XM Cyber for Crowdstrike Falcon

See the potential impact of every Crowdstrike Falcon incident and how to fix it

Enhance your Crowdstrike Falcon strategy by adding the additional information your team needs to truly understand the risk of every incident. The XM Cyber Attack-Centric Exposure Prioritization [ACEP] platform works together with Crowdstrike Falcon to add context. It shows you detailed information on how an incident might lead to a breach of your critical assets and how to best remediate. Working together, the two systems complete your incident response strategy.

XM Cyber expedites the entire exposure, assessment and remediation cycle and improves your security posture. This empowers the security team to focus on the most important issues that represent the greatest threat to business-critical assets.

Once an incident is identified in Falcon, the XM Cyber Platform can simulate an attack across all digital connections. Choke points, risk to critical assets and remediation steps are quickly presented to your team for quick action. You gain contextualized remediation effectiveness by applying the least effort to remove the highest risk from business-critical assets. You can also improve your security policies automatically by adding choke points and critical assets to groups with stricter requirements.

Optimize Your Crowdstrike Falcon Strategy with Attack Simulation

Let’s face it – you team is constantly receiving notices of incidents. It can be overwhelming. By adding context regarding potential impact, criticality of each asset, related connections and choke points, your team can prioritize their actions. Working together, XM Cyber and Falcon Crowdstrike optimize your resources and lower risk on a continuous basis.

Drill Down and Make Decisions Quickly

Incidents happen. But how does your team determine next steps? Imagine how important information such as the type of asset, potential lateral links, and steps to remediate can help your security and network teams.

See Each Incident in Your Own Battleground

To help visualize the true impact of an incident, the XM Cyber Platform presents a graphic battleground representing your network. The risk-free attack simulation links the incident from Crowdstrike Falcon to every other potential attack vector, lateral movement and digital asset. Your teams can quickly identify each step an attacker might take, as well as immediately drill down to see the exact remediation required to remove the risk.

Find Additional Exposures at the Same Time

In addition to incident reports from Crowdstrike Falcon, the XM Cyber Platform identifies other potential exposures that might exist but be unnoticed. Vulnerabilities, misconfigurations, excessive credentials and other weaknesses can magnify a small incident into a wide-open attack path. See the complete picture as you remediate incidents.
Identify and Resolve Choke Points

One crucial way to prioritize security team activities is to identify where a particular asset might be a jumping off point to many other systems. By eliminating or fixing issues with an individual choke point, you can quickly reduce overall risk and the number of potential attack paths.

Easy Integration Using APIs

Connecting XM Cyber to your Crowdstrike Falcon instance is easy via APIs. Data from XM Cyber is pushed to your Falcon dashboard, allowing you see quickly access critical information, as well and link to the XM Cyber Platform for risk-free attack simulations, drill downs on attack paths and assets, and remediation reporting.

Create Simulations Automatically from Incidents

Crowdstrike Falcon tells you the risk score for a particular incident. But how do you know what is the real attack potential? XM Cyber uses that to set a simulated breach point. Now your analysts can automatically see how an attacker could pivot towards critical assets. This additional context can help prioritize next steps as well as identify other assets within the overall attack path that might need additional attention.

Automatically Tag Assets with Context

Just because an incident has a low-risk score doesn’t mean it’s not a problem. XM Cyber shows how even low scoring incidents might be a potential issue. Is it a critical asset? Is it a choke point on the network that might allow an attacker to move laterally and reach other critical assets? XM Cyber automatically tags assets with contextual information, making your security analysts instantly aware of the true importance of each incident.

Automatically Set Risk-Based Policies

Strengthen your network constantly by using the additional incident context to make administrative changes. The XM Cyber Platform can automatically set stricter policies for chokepoints and critical assets by adding select assets to groups with more rigorous requirements.

Key Benefits of Crowdstrike Falcon Plus XM Cyber

Focus your resources on reducing risk

The goal of security is not just to remediate incidents. XM Cyber helps prioritize work for your security and network teams that will have the most impact on reducing risk to your business-critical systems.

Identify more than just vulnerabilities

Patching and version control are just part of the overall security strategy that you need to stay safe. By uncovering additional unknown problems like misconfigurations and available credentials, XM Cyber hardens your security beyond just checking security controls.

Improve your threat hunting

Cyber security is not just defensive. Gain the offense through attack simulations and get ahead of the attacker before they strike.

Add risk-free breach and attack simulation

Attack scenarios are safely activated simultaneously and continuously within the production environment, exposing attack vectors and compromised assets. XM Cyber gives you the ability to run multiple and simultaneous attack scenarios, including the latest attacks from XM Labs and the MITRE ATT&CK framework.

Protect your Cloud

As more and more data are migrated to the cloud, new risks emerge making it critical for companies to assess their risk posture and understand how attackers can operate within their cloud environment.

Improve your Vulnerability Management

XM Cyber combines advanced vulnerability scanning and patch management capabilities with its patented attack simulation engine to expose and remediate the greatest risks to your digital world. By adding additional context of how a particular vulnerability can be leveraged to compromise your critical assets, XM Cyber maximizes the effectiveness of your team’s ability to proactively secure what matters most.

Optimize your team with Prioritized remediation

XM Cyber expedites the entire exposure, assessment and remediation cycle and improves your security posture. This empowers the security team to focus on the most important issues.
Better Together – XM Cyber and Crowdstrike Falcon

By combining these two platforms, you greatly increase your situational awareness. Tagging, adding critical contextual information to your digital assets, and simulating attacks informs your entire security, IT operations and networking teams about potential problems before they happen. The results of the simulations provide both proof of risk as well as how to remediate, helping to align the goals across multiple departments.

CrowdStrike, a global cybersecurity leader, is redefining security for the cloud era with an endpoint and workload protection platform built from the ground up to stop breaches. The CrowdStrike Falcon® platform’s single lightweight-agent architecture leverages cloud-scale artificial intelligence [AI] and offers real-time protection and visibility across the enterprise, preventing attacks on endpoints and workloads on or off the network. Powered by the proprietary CrowdStrike Threat Graph®, CrowdStrike Falcon correlates 4 trillion endpoint-related events per week in real time from across the globe, fueling one of the world’s most advanced data platforms for security. With CrowdStrike, customers benefit from better protection, better performance and immediate time-to-value delivered by the cloud-native Falcon platform.