CROWDSTRIKE

COMPROMISE ASSESSMENT

Identify ongoing and past attacker activity

DETERMINE IF A BREACH HAS COMPROMISED YOUR ORGANIZATION

The CrowdStrike® Services Compromise Assessment is designed to identify ongoing or past attacker activity in an organization's environment. It leverages the Services team's years of experience in responding to intrusions by the most advanced attackers, together with the powerful CrowdStrike Falcon® platform, industry-leading cyber threat intelligence and 24/7 threat hunting. These forces combine to deliver the industry's most comprehensive assessment of your organization's IT environment, answering the critical question: "Has my organization been breached?"

Extensive experience with large and complex incident response (IR) investigations involving targeted threats allows the Services team to offer unique insights into the tactics, techniques and procedures (TTPs) leveraged by today's most skilled adversaries. This knowledge and expertise combines with the Falcon platform's award-winning, cloud-delivered endpoint technology to conduct a thorough and comprehensive assessment. CrowdStrike Services goes beyond traditional indicator-based detections and point-in-time monitoring to deliver a compromise assessment based on both expert analysis of historical forensic evidence and real-time threat detection and hunting. Knowing what has happened in the past and what is happening now on your endpoints is key to understanding how to defend your cyber environment in the future.

KEY BENEFITS

CROWDSTRIKE COMPROMISE ASSESSMENT PROVIDES THE FOLLOWING BENEFITS

Minimizes Dwell Time: Learn if attackers have breached your defenses and are moving unnoticed in your environment

Reduces Risk: Receive a thorough analysis that reduces the risk of attackers stealing financial assets, customer data or intellectual property

Improves Security: Proactively identify ineffective security practices that are putting your organization at greater risk

KEY CAPABILITIES

A HIGHLY SKILLED TEAM

- The CrowdStrike Services team has unrivalled expertise and skills, having recruited the top experts from within the world of cybersecurity, incident response, forensics and operations to conduct compromise assessments. The team provides unique insights into the TTPs used by today's most skilled adversaries.

THE INDUSTRY'S LEADING TOOLS

- **The Falcon platform** allows immediate, real-time visibility into your environment, identifying potential compromises and allowing you to work on eliminating them. This offers a significant advantage over standard compromise assessments, which use classic forensics-based approaches that scan only for indicators of compromise (IOCs).
- **Falcon Insight™** is CrowdStrike's endpoint detection and response (EDR) solution, offering advanced cloud-native protection in a single, lightweight agent deployed to each endpoint in your environment.
- **Falcon Forensics Collector (FFC)** is a cross-platform, non-persistent, single-run tool that collects data from more than 45 forensically significant artifacts on each endpoint. The data is aggregated and processed in the CrowdStrike cloud where it can be analyzed and cross-referenced against CrowdStrike Intelligence that tracks and identifies adversary TTPs.

A COMPREHENSIVE APPROACH

- The assessment combines expert analysis of historical forensic evidence and real-time threat detection and hunting, allowing CrowdStrike to search for attacker activity on the endpoint and in the network.
- A CrowdStrike Compromise Assessment begins with the efficient collection and analysis of forensic artifacts from Microsoft Windows, macOS, and many Linux-based operating systems — without the need for on-premises appliances or active indicator sweeping. Working in parallel, the CrowdStrike Falcon platform provides real-time threat detection and monitoring of your environment, looking for both malware and malware-free threats, along with indicators of attack (IOAs).
- A true assessment of whether malicious activity has taken place within your environment can't begin without comprehensive, historical, forensics-based context combined with dynamic monitoring. Every environment is unique, so the Services team quickly and efficiently collaborates with your team to learn your network topology and what systems comprise your environment.

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 our 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**

ACTIONABLE ANALYSIS AND FINDINGS

CrowdStrike recognizes that for any compromise assessment to be successful, the findings and analysis reports must be actionable and appropriate for all of the key stakeholders in IT security and enterprise risk management functions. Documentation provided by CrowdStrike consultants may include:

A written report detailing whether evidence of a targeted intrusion of your environment was discovered, coupled with recommendations for effective improvements to your security posture

A written executive summary intended to capture the most significant findings, conclusions and recommendations

Technical documentation of the CrowdStrike Services team's assessment, intended to provide your technical team with the information they need to remediate, remove and validate the Services team's findings

Additional discovery documentation of commodity malware, suspicious scripts and files, remote access utilities and administration practices that introduce significant risk

© 2022 CrowdStrike, Inc. All rights reserved.