CROWDSTRIKE

INCIDENT RESPONSE SERVICE

Detect, contain and recover from cybersecurity incidents with speed and precision

CROWDSTRIKE INCIDENT RESPONSE

The CrowdStrike® Incident Response (IR) team brings control, stability and organization to what can be a confusing and chaotic situation. Given the current threat landscape, most organizations will likely encounter a cyber incident, at some point that they will have to respond to and manage effectively. The speed, efficiency and experience with which you are able to respond to an incident is critical for avoiding catastrophic losses that can total hundreds of thousands or millions of dollars in direct and indirect costs associated with a breach.

The CrowdStrike IR team works collaboratively with organizations to handle critical security incidents — resolving immediate issues and implementing a long-term solution to stop recurrences. The IR team takes an intelligence-led, teamwork-driven approach to investigations, blending real-world incident response and remediation experience with cutting-edge technology via the unique, cloud-based CrowdStrike Falcon® platform. Falcon allows the team to identify attackers quickly and precisely, eradicating them from your environment. CrowdStrike's methodology and approach covers all aspects of incident response, including detection, investigation, containment, recovery and reporting along with lessons-learned. The team is laser-focused on getting your organization back to business faster and reducing the impact of a cyber incident.

CROWDSTRIKE INCIDENT RESPONSE SERVICE PROVIDES THE FOLLOWING BENEFITS

Technology
The scale and efficiency of the Falcon cloud-native platform allows us to identify attackers quickly and precisely and eject them from the environment.

Experience and Expertise
CrowdStrike recruits only the best from the world of cybersecurity, incident response and digital forensics, resulting in a team with unrivalled expertise and skills.

A Strong Partnership
CrowdStrike adopts a tailored approach, partnering alongside your team to develop a response and remediation plan that balances the business and security needs of the company.

Positive Outcomes
The IR team helps you deal with the latest attacks, extracting lessons-learned to improve your security posture going forward.

INCIDENT RESPONSE SERVICE

KEY CAPABILITIES

- Real-time IR: When an incident occurs, speed to remediation is critical. CrowdStrike's IR methodology and the Falcon platform provide many advantages over traditional IR approaches. CrowdStrike gets your organization back to business faster — in days or weeks, rather than months and reduces the impact of a cyberattack, resulting in the following benefits:
  - Accelerates time to visibility and remediation, resulting in lower forensic costs
  - Reduces business interruption losses by getting the organization back to business faster
  - Minimizes adversary impact by limiting adversary dwell time
- Experience and expertise: The CrowdStrike IR team has worked on some of the world's most significant cyber investigations, and members are constantly burnishing their skills and expertise as they help organizations battle advanced threat actors.
- High quality, high business value: CrowdStrike's technology and methodology, combined with superior skills and experience, allow the team to respond and resolve incidents faster and more efficiently. The result: less hours incurred and lower costs to you.
- A tailored approach: CrowdStrike partners with your team to develop a response and remediation plan that takes into consideration your operational needs as well as your existing investments and resources. This ensures a thorough investigation and allows the team to develop a highly customized remediation action plan that balances the business and security needs of your company.
- Positive outcomes: CrowdStrike documents the team's findings and strategic recommendations for improving your security posture. These recommendations are tailored to your existing technology environment and designed to balance your security and business goals. As expert IR and intelligence analysts, the services team can approach these findings from a unique perspective, providing a prioritized list of suggested changes that will enhance your ability to detect, respond to and actively defend against even the most advanced and motivated attackers.

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 our 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**

KEY INCIDENT TYPES COVERED

Intellectual Property Theft
This includes the theft of ideas, inventions, creative expressions, trade secrets or other sensitive information in attacks often conducted by sophisticated state-sponsored actors.

Financially-Motivated Crime
Business email compromise, payment card theft, extortion / ransomware, cryptojacking and others are examples of this type of attack.

Destructive Attacks
These can be anything from damaging, targeted malware deployed by sophisticated adversaries, to nuisance malware designed to cause business disruptions.

Data Breaches
This includes the theft of personally identifiable information (PII) that could potentially expose an individual or a customer of your business.

Insider Threats
These are malicious threats to an organization made by people from within the organization, such as employees, former employees, contractors or business associates.