SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection and Response Services for M365D

Credential Email Phishing Attack

KEY BENEFITS

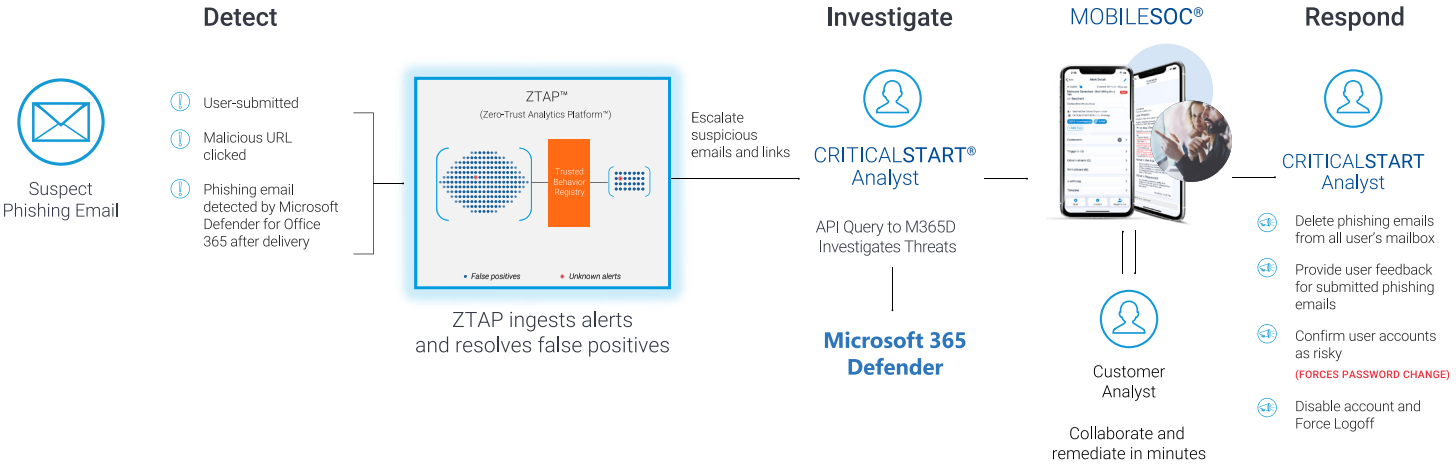
- ✓ Minimize risk and reduce exposure from email threats
- ✓ 24x7x365 coverage with investigation and response for user-reported phishing
- ✓ Deep investigation with additional email phishing analysis
- ✓ Supports your Security Awareness Training Program

Email phishing attacks are one of the fastest growing attack vectors to harvest user credentials – its estimated that 90% of cloud data breaches[1] can be attributed to human error. Successful attacks expose your organization to data breaches through standard user account access methods.

Solution

Critical Start MDR Services for Microsoft 365 Defender (M365D) provide email threat detection, investigation, and remediation options for user submitted email phishing. The Critical Start Security Operations Center (SOC) leverages the Microsoft 365 Defender security suite to detect and disrupt email threats.

How it works



Individual alerts from multiple Microsoft systems are ingested into ZTP™, our Zero Trust Analytics Platform™, where false positives are automatically resolved. Email that remains suspicious are escalated to our SOC for deeper human-led investigation and remediation.

Our pre-attack response and post-compromise activities are to:

- Remove suspicious email from the user's inbox and your entire Exchange Online environment
- Force password change
- Revoke user session token
- Disable the user's Azure Active Directory (AAD) account and logoff all "logged in sessions"
- Isolate the host

For more information: www.criticalstart.com

CRITICALSTART®

 [1] https://www.techradar.com/news/90-percent-of-data-breaches-are-caused-by-human-error