CROWDSTRIKE

INCIDENT RESPONSE

OVERVIEW

CrowdStrike Services stops breaches by providing pre and post Incident Response services to proactively defend against and respond to cyber incidents. Our team of incident responders has collectively worked hundreds of the world's most significant data breach investigations. Blending our real-world incident response and remediation experience with cutting-edge technologies, CrowdStrike identifies and tracks attackers in near-real time, focuses on quickly mitigating their unauthorized access to your environment, and gets your organization back to normal business operations – faster.

We regularly respond to incidents involving advanced attackers targeting organizations for their intellectual property, monetary theft, or both. Our consultants have responded to incidents perpetrated by nation-state actors, organized crime groups, hacktivists and malicious insiders.

ATTACKER OVERVIEW

Nation-State Actors	Target organizations of all sizes as well as government agencies in order to gain access to intellectual property and personal information (PII, PHI, etc).
Organized Crime Groups	Target financial institutions – banks, retailers, and card processors, among others - perpetrating crimes for financial gain. They steal money, personally identifiable information, credit/debit card data and/or take advantage of unauthorized wire transfers.
Hacktivitists	Target organizations for their own political or social agendas seeking to cause reputation damage or embarrassment to targeted organizations.
Malicious Insiders	Target their own organizations to seek vengeance, cause reputation damage or to provide sensitive information to competitors.

METHODOLOGY/APPROACH

CrowdStrike's approach to response focuses on rapid, yet comprehensive triage that mitigates unauthorized access by targeted attackers and enables organizations to identify their next steps as they occur, not after.

We recognize that every organization and every incident is unique. We partner with your team to develop a response and remediation plan that takes into consideration your operational needs, your existing investments, and your existing resources to ensure a thorough investigation and develop a highly customized remediation action plan that balances the business and security needs of the company.

CUTTING-EDGE TECHNOLOGY

In performing each investigation our consultants utilize CrowdStrike's Falcon Host detection capabilities and Falcon Forensics response capabilities to enable organizations to respond swiftly and more efficiently.

Our Falcon Host technology provides a forward view to continuously monitor for patterns of common attacker techniques - things like privilege escalation, lateral movement, and credential dumping – and allows you to prevent malicious activity from executing on endpoints within your environment.

Falcon Forensics allows us to apply traditional response methodology – looking for indicators of attack and stacking for example – to identify previous malicious actions within your network. Conducting analysis on this data allows us to construct a timeline of events and better assess where the attackers have been and what activities they have performed.

By utilizing the combined power of CrowdStrike Falcon technology we are able to detect not only previous attacker activity, but on-going activities as well; providing the most comprehensive visibility in the industry, offering a more thorough investigation and enabling faster time to remediation.

FOR MORE INFORMATION ABOUT HOW CROWDSTRIKE CAN HELP YOUR ORGANIZATION VISIT WWW.CROWDSTRIKE.COM/SERVICES

HEAR FROM OUR CLIENTS

"We operate in an industry that is heavily targeted by sophisticated adversaries. CrowdStrike Services truly customized offerings gave us the confidence to anticipate threats, prepare our networks and better defend against cyber attacks."

- CISO, Fortune 100 Financial Services

Speak to a representative to learn how CrowdStrike Services stops breaches and can help you prepare for and defend against targeted attacks.

LET'S DISCUSS YOUR NEEDS

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: www.crowdstrike.com/services

CROWDSTRIKE

15440 Laguna Canyon Road
Suite 250, Irvine, California 92618