Microsoft

Microsoft Security

Blog home

/ Incident response

Search the blog

Best practices Incident response Microsoft Incident Response

8 min read

How the Microsoft Incident Response team helps customers remediate threats

By Microsoft Incident Response

August 15, 2023

Microsoft Security Experts

Each year, organizations face tens of billions of malware, phishing, and credential threats—with real-world impacts. When an attack succeeds, it can result in grave impacts on any industry. For example, it could delay a police or fire department's response to an emergency, prevent a hospital from accessing lifesaving equipment or patient data, or shut down a business and hold an organization's intellectual property hostage.

Managing a security incident involves technical complexities, unknown variables—and often, frustration. Many organizations face a lack of specialized incident response knowledge, long breach resolution times, and difficulty improving their security posture due to ongoing demands on their stretched cybersecurity resources. Microsoft Incident Response is committed to partnering with organizations to combat the growing threat. Our team of experts has the knowledge and experience to help you quickly and effectively respond to any security incident, regardless of its size or complexity.

Who is the Microsoft Incident Response team?

Protecting customers is core to Microsoft's mission. That's why our worldwide Microsoft Incident Response service exists. Provided by Microsoft's Incident Response team with exceptional skills and expertise in the field in helping organizations detect, respond, and recover from cybersecurity incidents, we mobilize within hours of an incident to help customers remove bad actors, build resilience for future attacks, and mend your defenses.

We're global: Our Microsoft Incident Response team is available to customers around the clock. We serve 190 countries and resolve attacks from the most sophisticated nation-state threat actor groups down to rogue individual attackers.

We have unparalleled expertise: Since 2008, we've provided our customers with incident response services that leverage the full depth and breadth of Microsoft's entire threat intelligence network, and unparalleled access to our product engineering teams. These security defenders work in concert to help protect the platforms, tools, services, and endpoints that support our online lives.

We're backed by threat intelligence: Microsoft Incident Response conducts intelligence-driven investigations that tap into the 65 trillion signals collected every day, and track more than 300 unique threat actors, including 160 nation-state actors, 50 ransomware groups, and hundreds of others to detect, investigate, and respond to security incidents. These data signals and our deep knowledge of current threat actors are used to create a threat intelligence feedback loop, which imposes costs on the actors themselves. By sharing information with other organizations and law enforcement agencies, the team helps to disrupt the attackers' operations and make it more difficult for them to carry out their attacks. The team is committed to continuing to work with its partners to make the internet a safer place for everyone.

We collaborate: Microsoft Incident Response has been collaborating with government agencies and global security organizations to fight cybercrime everywhere it lurks for more than 15 years. Our long-term relationships have spanned the biggest attack recoveries around the globe, and our experience collaborating across internal and external teams helps us to swiftly cut through red tape and resolve critical, urgent security problems for our customers.

Our Microsoft Incident Response team members span several roles to give customers complete and deep expertise to investigate and secure their environment post-security breach and to help prevent a breach in the first place. This team has helped customers of all sizes and industries respond to and recover from cyberattacks. Here are a few examples of how we have helped customers:

- In 2022, we helped the Government of Albania recover from a sophisticated cyberattack. The attack was carried out by a state-sponsored actor, and it involved both ransomware and a wiper. We were able to help the government isolate the affected systems, remove the attackers, and restore its systems to full functionality.
- In 2021, we helped a large financial services company respond to a ransomware attack. The attack was particularly damaging, as it encrypted the company's customer data. We were able to help the company decrypt the data and restore its systems to full functionality.
- In 2020, we helped a healthcare organization respond to a phishing attack. The attack resulted in the theft of patient data. We were able to help the organization identify the compromised accounts, reset the passwords, and implement additional security controls to prevent future attacks.

These are just a few examples of how the Microsoft Incident Response team has helped customers. We are committed to helping our customers minimize the impact of a cyberattack and restore their systems to full functionality as quickly as possible. Figure 1 shows an example of an anonymized customer journey with Microsoft Incident Response.

A line graph that shows the flow of an incident response journey with four phases.

Figure 1. This image depicts a customer journey based on a typical ransomware scenario where the customer engaged Microsoft to assist with initial investigation and Entra ID recovery. It outlines four phases: collaboration and tool deployment (green), reactive incident response (blue), recovery with attack surface reduction and eradication plan (red), and compromise recovery with strategic recommendations for modernization (green). The journey involves hardening, tactical monitoring, and presenting modernization recommendations at the end of the Microsoft engagement.

What Microsoft Incident Response does

Up to 83 percent of companies will experience a data breach sometime. Stolen or compromised credentials are both the most common attacks *and* take the longest to identify (an average of 327 days).[1] We've seen the alarming volume of password attacks rise to an estimated 921 attacks every second—a 74 percent increase in just one year.[2] Our first step when a customer calls during a crisis is to assess their current situation and understand the scope of the incident. Over the years, our team has dealt with issues from crypto malware making an entire environment unavailable to a nation-state attacker maintaining covert administrative persistence in an environment. We work with a customer to identify the line of business apps affected and get systems back online. And as we work through the scope of the incident, we gain the knowledge our experts need to move to the next stage of managing an incident: compromise recovery.

Contrary to how ransomware is sometimes portrayed in the media, it is rare for a single ransomware variant to be managed by one end-to-end "ransomware gang." Instead, there are separate entities that build malware, gain access to victims, deploy ransomware, and handle extortion negotiations. The industrialization of the criminal ecosystem has led to:

- Access brokers that break in and hand off access (access as a service).

- Malware developers that sell tooling.
- Criminal operators and affiliates that conduct intrusions.
- Encryption and extortion service providers that take over monetization from affiliates (ransomware as a service).

All human-operated ransomware campaigns share common dependencies on security weaknesses. Specifically, attackers usually take advantage of an organization's poor cyber hygiene, which often includes infrequent patching and failure to implement multifactor authentication.

While every breach recovery is different, the recovery process for customers is often quite similar. A recovery will consist of scoping the compromise, critical hardening, tactical monitoring, and rapid eviction. For example, our experts conduct the following services:

- Restore directory services functionality and increase its security resilience to support the restoration of business.
- Conduct planning, staging, and rapid eviction of attackers from their known span of control, addressing identified accounts, backdoors, and command and control channels.
- Provide a baseline level of protection and detection layers to help prevent a potential re-compromise and to increase the likelihood of rapid detection should there be an indicator of re-compromise in the environment.

To mitigate a compromise, it is important to understand the extent of the damage. This is similar to how doctors diagnose patients before prescribing treatment. Our team can investigate compromises that have been identified by Microsoft or a third party. Defining the scope of the compromise helps us avoid making unnecessary changes to the network. Compromise recovery is about addressing the current attacker. Our team uses the following model to do this: Authentication (who performed the actions?), Access (where did the actions originate from?), and Alteration (what was changed on the system?).

Our teams then work to secure the assets that matter most to organizations, such as Active Directory, Exchange, and Certificate Authorities. Next, we secure the admin path. Simply put, we make sure you, our customers, regain administrative control of your environment. A daunting 93 percent of our investigations reveal insufficient privilege access controls, including unnecessary lateral movement.[2] Because our large team of experts helps so many customers, we understand what works well to secure an environment quickly. When it comes to tactical, swift recovery actions, we focus on what is strictly necessary for you to take back control first, then move on to other important security measures like hardening high-impact controls to prevent future breaches and putting procedures in place to ensure control can be maintained.

The assessment, containment, and recovery activities are the critical, immediate, and reactive services our experts deploy to help minimize breach impact and regain control. But our proactive services can help customers maintain that control, improve their security stance, and prevent future incidents.

All this expertise is supported by using a number of technologies that are proprietary to Microsoft.

What technologies we leverage

Microsoft products and services, proprietary and forensic tools, and data sourced from the breach incident all help our team act faster to minimize the impact of an incident. Combined with our on-demand specialized experts and our access to threat landscapes across different industries and geographies, these scanning and monitoring tools are part of a comprehensive security offense and defense.

For point-in-time deep scanning:

- Proprietary incident response tooling for Windows and Linux.
- Forensic triage tool on devices of interest.
- Entra ID security and configuration assessment.
- Additional Azure cloud tools.

For continuous monitoring:

- Microsoft Sentinel—Provides a centralized source of event logging. Uses machine learning and artificial intelligence.
- Microsoft Defender for Endpoint—For behavioral, process-level detection. Uses machine learning and artificial intelligence to quickly respond to threats while working side-by-side with third-party antivirus vendors.
- Microsoft Defender for Identity—For detection of common threats and analysis of authentication requests. It examines authentication requests to Entra ID from all operating systems and uses machine learning and artificial intelligence to quickly report many types of threats, such as pass-the-hash, golden and silver tickets, skeleton keys, and many more.

- Microsoft Defender for Cloud Apps—A cloud access security broker that supports various deployment modes including log collection, API connectors, and reverse proxy. It provides rich visibility, control over data travel, and sophisticated analytics to identify and combat cyberthreats across all your Microsoft and third-party cloud services.

Figure 2. This top-down image diagram highlights the Microsoft Incident Response team's broad visibility with various icons representing distinct aspects of the Microsoft tool advantages. The left column shows how Microsoft Incident Response proprietary endpoint scanners combine with enterprise data, including Active Directory configuration, antivirus logs, and global telemetry from Microsoft Threat Intelligence, which analyzes over 6.5 trillion signals every day to identify emerging threats to protect customers. The blue second column titled Continuous Monitoring illustrates how the team utilizes the toolsets of the Microsoft Defender platform, including Microsoft Defender for Office 365, Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft 365 Defender, Microsoft Sentinel, Microsoft Defender Experts for Hunting, and Microsoft Defender for Cloud. Incident response teams collaborate with different teams and technologies and utilize deep scans with proprietary toolsets, while also continuously monitoring the environment through Microsoft Defender.

A tenacious security mindset

Incident response needs vary by customer, so Microsoft Incident Response service options are available as needed or on a retainer basis, for proactive attack preparation, reactive crisis response, and compromise recovery. At the end of the day, your organization's cybersecurity is mostly about adopting a tenacious security mindset, embraced and supported by everyone in the organization.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1] Cost of a Data Breach Report 2022, IBM. 2022.

[2] Microsoft Digital Defense Report 2022, Microsoft. 2022.

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy

Sitemap Contact Microsoft Privacy Terms of use Trademarks Safety & eco Recycling About our ads © Microsoft 2024