M&A COMPROMISE ASSESSMENT

Identify and monitor cybersecurity risks during mergers and acquisitions (M&A) transactions

CYBER RISKS JEOPARDIZE M&A TRANSACTIONS

Mergers and acquisitions (M&A) activity is a key growth strategy in many industries for organizations seeking to expand their business capabilities. However, many M&A transactions encounter a critical cybersecurity issue or incident before, during or after the acquisition, potentially placing the transaction in jeopardy.

While an organization typically focuses on integrating financials and technology during the M&A process, a massive blind spot exists in securing the target entity throughout the transaction. Threat actors are keenly aware of these transactions and use them to identify big game targets, knowing that a third-party compromise in an entity being acquired can be an easy entry point to a larger target while the transaction is underway.

GAIN CONFIDENCE BY EXPOSING THREAT ACTIVITY AND REDUCING CYBER RISK

M&A business leaders must understand the scope and impact of any cyber risks they may be acquiring so they can prioritize the risk and take any corrective actions before, during and after the transaction.

A CrowdStrike M&A Compromise Assessment will identify active or past compromise activity that may indicate access to or loss of any personally identifiable information (PII) or intellectual property (IP) resulting from an unknown or undisclosed cyber breach. The assessment protects your acquisition investment through easy deployment of CrowdStrike Falcon® technology to deliver immediate visibility to active and past threats, full forensic analysis of cyber incidents, detailed reporting of IT assets and vulnerabilities, and 24/7 threat hunting to stop breach attempts during your M&A transaction.

KEY BENEFITS:

Identify compromise activity: Quickly identify ongoing and past compromise activity that could jeopardize the M&A transaction.

Reduce cyber risk: Reduce the level of cyber risk and exposure of the entity you are acquiring.

Monitor cyber threats: Monitor the environment throughout the integration period and remediate any threats that may appear.

Increase business confidence: Be confident your organization will be security-ready on Day One of network integration, with no surprises.

KEY SERVICE FEATURES

The M&A Compromise Assessment is a fixed-price engagement that can begin within one week of completing an agreement with CrowdStrike. The service is available for up to 5,000 systems, with two options: Option 1 includes one operating system and Option 2 includes any supported operating systems. Essential M&A Compromise Assessment capabilities are:

- **Falcon Technology Deployment:** CrowdStrike helps customers deploy Falcon sensors and Falcon Forensic Collector across their environment to capture real-time and historical security telemetry to identify compromise activity on endpoints.

- **Compromise Assessment:** Compromise Assessment: Upon deployment of Falcon sensors, the Falcon platform will identify current malicious activity on each endpoint (i.e., host computer). CrowdStrike will use Falcon Forensic Collector data to identify compromised endpoints and to gain deeper insight into identified threats, details related to associated threat actors and data that may have been exposed during an attack. In addition to compromise activity, CrowdStrike will report on security misconfigurations and weaknesses in the target environment that are commonly used by threat actors to breach a network..

- **Monitoring and Threat Hunting:** Monitoring and Threat Hunting: During the engagement, the Falcon OverWatch team will monitor the environment 24/7 for active threats to identify hands-on-keyboard activity and additional intrusion attempts.

- **Endpoint Recovery (Optional):** If CrowdStrike finds compromise activity within the environment, customers can choose to engage CrowdStrike Endpoint Recovery Services to clean the affected endpoints by removing malicious artifacts and persistence mechanisms using the Real Time Response capabilities of the Falcon platform and sensor.

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: **www.crowdstrike.com/services/**

Email: **services@crowdstrike.com**

WHY CHOOSE CROWDSTRIKE?

Quick client deployment: Deploy CrowdStrike's industry-leading Falcon security technology simply and quickly.

Immediate threat visibility: Gain immediate insight into threat actor compromise activity in your environment.

Accelerated analysis: Leverage the Falcon Forensics collector to investigate and gain deeper insight into compromise activity.

Threat monitoring: Monitor for threats using the Falcon OverWatch threat hunting team.

Increased hygiene: Gain a deeper understanding of the security posture of the endpoints in the entity you are acquiring.

Enhanced cybersecurity: Receive recommendations for post-acquisition security improvements and enhancement.

Rapid recovery (optional): Quickly clean and recover infected endpoints using the CrowdStrike Endpoint Recovery Service.