CROWDSTRIKE

CrowdStrike Products
Data Sheet

Falcon Fusion SOAR

Security automation to up-level your team and streamline security operations

Boost SOC productivity and reduce analyst burnout with automation

Security analysts struggle with endless false positives, repetitive tasks and swivel-chair syndrome from the various tools they must manage in the security operations center (SOC). This puts analysts at a disadvantage in the race against time, where adversaries are getting faster — the average eCrime breakout time dropped to 62 minutes in 2023, with the fastest observed time just over 2 minutes, according to the CrowdStrike 2024 Threat Hunting Report, and security analysts are rushing to stop threats before the damage is done.

CrowdStrike Falcon® Fusion SOAR, the native security orchestration automation and response (SOAR) capabilities of the CrowdStrike Falcon® platform, frees up valuable time for security analysts and makes investigation and response processes more efficient and effective. With Falcon Fusion SOAR, your security team can automate repeatable tasks and seamlessly orchestrate investigation and response actions across the Falcon platform and third-party tools to keep the focus on the threats that matter the most.

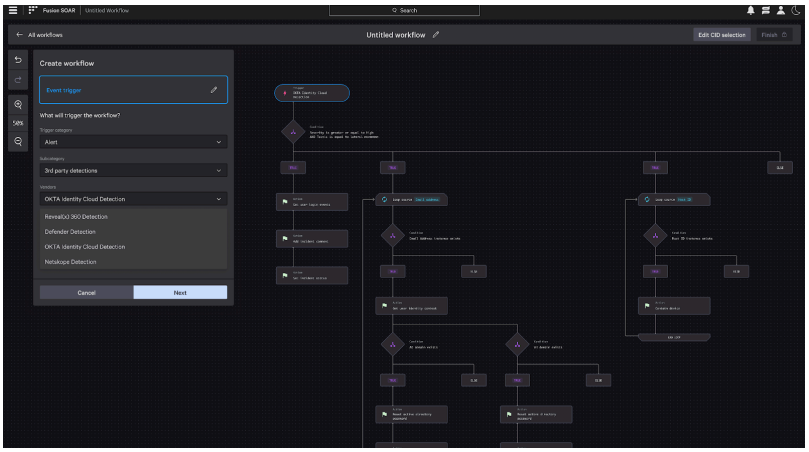

Figure 1. Deploy workflow automation in minutes with the new workflow builder interface.

Key benefits

- Accelerates threat investigation and response to reduce mean time to respond (MTTR)
- Eliminates repetitive, manual operations for improved consistency and accuracy
- Integrates seamlessly with the Falcon platform and product modules
- Up-levels your security team by giving them time back to focus on what matters most

Key capabilities

Speed up threat investigation and response with Falcon Fusion SOAR, which is built into the unified Falcon platform. Falcon Fusion SOAR leverages easy-to-use automation to lower the adoption bar across your team, improve security operations processes and reduce mean time to respond (MTTR). With Falcon Fusion SOAR, you can:

- **Eliminate repetitive, manual operations to improve analyst efficiency:** Falcon Fusion SOAR codifies your predefined investigation and response processes into workflows that streamline security operations and increase consistency and accuracy. For example, by clearly understanding the owners of assets or applications, your team will be able to easily create workflows to open tickets and assign them to the correct stakeholders to take action. Your security team can focus on high-risk threats and gain back valuable time to engage in higher-value activities like decision making.

- **Deploy workflow automation in minutes to strengthen your defenses**: Falcon Fusion SOAR offers a growing set of prebuilt workflows to get you started with automating processes. Its intuitive, no-code interface allows you to create workflows that enable data collection, enrichments, response actions and notifications by simply selecting the trigger, defining conditions and configuring actions. It also allows you to build complex workflows using conditional branching and sequencing logic. Workflow automation can be executed automatically based on a detection or event, scheduled or on demand.

- **Orchestrate CrowdStrike and third-party tools to respond to threats faster:** As a core capability of the Falcon platform, Falcon Fusion SOAR seamlessly integrates with other platform features and modules such as Falcon Real Time Response (RTR). It can also run workflows with a growing ecosystem of select third-party security and IT tools such as ServiceNow and Jira to expedite response processes.

- **Continuously improve your security posture to reduce MTTR:** Falcon Fusion SOAR features a metrics dashboard that offers at-a-glance insights to optimize your security operations. Analysts can view the actions automated by workflows along with related detections, enabling them to understand the status and context of an incident without switching between different security tools. Additionally, security teams can monitor workflow execution history and trends to enhance critical KPIs and reduce MTTR in your SOC.

Falcon Fusion SOAR by the numbers

30+
out-of-the-box playbooks

125+
workflow actions

65+
workflow triggers

20+
plug-ins for integrations

95K
unique workflow definitions

3M
daily workflow executions

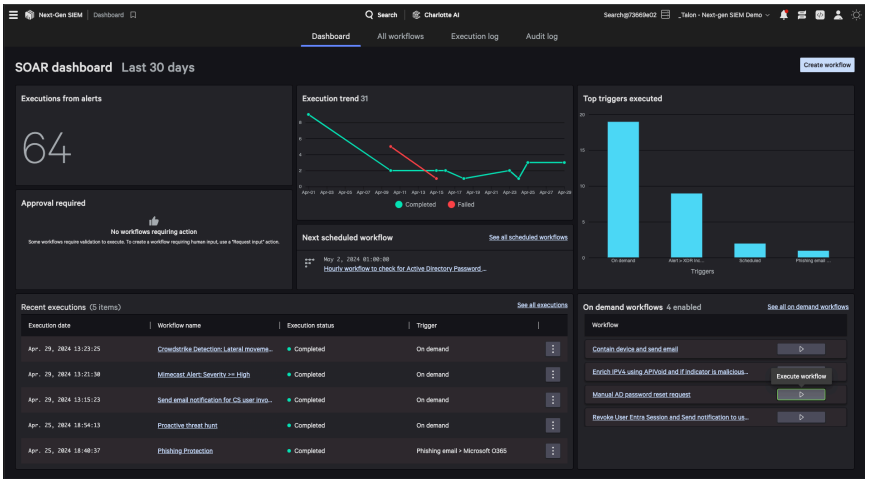

Figure 2. Understand and improve your security posture with SOAR insights at a glance.

Strengthen your defenses with workflows that run across Falcon modules

Falcon Fusion SOAR lets you deploy workflow automation that connects and leverages information from various product modules to address a growing number of use cases across security domains.

- **Accelerate incident investigation and response to stop breaches:** Falcon Fusion SOAR is natively integrated with CrowdStrike Falcon® Next-Gen SIEM, ensuring a seamless, end-to-end incident management process. This bidirectional integration enables Falcon Fusion SOAR to query and write data within Falcon Next-Gen SIEM, facilitating timely information sharing. Once an incident is identified from a detection or a group of detections, Falcon Fusion SOAR automatically initiates the investigation and remediation process with workflow automation that orchestrates actions with third-party security and IT tools.

- **Bridge the silos between security and IT to ease vulnerability patch management:** Falcon Fusion SOAR offers workflow templates for common security use cases such as vulnerability patch management. Triggered from CrowdStrike Falcon® Exposure Management or CrowdStrike Falcon® Spotlight vulnerability management, the pre-populated template creates an incident in ServiceNow, using the integration in the CrowdStrike Marketplace, to notify the application owner to patch the vulnerability. You can further customize the workflows based on your requirements such as vulnerability risk, assets or application, and owners.

- **Protect critical assets with comprehensive compensating controls:** Falcon Exposure Management enables platform-based response with Falcon Fusion SOAR. From deploying emergency patching, based on Falcon Spotlight information to activating compensating controls across compute, network, identity and hardware, workflows streamline asset management and threat investigation and response to save your team critical time.

- **Enhance your cloud security posture with timely investigation and response:** Falcon Fusion SOAR can activate remediation workflows based on findings from CrowdStrike Falcon® Cloud Security, such as misconfigured cloud accounts or suspicious activity in your cloud environment. Additionally, Falcon Fusion SOAR can help strengthen cloud workload protection by triggering workflows to report findings related to vulnerabilities and detections in your Kubernetes environment or containers.

- **Prevent credential dumping attacks by correlating endpoint and identity threats:** Falcon Fusion SOAR can trigger workflows based on identity-based endpoint detections. When a detection is triggered, Falcon Fusion SOAR can coordinate response actions such as containing a host to stop an attack or adding the user to a watchlist to limit lateral movement. You can also create policies in the CrowdStrike Falcon® Identity Threat Protection module to either block users on the watchlist or enforce multifactor authentication (MFA) if the user were to pivot to an unmanaged host, thereby preventing future attacks.

- **Address IT blind spots in your security architecture with continuous IT hygiene:** Falcon Exposure Management can initiate automated alerts and actions for asset and application changes in your environment. For example, you can send notifications or create ServiceNow incidents when drive encryption is removed from an endpoint or high CPU use is observed. These workflows can be augmented with Falcon RTR scripts to orchestrate response actions like removing unwanted applications installed by users.

- **Safeguard your brand and reputation with digital risk monitoring:** CrowdStrike Falcon® Adversary Intelligence can trigger Falcon Fusion SOAR workflows to reduce your digital risk. In addition to the Falcon Adversary Intelligence automated defenses for typosquatting domains and proactive identity threat mitigation, Falcon Fusion SOAR enhances collaboration with automated notifications and third-party ticketing integration to inform users, inside and outside the SOC, about emerging digital risks.

- **Investigate suspicious files and enrich them with threat intelligence information:** Falcon Fusion SOAR allows you to maximize your threat intelligence subscription by submitting suspicious files to CrowdStrike Falcon® Sandbox to gather additional context like indicators of attack (IOAs) and new artifacts, including those written to disk. This workflow can be customized with CrowdStrike® Threat Graph queries to verify the presence of IOAs in other machines.

About CrowdStrike

CrowdStrike (Nasdaq: CRWD), a global cybersecurity leader, has redefined modern security with the world's most advanced cloud-native platform for protecting critical areas of enterprise risk — endpoints and cloud workloads, identity and data.

Powered by the CrowdStrike Security Cloud and world-class AI, the CrowdStrike Falcon® platform leverages real-time indicators of attack, threat intelligence, evolving adversary tradecraft and enriched telemetry from across the enterprise to deliver hyper-accurate detections, automated protection and remediation, elite threat hunting and prioritized observability of vulnerabilities.

Purpose-built in the cloud with a single lightweight-agent architecture, the Falcon platform delivers rapid and scalable deployment, superior protection and performance, reduced complexity and immediate time-to-value.

CrowdStrike. We stop breaches.

Free Trial →