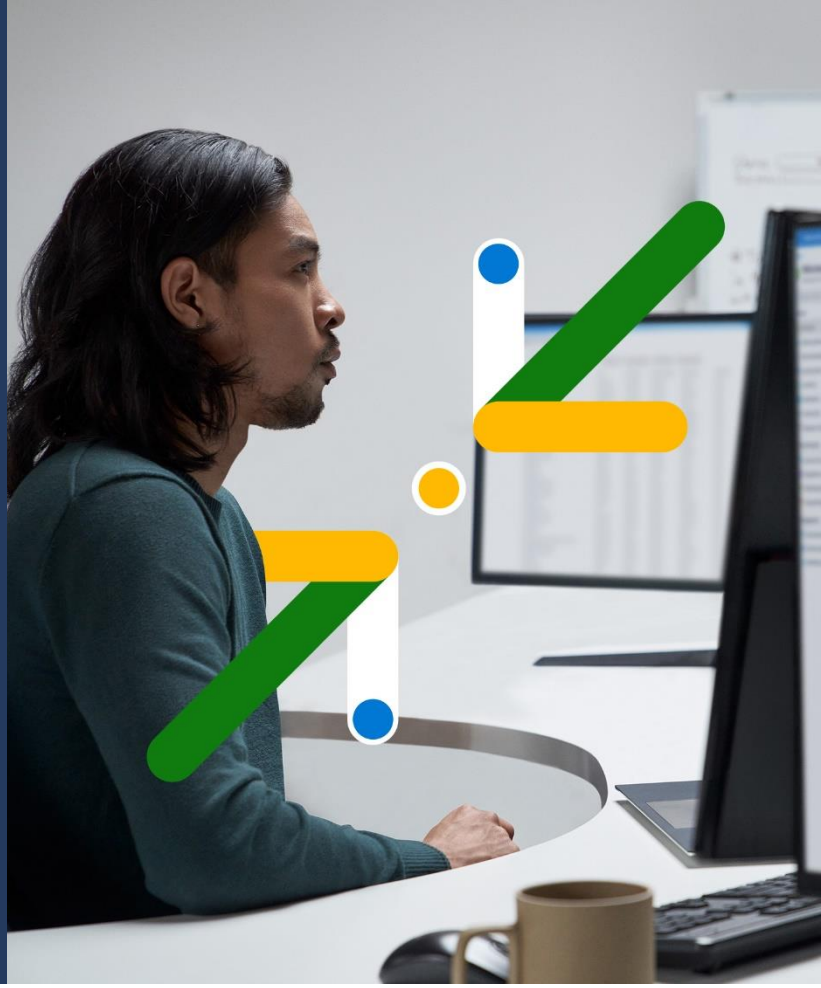
Microsoft Security

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 Capabilities

Microsoft Incident Response provides flexible capabilities to address incidents effectively. It offers a singular base plan accessible to all Microsoft Unified customers. This plan is available as an hourly service, enabling organizations to engage reactively when an incident occurs or proactively by purchasing in advance on retainer.*

Capabilities

Prioritized Response from Incident Response Experts – Two-hour response in the event of a security incident *(if purchasing Cybersecurity Incident Response proactively as a retainer.)*

Assigned Incident Response Coordinator – A Microsoft incident response expert to guide your engagement during an active security incident.

Incident Response – Threat investigation, digital forensics, log analysis, malware analysis, attacker containment, and recovery.

Proactive Compromise Assessments – Assessment of risks to your environment to increase security posture, including both on-prem and cloud.

Threat Briefings – Threat intelligence briefings with guidance on emerging threats tailored to your industry and geographical location.

Assigned Customer Success Account Manager (CSAM) – Your point of contact to schedule proactive services and to ensure you get the full value of your retainer contract.

***Microsoft Incident Response can be purchased in advance and during a security incident through onsite delivery and capacity for US clearances. Check with your Microsoft representative for citizenship clearance availability outside of the US.**

"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 → Contact your Microsoft Account Representative