

Falcon Next-Gen SIEM: High-Fidelity Threat Detection with UEBA

Uncover stealthy threats with behavioral detections, entity context, and AI-powered risk scoring built natively into the CrowdStrike Falcon platform

SOC teams everywhere share the same mission: Stop cyberattacks before damage is done. But legacy SIEMs make that mission nearly impossible.

They require significant time and resources to set up, forcing detection engineers to build and maintain thousands of correlation rules to uncover threats. Even with all of that effort, SIEMs still flood analysts with low-fidelity alerts. Analysts spend up to two hours every day investigating false positives,¹ driving up costs, complexity, and burnout. Teams need a new approach.

Detection powered by data, AI, and deep adversary insights

CrowdStrike redefines SIEM by combining the right data, AI, and expert-driven analytics for superior threat detection. The goal is simple: to deliver accurate, up-to-date detections that work from the start and offer maximum coverage with minimal tuning. This empowers teams to adapt at the pace of the adversary, an evolution that sets CrowdStrike Falcon® Next-Gen SIEM apart from its predecessors.

Falcon Next-Gen SIEM is built for faster threat detection. It collects and processes data quickly, avoiding the ingestion bottlenecks of legacy tools. Because it tightly integrates with CrowdStrike's endpoint security, threat intelligence, and SOAR capabilities, it can detect attacks immediately, without waiting for data handoffs or separate tools to trigger alerts and start triage workflows. This eliminates delays and ensures teams are always a step ahead of threats.

Key benefits

Context-Rich UEBA: Cut through the noise, surface real threats, and get the context you need to make fast, informed decisions.

10,000+ AI-Powered IOAs: Detect adversary behavior in real time using CrowdStrike Falcon® platform data and threat intelligence.

Laser-Precise Correlation Rules: Reveal attacker TTPs across all data sources with prebuilt, MITRE-mapped rule templates.

Detection-as-Code: Build and refine detection logic using repeatable, code-driven processes.

¹ Vectra AI, "Do SOC Professionals Know They're Spending Almost Two Hours a Day Investigating False Positives?" August 2024

Outsmarting adversaries with AI and the power of the crowd

Organizations need visibility across hundreds of data sources — but most detections come from just a few. Falcon Next-Gen SIEM simplifies detection engineering by focusing on these critical sources and delivering thousands of prebuilt, high-fidelity detections — out-of-the-box, with no rule-building required.

By bringing together endpoint detection and response (EDR), identity protection, and cloud security in a single platform, CrowdStrike enables instant value with over 10,000 indicators of attack (IOAs) built into the Falcon platform. These detections, which are ready to go on Day One, let organizations deprecate 70% or more of their legacy SIEM rules,² while boosting coverage of endpoint, identity, and cloud threats.

The Falcon platform combines machine learning and cloud-scale processing with a deep understanding of key data sources to power precise, AI-driven detections. The Falcon platform even interprets scripting languages and commands to expose threats legacy SIEMs miss.

Unlike static correlation rules, CrowdStrike's IOAs evolve automatically to counter new threats — eliminating manual rule maintenance and reducing noise. The result is more efficient, scalable security operations with less complexity.

Industry-leading detection, extended to all data sources

Attacks can come from anywhere — network devices, email gateways, user credentials, IoT, and more — and target anything. To deliver complete visibility and protection, Falcon Next-Gen SIEM connects the dots to correlate data and uncover the stealthiest attacks.

It detects techniques across the entire cyber kill chain with over 800 prebuilt correlation rules mapped to both specific adversaries and the MITRE ATT&CK® framework. Hundreds of precision-engineered correlation rules, combined with thousands of AI-powered IOAs for key data sources, empower teams to detect nearly any type of attack.

Falcon Next-Gen SIEM lets teams build custom correlation rules with a single, intuitive query language — the same one used for search and dashboards. Teams can streamline operations by adding custom attributes, or tags, to detection rules, simplifying rule management and organization. They can choose whether correlation rules will generate detections or incidents for added flexibility and can stay connected with instant alert notifications via email, Slack, and more.

"When we started, we had a large SOC and built most of our detections ourselves. Since shifting to [CrowdStrike], alerts have dropped 20x. It's head-over-heels more mature and effective than what we had in the past."

– DJ Goldsworthy
VP of Security
Operations, at Aflac

² Based on internal reporting from a CrowdStrike customer in the pharmaceutical industry. Results may vary.

Key capabilities

Reduce False Positives with Context-Rich User and Entity Behavior Analytics (UEBA)

Adversaries increasingly avoid malware, using built-in tools and stealthy techniques that blend in with routine activity. Detecting these threats requires behavioral analysis across all sources, enriched with context such as host and user details.

CrowdStrike empowers organizations to detect, prioritize, and assess threats at scale with context-rich UEBA. Security teams can accurately surface threats with behavioral detections and prioritize findings with an AI-powered risk score. Falcon Next-Gen SIEM speeds up investigations by collecting the relevant entity information needed to visualize and understand attacks — all within a unified security platform built to stop breaches.

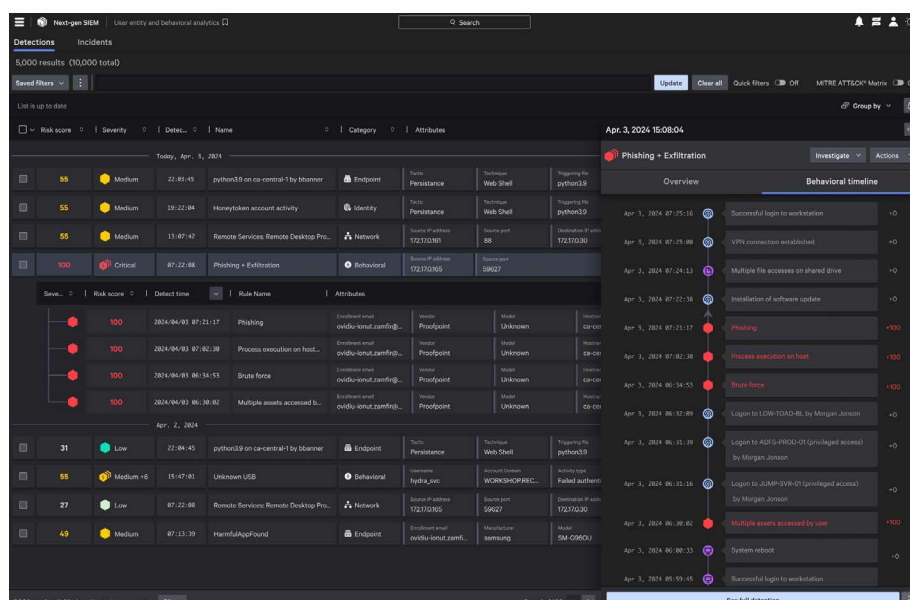


Figure 1. UEBA provides an AI-powered risk score to prioritize high-fidelity detections at scale and automate entity resolution to accelerate the investigation process.

With context-rich UEBA, security analysts can:

- Detect unknown and evasive threats with high-fidelity behavioral detections:** Behavioral detections analyze the sequence and relationship between events to identify stealthy, multi-stage attacks. Falcon Next-Gen SIEM delivers superior behavioral detections by leveraging unmatched data, including Falcon platform telemetry and third-party data. Analysts can use built-in detections or create their own detections with a guided authoring experience. By focusing on how attackers operate — rather than relying on IOCs and signatures — security teams can reduce false positives and find threats faster.

CrowdStrike Falcon® Identity Protection augments these detections with behavioral analytics. Behavioral analytics offers deep visibility into user and host behavior and accurately detects anomalies indicative of attack by baselining normal user activity with machine learning.

Falcon Next-Gen SIEM: High-Fidelity Threat Detection with UEBA

- **Prioritize alerts with an AI-powered, high-confidence risk score:** Analysts can focus on the threats that matter most by prioritizing detections based on a dynamic detection score. The detection score is customizable based on each organization's needs and risk tolerance. A clear explanation of the score is readily available to analysts, helping them understand how the score was calculated and guiding them through investigation and remediation steps.
- **Save time with automatic entity resolution:** Falcon Next-Gen SIEM enriches data, including Falcon platform and third-party data, with host and user information — which powers better detection and faster investigations. Security analysts can easily correlate and track entities across massive datasets with contextual information such as agent ID, IP address, username, and email address. They can also visualize risk trends and attack timelines to better understand the steps taken by the adversary to quickly eradicate threats.

Build, update, and scale detection rules with Detection-as-Code

Detection engineering and content management are foundational to create and maintain high-fidelity alerts — the lifeblood of a SOC. In traditional SIEMs, teams often build individual detections in-console that cannot be updated or modified. As a result, hundreds of rules can accumulate over time without a way to easily identify changes or determine if they should be deprecated.

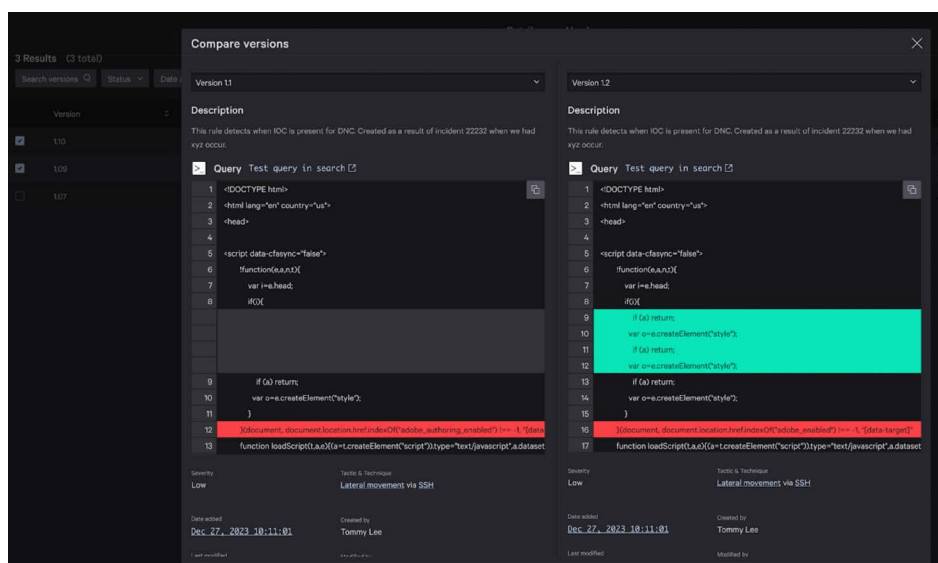


Figure 2. The Detection-as-Code authoring experience enables teams to adopt more agile security operations.

Detection-as-Code enables teams to build a scalable detection engineering practice leveraging principles from software engineering with:

- **Streamlined compliance and auditing:** Maintain a clear, comprehensive audit trail for all detection rules, and enhance version control with visual diffs.
- **Efficient rule management:** Import or export detection rules using YAML files to facilitate easy sharing and consistent application across different environments.
- **Robust integration capabilities:** Leverage the Falcon Next-Gen SIEM CRUD API to integrate detection rules with external pipelines and repositories such as GitHub, Terraform, and Jenkins.

Get a Crystal-Clear View of Detection Coverage

Legacy SIEMs depend on massive rule sets, but without the right data, detections can fail or never trigger at all, making coverage maps unreliable. Falcon Next-Gen SIEM changes that by streamlining collection of key data, providing a real-time view of defenses and showing how detection posture evolves as new rules are added.

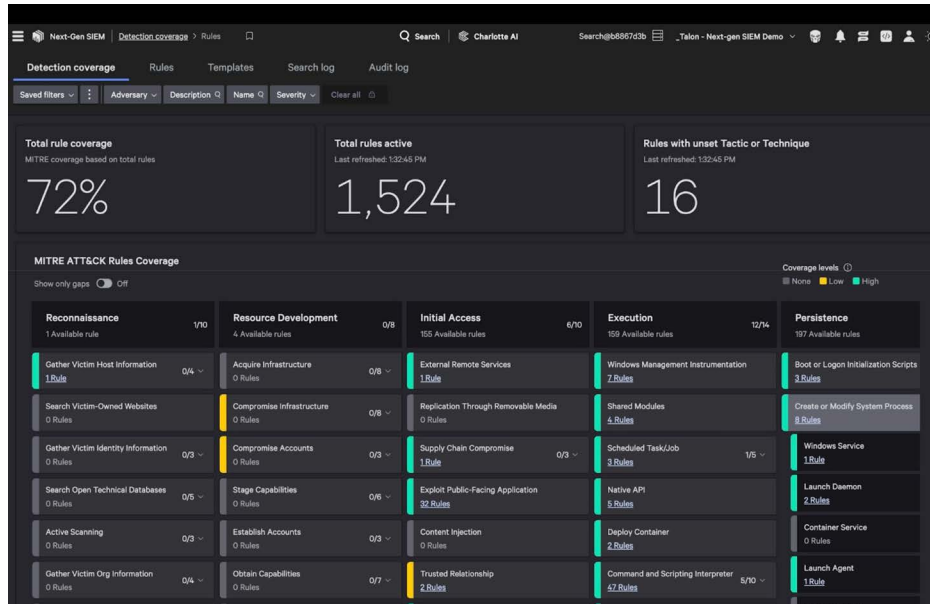


Figure 3. Detection Coverage in Falcon Next-Gen SIEM presents a unified view of all of your detections.

Detection engineers can easily see which ATT&CK techniques Falcon Next-Gen SIEM can detect, identify gaps in coverage, and determine the data sources needed to close them. They can also map data rules to specific adversaries and see which rules trigger the most alerts to fine-tune them and reduce false positives. Falcon Next-Gen SIEM's Detection Coverage helps teams discover blind spots and strengthen their security posture to stay ahead of evolving threats.

All detections — across endpoint, identity, cloud, and more — are displayed in a unified detections view to simplify triage and investigation. Falcon Next-Gen SIEM takes this even further with CrowdStrike Charlotte AI™ Detection Triage. Charlotte AI autonomously triages detections with over 98% accuracy,³ helping SOC teams scale and respond faster to the most critical threats.

Take detection capabilities to the next level

Falcon Next-Gen SIEM delivers up-to-date, cloud-native detection capabilities, including context-rich UEBA with behavioral detections and expertly crafted correlation rules. AI-powered IOAs for critical data sources identify stealthy threats without time-consuming rule building and tuning. This is what next-gen SIEM is all about: uncovering advanced threats and stripping away the noise so you can focus on stopping breaches.

See Falcon
Next-Gen SIEM in
action in a demo →

Request a free
virtual test drive →

³ Accuracy rating is a measure of Charlotte AI triage decisions that match the expert decisions from the CrowdStrike Falcon® Complete Next-Gen MDR team.

Availability of Future Products

These product descriptions include forward-looking statements including, but not limited to, statements concerning feature availability, and the benefits and capabilities of our current and future products and services. Customers should make decisions to purchase products and services based on features that are currently available.

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.

Learn more: <https://www.crowdstrike.com/>

Start a free trial today: <https://www.crowdstrike.com/free-trial-guide/>

