SECURE IMPACT

SERVICES

Microsoft 365 Security Assessment

Summary

Is your Microsoft 365 world secure? Dynamic cloud environments like M365 pose unique security challenges which cannot be addressed with traditional penetration testing methods. Frequently overlooked by organisations and pentesters alike, this causes blind spots and vulnerabilities, potentially exposing you to heightened cyber risks. Our specialised M365 Security Assessment dives deep into cloud concepts, beyond ordinary pentesting, giving you clear insight to your posture.

How is the SI approach different?

With the rapid pace of adoption in Software as a Service, security testing is racing to keep up. As a result, many offerings in the industry are poorly defined and executed. Methodologies developed for traditional, on-premise environments are often incorrectly applied to the cloud, where doing so serves only to validate your cloud service provider's security measures. With most security incidents, it is the *configuration* that leads to vulnerability, with the security of the underlying infrastructure being the responsibility of the service provider. The key is to test the security of your *implementation* of the services based on the **shared responsibility model** adopted by all major global cloud platforms, and relevant to all cloud services.

Cloud brings new patterns and architectures, with identity being of critical importance to security - your 'new perimeter'. If you are new to cloud and have a hybrid environment, penetration testing will be critical for you, as a mixed or hybrid identity environment presents new paths for attackers, with a variety of Single Sign-On technologies and implementations often being at the heart of authentication and authorisation.

For meaningful assessment of your specific cloud environment, this requires an experienced team, well-versed in the risks inherent in this new landscape, with expertise of how to navigate them in the most cost-effective way for you.

Once you have made the best efforts to address these areas from the inside, it is time to target the organisation from the outside.

How we can help

SI can give you assurance that your configuration is protecting you the way you expect it to. We do this by assessing the following:

- Microsoft EntraID, formerly Azure AD, including users, groups, applications, external identities, user experiences and hybrid management.
- EntraID Protection, including conditional access, authentication methods, MFA, password reset flows and risky activities.
- Microsoft 365 Defender, including email & collaboration, cloud apps.
- Exchange Online.
- Microsoft InTune.
- EntraID Governance.
- Microsoft Purview, RMS and AIP services, including Data Loss Prevention and Information Protection.
- SharePoint sites, policies and settings.
- Microsoft Teams, with a particular focus on external collaboration.
- Microsoft Fabric and Graph API.

Our Process

We leverage the latest tools and techniques to assess your cloud posture - what you use and how is it configured – to identify likely or potential weaknesses. We take this baseline understanding of your cloud configuration and use it to inform offensive testing activities; emulating the role and mindset of a skilled adversary.

We use Open-Source Intelligence techniques (OSINT), risk and modelling exercises to highlight logical vulnerabilities in your configuration and potential avenues for attack. We then verify your configuration by attempting to subvert it, using everything we have learned during the earlier phases to confirm that the measures you have in place hold up against real-world attacks, chaining together vulnerabilities where possible, to understand your resilience against more oblique attack vectors.

During testing, our consultants will be in frequent communication to report any high-risk findings, as well as collaborate on the most effective avenues of assessment and to discuss your detection and response measures where necessary.

Following the engagement phase, we provide a comprehensive report containing high-level summaries and strategy recommendations for the board-level audience, as well as a rigorous technical details section giving accurate evidence and reproducible steps, supported by technical remediations and further reading.

Service Options

Rapid M365 Assessment

- **One day assessment at £1,250**
- **Rapid insights to vulnerabilities**
- **Tailored recommendations**

Extensive M365 Assessment

- **Three to five days at £1,250/day**
- **Comprehensive security insights**
- **Thorough evaluation and learnings**
- **Tailored recommendations**
- **Comprehensive report**