Microsoft Security

Cybersecurity Assessment

Engagement Overview

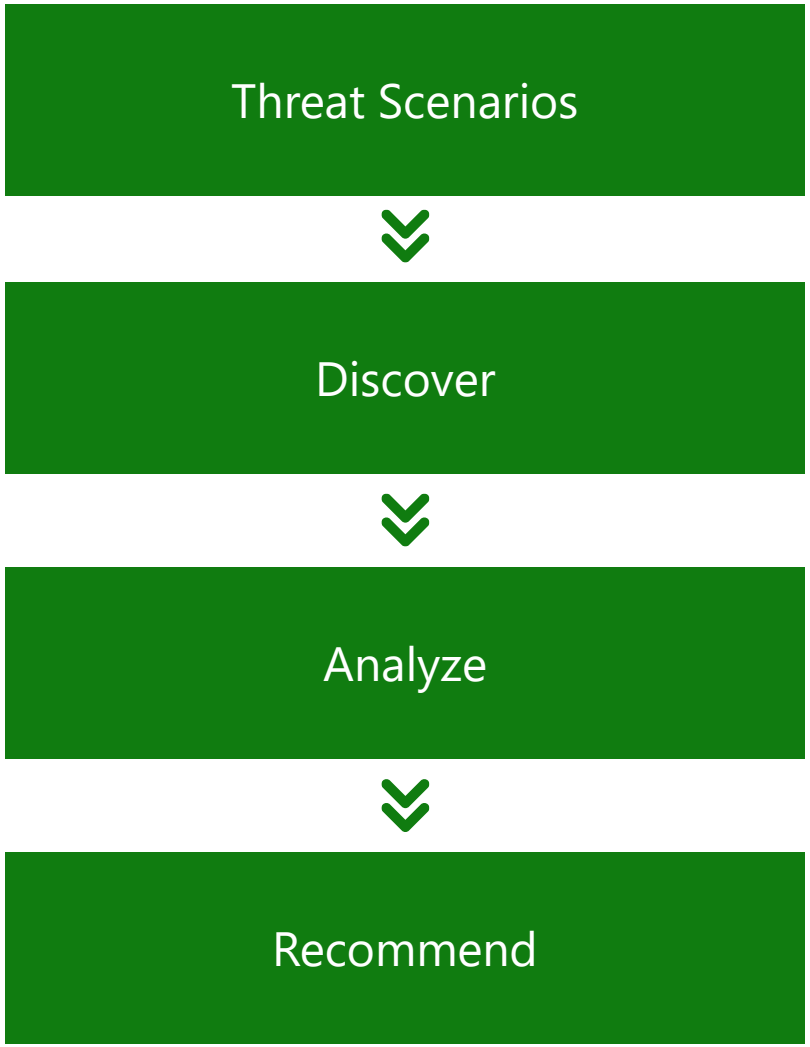
MAUREEN DATA SYSTEMS

Introducing the Cybersecurity Assessment

Discover vulnerabilities to Microsoft cloud and on-premises environments.

MAUREEN DATA SYSTEMS

Engagement Methodology



The engagement covers two commonly seen threat scenarios:

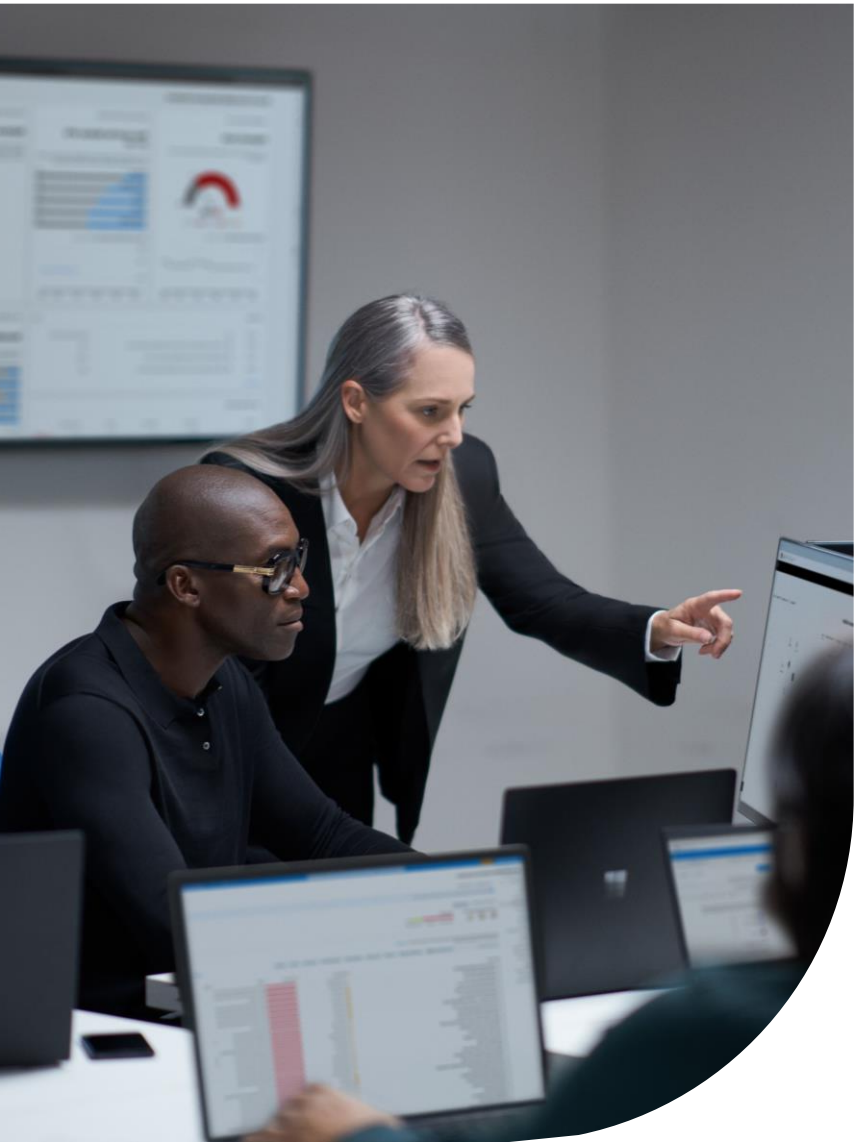
- Human-operated Ransomware
- Data Security risks from company insiders

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

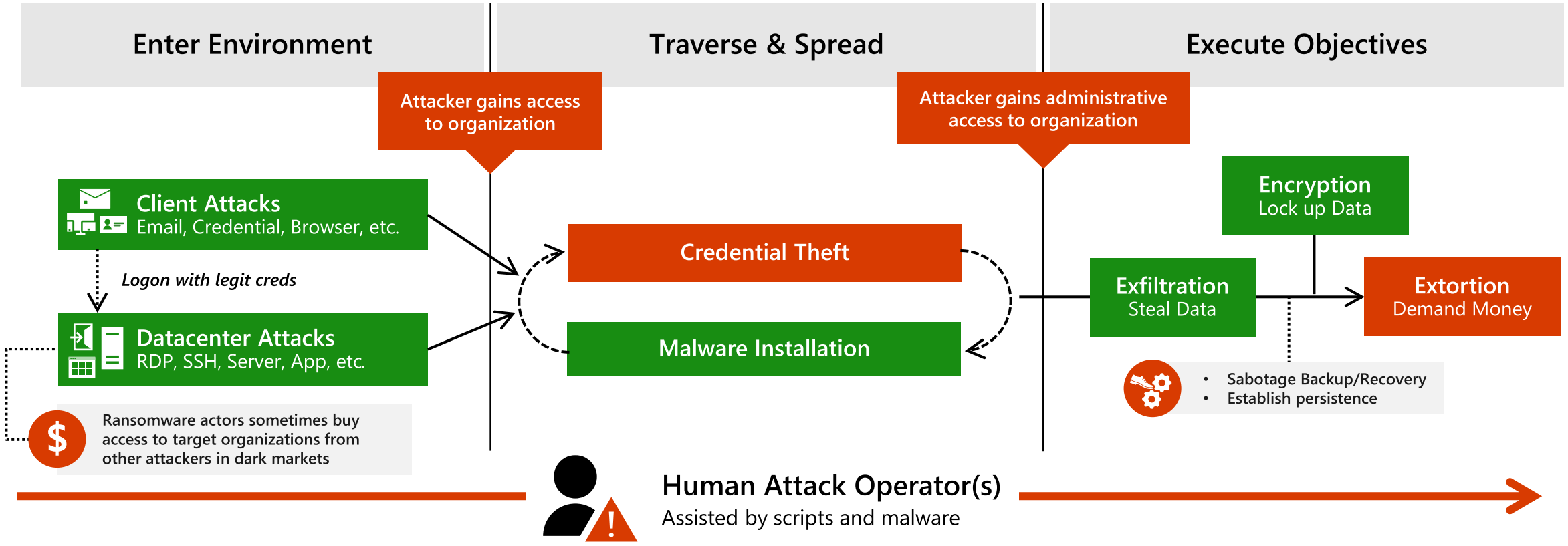
$1.85M

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

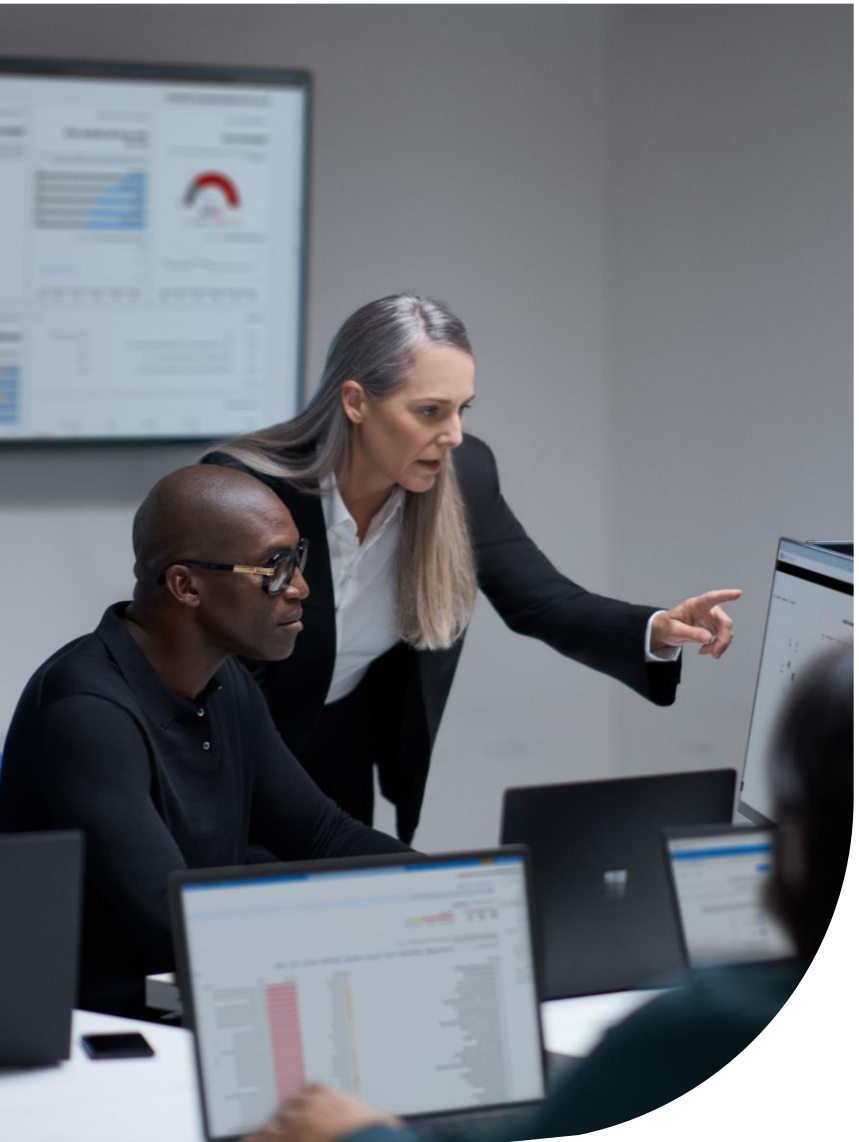
1. Digital Defense Report 2022, Microsoft
2. Ransomware Statistics, Trends and Facts for 2023 and Beyond
3. Ransomware Statistics, Trends and Facts for 2023 and Beyond

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

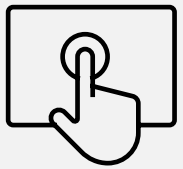
3

User inadvertently shares the file copy with a few colleagues

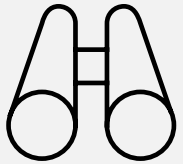
Data exposure by negligent insider

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.

MAUREEN DATA SYSTEMS

Cybersecurity Assessment phases and activities

Pre-engagement Call
– **1** hour

- Introductions
- Engagement walk-through
- Expectations
- What's next

Prepare, Send and Review the Engagement Questionnaire
– **0.5** hour

- Prepare and send the questionnaire.
- Review the completed questionnaire.

Engagement Setup and Scope Definition Meeting
– **1** hour

- Overview of the engagement products
- Engagement scope and design decisions

Change Management (Optional)

- Customer to go through their change management process and obtain approval for configuration changes as per defined scope

General Configuration
– **0.5** hour

- Setup trial licenses & subscription
- Setup pre-requisites for engagement tools
  - Configure any required Microsoft 365 tenant settings.
  - Microsoft Defender Vulnerability Management
  - Microsoft Purview Insider Risk Management analytics

Microsoft Defender Vulnerability Management Configuration
– **1.5** hours

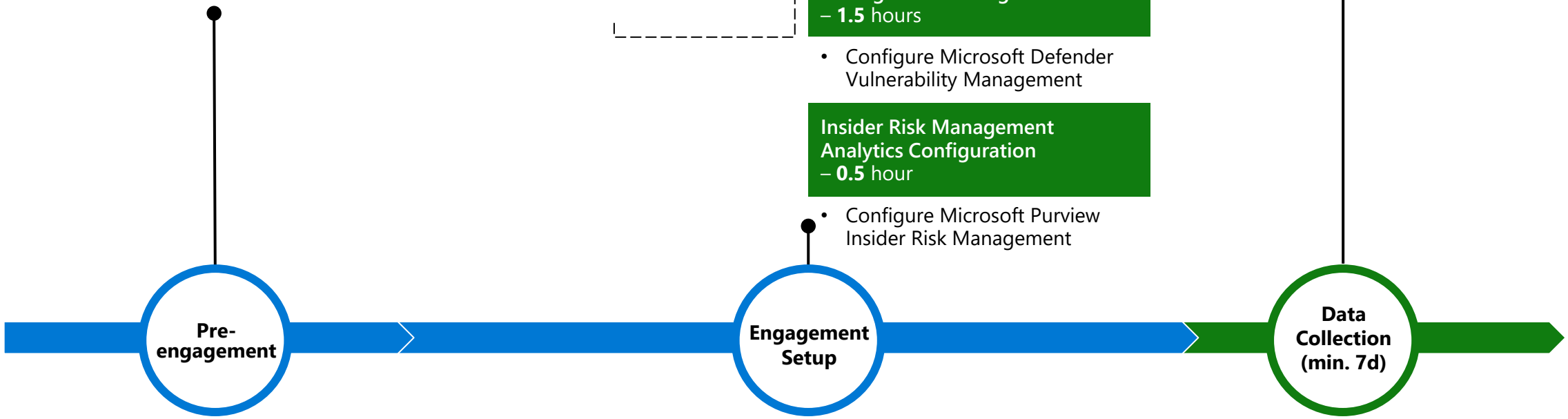
- Configure Microsoft Defender Vulnerability Management

Insider Risk Management Analytics Configuration
– **0.5** hour

- Configure Microsoft Purview Insider Risk Management

Cloud Discovery (Optional)

- One-time upload of cloud discovery logs *



* 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

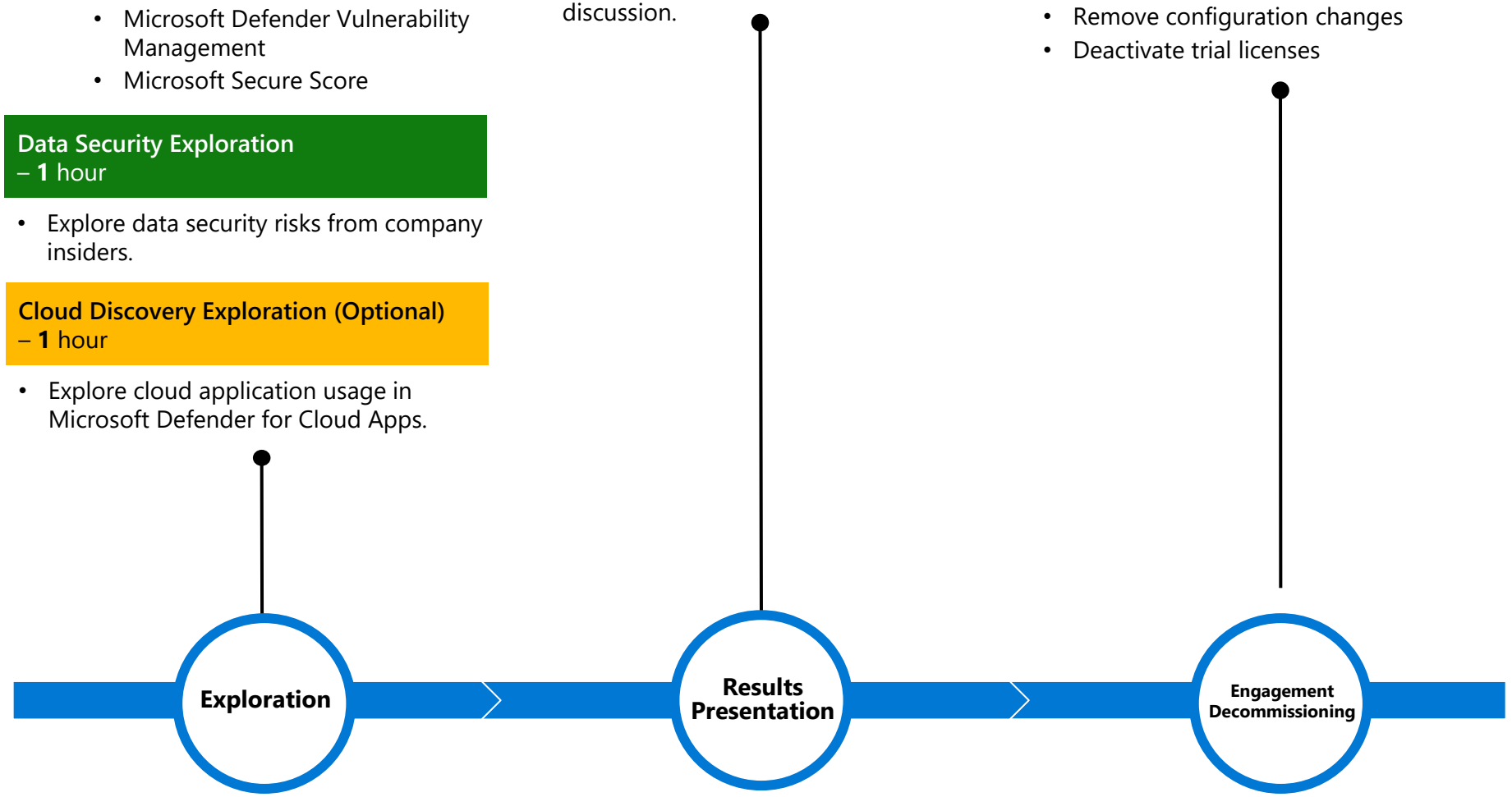
- Explore cloud application usage in Microsoft Defender for Cloud Apps.

Results Presentation
– **2** hours

- Results presentation and Next Steps discussion.

Engagement Decommissioning
– **1** hour

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

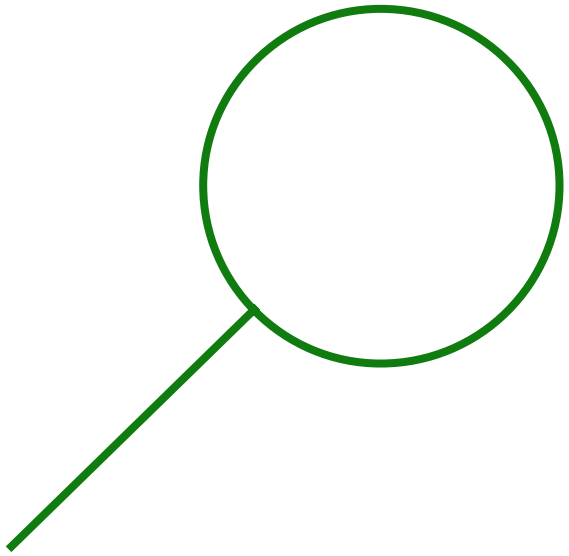


After the Cybersecurity Assessment, the customer will…

- 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.

MAUREEN DATA SYSTEMS

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

MAUREEN DATA SYSTEMS

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.

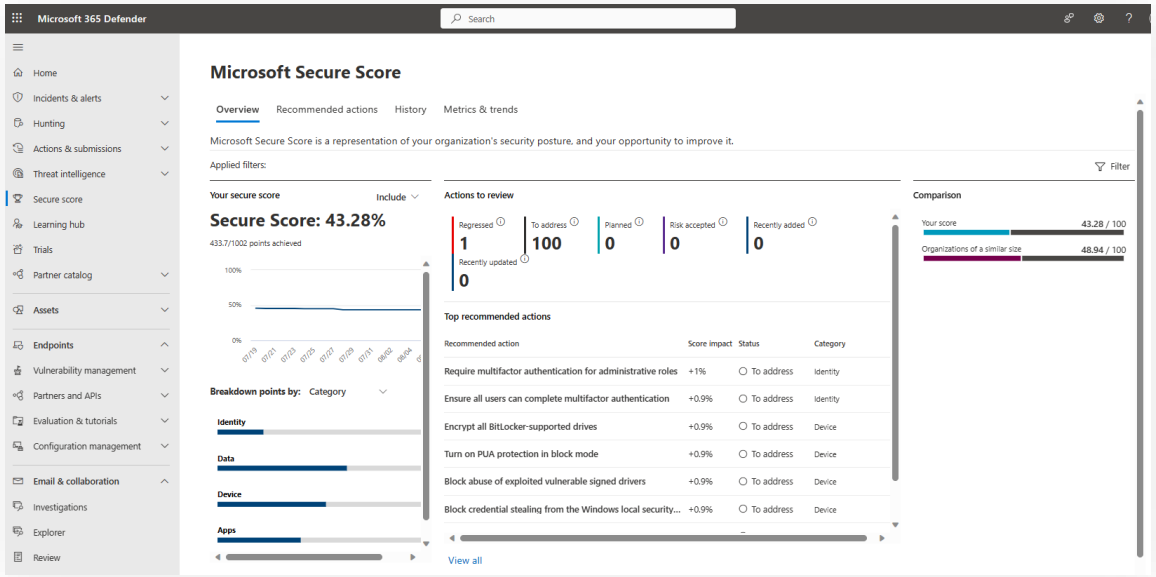
MAUREEN DATA SYSTEMS

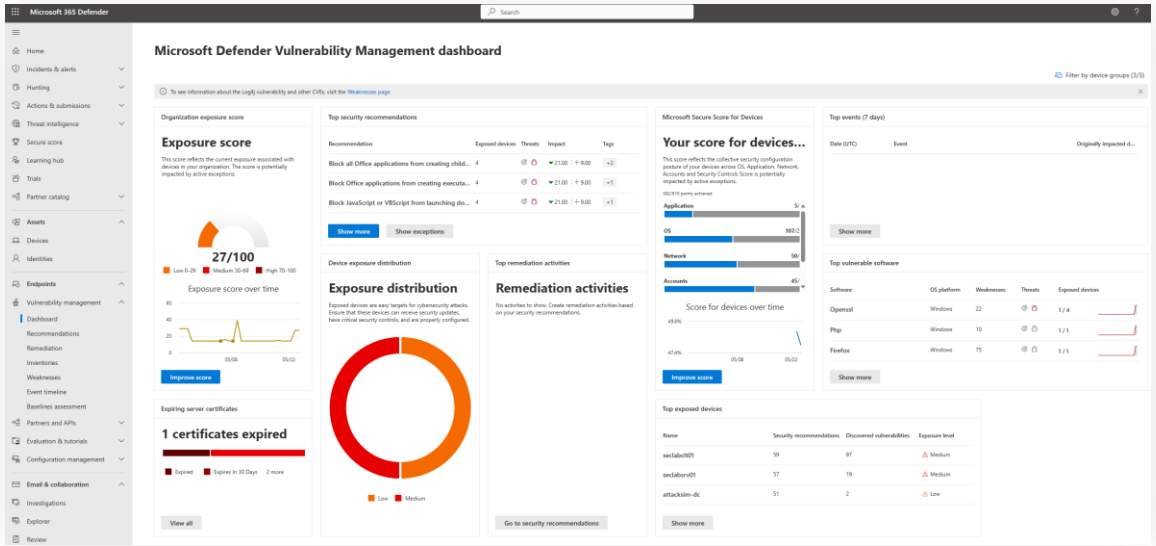
Engagement Phases: Exploration

MAUREEN DATA SYSTEMS

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.



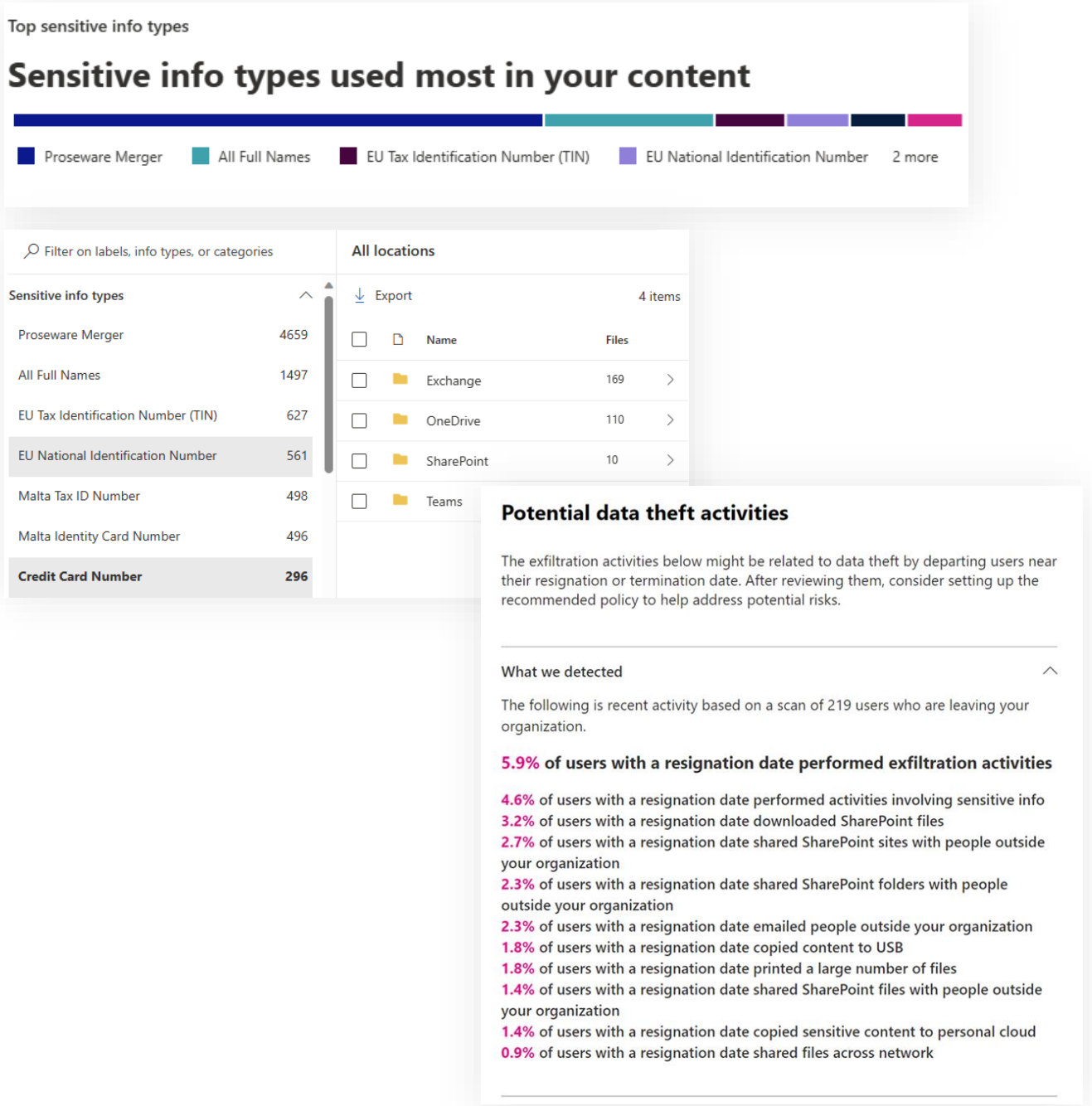


MAUREEN DATA SYSTEMS

Data Security Exploration

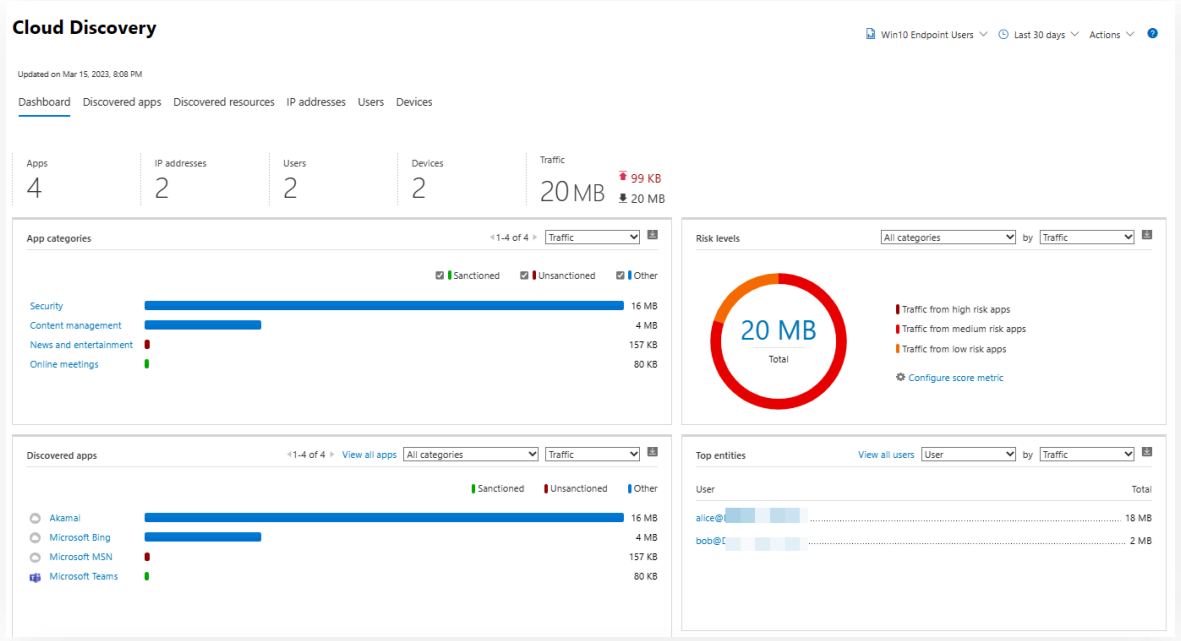
- Help the customer gain visibility into data security risks in their organization obtained through zero change management configurations.
- Provide snapshots of what sensitive information exists within the customer's Microsoft 365 environment
- Conduct an evaluation of potential insider risks in the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

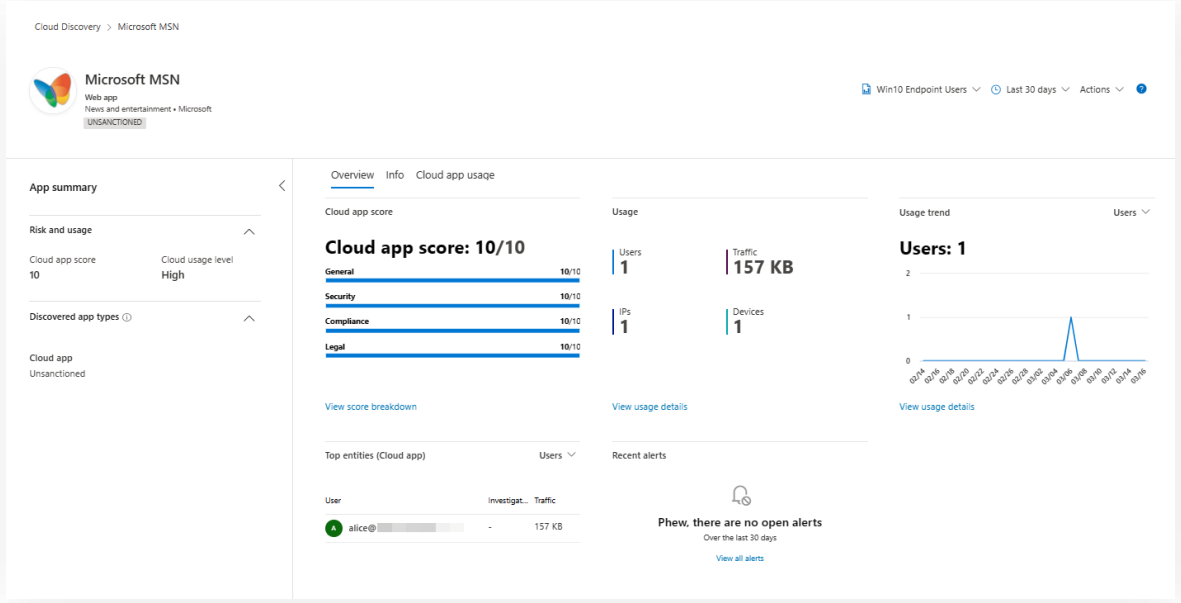
MAUREEN DATA SYSTEMS



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.





MAUREEN DATA SYSTEMS

Engagement Phases: Results Presentation and Next Steps Discussion

MAUREEN DATA SYSTEMS

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