SOLUTION QUICK CARD

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

Advanced Anti-Phishing Service

KEY BENEFITS

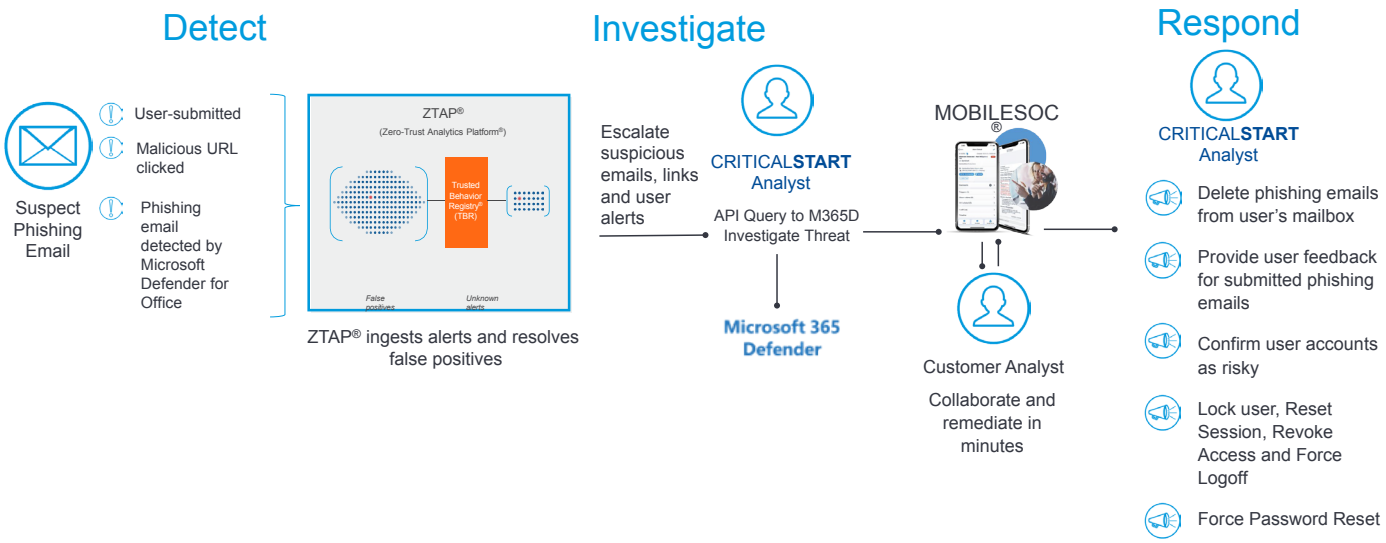
- ✓ Minimize risk and reduce exposure from email threats
- ✓ 24x7x365 coverage with investigation and response for detected and user-reported phishing
- ✓ Deep investigation with additional email phishing analysis
- ✓ Supports your Security Awareness Training Program

Email phishing attacks are one of the fastest growing attack vectors to harvest user credentials – it is estimated that 36% of breaches[1] can be attributed to phishing attacks. 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 phishing threat detection, investigation, and remediation options for detected and 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 ZTAP®, 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:

- Delete phishing emails from user's mailbox
- Provide user feedback for submitted phishing emails
- Confirm user accounts as risky
- Lock user, Reset Session, Revoke Access and Force Logoff
- Force Password Reset

[1]https://www.verizon.com/business/en-gb/resources/reports/dbir/