News Incident response Microsoft Security Experts
4 min read

New Microsoft Incident Response team guide shares best practices for security teams and leaders

By Microsoft Incident Response

December 11, 2023

Microsoft Incident Response

As enterprise networks grow in both size and complexity, securing them from motivated cyberthreat actors becomes more challenging. The incident response process can be a maze that security professionals must quickly learn to navigate—which is no easy task. Surprisingly, many organizations still lack a coordinated incident response plan, and even fewer consistently apply it. Having a well-thought-out plan can mean the difference between quickly containing a cyberthreat actor and spending a significant amount of time and money rebuilding assets or addressing widespread business impact. In fact, organizations with both an incident response team and an incident response plan identified breaches 54 days faster than organizations with neither.[1]

Cybersecurity incidents are like mazes: unpredictable, challenging, and easy to get lost in. But with the right map for the maze, organizations can navigate through the twists and turns of critical incidents, avoid common pitfalls, and emerge stronger and more secure. While there are a number of incident response guides and materials readily available online, the Microsoft Incident Response team has created a downloadable, interactive guide specifically focused on two key factors that are critical to effective, timely incident response: People and process. "Navigating the Maze of Incident Response" explains how to structure the human elements of an incident response with recommendations and best practices to help navigate those crucial hours after a breach is first detected**.**

One note—this guidance is not intended to replace comprehensive incident response planning, which should occur outside of a live incident. It is a tactical, people-centric guide to help both security teams and senior stakeholders navigate an incident response investigation, should you find yourself in the deep end during an incident.

People-centric planning for incident response

Incident response is always a shared responsibility. The first step during a major response is to assemble a team and define roles and responsibilities for each team member. The assumption is often that incident response is solely a technical endeavor requiring support from technical subject matter experts. While technical expertise is necessary, support is also required from other parts of the business to manage an incident efficiently and recover quickly. A comprehensive incident response team goes beyond technical staff to include leadership, communication, and regulatory support, allowing for an incident to be managed holistically.

At the leadership level, senior stakeholders are often not privy to the true impact and risk associated with a cybersecurity incident. This is often the result of a lack of clarity in communication channels that can be exasperated during a critical incident. Senior leaders can be left ill-equipped to make informed decisions and unable to quantify the true risk to the business. While the technical elements of an incident response are typically top of mind, responding effectively means having the right technical *and* non-technical support people, processes, and structure in place to manage the workstreams required during an incident response operation.

Microsoft Incident Response suggests organizations consider the command structure outlined in Figure 1 to help define workstreams, roles, and responsibilities. The diagram and the downloadable guide are only a starting point, and additional workstreams may be required depending on the context and complexity of each incident.

Figure 1. Example of an incident command structure.

Understanding roles, responsibilities, and relationships

Within the downloadable guide, the Microsoft Incident Response team details the key activities of each incident response workstream and the responsibilities they each have. It details the key actions, escalation points, potential blockers, and common pitfalls that can hinder a successful response to a major incident. It also surfaces often overlooked incident requirements—like shift planning for responses that span multiple time zones and the risk of team burnout.

An understanding of roles and responsibilities is essential for any organization that wants to be prepared to respond to a cybersecurity incident quickly and effectively. The guide helps leaders understand the "why?" of each workstream, as well as how they all work together. This is our most comprehensive role-based incident response guide yet, to help organizations deepen their understanding of critical people and processes needed for efficient incident response.

Processes to support people-centric incident response

The processes detailed in the guide are specific to each workstream and include links to collaborating roles that may need to be included in each process. For example, for the role of incident controller, the guide outlines the process of using situation reports (SITREPs) and includes a list of key components. It also notes that collaborators should include both the governance lead and the investigation lead roles. Like many processes, real-world situations necessitate some adjustments or refinements. The guide tries to capture those caveats and levers and calls them out in the "common pitfalls" sections. For the role of investigation lead, the guide includes a detailed description of how to define evidence requirements for both on-premises and cloud data, to help organizations understand what has occurred and preserve evidence. This is often a pivotal point in incident response, where the instinct to prioritize recovery efforts must be slowed enough to ensure forensic evidence can be collected first. And for the role of infrastructure lead, the guide outlines the importance of setting up an out-of-band communications channel as existing channels may not be safe for use during a response. These are just a few examples of processes that are defined in-depth within the downloadable guide.

We hope this interactive document delivers more detail, more nuance, and more actionable information on tactical responses to incidents, with a deeper focus on the people and processes required. Download the interactive guide today to see how you can improve your organization's ability to response effectively and limit impact during a cybersecurity incident.

Navigating the Maze of Incident Response

This downloadable, interactive guide explains how to structure the human elements of an incident response.

Download the guide ›

Learn more

Learn more about Microsoft Incident Response.

To learn more about Microsoft Incident Response, 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 X (formerly known as "Twitter") (@MSFTSecurity) for the latest news and updates on cybersecurity.

[1] Cost of a Data Breach Report, IBM. 2023.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

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