1ST EDITION

Microsoft Unified XDR and SIEM Solution Handbook

Modernize and build a unified SOC platform for future-proof security

RAGHU BODDU | SAMI LAMPPU

Foreword by Rod Trent

Senior Program Manager – Advocacy, Microsoft Corporation

Microsoft Unified XDR and SIEM Solution Handbook

Modernize and build a unified SOC platform for future-proof security

Raghu Boddu

Sami Lamppu

‹packt›

Microsoft Unified XDR and SIEM Solution Handbook

Group Product Manager: Pavan Ramchandani

Publishing Product Manager: Prachi Rana

Book Project Manager: Ashwini Gowda

Senior Editor: Athikho Sapuni Rishana

Technical Editor: Yash Bhanushali

Copy Editor: Safis Editing

Proofreader: Safis Editing

Indexer: Tejal Daruwale Soni

Production Designer: Alishon Mendonca

DevRel Marketing Coordinators: Marylou De Mello and Shruthi Shetty

First published: February 2024

Production reference: 1290224

Published by Packt Publishing Ltd.

Grosvenor House

11 St Paul's Square

Birmingham

B3 1RB, UK

ISBN 978-1-83508-685-8

www.packtpub.com

To my wife, Deepthi – without you, this book wouldn't be possible.

To my children, Avisha and Rishon – you are my life.

To my parents – you are the most beautiful memory inside my heart; you will always be remembered.

To all the cybersecurity professionals – this one is for you!

– Raghu Boddu

To my rock, Minna, whose unwavering support made this book possible.

To Eva and Mona, the joy in every page of our family story.

To our community, the guardians, and protectors of digital realms.

This book is yours as much as it is mine.

– Sami Lamppu

Foreword

The world of cybersecurity is constantly evolving and becoming more complex. Cyberattacks are becoming more frequent, sophisticated, and damaging, targeting organizations of all sizes and industries. Traditional security solutions, such as antivirus, firewalls, and endpoint protection, are no longer enough to defend against modern threats. Organizations need a new approach to security that is proactive, holistic, and intelligent.

This is where Microsoft's unified XDR and SIEM solution comes in. Microsoft's unified XDR and SIEM solution enables organizations to do the following:

- Detect and respond to threats faster and more effectively, using advanced analytics, artificial intelligence, and automation
- Gain visibility and insight into security posture and performance, using dashboards, reports, and alerts
- Reduce complexity and cost, using a single platform that integrates with existing security tools and processes
- Achieve compliance and governance, using built-in policies, controls, and audits

Microsoft's unified XDR and SIEM solution is not just a product but also a solution. It is designed to help organizations achieve their security goals and objectives, regardless of their size, industry, or maturity level. Whether you are an organization that is considering or evaluating Microsoft's unified XDR and SIEM solution, a cyber professional who wants to enter the realm of XDR and SIEM, an enterprise architect who wants to understand Microsoft's unified solution, a CISO looking for guidance who wants to see whether Microsoft's unified XDR and SIEM solution is a fit for you before you adopt it, or an organization looking for guidance on modernizing your security posture, this book is for you.

This book is a perfect companion for anyone wanting to keep up with Microsoft security platform technologies, as well as anyone who wants to stay relevant in a career in cybersecurity. Cybersecurity is a rewarding and exciting career option for many reasons. Here are some of them:

- **Cybersecurity is in high demand**: As cyberattacks become more frequent and sophisticated, organizations of all sizes and industries need skilled professionals who can protect their data, networks, and systems from cyber threats. According to the Bureau of Labor Statistics, the employment of information security analysts is projected to grow by 33% from 2020 to 2030, much faster than the average for all occupations.

- **Cybersecurity is well paid**: Due to the high demand and the skills gap, cybersecurity professionals can command competitive salaries and benefits. According to ZipRecruiter, the average annual salary for a cybersecurity engineer in the United States is over $99,000, and the average annual salary for a cybersecurity analyst is over $76,000.
- **Cybersecurity is diverse and dynamic**: Cybersecurity is a broad and diverse field that encompasses many subfields, such as machine learning, computer vision, natural language processing, and robotics. Moreover, cybersecurity is applied in various industries, such as healthcare, finance, and manufacturing. Therefore, cybersecurity professionals can choose from a variety of topics and domains that interest them the most and enjoy the challenge and variety of their work.
- **Cybersecurity is impactful and meaningful**: Cybersecurity professionals play a vital role in protecting the privacy and confidentiality of sensitive data and personal information from cyberattacks and other threats. They also contribute to the security and stability of society and the economy, by preventing and responding to cyberattacks that could compromise national security, public safety, or critical infrastructure. Cybersecurity professionals can make a difference and have a positive impact on the world.

This book is written by two Microsoft MVPs, Raghu Boddu and Sami Lamppu, who are experts and practitioners in the field of cybersecurity. They have extensive experience and knowledge in implementing and managing Microsoft's unified XDR and SIEM solution for various organizations and scenarios. They have also contributed to the Microsoft community by sharing their insights and best practices through blogs, webinars, podcasts, and events.

We hope that this book will help you to understand, appreciate, and adopt Microsoft's unified XDR and SIEM solution and to achieve your security goals and objectives. We also hope that this book will inspire you to share your feedback and experience with us and the Microsoft community, contributing to security knowledge and innovation.

Rod Trent

Senior Program Manager – Advocacy, Microsoft Corporation

Contributors

About the authors

Raghavendra (Raghu) Boddu is a Microsoft Security MVP based out of Texas. He works as a technical director and leads security and threat practice at Edgile, a Wipro company. A visionary leader with more than two decades of IT experience, he has helped many customers as an advisor, specializing in cybersecurity, legacy migration and modernization strategies, multi-cloud/hybrid implementations, digital cloud transformation roadmaps, cloud-native architectures, and so on. He has earned two masters (an MSc in information services and an MSc in information technology). He is also PMP-certified, Agile Scrum-certified, and Six Sigma Green Belt-certified, and he holds Azure and AWS solution architect certifications. You can find his author profile on LinkedIn by searching for the username `raghuboddu`.

To my beautiful wife, Deepthi, and our incredible children, whose unwavering love and support made writing this book a reality. Writing a book demands huge dedication and constant energy; this journey would have been impossible without your belief in me and every sacrifice you made along the way. In loving memory of my mom and dad, whose hearts were stolen too soon by COVID-19. Your guiding lights forever illuminate my path, and your love remains a treasure beyond measure. And finally, to my exceptional co-author, Sami Lamppu, whose dedication and brilliance were instrumental in shaping this book. Your invaluable partnership and tireless efforts made this journey an unforgettable one.

Sami Lamppu is a cloud security lead at Netox, a Finland-based cybersecurity company. With over 20 years of IT experience, he is a distinguished expert in the field. He is not only a Microsoft Security MVP but also a passionate advocate for cloud security. For the past eight years, he has been specializing in cloud security, focusing on innovative solutions and strategies. His expertise extends beyond the cloud, encompassing multi-cloud and hybrid implementations, as well as on-premises environments.

He is the co-author of *Entra ID Attack and Defense Playbook* (formerly known as *Azure AD Attack and Defense Playbook*), and he blogs frequently, sharing his knowledge at `https://samilamppu.com`. He holds a bachelor's degree in business information technology and holds of 50+ Microsoft certifications, dating back to Windows Server 2003 and Windows XP. You can find his author profile on LinkedIn by searching for the username `sami-lamppu`.

I dedicate this book to my cherished wife, Minna, and to our amazing children. Your unwavering support and love have made this journey possible. Thank you for making this dream a reality. Special thanks to my co-author, Raghu Boddu, whose collaborative spirit and shared passion breathed life into these pages. Your contribution has been invaluable, and I'm grateful for the opportunity to have worked alongside such a talented and inspiring partner.

About the reviewers

Thomas Naunheim is a cybersecurity architect at glueckkanja AG and a Microsoft MVP, from Koblenz, Germany. His principal focus is on identity and security solutions in Microsoft Azure and Microsoft Entra. Thomas shares his experience and research with the community as a blogger at `cloud-architekt.net`, and he is a speaker at conferences and co-author of *Entra ID Attack and Defense Playbook*. He is a member of the *Azure Meetup Bonn* and *Cloud Identity Summit* organization teams and is also co-host of the podcast *Cloud Inspires*.

Harri Jaakkonen is a Nordic security practice lead at Avanade and Microsoft Security MVP who lives in Finland. His principal focus is on identity and security solutions in Microsoft Azure and Microsoft Entra. He has over 28 years of experience in the field in various areas. Harri writes study guides and previews deep dives for the community at `cloudpartner.fi`.

Content contributors

Sakari Pajulampi: A review of the MDO and MDE sections in *Chapter 3*

Joosua Santasalo: Attack scenario simulation in *Chapter 5*

Armando Penumuri: A contribution to *Chapter 10*

Table of Contents

2

Introduction to XDR and SIEM 15

3

Microsoft's Unified XDR and SIEM Solution 31

Part 2 – Microsoft's Unified Approach to Threat Detection and Response

4

Power of Investigation with Microsoft Unified XDR and SIEM Solution 93

5

Defend Attacks with Microsoft XDR and SIEM 133

Part 3 – Mastering Microsoft's Unified XDR and SIEM Solution – Strategies, Roadmap, and the Basics of Managed Solutions

8

9

10

Preface

This book unlocks the basics and importance of Zero Trust, XDR, and SIEM, and dives deep into Microsoft's unified XDR and SIEM solution. You will learn about its powerful capabilities, holistic benefits, and real-world use cases. Plus, you will learn about individual defenders such as MDI, MDO, MDE, MDA, MDC, and Microsoft Sentinel.

Let's level up your security architecture! By the end of this book, you'll be a Microsoft XDR and SIEM pro, understanding Microsoft's unified approach and its power to break down silos and strengthen your defenses. This book is your one-stop guide to improving your security posture with ease. From early adopters to major players, the list of organizations embracing Microsoft's unified XDR and SIEM solution is growing rapidly.

In this book, you will learn about the following:

- The concepts of Zero Trust, XDR, and SIEM, and the importance of considering them to improve your security posture
- Microsoft's unified XDR and SIEM solution and the importance of adopting this unified solution and its holistic benefits
- How to elevate your security posture with the Microsoft Defender tools MDI, MDE, MDO, MDA, MDC, Sentinel SIEM, and SOAR
- The true capabilities of Zero Trust, XDR, and SIEM, and real-world use cases to improve your security posture with case-study-based learning
- How Microsoft's unified XDR and SIEM solution auto-disrupts some attacks
- How to adopt Microsoft's unified XDR and SIEM solution and some of the assessments and strategies worth considering
- How managed XDR and managed SOC services work and the importance of considering those managed services

Who this book is for

This comprehensive book is your one-stop guide to mastering Microsoft's unified XDR and SIEM solution.

This book is ideal for the following people:

- CISOs and IT executives, to help you make informed decisions about your security posture and streamline your security stack.
- Cloud security architects, to help you build a unified security strategy with Microsoft's powerful tools.

- Anyone struggling with fragmented security solutions, as it helps to eliminate siloed architectures and achieve better security faster.
- This book is especially relevant in today's remote work world. Many companies wrestling with a patchwork of security tools post-pandemic will find this guide invaluable. You will discover whether Microsoft's unified solution offers the perfect fit for your organization, especially with the added incentive of bundled tools with licenses such as E5, A5, and so on. You will also enhance your ROI and build a robust, unified security architecture with confidence.
- Aspiring SOC analysts and Microsoft Security enthusiasts, this guide is for you! Fast-track your SOC career or dive into Microsoft Security with this comprehensive Microsoft unified XDR and SIEM solution book.

What this book covers

Chapter 1, *Introduction to Zero Trust*, lays the groundwork for understanding why XDR and SIEM solutions are crucial by delving into the concept of Zero Trust: its importance, principles, architecture, implementation considerations, and significance for security operations. We'll explore these topics in detail with practical recommendations, building a solid foundation for your decision-making.

Chapter 2, *Introduction to XDR and SIEM*, dives deep into the world of XDR and SIEM, explaining their core functions and why they're essential for modern cybersecurity. It explores their true capabilities, practical use cases, and implementation strategies, untangling buzzwords such as EDR, MDR, NDR, and SIEM along the way. Ultimately, it proposes a solution to break down siloed security architectures and streamline SOC operations, empowering analysts with improved triaging, investigation, and threat-hunting tools.

Chapter 3, *Microsoft's Unified XDR and SIEM Solution*, dives deep into Microsoft's unified XDR and SIEM solution, showcasing its seamless integration and benefits. It then explores each defender within Microsoft Defender XDR (MDE, MDI, MDO, MDA, and MDC) and Microsoft Sentinel, the SIEM and SOAR solution. Finally, it makes a compelling case for why adopting this unified approach can break down siloed security tools and propel your enterprise to a whole new level of protection.

Chapter 4, *Power of Investigation with Microsoft's Unified XDR and SIEM Solution*, delves into how Microsoft's unified XDR and SIEM solution empowers enterprises to revamp their SOC, streamlining daily operations and life cycle management. It explores the critical benefits this integration offers over traditional siloed technologies, enabling faster threat response and enhanced triaging, investigation, and remediation workflows.

Chapter 5, *Defend Attacks with Microsoft's Unified XDR and SIEM*, examines the application of Microsoft's unified XDR and SIEM solution in safeguarding organizations against cyber threats such as identity-based supply chain attacks in cloud, **human-operated ransomware** (**HumOR**), and **business email compromise** (**BEC**) attacks. Beyond a thorough analysis of the threat landscape, practical demonstrations of these tools' effectiveness will be covered.

Chapter 6, *Security Misconfigurations and Vulnerability Management*, delves into the critical nature of security misconfigurations and vulnerabilities, outlining a high-level vulnerability management process and showcasing how Microsoft's unified XDR and SIEM solution tackles these challenges head-on.

Chapter 7, *Understanding Microsoft Secure Score*, empowers you to strengthen your organization's security posture by navigating effective strategies to boost your Secure Score and understanding the reasoning behind each recommendation.

Chapter 8, *Microsoft XDR and SIEM Implementation Strategy, Approach, and Roadmap*, guides you through successfully implementing Microsoft's unified XDR and SIEM solution, highlighting crucial topics such as assessments, strategic considerations, and best practices for effective adoption and deployment.

Chapter 9, *Managed XDR and SIEM Services*, dives into the fundamentals and advantages of managed XDR and SIEM services, revealing how their effective management can shield you against a vast spectrum of cyber threats.

Chapter 10, *Useful Resources*, offers valuable resources to sharpen your skills in Microsoft's unified XDR and SIEM solution, empowering you to defend your organization against evolving threats with confidence.

Conventions used

There are a number of text conventions used throughout this book.

`Code in text`: Indicates code words in text, database table names, folder names, filenames, file extensions, pathnames, dummy URLs, user input, and Twitter handles. Here is an example: "All alerts, incidents, and relevant data are synced between the solutions, and data is populated in Sentinel to the **SecurityAlert** and **SecurityIncident** tables."

Bold: Indicates a new term, an important word, or words that you see onscreen. For instance, words in menus or dialog boxes appear in **bold**. Here is an example: "If you need to verify the MSSP's permissions, they can be accessed from the **Service providers** blade in the Azure portal."

> **Tips or important notes**
> Appear like this.

Get in touch

Feedback from our readers is always welcome.

General feedback: If you have questions about any aspect of this book, email us at `customercare@packtpub.com` and mention the book title in the subject of your message.

Errata: Although we have taken every care to ensure the accuracy of our content, mistakes do happen. If you have found a mistake in this book, we would be grateful if you would report this to us. Please visit `www.packtpub.com/support/errata` and fill in the form.

Piracy: If you come across any illegal copies of our works in any form on the internet, we would be grateful if you would provide us with the location address or website name. Please contact us at `copyright@packt.com` with a link to the material.

If you are interested in becoming an author: If there is a topic that you have expertise in and you are interested in either writing or contributing to a book, please visit `authors.packtpub.com`.

Share Your Thoughts

Once you've read *Microsoft Unified XDR and SIEM Solution Handbook*, we'd love to hear your thoughts! Please `click here to go straight to the Amazon review page` for this book and share your feedback.

Your review is important to us and the tech community and will help us make sure we're delivering excellent quality content.

Download a free PDF copy of this book

Thanks for purchasing this book!

Do you like to read on the go but are unable to carry your print books everywhere?

Is your eBook purchase not compatible with the device of your choice?

Don't worry, now with every Packt book you get a DRM-free PDF version of that book at no cost.

Read anywhere, any place, on any device. Search, copy, and paste code from your favorite technical books directly into your application.

The perks don't stop there, you can get exclusive access to discounts, newsletters, and great free content in your inbox daily

Follow these simple steps to get the benefits:

1. Scan the QR code or visit the link below

`https://packt.link/free-ebook/9781835086858`

2. Submit your proof of purchase
3. That's it! We'll send your free PDF and other benefits to your email directly

Case Study – High Tech Rapid Solutions Corporation

In this book we will consider a scenario of driving digital transformation and security enhancement at High Tech Rapid Solutions Corp (a fictional company name we will use throughout this book).

Introduction

High Tech Rapid Solutions Corp, a global leader in manufacturing and distribution, has 60,000 employees spread across multiple office locations on three continents. The company management understands the need to modernize their security operations, leverage modern cloud-based technologies, and enhance current security measures. Before the COVID-19 pandemic, they had a more traditional approach and had been less attracted toward remote work. However, the COVID-19 pandemic forced the company to quickly adapt remote work practices, leading to major improvements needs in the company security practices and technologies. This new situation led to a reevaluation of High Tech Rapid Solutions Corp security measures, prompting the organization to consideration of a security monitoring strategy and architecture to address their security needs and tackle the challenges caused by their siloed architecture.

Alongside the security landscape changes, High Tech Rapid Solutions Corp faces challenges in driving its new technology initiatives. The adoption of modern cloud-based technologies requires careful planning, time, dedicated resources, and a workforce equipped with the necessary skills. The organization understands how important it is to find new and retaining existing professionals who can effectively implement and manage their planned transformation initiatives. The company does manage its **Security Operations Center** (**SOC**) by itself and does not leverage any service provider's managed services in this area, even though it has been under consideration.

Furthermore, the pandemic presented unique challenges to High Tech Rapid Solutions Corp, accelerating the need for a **cloud-first strategy**. The company appointed a new **Chief Information Security Officer** (**CISO**) to the management team in order to guarantee the secure adoption of modern cloud-based technologies. CISO, who provides extensive experience in the cloud security domain, plays a key role in supporting the company's strategy, security teams, and business to maintain security as the top priority.

The current environment

High Tech Rapid Solutions Corp operates in a dynamic environment, characterized by diverse technologies and platforms. The key aspects of its current environment are as follows.

A cloud environment

Currently the company is operating in a multi-cloud environment, leveraging both Azure and AWS for its cloud infrastructure and business needs. This strategic adoption allows the company to benefit from the unique security features and capabilities offered by each cloud provider, while ensuring strong data protection across its operations.

A hybrid cloud architecture

Currently the company maintains a hybrid cloud architecture, combining on-premises infrastructure with cloud resources. This approach enables this company to maximize security controls and compliance requirements, while capitalizing on the scalability, agility, and cost-effectiveness of the cloud.

User entities

They have a hybrid identity architecture in place that allows seamless authentication and authorization for employees, granting them secure access to resources and applications across the hybrid cloud environment.

Collaboration with partners

High Tech Rapid Solutions Corp collaborates with external partners to drive business growth and innovation. To establish secure collaboration, the company extends its identity management capabilities to partners by leveraging Entra ID External ID (former Azure Active Directory) B2B collaboration and cross-tenant capabilities, enabling partners to access specific resources and collaborate within designated workflows.

End user devices

High Tech Rapid Solutions Corp operates in a diverse device landscape that supports both Windows and macOS platforms. The following aspects outline the current device environment:

- **Windows devices**: Windows devices form the majority of the organization's device ecosystem. Approximately 80% of the devices within the organization run on Windows operating systems.
- **macOS devices**: The company recognizes the need to take care user preferences and are having macOS devices in its device catalog as well These devices, comprising approximately 20% of the overall device inventory, are equipped with security features and management tools to maintain consistent security standards across platforms.
- **Mobile phones**: The company operates on diverse platforms such as iOS and Android.

Server infrastructure

High Tech Rapid Solutions Corp maintains a diverse server infrastructure to support its operations. The server landscape includes a mix of Windows and Linux servers, with the majority being Windows-based.

An application landscape

High Tech Rapid Solutions Corp's applications are distributed across both on-premises and cloud environments. While legacy applications may still reside on-premises, they prefer modern technologies and cloud-native architectures for new application development, incorporating strong security measures to protect sensitive data and protect against cyber threats.

An IoT/OT environment

In the company's IoT/OT environment, **Internet of Things** (**IoT**) devices are integrated with traditional **Operational Technology** (**OT**) to optimize operations. Interconnected sensors and machines collect real-time data from production to supply chain, feeding into centralized analytics for quick decision-making. The main challenge with IoT/OT environment is that it is lacking proper security monitoring and visibility to the environment from monitoring point if view is limited.

Security challenges

High Tech Rapid Solutions Corp has identified the following security-related challenges for their multi-cloud environment:

- **Siloed security architecture**: High Tech Rapid Solutions Corp's existing security infrastructure consists of disparate products that operate in isolation, resulting in limited visibility, missing threat intelligence, and inefficient incident response capabilities.
- **Incomplete security insights**: The lack of centralized security monitoring and analytics hinders the ability to correlate and analyze security events, making it difficult to identify security threats and vulnerabilities promptly.
- **Inefficient threat response**: The absence of a unified security platform and standardized processes undermines the effectiveness and agility of High Tech Rapid Solutions Corp's incident response, leading to delays in containing and mitigating security incidents. Currently, they use a legacy **Security and Information Management System** (**SIEM**) and is keen to modernize SIEM with a cloud-based solution.
- **Regulatory compliance**: High Tech Rapid Solutions Corp must adhere to industry-specific regulations and compliance frameworks. Ensuring continuous compliance with standards presents challenges in terms of data protection, access controls, and security audits.

Management concerns

Management is especially concerned about the following specific areas and several possible attack scenarios, based on the history they have had with breaches:

- **Lack of visibility and control in an IoT/OT environment**: High Tech Rapid Solutions Corp's IoT/OT environment includes a wide range of devices and systems with varying security controls. This lack of standardized visibility and control makes the environment difficult to monitor and they are lacking of managing potential security vulnerabilities and incidents effectively.

- **Lack of visibility on internet-exposed digital assets**: High Tech Rapid Solutions Corp doesn't have a clear understanding of its digital assets that are reachable from the internet, as well as the possible weak configurations on them. Their digital assets includes domains, subdomains, web applications, cloud services, APIs, and IoT devices. The compliance and regulatory requirements that the organization must adhere to in different regions and industries mandate strict security standards and best practices, protecting customer data and intellectual property.
- **A Threat Intelligence (TI) data (feed) does not exist**: High Tech Rapid Solutions Corp's security teams don't have TI data available, which can lead to a situation where they don't have full visibility of potential attack vectors, and they are incapable of prioritizing the most critical threats and vulnerabilities. In addition, the company wasting valuable time and resources on false positives and irrelevant alerts, often missing key indicators of compromise and early warning signs of breaches. As it struggles to keep up with constantly developing security threats, High Tech Rapid Solutions Corp risks losing reputation, customer trust, and revenue due to data breaches and downtime.

Challenges emphasized by security teams

High Tech Rapid Solutions Corp's security team raised some concerns and challenges that they faced during the last year:

- The finance department noticed some suspicious activities in their mailboxes, the creation of suspicious mail rules, and a few confidential emails leaking outside their department.
- The SOC team noticed many incidents, and they are confident that handling certain vulnerabilities would fix these incidents and reduce the number of incidents/alerts, but they struggling to gain visibility on the vulnerabilities.
- The SOC team has limited resources, which leads to triage, investigation, and remediation challenges, and these delays cause escalations to senior management (i.e., lack of auto-remediation and mitigations).
- The SOC team spends long hours fulfilling management ad hoc reporting needs.
- Management is concerned about the SOC team's inability to promptly address vulnerabilities and misconfigurations, which is attributed to the absence of a defined process and a dedicated vulnerability management team.
- The HR department raised concerns to the security team about unauthorized users accessing their apps or servers.
- Management initiated cost reduction strategies across the organization and allocated limited funds to the security team, asking them to reduce their cost, reduce the headcount, and submit **Return on Investment** (**ROI**) for any proposals, while simultaneously enhancing their security.

- The existing security team is not ready to adopt new technologies and needs training and guidance for new initiatives.
- The security team noticed too many users responding to spam messages and noticed URL clicks, and management asked the team to control these activities and train end users.
- Management asked the security team to keep an extra eye on certain assets, as well as terminate employees and contractors/vendors.
- The security team noticed too many false positives and spent a lot of time addressing these.
- The SecOps team struggles to track apps in the organization and control them.
- The SecOps team don't have enough knowledge about the Entra ID application consent framework and on how new and existing application registrations and permissions should be evaluated.
- The SOC team doesn't have active security monitoring for on-premises identities.
- The SecOps team doesn't have active security posture management for their cloud or on-premises resources
- High Tech Rapid Solutions Corp operations runs in three different continents, and some employees travel between office locations, factories, and so on. For the SOC team, it's complicated to identify false/positive and true/positive logins with the current security monitoring solutions.
- In a multi-cloud environment, High Tech Rapid Solutions Corp has been struggling to deploy agents on all servers.
- High Tech Rapid Solutions Corp's SecOps team has been failing to identify possible attack paths to cloud resources.

Concerns raised by CISO

The following are the concerns raised by the CISO:

- **Attacks on M365 collaboration workloads (BEC)**: As High Tech Rapid Solutions Corp extensively use various collaboration tools, such as Microsoft Teams and SharePoint Online, it needs to address potential data leaks, phishing attempts, and other security risks associated with cloud-based collaboration. Additionally, the organization is concerned about the growing threat of **Business Email Compromise** (**BEC**) attacks, where cybercriminals target employees through email communications to compromise sensitive data, initiate fraudulent financial transactions, or gain unauthorized access to company resources. Mitigating the risks posed by BEC attacks has become one of the top priorities for the company, as these attacks can lead to severe financial and reputational consequences.

- **Ransomware attacks**: High Tech Rapid Solutions Corp is increasingly concerned about the rising threat of ransomware attacks. The potential impact of a successful ransomware attack on its critical data and operations is a major risk. The organization seeks robust security measures and proactive incident response capabilities to prevent, detect, and respond effectively to ransomware incidents. Ransomware attacks, combined with the potential threat of BEC attacks, have emphasized the need for a comprehensive and layered security approach. High Tech Rapid Solutions Corp aims to implement advanced threat detection and prevention solutions, conduct regular security awareness training for employees, and enforce strict access controls to minimize the risk of ransomware and BEC attacks.

A recent incident response case

The company faced a targeted BEC attack six months ago that had a financial impact on business, and they want to detect and prevent similar attacks from happening in the future.

The BEC attack on High Tech Rapid Solutions Corp contained the following phases:

- **Initial reconnaissance**:

  The attacker gained information about the company and identified key personnel through company's websites and LinkedIn.

- **A phishing email**:

  The attacker needed credentials to get access to the environment, and one of the most common ways is to do so is by some form of phishing email. On this occasion, they used a spearphishing attachment (T1566.001 in MITRE ATT&CK `https://packt.link/eOJcm`) that included a malicious attachment. By clicking the link, the user believed that they were logging into a Microsoft sign-in page and entered their credentials.

- **Persistence and exfiltration**:

  After gaining access to the target user's mailbox, the attacker created a forwarding rule to the mailbox for data exfiltration.

- **Financial fraud**:

  The actual victim of this attack was a procurement manager who believed that the email (marked as **Important** and **Confidential**) urging for immediate payment came from CFO.

- **Impact**:

  As a result of the successful BEC attack, the following occurred:

  - The financial team transferred a significant sum of money to the attacker's account, thinking it was a legitimate payment.
  - The real vendor who should have received this payment but did not receive it, contacted the company to inquire about the overdue invoice.

- The financial team realized it had been scammed, but it was too late to recover the funds, as they had already been transferred to an overseas account.
- The company suffered a financial loss, damage to its reputation, and potential legal consequences for failing to secure sensitive financial transactions.

To prevent such attacks in the future, the company is committed to strengthening its security environment security posture, focusing on implementing robust email security measures, employee training, and verification protocols for financial transactions.

Summary

This case study will be explored throughout the book in the different chapters, focusing on how High Tech Rapid Solutions Corp can benefit from leveraging Microsoft's unified XDR and SIEM solution to address security challenges.

Part 1 – Zero Trust, XDR, and SIEM Basics and Unlocking Microsoft's XDR and SIEM Solution

This part breaks down the basics of Zero Trust, XDR, and SIEM, and explains why you should think about using both XDR and SIEM together, especially Microsoft's unified XDR and SIEM solution. It's like having a security toolbox with all the right tools for the job, making it easier to protect yourself from cyber threats.

This part has the following chapters:

- *Chapter 1*, *Introduction to Zero Trust*
- *Chapter 2*, *Introduction to XDR and SIEM*
- *Chapter 3*, *Microsoft's Unified XDR and SIEM Solution*