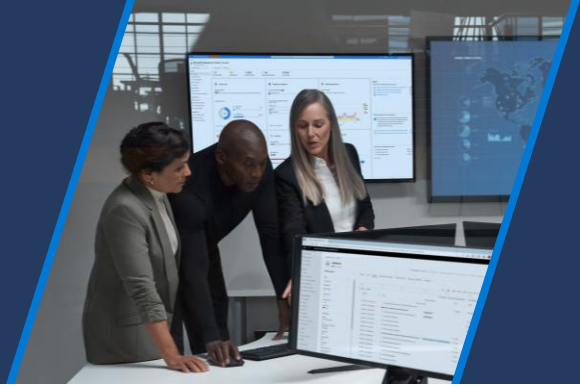
Microsoft Unified

Cybersecurity Incident Response

Microsoft experts to enable faster and more comprehensive response to cyber incidents



Cybersecurity incidents cost companies time and money. Unresolved vulnerabilities expose companies to damaging incidents. The longer vulnerabilities are unresolved, the higher the risk of a bad actor causing lasting damage impacting business operations, revenue, and organization reputation.

For companies that want to reduce the likelihood of getting breached, combat cyberattacks, and be prepared to respond and recover quickly, Microsoft created this offer that works for your complex needs.

On-call global response

Get incident response from experts across the globe, including options for onsite and remote assistance.

Industry proven expertise

Benefit from Microsoft Threat Intelligence, unmatched product engineering access, and longstanding relationships with government agencies and international security organizations.

Flexibility and simplicity

Singular base plan for Microsoft Unified customers, regardless of product. Delivered as an hourly service and can be purchased reactively and in advance with the ability to add capacity as needed.

Capabilities

Prioritized Response from Incident Response Experts – Enhanced two-hour response in the event of a security incident *(if purchasing Cybersecurity Incident Response proactively)*

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 contract.

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.

Microsoft Unified

Pre-incident Service

Compromise Assessment

Keeping pace with the rapidly changing cyber threat landscape

Understand and reduce your exposure to the risks posed by today's targeted attacks from determined human adversaries and sophisticated criminal organizations. The Compromise Assessment pre-incident service involves a team of highly-specialized Microsoft resources providing remote analysis. This is, in effect, an incident response prior to an actual emergency. You will get:

- **Findings:** Identify systems that may be compromise or vulnerable
- **Recommendations:** Guidance for your team to take proactive measures to improve security posture

Microsoft Compromise Assessment

Is utilized globally by leading defense, government, and commercial entities to help secure their most sensitive, critical environments

We work in all commercial sectors

including financial services, utilities, education, health services, pharma, medical, manufacturing, chemical & petrochemical, professional services, technology, natural resources, and critical infrastructure

Microsoft Detection and Response Team

Supports organizations' peace-of-mind in 54 countries and regions across Africa, the Americas, Asia, Europe, The Middle East, and the Pacific.

Our team's comprehensive approach

Investigate

Leverage the experience and expertise of Microsoft's Incident Response professionals for proactive investigation

Analyze

Compare your organization's needs with the state of your current security and today's threat environment.

Manage

Improve your ability to respond effectively to risk in a constantly evolving threat landscape.

Scope

Scope

Determine the level of effort for analysis week, based on total number of endpoints and number of tenants.

Kickoff

Deploy Defender and validate connection with your environment

Analysis

Perform assessment on data collected from customer's environment

Brief

Present an Executive Summary that shares our Findings and Recommendations.

Remediate

Work with you to identify Microsoft services and products that can help you address your security challenges