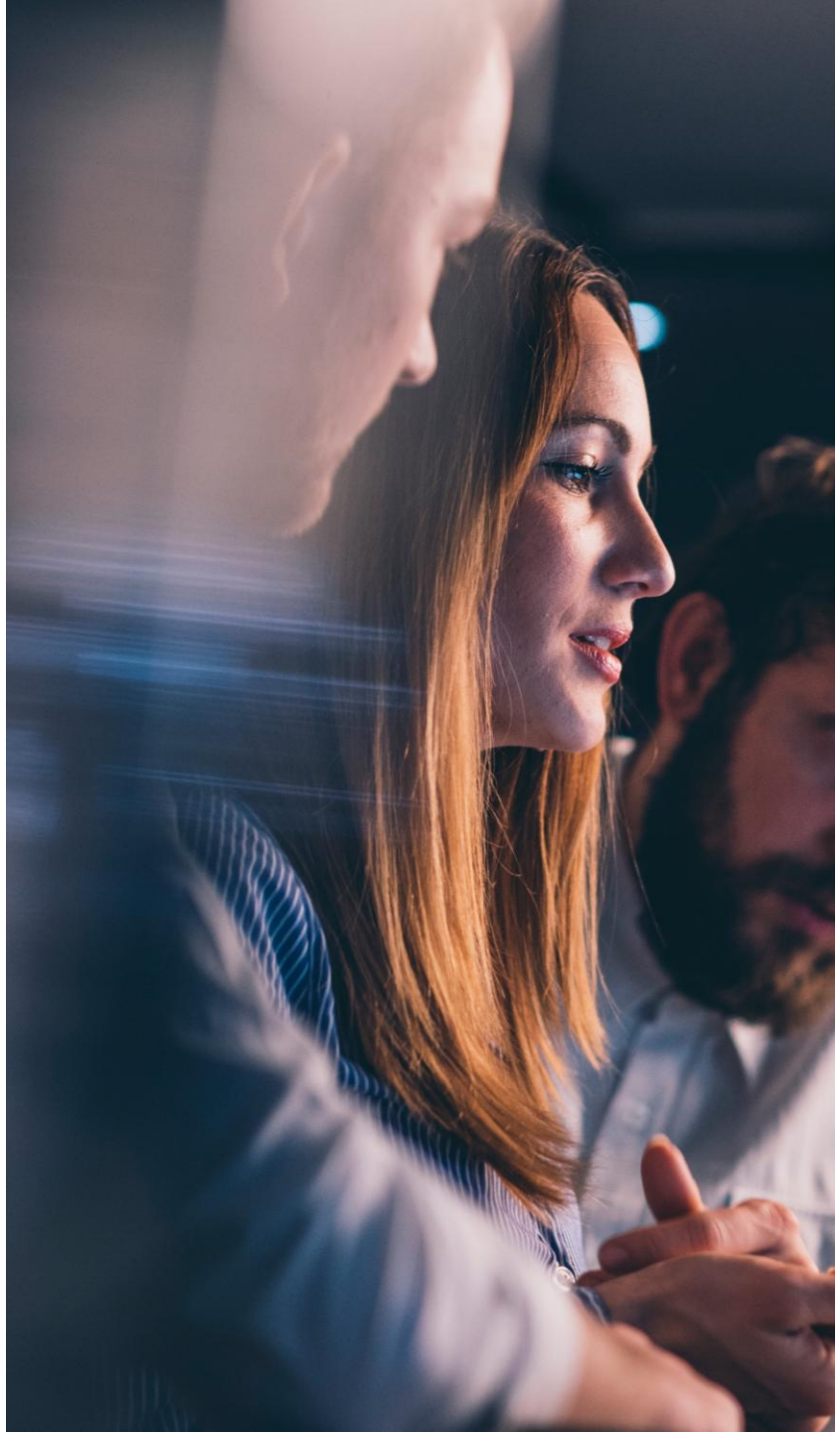
THREAT PROTECTION ENGAGEMENT

MOVING BUSINESS THROUGH TECHNOLOGY



INTRODUCING THE THREAT PROTECTION ENGAGEMENT

Discover threats and vulnerabilities to Microsoft cloud and on-premises environments

WHAT WE'LL DO DURING THE ENGAGEMENT

Analyze requirements and priorities for a Unified Security Operations Platform with Microsoft Defender XDR and Microsoft Sentinel

Define scope & deploy selected Microsoft security solutions in production environment.

Discover threats to cloud and on-premises and across email, identity, servers, endpoints and data.

Discover and prioritize vulnerabilities and misconfigurations across the organization.

Plan next steps on how to work together.

AFTER THE THREAT PROTECTION ENGAGEMENT, THE CUSTOMER WILL...

- Better understand, prioritize, and mitigate potential threats.
- Better understand, prioritize, and address vulnerabilities.
- Accelerate their security journey with Microsoft.
- Have defined next steps based on their needs and objectives.

OBJECTIVES

Discover threats

Gain visibility into threats to Microsoft 365 cloud and on-premises environments across email, identity, servers, endpoints and data to better understand, prioritize and mitigate potential vectors of cyberattacks against the organization.

Discover vulnerabilities

Gain visibility into vulnerabilities to Microsoft 365 cloud and on-premises environments to better understand, prioritize and address vulnerabilities and misconfigurations across the organization.

Define next steps

As part of the engagement, we will work with the customer to define a list of next steps based on needs, objectives, and results from the Threat Protection Engagement.

THREAT PROTECTION ENGAGEMENT

PHASES AND ACTIVITIES

Pre-engagement Call

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

Engagement Questionnaire

Fill in and return the questionnaire

- Other pre-engagement preparations

Readiness (Optional)

- Threat Protection solution play pitch deck
- Modernize your SOC with Microsoft Sentinel solution play pitch deck
- Microsoft Defender XDR customer deck
- Microsoft Defender for Office 365 customer deck
- Microsoft Defender for Cloud Apps customer deck
- Microsoft Defender for Endpoint product pitch deck
- Microsoft Defender for Cloud, Security Posture Management and Defender for Servers

Kick-Off Meeting

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

Define Scope

- Finalize "Selectable Modules"
- Define and document deployment scope

Change Management (Optional)

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

General Setup

- Setup trial licenses
- Configure tenant

Mandatory Modules

- Microsoft Defender Portal
- Cloud Identity Protection

Selectable Modules

- Unified SecOps Platform
- Email Protection
- Endpoint and Cloud Apps Protection
- Server Protection
- Microsoft Copilot for Security Demonstration

* Three (3) modules must be selected and delivered. Delivery time dependent on selected modules.

THREAT PROTECTION ENGAGEMENT

PHASES AND ACTIVITIES

Cloud Discovery Log Collection

- One-time upload of cloud discovery logs *

Threat and Vulnerabilities Exploration

Threats and Vulnerabilities Exploration

- Mandatory modules
  - Microsoft Defender Portal
  - Cloud Identity Protection
- Selectable modules
  - Unified SecOps Platform
  - Email Protection
  - Endpoint and Cloud Apps Protection
  - Server Protection

Microsoft Copilot for Security Demonstration

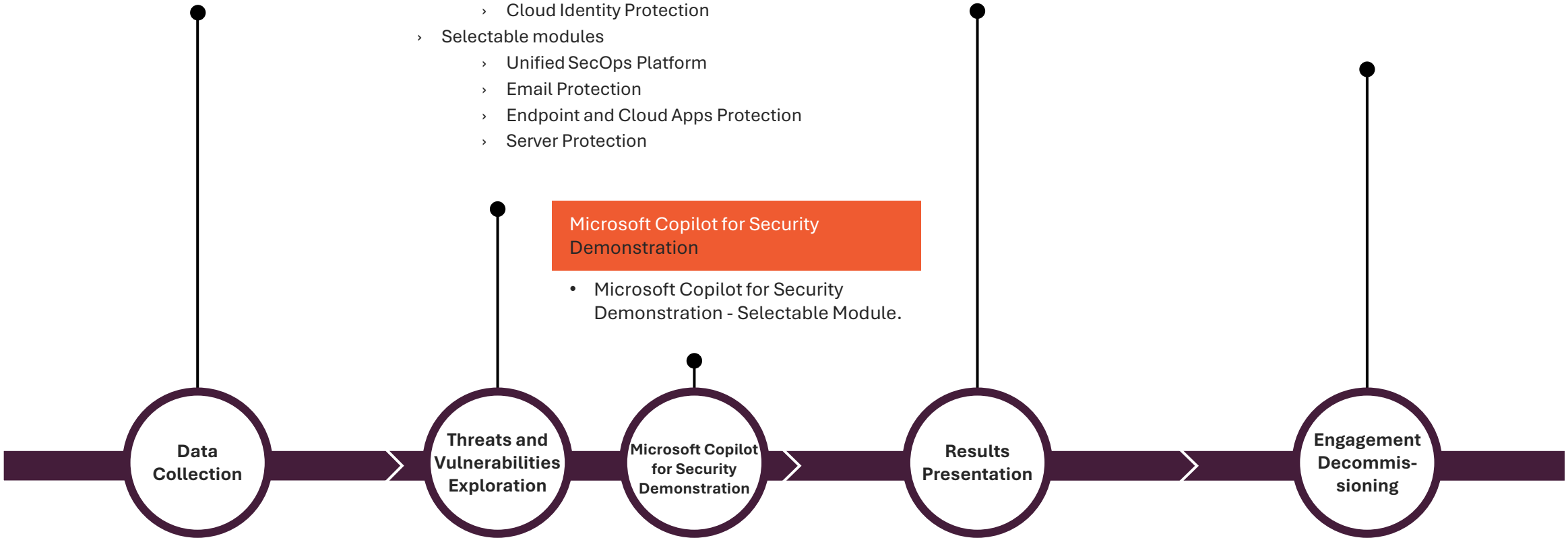
- Microsoft Copilot for Security Demonstration - Selectable Module.

Results Presentation

- Results presentation and Next Steps discussion.

Engagement Decommissioning

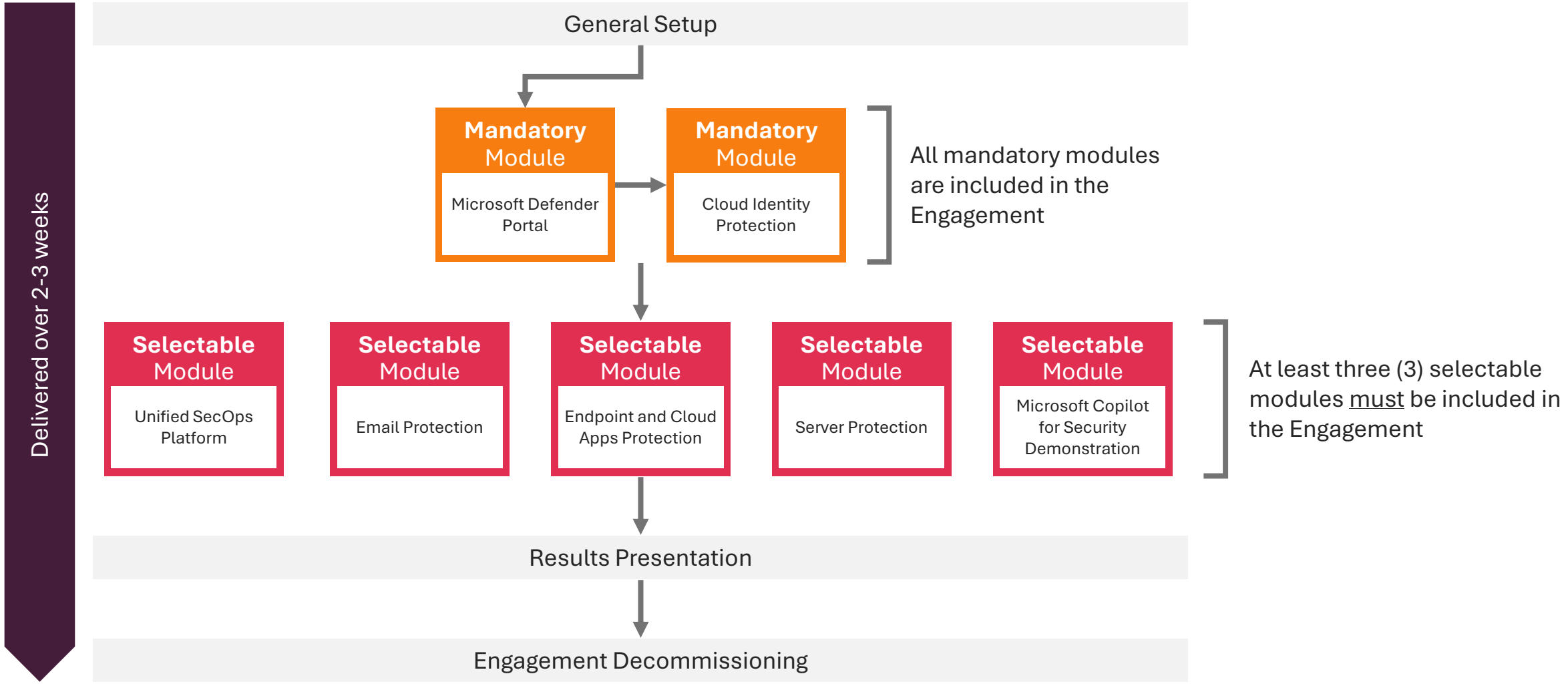
- Remove uploaded logs
- Remove configuration changes
- Deactivate trial licenses/subscription



* Unless using Microsoft Defender for Endpoint as a source of the cloud discovery data.
** Delivery time dependent on selected modules.

THREAT PROTECTION ENGAGEMENT

MODULAR DESIGN



OUTCOMES

Threat Exploration Results

Findings from the exploration of cyber security threats currently targeting the organization, as observed in this engagement.

Threat Recommendations

Maps observed threats to Microsoft 365 security products and features to mitigate impact.

Vulnerability Exploration Results

Findings from the exploration of vulnerabilities and misconfigurations, as observed in this engagement.

Vulnerability Recommendations

Guidance on how to prioritize and address vulnerabilities and misconfiguration.

OUT OF SCOPE

- Configuration of Microsoft security solutions beyond the guidance provided in the Delivery Guide
- Deep analysis (investigation) of threats found during the engagement
- Incident response
- Forensic analysis
- Technical designs or implementations
- Proof of Concept or Lab Deployment

READINESS (OPTIONAL)

Readiness is an optional phase of the Threat Protection Engagement designed to ensure that all attendees will have a basic understanding of the Microsoft Security products included as part of the engagement.

The following readiness presentations can be delivered as part of the Threat Protection Engagement:

- Threat Protection Overview
- Modernize your SOC with Microsoft Sentinel
- Microsoft Defender XDR
- Microsoft Defender for Office 365
- Microsoft Defender for Cloud Apps
- Microsoft Defender for Endpoint
- Microsoft Defender for Cloud, Security Posture Management and Defender for Servers

ENGAGEMENT SETUP

Kick-off Meeting

Introduce the Threat Protection Engagement, discuss the upcoming activities, align expectations and establish timelines.

Define Scope

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

Change Management (optional)

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

General Setup

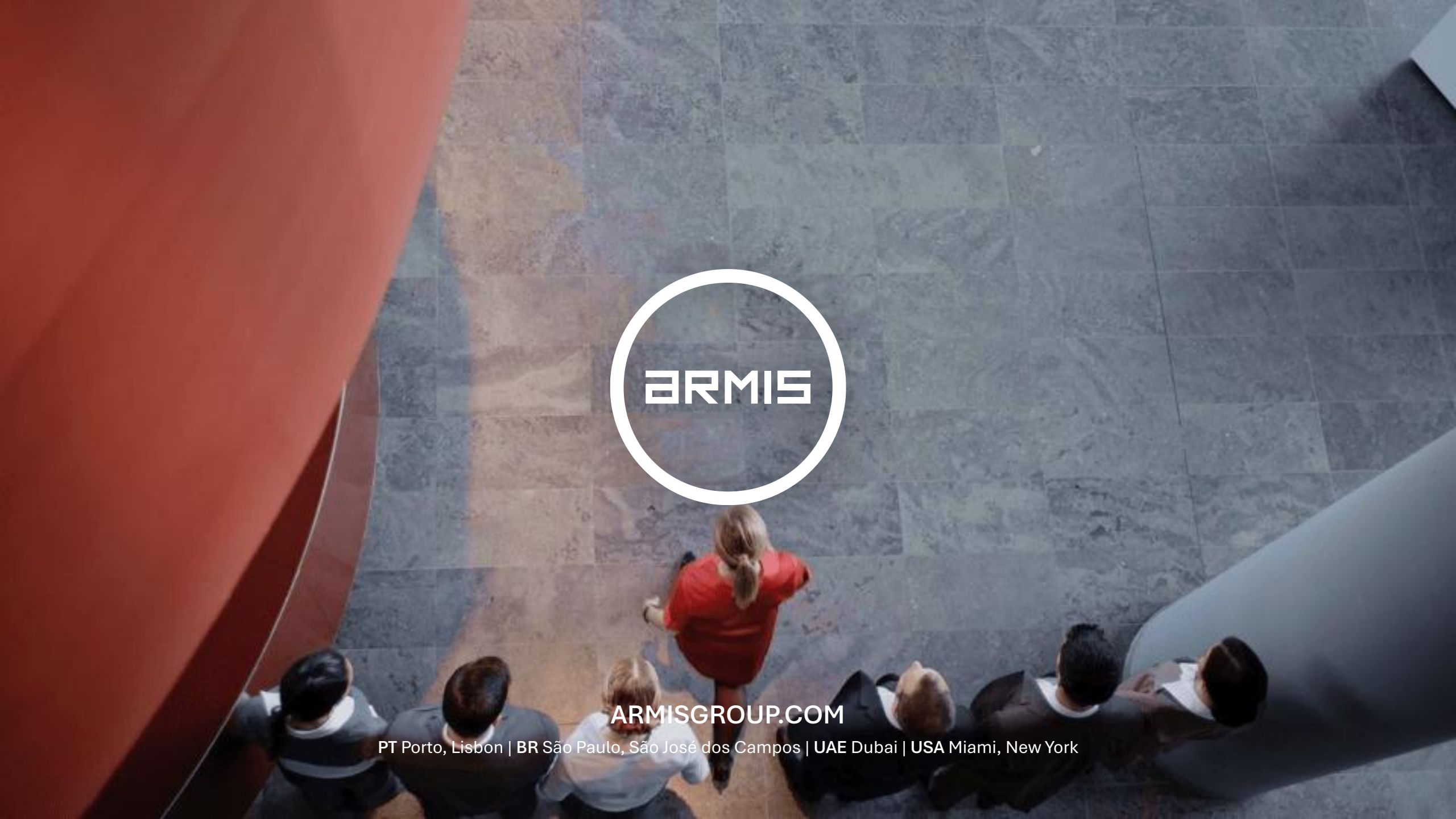
Apply engagement trial licenses and complete tenant configuration.

Mandatory Modules Configuration

Configure the mandatory modules: Microsoft Defender Portal, Cloud Identity Protection

Selectable Modules Configuration

Configure the selectable modules included in the engagement: Unified SecOps Platform, Email Protection, Endpoint and Cloud Apps Protection



ARMISGROUP.COM

PT Porto, Lisbon | **BR** São Paulo, São José dos Campos | **UAE** Dubai | **USA** Miami, New York