

## Threat Protection Engagement

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

Do you know how many phishing attacks your organisation has received? If employees are using the right password protocols? Whether personal data is being exposed?

In short, is your organisation's cloud environment as secure as you think it is?

### Improve your security posture with a Threat Protection Engagement.

Organisations today are managing a growing volume of data and alerts while dealing with tight budgets and vulnerable legacy systems. Get help achieving your broader security objectives — and identify current and real threats.

We can help you develop a strategic plan customised for your organisation, providing validation from Microsoft security experts.

You'll gain visibility into immediate threats across email, identity, and data, plus clarity and support on how to remediate vulnerabilities and upgrade your security posture for the long term.



### Key engagement deliverables:



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



**Discover vulnerabilities:** Gain visibility into vulnerabilities to Microsoft 365 cloud and on-premises environments to better understand, prioritise and address vulnerabilities and misconfigurations across the organisation.



**Actionable recommendations:** Actionable recommendations to help immediately mitigate the identified threats and discovered vulnerabilities.



**Next steps:** We'll work with you to define a list of needs, objectives, and strategy, based on the results from the Threat Protection Engagement.

## Engagement structure:



### **Pre-engagement scoping call:**

Introductions, expectation setting, overview, and completion on engagement questionnaire.



**Readiness (optional):** Ensuring your organisation has a basic understanding of the Microsoft security products included in the engagement, such as Defender XDR, Sentinel and more.



**Engagement setup:** Kick-off meeting, define and agree engagement scope, select optional modules, and agree change management processes. Mandatory and selectable modules configuration.



**Data collection:** Detection of threats, analyse vulnerabilities and any misconfigurations in your environment, upload of Cloud Discovery logs.



**Threats and vulnerabilities exploration:** Gain visibility into threats and vulnerabilities via reports, and explore findings.



**Results presentation:** We'll present all findings and recommendations from the engagement, discussing the strategic and technical next steps and agree any follow-up engagements needed.



**Engagement decommissioning or extension (optional):** Removal of uploaded logs and any trial licences used.

**Length of engagement approx. 3-4 weeks.**

## Threat protection engagement modules:

### Mandatory Modules

- Microsoft Defender Portal
- Cloud Identity Protection

All mandatory modules are included in the engagement.

### Selectable Modules

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

At least three (3) selectable modules must be included in the engagement.

## Who should attend:

The engagement is intended for security decision-makers such as:

- Chief Information Security Officer (CISO)
- Chief Information Officer (CIO)
- Chief Security Officer (CSO)
- IT Security Architects
- IT Security Administrators
- IT Security Operations (Sec Ops)

## Become greater with Kocho

Our mission is to take your organisation on a journey of secure transformation.

Are you ready to get started? Talk to us today.

→ [Contact us](#)

## About Kocho

At Kocho, we connect users and devices securely to Microsoft cloud services.

We believe greatness lies in everyone, and we offer a unique blend of professional, and managed IT solutions, to help ambitious companies realise their full potential.

**Kocho. Become greater.**

**1** of **7**  Microsoft  
global partners with all  
Security Accreditations

Member of  
Microsoft Intelligent  
Security Association

 Microsoft Security

 Microsoft Verified  
Managed XDR Solution

 Microsoft  
Solutions Partner  
Security

 Microsoft  
Solutions Partner  
Modern Work

 Microsoft  
Solutions Partner  
Data & AI (Azure)

 Microsoft  
Solutions Partner  
Infrastructure (Azure)

 Microsoft  
Solutions Partner  
Digital & App Innovation (Azure)

 Microsoft  
Specialisation

Cloud Security  
Threat Protection  
Modernise Endpoints  
Infra & Database Migration  
Identity & Access Management  
Information Protection & Governance

