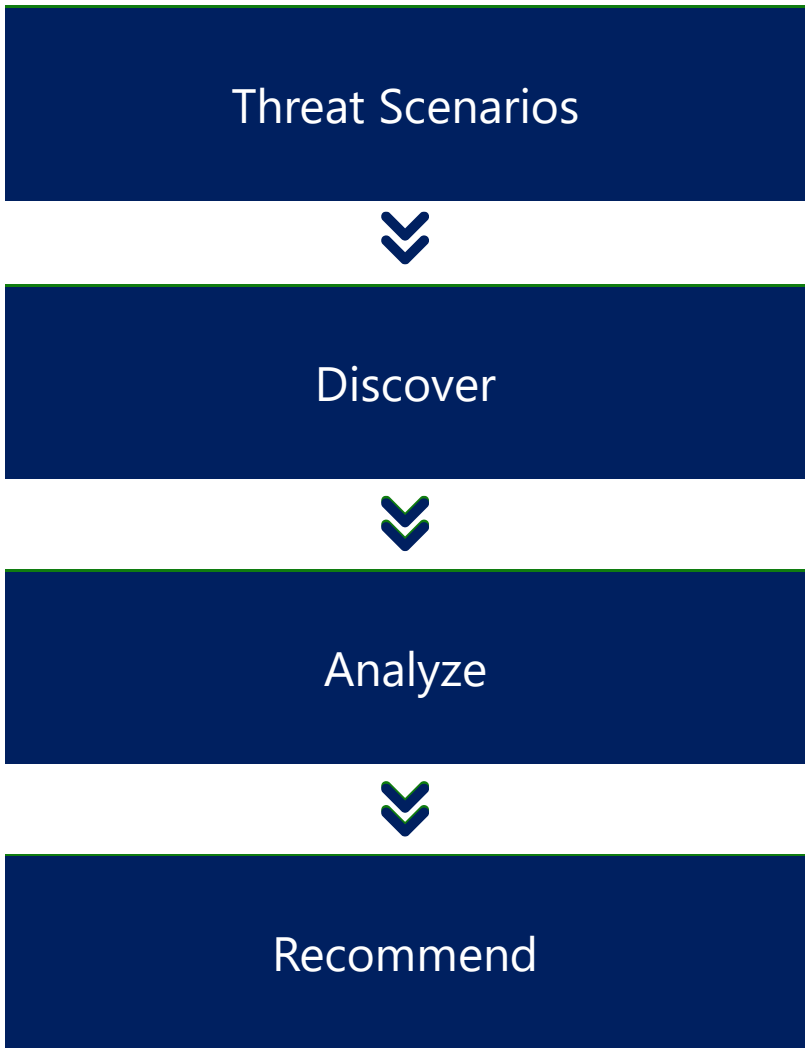
AKINSIT

Microsoft Cybersecurity Assessment

Engagement Overview

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.

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

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

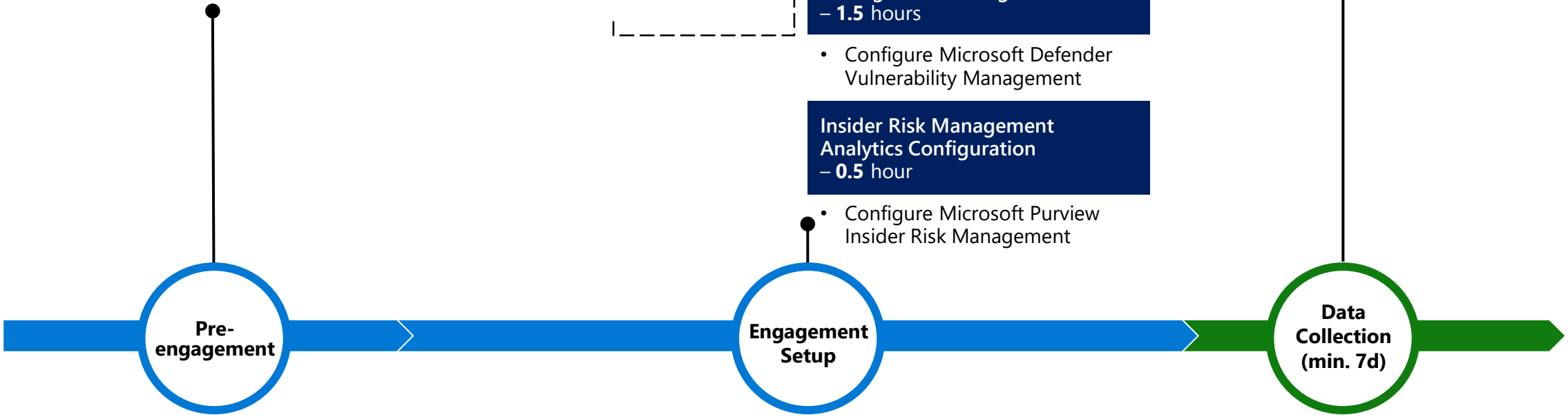
- Configure Microsoft Defender Vulnerability Management

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

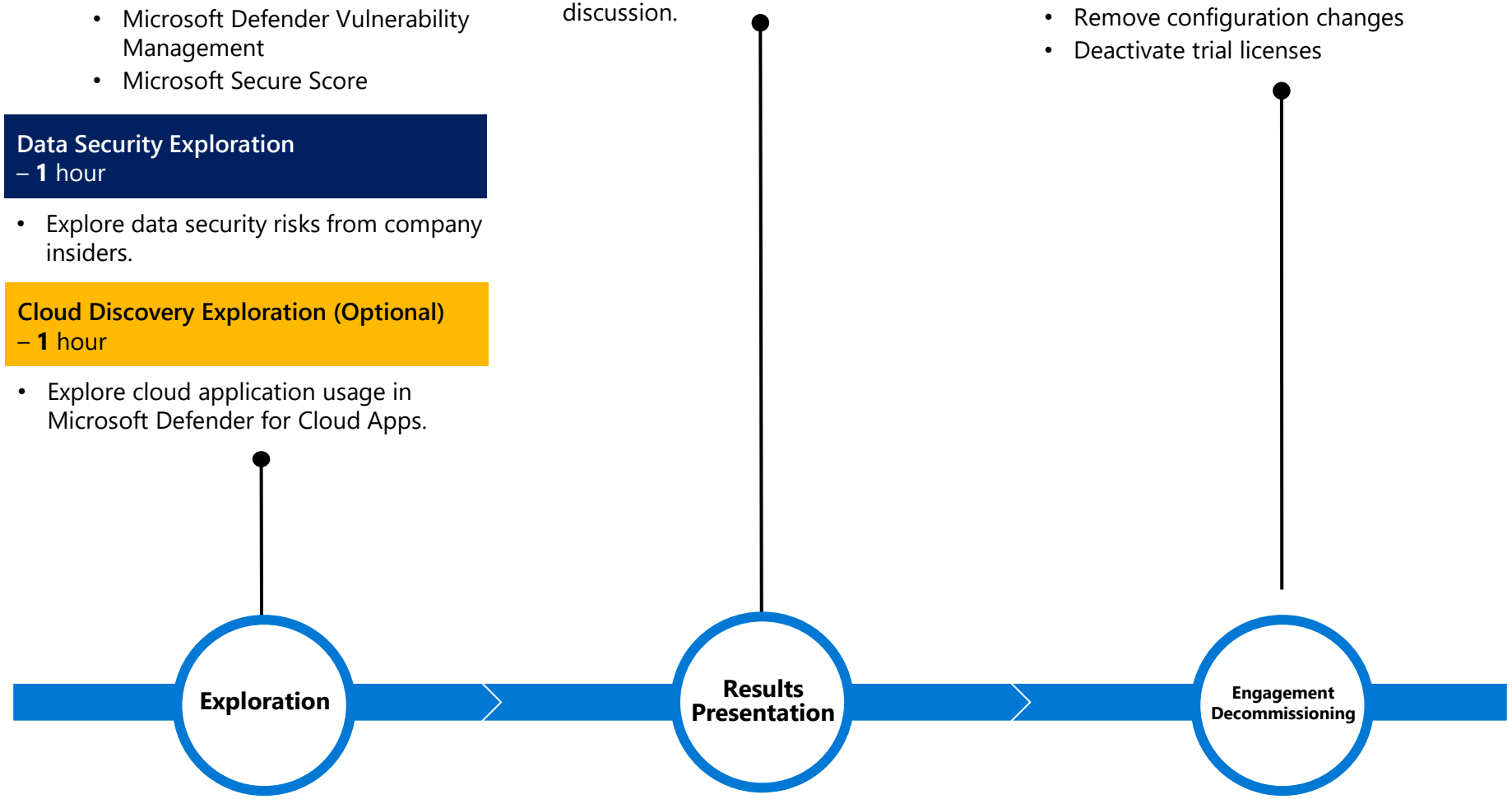
- Explore cloud application usage in Microsoft Defender for Cloud Apps.

Results Presentation
– **2** hours

- Results presentation and Next Steps discussion.

Engagement Decommissioning
– **1** hour

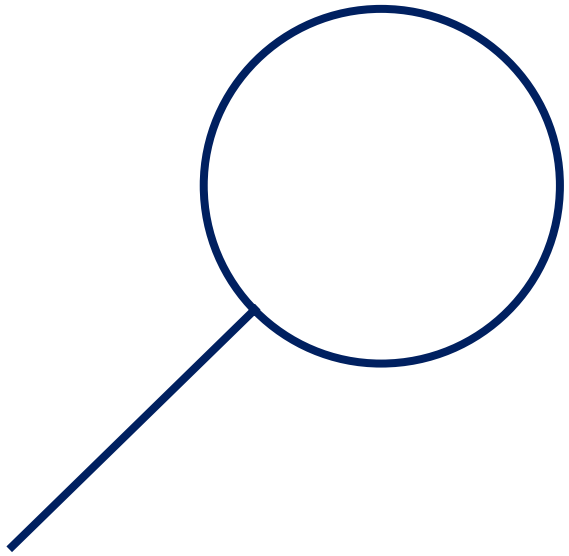
- Remove uploaded logs
- Remove configuration changes
- Deactivate trial licenses



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.

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

AKINSIT

Next Steps

Schedule your assessment today!

https://www.akinsit.com/contact