CrowdStrike Services helps organizations determine if their Microsoft Office 365 email system has been compromised.

Business Email Compromises (BECs) are a growing problem across all industries, impacting companies both large and small. Threat actors, such as Nigerian Confraternities, are the spearhead of this genre of cyber fraud, triggering losses that run into the billions of dollars. The result? Organizations are struggling to know if their corporate email systems have been compromised.

CrowdStrike® Services Business Email Compromise Assessment can quickly identify ongoing or past attacker activity in your organization’s Microsoft Office 365 environment. The assessment covers a full gamut of tactics, techniques and procedures (TTPs) used by BEC threat actors. CrowdStrike hunts for BEC threat actor TTPs using proprietary threat intelligence — hunting for the use of anomalous client types or login locations, identification of malicious attachments, spoofed sender addresses or the use of unauthorized mail transfer agents (MTAs) and much more. Combined with applying powerful analytical techniques, CrowdStrike is able to swiftly identify actions of intruders in your Microsoft Office 365 environment. The assessment delivers detailed mailbox audit log forensics enabling appropriate triage and remediation actions, as well as providing recommendations to enhance the security posture of your corporate email environment going forward.

CrowdStrike’s Business Email Compromise Assessment (BECA) provides the following benefits:

- Quickly determines if a corporate email system has been compromised by attackers by proactively hunting for on-going or previous BEC activity in the environment.
- Identifies misconfigurations and poor security practices within the corporate email system to expose the risk of BEC.
- Evaluates whether security and configuration best practices are being followed and provides recommendations for improvement.
- Provides the full context of how an attacker gained access and compromised the environment.
- Employs proven tools and methodology that facilitate significantly faster, more cost-effective and accurate investigations of BEC.

CrowdStrike Services
1. RISK REDUCTION

- CrowdStrike determines whether you are a victim of a BEC currently or have been in the past within your Microsoft Office 365 mail environment, enabling swift triage and remediation actions.
- The Services team determines if a BEC has led to the theft of data, money or intellectual property against the organization, employees or partners.
- CrowdStrike gets you ahead of issues by proactively hunting for signs of BEC within your environment.

2. COST EFFECTIVENESS

- CrowdStrike tools and methodology facilitate significantly faster and more cost-effective and accurate investigations.
- Early and proactive identification of attacker activity can impact the financial loss and reputational impact of a BEC.

3. ACTIONABLE FINDINGS

- The CrowdStrike Services team identifies misconfigurations and poor security practices within the Microsoft Office 365 environment, allowing stakeholders to take appropriate remediation actions.
- CrowdStrike offers technical and operational recommendations that will enhance your security posture going forward.

ABOUT CROWDSTRIKE SERVICES

CrowdStrike Services equips organizations with the protection and expertise they need to defend against and respond to security incidents. Leveraging the cloud-delivered CrowdStrike Falcon® platform — next-generation endpoint protection, cyber threat intelligence gathering and reporting operations, and a 24/7 proactive threat hunting team — the CrowdStrike Services security team helps customers identify, track and block attackers in real time. This unique approach allows CrowdStrike to stop unauthorized access faster and prevent further breaches. CrowdStrike also offers proactive services so organizations can improve their ability to anticipate threats, prepare their networks, and ultimately stop breaches.

Learn more at www.crowdstrike.com
Email: services@crowdstrike.com