CROWDSTRIKE

TECHNICAL RISK ASSESSMENT

Discover weaknesses in your endpoint devices, applications, user identities and Active Directory configuration

HACKERS CONSTANTLY TRY TO EXPLOIT WEAK IT CONFIGURATION SETTINGS

Common IT misconfigurations continue to be the root cause of many security breaches. Groups with too many permissions, legacy or unpatched systems, or excessive administrative rights are frequently found in organization's IT environments. In addition to deploying an effective endpoint security platform, securing system configurations is the most important step organizations can take to protect their endpoints from malicious activity.

PROACTIVELY DISCOVER VULNERABILITIES

IT security leaders must understand their cyber threat risk profile and fortify their security controls so they can enhance their cyber resiliency and prevent a breach from disrupting their business.

A CrowdStrike Technical Risk Assessment highlights security vulnerabilities, weaknesses and gaps in your IT environment across endpoint devices, applications and user identities.

The assessment delivers comprehensive context around network traffic and security gaps by providing improved visibility into applications, accessibility and account management within your network. Identifying vulnerabilities and missing patches enables you to proactively safeguard your network before a breach occurs.

KEY BENEFITS

- Proactively strengthen your cybersecurity posture and reduce your risk
- Gain visibility into assets and applications running in your environment
- Understand cybersecurity weaknesses across your devices, applications and user identities
- Expose unpatched systems and vulnerabilities that could be exploited by threat actors
- Discover user accounts with excessive permissions and access rights

KEY SERVICE FEATURES

The CrowdStrike Technical Risk Assessment team starts by helping you rapidly deploy the lightweight CrowdStrike Falcon® sensor across your environment to collect information from your endpoint devices, applications, user identities and Active Directory. The data is collected by the Falcon sensor into the CrowdStrike Security Cloud, so there is no need to deploy any on-premises hardware.

The CrowdStrike team analyzes information from specific Falcon modules including: IT hygiene using Falcon Discover™, vulnerability management using Falcon Spotlight™ and Microsoft Active Directory using the Falcon Identity Threat Protection solutions.

ACCOUNTS:

Account monitoring provides visibility into the use of local and domain credentials, permission-level data and password reset data across all managed assets.

- **Prevents** identity misuse of local and domain credentials

APPLICATIONS:

Detect unpatched, vulnerable and potentially unwanted applications being used so you can address them before an attacker can take advantage.

- **Detects** vulnerable or risky applications and reconciles license costs

DEVICES:

The system inventory allows you to find and protect unmanaged systems and address those that could pose a risk to the organization's network, such as unprotected BYOD or third-party systems.

- **Helps remediate** unprotected devices and rogue systems

ACTIVE DIRECTORY:

Identify Active Directory attack paths likely to be utilized by adversaries for privilege escalation and lateral movement.

- **Prevents** Active Directory abuse and misuse

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.**

Learn more at **www.crowdstrike.com/services/**
Email: **services@crowdstrike.com**

22-PP-027

WHY CHOOSE CROWDSTRIKE?

Deep security expertise: CrowdStrike security consultants bring deep knowledge of the advanced tactics, techniques and procedures (TTPs) used by modern threat actors to exploit weaknesses in your IT environment.

Unlimited visibility: The unified Falcon platform is quickly deployed across your IT environment to provide unlimited visibility to assets, applications and accounts in a single powerful dashboard, highlighting your security posture around endpoint protection, cloud workload protection, identity protection and security operations.

Superior threat intel: CrowdStrike Threat Graph® delivers superior threat intelligence for common vulnerabilities and exposures, zero-day exploits and hands-on-keyboard activity.