CROWDSTRIKE

CrowdStrike Services

Data Sheet

Red Team / Blue Team Exercise for Cloud

Prepare your cybersecurity team to defend against a targeted attack on your cloud environment

Cloud attacks are evolving rapidly

Cloud attack tactics and techniques are constantly evolving as threat actors look to take advantage of ineffective and misconfigured cloud security settings.

Many organizations have a complex suite of security tools they count on for protection. The challenge is understanding whether these tools and the associated policies and procedures implemented in them are efficient and capable of preventing an attack on their cloud environment.

Prepare to defend against a targeted cloud attack

A CrowdStrike Red Team / Blue Team Exercise for your cloud environment is a week-long engagement that helps prepare your cybersecurity team by learning from experts, as the CrowdStrike Red Team emulates adversary tactics and attacks your AWS or Azure environment, while the CrowdStrike Blue Team simultaneously coaches your security team through the related response and investigation.

During this exercise, the Red Team uses real-world attacker techniques as it attempts to compromise your cloud environment, while the Blue Team of incident responders works side-by-side with your security resources using your existing tools to identify, assess and respond to the malicious activity.

The exercise identifies gaps in your logging, visibility, processes, tooling and people as they relate to incident response for your AWS or Azure cloud environment.

Key benefits

Discover and identify misconfigurations and coverage gaps in existing cloud security products

Mature your security team's cloud threat hunting knowledge and incident response processes in a safe environment

Enable your security resources to walk through the phases of a targeted cloud attack and understand the mindset and tactics of a real-world threat actor

Key service features

RED TEAM	BLUE TEAM
Active reconnaissance	
Scan your cloud environment looking for misconfigurations and vulnerabilities to exploit.	Help your security resources detect adversary reconnaissance and identify preventive measures.
Delivery and exploitation	
Use real-world threat actor tactics and techniques to exploit and compromise your cloud environment.	Help your security resources triage the incident and identify the source of the attack, the exploitation method and rogue processes.
Command and control	
Use threat actor tooling and techniques to beacon out to your cloud infrastructure under attack.	Help your security resources identify malicious traffic and search for other potential points of access and compromise.
Operations	
Escalate privileges, enumerate vulnerabilities, expand access and simulate data exfiltration in your cloud environment.	Help your security resources track these actions and assess the attack objectives to understand the risk posed by the incident.
After-action review	
Highlight details of the attack scenario to provide a complete understanding of the attack campaign that was executed.	Help your security resources to piece together a timeline and narrative of the events that transpired.

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?

Real-world cloud attack scenarios: CrowdStrike's Red Team has extensive penetration testing experience and in-depth understanding of the tactics and techniques used in today's cloud attacks.

Cyber kill chain process: CrowdStrike's Red Team incorporates the same tools and techniques that adversaries use to mirror a targeted attack that follows the steps of the cyber kill chain.

Advanced threat intelligence: CrowdStrike's Blue Team provides insight into adversarial tactics and techniques that specifically target cloud platforms. The exercise helps you better understand potential threats and how to protect yourself against a targeted cloud attack.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com