SOLUTION QUICK CARD

CRITICAL**START**® Managed Detection & Response Services for Microsoft Defender XDR

Attacks Against Data in Cloud Applications

KEY BENEFITS

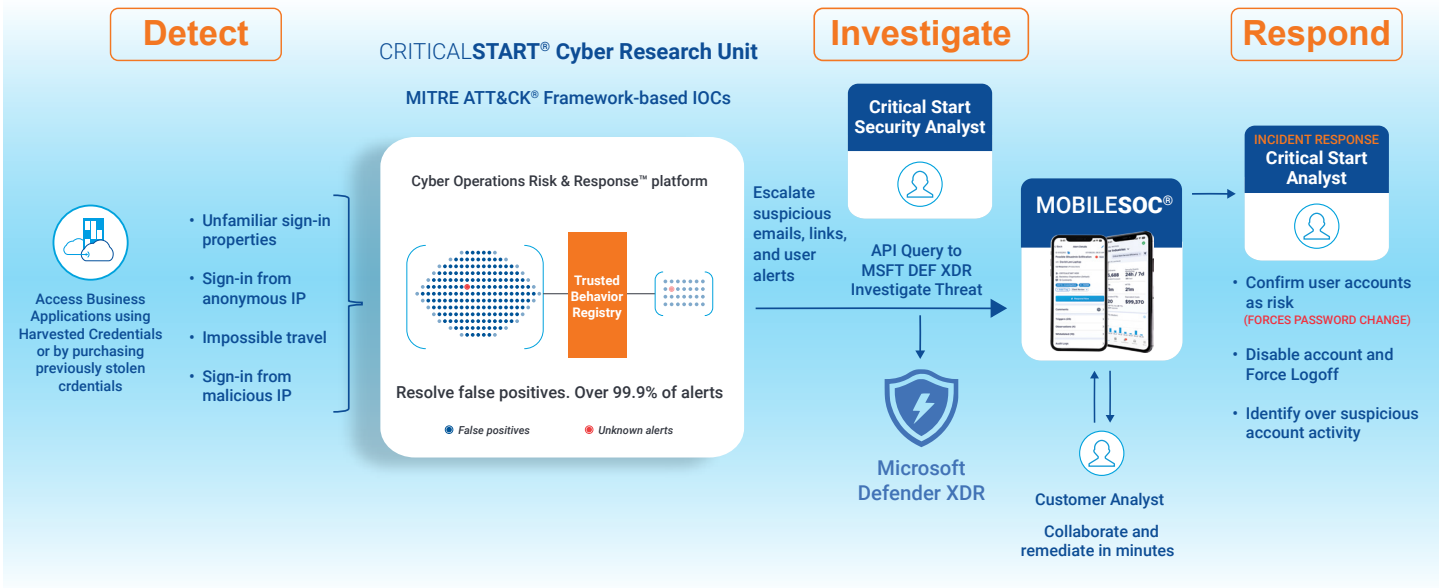
- ✓ Prevent takeover of user's credentials
- ✓ Obstruct lateral movement to other applications
- ✓ Stop adversaries from exfiltrating sensitive data
- ✓ Disrupt attacks against Cloud Apps
- ✓ Protect user identities and credentials stored in Entra ID

Adversaries acquire credentials through their own harvesting methods or by purchasing previously stolen credentials to gain access to your organization's cloud applications directly through user login. Adversaries know that by using legitimate credentials, they have insider access, making it harder for you to detect them. They can gain unrestricted access to your cloud applications and create more accounts to help achieve their goals.

Solution

Critical Start MDR Services for Microsoft Defender XDR provide threat detection, investigation, and remediation options. The Critical Start Risk & Security Operations Center (**RSOC**) leverages the Microsoft Defender XDR security suite to detect and disrupt attacks against your data stored in the cloud.

How it works



Individual alerts from the Microsoft Defender Suite (Entra ID and Defender for Cloud Applications) are ingested into our **Cyber Operations Risk & Response™ platform**, where automated investigation and triage occur, removing false positives. True positives are escalated to our RSOC for further enrichment and deeper human-led investigation and remediation.

For user accounts that have been identified as compromised, our Critical Start security analysts can:

- Isolate the threat and compromised user's account
- Disable the account and force logoff
- Force password change