Identity Security Assessment

Gain insight into your Active Directory attack surface

Threat actors are targeting Active Directory domains

Active Directory continues to be one of the first services enumerated by advanced threat actors the moment unauthorized access is gained into an environment. Abusing Active Directory gives threat actors faster methods for both privilege escalation and lateral movement so they can move undetected across your network.

CrowdStrike frequently observes misconfigured features and users or groups with too many permissions in many Microsoft Active Directory environments. One of the most important steps organizations can take to protect their environments is understanding and securing their account privileges while deploying an effective identity protection solution.

Proactive risk discovery for domain accounts

A CrowdStrike Services Identity Security Assessment provides a comprehensive look into your Active Directory domain configuration, account configuration, privilege delegation and potential attack paths.

The assessment helps you understand your Active Directory attack surface by gaining insight into misconfigurations, domain account privileges and anomalous authentication activity by a potential threat actor. By identifying these misconfigurations and attack paths, you are able to proactively safeguard your network before a breach occurs.

CrowdStrike leverages the full power of CrowdStrike Falcon® Identity Threat Detection to provide insight into the common Active Directory misconfigurations likely to be exploited by these threat actors.

Key benefits

Gain deep insight into your Active Directory environment

Identify stealthy administrators in your Active Directory domain

Gain visibility into potentially malicious account activity

Proactively strengthen your domain account security posture

Key service features

Falcon Identity Threat Detection can be deployed instantly for immediate time-to-value. It starts working from the moment it's installed, allowing the CrowdStrike assessment team to review configurations within your Microsoft Active Directory environment without requiring additional reboots, query writing, staging or complex configuration.

Domain account security

- Understand what features are being utilized and how permissions are delegated so you are prepared to defend them.
- Identify unauthorized systems and applications to proactively address security issues.
- Monitor and mitigate the abuse of Active Directory permissions and misconfigurations, ensuring they are being used appropriately.
- Highlight major risk areas, including privileged accounts, compromised passwords, password aging, and stale or inactive accounts.

Attack paths

- Determine hidden relationships between user accounts and groups, and attack paths likely to be utilized during an attack.
- Get visual representations of attack paths, including details of how threat actors will likely target your environment.

Actionable recommendations

- Receive a detailed report of Active Directory issues, misconfigurations and identity-related gaps with actionable supplemental technical data designed for your IT team.
- Get weekly status reports to review and discuss all assessment findings.

Why choose CrowdStrike?

Superior technology platform: Falcon Identity Threat Detection provides instant visibility into anomalous user activity and lateral movement by potential threat actors.

Deep threat intelligence: CrowdStrike experts provide deep insight into the attack paths executed by threat actors using compromised credentials.

Identity security best practices: CrowdStrike consultants provide actionable recommendations to implement best practices and controls that help you enhance the cybersecurity posture of your user identities.

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.

Learn more
www.crowdstrike.com/services/

Email
services@crowdstrike.com