

Cloud Breach Emulation and Response Exercise

Prepare your cybersecurity team to defend against cloud attacks

Organizations operating in cloud environments face increasingly sophisticated threats that exploit weaknesses in detection, response, and security configurations. Legacy security measures often fail to detect advanced attacks, leaving gaps that adversaries can leverage for unauthorized access, privilege escalation, data theft, or operational disruption.

The CrowdStrike Cloud Breach Emulation and Response Exercise is designed to help organizations test and enhance their cloud detection and response capabilities through real-world adversary simulation. By conducting structured, step-by-step attack scenarios emulating cloud-conscious adversaries in AWS, Azure, and Entra ID environments, CrowdStrike experts help your cloud defense team develop and strengthen its detection and response capabilities and gain invaluable experience responding to realistic cloud threats.

New and unattributed cloud intrusions increased 26% year-over-year in 2024, and 35% of initial access to cloud environments was achieved through valid accounts rather than malware.¹

Key benefits

- **Simultaneously evaluate and improve your detection and response effectiveness**
- **Gain invaluable experience responding to realistic cloud threats**

¹ [CrowdStrike 2025 Global Threat Report](#)

Be prepared for cloud-based attacks

The CrowdStrike Cloud Breach Emulation and Response Exercise provides a comprehensive assessment of an organization's ability to detect and respond to cloud-based attacks. Using tactics, techniques, and procedures (TTPs) commonly employed by adversaries, CrowdStrike's Cloud Offensive Operator emulates attacks while the Cloud Defensive Operator collaborates with your SOC and incident response team to simultaneously evaluate and improve your detection and response effectiveness. The exercise includes:

- **Attack Simulation:** A controlled, stepwise execution of attack techniques aligned with real-world threats to uncover visibility and detection gaps, led by a dedicated CrowdStrike Cloud Offensive Operator
- **Blue Team Collaboration:** Joint incident triage and response efforts supported by a dedicated CrowdStrike Cloud Defensive Operator to accelerate detection, investigation, and response capabilities
- **Detection and Response Enhancement:** Hands-on detection engineering challenges to address visibility gaps and strengthen monitoring, alerting, and defensive countermeasures
- **Actionable Recommendations:** A final report detailing findings and prioritized recommendations to improve cloud security detection and response capabilities

With CrowdStrike's extensive experience in incident response and cloud security, this exercise equips organizations with the skills and experience needed to fortify cloud security response, fine-tune defensive capabilities, and intercept cloud threats before attackers can execute on their objectives.

Key capabilities

- **Identify critical weaknesses in your cloud security:** Pinpoint the most critical security gaps that adversaries exploit to gain unauthorized access, escalate privileges, steal data, or disrupt operations.
- **Strengthen detection and response capabilities:** Work alongside CrowdStrike's Cloud Defensive Operator to analyze security events, refine threat detection, and enhance incident response.
- **Optimize logging practices:** Evaluate logging mechanisms and monitoring configurations to enable comprehensive, cost-sensitive visibility into cloud activity.
- **Analyze attack paths and prioritize detections:** Map potential attack vectors within your cloud environment, and prioritize detection and response efforts based on real-world threat scenarios.
- **Receive tactical and strategic security enhancements:** Get short- and long-term recommendations to improve cloud security detection architecture, investigation processes, and technology integrations.
- **Enhance cross-team collaboration and security readiness:** Improve coordination between security teams, incident responders, and cloud architects to bolster organizational defenses against evolving threats.

By engaging in CrowdStrike's Cloud Breach Emulation and Response Exercise, organizations build experience detecting and containing real-world techniques, strengthen their cloud defenses, and stay ahead of ever-adapting adversaries in the cloud domain.

Why choose CrowdStrike?

- **Industry-leading cloud security platform:** CrowdStrike Falcon® Cloud Security delivers real-time threat detection, proactive risk mitigation, and seamless cloud workload protection, enabling organizations to secure their cloud environments without disrupting operations.
- **Unmatched cloud threat intelligence:** CrowdStrike's deep threat intelligence uncovers sophisticated attack patterns, providing unparalleled insight into evolving cloud threats and the adversaries targeting cloud infrastructure.
- **An incident response leader with top cloud expertise:** With years of experience responding to the most advanced cloud breaches, CrowdStrike offers targeted proactive recommendations to minimize impact and strengthen resilience against future attacks.

About CrowdStrike

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.

Learn more: www.crowdstrike.com/services/

Email: services@crowdstrike.com

