Overview:

With the transition to the cloud, there is a notable rise in security incidents involving cloud platforms and services. Microsoft 365 is highly targeted due to its popularity and the valuable hosted data. Compromising Microsoft 365 tenants allows attackers to remotely access sensitive data in the cloud without having to penetrate the corporate perimeter.

- Weak or legacy authentication mechanisms
- Security controls which have not been optimally configured
- Accounts with privileged access levels
- Accounts with weak passwords or those that do not require multifactor authentication

Our Approach:

This Techhub PS security assessment evaluates common Microsoft 365 authentication platforms and access controls across six core focus areas:

- Security architecture and hardening
- Identity and access management
- Visibility
- Data protection
- Disaster recovery
- Threat detection and response

WHAT YOU GET

AD Synchronization Services Evaluation
Recommendations For Security Hardening
Synchronization Accounts & Permissions
Synchronization Services Setup & Location
High Availablity Synchronization Tools
Services Microconfigurations (OneDrive, SharePoint, Exchange, Etc.)

ASSESSMENT DURATION

The O365 security assessment typically takes four weeks, consisting of four phases plus one optional phase.
Techhub PS perform the following activities

Documentation Review (0.5 week)
Includes an offsite review of migration strategies, email design and architecture documentation, hardening documentation, logging standards and Mobile Device Management (MDM) configurations as they relate to accessing an M365 tenant.

Optional Security Testing (0.5 week)
A remote security configuration test of the M365 tenant with the goal of identifying legacy portals, misconfigured applications and related infrastructure (such as ADFS Servers), weak user credentials and other ways to bypass implemented security controls.

Reporting (2 week)
A report that details practical technical recommendations to harden the M365 tenant, enhance visibility and detection and improve processes to reduce the risk of compromise for the cloud tenant and related infrastructure.

Configuration Review (1 week)
A thorough configuration review of the M365 tenant to ensure that security configurations are optimized in accordance with hardening, security, and protective guidance.

Onsite Workshops (1 week)
A series of onsite workshops for each core focus area in collaboration with key client stakeholders.

Deliverables
At the completion of the engagement, Techhub PS provides a detailed report that includes:

A snapshot of the existing O365 tenant security configuration.
Specific O365 security best practices to align with current configurations and operational processes.
Practical recommendations for enhancing visibility and detection.
Prioritized and detailed recommendations for further hardening the security posture of the O365 tenant.

Assessment Objectives

Understand cloud security objectives and requirements
Gain a common understanding of cloud security objectives and requirements

Microsoft 365 security readiness
Provide guidance, recommendations and best practices on how to successfully implement Microsoft 365 security features

Create an Microsoft 365 security roadmap
Provide a prioritized and actionable Microsoft 365 security roadmap. Map Microsoft 365 security capabilities to customer security objectives and requirements