Service Definition_

UNITE: Cybersecurity Assessment_
April 2024_
V1_

Table of contents_

1. Overview_

The Microsoft Cybersecurity Assessment is designed to provide an in-depth understanding of cybersecurity challenges and solutions. It includes a series of modules that cover various aspects of cybersecurity, such as resilience, threat acceleration, digital transformation, and critical security hygiene. Participants can expect to learn about the Microsoft cybersecurity reference architecture and gain insights into the Internet of Things (IoT) and operational technology security.

The assessment is structured into several parts, each focusing on different elements of cybersecurity. For instance, there are dedicated sections on identity and access, security operations centres, PC and mobile device security, hybrid cloud infrastructure, and software as a service. Additionally, the workshop addresses information protection and provides a comprehensive conclusion summarising the CISO Workshop approach.

Moreover, the Cybersecurity Assessment aims to help organisations identify real threats to their cloud environment, understand their security goals and objectives, and develop a strategic plan based on cybersecurity expert's recommendations. It includes practical demonstrations and actionable recommendations to mitigate identified threats, offering a holistic view of Infinity Group and Microsoft's approach to security.

2. Agenda_

The Cybersecurity Assessment helps buyers assess their security posture and risk to insider threats and includes the following components:

- A questionnaire to help analyse the buyer's environment and their current cybersecurity maturity level based on v8 of the CIS Critical Security Controls.
- A vulnerability assessment using:
    - Microsoft Defender Vulnerability Management.
    - Microsoft Secure Score.
- A data security assessment using:
    - Microsoft Purview Information Protection
    - Microsoft Purview Insider Risk Management analytics.
- An optional Cloud discovery using Microsoft Defender for Cloud.
- A list of next steps based on the buyer's needs, objectives, and results from the Cybersecurity Assessment.

3. Engagement objectives

The objectives for the Cybersecurity Assessment are:

- **Understand current cybersecurity maturity level**: Help the buyer understand their current cybersecurity maturity level using a questionnaire based on the CIS Critical Security Controls v8, providing recommendations and guidance on the next steps to improve their cybersecurity posture.
- **Discover and understand how to address vulnerabilities on clients and servers**: Help the buyer understand how to use Microsoft Defender Vulnerability Management to discover, prioritise and address vulnerabilities and misconfigurations across clients and servers within their organisation.
- **Discover and analyse cloud application usage (Optional):** Help the buyer understand their current cloud application usage using Microsoft Defender for Cloud, demonstrating how to detect and block risky applications.
- **Discover and understand risk related to data security and insider threats:** Help the buyer understand the possible sensitive information that exists in their Microsoft 365 environment and the types of actions users are performing on that data that could be seen as potentially risky activities.
- **Define next steps:** The buyer will work together with the delivery resource to define a list of next steps based on their needs, objectives, and results from the Cybersecurity Assessment.

4. Engagement scope

In scope

The standard scope of this part of the engagement includes:

- Analysis of buyer questionnaire.
- Deployment of Cybersecurity Assessment Microsoft 365 trial licenses in the buyer tenant, if required.
- Configuration of the Microsoft products used as part of the engagement, as per guidance provided in this document.
- Remediation of potential technical issues during the deployment.
- Scanning and assessment of vulnerabilities on on-premises Windows servers and clients within a single Active Directory domain.
- Exploration of vulnerabilities to discover and prioritise vulnerabilities and misconfigurations.
- Exploration of the sensitive information identified in the Microsoft 365 environment using out-of-the-box Microsoft Purview capabilities.
- Optional analysis of cloud applications used by users in the buyer environment through the Cloud Discovery part of Microsoft Defender for Cloud Apps, based on either Microsoft Defender for Endpoint, if already deployed by the buyer, or based on a one-time manual upload of logs from a single on-premises perimeter security device such as a firewall or proxy server.
- Decommissioning of configuration and licenses at the end of engagement.

Out-of-scope

The standard scope of this part of the engagement excludes anything that was not put in scope, in particular:

- Configuration of Microsoft products beyond the guidance provided in this document.
- Scanning and assessment of vulnerabilities on machines outside of corporate on-premises networks.
- Automatic upload of firewall or proxy server logs to Microsoft Defender for Cloud Apps (through Log Collector).
- Analysis (investigation) of security incidents.
- Forensic analysis.
- Technical designs or implementations.
- Explore E5 Security workshop (optional)

5. Buyer requirements

Successful delivery of the engagement is dependent on the buyer's involvement in all aspects of the engagement. The buyer must ensure that accurate and complete information is provided in a timely fashion as needed, that appropriate resources are committed, and that any activities are completed in a timely and effective manner.

The buyer will need to perform the tasks, provide the resources, and take ownership of the following activities:

- The buyer will need to provide adequate access to the necessary personnel needed to successfully complete the engagement, including:
    a) A buyer project manager responsible for the overall coordination and for scheduling logistics.
    b) IT object owners for identity and security during all phases of the assessment.
    c) An Executive Sponsor.
- The buyer will need to provide one or more virtual or physical machines to be used by the Microsoft Defender Vulnerability Management scanner.
- The buyer will provide the following to the delivery resource:
    - Access to any relevant documentation.
    - Network connectivity, adequate workspace, parking permits, building access, and appropriate identification badges within the first day if you are planning to deliver the engagement onsite.
    - Appropriate-sized room with whiteboard and projector for knowledge transfer sessions.

6. Recommended resources

Recommended buyer resources
Executive Sponsor

- Owns the business case.
- Keeps project aligned with organisation's strategy and portfolio direction.
- Governs project risk.
- Focuses on realisation of benefits.
- Provides assurance.
- Suggested candidates: CSO, CISO, CEO, CFO, CIO, CRO or CTO.

We recommend making sure the executive sponsor participates in the following activities:

- Pre-engagement Call.
- Results Presentation and Next Steps Discussion.

Architects

- IT
- Security

- Network
- Server Infrastructure
- Identity

We recommend making sure the Architects participate in the following activities:

- Pre-engagement Call.
- Prepare, Send and Review the Cybersecurity Assessment Questionnaire
- Engagement Setup and Scope Definition Meeting.
- Change Management (Optional).
- Vulnerabilities Exploration.
- Data Security Exploration.
- Results Presentation and Next Steps Discussion.

Administrators

- Security
- Network
- Server Infrastructure
- Identity
- Microsoft 365 and Azure Tenant Administrators

We recommend making sure the Administrators participate in the following activities:

- Pre-engagement Call.
- Engagement Setup and Scope Definition Meeting.
- Change Management (Optional).
- General Configuration.
- Microsoft Defender Vulnerability Management Configuration.
- Insider Risk Management Analytics Configuration.
- Vulnerabilities Exploration.
- Data Security Exploration.
- Results Presentation and Next Steps Discussion
- Engagement Decommissioning.

We recommend making sure Security Operations participate in the following activities:

- Engagement Setup and Scope Definition Meeting.
- General Configuration.
- Microsoft Defender Vulnerability Management Configuration.
- Insider Risk Management Analytics Configuration.
- Vulnerabilities Exploration.
- Data Security Exploration.
- Results Presentation and Next Steps Discussion
- Engagement Decommissioning

We do *IT* differently_

0345 450 4600
infinitygroup.co.uk
hello@infinitygroup.co.uk

HQ:
The Coach House
Spencer Mews
Tunbridge Wells
Kent TN1 2PY

London:
6th Floor
2 Kingdom Street
Paddington
London
W2 6BD