Shut down a cybersecurity attack and regain control quickly

Incident Response with Compromise Recovery

Determined attackers are sophisticated—they frequently change their tools, tactics, and procedures to exploit target's defenses and gain control of their systems. To remove an attacker and regain confidence your critical data and processes, you need understand the attack, harden your security, and monitoring and manage disruption events.

Incident Response with Compromise Recovery from Microsoft Consulting Services combines investigation and recovery into a single seamless offer so you can investigate, respond, and recover faster—all with visibility into the end-to-end engagement

Outcomes

Respond

With deep understanding of the attack and analysis of current your security posture.

Regain

Trust in your environment, and the confidence that it's under your control.

Improve

Your ability to detect further efforts by the attacker to compromise your environment.

Apply

Hardening by segment to your critical privileged identities with high-impact controls.

Capabilities

Incident Response and Compromise Recovery is built on years of experience successfully identifying and evicting adversaries around the globe. Our approach is two-fold:

Incident Response

Investigate the Incident, compromised accounts, back-doors, and command & control channels.

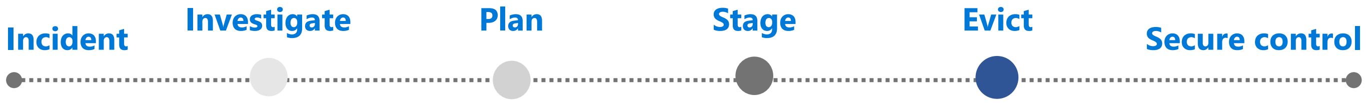
+

Compromise Recovery

Regain secure administrative control of your environment and evict the adversary using our world-class methodology.

Scope

Average Duration: between 6 to 8 weeks



Incident

Investigate

Identify compromised accounts, back-doors, & C2 channels.

Plan

Understand environment and design a tactical recovery.

Stage

Prepare the tasks that do not alert the adversary.

Evict

Execute rapid removal of adversary's control and apply critical hardening to your environment.

Secure control

Activities

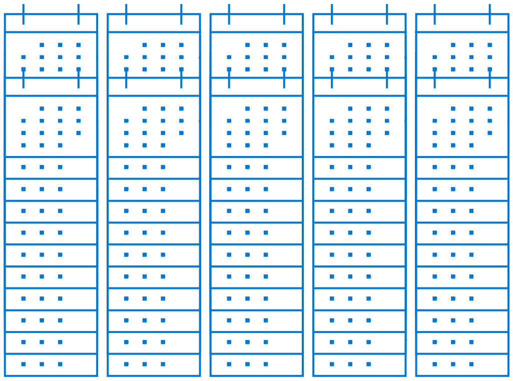
Scope Compromise: Generate incident response findings, indicators of compromise, and assessment of critical accounts and systems.

Critical Hardening: Apply controls to reduce the highly-privileged attack surface and prevent the adversary from regaining control.

Tactical Monitoring: Utilize Microsoft Threat Protection products to monitor for potential adversary activity.

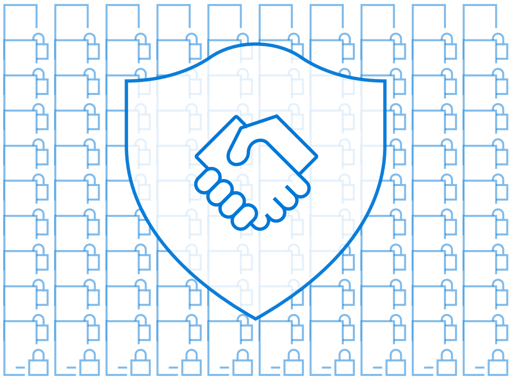
Rapid Eviction: Remove the adversarial control during a time-bound event, along with deployment of rebuilt systems.

Perspective



Over 10 years

of experience investigating and recovering customer systems.



Hundreds

Of successful investigations and recoveries Worldwide by Microsoft Consulting Services.

Additional information

Why Microsoft Consulting Services? For over 35 years we've been committed to promoting security in our products and services—from helping our customers and partners protect their assets to working to help make sure that their data is kept secure and private. Our focus on security and identity, especially information protection ecosystems, along with an active partnership with many vendors and consulting firms around the world, has driven changes in our products and services that have benefited organizations with protection and helps promote safety of their intellectual assets.

Next Steps Contact your MCS representative or visit https://microsoft.com/mcs to learn how your organization can recover from a security incident and regain control with *Incident Response with Compromise Recovery* services.