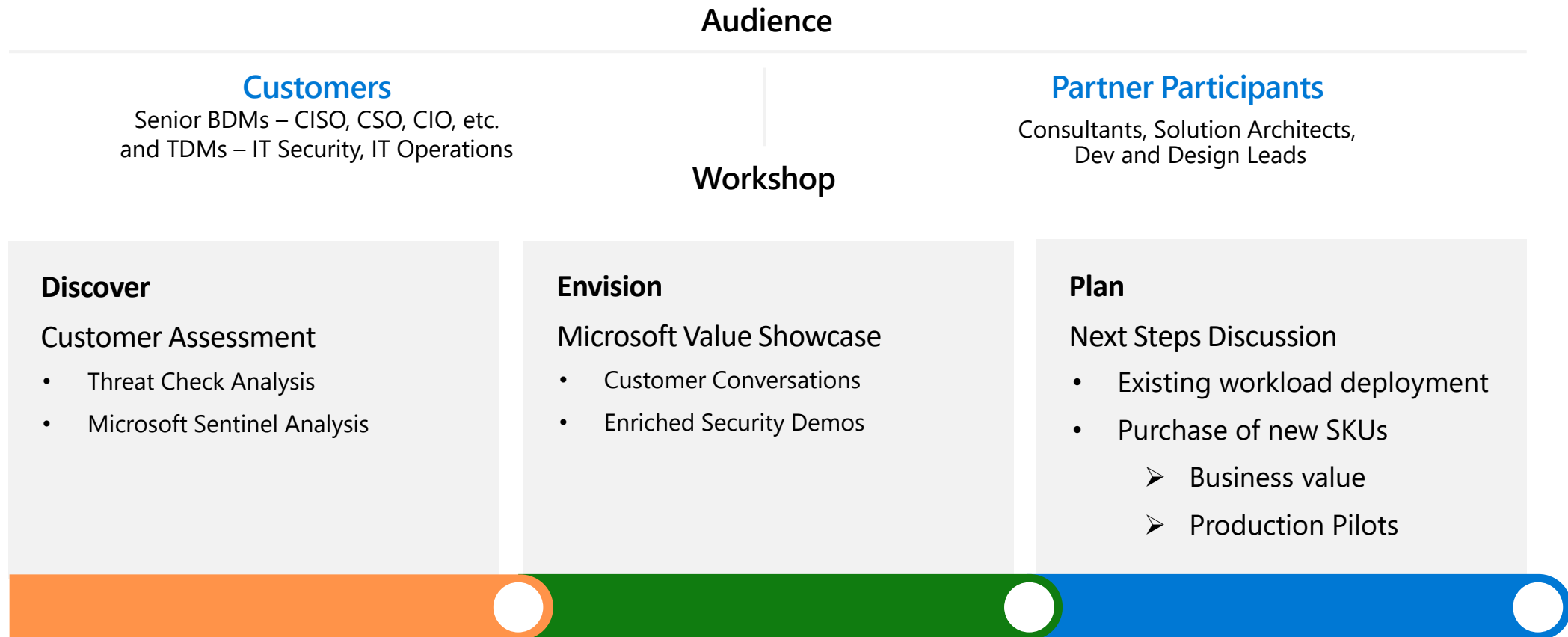# Defend Against Threats with SIEM Plus XDR

# Defend Against Threats with SIEM Plus XDR Workshop overview

Designed as a three-to-four-day engagement, the **Defend Against Threats with SIEM Plus XDR Workshop** enables partners to build intent for sales and deployment of advanced Microsoft Security workloads. The workshop uses a specialized Threat Check SKU for identifying real-time threats in a customer environment and will help define clear next steps and the best ways to mitigate risks.

Audience

Customers
Senior BDMs – CISO, CSO, CIO, etc.
and TDMs – IT Security, IT Operations

Partner Participants
Consultants, Solution Architects,
Dev and Design Leads

Workshop

Discover

Customer Assessment

- Threat Check Analysis
- Microsoft Sentinel Analysis

Envision

Microsoft Value Showcase

- Customer Conversations
- Enriched Security Demos

Plan

Next Steps Discussion

- Existing workload deployment
- Purchase of new SKUs
  - ➢ Business value
  - ➢ Production Pilots

What we'll do during the Workshop

Analyze your priorities and requirements for deployment of Security Information and Event Management (SIEM) and eXtended Detection and Response (XDR) systems
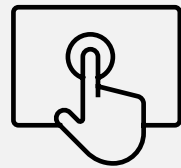
Define scope & deploy Microsoft Sentinel and Microsoft 365 Defender in production environment, integrating them with Microsoft and 3rd party solutions
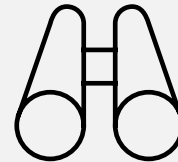
Discover threats to cloud and on-premises and across email, identity, and data and demonstrate how to automate responses
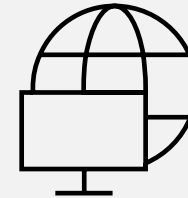
Learn about Microsoft's approach to security with an immersive experience.

Plan next steps on how we can work together.

THE PARTNER MASTERS

Defend Against Threats with SIEM Plus XDR Workshop phases and activities

Pre-engagement Call – 2 hours

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

Defend Against Threats with SIEM Plus XDR Workshop questionnaire

- Fill in and return the questionnaire
- Other pre-engagement preparations

Readiness [optional] – 1-8 hours **

- Microsoft Sentinel Overview presentation
- Microsoft 365 Defender Overview presentation
- Microsoft Defender for Office 365 Overview presentation
- Azure Active Directory Identity Protection Overview presentation
- Microsoft Defender for Identity Overview presentation
- Microsoft Defender for Cloud Apps Overview presentation
- Microsoft Defender for Endpoint and Microsoft Defender Vulnerability Management Overview presentation

Kick-Off Meeting – 2 hours

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

Define Scope – 2 hours

- Define and document deployment scope

Change Management [if required]

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

Configuration – 4-12 hours *

- Setup trial licenses & subscription
- Configure engagement tools
  - Threat Check
  - Microsoft Sentinel
  - Endpoint Protection module
  - Hybrid Identity Protection module

Hybrid Identity Protection – Complete Sensor Deployment

- Customer to complete deployment of Microsoft Defender for Identity sensors on their own after initial set deployed together with the partner

Pre-engagement

Readiness [optional]

Engagement Setup

* Effort depends on modules delivered
** Effort depends on presentations delivered

THE PARTNER MASTERS

Defend Against Threats with SIEM Plus XDR Workshop phases and activities

Cloud Discovery Log Collection – 1 hour

- Upload cloud discovery logs

Exploration and Report Generation – 3-9 hours *

- Threat Exploration
  - Threat Check
  - Microsoft Sentinel
  - Endpoint Protection module
  - Hybrid Identity Protection module
- Proactive threat hunting [optional]
  - Microsoft Sentinel
  - Endpoint Protection module
- Report Generation
  - Threat Check
  - Microsoft Sentinel
  - Endpoint Protection module
  - Hybrid Identity Protection module

Results Presentation – 3 hours

- Present and discuss results
- Record next steps

Customer Conversations – 1 hour

- Selected MS Security Conversation
- Customer Cost Savings Conversation

Microsoft Security Demos – 1 hours

- MS security experience

Next Steps Discussion – 1 hour

- Discuss next steps

Engagement Decommissioning – 2 hours

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

Data Collection

Exploration and Report generation

Workshop Day

Engagement Decommis-sioning

2-3 weeks

* Effort depends on modules delivered