MICROSOFT THREAT CHECK ASSESSMENT

Value proposition

The Microsoft Threat Check Assessment offering is designed to understand customer's security goals and objectives, identify security threats across M365 services and provide recommendations to mitigate those risks using Microsoft 365 Security tools.

Eligible workloads
- Azure AD Identity Protection, Microsoft Cloud App Security, Microsoft Defender for Office 365
- Microsoft Defender for Endpoint (Optional)
- Azure Sentinel

Customer benefits
- Quick view on your M365 environment for security related events across identity, Apps, Device & Data.
- Learn where you are in your security posture and understand the gaps.
- Understand how to mitigate security risk using Microsoft integrated security solutions.
- Microsoft 365 Defender presentation and demo.
- Integrated security customer immersion experience.
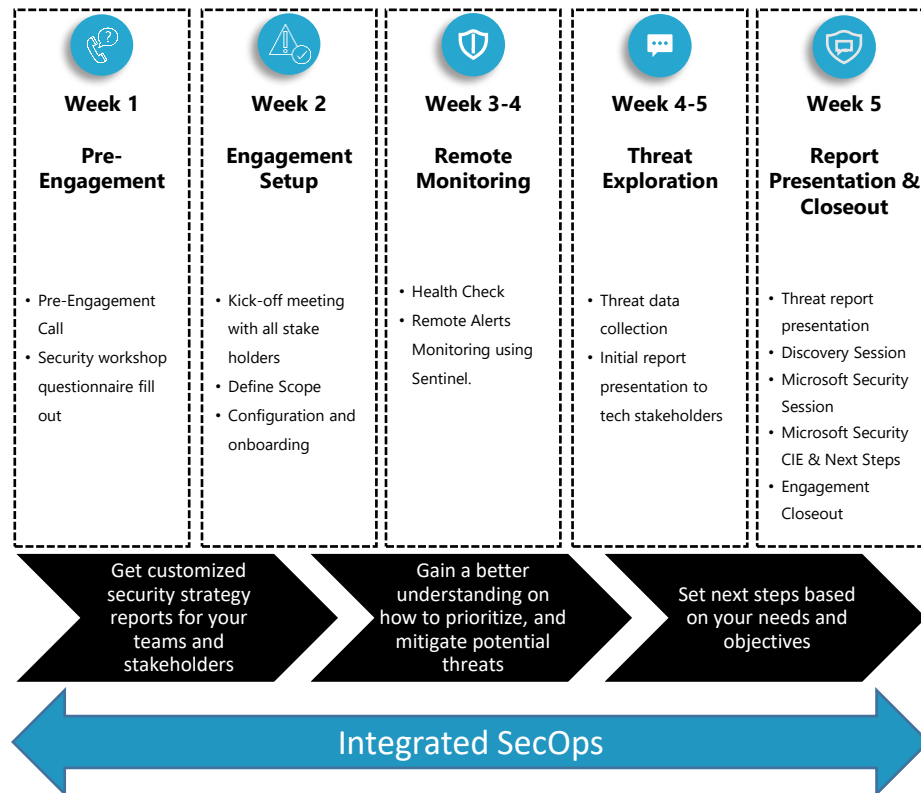- Discuss and review to embark on the end-to-end security journey with Invoke

Planning workshop offer*
- *Microsoft funding for Invoke-led PoC may be available upon request*

Invoke scope of delivery
- Invoke engineer will optionally monitor all these services remotely
- Invoke will setup a M365 Demo Lab to help you explore features and functionalities, test new capabilities, understand new security enhancements, explore deployment options and evaluate infrastructure dependencies.
- Final threat assessment report and recommendations will be submitted at the end of the engagement.

Timeline – Customer customizable agenda and timeline

Week 1	Week 2	Week 3-4	Week 4-5	Week 5
Pre-Engagement	**Engagement Setup**	**Remote Monitoring**	**Threat Exploration**	**Report Presentation & Closeout**
• Pre-Engagement Call • Security workshop questionnaire fill out	• Kick-off meeting with all stake holders • Define Scope • Configuration and onboarding	• Health Check • Remote Alerts Monitoring using Sentinel.	• Threat data collection • Initial report presentation to tech stakeholders	• Threat report presentation • Discovery Session • Microsoft Security Session • Microsoft Security CIE & Next Steps • Engagement Closeout

Get customized security strategy reports for your teams and stakeholders

Gain a better understanding on how to prioritize, and mitigate potential threats

Set next steps based on your needs and objectives

Integrated SecOps