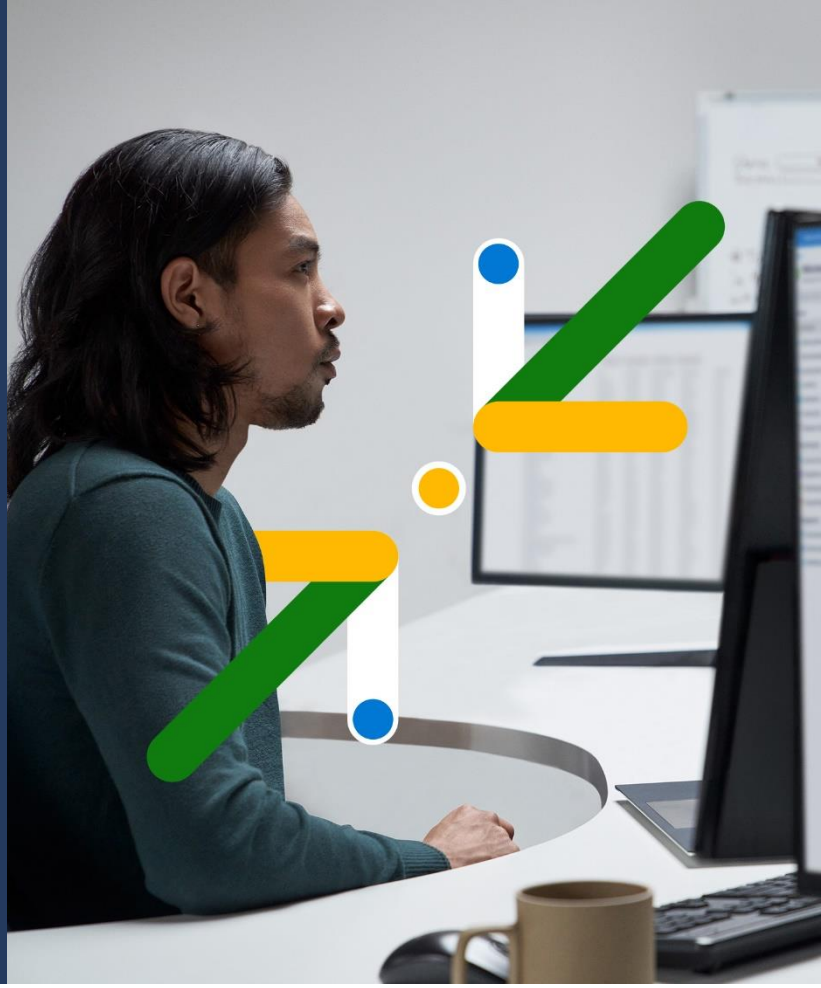
Microsoft Security

Microsoft Incident Response Retainer

Retain Microsoft experts to enable faster and more effective response to cyber incidents.



Security

What are the advantages to having the Incident Response Retainer?

Cybersecurity incidents cost companies time and money. The longer that vulnerabilities go unresolved, the more likely it is that the bad actor will cause lasting damage that impacts business operations, revenue, and organization reputation.

For companies that want to proactively combat cyberattacks to reduce the likelihood of getting breached and be prepared to respond and recover quickly, Microsoft created a retainer that includes prepaid hours that can be used by customers to build the IR program that works for their unique needs.

Incident response needs vary, and the Incident Response Retainer provides a streamlined path for proactive attack preparation, reactive crisis response, and compromise recovery so you have peace of mind that your team is positioned to avoid attack but prepared to quickly evict bad actors, contain damage, and regain control of your environment so you can resume regular business operations.

On-call global response

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

Industry proven expertise

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

Flexible delivery options

Leverage streamlined onboarding and contracting with a dedicated delivery manager that pivots to address top of mind security concerns.

Service overview

The Incident Response Retainer provides pre-paid hours for highly specialized incident response and recovery services before, during, and after a cybersecurity crisis. It's contracted on an annual basis and if reactive services are not needed, the retainer hours can be used for proactive services. The retainer contract can be easily uplifted if additional hours are needed.

- Assigned Security Delivery Manager (SDM) – A named SDM will work with you throughout the year to proactively schedule services, and ensure you get the full value of your retainer contract.
- Assigned Incident Manager – A Microsoft incident response expert to guide your engagement during an active security attack.
- Intelligence-driven investigation – Threat investigation, digital forensics, log analysis, and malware analysis support, attacker containment.
- Compromise recovery – Assistance in recovery and remediation of critical infrastructure, removing attacker control from an environment, regaining administrative control, and tactically hardening high-impact controls to prevent future breaches.
- Proactive services – Compromise Assessments will help test your team's defenses, increase your security posture, and improve resilience.
- Quarterly threat briefings – Threat Intelligence briefings with tailored guidance on emerging trends/ threats, analysis, and validation of IOCs and alerts, and premium delivery of Nation State Notifications. (Plan 2 only).

Expertise to respond and recover fast

Fast response times and direct access to our global team of experts

Complete incident coverage with forensic investigation and compromise recovery

Flexibility to meet your needs

Flexible delivery options available to meet the unique needs of each customer

Works with cyber insurance*
**Conditions apply*

Proactive services to build resilience

Test your teams' defenses with annual readiness exercises and assessments

Quarterly expert-led threat intelligence briefings to support your existing team

Next step → Contact us at MicrosoftIR@microsoft.com