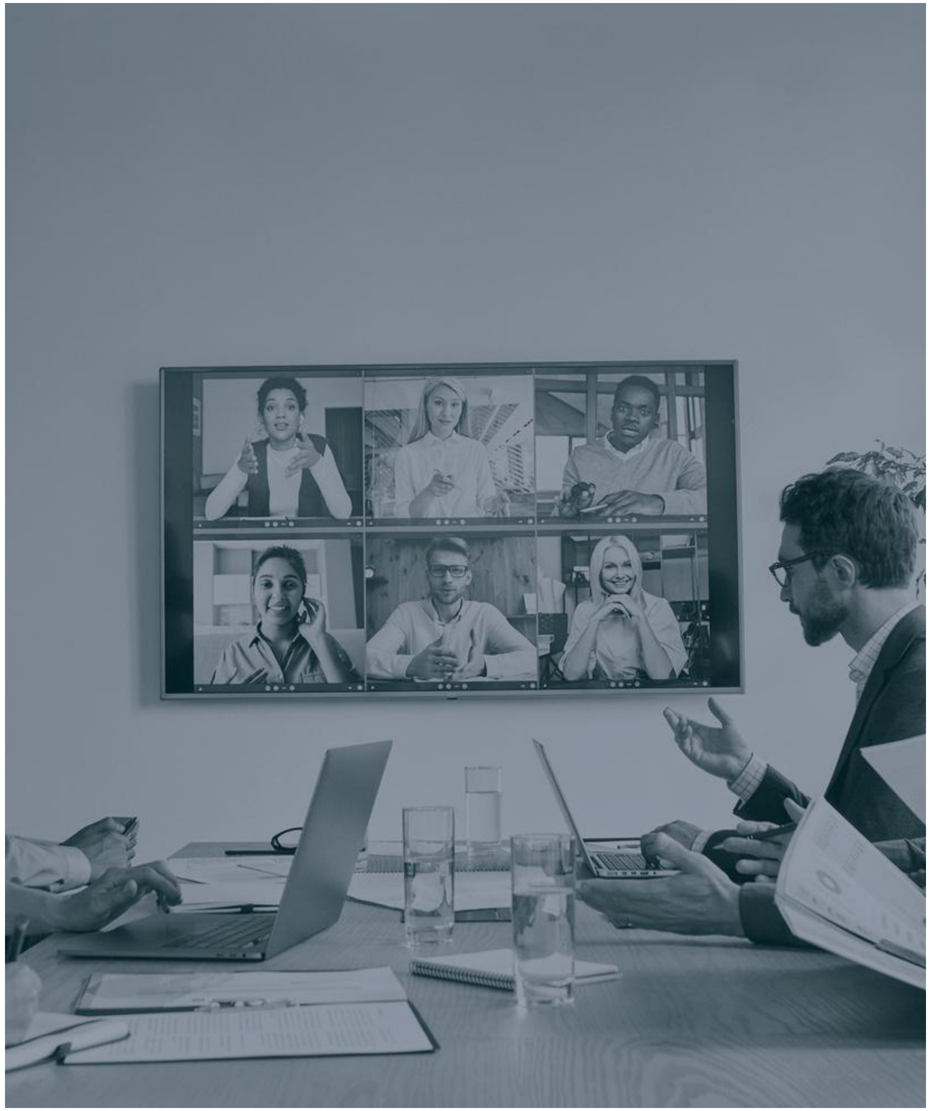
eGroup | ENABLING TECHNOLOGIES
together we make IT happen

Microsoft

Trends and Defenses Against Ransomware

Understanding ransomware threats and your response



Your Commentators

David Branscome

Global Partner Solutions - Security Architect

Microsoft

Micah Linehan

Field CTO, Security

eGroup | ENABLING TECHNOLOGIES

Chris Stegh

CTO
Microsoft MVP

eGroup | ENABLING TECHNOLOGIES

Agenda Items

- Recent Ransomware Headlines and TTPs
- Microsoft's 2024 Digital Defense Report
- NIST CSF Basics and Microsoft Tools
- MITRE Integration in Microsoft Threat Intelligence
- Final Thoughts for Enterprise Defenders

Recent Headlines and TTPs

Medusa – Turning Your Files into Stone

- **Targeted Attacks -** Medusa ransomware is known for its selective and strategic targeting of specific organizations and individuals.

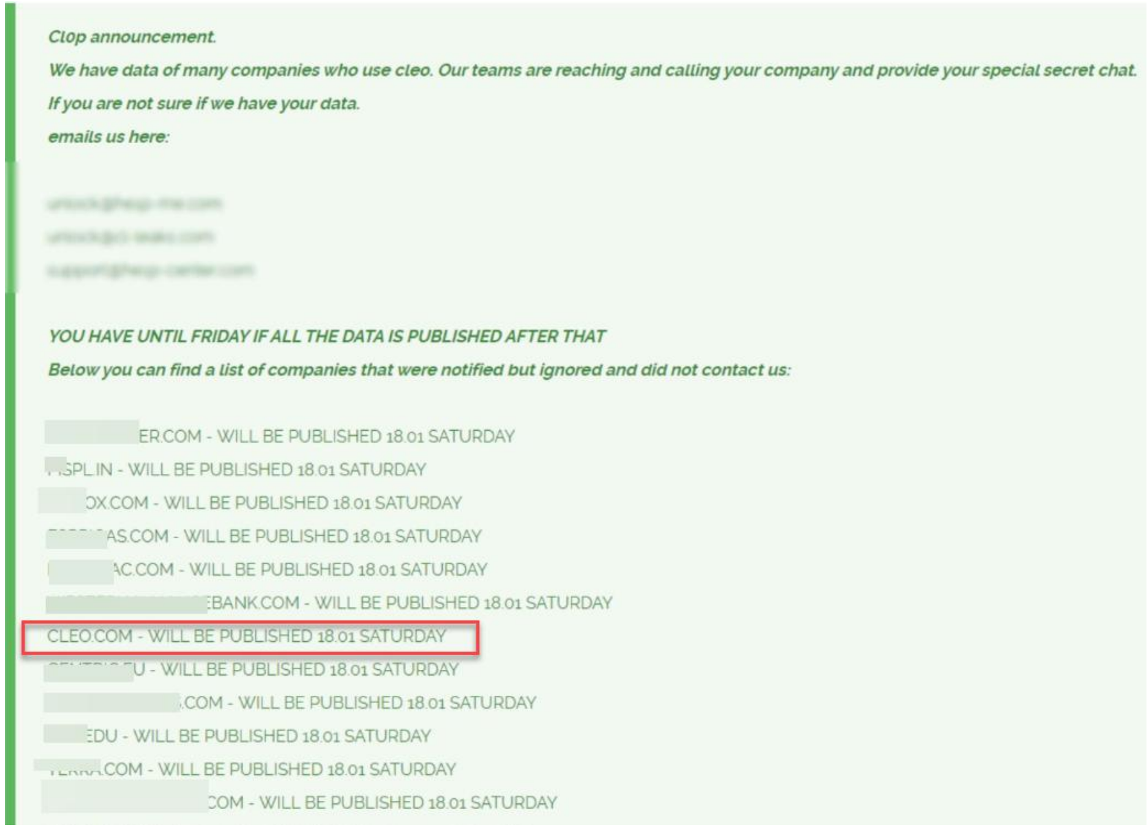
- **Advanced Tactics -** The ransomware employs sophisticated techniques and tools to infiltrate systems and encrypt files, making it a formidable threat.

- **Complex Encryption** - Medusa utilizes advanced encryption algorithms to lock victim's files, making it difficult to recover data without paying the ransom.

- **Evolving Tactics** - The Medusa operators continuously update their methods to adapt to new security measures and bypass defenses.

COLONIAL PIPELINE CO.	UNIVERSAL HEALTH SERVICES	BCP
JBS	Kaseya	medibank

Asked to MoveIT elsewhere, Cl0p clips Cleo



Clop announcement.

We have data of many companies who use cleo. Our teams are reaching and calling your company and provide your special secret chat.

If you are not sure if we have your data.

emails us here:

[redacted]

YOU HAVE UNTIL FRIDAY IF ALL THE DATA IS PUBLISHED AFTER THAT

Below you can find a list of companies that were notified but ignored and did not contact us:

[redacted]ER.COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]SPL.IN - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]OX.COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]AS.COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]AC.COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]EBANK.COM - WILL BE PUBLISHED 18.01 SATURDAY
CLEO.COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]U - WILL BE PUBLISHED 18.01 SATURDAY
[redacted].COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]EDU - WILL BE PUBLISHED 18.01 SATURDAY
[redacted].COM - WILL BE PUBLISHED 18.01 SATURDAY
[redacted]COM - WILL BE PUBLISHED 18.01 SATURDAY

- **Cl0p is a Russian-speaking cybercriminal gang**
- Known for **large-scale ransomware and extortion campaigns**
- In 2023, C10p compromised **MoveIT file transfer** service
- In 2025, C10p exploited **CVE-2024-50623**, in Cleo file sharing and transfer service (*are you detecting a theme?*)
- Attack on Cleo **compromised data on 60+ organizations**

Chart: CLOP Ransomware : Latest Attacks - CYFIRMA
#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability | CISA

24x7 MXDR for Manufacturer

eGroup | ENABLING TECHNOLOGIES | Microsoft

- **Industry:** Food products
- **Challenge:** FDA compliance and securing critical IT infrastructure at multiple plants each with $1M daily business

Technical Solution: Microsoft E5 Defender Suite, Sentinel

Services: ThreatDefender (Managed Security Services)

Path To Success

- Steady migration to M365 E5 security
- Setup of Defender Suite and Sentinel

Breach Thwarted:

1. Our team detected high-severity events tied to **a known ransomware group** using automated monitoring systems.
2. A **compromised shared account with additional privileges** was executing unauthorized actions.
3. **Our team swiftly contained the threat** by disabling compromised accounts, shutting down the Remote Desktop Web Server, and enhancing monitoring.
4. **Collaboration with the client's Forensic Incident Response Team** ensured thorough investigation containment.
5. The attack was **stopped before any data encryption occurred.**

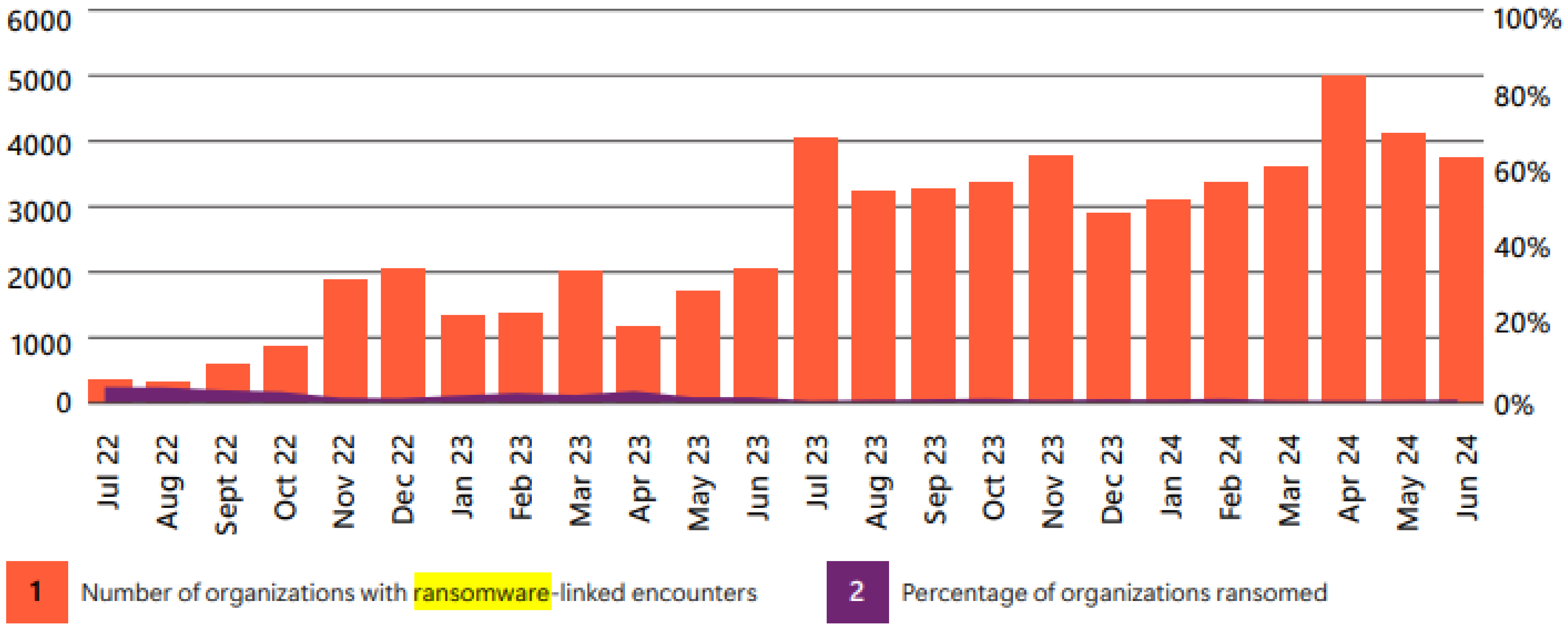
Results:

Ongoing Improvements
To Security Posture

Smooth Operation Of
$3M / Day Business

Rapid Response
To Avert Breach(es)

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022–June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the past two years.

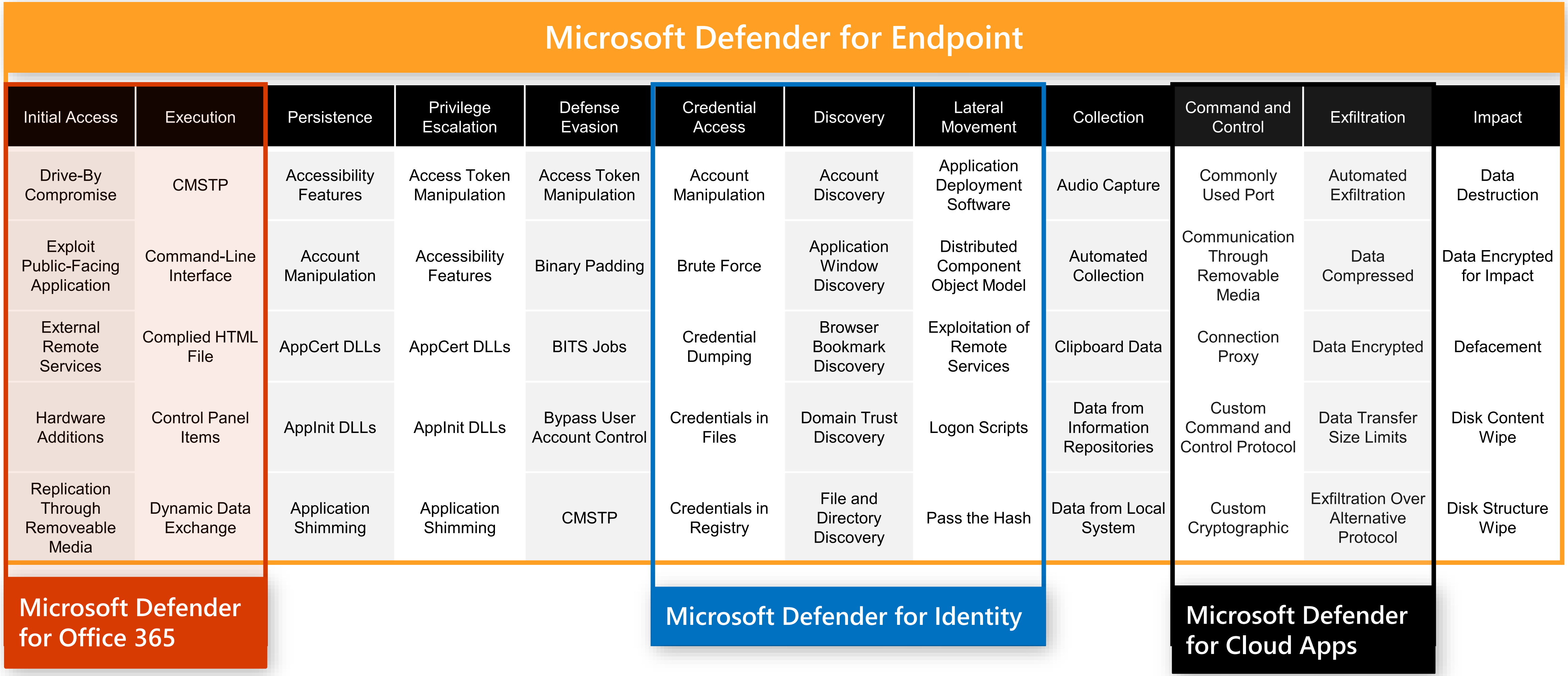
Source: Microsoft Defender for Endpoint

Microsoft's 2024 Digital Defense Report

Overview of Microsoft’s Digital Defense Report

- People are still too predictable
- AI is a double-edged sword
- Must address technical debt and outdated security controls

MITRE and Microsoft Defender Products



Microsoft Defender for Endpoint

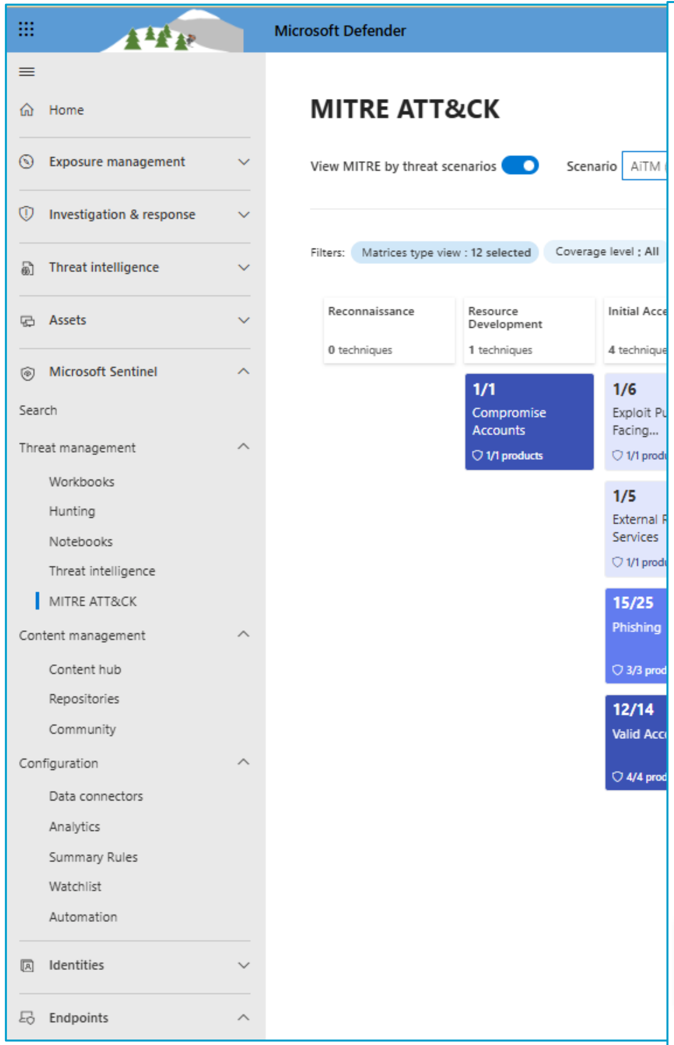
Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Drive-By Compromise	CMSTP	Accessibility Features	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	Application Deployment Software	Audio Capture	Commonly Used Port	Automated Exfiltration	Data Destruction
Exploit Public-Facing Application	Command-Line Interface	Account Manipulation	Accessibility Features	Binary Padding	Brute Force	Application Window Discovery	Distributed Component Object Model	Automated Collection	Communication Through Removable Media	Data Compressed	Data Encrypted for Impact
External Remote Services	Complied HTML File	AppCert DLLs	AppCert DLLs	BITS Jobs	Credential Dumping	Browser Bookmark Discovery	Exploitation of Remote Services	Clipboard Data	Connection Proxy	Data Encrypted	Defacement
Hardware Additions	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credentials in Files	Domain Trust Discovery	Logon Scripts	Data from Information Repositories	Custom Command and Control Protocol	Data Transfer Size Limits	Disk Content Wipe
Replication Through Removeable Media	Dynamic Data Exchange	Application Shimming	Application Shimming	CMSTP	Credentials in Registry	File and Directory Discovery	Pass the Hash	Data from Local System	Custom Cryptographic	Exfiltration Over Alternative Protocol	Disk Structure Wipe

Microsoft Defender for Office 365

Microsoft Defender for Identity

Microsoft Defender for Cloud Apps

Where ATT&CK TTP's are referenced



MITRE ATT&CK

View MITRE by threat scenarios ● Scenario AiTM

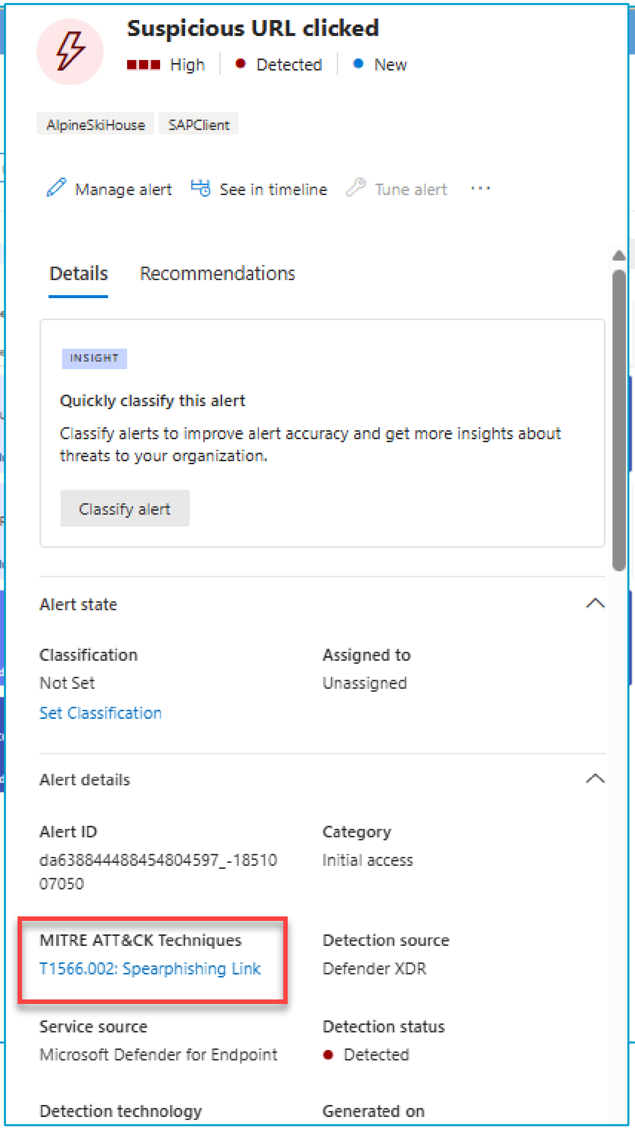
Filters: Matrices type view : 12 selected Coverage level : All

Reconnaissance 0 techniques

Resource Development 1 techniques
- 1/1 Compromise Accounts 1/1 products

Initial Acce 4 technique
- 1/6 Exploit Pu Facing... 1/1 prod
- 1/5 External R Services 1/1 prod
- 15/25 Phishing 3/3 prod
- 12/14 Valid Acc 4/4 prod

Credentia 5 techniqu
- 4/5 Adversa the-Mid 3/3 pr
- 1/2 Brute Fo 2/2 pr
- 0/1 Multi-Fa Authent 1/1 pro
- 2/2 Steal We Session 1/1 pro
- 0/2 Steal Ap Access T 1/1 pro



Suspicious URL clicked

High | ● Detected | ● New

AlpineSkiHouse SAPClient

INSIGHT

Quickly classify this alert

Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Classify alert

Alert state

Classification: Not Set

Assigned to: Unassigned

Set Classification

Alert details

Alert ID: da638844488454804597_-1851007050

Category: Initial access

MITRE ATT&CK Techniques: T1566.002: Spearphishing Link

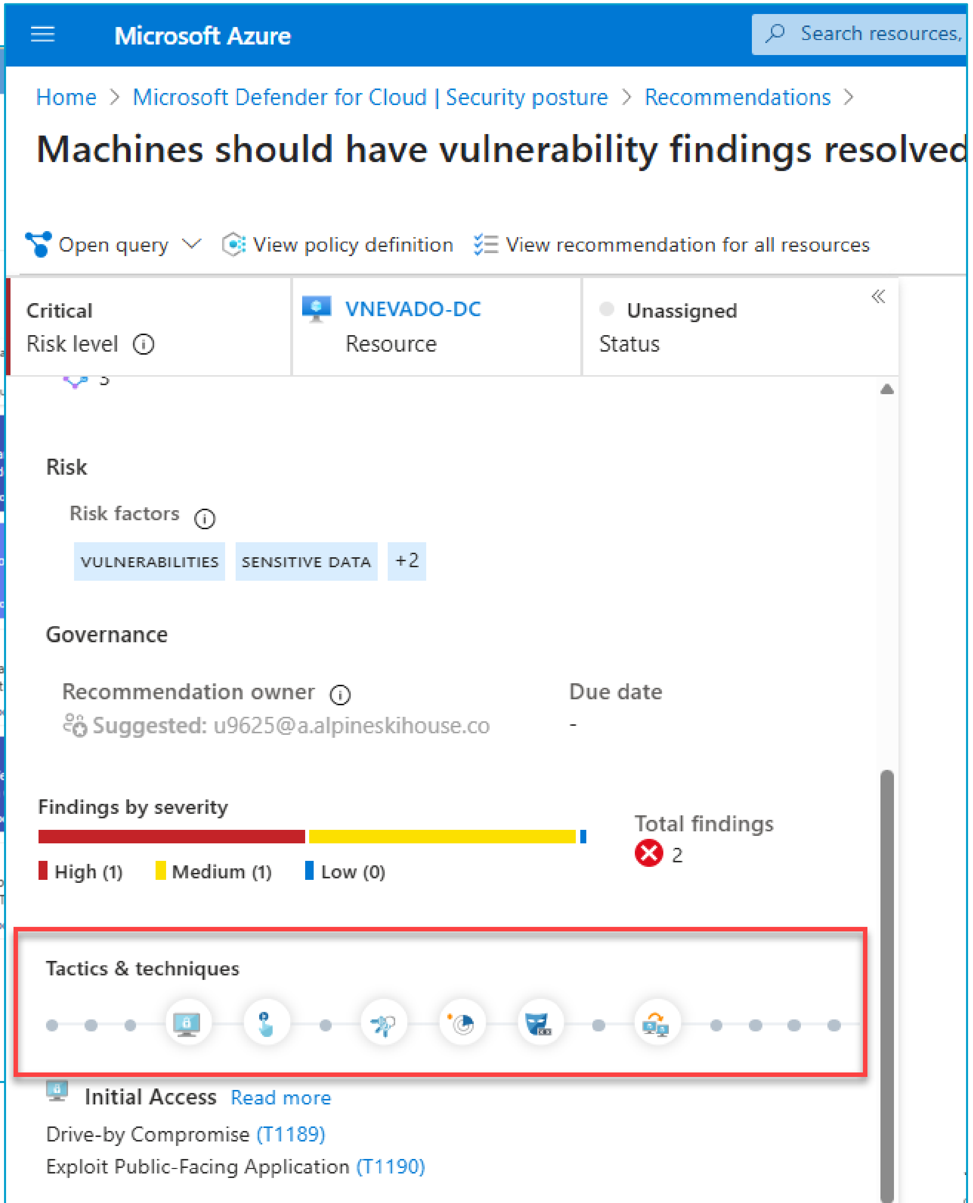
Detection source: Defender XDR

Service source: Microsoft Defender for Endpoint

Detection status: ● Detected

Detection technology

Generated on



Home > Microsoft Defender for Cloud | Security posture > Recommendations >

Machines should have vulnerability findings resolved

Critical — Risk level

VNEVADO-DC — Resource

Unassigned — Status

Risk

Risk factors: VULNERABILITIES SENSITIVE DATA +2

Governance

Recommendation owner: Suggested: u9625@a.alpineskihouse.co

Due date: -

Findings by severity: High (1) Medium (1) Low (0)

Total findings: 2

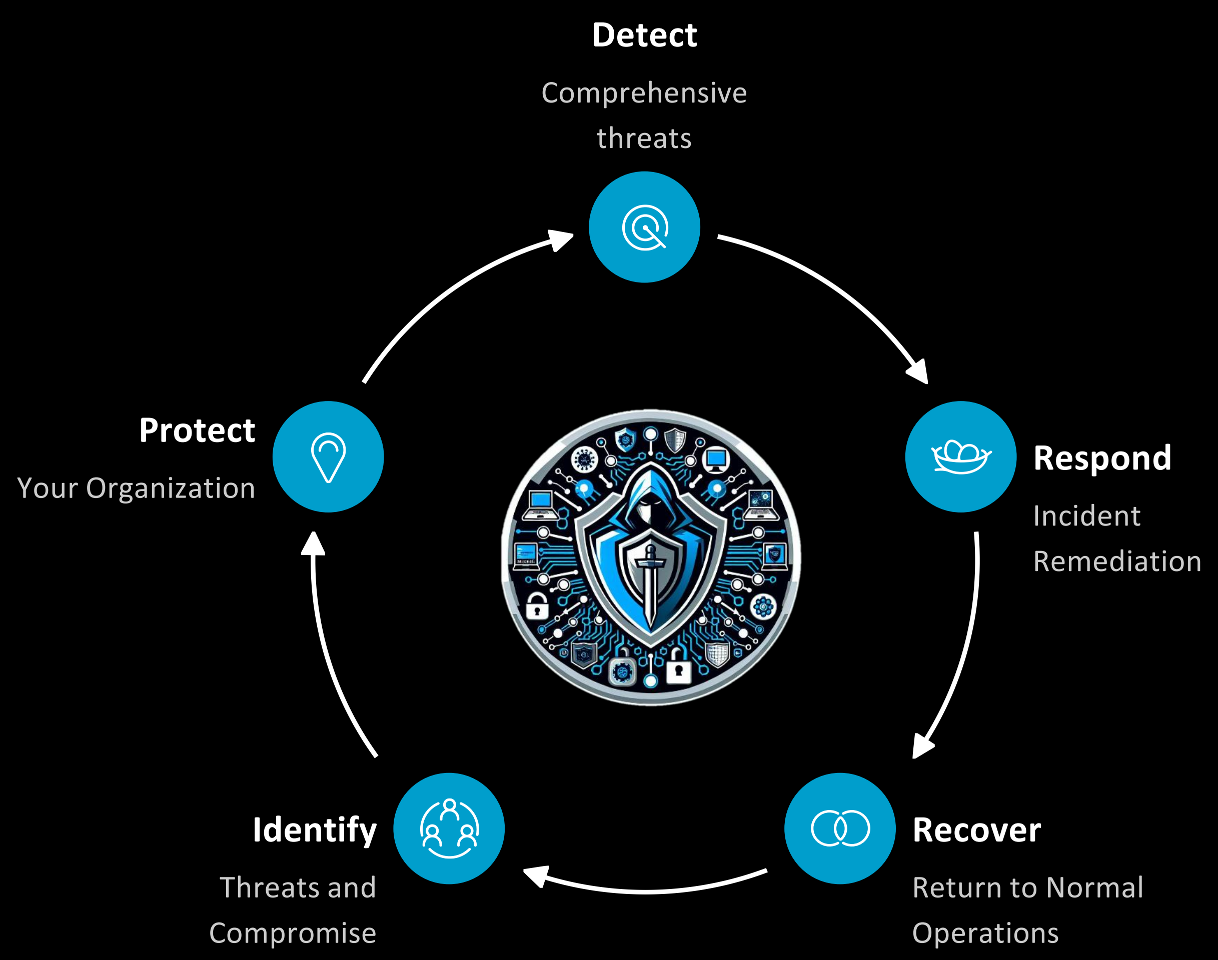
Tactics & techniques

Initial Access Read more

Drive-by Compromise (T1189)

Exploit Public-Facing Application (T1190)

MITRE ATT&CK with ThreatDefender MXDR



Detect

Comprehensive threats

Respond

Incident Remediation

Recover

Return to Normal Operations

Identify

Threats and Compromise

Protect

Your Organization

24x7 MXDR for Carolina Eastern

eGroup | ENABLING TECHNOLOGIES | Microsoft

- **Line of Business:** $600M ag-business with over 40 locations and 500 employees
- **Challenge:** ***"We were always in a reactive state with our security. Our outlook was 'We are not trying to get hacked.' We thought we were doing fine, but we didn't know. We were hacked, and it was a lot of pain." -CFO***

Breach Background:

1. Prior to eGroup Enabling Technologies' involvement, client was hacked.

Technical Solution: Microsoft E5 Defender Suite, Sentinel

Services: ThreatDefender and IT Managed Services

Path To Success

- Post-breach, we rapidly deployed the Microsoft Defender Suite and Sentinel

Results:

"I feel a lot more secure. I know every company's going to get hacked. Just being able to react is key."

-CFO Tom Hallex

NIST CSF and Microsoft Tools

What is the NIST Cybersecurity Framework?

A voluntary, risk-based set of guidelines, standards, and best practices to manage cybersecurity risk for critical infrastructure organizations.

Purpose of the NIST CSF

Helps organizations manage and reduce cybersecurity risk through a flexible, repeatable, and cost-effective approach.

Five Core Functions

The NIST CSF consists of five core functions: Identify, Protect, Detect, Respond, and Recover.

Adoption and Implementation

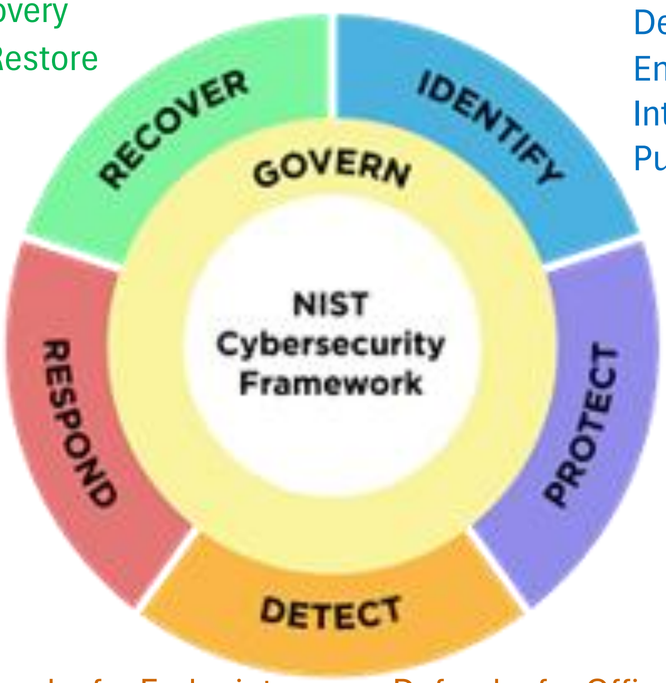
The NIST CSF can be customized and implemented by organizations of all sizes and industries to address their unique cybersecurity needs.

The NIST Cybersecurity Framework provides a comprehensive and flexible approach to managing cybersecurity risk, helping organizations of all sizes and industries strengthen their security posture and enhance their overall resilience.

NIST Cybersecurity Framework

Microsoft Security

Purview Compliance Manager
Microsoft Secure Score
Defender for Cloud
Sentinel



Defender for Endpoint
Defender for Servers
Defender for Cloud Apps
Entra ID
Intune
Purview Information Protection

Defender for Endpoint
Defender for Office 365
Defender for Cloud Apps
Defender Vulnerability Management
Defender for Cloud
Defender for Servers
Entra ID
Intune

Defender for Endpoint
Defender for Identity
Defender Threat Intelligence
Entra ID

Purview

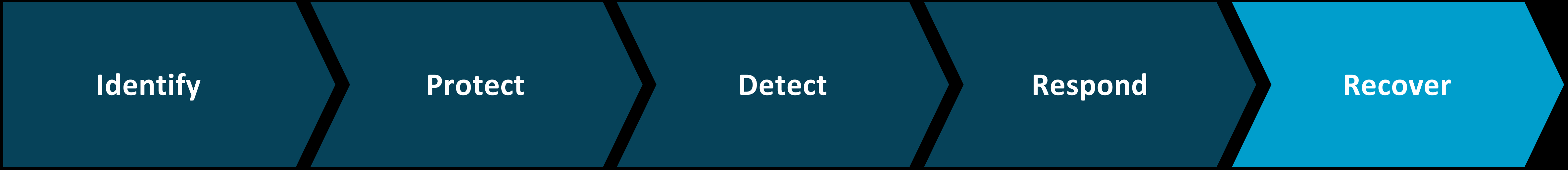
Defender for Office 365
Defender for Cloud Apps
Defender for Storage
Sentinel

Defender for Endpoint
Defender for Identity
Defender for Cloud Apps
Defender for Office 365
Entra ID
Purview
Sentinel

Azure Backup
Azure Site Recovery
OneDrive File Restore
Intune

eGroup | ENABLING TECHNOLOGIES
together we make IT happen

NIST CSF Core Functions



Identify

Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect

Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect

Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

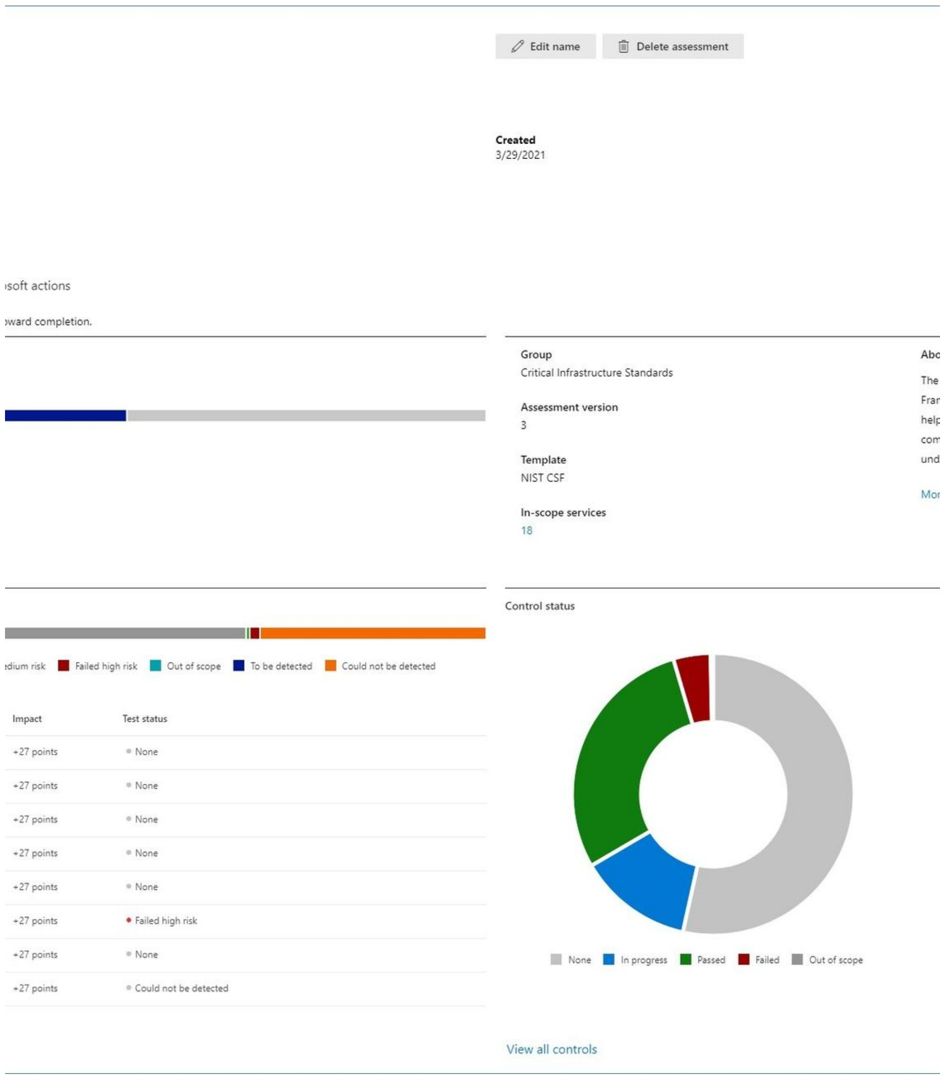
Respond

Develop and implement the appropriate activities to take action regarding a detected cybersecurity incident.

Recover

Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Leveraging Microsoft for NIST CSF



Created
3/29/2021

Group
Critical Infrastructure Standards

Assessment version
3

Template
NIST CSF

In-scope services
18

Impact	Test status
+27 points	● None
+27 points	● None
+27 points	● None
+27 points	● None
+27 points	● None
+27 points	● Failed high risk
+27 points	● None
+27 points	● Could not be detected

- **Comprehensive Security Coverage**

  The Microsoft Defender Suite provides a unified platform that addresses multiple aspects of cybersecurity, including endpoint protection, threat detection, and response, aligning with the various NIST CSF categories.

- **Streamlined NIST CSF Implementation**

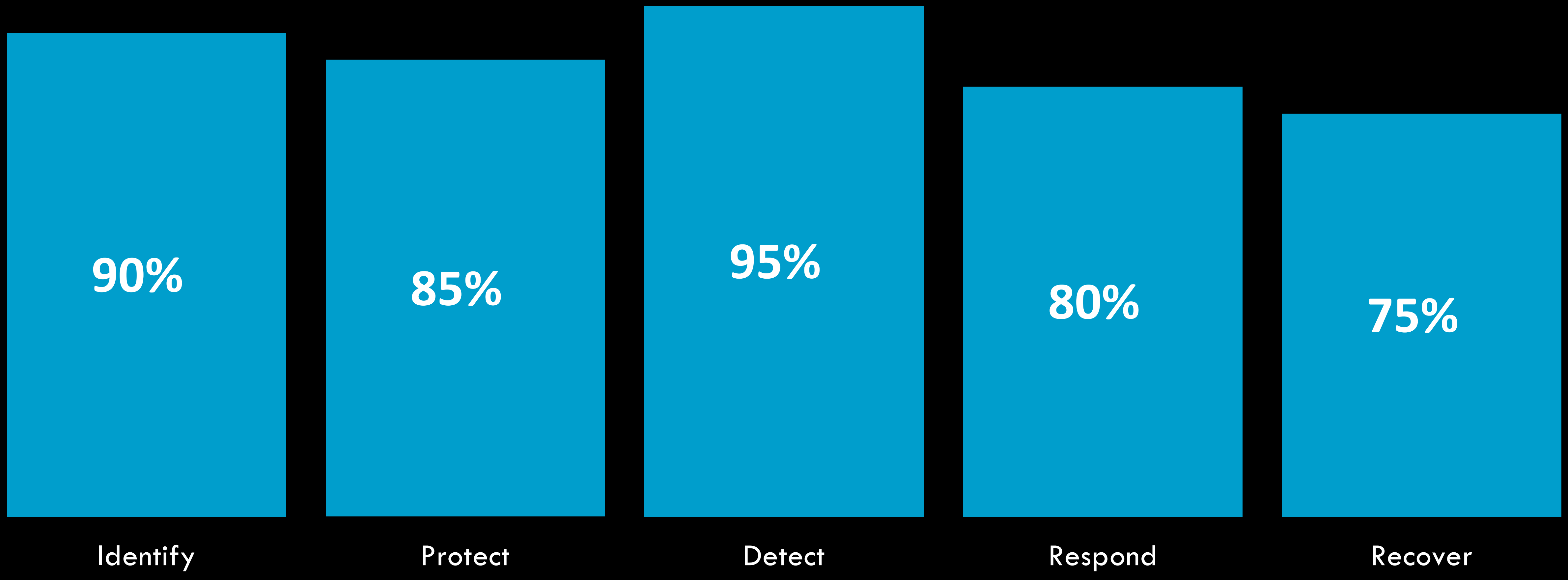
  The integration of the Microsoft Defender Suite tools with the NIST CSF categories enables organizations to efficiently implement the framework, leveraging the suite's capabilities to address the required security controls.

- **Improved Visibility & Threat Detection**

  The Microsoft Defender Suite's advanced threat detection and analytics capabilities provide organizations with enhanced visibility into their security posture, enabling them to quickly identify and respond to potential threats.

Aligning Microsoft Defender Suite to NIST CSF

Percentage of NIST CSF categories covered by Microsoft Defender Suite tools



24x7 MXDR for Charleston Stevedoring

eGroup | ENABLING TECHNOLOGIES | Microsoft

- **Industry:** Shipping / Receiving Port
- **Challenge:** Limited IT control, bottlenecks in operations, and weak security measures.

Technical Solution: Microsoft E5 Defender Suite, Sentinel

Services: ThreatDefender (Managed Security Services)

Path To Success

- New tenant
- Data center → Azure migration
- Setup of Defender Suite and Sentinel

Breach Thwarted:

1. A high-level manager was phished.
2. IT Manager sits just 30 feet away from them
3. eGroup's team alerted IT Manager first.
4. **"It was an adversary in the middle attack," Kevin recalled. "It could have been bad, but eGroup blocked their device and isolated the account before they were even able to tell me."**
5. By acting quickly, no exfiltration nor further phishing attacks occurred.

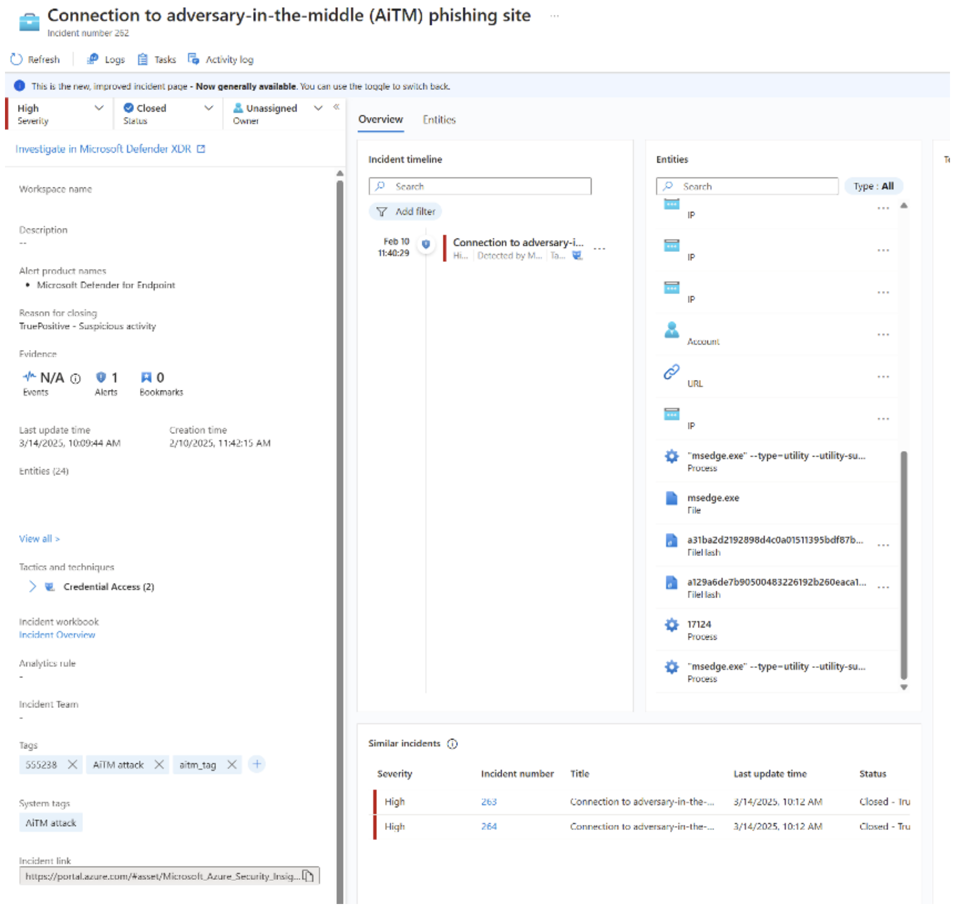
Results:

Fast response times

Ongoing improvements

Visibility into anomalies

AiTM Detected by Defender XDR



Connection to adversary-in-the-middle (AiTM) phishing site

Incident number 262

This is the new, improved incident page - **Now generally available**. You can use the toggle to switch back.

High
Severity

Closed
Status

Unassigned
Owner

Workspace name

Description
--

Alert product names
- Microsoft Defender for Endpoint

Reason for closing
TruePositive - Suspicious activity

Evidence

N/A Events | 1 Alerts | 0 Bookmarks

Last update time
3/14/2025, 10:09:44 AM

Creation time
2/10/2025, 11:42:15 AM

Entities (24)

Tactics and techniques
Credential Access (2)

Incident workbook
Incident Overview

Analytics rule
-

Incident Team
-

Tags
555238 | AiTM attack | aitm_tag

System tags
AiTM attack

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insig...

Incident timeline

Feb 10 11:40:29 Connection to adversary-i... Hi... | Detected by M... | Ta...

Entities

IP
IP
IP
Account
URL
IP
"msedge.exe" --type=utility --utility-su... Process
msedge.exe File
a31ba2d2192898d4c0a01511395bdf87b... FileHash
a129a6de7b90500483226192b260eaca1... FileHash
17124 Process
"msedge.exe" --type=utility --utility-su... Process

Similar incidents

Severity	Incident number	Title	Last update time	Status
High	263	Connection to adversary-in-the-...	3/14/2025, 10:12 AM	Closed - Tru
High	264	Connection to adversary-in-the-...	3/14/2025, 10:12 AM	Closed - Tru

How They Do It

- **Attack-in-The-Middle -** The attacker positions themselves in the middle of the communication path between the legitimate parties, intercepting and manipulating the data exchange.
- **Active Manipulation -** The attacker can actively modify the communication, altering the content, redirecting traffic, or even impersonating one of the legitimate parties.

How it is Visualized

- **Indicators of Compromise -** The system identifies key indicators of compromise (IOCs) such as malicious URLs and IP addresses that pose security threats.
- **Intelligence Delivery -** The intelligence gathered is delivered in a format that security teams can easily understand and act upon to enhance security measures.

24x7 MXDR for Becket & Lee

eGroup | ENABLING TECHNOLOGIES | Microsoft

- **Industry:** Legal (Bankruptcy Servicing)
- **Challenge:** One Security Pro, Securing sensitive data and compliance requirements from clients

Technical Solution: Microsoft E5 Defender Suite, Sentinel

Services: ThreatDefender (Managed Security Services)

Breach Thwarted:

- Misconfigured work-from-home device (firewall inactive), allowing an RDP spray attack
- ThreatDefender alerted and prevented potential breach
- “That’s a true ‘save your bacon’ incident. Who knows what would have happened before we were going down this MSSP path?”

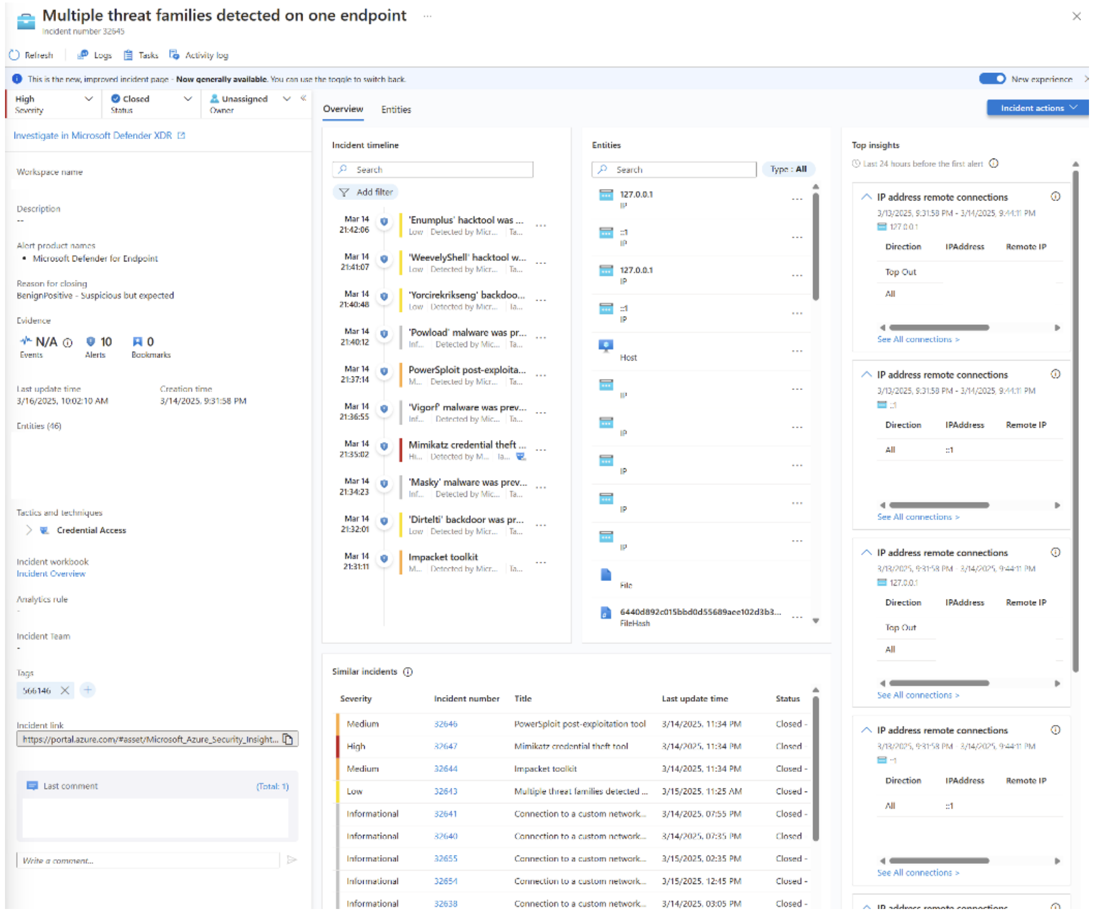
Results:

- Improved security posture
- Faster incident detection and response
- Compliance with client requirements
- Averted breach(es)

Path To Success

- Onboarding workshop
- Integration with existing Microsoft 365 E5 licenses
- Setup of Defender Suite and Sentinel

Multiple Threat Scenario that used RDP Spray Attack



Multiple threat families detected on one endpoint
Incident number 32645

This is the new, improved incident page - **Now generally available.** You can use the toggle to switch back.

High Severity | Closed Status | Unassigned Owner

Investigate in Microsoft Defender XDR

Workspace name

Description
--

Alert product names
- Microsoft Defender for Endpoint

Reason for closing
BenignPositive - Suspicious but expected

Evidence
N/A Events | 10 Alerts | 0 Bookmarks

Last update time
3/16/2025, 10:02:10 AM

Creation time
3/14/2025, 9:31:58 PM

Entities (46)

Tactics and techniques
Credential Access

Incident workbook
Incident Overview

Analytics rule
-

Incident Team
-

Tags
566146

Incident link
https://portal.azure.com/#asset/Microsoft_Azure_Security_Insight...

Last comment (Total: 1)

Incident timeline

Mar 14 21:42:06	'Enumplus' hacktool was ... Low | Detected by Micr... | Ta...
Mar 14 21:41:07	'WeevelyShell' hacktool w... Low | Detected by Micr... | Ta...
Mar 14 21:40:48	'Yorcirekrikseng' backdoo... Low | Detected by Micr... | Ta...
Mar 14 21:40:12	'Powload' malware was pr... Inf... | Detected by Mic... | Ta...
Mar 14 21:37:14	PowerSploit post-exploita... M... | Detected by Micr... | Ta...
Mar 14 21:36:55	'Vigorf' malware was prev... Inf... | Detected by Mic... | Ta...
Mar 14 21:35:02	Mimikatz credential theft ... Hi... | Detected by M... | Ta...
Mar 14 21:34:23	'Masky' malware was prev... Inf... | Detected by Mic... | Ta...
Mar 14 21:32:01	'Dirtelti' backdoor was pr... Low | Detected by Micr... | Ta...
Mar 14 21:31:11	Impacket toolkit M... | Detected by Micr... | Ta...

Entities

- 127.0.0.1 IP
- ::1 IP
- 127.0.0.1 IP
- ::1 IP
- Host
- IP
- IP
- IP
- IP
- IP
- File
- 6440d892c015bbd0d55689aee102d3b3... FileHash

Top insights
Last 24 hours before the first alert

IP address remote connections
3/13/2025, 9:31:58 PM - 3/14/2025, 9:44:11 PM
127.0.0.1

Direction	IPAddress	Remote IP
Top Out		
All		

IP address remote connections
3/13/2025, 9:31:58 PM - 3/14/2025, 9:44:11 PM
::1

Direction	IPAddress	Remote IP
All	::1	

IP address remote connections
3/13/2025, 9:31:58 PM - 3/14/2025, 9:44:11 PM
127.0.0.1

Direction	IPAddress	Remote IP
Top Out		
All		

IP address remote connections
3/13/2025, 9:31:58 PM - 3/14/2025, 9:44:11 PM
::1

Direction	IPAddress	Remote IP
All	::1	

IP address remote connections

Similar incidents

Severity	Incident number	Title	Last update time	Status
Medium	32646	PowerSploit post-exploitation tool	3/14/2025, 11:34 PM	Closed -
High	32647	Mimikatz credential theft tool	3/14/2025, 11:34 PM	Closed
Medium	32644	Impacket toolkit	3/14/2025, 11:34 PM	Closed -
Low	32643	Multiple threat families detected ...	3/15/2025, 11:25 AM	Closed -
Informational	32641	Connection to a custom network...	3/14/2025, 07:55 PM	Closed -
Informational	32640	Connection to a custom network...	3/14/2025, 07:35 PM	Closed
Informational	32655	Connection to a custom network...	3/15/2025, 02:35 PM	Closed -
Informational	32654	Connection to a custom network...	3/15/2025, 12:45 PM	Closed -
Informational	32638	Connection to a custom network...	3/14/2025, 03:05 PM	Closed -

- **RDP Exploitation -** The RDP Spray Attack leverages the Remote Desktop Protocol (RDP) to gain unauthorized access to multiple systems by attempting to guess weak or commonly used credentials.

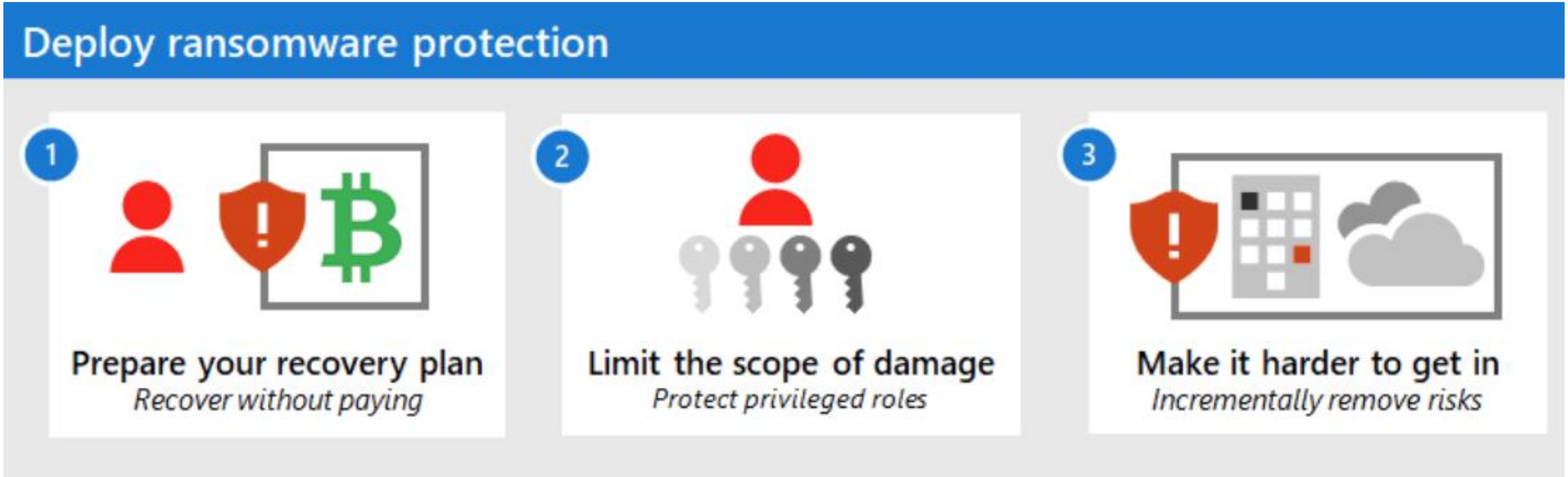
- **Leaked Credentials -** The attacker uses a list of common or previously leaked credentials to systematically attempt logins across a range of target systems that have RDP enabled.

- **Lateral Movement -** Once the attacker gains access to a system through a successful RDP login, they can then move laterally across the network, compromising additional systems and resources.

- **Data Exfiltration -** The attacker can then leverage the RDP access to steal sensitive data, deploy malware, or carry out further malicious activities within the network.

Next Steps for Enterprise Defenders

Things to do Tomorrow (David)



Deploy ransomware protection

1 Prepare your recovery plan
Recover without paying

2 Limit the scope of damage
Protect privileged roles

3 Make it harder to get in
Incrementally remove risks

Get started quickly configuring ransomware prevention so you can stop ransomware cybercriminals from targeting your organization. | Microsoft Learn

Things to do Tomorrow

Leverage Microsoft Defender's Comprehensive Protection

Utilize the robust security capabilities of Microsoft Defender to shield yourself from a wide range of cyber threats, including malware, phishing, and advanced persistent threats.

Implement NIST CSF Best Practices

Adopt the NIST Cybersecurity Framework (NIST CSF) to establish a holistic, risk-based approach to cybersecurity, ensuring your security measures are aligned with industry standards.

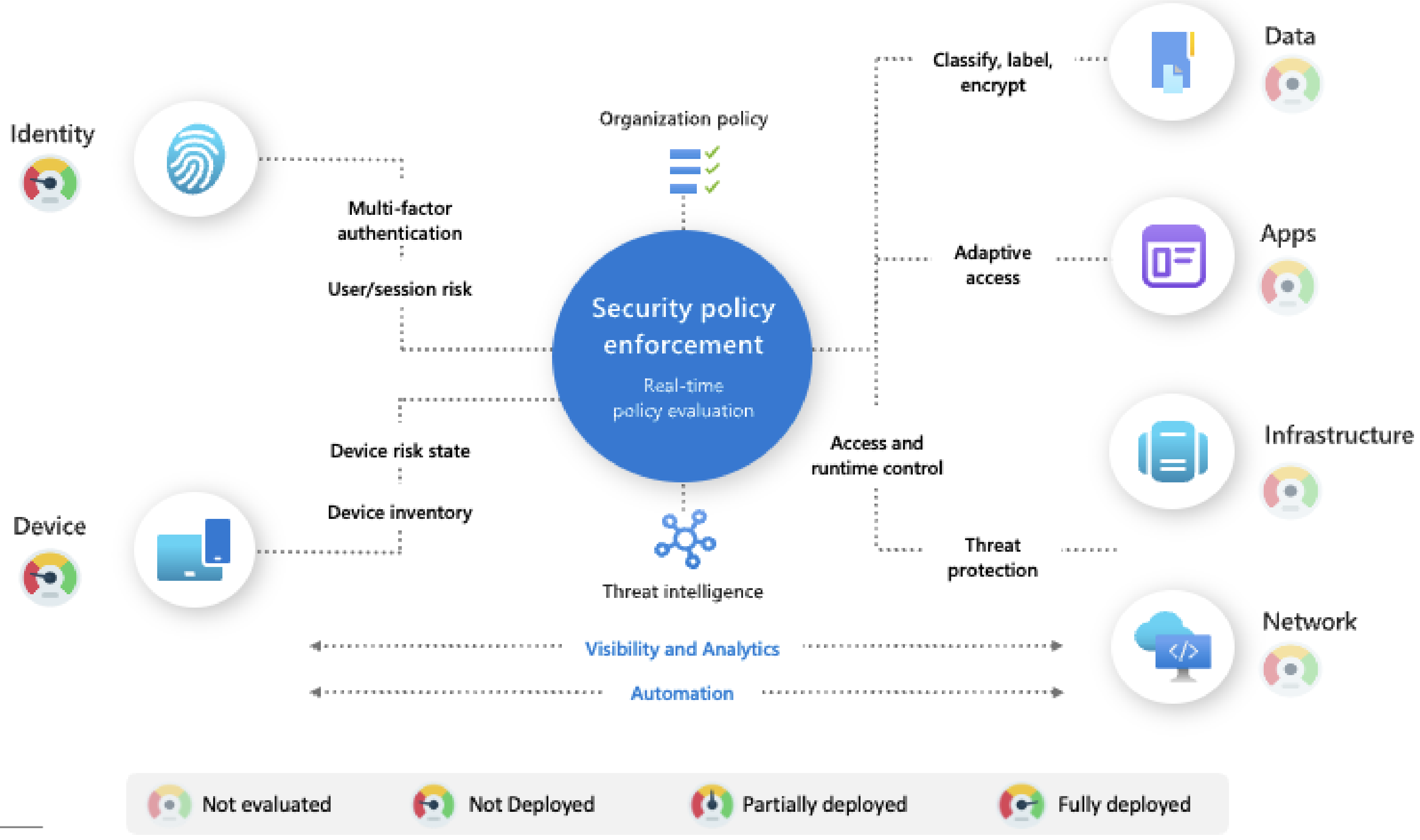
Integrate Microsoft Defender and NIST CSF

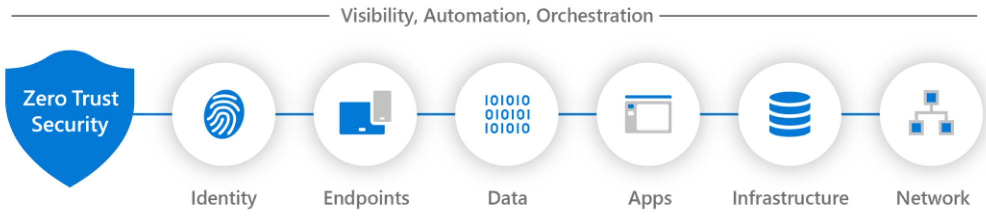
Combine the power of Microsoft Defender's advanced security tools with the guidance of the NIST CSF to create a comprehensive, layered defense against evolving cyber threats.

Protect yourself today by embracing the powerful combination of Microsoft Defender and the NIST Cybersecurity Framework. Secure your digital life and stay ahead of the curve in the ever-evolving landscape of cyber threats.

Zero Trust Assessment

- Pinpoint areas where your organization's security measures may be lacking, enabling targeted improvements.
- Assess current security metrics and receive actionable recommendations for enhancement.
- Create a structured plan that outlines a phased implementation of Zero Trust principles.





“The best way to prepare for a cyberattack is to simulate one.”

MICROSOFT SECURITY TEAM

Microsoft Defender Attack Simulation

Phishing Simulation

Showcasing the Attack Simulator's ability to create and launch realistic phishing campaigns to test employee awareness and response.

Credential Harvesting

Demonstrating how the Attack Simulator can simulate credential theft attacks to uncover vulnerabilities in user authentication processes.

Ransomware Simulation

Illustrating the Attack Simulator's capability to mimic ransomware attacks and assess an organization's readiness to respond and recover.

Insider Threat Scenario

Showcasing the Attack Simulator's ability to simulate insider threats, such as data exfiltration or unauthorized access, to test security controls and user behavior.

24x7 MXDR for Genesis Healthcare

eGroup | ENABLING TECHNOLOGIES | Microsoft

- **Industry:** Regional Healthcare Provider
- **Challenge:** Staff limited IT control, bottlenecks in operations, and weak security measures.

Technical Solution: Microsoft E5 Defender Suite, Sentinel

Services: ThreatDefender (Managed Security Services)

Path To Success

- Transition from old MSP
- SentinelOne → Defender migration
- Setup of Defender Suite and Sentinel

Breach Thwarted:

1. A potentially critical incident involved suspicious activity on a CxO's account.
2. eGroup's quick response averted a potential breach preventing a major disruption to operations.
3. "If that account had been compromised, it would have been a very bad day for everybody involved."
4. By acting quickly, no exfiltration nor further phishing attacks occurred.

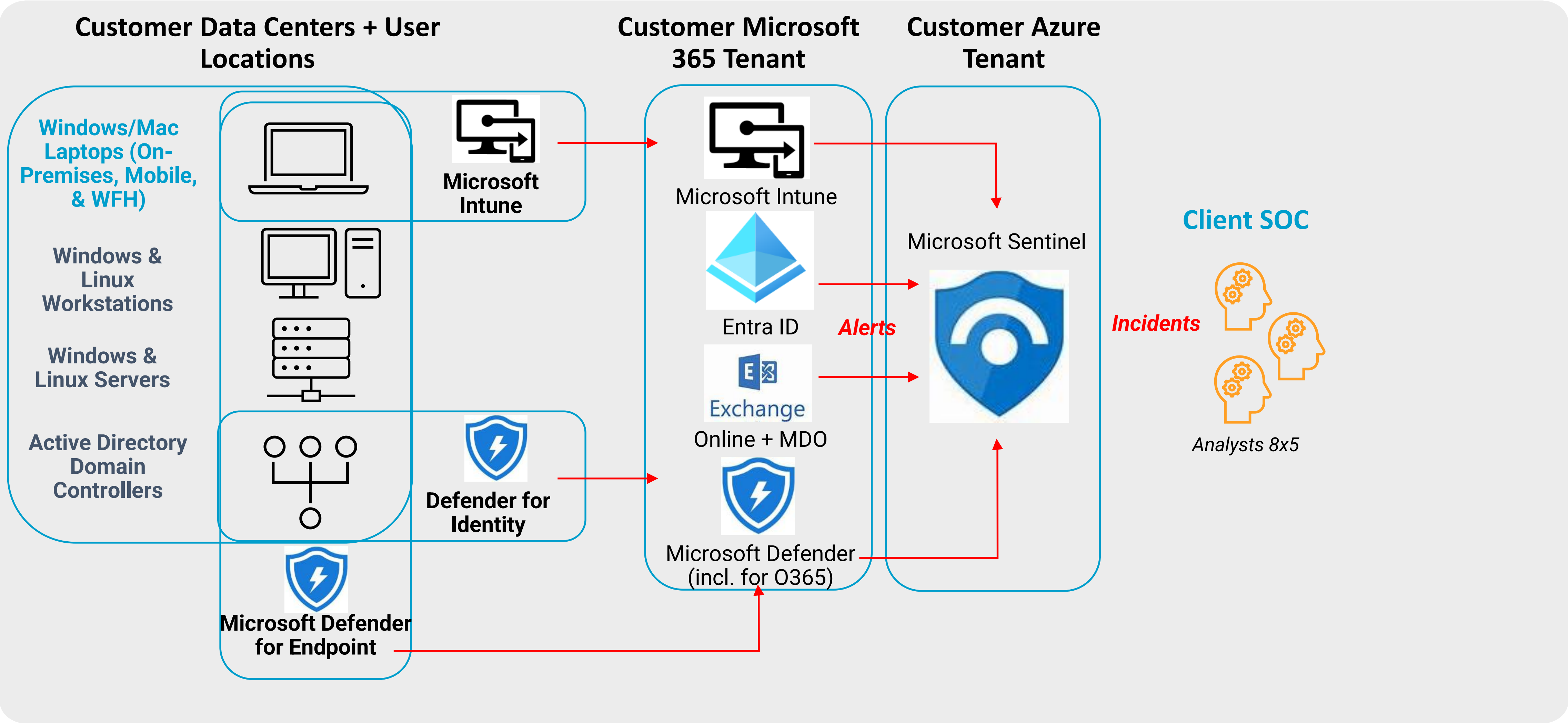
Results:

Fast response times remove threats

Higher Secure and Compliance Scores

Less noise. Actionable insights.

XDR Architecture



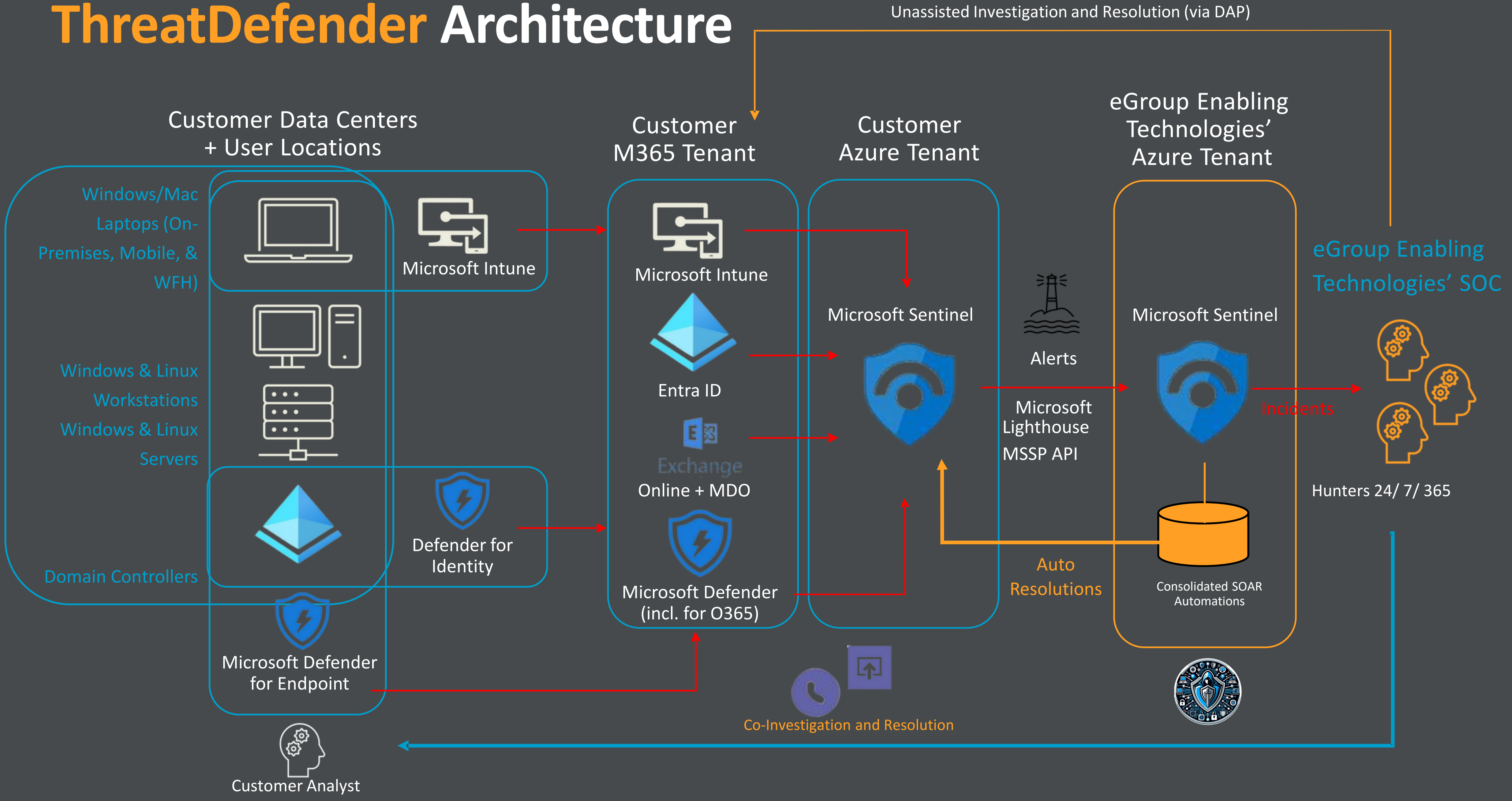
Customer Data Centers + User Locations

Customer Microsoft 365 Tenant

Customer Azure Tenant

Windows/Mac Laptops (On-Premises, Mobile, & WFH)
Windows & Linux Workstations
Windows & Linux Servers
Active Directory Domain Controllers
Microsoft Intune
Defender for Identity
Microsoft Defender for Endpoint
Microsoft Intune
Entra ID
Exchange
Online + MDO
Microsoft Defender (incl. for O365)
Alerts
Microsoft Sentinel
Incidents
Client SOC
Analysts 8x5

ThreatDefender Architecture



Unassisted Investigation and Resolution (via DAP)

Customer Data Centers + User Locations

Windows/Mac Laptops (On-Premises, Mobile, & WFH)

Microsoft Intune

Windows & Linux Workstations

Windows & Linux Servers

Domain Controllers

Defender for Identity

Microsoft Defender for Endpoint

Customer M365 Tenant

Microsoft Intune

Entra ID

Exchange Online + MDO

Microsoft Defender (incl. for O365)

Customer Azure Tenant

Microsoft Sentinel

Alerts

Microsoft Lighthouse MSSP API

Auto Resolutions

eGroup Enabling Technologies' Azure Tenant

Microsoft Sentinel

Consolidated SOAR Automations

Incidents

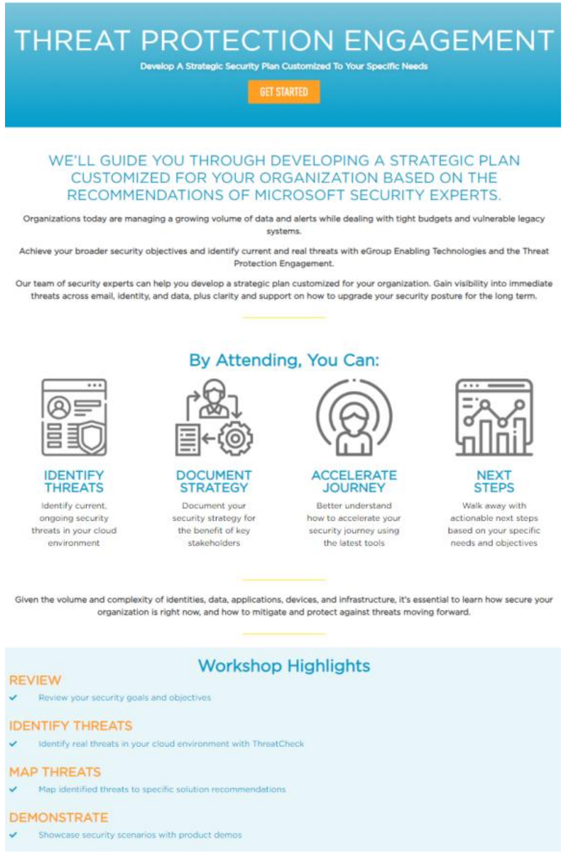
eGroup Enabling Technologies' SOC

Hunters 24/ 7/ 365

Co-Investigation and Resolution

Customer Analyst

Potential ways to Get Started



THREAT PROTECTION ENGAGEMENT

Develop A Strategic Security Plan Customized To Your Specific Needs

GET STARTED

WE'LL GUIDE YOU THROUGH DEVELOPING A STRATEGIC PLAN CUSTOMIZED FOR YOUR ORGANIZATION BASED ON THE RECOMMENDATIONS OF MICROSOFT SECURITY EXPERTS.

Organizations today are managing a growing volume of data and alerts while dealing with tight budgets and vulnerable legacy systems.

Achieve your broader security objectives and identify current and real threats with eGroup Enabling Technologies and the Threat Protection Engagement.

Our team of security experts can help you develop a strategic plan customized for your organization. Gain visibility into immediate threats across email, identity, and data, plus clarity and support on how to upgrade your security posture for the long term.

By Attending, You Can:

IDENTIFY THREATS
Identify current, ongoing security threats in your cloud environment

DOCUMENT STRATEGY
Document your security strategy for the benefit of key stakeholders

ACCELERATE JOURNEY
Better understand how to accelerate your security journey using the latest tools

NEXT STEPS
Walk away with actionable next steps based on your specific needs and objectives

Given the volume and complexity of identities, data, applications, devices, and infrastructure, it's essential to learn how secure your organization is right now, and how to mitigate and protect against threats moving forward.

Workshop Highlights

REVIEW

- ✓ Review your security goals and objectives

IDENTIFY THREATS

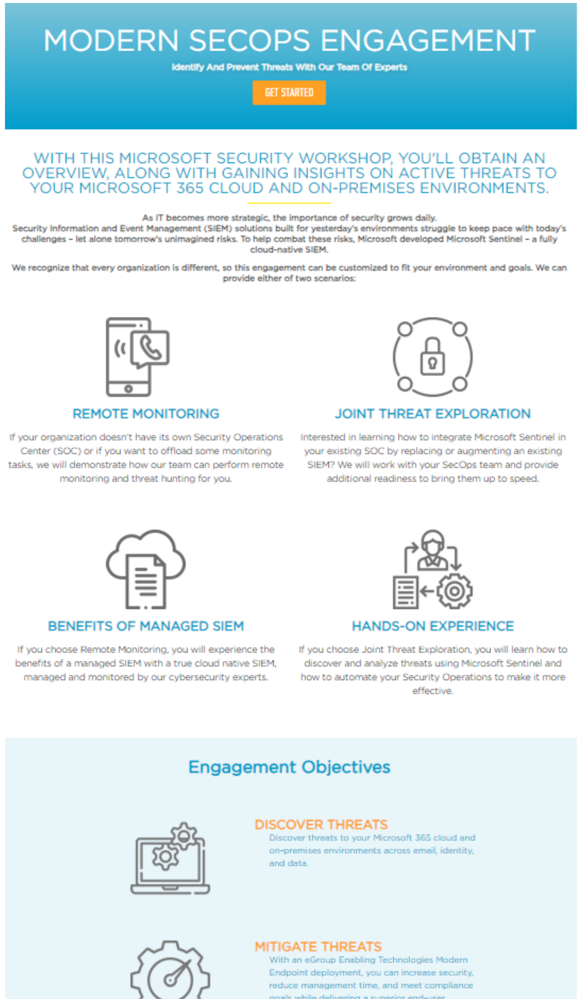
- ✓ Identify real threats in your cloud environment with ThreatCheck

MAP THREATS

- ✓ Map identified threats to specific solution recommendations

DEMONSTRATE

- ✓ Showcase security scenarios with product demos



MODERN SECOPS ENGAGEMENT

Identify And Prevent Threats With Our Team Of Experts

GET STARTED

WITH THIS MICROSOFT SECURITY WORKSHOP, YOU'LL OBTAIN AN OVERVIEW, ALONG WITH GAINING INSIGHTS ON ACTIVE THREATS TO YOUR MICROSOFT 365 CLOUD AND ON-PREMISES ENVIRONMENTS.

As IT becomes more strategic, the importance of security grows daily.
Security Information and Event Management (SIEM) solutions built for yesterday's environments struggle to keep pace with today's challenges – let alone tomorrow's unimagined risks. To help combat these risks, Microsoft developed Microsoft Sentinel – a fully cloud-native SIEM.

We recognize that every organization is different, so this engagement can be customized to fit your environment and goals. We can provide either of two scenarios:

REMONITORING

REMOTE MONITORING
If your organization doesn't have its own Security Operations Center (SOC) or if you want to offload some monitoring tasks, we will demonstrate how our team can perform remote monitoring and threat hunting for you.

JOINT THREAT EXPLORATION
Interested in learning how to integrate Microsoft Sentinel in your existing SOC by replacing or augmenting an existing SIEM? We will work with your SecOps team and provide additional readiness to bring them up to speed.

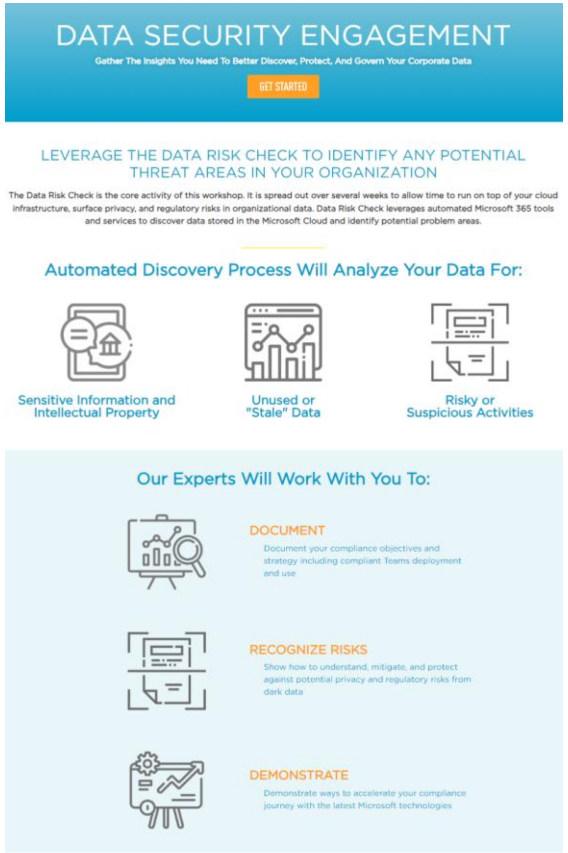
BENEFITS OF MANAGED SIEM
If you choose Remote Monitoring, you will experience the benefits of a managed SIEM with a true cloud native SIEM, managed and monitored by our cybersecurity experts.

HANDS-ON EXPERIENCE
If you choose Joint Threat Exploration, you will learn how to discover and analyze threats using Microsoft Sentinel and how to automate your Security Operations to make it more effective.

Engagement Objectives

DISCOVER THREATS
Discover threats to your Microsoft 365 cloud and on-premises environments across email, identity, and data.

MITIGATE THREATS
With an eGroup Enabling Technologies Modern Endpoint deployment, you can increase security, reduce management time, and meet compliance goals while delivering a superior end-user



DATA SECURITY ENGAGEMENT

Gather The Insights You Need To Better Discover, Protect, And Govern Your Corporate Data

GET STARTED

LEVERAGE THE DATA RISK CHECK TO IDENTIFY ANY POTENTIAL THREAT AREAS IN YOUR ORGANIZATION

The Data Risk Check is the core activity of this workshop. It is spread out over several weeks to allow time to run on top of your cloud infrastructure, surface privacy, and regulatory risks in organizational data. Data Risk Check leverages automated Microsoft 365 tools and services to discover data stored in the Microsoft Cloud and identify potential problem areas.

Automated Discovery Process Will Analyze Your Data For:

Sensitive Information and Intellectual Property

Unused or "Stale" Data

Risky or Suspicious Activities

Our Experts Will Work With You To:

DOCUMENT
Document your compliance objectives and strategy including compliant Teams deployment and use

RECOGNIZE RISKS
Show how to understand, mitigate, and protect against potential privacy and regulatory risks from dark data

DEMONSTRATE
Demonstrate ways to accelerate your compliance journey with the latest Microsoft technologies

Conclusion

Ransomware Trends

Understanding current ransomware trends is crucial for organizations to stay ahead of potential threats and vulnerabilities.

Microsoft Security Tools

Leveraging Microsoft’s security frameworks and tools can significantly enhance an organization's defenses against ransomware attacks.

Proactive Strategies

Implementing proactive strategies and maintaining ongoing vigilance are essential for safeguarding organizational data and resources.