Incident response Insights | Microsoft Security Blog

Published: 2026-03-16 · Archived: 2026-04-05 20:56:21 UTC

Incident response is the process of detecting, investigating, and responding to cyberattacks, security breaches, or IT incidents. Explore the latest trends and intelligence-driven strategies that help you prevent future attacks.

Filtered by

Clear All

- Incident response

Refine results

- **Help on the line: How a Microsoft Teams support call led to compromise**

A DART investigation into a Microsoft Teams voice phishing attack shows how deception and trusted tools can enable identity-led intrusions and how to stop them.

- **Explore the latest Microsoft Incident Response proactive services for enhanced resilience**

  The new proactive services from Microsoft Incident Response turn security uncertainty into readiness with expert-led preparation and advanced intelligence.

- **Introducing the Microsoft Defender Experts Suite: Elevate your security with expert-led services**

  Announcing Microsoft Defender Experts Suite, a integrated set of expert-led services that helps security teams keep pace with modern cyberattacks.

-

- **SesameOp: Novel backdoor uses OpenAI Assistants API for command and control**

  Microsoft Incident Response – Detection and Response Team (DART) researchers uncovered a new backdoor that is notable for its novel use of the OpenAI Assistants Application Programming Interface (API) as a mechanism for command-and-control (C2) communications.

- **Retail at risk: How one alert uncovered a persistent cyberthreat**

  In the latest edition of our Cyberattack Series, we dive into real-world cases targeting retail organizations.

- **Elevate your protection with expanded Microsoft Defender Experts coverage**

  Defender Experts now offers 24/7, expert-driven protection for cloud workloads, beginning with hybrid and multicloud servers in Microsoft Defender for Cloud.

- **StilachiRAT analysis: From system reconnaissance to cryptocurrency theft**

  Microsoft Incident Response uncovered a novel remote access trojan (RAT) named StilachiRAT, which demonstrates sophisticated techniques to evade detection, persist in the target environment, and exfiltrate sensitive data.

- **Build a stronger security strategy with proactive and reactive incident response: Cyberattack Series**

  Find out how a cyberattack by Storm-2077 was halted faster because the Microsoft Incident Response team is both proactive and reactive at the same time.

- **The art and science behind Microsoft threat hunting: Part 3**

  In this blog post, read how Microsoft Incident Response leverages three types of threat intelligence to enhance incident response scenarios.

- **Windows Security best practices for integrating and managing security tools**

  We examine the recent CrowdStrike outage and provide a technical overview of the root cause.

- **How to boost your incident response readiness**

  Discover key steps to bolster incident response readiness, from disaster recovery plans to secure deployments, guided by insights from the Microsoft Incident Response team.
