

WHITEPAPER

MINI SOC WHITEPAPER

Building an effective
Security Operations capability
with Microsoft Defender XDR

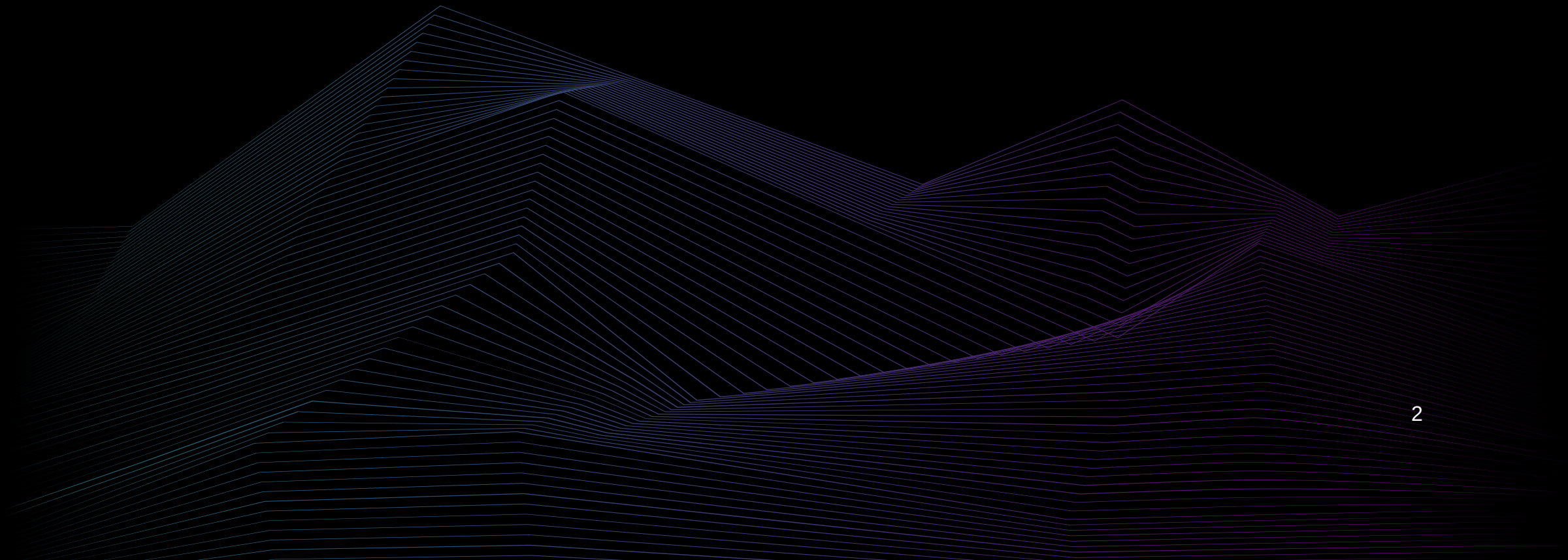
Created by

Tibor Luter | SOC
June 2026



TABLE OF CONTENTS

ABOUT BLACKCELL	3
EXECUTIVE OVERVIEW	5
INTRODUCTION	6
THE TRADITIONAL ROLE OF SIEM	7
SECURITY VISIBILITY AND TELEMETRY	8
WHY EDR AND XDR CHANGED THE GAME	10
BUILDING A MINI SOC WITH DEFENDER XDR	12
OPERATIONAL USE CASES FOR A MINI SOC	13
THREAT HUNTING WITHOUT A SIEM	15
PHISHING INVESTIGATION AND RESPONSE	16
VULNERABILITY MANAGEMENT AND EXPOSURE	17
REDUCTION	
LIMITATIONS OF THE MINI SOC MODEL	18
CONCLUSION	20



ABOUT BLACK CELL

Black Cell is a European cybersecurity company focused on protecting critical infrastructures and the organizations that support them. Our business units cover SOC, Integration, Offensive Security, Cloud Security, Compliance, and ESM (Enterprise Security Monitoring). We take a customer first approach that starts with listening, then shaping solutions to fit the way our clients operate.

Our teams are adaptable and draw on deep knowledge across industries and technologies, from IT and Cloud to ICS/OT. We engage for the long term, providing continual support, service improvement, and measurable outcomes over the lifecycle of the relationship. Clients rely on us to connect regulatory requirements with technology choices and to guide organizational transformation that sticks.

We combine architecture, implementation, and managed operations to close gaps quickly and build sustainable capability. Local presence in Central Europe matters to us, with teams in Budapest and Frankfurt am Main that understand the regional context. This proximity helps us respond faster, coordinate with partners, and keep stakeholders aligned. Above all, we aim to be a trusted partner who strengthens resilience today and prepares you for what comes next.

DISCLAIMER

The information provided in this document is for general guidance only and is used at your own risk. No contractual or advisory relationship is created between Black Cell and any person accessing or using this document or any part of it. Black Cell accepts no liability for any actions, decisions, or consequences arising from the use of this material.

References to third-party sources are included where appropriate. Black Cell is not responsible for the content, accuracy, or availability of external sources, including websites mentioned in this publication.

CONTACT

Tibor Luter
SOC Director
tibor.luter@blackcell.io

COPYRIGHT NOTICE

© 2026 Black Cell Hungary Zrt. & Black Cell Germany GmbH (hereinafter jointly referred to as Black Cell).

All rights reserved. This publication may be freely distributed in its complete and unaltered form for informational purposes. However, reproduction, modification, or extraction of any part of this document (by any means, including electronic, mechanical, photocopying, or recording) is strictly prohibited without prior written permission from Black Cell.

EXECUTIVE OVERVIEW

Security Operations Centers (SOCs) have traditionally relied on Security Information and Event Management (SIEM) platforms as the central nervous system for security monitoring, investigation, and response. However, the evolution of Extended Detection and Response (XDR) platforms has fundamentally changed this paradigm. Modern XDR solutions provide **deep telemetry, built-in analytics, automated correlation, investigation workflows, threat hunting capabilities,** and response actions that historically required a dedicated SIEM deployment.

This whitepaper examines the concept of a “Mini SOC” operating without a traditional SIEM. The approach is particularly relevant for small and medium-sized organizations, cloud-first enterprises, and organizations heavily invested in the Microsoft ecosystem. Rather than collecting and normalizing every log source into a central repository, the Mini SOC model prioritizes actionable visibility, high-quality detections, operational efficiency, and rapid response.

The paper analyzes the traditional role of SIEM platforms, the emergence of XDR, the Microsoft Defender ecosystem, operational use cases, threat hunting, phishing investigations, vulnerability management, limitations, and decision criteria for determining when a SIEM remains necessary.

INTRODUCTION

The security landscape has become increasingly complex. Organizations operate hybrid infrastructures spanning endpoints, cloud services, identities, SaaS applications, and remote work environments. At the same time, cyber attackers exploit multiple attack vectors and move laterally across environments.

Historically, SIEM platforms were deployed to aggregate logs from disparate sources and provide a centralized location for analysis. Over time, however, endpoint detection and response technologies matured significantly. Modern XDR platforms now integrate telemetry from endpoints, identities, email systems, cloud workloads, and SaaS services. They also incorporate machine learning, threat intelligence, automated investigations, and response capabilities.

As a result, organizations must reconsider whether every environment truly requires a full SIEM deployment. For many organizations, a focused security operation based primarily on XDR capabilities can provide sufficient visibility and protection while significantly reducing operational complexity and cost.

THE TRADITIONAL ROLE OF SIEM

Traditional SIEM platforms deliver several core functions. They centralize alerts from multiple technologies, normalize data, support correlation rules, provide long-term log retention, generate compliance reports, and enable forensic investigations.

Common SIEM use cases include:

- Centralized alert management.
- Correlation across multiple vendors.
- Long-term forensic log retention.
- Compliance and audit reporting.
- Custom detection development.
- Integration of specialized log sources.
- Security dashboards and operational metrics.

These capabilities remain valuable. However, many organizations use SIEM platforms primarily for alert aggregation while relying on endpoint security tools for actual detection and response. This creates duplication of effort and increases operational overhead.

SECURITY VISIBILITY AND TELEMETRY

Visibility remains the most important requirement for any security operation. Without telemetry, organizations cannot detect, investigate, or respond to threats.

Typical security data sources include network security devices, Active Directory and identity systems, cloud services, email platforms, business applications, databases, endpoints, and servers. Historically, SIEM platforms acted as the central repository for these sources.

Modern XDR platforms increasingly provide native access to these data streams. Microsoft Defender (MDE), for example, integrates endpoint activity, identity signals, email telemetry, cloud application events, SaaS activity, vulnerability information, and threat intelligence. This integrated telemetry model reduces the need to build complex data pipelines while improving contextual awareness during investigations.

Telemetry Feature Category	MSI	Symon	Carbon Black	Cortex XDR	Dynatrace	Blasir	IBM Regard	FortiEDR	SecurixOne	Trellix	Trend Micro
Process Activity	6/7	6.5/7	5/7	5.5/7	6.5/7	7/7	4.5/7	2/7	5/7	5/7	5.5/7
File Manipulation	4/5	2/5	5/5	4/5	4.5/5	5/5	1.5/5	3/5	4/5	5/5	4/5
User Account Activity	4/6	4/6	1/6	1.1/6	4.1/6	1.1/6	4/6	1.1/6	4/6	4/6	2.1/6
Network Activity	4/6	4/6	4/6	4/6	4/6	1.1/6	1.1/6	2.1/6	2.1/6	4/6	4/6
Registry Activity	3/3	3/3	3/3	3/3	1/3	3/3	3/3	1.5/3	3/3	3/3	3/3
Schedule Task Activity	3/3	4/3	4/3	1.5/3	3/3	1.5/3	1/3	1.5/3	3/3	1/3	1.5/3
Service Activity	1/1	4/1	4.1/1	1/1	1.1/1	1.1/1	1/1	1.1/1	1.1/1	1/1	1.1/1
Driver Module Activity	1/1	1/1	4/1	1/1	2/1	1/1	1/1	4.1/1	1.1/1	4/1	4.1/1
Device Operations	4/4	4/4	4.1/4	1.1/4	4/4	4/4	1/4	4/4	1/4	4/4	4/4
Group Policy Modification	1/1	4/1	4/1	4/1	4/1	4/1	4/1	4/1	1/1	4/1	4/1
Named Pipe Activity	2/2	2/2	4.5/2	4/2	2/2	4/2	1/2	4/2	1/2	1/2	1/2
WMI Activity	4/4	4/4	4/4	1.1/4	4/4	4/4	4/4	1.1/4	4/4	4/4	1.1/4
BitLocker Activity	4/4	4/4	4/4	4.1/4	1/4	4/4	1/4	4.1/4	4.1/4	1/4	4.1/4
PowerShell Activity	1/1	4/1	1/1	4.5/1	1/1	4.5/1	1/1	4.5/1	1/1	1/1	1/1
TOTAL	10/46	26.5/46	18.5/46	26.5/46	17/46	26.5/46	26.5/46	17.5/46	16/46	16/46	26.5/46

Figure 1 - Source: edr-telemetry.com

WHY EDR AND XDR CHANGED THE GAME

Endpoint Detection and Response (EDR) platforms transformed security operations by providing detailed telemetry directly from managed endpoints. Process creation, file activity, network connections, PowerShell execution, registry modifications, persistence mechanisms, and user activity can all be monitored in near real time.

The next evolution, XDR, extends this visibility beyond endpoints. Instead of investigating isolated events, analysts gain access to correlated incidents spanning identities, endpoints, email, cloud applications, and infrastructure.

Modern XDR capabilities include:

- High-quality behavioral detections.
- Automated incident correlation.
- Attack path visualization.
- Integrated threat intelligence.
- Threat hunting workspaces.
- Automated investigation and remediation.
- Cross-domain visibility.

This convergence reduces reliance on traditional SIEM architectures for many operational security functions.

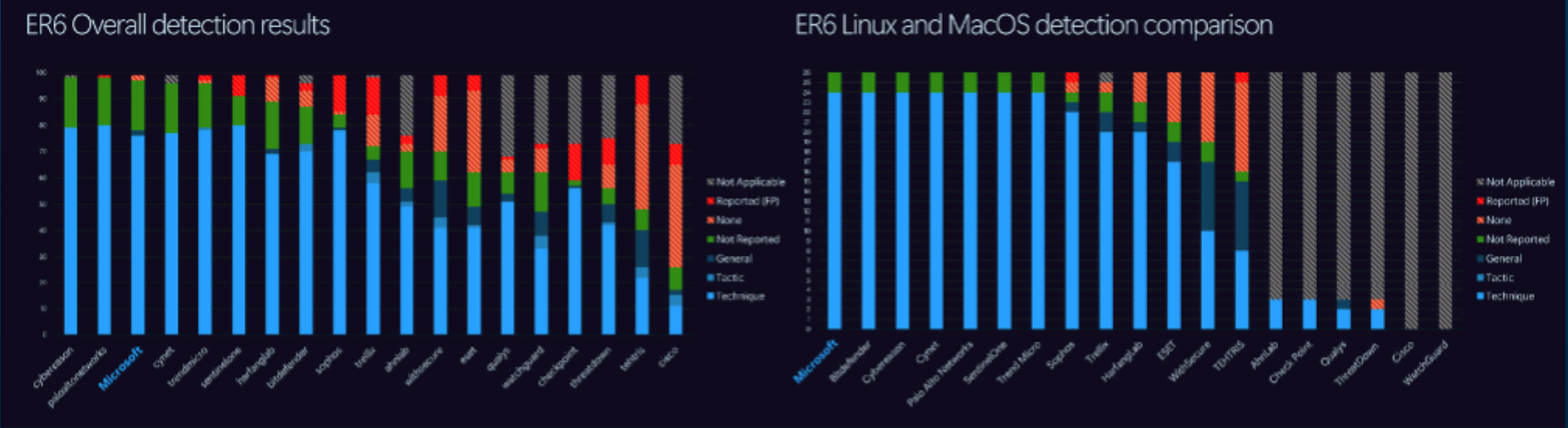


Figure 2 - Source: [MITRE ATT&CK Evaluations - Enterprise 2024](#)

BUILDING A MINI SOC WITH DEFENDER XDR

The Microsoft security ecosystem demonstrates how a Mini SOC can operate without a dedicated SIEM. Defender for Endpoint, Defender for Office 365, Defender for Identity, Defender for Cloud Apps, Defender for Cloud, Microsoft Entra ID Protection, and Microsoft Purview collectively provide visibility across critical attack surfaces.

The platform delivers a single pane of glass where analysts can review incidents, investigate evidence, execute response actions, and conduct threat hunting activities. Because telemetry is collected natively across Microsoft services, contextual correlation occurs automatically.

This approach enables security teams to focus on security outcomes rather than infrastructure management. Instead of maintaining collectors, parsers, normalization rules, and storage architectures, analysts can concentrate on detection engineering and incident response.

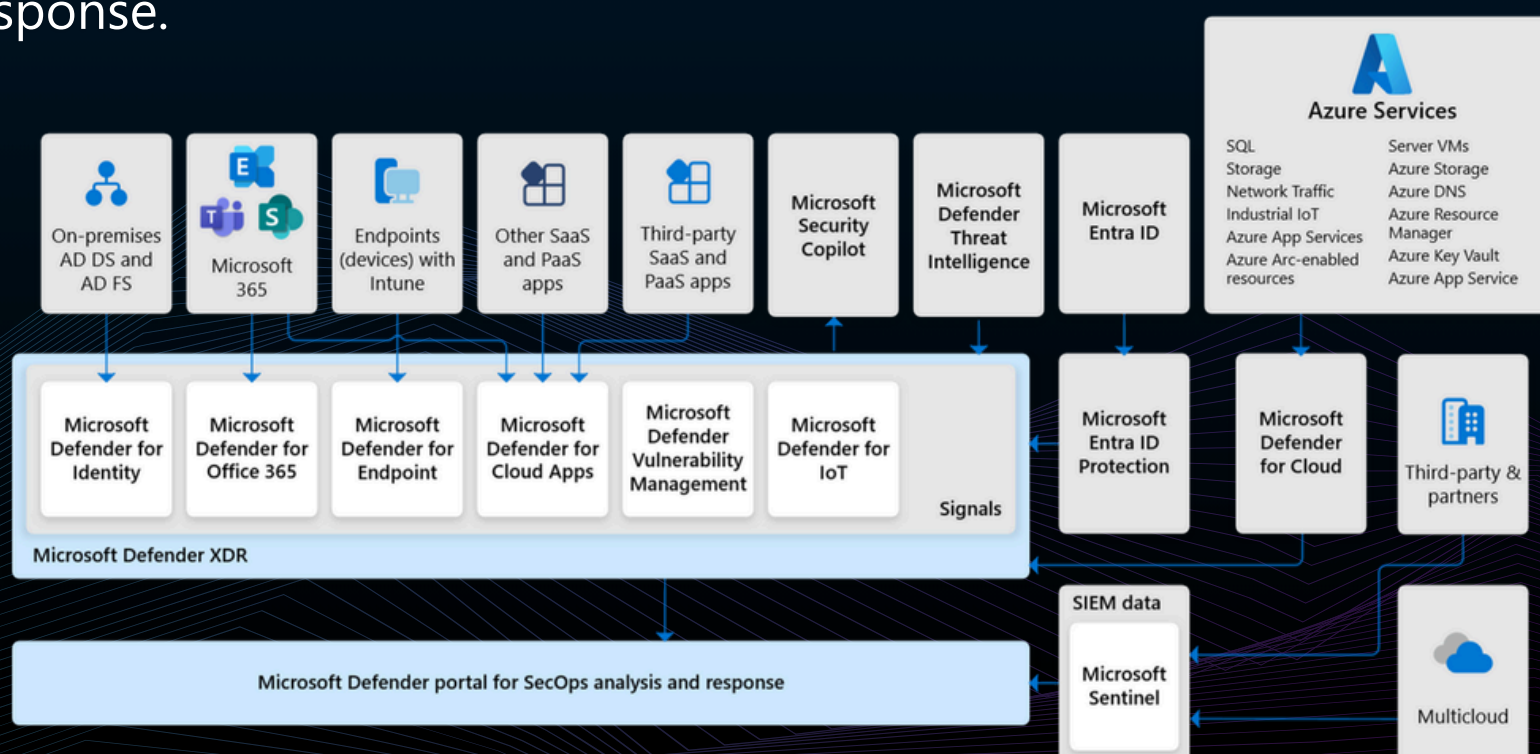


Figure 3 - Microsoft Security ecosystem

OPERATIONAL USE CASES FOR A MINI SOC

A Mini SOC should prioritize practical operational outcomes.

INCIDENT DETECTION:

Native analytics and machine learning identify suspicious activity such as credential theft, malware execution, ransomware behavior, phishing attacks, lateral movement, and cloud abuse.

INVESTIGATION:

Analysts can review timelines, process trees, user activity, authentication events, email artifacts, and cloud activity within a unified investigation experience.

RESPONSE:

Remote device isolation, malware removal, user account containment, session revocation, and automated remediation significantly reduce response times.

AUTOMATION:

Security workflows can trigger predefined playbooks and API-driven actions, reducing analyst workload and improving consistency.

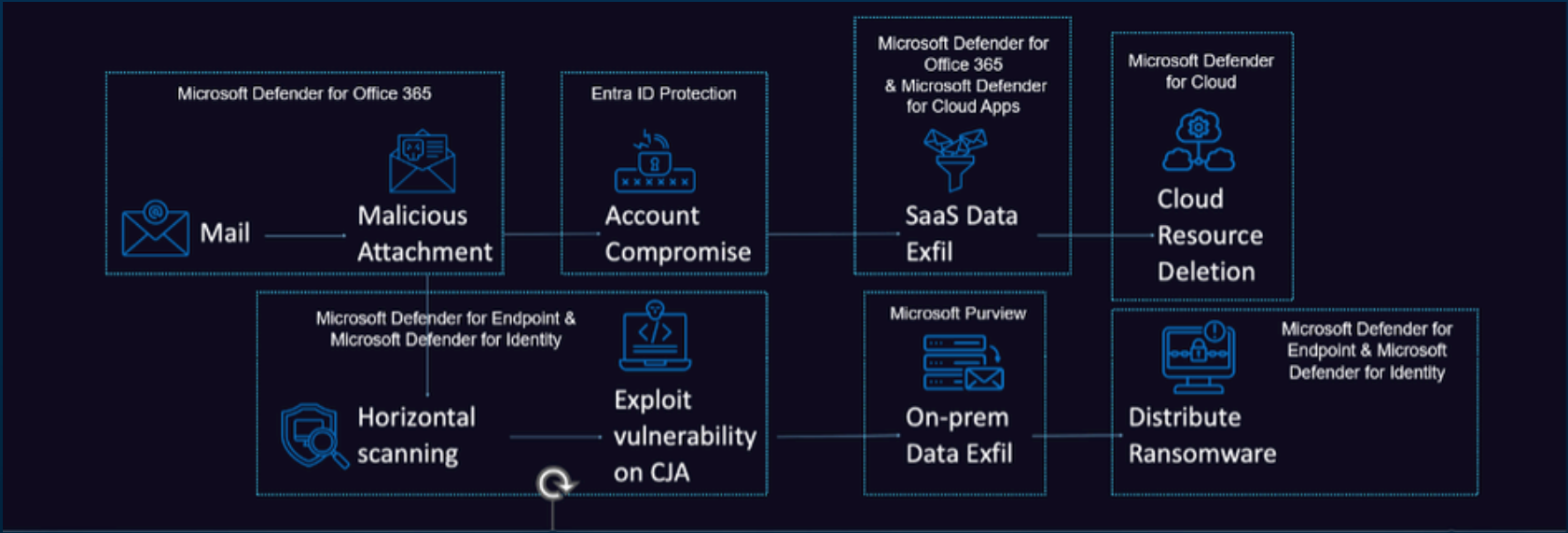


Figure 4 - Attack chain logic

THREAT HUNTING WITHOUT A SIEM

Threat hunting is often cited as a reason for maintaining a SIEM platform. However, modern XDR environments provide robust hunting capabilities.

Microsoft Defender Advanced Hunting allows analysts to perform hypothesis-driven investigations across endpoints, identities, email systems, and cloud workloads. Analysts can search for indicators of compromise, suspicious administrative activity, credential abuse, persistence mechanisms, and attack techniques aligned with the MITRE ATT&CK framework.

The value of threat hunting depends more on telemetry quality and analyst expertise than on the underlying storage platform. When telemetry is sufficiently rich and accessible, effective hunting can occur without a traditional SIEM.

PHISHING INVESTIGATION AND RESPONSE

Phishing remains one of the most common attack vectors. Integrated XDR platforms significantly improve investigation efficiency.

Security teams can analyze email headers, URLs, attachments, user interactions, authentication events, endpoint execution activity, and cloud access patterns from a unified interface. Analysts can determine whether a malicious email resulted in credential compromise, malware execution, or data exposure.

Response actions may include:

- Message removal.
- User notification.
- Account protection measures.
- Session revocation.
- URL blocking.
- Campaign-aware tenant-wide remediation.

These capabilities allow rapid containment without requiring SIEM-based workflows.

VULNERABILITY MANAGEMENT AND EXPOSURE REDUCTION

Modern security operations extend beyond incident response. Effective security teams continuously reduce organizational exposure.

Microsoft Defender XDR Threat and Vulnerability Management provides continuous asset discovery, software inventory, vulnerability identification, risk prioritization, and remediation guidance. Rather than relying solely on periodic vulnerability scans, organizations gain ongoing visibility into exposure levels.

Risk-based prioritization helps security teams focus on vulnerabilities most likely to be exploited. Integration with ticketing and operational processes further supports scalable remediation programs.

LIMITATIONS OF THE MINI SOC MODEL

A SIEM-less SOC is not appropriate for every organization.

Limitations may include:

- Reduced support for highly specialized log sources.
- Limited long-term retention compared with dedicated SIEM deployments.
- Constraints around advanced compliance reporting.
- Less flexibility for highly customized correlation requirements.
- Dependence on vendor-provided analytics and data models.

Organizations should evaluate several factors when deciding whether our Mini SOC approach is appropriate.

A Mini SOC is often suitable when:

- The environment is predominantly Microsoft-based.
- Security teams are small.
- Operational efficiency is a priority.
- Compliance requirements are moderate.
- Long-term log retention is not the primary driver.

A traditional SIEM remains appropriate when:

- Regulatory requirements mandate extended retention.
- Multiple non-native technologies must be integrated
- Advanced custom analytics are required.
- Large-scale enterprise monitoring is necessary
- Data sovereignty constraints exist.

Organizations operating in critical infrastructure, highly regulated environments, or complex multi-vendor ecosystems may still require a SIEM for governance, compliance, and specialized monitoring needs.

CONCLUSION

The rise of XDR represents a significant shift in security operations. Many capabilities once associated exclusively with SIEM platforms are now delivered directly through integrated security ecosystems. For organizations operating primarily within the Microsoft ecosystem, Defender XDR can provide sufficient visibility, detection, investigation, response, threat hunting, and vulnerability management capabilities to support an effective Mini SOC.

This does not mean SIEM platforms are obsolete. Rather, their role has become more specialized. The most successful organizations will align their security architecture with operational requirements, regulatory obligations, and risk tolerance.

For many small and medium-sized enterprises, the Mini SOC model provides a pragmatic path toward mature security operations without the complexity and cost traditionally associated with SIEM deployments. By focusing on visibility, high-quality detections, rapid response, and automation, organizations can achieve meaningful security outcomes while maintaining operational simplicity.