CROWDSTRIKE

CrowdStrike Services

Data Sheet

Incident Response for Cloud

Respond to a cloud security breach with speed and precision

Adversaries are targeting cloud platforms

Adversaries have their heads in the clouds and are targeting dynamic cloud environments that have ineffective cloud security settings. These threat actors constantly try to exploit weak cloud configuration settings in an attempt to gain access to data and disrupt workloads.

Cloud misconfigurations like excessive account permissions, exposed access keys, disabled logging and ineffective network segmentation are common causes of cloud data breaches and unauthorized access by a threat actor.

Respond to an attack in your cloud environment

CrowdStrike delivers incident response (IR) services to investigate a cloud security incident and contain the active threat from further malicious activity.

The CrowdStrike Services IR team leverages the full power of the CrowdStrike Falcon® platform along with the CrowdStrike Cloud Collector tool to accelerate the collection of key forensic artifacts and cloud log trails. These dedicated cloud incident responders provide expert investigation and analysis of the forensic artifacts to provide visibility into the malicious actions executed by the threat actor.

CrowdStrike Services will help you eject threat actors from your cloud environment and stop cloud breaches from disrupting your business operations so you can get back to business faster.

Key benefits

Accelerate the investigation of a cloud security incident

Contain the active cloud threat from further malicious activity

Eradicate the threat actor from your cloud environment

Stop cloud breaches from disrupting your business operations

Key service features

A CrowdStrike Incident Response for Cloud engagement leverages a dedicated team of cloud IR specialists who are experts at investigating cloud data breaches in leading cloud platforms including AWS, Azure and GCP. The services include:

- Support for the deployment of the Falcon sensor in your cloud environment.
- Collection of additional cloud artifacts using the CrowdStrike Cloud Collector tool.
- Forensic investigation and analysis of your cloud environments and artifacts to determine the scope of malicious threat actor activity.
- Visibility into the malicious actions and potential data exfiltration executed by the threat actor informed by CrowdStrike Falcon® Insight XDR, CrowdStrike Falcon® Identity Threat Protection and CrowdStrike Falcon® Horizon cloud security posture management.
- Containment of the active threat using Falcon prevention and blocking mechanisms and custom indicators of attack (IOAs).
- Ejection of the threat actor from the network.
- Recommendations for secure cloud configuration and policy changes to prevent further incidents.

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.

Why choose CrowdStrike?

Seasoned specialists: CrowdStrike's dedicated team of IR cloud specialists have engaged in hundreds of cloud security incidents on leading cloud platforms.

Superior technology: The CrowdStrike Falcon technology platform accelerates the collection and investigation of cloud artifacts that inform the investigation.

Rapid response: CrowdStrike specialists and the Falcon technology platform enable rapid response, investigation and containment of cloud security incidents.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com