Cloud Security Assessment

Identify cloud security misconfigurations and deviations from cloud security best practices

Cloud misconfigurations continue to be the root cause of many security breaches

Threat actors are constantly trying to exploit ineffective cloud configuration settings to gain access to data and disrupt workloads. Common cloud misconfigurations are the root cause of many cloud security breaches, including:

- **Improper public access configured and exposed access keys**
- **Excessive account permissions and ineffective identity architecture**
- **Disabled logging, missing alerts and inadequate network segmentation**
- **Public snapshots and images, and open databases and caches**

Fortify the security of your cloud environment

A CrowdStrike Cloud Security Assessment provides actionable insights into your security misconfigurations and deviations compared to recommended cloud security architecture settings from CrowdStrike and leading cloud vendors including Amazon AWS, Microsoft Azure/O365 and Google Cloud Platform (GCP).

With CrowdStrike's experience in responding to and investigating cloud data breaches, and hands-on experience in cloud security architecture, the Cloud Security Assessment you receive will give you the prioritized recommendations you need to maximize your capabilities to detect, prevent and recover from security incidents in your cloud environment.

Key benefits

Determine if your cloud environment has critical gaps in security to better understand your organization's technical risk

Receive prioritized findings and recommendations to help prevent attacks and survive incidents with enhanced security practices for your cloud workloads

Proactively strengthen cloud configuration settings to fortify your cloud environments

Key service features

The CrowdStrike Cloud Security Assessment combines cloud service plane configuration reviews, documentation reviews and key staff interviews to help determine if the appropriate levels of security and governance have been implemented to protect the workloads in your cloud platforms.

The assessment reviews your cloud platform policies, configurations and permissions by account (for AWS), tenant (for Azure) or project (for GCP). CrowdStrike Services evaluates the following key areas to identify security vulnerabilities in your cloud infrastructure, management and compliance:

- Overall cloud security posture
- Access control and management
- Incident management
- Data protection
- Network security
- Risk management and compliance

CrowdStrike consultants deliver their findings related to cloud security weaknesses, along with associated recommendations organized by criticality and impact.

About CrowdStrike Services

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

We help our customers assess and enhance their cybersecurity posture, implement technologies, test 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?

Cloud threat intel: CrowdStrike consultants use experience gained from cloud incident response investigations and threat intelligence to understand the security controls that matter most to mitigate risk.

Beyond simple image scans: CrowdStrike consultants go beyond image scans to review and evaluate your cloud security architecture and governance practices to recommend areas for enhancement.

Assessing complex environments: CrowdStrike consultants evaluate complex, multi-cloud security environments and configurations to identify gaps in inter-account relationships that could lead to ongoing vulnerabilities.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com