CrowdStrike Services

TRIMARC

CROWDSTRIKE

Data Sheet

SECURITY ASSESSMENT FOR MICROSOFT CLOUD

Enhance the cybersecurity posture of your Microsoft Cloud environment

CLOUD MISCONFIGURATIONS ARE THE ROOT CAUSE OF MANY SECURITY BREACHES

Hackers constantly try to exploit ineffective cloud configuration settings in an attempt to gain access to data and disrupt workloads. Common misconfigurations in Microsoft Office 365 or Azure Active Directory (Azure AD) continue to be the root cause of many security breaches.

ENHANCE THE SECURITY OF YOUR MICROSOFT CLOUD ENVIRONMENT

A Security Assessment for Microsoft Cloud provides actionable insights into your security misconfigurations and deviations when compared to recommended cloud security architecture settings and best practices. The assessment will identify any misconfigurations with specific focus on Administration and Security Controls within your Office 365 and Azure AD environments.

The Administration review provides guidance around how the environment is currently managed and provides recommendations to enhance the level of security administration. The assessment team also helps identify how to best leverage existing Microsoft Cloud subscriptions as well as additional beneficial security controls available with other service subscriptions as appropriate.

The output of the assessment is a report that includes the recommendations needed to improve the security posture of your Microsoft Cloud environment.

KEY BENEFITS

Comprehensive review of your Microsoft Cloud environment with prioritized, actionable recommendations to enhance your security posture

Better protection and reduced risk for your cloud infrastructure and workloads

KEY SERVICE FEATURES

A Security Assessment for Microsoft Cloud is a partner-delivered service from Trimarc. The assessment provides an in-depth security analysis of the Azure AD and Microsoft Office 365 tenant, and focuses on the most important security configuration controls, including: administration, access controls and key security features. The assessment identifies issues in the environment that attackers could leverage to access data, escalate permissions and establish persistence. Trimarc reviews the Microsoft Cloud configuration using a proprietary Trimarc toolset and the Microsoft Cloud web portal. The assessment includes a review of your:

- Current tenant configuration
- Administration
- Privileged roles and accounts
- Azure AD PIM configuration (if applicable)
- Azure AD applications and permissions
- Azure AD multifactor authentication (MFA) configuration
- Conditional access
- Azure AD Connect configuration (based on tenant data)
- Exchange Online

ABOUT TRIMARC

Trimarc is a professional services company that helps organizations secure their Microsoft platform, both on-premises and in the cloud. Trimarc is on a mission to help organizations better secure their critical IT infrastructure by focusing on a "reality-based security model" which targets attacker tactics and how to best stop them. Trimarc identifies security issues in an organization that attackers could exploit to fully compromise the environment and provides custom recommendations to effectively mitigate these issues.

CONTACT CROWDSTRIKE

CrowdStrike: **We stop breaches.**

Learn more: **www.crowdstrike.com/services/**

Email: **services@crowdstrike.com**

Request information: **click here**

WHY CROWDSTRIKE PARTNERS WITH TRIMARC

CrowdStrike has established an ecosystem of trusted partners to deliver expertise and capacity in key areas of cybersecurity.

Deep Microsoft expertise: Trimarc brings deep expertise and seasoned consultants with hands-on experience in Microsoft Cloud Security architecture.

In-depth security analysis: The key differentiator and driving force in the assessment is industry-leading security research, some of which is not public knowledge.

Leading security research: Trimarc has been researching Azure AD and Microsoft Office 365 security since 2016.