

Insider Risk Services

Anticipate, detect and respond to insider risks

The Challenge: Insider Risk

Insider risk is the potential for an individual (an “insider threat”) who has or used to have authorized access to or knowledge of an organization's resources to leverage that access, either wittingly or unwittingly, to negatively impact the organization.

In 2024, CrowdStrike observed an increase in incident response cases involving insider risk, and many of those cases involved the North Korean-linked threat actor FAMOUS CHOLLIMA. One of FAMOUS CHOLLIMA's primary tactics is to gain contingent or full-time employment with an organization to perform actions on their objectives such as revenue generation or data theft. This nation-state group has been successful in gaining insider access to companies across markets globally, with a prolific presence in the U.S., and is just one example of an organized insider risk.

Insider threats pose a unique challenge to organizations because they exploit the trust and access naturally given to insiders. Organizations must adopt multi-layered proactive and reactive measures to stay ahead of these risks and mitigate them. Effective strategies involve not just detecting insider risk activity but also anticipating and mitigating potential threats before they cause harm.

The solution: Insider Risk Services

Recognizing the critical need for organizations to defend against these insider risks, CrowdStrike has tailored a new set of services specifically designed to address insider risk. Built on cutting-edge insights and real-world experience, this solution offers a multi-layered defense to help organizations mitigate insider risk. CrowdStrike is uniquely positioned to deliver these services, combining world-class expertise with the advanced threat intelligence needed to stay ahead of evolving threats.

Key benefits

- Hone detection and response around intentional and unintentional insider risks
- Improve understanding of limitations that are commonly exploited by insider threats
- Adopt a multi-pronged approach to mitigating and preventing insider risk to your organization
- Review the environment for any current or historical signs of common insider risk indicators
- Strengthen access controls and identity security measures around insider risk

Key capabilities

CrowdStrike's comprehensive Insider Risk Services equip organizations with the tools needed to detect, respond to, mitigate and prevent insider risks. These services can be purchased as a bundle or ad hoc, depending on your organization's needs.

Insider Risk Incident Response: Insider-specific incident response service providing industry-recognized expertise to support your organization in responding to a suspected or validated insider threat.

Insider Risk Technical Assessment: A focused compromise assessment aimed to mitigate insider risk by detecting historical or current signs of known insider risk indicators. The assessment includes leveraging threat intelligence and threat hunting from CrowdStrike's Counter Adversary Operations team.

Insider Risk Program Review: Examination of existing capabilities to prevent, detect and respond to insider threats. This review identifies opportunities to strengthen security posture against insider risks.

Insider Risk Tabletop Exercise: People- and process-oriented simulations that prepare teams to effectively respond to insider risk scenarios, improving coordination and identifying process gaps.

Insider Risk Red Team Services: Technical red team simulations and red team / blue team exercises simulating real-world internal threat tactics, allowing organizations to test their defenses, develop detection capabilities and identify vulnerabilities specific to insider threats.

71% of organizations reported experiencing 21-41 insider incidents in 2023¹

Common insider risks include job moonlighting, disgruntled employees, negligence and organized advanced persistent threat schemes.

[Learn More](#)

About CrowdStrike Services

CrowdStrike Services delivers Incident Response, Technical Assessments, Training and Advisory Services that help you prepare to defend against advanced threats, respond to widespread attacks and enhance your cybersecurity practices and controls.

We help our customers assess and enhance their cybersecurity posture, test their defenses against real-world attacks, respond to incidents, accelerate forensic investigations and recover from a breach with speed and precision. Harnessing the power of the CrowdStrike Security Cloud and the CrowdStrike Falcon® platform, we help you protect critical areas of enterprise risk and hunt for threats using adversary-focused cyber threat intelligence to identify, track and prevent attacks from impacting your business and brand.

CrowdStrike: We stop breaches.

Learn more at www.crowdstrike.com/services/

Email: services@crowdstrike.com

© 2025 CrowdStrike, Inc. All rights reserved.

1. Ponemon, 2023 Cost of Insider Risks: Global