Microsoft Security PSM TECHNOLOGY | TALENT

Healthcare and Education Cybersecurity Assessment

Engagement Overview

PSM Partners
sales@psmpartners.com
312-940-7830

Hidden

Latest Version

Always make sure you have the latest version of the toolkit before you start a new engagement!

The latest version of the toolkit can be obtained from: https://aka.ms/CybersecurityAssessment/Resources

Do not deliver the engagement using a previously downloaded version of the toolkit!

Hidden

Feedback

We want to hear from you about how you are using the tools and assets, what works, and what does not.

If you feel there is anything missing, or any other feedback that you would like to provide, please go to https://aka.ms/CybersecurityAssessment/Feedback to provide your feedback.

Hidden

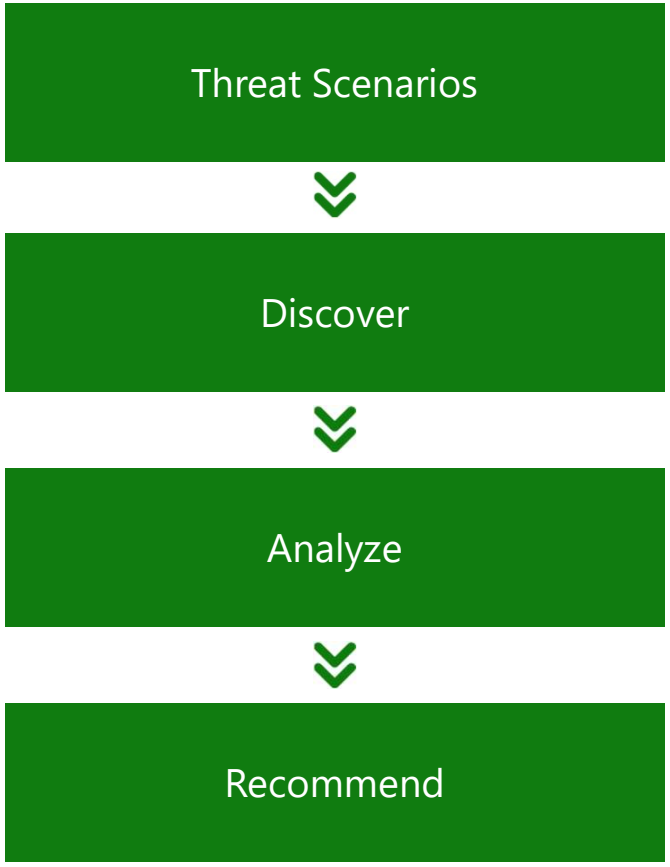
Version History

Version	Changes	Date
1.0	Initial release.	October 2023
1.1	Added the following two options to enable the assessment of vulnerabilities using MDVM: • Analyzing at least 50 machines already onboarded to Microsoft Defender for Endpoint. • Onboarding and analyzing at least 50 machines to Microsoft Defender for Endpoint.	February 2024

Introducing the Cybersecurity Assessment

Discover vulnerabilities to Microsoft cloud and on-premises environments.

Engagement Methodology



The engagement covers two commonly seen threat scenarios:

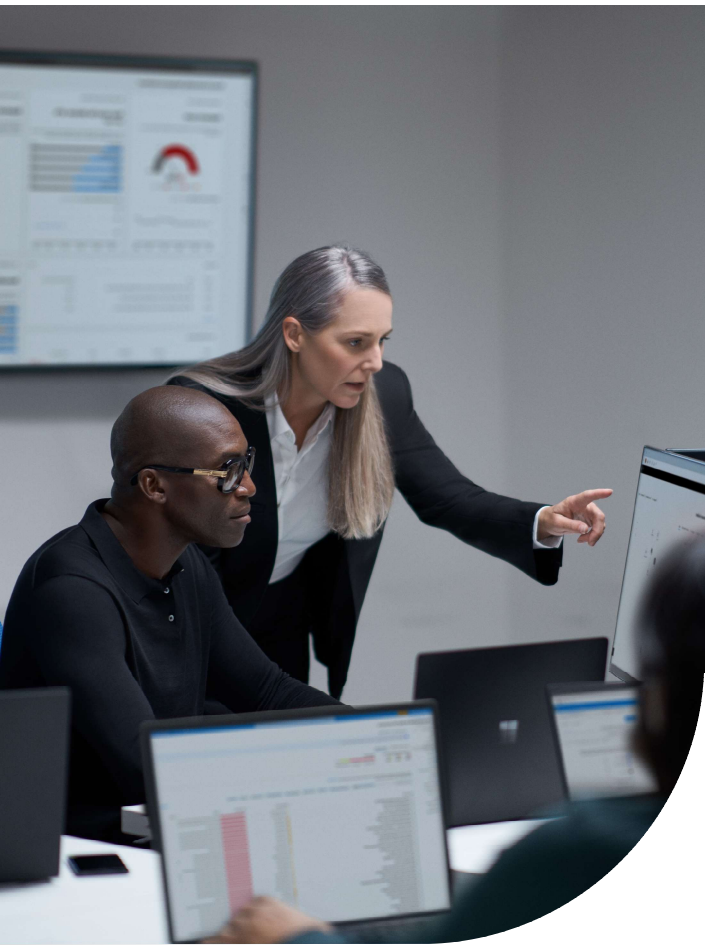
- Human-operated Ransomware
- Data Security risks from company insiders

Using the engagement tools, discover vulnerabilities within the customer's production environment across cloud, servers and endpoints.

The vulnerabilities and risks are analyzed and prioritized to show how prepared the customer's defenses are against the included threat scenarios.

Prepare detailed recommendations from the assessment to help the customer prioritize the improvements to their cybersecurity posture.

Top Human-operated Ransomware Concerns



Organizations struggle with maintaining basic cybersecurity hygiene

98%

of ransomware attacks can be traced to common configuration errors in software and devices. [1]

Ransomware attacks have been steadily increasing

37%

of all businesses and organizations were hit by ransomware in 2021. [2]

Recovering from a ransomware attack is costly

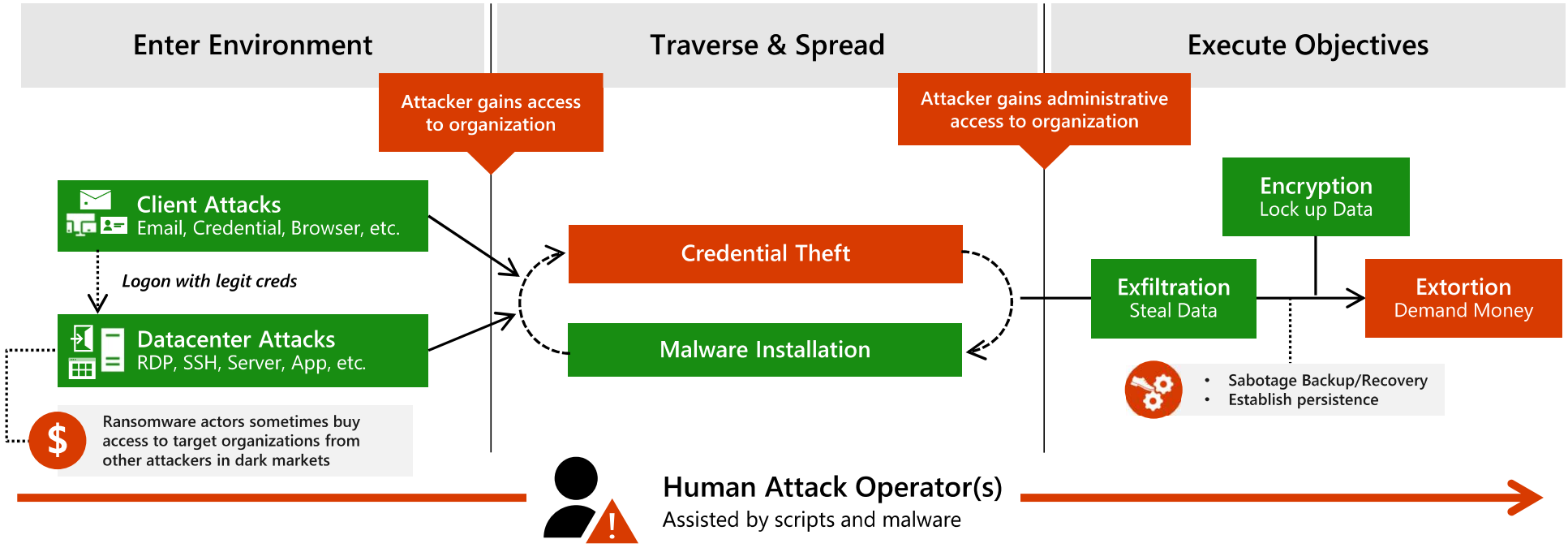
$1.85M

Recovering from a ransomware attack cost businesses $1.85 million on average in 2021.[3]

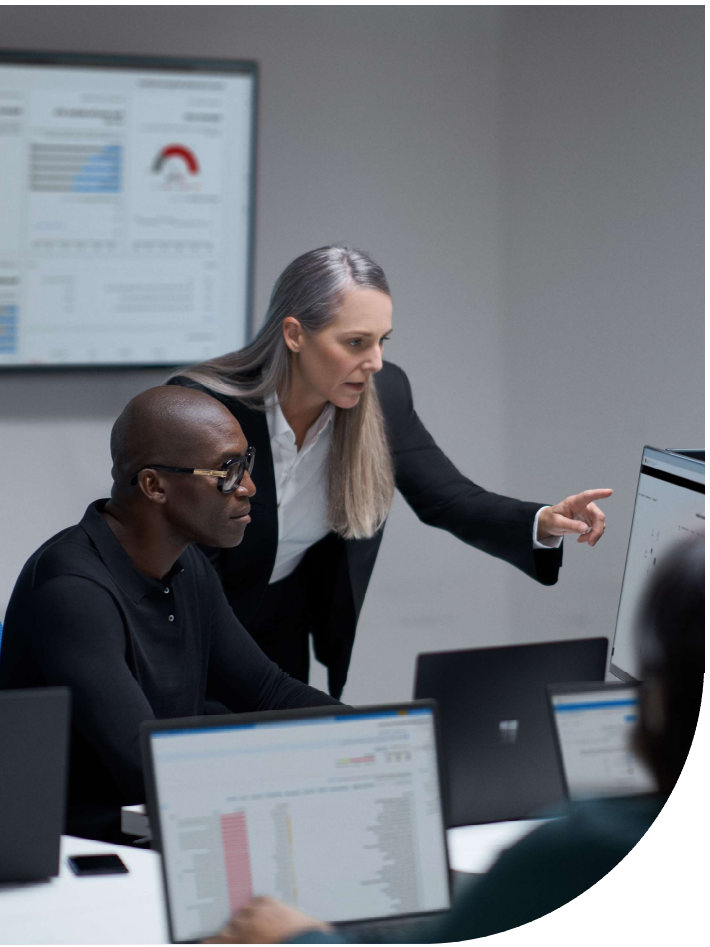
1. Digital Defense Report 2022, Microsoft
2. Ransomware Statistics, Trends and Facts for 2023 and Beyond
3. Ransomware Statistics, Trends and Facts for 2023 and Beyond

Human-operated Ransomware Overview

Human-operated ransomware is the result of an **active attack** by cybercriminals that infiltrate an organization's on-premises or cloud IT infrastructure, elevate their privileges, and deploy ransomware to critical data.



Top data security concerns



Data security incidents are widespread

83% of organizations experience more than one data breach in their lifetime[1]

Malicious insiders account for 20% of data breaches, adding to costs

$15.4M Total average cost of activities to resolve insider threats over 12 month period[2]

Organizations are struggling with a fragmented solution landscape

80% of decision makers purchased multiple products to meet compliance and data protection needs[3]

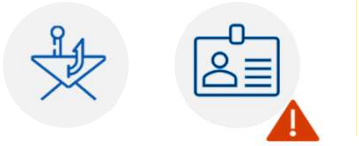
1. Cost of a Data Breach Report 2022, IBM
2. Cost of Insider Threats Global Report 2022, Ponemon Institute
3. February 2022 survey of 200 US compliance decision-makers (n=100 599-999 employees, n=100 1000+ employees) commissioned by Microsoft with MDC Research

Data security incidents can happen anytime, anywhere

Data at risk of misuse if organization has no visibility into their data estate

1

User falls prey to phishing attack, compromises user credentials



Data compromise by external threat

2

User copies file to a USB, then uploads to a personal Dropbox

Data theft by malicious insider

3

User inadvertently shares the file copy with a few colleagues

Data exposure by negligent insider

What we'll do during the engagement

Analyze the customer's environment and current cybersecurity maturity level based on v8 of the CIS Critical Security Controls.

Define scope & deploy Microsoft Defender Vulnerability Management and Insider Risk Analytics in the customer's production environment.

Perform a vulnerability assessment and assist with the prioritization of vulnerabilities and misconfigurations across the customer's organization.

Perform a data security assessment, discover and evaluate sensitive information and potential insider risks in the customer's organization.

Plan next steps on how to improve the customer's cyber and data security posture and how you can work together for future engagements.

Objectives and Approach

Discover vulnerabilities

Gain visibility into vulnerabilities to the customer's Microsoft 365 cloud using Microsoft Secure Score.

Discover and analyze vulnerabilities to servers and endpoints using Microsoft Defender Vulnerability Management.

Explore and Evaluate sensitive information and potential insider risk

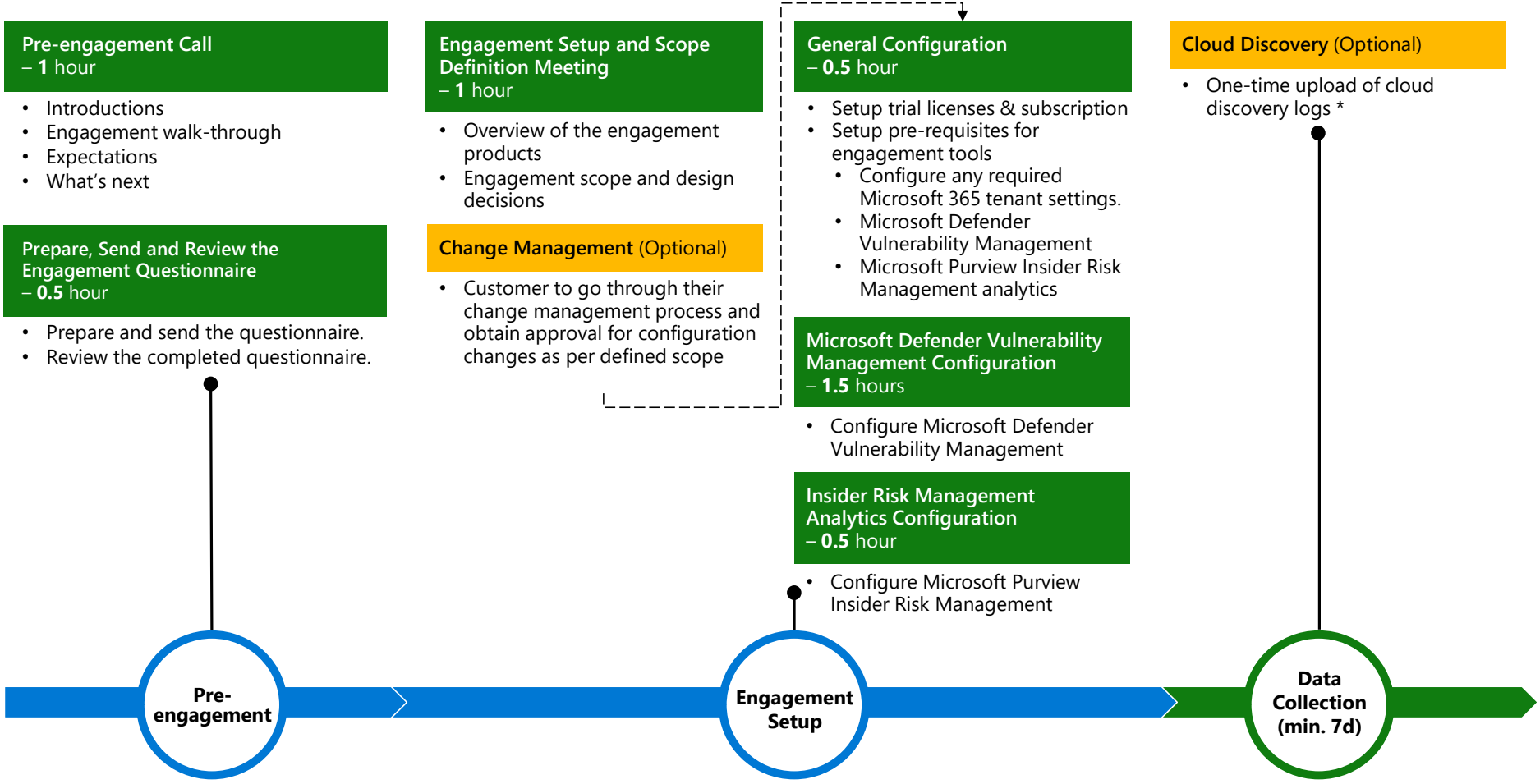
Gain visibility into sensitive information discovered by Microsoft Purview Information Protection.

Explore potentially risky data handling activities identified by Microsoft Purview Insider Risk Management Analytics.

Define next steps

As part of the engagement, work together with the customer to define a list of next steps based on their needs, objectives, and results from the Cybersecurity Assessment.

Cybersecurity Assessment phases and activities



* Unless using Microsoft Defender for Endpoint as a source of the cloud discovery data.

Cybersecurity Assessment phases and activities

Vulnerabilities Exploration
– **1** hour

- Explore vulnerabilities in:
  - Microsoft Defender Vulnerability Management
  - Microsoft Secure Score

Data Security Exploration
– **1** hour

- Explore data security risks from company insiders.

Cloud Discovery Exploration (Optional)
– **1** hour

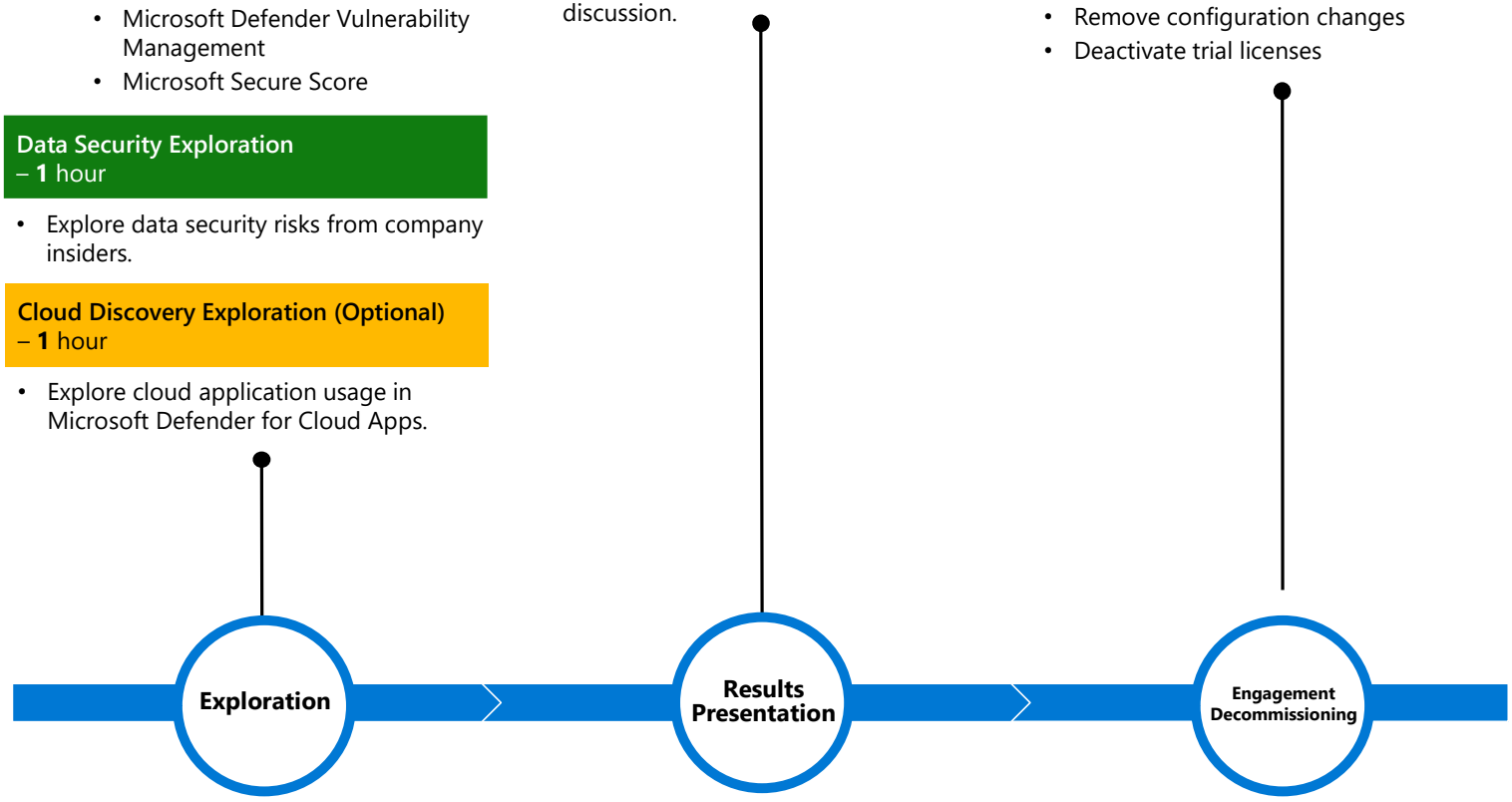
- Explore cloud application usage in Microsoft Defender for Cloud Apps.

Results Presentation
– **2** hours

- Results presentation and Next Steps discussion.

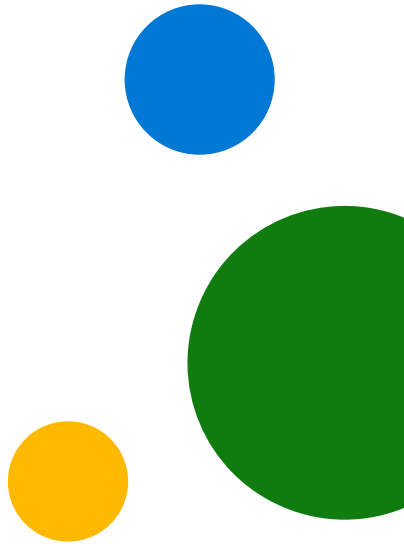
Engagement Decommissioning
– **1** hour

- Remove uploaded logs
- Remove configuration changes
- Deactivate trial licenses

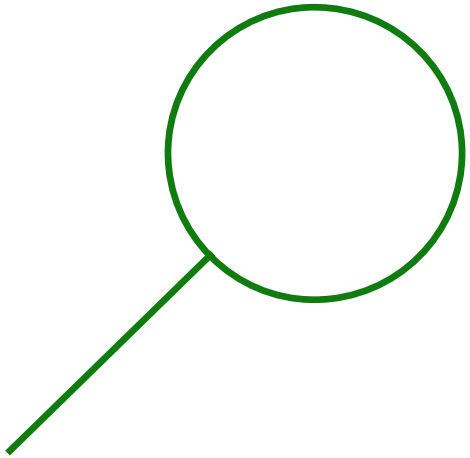


After the Cybersecurity Assessment, the customer will…

- Better understand, prioritize, and address cybersecurity vulnerabilities and how to improve their defenses against human-operated ransomware.
- Better understand, prioritize, and address data security vulnerabilities and how to minimize data security risks from company insiders.
- Have defined next steps based on the engagement findings and their needs and objectives.



Out of Scope



- Configuration of Microsoft Security tools beyond the engagement tools:
  - Microsoft Defender for Endpoint
  - Microsoft Defender Vulnerability Management
  - Microsoft Purview Information Protection
  - Microsoft Purview Insider Risk Management Analytics.
- Deep analysis (investigation) of threats found during the engagement
- Incident response
- Forensic analysis
- Technical designs or implementations
- Proof of Concept or Lab Deployment

Engagement Phases: Engagement Setup

Engagement Setup

Engagement Setup and Scope Definition Meeting

Define and finalize the engagement scope and required configuration settings for the engagement tools.

Change Management

If needed, assist the customer with any required change management processes and approvals for the configuration changes as per defined scope.

General Configuration

Configuration of the customer's Microsoft 365 production tenant including setting up trial licenses, configuration of tenant and included Microsoft Defender XDR security products.

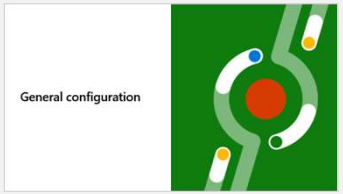
Microsoft Defender Vulnerability Management Configuration

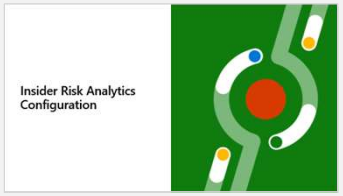
Configuration of Microsoft Defender Vulnerability Management in the customer's production tenant including the configuration of a machine to be used to scan for vulnerabilities on-premises, if needed.

Insider Risk Analytics Configuration

Configuration of Microsoft Purview Risk Management products in the customer's production tenant.

Zoom in for additional details of each activity, if needed:





Engagement Phases: Data Collection

Data Collection

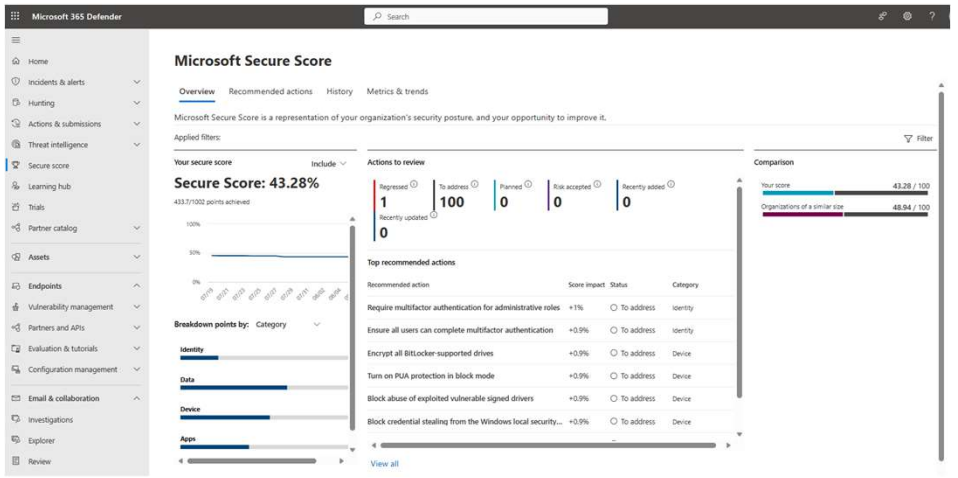
- Vulnerabilities and misconfigurations detected by the engagement tools.
- Minimum of 7 days duration to allow us to gather enough data to analyze.
- Upload of Cloud Discovery logs (towards the end)*.

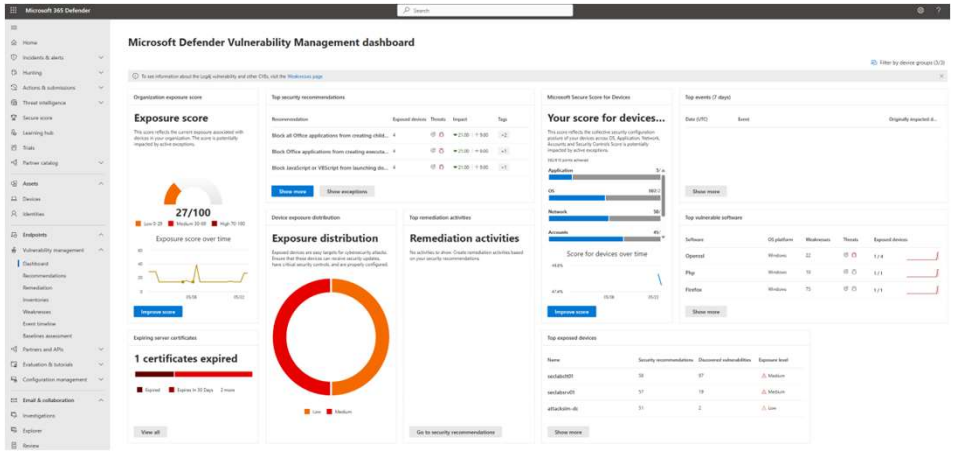
* Unless using Microsoft Defender for Endpoint as a source of the cloud discovery data.

Engagement Phases: Exploration

Vulnerabilities Exploration

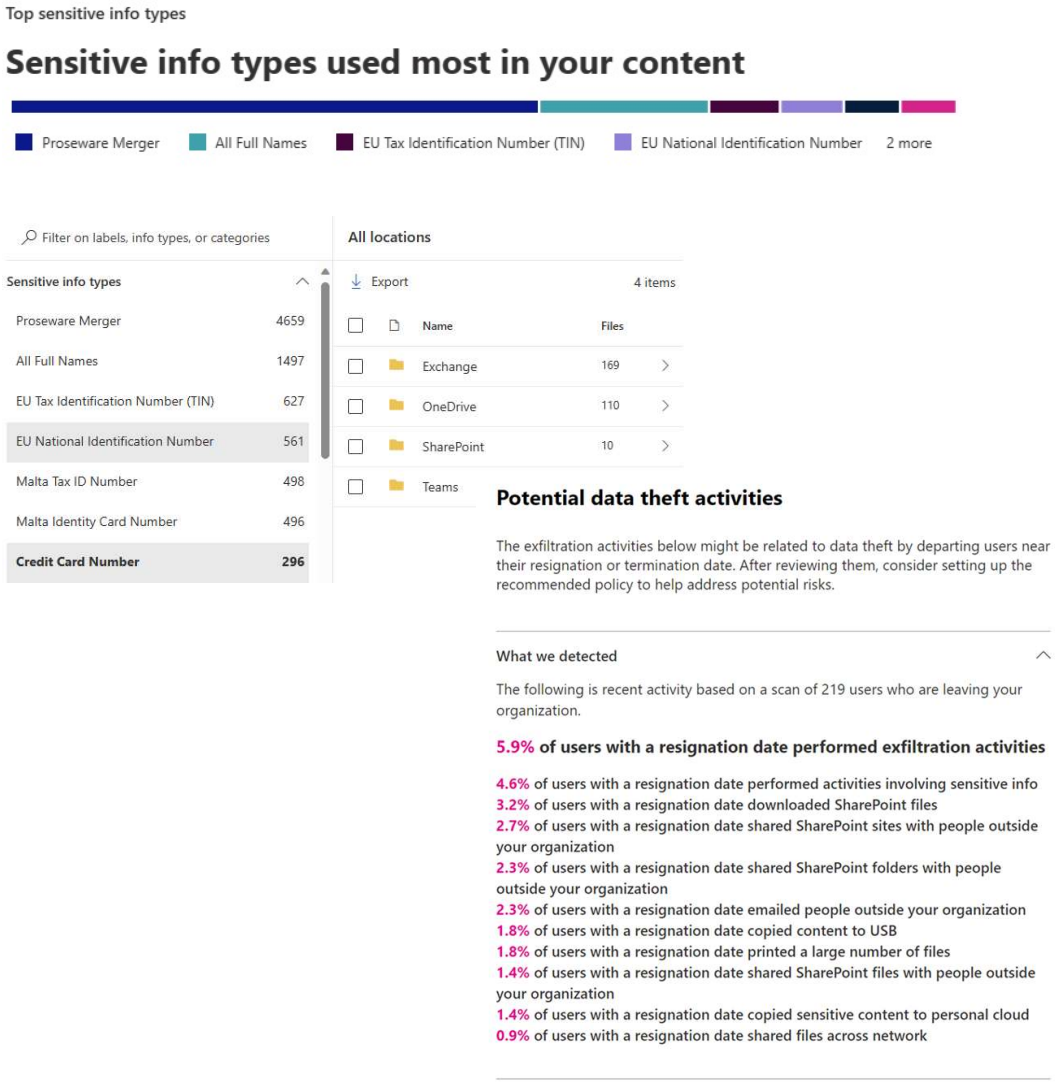
- Help the customer gain visibility into vulnerabilities in their cloud and on-premises environments obtained through Microsoft Secure Score and Microsoft Defender Vulnerability Management.
- Provide recommendations on:
  - How to discover and prioritize vulnerabilities and misconfigurations.





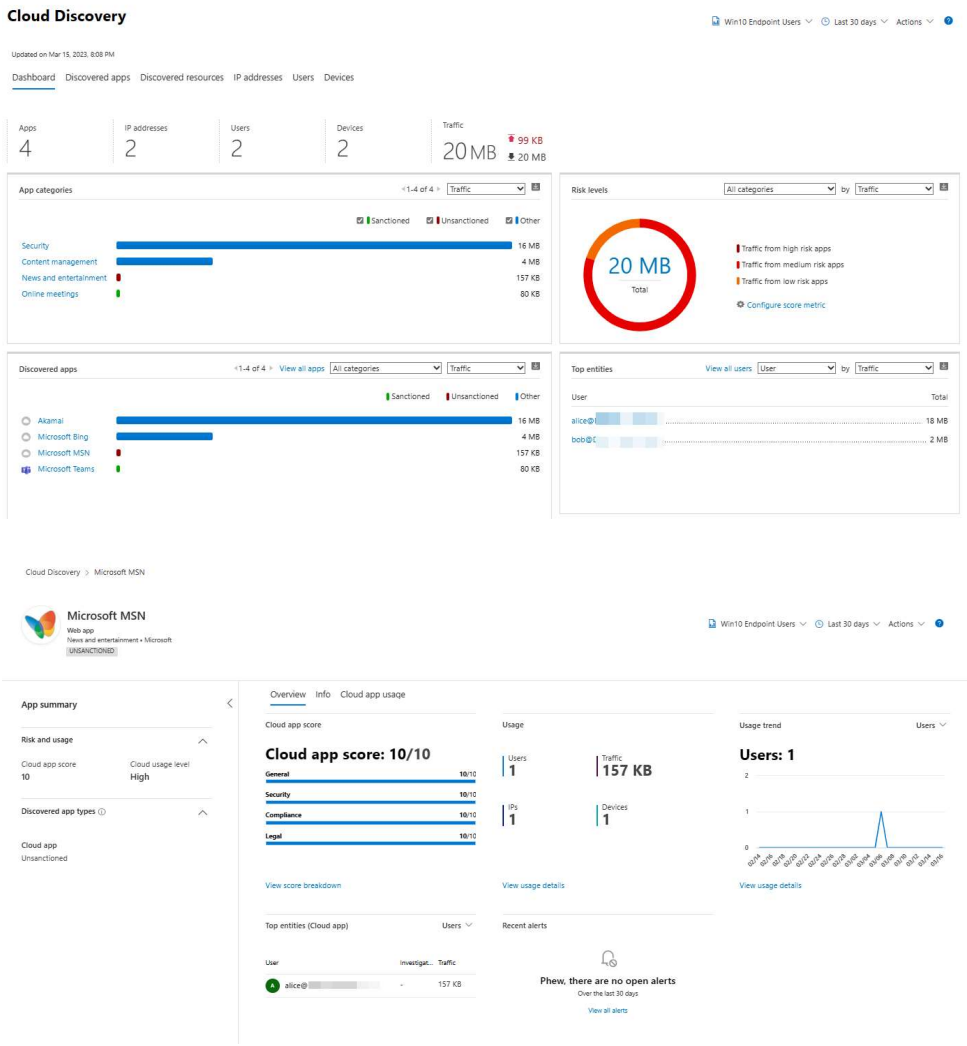
Data Security Exploration

- Help the customer gain visibility into data security risks in their organization obtained through zero change management configurations.
- Provide snapshots of what sensitive information exists within the customer's Microsoft 365 environment
- Conduct an evaluation of potential insider risks in the customer's organization without configuring any insider risk policies.



Cloud Discovery Exploration - Optional

- Help the customer gain visibility into Shadow IT usage, identifying apps accessed by users across their organization using Microsoft Defender for Cloud Apps.
- Evaluate discovered apps for more than 90 risk indicators, allowing you to sort through the discovered apps and assess the customer's security and compliance posture.



Engagement Phases: Results Presentation and Next Steps Discussion

Results Presentation and Next Steps Discussion

- Findings and recommendations from the Vulnerabilities Exploration
- Findings and recommendations from the Data Security Exploration
- Findings and recommendations from the Cloud Application Discovery
- Technical and strategic-level next steps
- Agree on follow-up engagements

Resources

Resources

- Cybersecurity Assessment partner webpage:
  https://aka.ms/CybersecurityAssessment
- Delivery resources & guides:
  https://aka.ms/CybersecurityAssessment/Resources
- Engagement Overview Video
  https://aka.ms/CybersecurityAssessment/EngagementOverviewVideo

Join the Microsoft Security, Compliance & Identity Yammer Group

Microsoft Security

Thank you.

Detailed Slides

Engagement Setup and Scope Definition Meeting

Engagement Setup and Scope Definition Meeting

Overview of the engagement products

Overview of the engagement products including specific requirements to ensure a successful deployment:

- Microsoft Defender Vulnerability Management
- Microsoft Purview Insider Risk Management

Engagement Scope

Discuss and decide on the engagement scope:

- Microsoft Defender Vulnerability Management
  - What devices (servers/clients) should be scanned for vulnerabilities?
- Microsoft Defender for Cloud Apps – Optional
  - How should we gather logs?
- Microsoft Purview Insider Risk Management

Design Decisions

Discuss and decide how the engagement products will be configured.

General configuration

General configuration

The General Configuration activity includes following steps:

- Deploy the Cybersecurity Assessment Microsoft 365 trial licenses
- Turn on audit logging in Microsoft 365, if needed
- Activate Microsoft Defender XDR, if needed
- Configure pre-requisites for the Microsoft Defender Vulnerability Management Authenticated scan for Windows, if needed
- Configure Microsoft Defender for Cloud Apps - Optional

Microsoft Defender for Cloud Apps

What is Microsoft Defender for Cloud Apps?

A multi-mode Cloud Access Security Broker.

Insights into threats to identity and data

Raise alerts on user or file behavior anomalies in cloud apps leveraging their API connectors.

In scope for this engagement with Office 365 and Azure.

Out of scope for this engagement with other API connectors.

Discover the use of unsanctioned cloud application and services (aka “shadow IT”)

In scope for this engagement.

Ability to respond to detected threats, and configuration of application monitoring and control

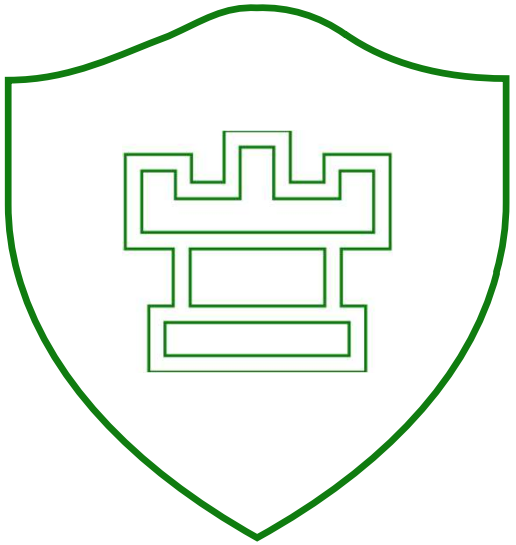
Out of scope for this engagement.

Requirements

Available to organizations with Office 365 or Microsoft 365 enterprise, education or government subscriptions and with tenant in the commercial (public) cloud or in any type of U.S. Government Community cloud.

Microsoft Defender Vulnerability Management Configuration

Microsoft Defender Vulnerability Management



What is Microsoft Defender Vulnerability Management (MDVM)?

A comprehensive risk-based vulnerability management to identify, assess, remediate, and track vulnerabilities across most critical assets, all in a single solution.

Asset discovery and monitoring

Analysis of Defender Vulnerability Management vulnerability and configuration assessment results to help understand and assess cybersecurity exposure.

In scope for this engagement.

Licensing

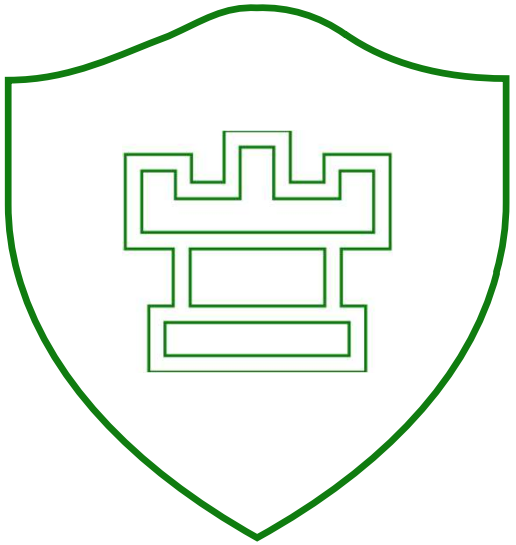
Endpoints:

- Premium MDVM capabilities included as part of the Defender Vulnerability Management Add-on – a trial is provided as part of this engagement.
- MDVM Standalone provides full Defender Vulnerability Management capabilities for any EDR solution.

Servers (in Microsoft Defender for Cloud):

- Premium MDVM capabilities included as part of the Defender for Servers Plan 2.

Microsoft Defender Vulnerability Management Assessment Options

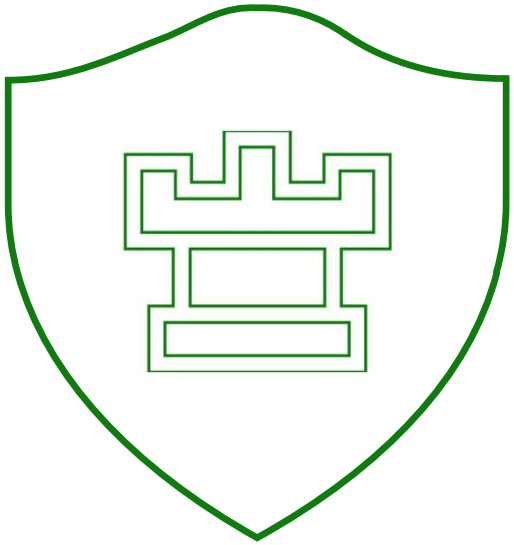


Microsoft Defender Vulnerability Management Assessment Options

To allow Microsoft Defender Vulnerability Management to assess vulnerabilities, we have following three options:

1. **Remotely scan Windows 10/11 clients or servers using the Microsoft Defender Vulnerability Management Authenticated Scanner** – This option requires you to have an on-premises Active Directory and at least 50 on-premises Windows 10/11 clients or Windows servers to be scanned. Scanned clients or servers do NOT need to be onboarded to Microsoft Defender for Endpoint.
2. **Onboarding Windows 10/11 Client or Servers to Microsoft Defender for Endpoint** – We can onboard the required 50 Windows 10/11 clients or Windows servers to Microsoft Defender for Endpoint as part of the engagement.
3. **Assessing Windows 10/11 clients or servers already onboarded to Microsoft Defender for Endpoint** – We can assess at least 50 Windows 10/11 clients or Windows servers which have already been onboarded to Microsoft Defender for Endpoint.

Microsoft Defender Vulnerability Management Authenticated Scan



What is the Microsoft Defender Vulnerability Management (MDVM) Authenticated Scan?

Authenticated Scan for Windows provides the ability to run scans on remote Windows devices. Once configured, the targeted devices will be scanned regularly for software vulnerabilities.

Requirements

Scanner:

- On-premises machine with Windows 10 (version 1903), Windows Server (version 1903) and later.
- Must be onboarded to MDE (MDE can be configured as part of this engagement if needed).
- Detailed machine requirements will be provided after this meeting to allow you to prepare it before we start the engagement.

Scanning Account:

- This must be a Group Managed Service Account (gMsa):
  - The account is a least privileged account with only the minimum required scanning permissions.
  - The account will be removed at the end of the engagement.

Required Device Configuration:

- Each device to be scanned needs to be configured with the permissions needed by the scanner:
  - This can be completed either manually or using group policies.
  - We recommend applying the required settings using a provided PowerShell script which creates a group policy scoped specifically to the scanned devices.

Insider Risk Analytics Configuration

Insider Risk Analytics

What is Microsoft Purview Insider Risk Management

Microsoft Purview Insider Risk Management is a compliance solution that helps minimize internal risks by enabling you to detect, investigate, and act on malicious and inadvertent activities.

Insider Risk Analytics

Insider Risk Management analytics enables you to conduct an evaluation of potential insider risks **without configuring any insider risk policies**. This evaluation can help organizations identify potential areas of higher user risk and help determine the type and scope of insider risk management policies they might want to configure.

In scope for this engagement.

Requirements

- Microsoft Purview Audit Log enabled in the customer's organization.
- An account with membership in:
  - Insider Risk Management
  - Information Protection
  - Compliance Data Administrator

Insider Risk Analytics Configuration

What is Microsoft Purview Insider Risk Management Analytics Overview

Analytics scans offer the following:

Easy to configure: To get started with analytics scans, select **Run scan** when prompted by the analytics recommendation.

Privacy by design: Scanned results and insights are returned as aggregated and anonymized user activity. Individual usernames aren't identifiable by reviewers.

Understand potential risks through consolidated insights: Scan results can help you quickly identify potential risk areas for users and which policy would be best to help mitigate these risks

Areas Scanned

Analytics scans offer the following:

Microsoft 365 audit logs: Included in all scans, this is the primary source for identifying most of the potentially risky activities.

Exchange Online: Included in all scans, Exchange Online activity helps identify activities where data in attachments are emailed to external contacts or services.

Microsoft Entra ID: Included in all scans, Microsoft Entra ID history helps identify risky activities associated with users with deleted user accounts.

Microsoft 365 HR data connector: If configured