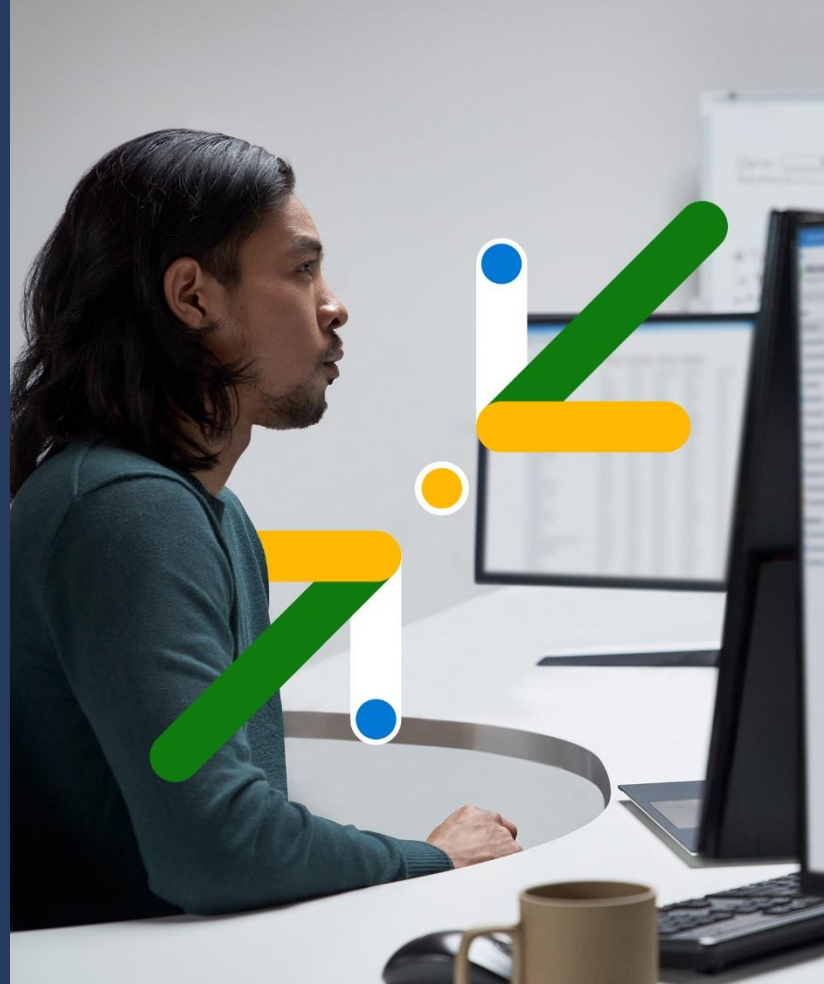


Microsoft Incident Response

Your first call before, during,
and after a cybersecurity
incident.



Security



What is Microsoft Incident Response?

Microsoft Incident Response provides fast, flexible services that will remove a bad actor from your environment, build resilience for future attacks, and help mend your defenses after a breach.

Our global team of incident responders leverage expertise from Microsoft product engineers, security analysts, and threat researchers, along with governments around the world, to help customers keep their most sensitive, critical environments secure.

Incident response needs vary, and Microsoft provides service options for proactive attack preparation, and reactive crisis response, and compromise recovery so you can regain full control of your environment after damage is contained.

Global response

Receive all day, everyday incident response expertise, with options for onsite and remote assistance on a global scale.

Industry proven expertise

Leverage the full depth and breadth of Microsoft's security research and unparalleled access to product engineering.

Proactive collaboration

Get up to date threat intelligence from Microsoft, who collaborates with government agencies and global security organizations to fight cybercrime.

Our services

Microsoft Incident Response provides support for customers before, during, and after a cybersecurity incident.

Proactive services

Compromise Assessment

Point-in-time, deep analysis of your environment, including proactive investigation for persistent threats and security risks.

Reactive services

Incident Response

Incident response investigation and guidance to help evaluate incident scope, contain attacks, and restore critical systems delivered onsite and remotely.

Compromise Recovery

Post-attack processes to help prevent future incidents by regaining control, addressing security gaps, improving your security posture. This service helps build resilience for future attacks by mending defenses after a breach, through hardening of Tier-0 assets, Azure-provisioned admin workstations, and tactical monitoring.

Investigation



Containment



Recovery



Modernization



“The team arrived quickly onsite with tools specifically designed for them to bring the systems back online in a secure operating environment.”

Dean Wells
Chief of Information Technology, Government of Nunavut

Learn more → https://aka.ms/Microsoft_Incident_Response