Compromise Recovery

Regain secure administrative control after a serious cybersecurity incident

Microsoft follows a strict set of procedures and a methodology built on core principles

- Without a well-formed recovery plan results have limited effectiveness or are ineffective against adversaries.
- Security hardening, monitoring, and disruption events have proven time and time again to be an effective strategy for removing an adversary.
- Quickly regaining confidence in the identity directory and its administrative control is the focus of Compromise Recovery.

Outcomes

Regain Control and Remove Persistence

Regain trust and confidence that your environment is under your control

Improved Detection

Increase the likelihood that new adversary activity will be detected

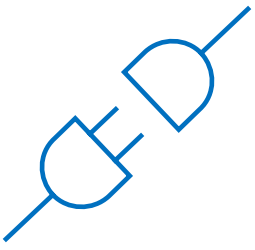
Critical Hardening Applied

High-impact controls to segment and harden your critical privileged identities

Capabilities

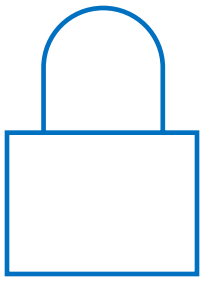
Microsoft's Compromise Recovery is built through years of experience successfully evicting adversaries throughout the globe.

Our methodology operates on four principles: scope the compromise, tactical monitoring, critical hardening, and rapid eviction.



Rapid Ransomware Recovery

Optional: Regain core identity functionality in the event the adversary is actively disrupting your identity services, which is often the case in human operated attacks



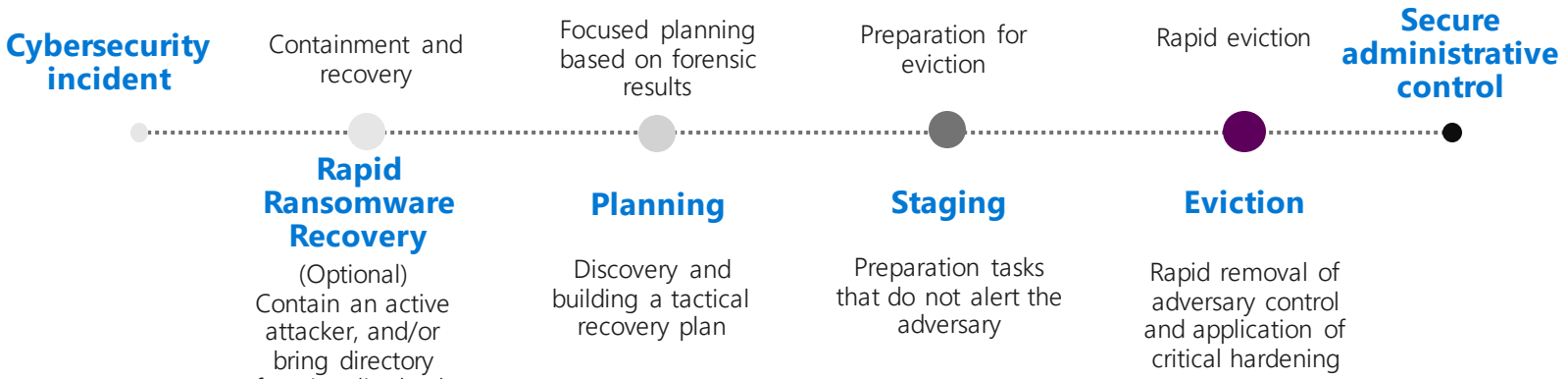
Compromise Recovery

Mandatory: Our methodology to regain secure administrative control of your environment and evict the adversary

Microsoft

Scope

Average Duration: 6-8 Weeks



Stats

5+

Years of experience delivering Compromise Recovery by Microsoft Industry Solutions Delivery

Hundreds

Successful recoveries over the history of Microsoft Industry Solutions delivering Compromise Recovery services

Additional information

Scope Compromise: Review incident response findings, indicators of compromise, and assessment of critical accounts and systems.

Tactical Monitoring: Utilizing Microsoft Threat Protection products, monitor for potential adversary activity.

Critical Hardening: Controls applied to reduce highly privileged attack surface and prevent the adversary from regaining control.

Rapid Eviction: Removal of adversarial control during a time-bound event, along with deployment of rebuilt systems.

Next steps: Contact your Microsoft Delivery account representative to engage with the Compromise Recovery pre-sales team.