CROWDSTRIKE

CROWDSTRIKE **FALCON X** THREAT ANALYSIS SERVICE

CROWDSTRIKE FALCON X ORCHESTRATES THREAT ANALYSIS - SIMPLIFYING AND ACCELERATING INCIDENT INVESTIGATIONS

ENABLING A NEW ERA OF PROACTIVE SECURITY

For organizations that are struggling to respond to cybersecurity alerts and don't have the time or expertise to get ahead of emerging threats, CrowdStrike® Falcon X™ delivers the critical intelligence you need, while eliminating the resource-draining complexity of incident investigations. Falcon X is the only solution that automatically operationalizes threat intelligence and enables security teams to move from a reactive to a proactive state.

With the unique cloud-native CrowdStrike Falcon® platform as a foundation, cybersecurity teams can now automatically analyze malware found on endpoints, find related samples from the industry's largest malware search engine and enrich the results with customized threat intelligence. As a result of this closed-loop system, security teams immediately receive customized indicators of compromise (IOCs) to share with their other security tools as well as intelligence reporting that tells the complete story of the attack. This helps decision-makers understand the attacker, the motivation, and the tools behind the threat.

Falcon X enables customers of all sizes to better understand the threats they face and improves the efficacy of their other security investments with actionable and customized intelligence to defend against future attacks, making proactive security a reality.

KEY BENEFITS

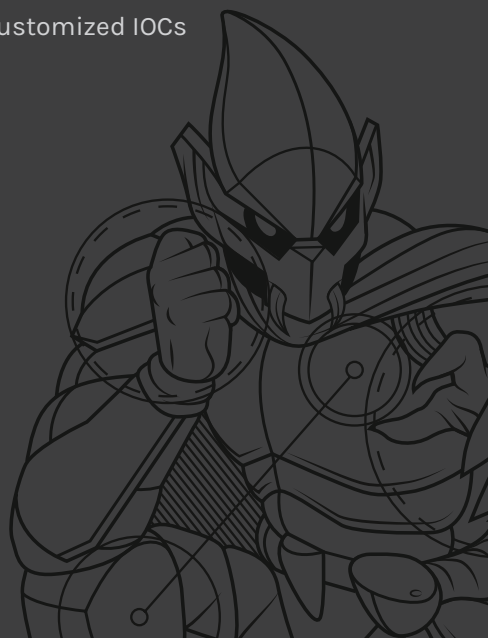
» Investigate cyber threats in minutes, not days

» Elevate security teams to make better security decisions

» Gain total understanding of the attacks hitting your endpoints

» Simplify operations with cloud-delivered threat analysis

» Optimize other security infrastructure with customized IOCs



KEY PRODUCT CAPABILITIES

1. IMMEDIATELY UNDERSTAND ATTACKS AGAINST YOUR ORGANIZATION

- **Gain complete visibility —** Falcon X results are visible within the CrowdStrike Falcon platform, presented alongside the threat detection. Tightly coupling detections and threat intelligence enables teams to make faster, better decisions and elevates the capabilities of all members.
- **Full analysis of the most relevant threats —** Analyze high-impact threats taken directly from your endpoints that are protected by CrowdStrike Falcon. Security teams, regardless of size or skill level, will never miss an opportunity to learn from a real-world attack.
- **Immediately operational —** Cloud-based Falcon X is delivered by the CrowdStrike Falcon platform and doesn't require any on-premises management infrastructure.

2. ACCELERATE AND SIMPLIFY THREAT INVESTIGATIONS

- **Save time, effort and money —** Automate each step of a cyberthreat investigation and reduce the time it takes to complete them from days to minutes. Falcon X combines malware analysis, malware search and threat intelligence into a seamless solution. The resulting intelligence is ready and waiting for the investigator, dramatically accelerating incident response time.
- **Defend against related threats —** Connect the dots between your threat and any related campaigns or malware family. Falcon X leverages the industry's largest malware search engine to find related samples and within seconds expands the analysis to include all files. This exclusive capability of recursive analysis leads to a deeper understanding of the threat and a customized set of IOCs to defend against future attacks.
- **Stop bad actors in their tracks —** CrowdStrike threat intelligence provides actor attribution to expose the motivation, tools and favored exploits of the attackers. Practical guidance and proactive steps are prescribed to stop attacks in the future.

3. STRENGTHEN DEFENSES ACROSS YOUR SECURITY INFRASTRUCTURE

- **Expanded set of IOCs —** Protect against future attacks with IOCs that are easily consumed by your network security infrastructure. Falcon X's recursive analysis provides more comprehensive defenses by providing a larger, more relevant set of IOCs than any other threat service.
- **YARA and Suricata rules —** Expand protections with YARA and Suricata rules generated from threats seen in your environment.
- **Easy integration —** A rich suite of APIs and pre-built tools enable easy integration with existing security solutions.

THE FASTEST AND EASIEST WAY TO TAKE CONTROL OF THREATS

Today, threat analysts must perform deep analysis when a threat is detected and being able to correlate that with strategic and tactical intelligence quickly is critical. CrowdStrike built Falcon X to help customers cut investigation and response time to within seconds, adding massive efficiencies for all organizations.

CROWDSTRIKE

CrowdStrike is the leader in cloud-delivered next-generation endpoint protection. CrowdStrike has revolutionized endpoint protection by being the first and only company to unify next-generation antivirus, endpoint detection and response (EDR),and a 24/7 managed hunting service — all delivered via a single lightweight agent.