECURITY FOCUS	Endpoints only	Logs from multiple sources	Unified cross-domain detection
THREAT CORRELATION	Limited to endpoint activity	Requires manual rule creation	AI-driven automatic correlation
AUTOMATION	Basic remediation	Manual response workflows	Automated incident response
VISIBILITY	Device-level only	Requires complex integrations	Unified, real-time monitoring
ALERT FATIGUE REDUCTION	No	No	Yes (AI-driven filtering)

Table 1 XDR comparison with other tools

5 Proactive vs. Reactive Cybersecurity Approaches

In today's fast-paced digital world, organizations must deal with numerous cyber threats, making strong security strategies essential. Cybersecurity can be divided into two main strategies: Reactive cybersecurity and Proactive cybersecurity. Reactive cybersecurity deals with threats after they occur and respond to them, while proactive cybersecurity aims to identify and stop threats before they occur and cause harm (Fortinet, 2019).

Proactive cybersecurity is becoming the preferred choice for organizations, those actively trying to improve their security. By using advanced threat detection, continuous monitoring, and predictive analytics, proactive cybersecurity helps prevent breaches before they occur. This approach not only lowers the risk of cyber incidents but also reduces operational disruptions, financial losses, and damage to reputation. Organizations that focus on proactive security are better equipped to handle new cyber threats and stay compliant with regulations (Fortinet, 2019).

The choice between these approaches has a significant impact on an organization's security posture, incident response efficiency, and overall resilience to cyber threats. This chapter discusses both cybersecurity approaches, comparing their features, benefits, and strategic impacts on organizations (Fortinet, 2019).

5.1 Reactive Cybersecurity

Definition and Characteristics of Reactive Cybersecurity

Reactive cybersecurity focuses on responding to security incidents after they have occurred. This approach aims to limit the damage, investigate what went wrong, and take steps to prevent similar issues in the future. Key elements of reactive cybersecurity include:

Incident Response: Quickly activating protocols to manage and contain cyber incidents.
Forensic Analysis: Investigating compromised systems to understand the attack's origin, scope, and method.
Patch Management: Applying updates and patches to fix vulnerabilities that were exploited.

Threat Intelligence Updates: Updating security systems with new threat signatures and attack patterns.
System Restoration: Recovering affected systems and getting them back to normal operations.

While reactive cybersecurity is essential for dealing with ongoing threats, its effectiveness is limited, due to its inability to prevent threats before they occur (Cole, E., 2013).

Key Differences and Benefits of Reactive Approaches

Although reactive cybersecurity is sometimes viewed as a passive strategy, it has several important advantages:

Damage Control: An effective incident response plan can minimize the damage caused by security breaches.
Regulatory Compliance: Organizations can document and analyze incidents to comply with legal and industry-specific security standards.
Continuous Improvement: Learning from previous security breaches helps organizations enhance their defenses.
Incident Investigation: It allows cybersecurity teams to examine and counteract the methods used by attackers.

However, relying solely on a reactive security approach can leave organizations exposed, as it doesn't address threats before they occur, reactive security is still crucial to defend organizations and improve their overall cyber resilience (Cole, E., 2013).

Challenges in Reactive Cybersecurity

While reactive cybersecurity measures are essential for responding to incidents, they come with several inherent challenges. These challenges can significantly impact an organization's ability to effectively manage and mitigate cyber threats. Understanding these limitations is crucial for developing a comprehensive cybersecurity strategy. Reactive cybersecurity faces several significant challenges:

Delayed Response: Actions are taken only after an incident occurs, which means the damage might already be extensive.
High Financial Costs: Managing incidents, recovering from them, and handling legal issues can be very expensive.
Reputational Damage: Cyberattacks and data breaches can severely damage an organization's reputation.
Resource Intensive: Responding to incidents requires specialized personnel and tools, which can strain resources.
Ineffective Against Advanced Threats: Sophisticated cyberattacks might go undetected until they have caused substantial harm (CSOonline, 2023).

5.2 Proactive Cybersecurity

Definition and Characteristics of Proactive Cybersecurity

Proactive cybersecurity is anticipating, identifying, and neutralizing threats before they can cause harm. Organizations that adopt this approach prioritize preventing attacks rather than merely responding to them.
Key aspects of proactive cybersecurity include:

Threat Hunting: Threat hunting is a proactive method in cybersecurity where experts actively search through networks, systems, and data to find malicious activities or security threats that might slip past automated defenses. Unlike traditional security measures that depend on alerts, threat hunting involves investigating potential threats before they occur by actively seeking out vulnerabilities and potential indicators of attacks within the organization's network (MITRE ATT&CK, n.d.).

Vulnerability Management: Vulnerability management is an essential part of a proactive cybersecurity strategy. Vulnerability management is the process of continually identifying, assessing, prioritizing, and remediating vulnerabilities in an organization's systems, software, and networks. The goal is to reduce cyber risks by preventing these vulnerabilities from being exploited by attackers. Continuous evaluation is very important for prioritizing. Vulnerability management is an important

part of a proactive cybersecurity strategy and can pose serious risks to attacks if not done regularly (CISA, 2016).

Security Awareness Training: Security Awareness Training is a training program designed to raise awareness among employees and organizational members about cybersecurity threats, risks, and best practices. The aim is to reduce security vulnerabilities caused by human errors and to ensure that employees are more vigilant and prepared for cyberattacks. Security awareness training is an important element in strengthening an organization's proactive cyber defenses because most cyber-attacks use the human factor (Proofpoint, 2024).

Key Differences and Benefits of Proactive Cybersecurity Approaches

The basic advantages and differences of proactive cybersecurity are:

Threat Prevention: Vulnerabilities of the environment monitored and fixed continuously to prevent possible exploits.
Cost Efficiency: Legal issues, fines or reputational damages may cost too much to organizations. It is possible to lower them by preventing exploits before they occur.
Operational Continuity: Operational continuity is considered proactively while taking actions on possible issues.
Resource Optimization: By taking proactive measures, IT teams significantly reduce the number of attacks and incidents and use resources efficiently.
Reputation Protection: It is the totality of activities carried out to protect the online and offline reputation of the organization and prevent it from being negatively affected.

By focusing on prevention rather than response, organizations that implement a proactive cybersecurity strategy improve the overall security resilience.

5.3 Comparative Analysis of Proactive vs. Reactive Cybersecurity

Proactive strategies are vital to defend against emerging cyber threats. Reactive monitoring of threats, on the other hand, plays a crucial role in responding to attacks and minimizing damage (Fahreen, F., 2024). In this context, these strategies must be planned correctly to increase overall

security posture. The table below provides a comparison of proactive and reactive cybersecurity approaches and the key differences between them.

FEATURE	REACTIVE CYBERSECURITY	PROACTIVE CYBERSECURITY
APPROACH	Responds after an attack	Prevents attacks before they occur
FOCUS	Incident containment and recovery	Threat detection, prevention, and mitigation
TECHNOLOGY USED	Firewalls, antivirus, and forensic tools	AI-driven analytics, threat intelligence, and penetration testing
RISK MITIGATION	Addresses risks after impact	Minimizes risk before impact
COST EFFICIENCY	Can be expensive due to damage control	More cost-effective by reducing breach risks
REGULATORY COMPLIANCE	Requires post-breach compliance reporting	Helps meet compliance proactively

Table 2 Differences between proactive and reactive cybersecurity

Reactive and proactive cybersecurity are two approaches to safeguard digital assets. Reactive cybersecurity responds to threats only after the attack has occurred, and its emphasis is on containing incidents and recovery. It usually relies on traditional tools such as firewalls, antivirus, and forensic analysis. While it is important to contain breaches, it may involve greater costs as damage control and post-incident responses are involved. Also, it typically demands that organizations achieve regulatory compliance after the breach has occurred. Proactive cybersecurity, however, attempts to prevent attacks beforehand. It revolves around early detection of threats, prevention, and reduction of threats using more advanced technologies like security posture management, threat intelligence, and employee training. By identifying vulnerabilities early and repairing them before they are used to launch attacks, proactive activities lower risks and are generally cost-effective in the long run. Further, they help organizations always be regulatory compliant, not after a security breach.

6 Case Studies and Real-World Implementations

6.1 Microsoft Defender XDR

6.1.1 Introduction

Microsoft Defender XDR (Extended Detection and Response) is a powerful security platform that brings together protection across many areas, like devices, user identities, emails, apps, and cloud services all in one place. It uses advanced analytics, behavior algorithms and artificial intelligence to help detect, investigate, and respond to cyber threats more effectively.

By gathering security data from different sources, Defender XDR gives security teams a clearer, unified picture of what's happening, so they can react quickly when suspicious activities occur. Its proactive features make it a vital part of today's cybersecurity strategies.

Unlike older security tools that work separately, Defender XDR connects multiple security solutions into a single platform. This means it provides centralized monitoring and automation, making it easier and faster to manage threats.

By combining signals from various sources and using smart threat intelligence and machine learning, Defender XDR can spot complex attacks that might otherwise go unnoticed—and help stop them before they cause damage (Microsoft Learn, n.d.).

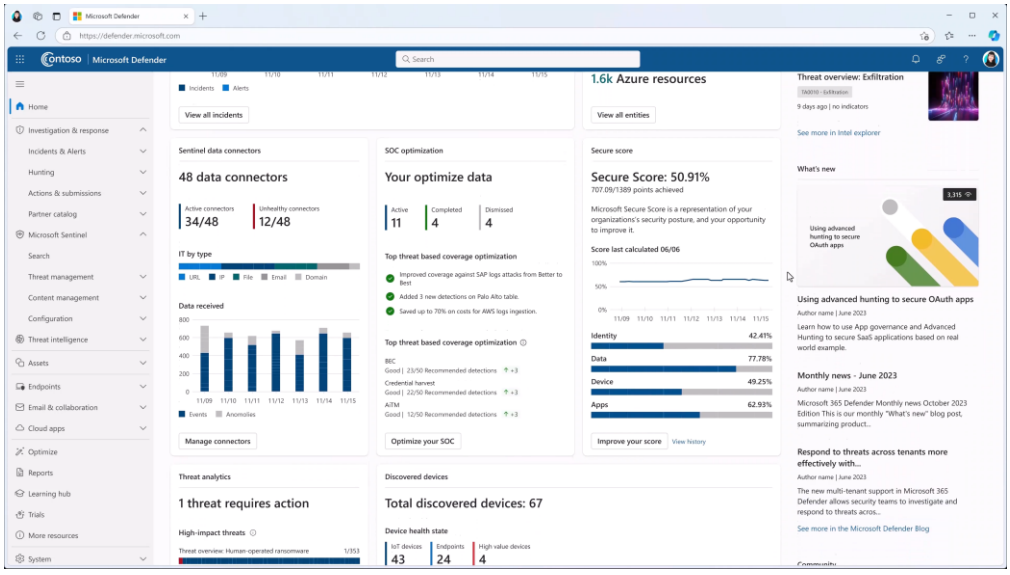


Figure 2 Defender XDR Unified Portal (Microsoft Learn, n.d.).

6.1.2 How Microsoft Defender XDR Works

Microsoft Defender XDR employs artificial intelligence, machine learning, and behavioral analysis to identify anomalies and suspicious activities. Microsoft Defender XDR uses artificial intelligence, machine learning, and behavioral analysis to spot unusual and suspicious activities across various areas like endpoints, user identities, emails, and cloud apps. It collects and correlates data from these different sources to get a full picture of security posture. By analyzing this data with advanced threat intelligence, it can detect potential threats before they occur. When incidents occur, Defender XDR links related events together to show the entire attack story, helping security teams understand and respond better. It also includes automated actions to quickly contain and fix issues, reducing the damage caused by cyberattacks. Furthermore, the system keeps improving over time to catch new and evolving threats by continuous monitoring and adaptive learning, before they become a problem (Microsoft learn, n.d.).

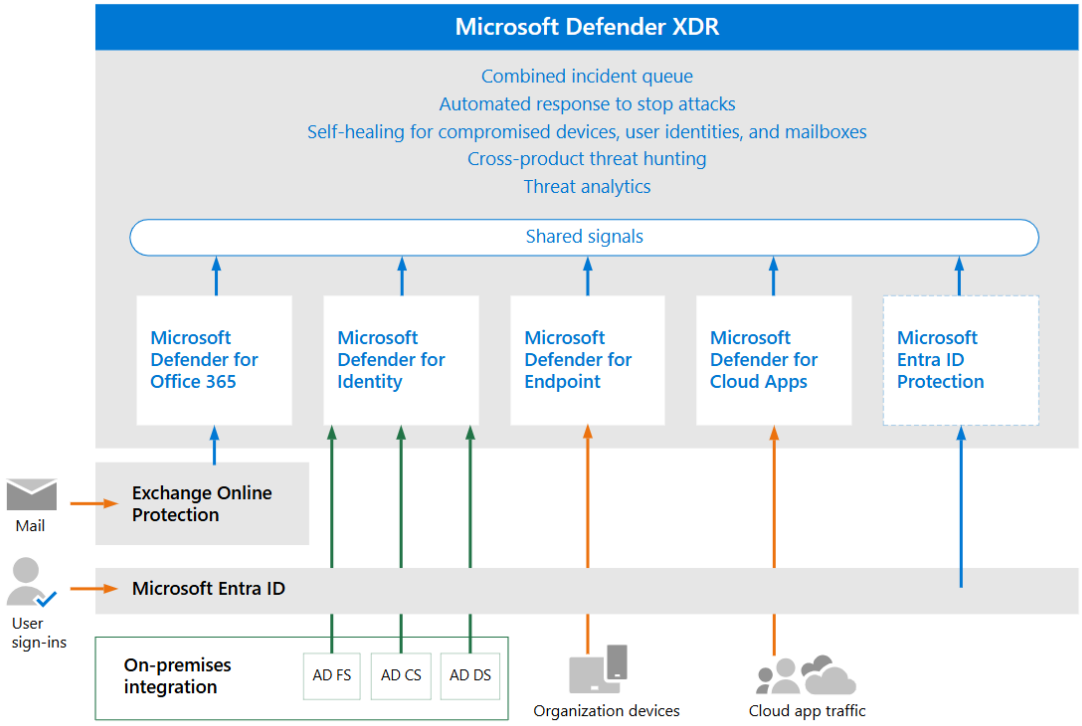


Figure 3 Microsoft Defender XDR Components (Microsfot Learn, n.d.).

Figure 3 shows how Microsoft Defender XDR brings signals together from different Defender components to offer extended detection and response across multiple areas. This means it provides a

single, unified incident queue, automated responses to attacks, and even self-healing for compromised devices, user accounts, and mailboxes. It also supports cross-threat hunting and detailed threat analytics to stay ahead of attackers.

For example, Microsoft Defender for Office 365 protects organizations from harmful threats in emails, malicious links, and collaboration tools. It sends important signals with Defender XDR and works closely with Exchange Online Protection (EOP) to keep emails and attachments safe.

Microsoft Defender for Identity focuses on securing the organization's hybrid identities by collecting signals from Active Directory domain controllers and servers. It helps prevent hackers from moving laterally inside the network using compromised accounts. In addition, Microsoft Defender for Endpoint monitors and protects all the devices managed by the organization.

Finally, Microsoft Defender for Cloud Apps monitors how cloud applications are used within the organization, securing data flow between the IT environment and both approved and unapproved cloud apps (Microsoft Learn, n.d.).

6.1.3 Microsoft Defender XDR Products

Microsoft Defender XDR consists of several products, each specializing in protecting specific components of an organization's digital ecosystem. These products include:

Microsoft Defender for Endpoint

Microsoft Defender for Endpoint is an EDR solution of Microsoft designed to protect an organization's devices like laptops, desktops, mobile phones from advanced cyber threats. It uses built-in sensors in the operating system to monitor how devices behave and sends this data to Microsoft's cloud, where big data and machine learning analyze it to detect potential threats. Microsoft's threat intelligence helps security professionals to identify attacker's techniques and improve detection.

Key features include real-time vulnerability management to quickly find and fix weaknesses, reducing the attack surface by limiting exploitable entry points, and next-generation protection that

uses behavior analysis to block new threats. It also offers tools for near-real-time attack detection and response, along with AI-powered automated investigations to resolve complex threats with less manual effort. These elements make Microsoft Defender for Endpoint a comprehensive solution for safeguarding an organization's digital assets against a wide range of cyber risk (Microsoft Learn, n.d.).

Microsoft Defender for Office 365

Microsoft Defender for Office 365 is a security tool designed to protect organizations from sophisticated threats targeting email and collaboration platforms like Exchange Online, SharePoint, OneDrive, and Microsoft Teams.

It offers several key features to keep users safe: Safe Attachments scans email attachments in a secure virtual environment to catch malware before it reaches recipients; Safe Links checks URLs at the same time they're clicked and blocks any harmful websites; and anti-phishing policies use machine learning to detect and stop phishing attempts aimed at stealing sensitive information.

In addition to email protection, it also protects collaboration tools by identifying and blocking malicious files in teams, SharePoint and document libraries. Moreover, security administrators get real-time reports and insights, helping them quickly spot and address potential security risks with clear recommendations.

Microsoft Defender for Office 365 provides a solid, proactive defense for organizations' communication and collaboration environments by using these features (Microsoft Learn, n.d.).

Microsoft Defender for Identity

Microsoft Defender for Identity is a cloud-based security tool that helps protect organizations' hybrid environments by securing both on-premises Active Directory and cloud identities. It gives a clear view of an organization's identity systems and works to reduce risks by assessing identity security posture and suggesting best practices.

Defender for Identity detects threats throughout the different stages of a cyber-attack, from early reconnaissance attempts and compromised credentials to attackers moving laterally across the

network and even gaining control over the domain. It detects lateral movement activities at early stages.

It integrates seamlessly with Microsoft Defender XDR, allowing security teams to manage identity and other security alerts all in one place for a complete picture of threats. The sensors are installed on domain controllers and related servers to monitor network traffic, filtering and sending important data to the cloud service for analysis.

It is a cloud-based tool, so it provides advanced intelligence to detect suspicious activities and help security professionals to stay ahead of attackers without slowing down their systems (Microsoft Learn, n.d.).

Microsoft Defender for Cloud Apps

Organizations are increasingly relying on Software as a Service (SaaS) application to enhance productivity and collaboration, but these tools also bring security challenges like unauthorized access, data leaks, and compliance risks.

Microsoft Defender for Cloud Apps (MDCA) is Microsoft's Cloud Access Security Broker (CASB) solution that helps organizations to solve these issues by giving them clear visibility and control over their cloud environments. It identifies all the cloud apps which employees use, including unauthorized ones, often called Shadow IT, by analyzing network traffic and evaluating apps against numerous risk factors. Furthermore, it also helps to maintain a strong security posture by detecting misconfigurations and offering guidance based on industry standards, all while integrating with Microsoft Secure Score to track overall security posture. It protects sensitive information by applying data classification, blocking risky downloads, and managing external collaborators to prevent leaks. With advanced threat detection powered by behavior analytics and integration with Microsoft Defender XDR, MDCA provides powerful tools for spotting and responding to threats. Additionally, it offers app governance to monitor and control third-party apps that connect to organizational data via OAuth, helping prevent unauthorized access and keep cloud applications secure (Microsoft Learn, n.d.).

6.2 Proactive Strategies Utilizing Microsoft Defender XDR Tools

6.2.1 Exposure management

Microsoft Security Exposure Management is a proactive security solution that provides organizations a comprehensive view of their entire security landscape. Instead of waiting for problems to occur, it helps security teams to understand and manage risks before they become threats. It becomes easier to protect critical systems, uncover potential vulnerabilities, and take action to reduce exposure by adding security context to asset information. This ongoing, integrated approach supports continuous improvement and aligns well with modern security strategies (Microsoft Learn, n.d.).

Vulnerability Management

Modern cybersecurity frameworks emphasize proactive defense, where identifying and mitigating system vulnerabilities precedes potential exploitation. Microsoft Defender XDR incorporates an integrated vulnerability management solution, designed to provide continuous visibility, prioritization, and remediation of weaknesses across endpoints. This capability is central to reducing an organization's attack surface by aligning asset management, threat intelligence, and risk-based remediation into a unified security model. Figure 4 shows vulnerability dashboard. It provides various information like exposure score, top recommendations, and exposure distributions. This information is crucial for security admins to monitor the overall status of the organization.

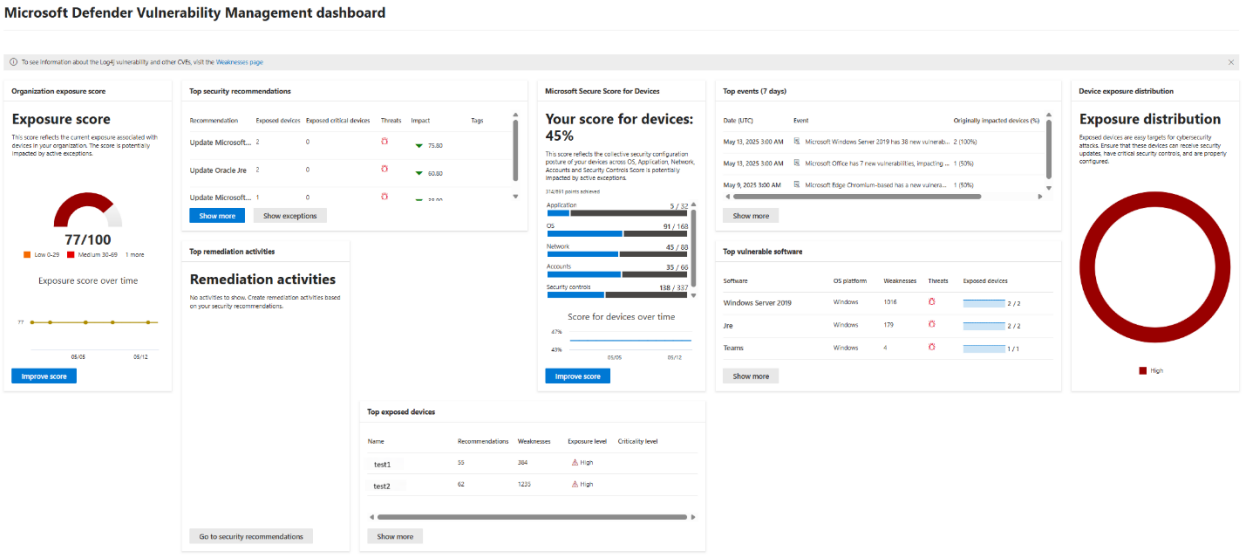


Figure 4 Vulnerability management dashboard (XDR Portal)

Figure 5 shows the recommendations in the Vulnerability portal based on Microsoft's agentless scanning. The remediation type can be configuration change or software patch, or update. Vulnerabilities are prioritized by the impact score and exposure status. The red bug shows that there is an exploit regarding the specific vulnerability and should be remediated as soon as possible.

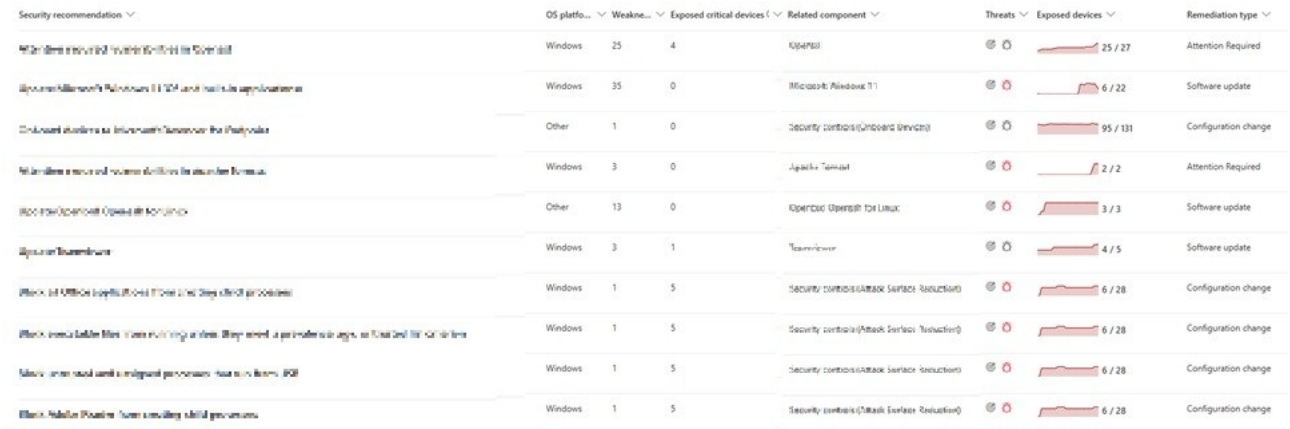


Figure 5 Vulnerability recommendations (Anonymized)

Security professionals prioritize actions based on exploit status, the impact of vulnerability and organizations policy and decisions. It is important to take the exposure score to the low-level as possible by following these steps.

Use of Inventories page

The inventory page shows the software inventory of the organizations. It is utilized to manage the inventories of organization. Figure 6 shows the inventory page and their impact on the overall vulnerability to the organization. Patches are done by prioritizing them based on, for example, their effect. In this case the first three vulnerable components (Software1, software 2, software 3) should be updated or patched primarily, based on organizations' policies in the next cycle.

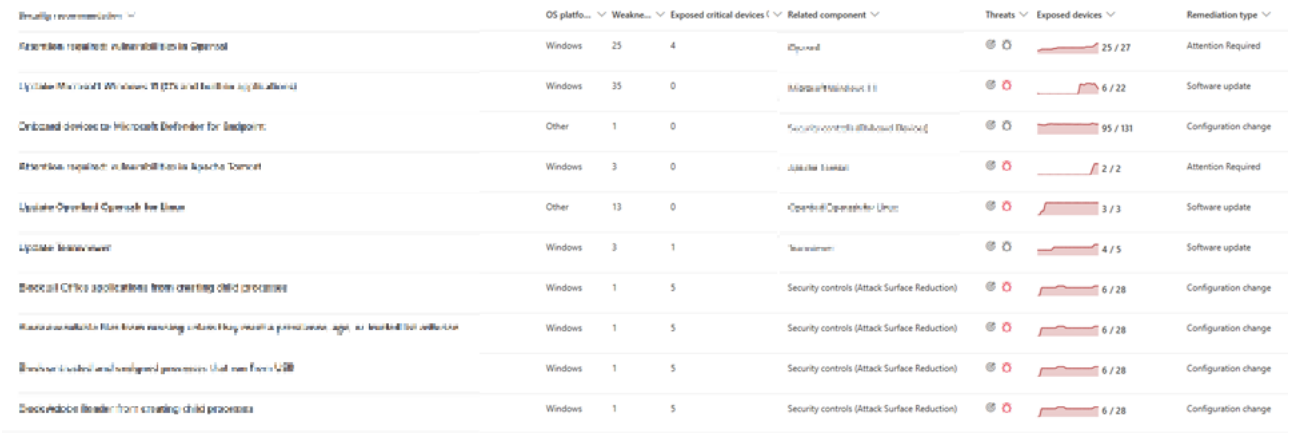


Figure 6 Inventories page for vulnerability management (Anonymized)

6.2.2 Attack Surface and Attack Paths Analyzes

Microsoft Security Exposure Management's attack paths enable organizations and security professionals to proactively identify and visualize potential routes that attackers might exploit through vulnerabilities, gaps, and misconfigurations. By simulating attack paths, potential threats can be investigated and addressed before they become issues.

The Attack path dashboard provides a high-level overview of all identified attack paths within the environment. It enables security teams to gain valuable insights into the types of paths identified, top entry points, target assets, and more, helping to prioritize risk mitigation effectively (Microsoft Learn, n.d.).

Figure 7 shows the Attack Path dashboard. The overview includes:

- Graph of attack paths over time: Shows the change of attack paths on a timeline
- Top choke points: The vulnerable points where attackers can penetrate systems and affect a large scale
- Top attack path scenarios: The scenarios that show how attackers bypass the controls by utilizing the vulnerabilities and gain control of critical assets based on an organization's critical assessment.
- Top targets: Critical assets of the organizations
- Top entry points: The most affective entry points

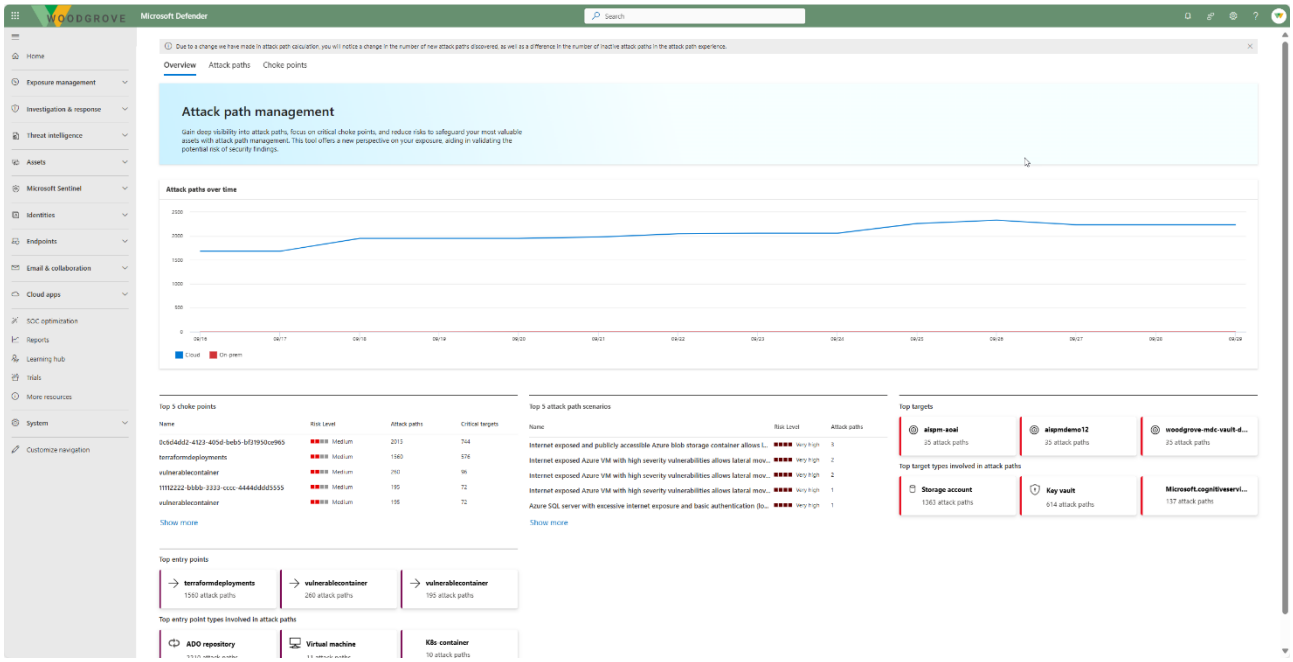


Figure 7 Attack path dashboard

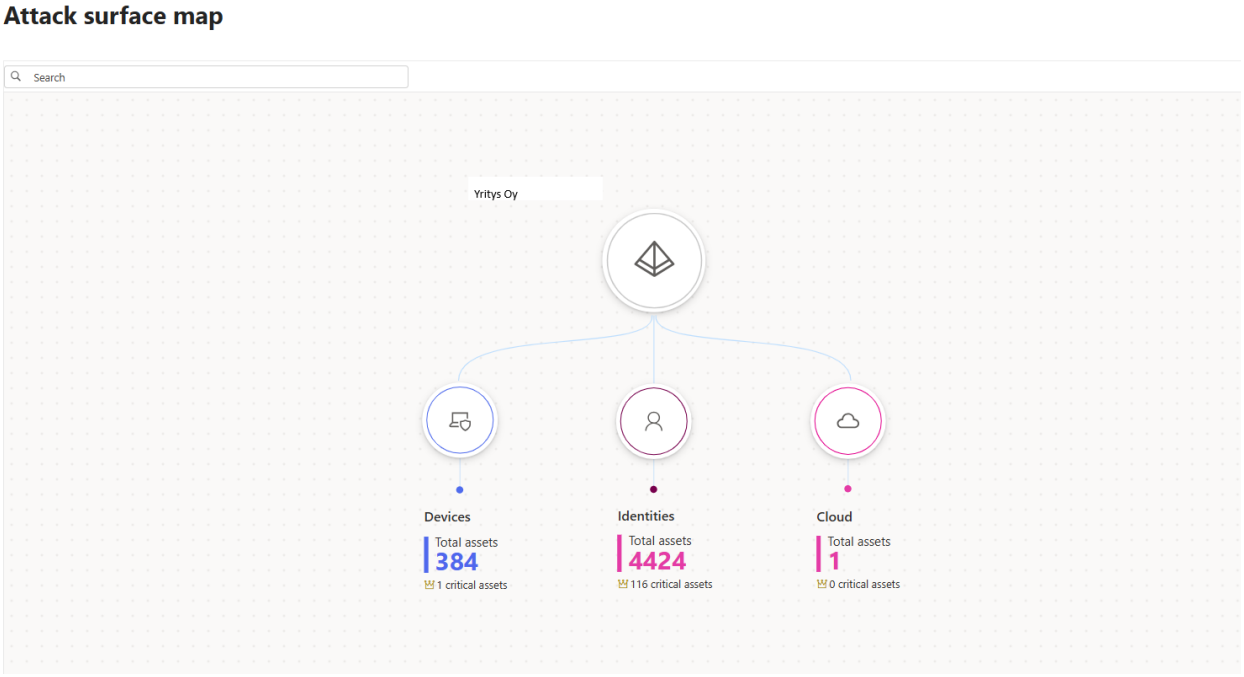


Figure 8 Attack Surface Map

Figure 8 above shows the Attack Surface Map. The purpose of the attack surface map is to present the organization's assets in a visual map for security administrators. This allows security admins to view devices, identities, and cloud assets through a graphical interface and assess how many critical assets they have.

Critical Asset Management

Microsoft Defender XDR incorporates critical asset management to identify and safeguard the most important assets in an organization. By designating certain devices, user accounts, or cloud resources as critical, Defender XDR ensures these assets receive elevated protection and attention. This capability is part of Microsoft's Security Exposure Management, which unifies context from endpoints, identities, and cloud workloads into an enterprise exposure graph. The graph-driven approach enables Defender XDR to not only classify critical assets but also map how an attacker might move through the network toward those assets. Importantly, the attack path analysis is continuous and dynamic. If the environment changes – for instance, a new server is added, a patch is applied, or an employee's permissions change – the exposure graph and attack paths update to reflect the new reality (Microsoft, Learn, n.d.). This ensures that the identified paths are always relevant to the current state of the enterprise. In cases where not all data is available (e.g.,

certain workloads not integrated or critical assets not fully defined), some paths might not be found (Sami Lamppu, 2024).

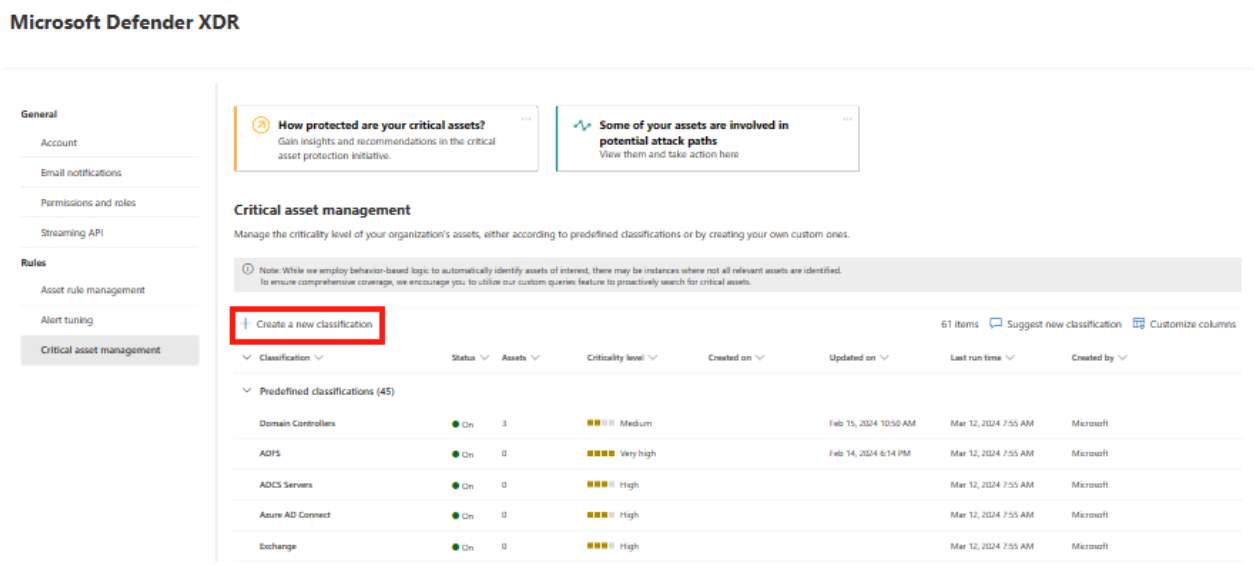


Figure 9 Critical asset management

Critical assets can be for example:

- Domain controllers, Tier-0 Servers
- Databases which contain sensitive data
- Groups, Service accounts
- Privileged Roles like Global Administrator role

Real World Implementations of Attack Paths

After the critical assets are identified and the environment is configured correctly, the Attack Paths tab under Exposure management simulates information such as the entry points of the system, which vulnerabilities can be used to gain access, and which critical asset can be accessed by privilege escalation, based on Defender XDR's analysis. Security admins receive possible attack paths graphically and proactively protect the system by performing the necessary remediations before the attack occurs. Figure 10 shows the process of how Attack Path works. Critical assets are

configured to get paths to them in real time, choke/entry points analyzed for necessary remediations.

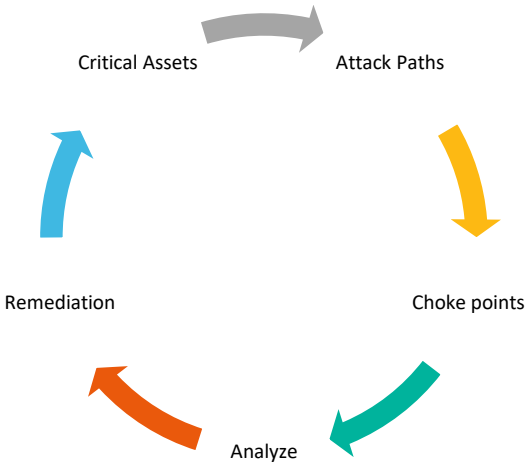


Figure 10 Attack path analysis cycle

Figure 11 below shows an attack path. Here, the attacker who takes advantage of the vulnerabilities in the Device-endpoint and captures the Entra-cookies it contains, uses this cookie to capture the session of the user_admin account that has previously logged in with the endpoint and is defined as a critical asset. Then, this admin can access the vault using the user's account information and permissions, and access the secrets or certificates held there. The user's use of strong authentication such as MFA cannot prevent this attack because the information is embedded in the session cookies.

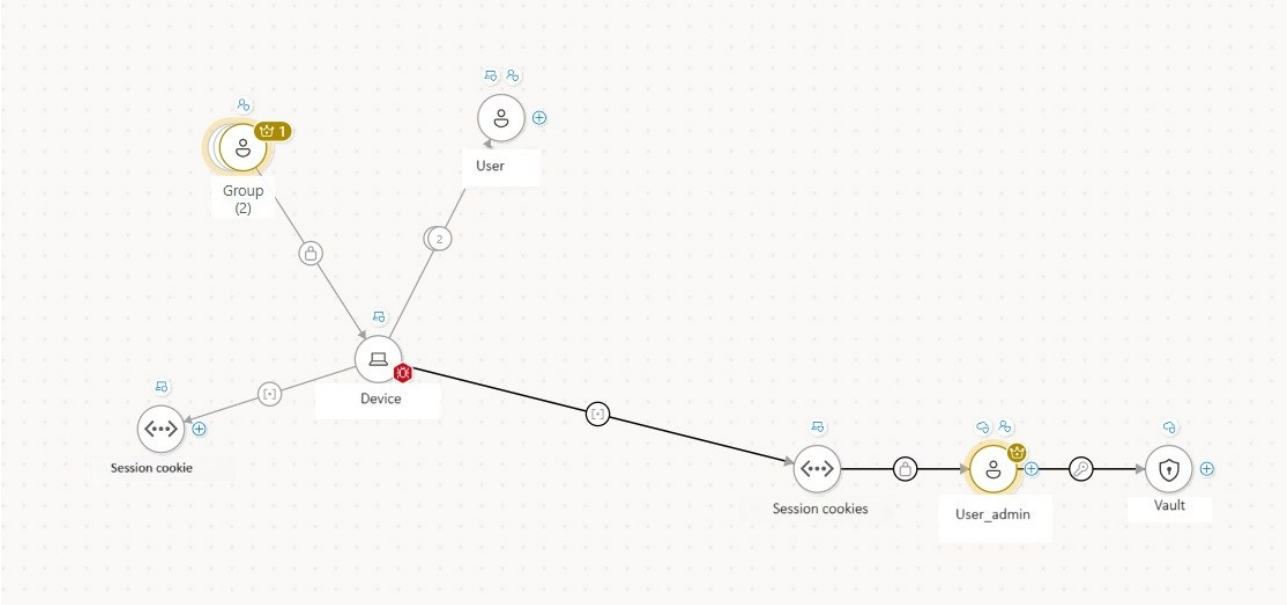


Figure 11 Attack path graph (Anonymized)

After attack path analyses are performed, remediation operations are performed in order of prioritization and the vulnerabilities found on the device are fixed. In this way, the exploitation of vulnerabilities is prevented proactively and access to critical assets of the system is prevented.

Device has critical vulnerabilities and if attackers gain access to this endpoint, the session tokens which contain user_admin credentials. Since users use extra security layers like Multi Factor Authentication (MFA), attackers can bypass it by using session cookies since MFA information is embedded in it.

6.2.3 Security Posture Management and Secure score

Security posture refers to the overall strength and readiness of an organization's cybersecurity efforts, including its ability to detect, respond to, and recover from threats. It reflects the organization's ability to identify, prevent, detect, and respond to security incidents. A robust security posture is indicative of an organization's resilience against cyberattacks and its commitment to maintaining the confidentiality, integrity, and availability of its information systems (Gsctechnologies, 2024).

Because of the complexity and frequency of cyber threats, it is essential for organizations to take a proactive stance in protecting their digital environments. Microsoft Defender Secure Score serves also as a critical resource in this effort, offering a measurable overview of an organization's current security status. It also delivers practical guidance to address weaknesses and enhance overall protection. This paper examines the concept of security posture, highlights the importance of tailored security recommendations, and discusses how organizations can effectively leverage Secure Score to strengthen their cybersecurity framework (SMS, 2024).

Prioritization matters when remediation/mitigations are performed. Secure score also gives security admins to prioritize the assets, vulnerabilities and mitigation/remediations based on recommendations.

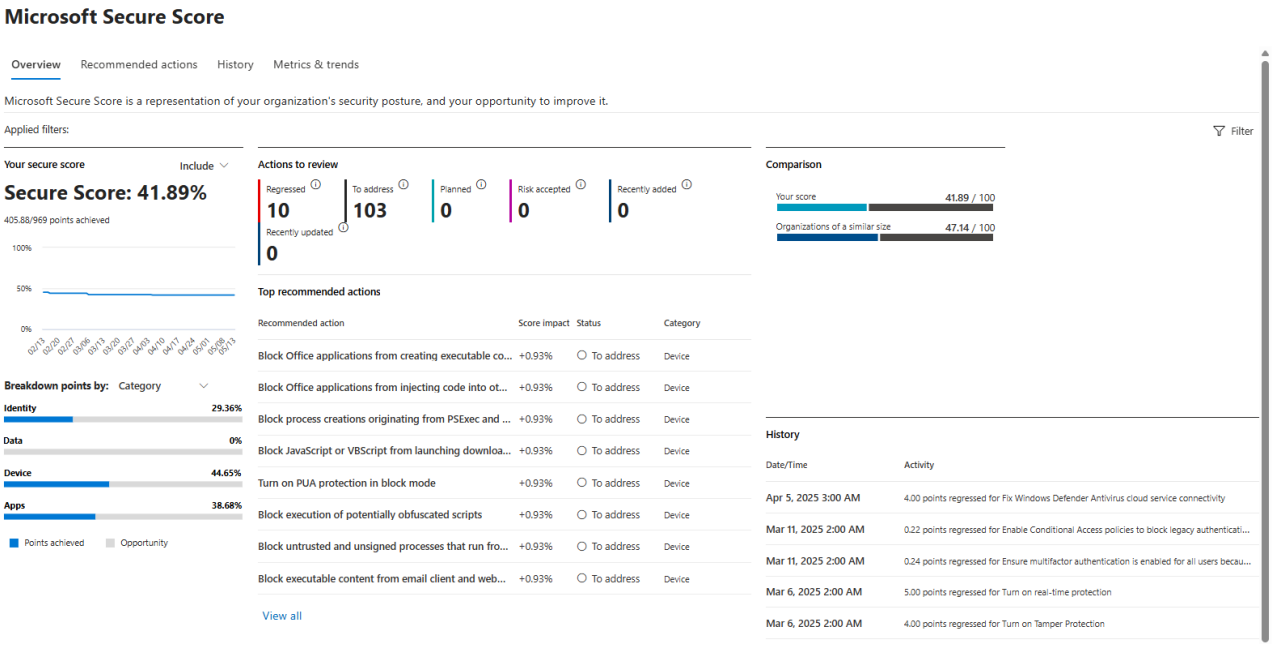


Figure 12 Secure Score Dashboard

Figure 12 shows the secure score dashboard. There are several components in Secure score dashboard which helps security professionals to identify, prioritize the security posture and give insights to improve it. The main components are:

1. Overall Score

This is the main number seen at the top of the dashboard. It reflects how many of the suggested security measures of the organization have been implemented. The score is updated regularly and is based on Microsoft's own list of prioritized security recommendations. The goal is to take it as high as possible.

2. Recommended Actions

Recommended actions all the specific tasks can be done to improve security. Each recommendation includes a short description, the impact it will have on the score, and step-by-step instructions. Actions may include enabling multi-factor authentication, limiting admin access, policy configurations or applying device compliance policies.

3. Score Comparison

This feature lets admins see how the organization's score compares to similar companies in the industry or region. This helps them understand whether the security level is below or above average.

4. Improvement Opportunities

This area highlights actions that haven't been taken but could be adopted to strengthen the overall protection. It also shows whether each action is considered high, medium, or low impact which is crucial for prioritization.

5. History and Trends

It can be tracked how the score has changed over time. This is helpful for evaluating the progress of the security efforts and showing improvements after changes or updates.

6. Filter and Scope Options

The scope and filter options can be used to narrow down the recommendations by product, status or category. It is used to narrow down the options as needed.

Real World Implementations of Secure Score

This section will cover the configurations and hardenings, as well as Secure Score changes and prioritization. With the recommendations on the Secure Score page, changes are made to the organization context, and possible weaknesses are proactively monitored with continuous security posture development.

Figure 13 shows an example of recommendations for secure score. The impact of each recommendation is shown under secure impact. It also helps security admins to prioritize the actions.

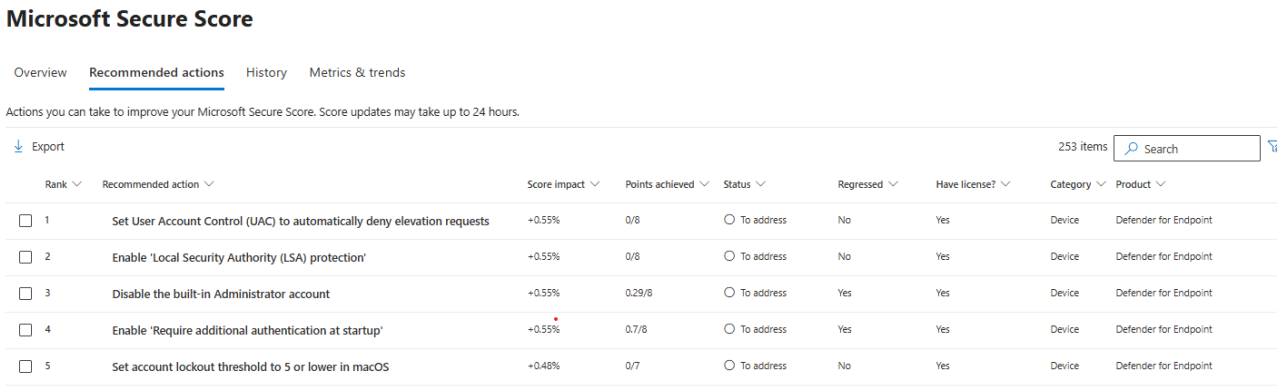


Figure 13 Secure Score recommendations

Case 1

As Figure 14 and 15 show, the secure score of the environment was 36.4. After the configurations and hardenings, it increased to 64.26. According to Microsoft's statistics, the security score of organizations of similar size is 43.44, and the general security posture has been increased above this score. These changes proactively prevent attackers from using weaknesses, misconfigurations, etc. to make unauthorized access to the system.

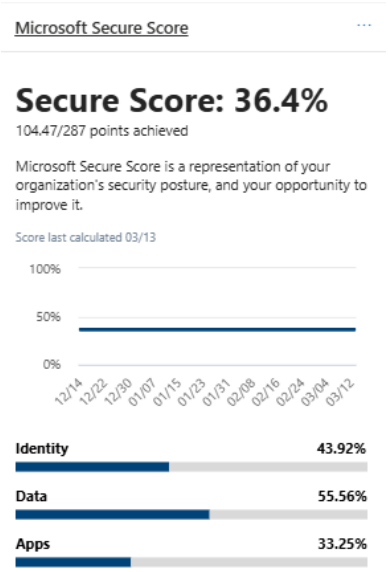


Figure 14 Secure score before Hardenings

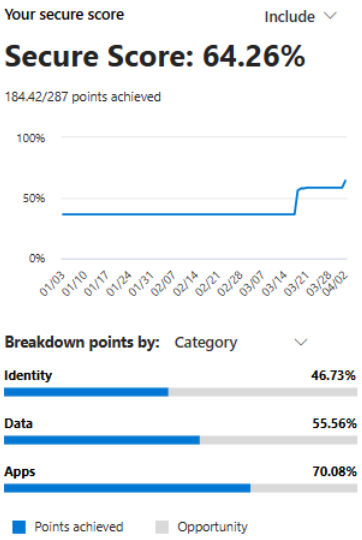


Figure 15 Secure Score After Hardenings

the secure score of the environment was 36.4. After the configurations and hardenings, it increased to 64.26. According to Microsoft's statistics, the security score of organizations of similar size is 43.44, and the general security posture has been increased above this score.

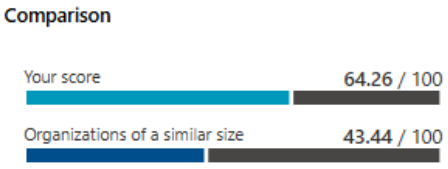


Figure 16 Microsoft Secure score comparison

The changes made based on the recommendations to increase the security score and improve the security posture are:

- Defender for Office 365 policy hardening for e-mail security
- Conditional access policies for hardening identity security
- Password protection features enabled.

These proactive actions require continuous operations and aim to reduce the attack surface.

Case 2

As Figure 17 and 18 show, the secure score of the environment was 63.68, after the configurations and hardenings, it increased to 73.64. As the secure score increases, recommended actions become more complex and detailed. The reason for this is that the changes are selected according to priority order and will have the least impact on the environment and users.

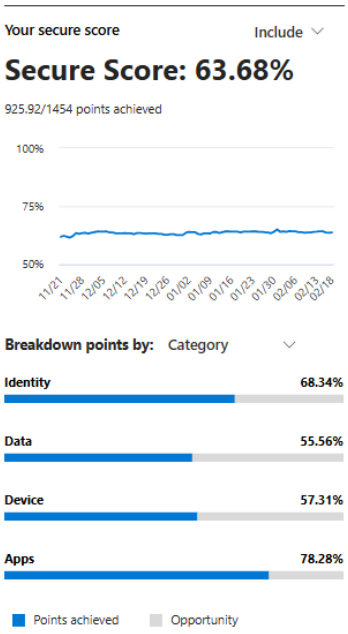


Figure 18 Secure Score Case2 Before

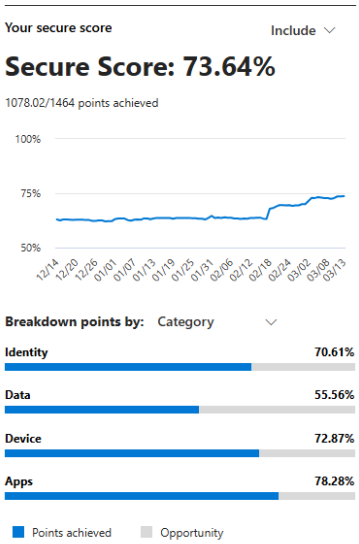


Figure 17 Secure Score Case2 After

The changes made based on the recommendations to increase the security score and improve the security posture are:

- ASR (Attack Surface Reduction) rules enabled
- Defender Antivirus e-mail scanning feature enabled
- Potentially Unwanted Application (PUA) protection features enabled

6.2.4 Security Awareness and training

The Human Factor in Cyber Defense

Phishing remains one of the most effective and commonly used attack vectors by adversaries. It leverages social engineering to exploit trust and trick users into revealing credentials, downloading malware, or accessing malicious links (Hadnagy, 2018). Defender XDR recognizes this risk by offering tools to evaluate and enhance user resilience through repeated exposure to controlled, simulated threats.

Security Awareness in Defender XDR

In modern enterprise environments, technical defenses are only one component of a robust cybersecurity posture. Human error remains a leading cause of successful cyberattacks, particularly through phishing (Verizon, 2023). As a response, organizations are increasingly adopting proactive security awareness programs to reduce user susceptibility. Microsoft Defender XDR supports such initiatives by integrating phishing simulation and training capabilities, particularly through its connection with Microsoft Defender for Office 365. Attack simulation training requires Defender for Office Plan 2 license.

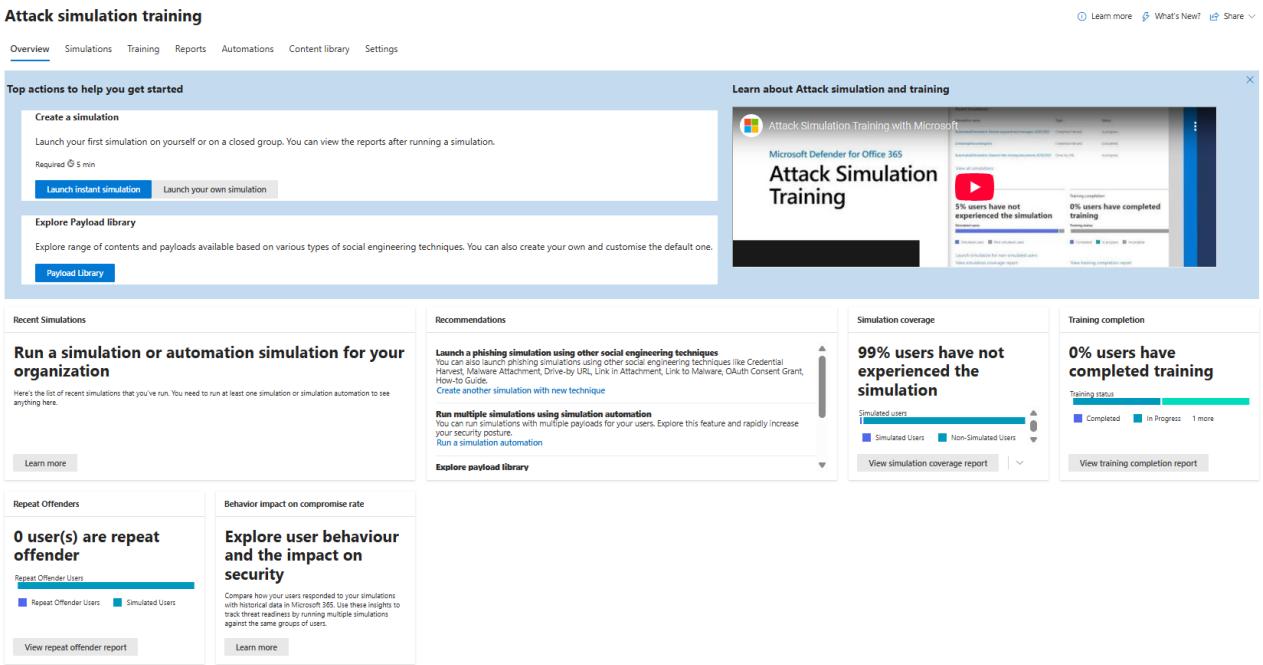


Figure 19 Attack simulation dashboard

Figure 19 shows the Attack simulation dashboard. Microsoft Defender Attack Simulation Training Dashboard is a comprehensive tool designed to evaluate and improve user awareness against phishing attacks. It helps organizations proactively test their employees through realistic simulations and track behavioral responses, training completion, and exposure metrics.

1. Create a Simulation

This feature allows security teams to launch phishing tests quickly. Simulations can be instant—run on individuals or closed groups—or customized with detailed targeting. It's a straightforward process typically requiring about five minutes to initiate.

2. Payload Library

A library of phishing attack templates is available here, covering various real-world techniques such as credential harvesting, malicious links, and deceptive attachments. Custom payloads can also be built to match specific organizational needs.

3. Recent Simulations

Displays a history of previously run simulations. This area stays empty until a simulation or automation is launched, encouraging security teams to begin assessments.

4. Recommendations

The dashboard suggests ways to enhance simulation effectiveness. These include diversifying attack styles, automating simulations, and examining behavior reports to optimize awareness strategies.

5. Simulation Coverage

This part tracks the percentage of users who have experienced simulations. The percentage of users can be tracked here.

6. Training Completion

Displays statistics on how many users have finished assigned training after simulations. It shows the percentage of users who have completed their modules, and the interface breaks down completion status into categories like 'In Progress' and 'Not Started'.

7. Repeat Offenders

Shows users who have failed multiple phishing simulations. This data helps identify individuals needing focused interventions.

8. Behavior Impact

This panel enables analysis of user behavior trends. It helps organizations see how simulation performance influences compromise rates, pinpoint improvement, and evaluate which social engineering tactics remain effective.

Real World Implementations of Attack Simulation Training

Human factors are very important for organizations' overall security posture. Employees should be trained proactively and be aware of the popular threats to changing cyber landscape (Laine, M). Phishing campaigns are very popular, and attackers always aim to gain access to users accounts and move laterally for privilege escalation. Attacks usually start with phishing emails to use human nature. Microsoft Defender XDR offers an embedded tool to create simulations, sending them to the end users.

Creating the Simulation from Defender XDR Admin Portal

We chose Email & collaboration tab in Defender portal and selected Attack simulation training as Figure 20 shows below. Then we choose "Launch a simulation" option as shown in Figure 21.

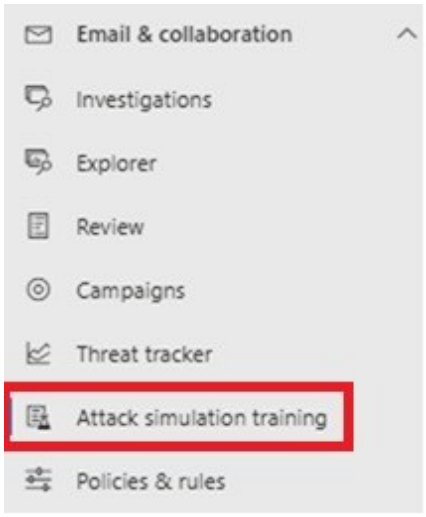


Figure 20 attack surface training in Defender XDR

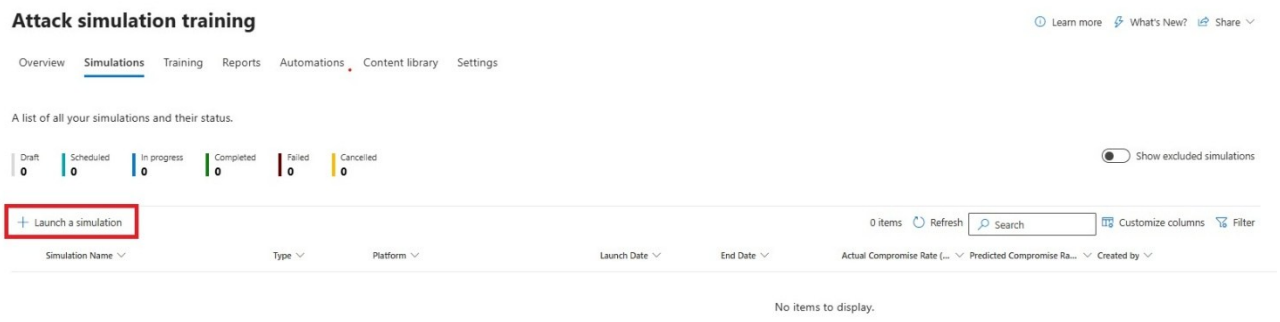


Figure 21 Launch a simulation

Figure 22 shows the attack techniques which are widely used in the real world. It is possible to use various social engineering techniques like credential harvest, malware attachment, link in attachment or more popular techniques like QR-Code phishing.

We use credential harvesting techniques as an example in this case. Figure 19 shows the payloads that can be used in simulations.

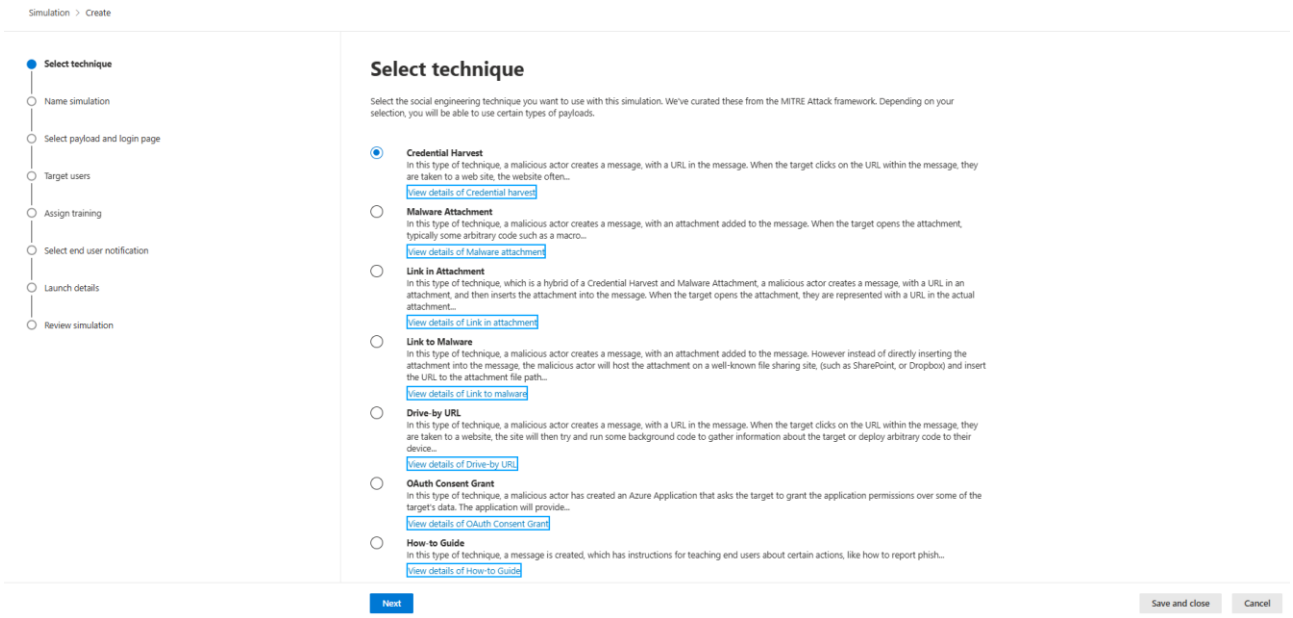


Figure 22 Attack techniques

In this example, Microsoft's Reset Password Payload is used. By clicking on the relevant payload, you can see the email that will be sent to the user, the login page, etc. The username is automatically retrieved from the system and placed in the email. Figures 23 and 24 show the user pages.

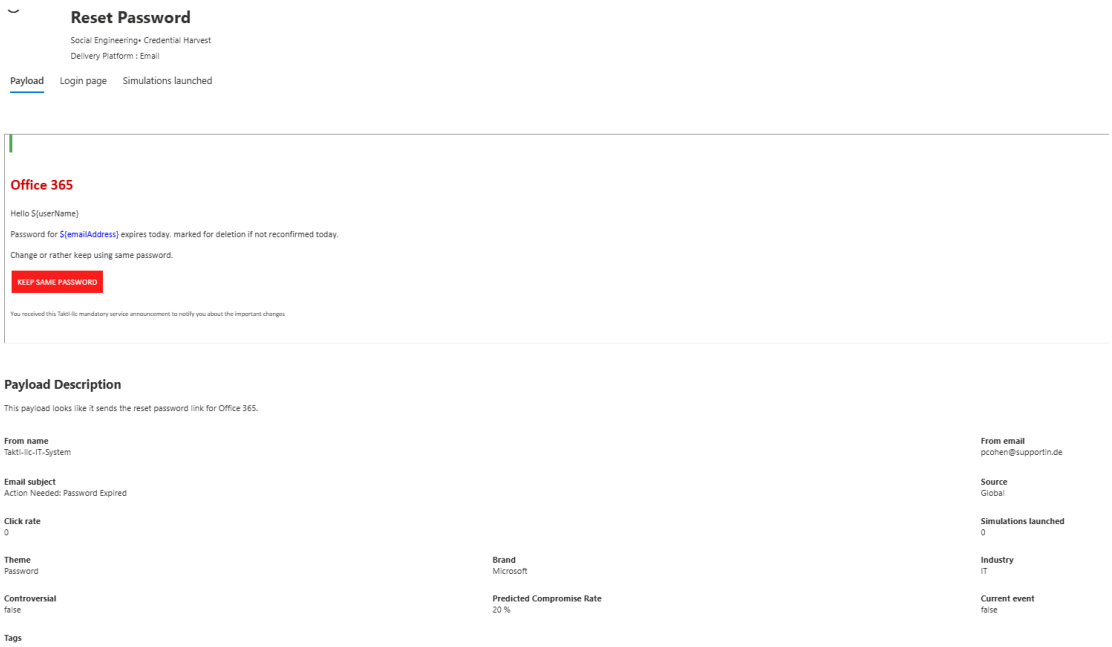


Figure 23 Reset password payload message

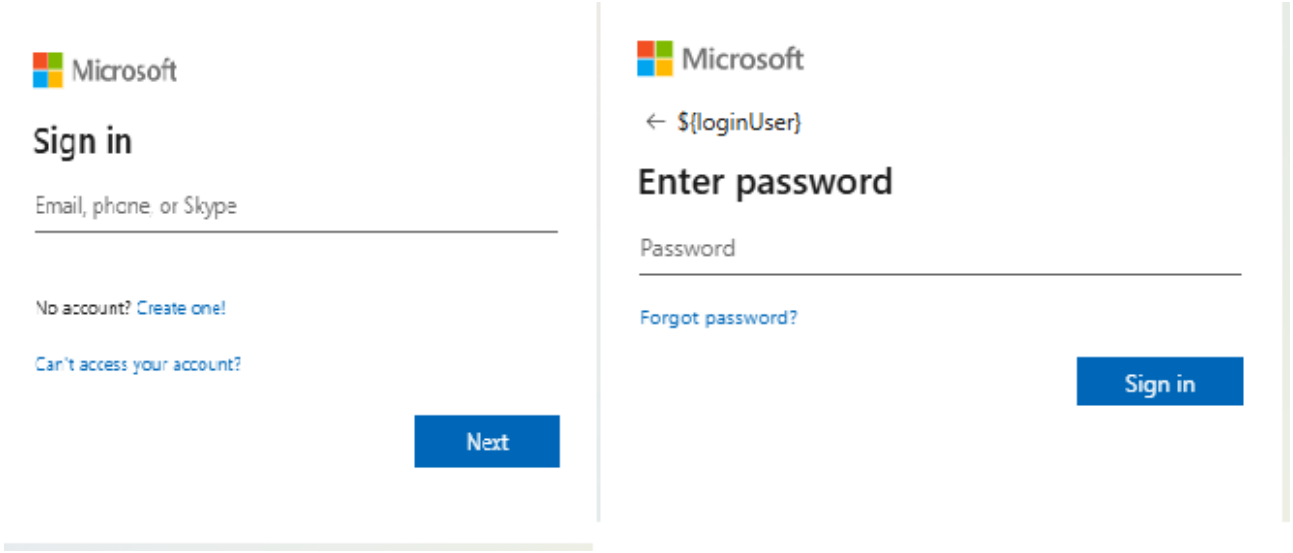


Figure 24 Reset paswoord login page

Training can be assigned to the user based on results automatically or manually. In this case we assign training to the user automatically based on its behavior. Figure 25 shows the training assignment settings.

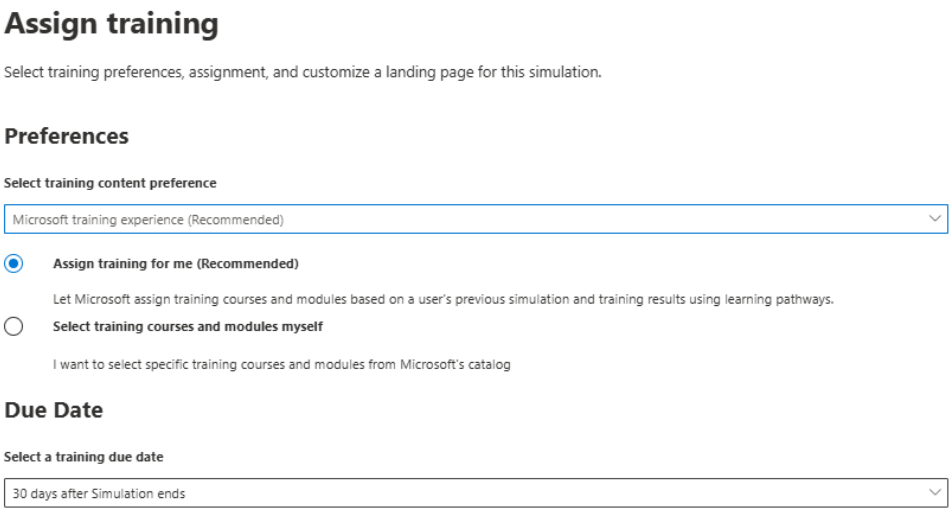


Figure 25 Training assignment page

The last phase is to assign and submit the simulation. It is assigned to one user and now seen in simulation list.

Simulation from User Side

The simulation was assigned and phishing email sent to the test user within minutes. Figure 26 shows how it seems on the user side.

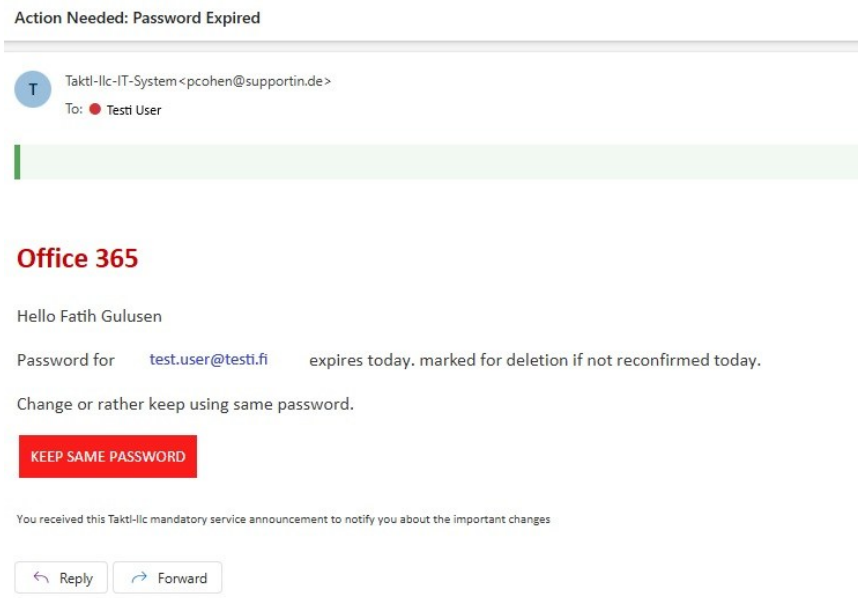


Figure 26 Email view on user side

Figure 27 shows the pages after clicking “Keep Same Password” and username and password are entered.

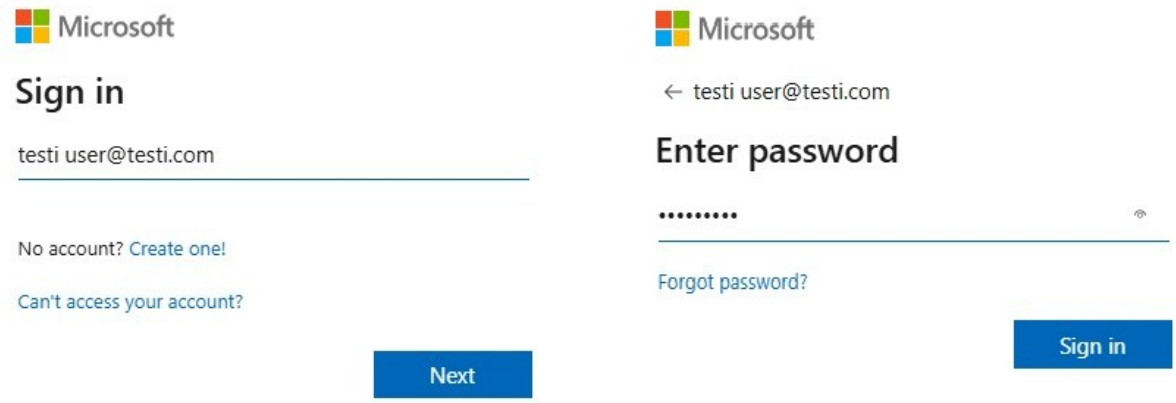


Figure 27 User credentials

When the user enters their username and password, the system sends a feedback page explaining that this was a simulation. The tips are shown in the same message which tell the user how to identify the phishing messages. Users can go to the training page by clicking ***go to training*** button. The user receives a separate mail for the training which is assigned by the system based on its behavior. Figure 28 shows the feedback page.

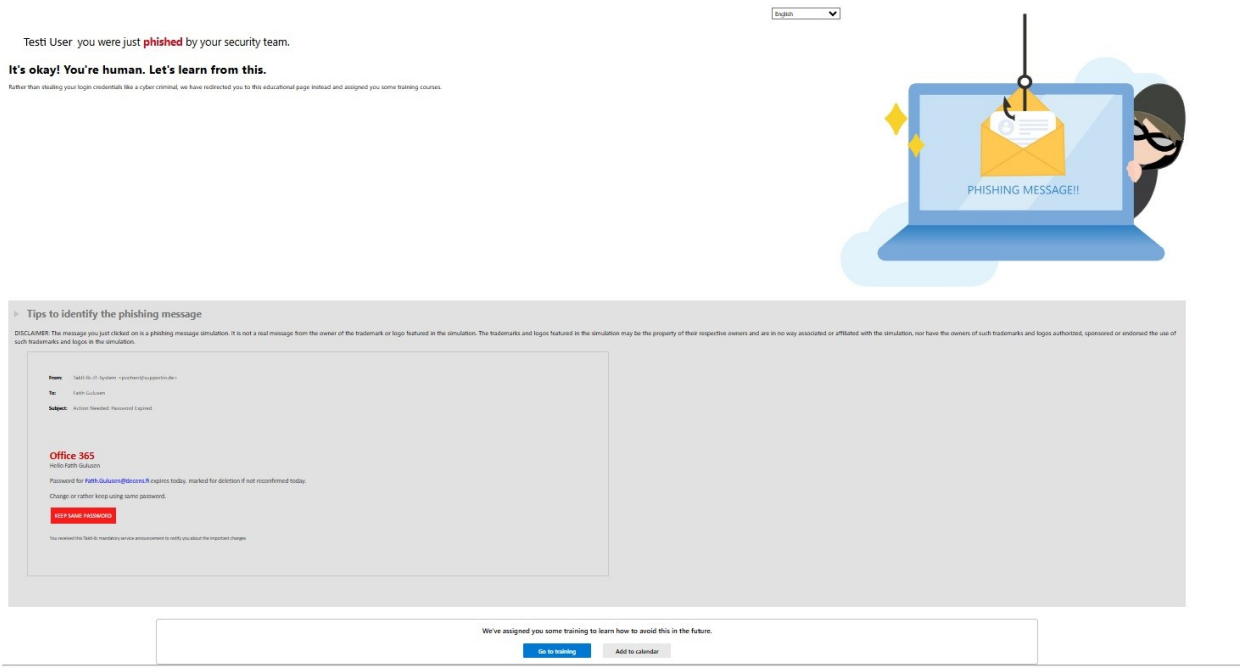


Figure 28 User feedback page

Training in Ransomware and Business Email Compromise are assigned to the user as a part of the internal phishing campaign. It must be done within a month, and the reminder goes to the user every week for this training. Figure 29 and Figure 30 show the e-mail that the user received from the system.

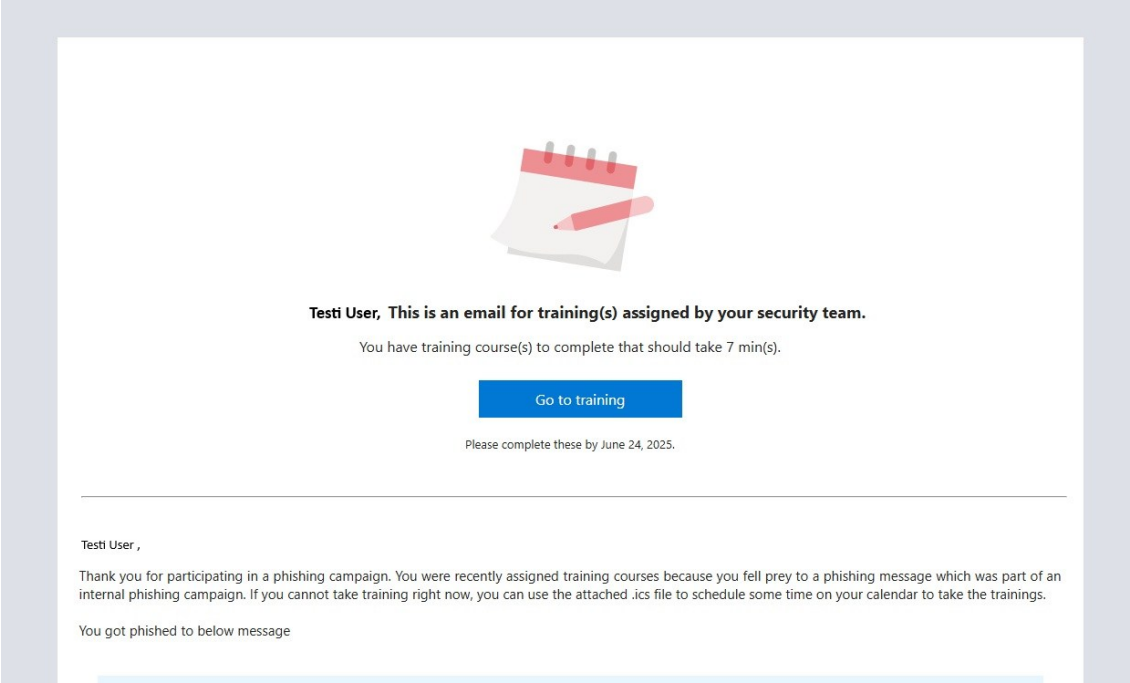
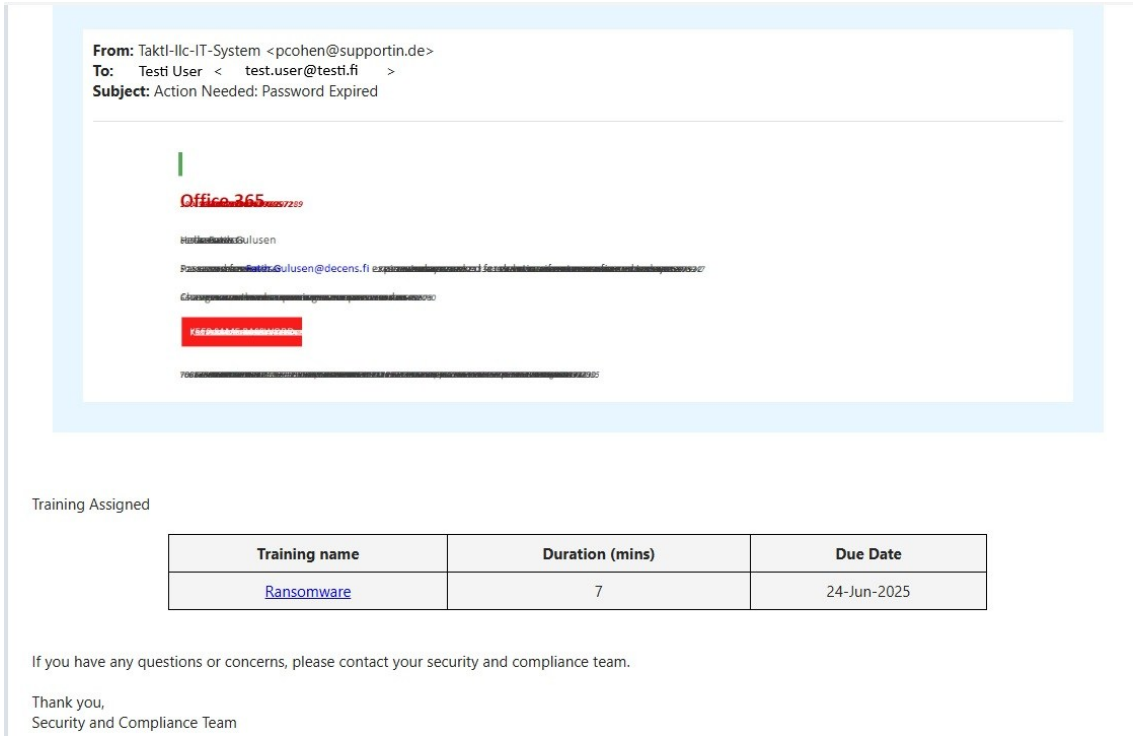


Figure 29 E-mail for course assignment



From: TaktI-llc-IT-System <pcohen@supportin.de>
To: Testi User < test.user@testi.fi >
Subject: Action Needed: Password Expired

Office 365

Training Assigned

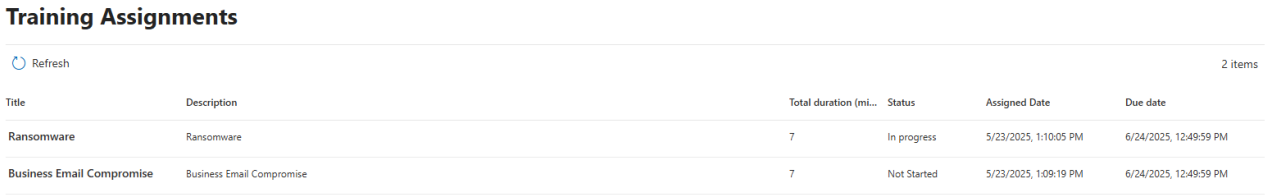
Training name	Duration (mins)	Due Date
Ransomware	7	24-Jun-2025

If you have any questions or concerns, please contact your security and compliance team.

Thank you,
Security and Compliance Team

Figure 30 Email for course assignment-course name

The user goes to the training assignment page by clicking the link and can see and take the assigned courses. The status column shows the current state like “not started”, “in progress” etc. Figure 31 shows the course list and Figure 32 shows the course start page. Employees can start the assigned courses at a specified time.



Training Assignments

Refresh 2 items

Title	Description	Total duration (mi...	Status	Assigned Date	Due date
Ransomware	Ransomware	7	In progress	5/23/2025, 1:10:05 PM	6/24/2025, 12:49:59 PM
Business Email Compromise	Business Email Compromise	7	Not Started	5/23/2025, 1:09:19 PM	6/24/2025, 12:49:59 PM

Figure 31 User assigned courses

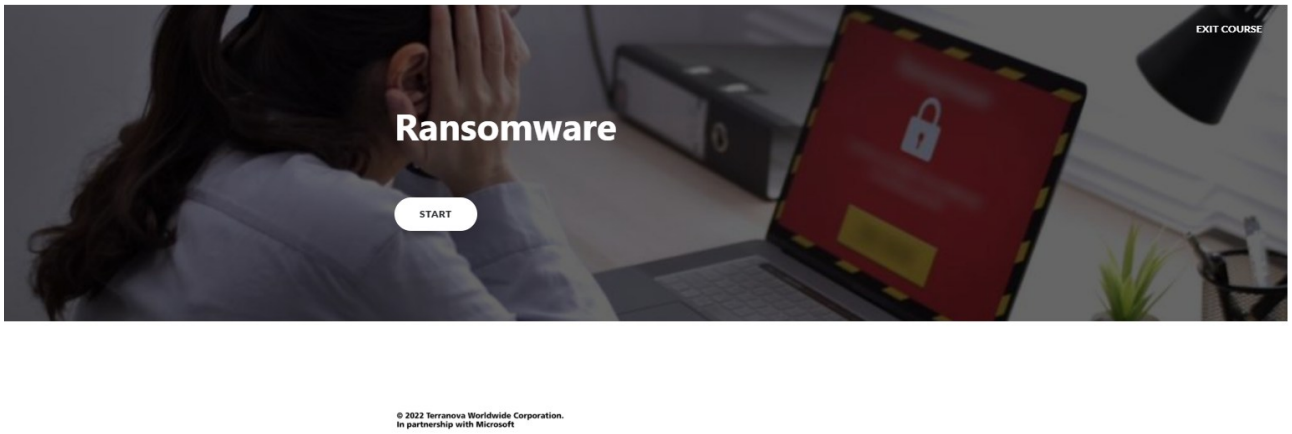


Figure 32 Ransomware course start page

Increasing employees' information security awareness is vital for organizations. Microsoft Defender XDR Attack simulation training allows organizations to achieve this proactively. In addition, well-trained employees help increase the organization's overall cybersecurity posture and prevent threats from entering the environment.

7 Results and Discussion

This thesis explored how proactive utilization of Microsoft Defender XDR tools can significantly enhance an organization's cybersecurity resilience. By focusing on four critical components like Exposure and Vulnerability Management, Attack Path Analysis, Security Posture Management, and Attack Simulation Training, the study demonstrated how organizations can shift from reactive defense models to a forward-looking, preventive security posture.

Exposure and Vulnerability Management within Microsoft Defender empowers security teams to identify and prioritize vulnerabilities based on real-time threat intelligence and business context. Rather than responding to known breaches, organizations can proactively patch high-risk systems and reduce the overall attack surface. The integration of threat context, inventory vulnerabilities, device exposure levels, and active vulnerability insights forms a dynamic approach that aligns with modern risk-based vulnerability management practices.

Attack Path Analysis enhances security resilience by determining the critical assets and simulating lateral movement routes that attackers might exploit. By mapping out these paths before they are leveraged by threat actors, defenders can proactively harden critical nodes and configure essential configurations. This feature transforms traditional incident response and helps security professionals to take actions before bad things occur.

Security Posture Management supports continuous monitoring and improvement of the organization’s security configurations. Through real-time insights, misconfigurations and deviations from best practices are flagged, allowing teams to implement security baselines efficiently. This continuous visibility helps ensure that security hygiene is maintained, especially in hybrid and cloud environments where misconfigurations are a common vector for breaches. The increase of secure score is demonstrated in this research and real word examples showed how organizations security posture enhanced. Microsoft’s secure score for similar organizations intelligence also shows the current status concretely.

Attack Simulation Training adds a vital human-centric layer to defense. By simulating real-world phishing, malware, and social engineering scenarios, organizations can proactively assess user

readiness and tailor training programs. This not only reduces the likelihood of successful attacks but also fosters a culture of security awareness.

Collectively, the proactive use of these Microsoft Defender XDR tools establishes a holistic security strategy that anticipates threats rather than merely responding to them. The findings suggest that organizations embracing this model experience reduced exposure scores, faster incident detection, and improved operational efficiency. More importantly, these tools empower defenders to outpace adversaries—an essential capability in today's evolving threat landscape. Only credential harvesting techniques were used in this research; however, the other techniques can be used in future research.

Future research could focus also on quantitative metrics related to risk reduction over time or explore the integration of AI-driven automation within these proactive workflows to further enhance response speed and accuracy.

8 Conclusion

In this research the overall picture of Proactive use of Defender XDR in Organization's cyber defense described and the benefits of it pointed out.

The main research question of this research was How do organizations benefit from implementing Microsoft Defender XDR in their cybersecurity strategy?

The study discussed how we implement various tools within Microsoft Defender XDR to enhance the cyber resilience of the organization proactively. The research answered this question with concrete use cases and examples of these technologies in the real world.

The second question was How can Microsoft Defender XDR tools be utilized to proactively enhance cybersecurity posture?

Proactive and reactive cybersecurity approaches were discussed and the differences between these approaches were explained. There may be different focuses of proactive cybersecurity for further research like threat hunting, threat intelligence etc.

This study demonstrated concrete examples of using proactive strategies by using various tools and technologies. It is shown that implementing proactive strategies is a continuous process and should be aligned with the overall security policy of the organization. Uses cases show how organizations prioritize threats, how to control and increase overall security posture and how to reduce human error by training users continuously. Security teams should create and plan their own strategies based on this example use cases.

9 Liability and Ethics

The thesis, Enhancing Cybersecurity Resilience: Proactive Strategies Utilizing Microsoft Defender XDR Tools, has been conducted in accordance with the ethical principles and research guidelines determined by JAMK University of Applied Sciences. The findings in the research have been handled in an accurate, transparent and reliable manner.

The author confirms that all sources, frameworks and tools (including Microsoft Defender XDR and related Microsoft local cybersecurity tools) referenced or implemented in this study have been cited and used in accordance with the relevant licensing and usage agreements.

No private or confidential information from third parties has been accessed, disclosed or used without explicit permission. In addition, this research has been designed and conducted in accordance with the principles of privacy and data protection. No personal, sensitive or identifiable institutional data has been collected, processed or analyzed during this study.

All tests, configurations, and simulations were conducted in isolated or non-production environments, and there is no risk for external systems or unexpected security impacts. The author accepts full responsibility for the content, results, and interpretations presented in this thesis. Even best efforts have been made to ensure the accuracy and relevance of the findings, JAMK Univer-

sity of Applied Sciences bears no responsibility for the practical application, operational use, or results resulting from the implementation of the recommendations or strategies outlined in this study.

References

Andress, Jason & Winterfeld, S. (2014). The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice: Second Edition. 1-217.

CISA (2016). Vulnerability Management Retrieved from https://www.cisa.gov/sites/default/files/publications/CRR_Resource_Guide-VM_0.pdf

Cisa (2021). Threats for organizations. Retrieved from https://www.cisa.gov/resources-tools/resources

Chapple, M. (2024) CC Certified in Cybersecurity Study Guide. Retrieved from https://viewer.books24x7.com/assetviewer.aspx?bookid=166653&chunkid=631774389

Cole, Eric. (2013) Advanced Persistent Threat: Understanding Danger and How to Protect Your Organization. Chapter 1: The changing threat

Crowdstrike (n.d). Secure the endpoint. Stop the breach. Retrieved from https://www.crowdstrike.com/en-us/platform/endpoint-security/

CSO online 2023. Retrieved form https://www.csoonline.com/article/3213279/what-is-reactive-security.html

Dave, Daksh & Sawhney, Gauransh & Aggarwal, Pushkar & Silswal, Nitish & Khut, Dhruv. (2023). The New Frontier of Cybersecurity: Emerging Threats and Innovations. Retrieved from https://www.researchgate.net/publication/376965928_The_New_Frontier_of_Cybersecurity_Emerging_Threats_and_Innovations/citation/download

Edwards, Jason (2024). Critical Security Controls for Effective Cyber Defense. Retrieved from https://link.springer.com/book/10.1007/979-8-8688-0506-6

Fahreen,Fatima (2024). A Qualitative Exploratory Study of Cyber Threats to Financial Organizations. Retrieved from https://www.proquest.com/docview/3058334090

Fortinet (2019). Reactive vs. Proactive Cybersecurity: Which Strategy is Best? Retrieved from https://www.fortinet.com/blog/industry-trends/reactive-vs--proactive-cybersecurity--5-reasons-why-traditional-

Fruhlinger, J. (2020) The OPM Hack Explained: Bad Security Practices Meet China's Captain America. Retrieved from https://www.csoonline.com/article/566509/the-opm-hack-explained-bad-security-practices-meet-chinas-captain-america.html

Gartner (2019). Magic Quadrant for Endpoint Protection Platforms. Retrieved from Gartner-Reprint-CRWD-1.pdf

Gartner (2024). Market Guide for Extended Detection and Response https://www.gartner.com/en/documents/5859979

Gharibi, W. (2011) Security Risks and Modern Cyber Security Technologies for Corporate Networks. Retrieved from https://www.researchgate.net/publication/49966083_Security_Risks_and_Modern_Cyber_Security_Technologies_for_Corporate_Networks

Gsctechnologies (2024). Ultimate-Guide-To-Microsoft-Secure-Score. Retrieved from https://www.gcstechnologies.com/wp-content/uploads/2023/05/GCS-Ultimate-Guide-To-Microsoft-Secure-Score.pdf

Guembe, B., Azeta, A., Misra, S., Osamor, V. C., Fernandez-Sanz, L., & Pospelova, V. (2022). The Emerging Threat of Ai-driven Cyber Attacks: A Review. Applied Artificial Intelligence, 36(1). Retirieved from https://doi.org/10.1080/08839514.2022.2037254 on 02.03.2025

IBM QRadar EDR (n.d) Retrieved from IBM QRadar EDR - Endpoint Detection and Response Solutions

IBM (2024). What is social engineering? Retrieved from https://www.ibm.com/think/topics/social-engineering

Agrafiotis, I., Nurse J., Goldsmith, M., Creese, S, Upton, D. (2018) A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate, Journal of Cybersecurity, Volume 4, Issue 1. Retrieved from https://doi.org/10.1093/cybsec/tyy006 on 04.03.2025

Kala, E. (2023) The Impact of Cyber Security on Business: How to Protect Your Business. Open Journal of Safety Science and Technology. doi: 10.4236/ojsst.2023.132003.

Laine, M. (2024). Preparing DevOps for ISO 27001 certification Retrieved from https://www.theseus.fi/bitstream/handle/10024/874323/Laine_Marjo.pdf?sequence=2&isAllowed=y

Liu, C., & Babar, M. A. (2024). Corporate cybersecurity risk and data breaches: A systematic review of empirical research. Australian Journal of Management. https://doi.org/10.1177/03128962241293658

Mason, J, Amelia, O. (2024) Emerging Threats and Mitigation Strategies in Cyber Security: A Comprehensive Guide for Financial Services and Strategic Management. Retrieved from Emerging Threats and Mitigation Strategies in Cyber Security: A Comprehensive Guide for Financial Services and Strategic Management

Microsoft Defender XDR components and architecture How do I pilot and deploy Microsoft Defender XDR? - Microsoft Defender XDR | Microsoft Learn

Microsoft Learn (n.d) How Defender for Cloud Apps helps protect your Microsoft 365 environment Retrieved from https://learn.microsoft.com/en-us/defender-cloud-apps/protect-office-365

Microsoft Learn (n.d) Retrieved from Overview of endpoint detection and response capabilities - Microsoft Defender for Endpoint | Microsoft Learn

Microsoft Learn (n.d) Retrieved from Microsoft 365 and Office 365 service descriptions - Service Descriptions | Microsoft Learn

Microsoft Learn (n.d.) Microsoft Security Exposure Management https://learn.microsoft.com/en-us/security-exposure-management/microsoft-security-exposure-management

Microsoft Learn (n.d.) https://learn.microsoft.com/en-us/microsoft-365/security/defender/xdr-overview?view=o365-worldwide

MITRE ATT&CK Framework (n.d.) Retrieved from https://attack.mitre.org

NIST. (2021). IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements. Retrieved from IoT Device Cybersecurity Guidance for the Federal Government: Establishing IoT Device Cybersecurity Requirements

Outsource Accelerator (2024). Data confidentiality explained: Privacy in a digital world Retrieved from https://www.outsourceaccelerator.com/articles/data-confidentiality/

Paloalto Networks (2025) Retrieved from https://www.paloaltonetworks.com/cyberpedia/what-is-xdr-vs-siem

Palo Alto Networks (2025) Retrieved from https://www.paloaltonetworks.com/cortex/cortex-xdr

Proofpoint (2024). The Human Firewall: Why Security Awareness Training Is an Effective Layer of Defense. Retrieved from https://www.proofpoint.com/us/blog/security-awareness-training/security-awareness-training-effectiveness

Sami Lamppu (2024). Defender XDR, Security Exposure Management. Retrieved from https://samilamppu.com/2024/04/25/microsoft-security-exposure-management-xspm-deep-dive-part-2/

Sentinelone (n.d.) What is SIEM (Security Information and Event Management)? Retrieved from https://www.sentinelone.com/cybersecurity-101/data-and-ai/what-is-security-information-and-event-management-siem/

Sms Business Cloud (2024) Understanding Microsoft Secure Score: A Comprehensive Guide Retrieved from https://smsbusinesscloud.com/news/understanding-microsoft-secure-score-a-comprehensive-guide/

Strategies, W and Ghulam, S. (2024) Emerging Cybersecurity Threats: Trends, Implications, and Mitigation. Retrieved from https://www.researchgate.net/publication/377382312_Emerging_Cybersecurity_Threats_Trends_Implications_and_Mitigation

Gharibi, Wajeb (2021) Studying and Classification of the Most Significant Malicious Software, Retrieved from https://arxiv.org/pdf/1106.0853

The New Frontier of Cybersecurity: Emerging Threats and Innovations (2023) Daksh Dave and others. Retrieved from The New Frontier of Cybersecurity: Emerging Threats and Innovations

The Basics of Information Security: Understanding the Fundamentals of InfoSec in Theory and Practice, Second Edition. Publisher: Syngress Publishing 2014

University of Berkeley (2024). Phishing. Retrieved from https://security.berkeley.edu/education-awareness/phishing

What is the CIA triad? A principled framework for defining infosec policies. Josh Fruhlinger, 2024 Retrieved from What is the CIA triad? A principled framework for defining infosec policies | CSO Online

What is cybersecurity, 2021. Retrieved form https://www.cisa.gov/news-events/news/what-cybersecurity