CROWDSTRIKE

COMPROMISE ASSESSMENT

CROWDSTRIKE SERVICES

COLLECT. ANALYZE. KNOW.

Extensive experience with large and complex incident response (IR) investigations involving targeted threats allows the CrowdStrike ® 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 CrowdStrike Falcon® platform's award-winning, cloud-delivered endpoint technology, to enable comprehensive compromise assessment of your organization's IT environment, answering the critical question, "Has my organization been breached?"

CrowdStrike Services goes far beyond traditional indicator-based detections and point-in-time monitoring: CrowdStrike's Compromise Assessment emphasizes 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.

CROWDSTRIKE METHODOLOGY AND APPROACH

A CrowdStrike Compromise Assessment begins with the efficient collection and analysis of forensic artifacts from Microsoft Windows, Mac OS X, and many Linux-based operating systems — without the need for on-premises appliances or active indicator sweeping. 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), which are often indicative of active malicious "hands-on-keyboard" activity.

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 CrowdStrike Services quickly and efficiently collaborates with your team to learn your network topology and what systems comprise your environment. With this knowledge, the team can understand and leverage the applications

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 the key stakeholders in IT security and enterprise risk management functions. Documentation provided by CrowdStrike consultants can include:

- **A presentation covering the summary findings of whether evidence of a targeted intrusion of your environment was discovered, coupled with custom 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 team's assessment, intended to provide your technical team with the information they need to remediate, remove, and validate the CrowdStrike team's findings**
- **Additional discovery documentation of commodity malware, suspicious scripts and files, remote access utilities, and administration practices that introduce significant risk**

and tools used within your organization. This crucial relationship allows CrowdStrike to identify normal activity and provide you with a forensics collection, network monitoring, and endpoint detection and response (EDR) effort that is unrivaled in the cybersecurity services industry.

AWARD-WINNING TECHNOLOGY PROVIDES VISIBILITY FAST

The Compromise Assessment is conducted by CrowdStrike consultants using the following:

- **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 is deployed remotely and collects data from more than 45 forensically significant artifacts on each endpoint
- **Forensic metadata** collected by FFC, then aggregated and processed in the CrowdStrike cloud where it can be analyzed and cross-referenced against CrowdStrike Falcon Intelligence™, the cyber threat intelligence offering that tracks and identifies adversary TTPs

CrowdStrike consultants investigate the collected data for IOAs; identify statistical anomalies (e.g. suspicious patterns of process execution within your environment as a whole); track and trace evidence of lateral movement and suspicious user behavior; and highlight known malware and hacking tools.

The CrowdStrike Falcon platform provides real-time, forward-looking visibility to continuously monitor for patterns of attacker tradecraft. Malicious activities such as privilege escalation, lateral movement, malware deployment, and credential dumping can all be detected immediately, allowing you to prevent further attacker activity from compromising your endpoints.

When even greater visibility is required, CrowdStrike can provide Falcon Network Sensor technology to monitor your network ingress/egress points and identify potential malicious communications in-flight. The Falcon Network Sensor is a stealth technology that passively captures, analyzes, and dissects network traffic, leveraging CrowdStrike Falcon Intelligence and custom detection patterns to alert on suspicious communications. Just as with FFC and Falcon platform data, the Falcon Network Sensor telemetry is aggregated within the CrowdStrike cloud infrastructure and analyzed by the CrowdStrike team of experienced network security monitoring (NSM) hunters.

LEARN HOW CROWDSTRIKE STOPS BREACHES:

VISIT WWW.CROWDSTRIKE.COM/SERVICES

Speak to a representative to learn more about how CrowdStrike Services can help you prepare for and defend against targeted attacks.

LET'S DISCUSS YOUR NEEDS

Phone: 1.888.512.8906
Email: sales@crowdstrike.com
Web: http://www.crowdstrike.com/services