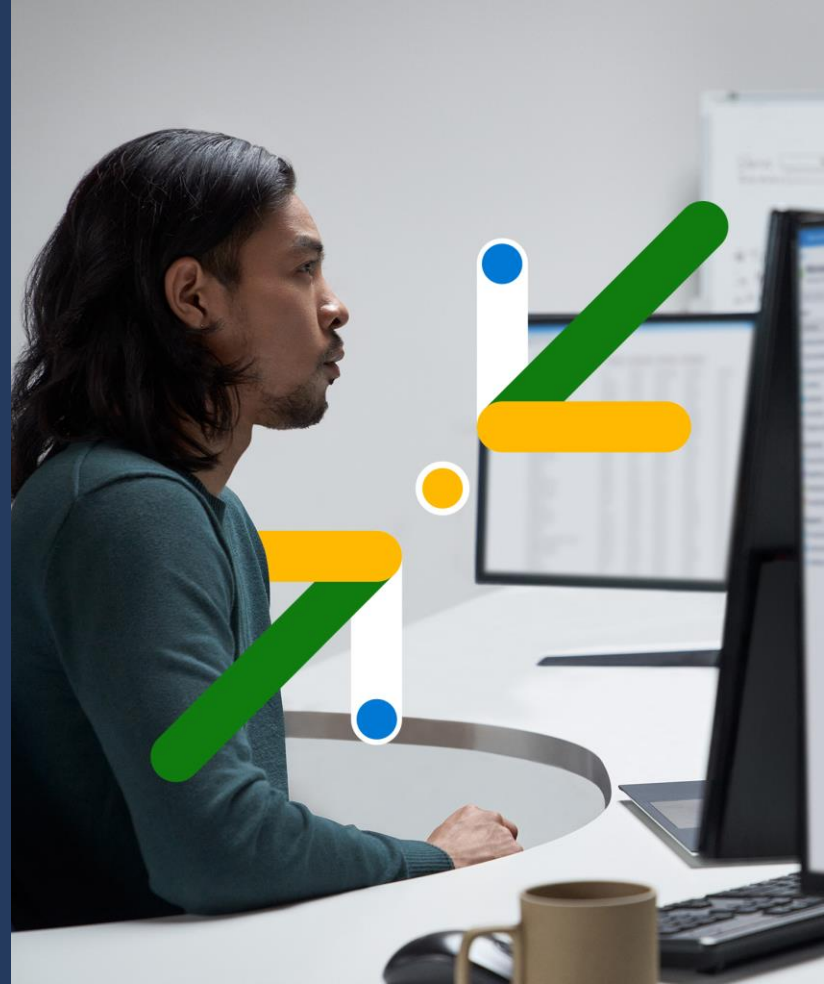**Microsoft Security**

Microsoft Security Services for Incident Response

Highly-specialized support before, during, and after a cybersecurity crisis

Security

What is Microsoft Security Services for Incident Response?

The Microsoft Security Services for Incident Response service will help you remove a bad actor from your environment, build resilience for future attacks, and mend your defenses after a breach.

Our global team of experts leverages Microsoft's strategic partnerships with security organizations and governments around the world and with internal Microsoft product groups to respond to incidents and help customers secure their most sensitive, critical environments.

By leveraging comprehensive toolsets, Microsoft's threat research, and signals from our security product stack, our experts will assist your organization in removing attackers, recovering your environment, and reducing your attack surface.

Global response
Rely on a complete investigative service that provides remote and on-site response and recovery services.

Industry proven practices
Our processes have been refined through thousands of customer engagements and can quickly restore confidence and business operations.

Actionable reporting
Receive an executive overview with recommendations for short and long-term steps to improve overall security posture.

Our services

Security Services for Incident Response provides services that support customers before, during, and after a breach.

Proactive services

Cybersecurity Operations Services
Proactive approach to determine customer exposure through deep point-in-time analysis and forensic investigation of the customer environment.

Security and Crisis Response Exercise
Interactive tabletop exercises that uses real-world observations, centered around understanding crisis situations & response tactics.

Advanced Threat Hunting
Hunts for existing threats in your production environment providing your security operations team the knowledge they need to hunt new threats and prioritize their focus on the most critical risks.

Incident response

Cybersecurity Incident Response
Onsite incident response investigation to determine whether systems are under targeted exploitation

Office 365 Incident Response
Analysis of attacker persistence in Office 365, compromised accounts and potential account traversal

Recovery services

Compromise Recovery
Removing attacker control from an environment, regaining administrative control after a cybersecurity incident, and tactically hardening high-impact controls to prevent future breaches.

Ransomware Recovery
Attack containment, restoration of critical identity infrastructure and work to limit exposure of ransomware across your environment.
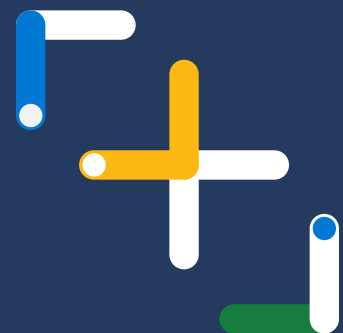
"The team arrived quickly onsite with tools specifically designed for them to bring the systems back online in a secure operating environment."

Dean Wells
Chief of Information Technology, Government of Nunavut

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