



White Paper

Unlocking the AI-Native SOC

with CrowdStrike Falcon®
Next-Gen SIEM

Table of Contents

Legacy SIEMs Hold Security Teams Back from Achieving Their Objectives	3
Redefining SIEM to Modernize the SOC	4
Introducing CrowdStrike Falcon Next-Gen SIEM	4
Falcon Next-Gen SIEM Addresses All Stages of Incident Response	6
Ingest Data Sources Across Your Environment	7
Rapidly Detect Threats	10
Investigate Incidents with a Modern Analyst Experience	15
Respond at Machine Speed to Fight Adversaries Gaining Speed and Sophistication	18
Hunt with Blazing-Fast Search	22
Get 24/7 Security from the Experts	24
Conclusion	25

In the fast-paced world of security operations, speed is everything. Adversaries use sophisticated, hands-on-keyboard attacks that overwhelm traditional tools like legacy SIEMs. Once lauded as the “single pane of glass” for SOCs to use in incident response and reporting for compliance, the SIEMs of the past now struggle with massive data volumes and complexity from dozens of disparate tools in modern environments. No longer able to keep pace, SIEMs have been relegated to becoming mere data dumping grounds.

2'07"

fastest recorded
eCrime breakout time¹

70%

of critical incidents take
over 12 hours to resolve²

Legacy SIEMs Hold Security Teams Back from Achieving Their Objectives

Modern security teams are on a continuous quest for better outcomes – faster time to detect, triage, investigate and respond to incidents. Yet it is impossible to achieve their objectives when relying on outdated legacy SIEMs. These teams face several key challenges.

Silos and Complexity	Overburdened SOC Teams	Manual Investigation and Response	Poor SIEM Performance
Security teams must ingest and analyze data from an average of 50 disparate tools deployed in the SOC ³	Analysts face a flood of hundreds of alerts per day, many of which are low-fidelity or false positives	Teams suffering from “swivel chair syndrome” and lacking sufficient context spend hours on manual, tedious investigation and response	Search speeds decrease as infrastructure, storage and license costs escalate, making it impossible to scale

Figure 1. Challenges in today's SOC

(1) [CrowdStrike 2024 Global Threat Report](#)

(2) [CrowdStrike 2024 State of Application Security Report](#)

(3) IDC, “How Many Security Tools Do Organizations Have, and What Are Their Consolidation Plans?”

Redefining SIEM to Modernize the SOC

Security teams need a platform that integrates advanced data collection, massive scalability and artificial intelligence (AI) to revolutionize SOC operations. The next generation of SIEM must be built from the ground up to support modern data demands so teams can break down data silos and consolidate multiple tools to slash complexity and cut costs.

To outpace threat actors, it's time for SOCs to undergo radical transformation. It's time for a new generation of SIEM.

Introducing CrowdStrike Falcon Next-Gen SIEM

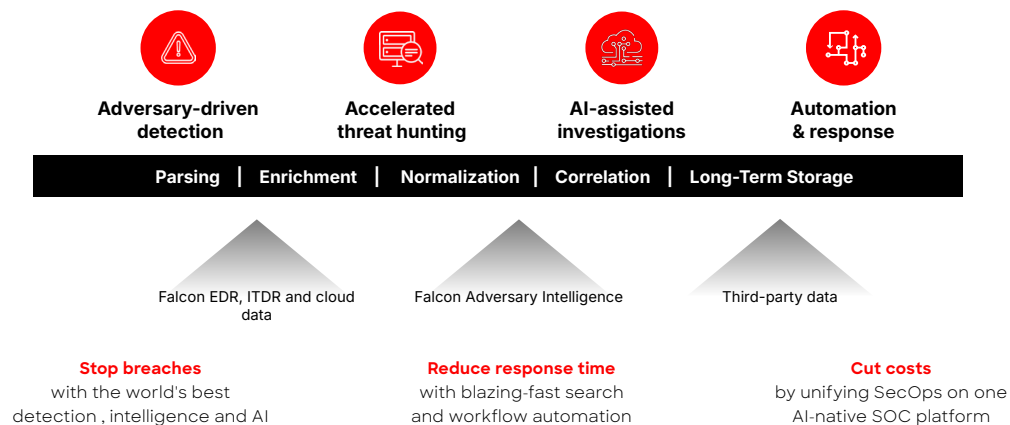


Figure 2. Falcon Next-Gen SIEM combines AI and automation with a modern log management platform to achieve superior security outcomes

CrowdStrike Falcon® Next-Gen SIEM unifies data, threat intelligence, AI and workflow automation to stop breaches. It delivers more capabilities and up to 150x faster search performance than legacy SIEMs at up to an 80% lower total cost of ownership.⁴ Built from the ground up around a modern security analyst experience, Falcon Next-Gen SIEM consolidates AI-powered detections, investigation workflows and recommended response actions across all data on one platform managed through a single console.

Security teams can detect and respond faster than you ever thought possible with real-time alerts, live dashboards and world-class intelligence. Threat hunters can scour petabytes of data at blazing-fast speed with index-free search. AI uplevels every team by correlating threats with adversary behavior to reveal the timeline and impact of an attack and automating manual investigation steps. What took hours or days now takes minutes – and years of human expertise power every decision analysts make.

Stop breaches with the AI-native Falcon platform

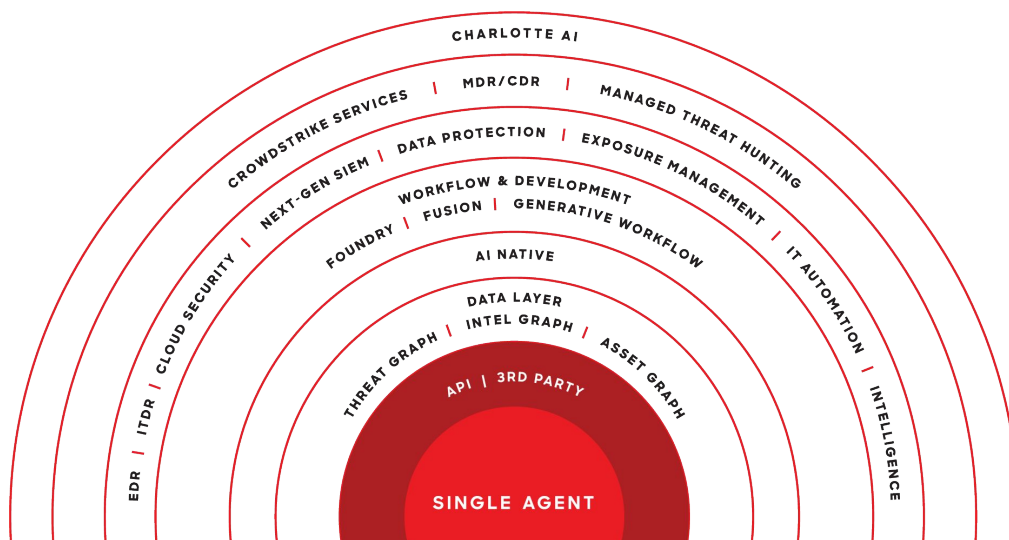


Figure 3. Falcon Next-Gen SIEM is part of the industry-leading CrowdStrike Falcon platform

(4) These numbers are projected estimates of average benefits based on recorded metrics provided by customers during pre-sale motions that compare the value of CrowdStrike with the customer's incumbent solution. Actual realized value will depend on individual customer's module deployment and environment.

Unify Your SOC Operations on One Platform

As part of the CrowdStrike Falcon® platform, Falcon Next-Gen SIEM further extends industry-leading, comprehensive security from the company that understands adversaries better than anyone. Defenses are further fortified with support from experts in managed detection and response services working around the clock.

Falcon Next-Gen SIEM empowers organizations to:

- Achieve instant time-to-value with critical data already in the Falcon platform and easily extend data collection to third-party data sources
- Reduce mean time to respond, and say goodbye to tedious tasks with workflow automation
- Coordinate response across your infrastructure and drive any endpoint remediation action through tight integration with the Falcon agent
- Slash SOC costs by consolidating tools and streamlining operations on a single-agent, single-platform architecture

Falcon Next-Gen SIEM Addresses All Stages of Incident Response

Read on to discover key capabilities of Falcon Next-Gen SIEM at each stage of incident response.

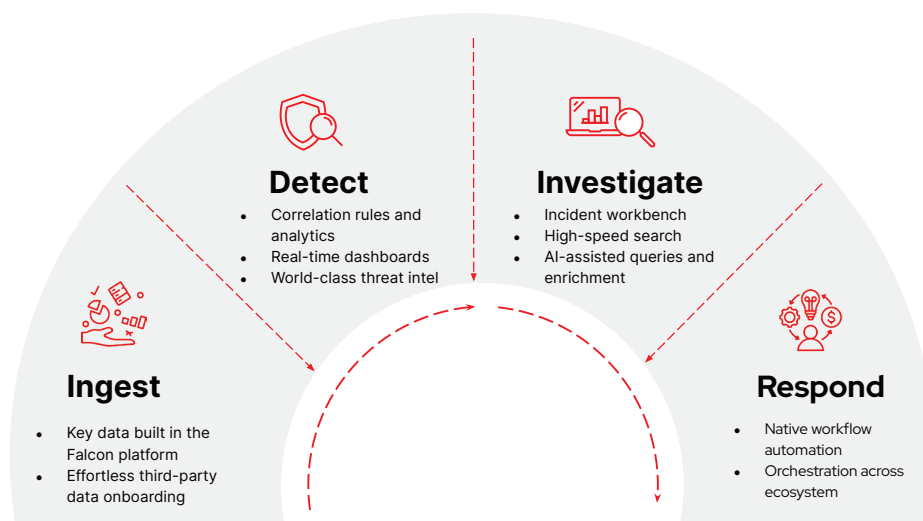


Figure 4. Falcon Next-Gen SIEM utilizes AI and automation to tackle each stage of the incident lifecycle

Ingest Data Sources Across Your Environment

Data drives nearly every aspect of security operations, but legacy approaches to data collection have turned SIEM administrators into data wranglers. Manual processes force them to spend more time onboarding, tuning and managing data than stopping adversaries. Falcon Next-Gen SIEM changes everything by radically simplifying data ingestion and management.

Gain Instant Visibility with Falcon Data

“Often, 80-85% of the security data that goes into the SIEM comes from the endpoint.”

George Kurtz

CEO and Founder, CrowdStrike

Telemetry data from key native sources like endpoints, identity and cloud services is already resident and readily available for threat modeling and analysis within the Falcon platform. The AI-native platform offers cloud-delivered endpoint detection and response (EDR), cloud security, exposure management, identity protection and world-class threat intelligence. Instead of routing data to a SIEM or managing duplicate data stores, which can require time spent on configuration, parsing, normalization or correlation, teams can get immediate value from data already in the platform. This key data covers the majority of SIEM use cases without incurring additional ingestion costs or operational complexity.

“My previous experience with SIEM was painful to say the least. Logs are generated and piped across the network. If that piping isn’t available, logs queue, they backlog, and now you’re waiting on alerts to trigger from two days ago, which is expensive from an incident response perspective. With [Falcon] Next-Gen SIEM, the key data is already in the platform.”

— Larry Wiggins, CISO, Cloudflare

A single, lightweight agent protects endpoints against all types of attacks, from commodity malware to novel threats, using multiple layers of defense including AI, behavioral protection and exploit prevention. Deployed in minutes without complex tuning, the Falcon agent safeguards your organization from the most sophisticated threats while collecting rich telemetry for detection and response.

Extend Visibility to Third-Party Data

Pre-built connectors and HTTP Event Collectors (HEC) allow teams to extend visibility to diverse sources like firewalls, hypervisors, cloud services and more. All CrowdStrike Falcon® Insight XDR customers receive 10GB of daily ingestion for third-party data sources at no additional cost and can ingest higher volumes of data with a Falcon Next-Gen SIEM subscription.

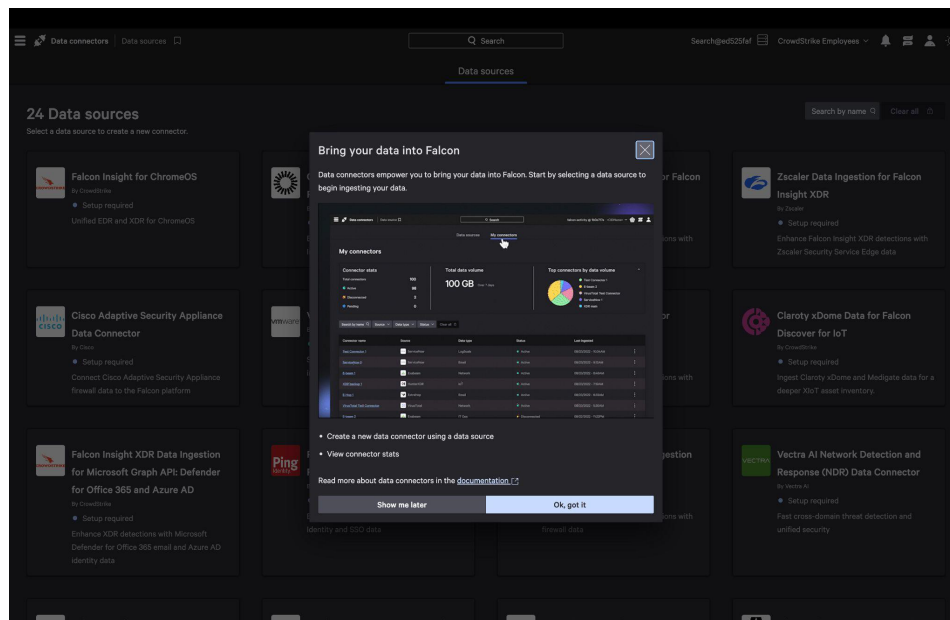


Figure 5. Easily bring data into Falcon Next-Gen SIEM using out-of-the-box data connectors, including a HTTP event collector (HEC) receiver

Simplify Setup with Connectors and Parsers

Getting data in is easy with a rapidly growing number of data connectors and parsers available via the CrowdStrike Marketplace. Aligned to the CrowdStrike Parsing Standard, pre-built connectors and parsers let you easily collect, correlate and analyze your choice of data. Full parser management, including editing and custom parsers, is available from one console, further enhancing efficiency. For cloud-based data sources, engineers can use APIs and webhooks to write data to a SIEM, such as bringing in third-party enrichments.

Gather, Aggregate and Forward Logs with the Falcon Log Collector

The Falcon Log Collector provides a robust, reliable way to forward logs from Linux, Windows and macOS hosts to Falcon Next-Gen SIEM. Gathering data from a variety of sources – including files, command sources, and syslog and Windows events – the Falcon Log Collector swiftly sends events with sub-second latency between when a line is written on the host and when it is forwarded to Falcon Next-Gen SIEM.

Store Log Data at Petabyte Scale

CrowdStrike Falcon® Search Retention offers cost-effective long-term storage for compliance and forensic investigations, keeping log data from both the Falcon platform and third-party data sources accessible for up to three years. This is essential for maintaining audit trails and supporting thorough investigations.

Rapidly Detect Threats

Assess and Strengthen Detection Posture

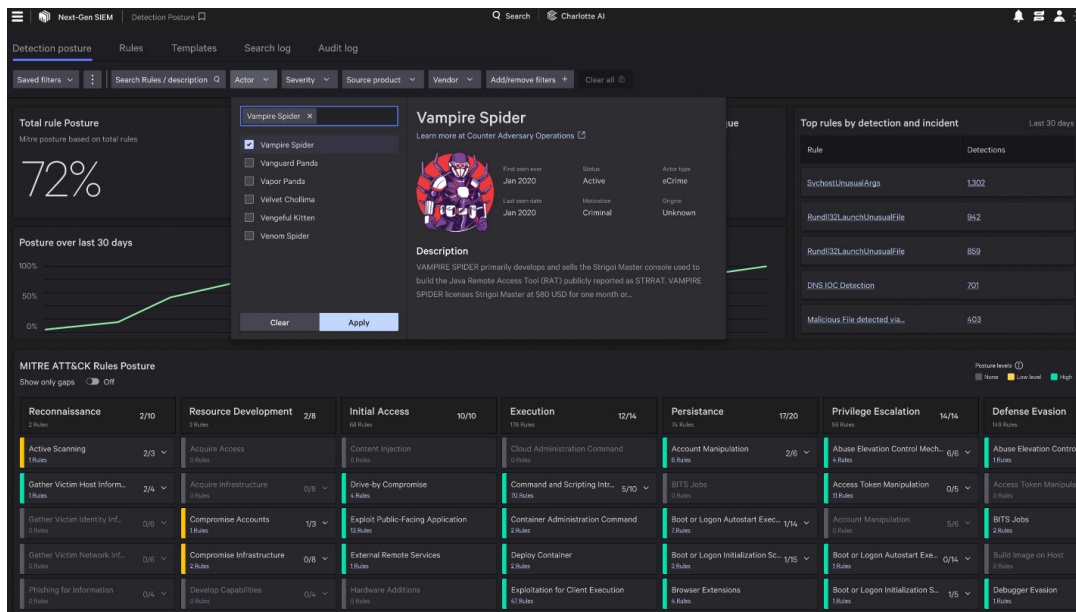


Figure 6. Detection Posture Management presents a unified view of all your detections

Security teams often spend inordinate amounts of time and resources to increase detection coverage with their SIEM by onboarding different data sources or configuring different rules. Legacy tools often come with hundreds if not thousands of rules, but without the right data sources, detections may not trigger correctly, if at all. As a result, so-called “coverage maps” may not accurately reflect a SIEM’s effectiveness.

Detection Posture Management, a part of Falcon Next-Gen SIEM, gives security teams a real-time view into the depth and breadth of out-of-the-box detection coverage. They can also see how detection posture changes over time as additional rules are added by their own detection engineers as well as from CrowdStrike. Mapped to the MITRE ATT&CK® framework, analysts can quickly understand not only which rules are mapped to tactics, techniques and procedures (TTPs), but also how data sources can enable different rules, where gaps exist and which areas can be improved, from low to high. Detection engineers can also view the most triggered rules to further guide tuning efforts and cut down on false positives. With native integration with CrowdStrike Falcon® Adversary Intelligence Premium, analysts can also easily filter for different views to understand which data sources or rules are associated with various adversary activities. With Detection Posture Management, security teams can truly understand the value of any given data source and advance their detection posture over time.

Detect Advanced Threats and Ransomware with AI and Indicators of Attack (IOAs)

Traditional detections in legacy solutions often rely on indicators of compromise (IOCs) or “known bads” such as individual file hashes or IP addresses, which serve as confirming evidence of an attack after the fact. However, adversaries can easily slip past IOC-based defenses by modifying their activity.

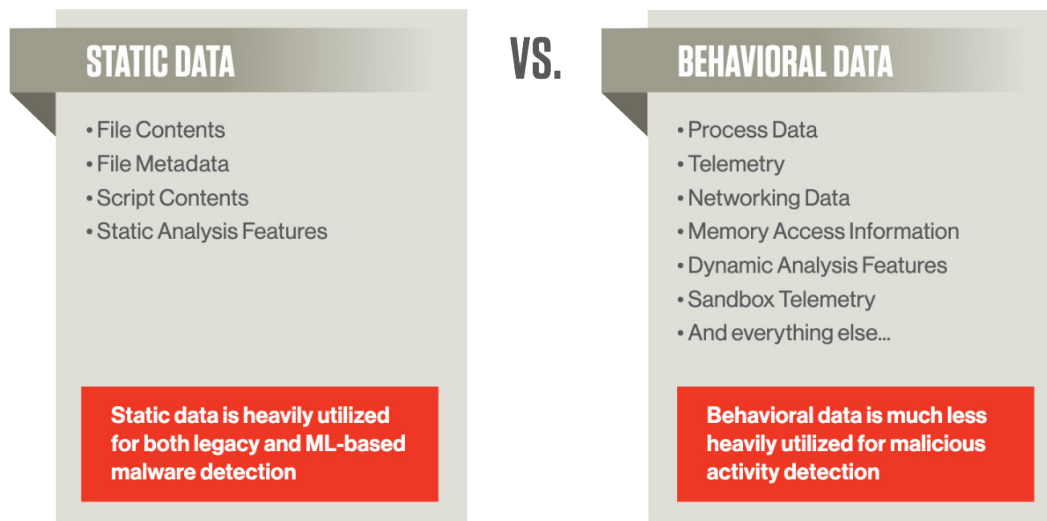


Figure 7. Behavioral data captures activities and processes occurring in a user’s environment

CrowdStrike pioneered a new approach to applied machine learning (ML) to perform behavioral analysis, resulting in a new approach to detection: indicators of attack (IOAs). Complementing traditional detections, IOAs look for signals of in-progress attacks, analyzing how observed behaviors could serve adversary intent. This allows defenders to detect malicious activity even when adversaries exploit legitimate tools or user accounts.

IOAs are built from the expertise of threat hunters and the observed patterns of attacker activity and intent across large volumes of data. The Falcon platform regularly processes trillions of events of high-resolution behavioral and contextual data that is further enriched with deep adversary intelligence. This data feeds robust models that analyze processes on a machine and associated context at run time to distinguish whether a process is being run legitimately (e.g., a file is being encrypted by a known user to safeguard its contents) or if it’s being run maliciously (e.g., a file is being encrypted to conduct a ransomware attack). CrowdStrike also offers on-sensor ML and cloud ML for additional detections.

New IOAs generated by AI further fortify existing defenses and expand coverage across emerging attack vectors. This enables teams to convert isolated or weaker indicators across environments into strong, higher-fidelity detections.

Correlate Data Across Domains

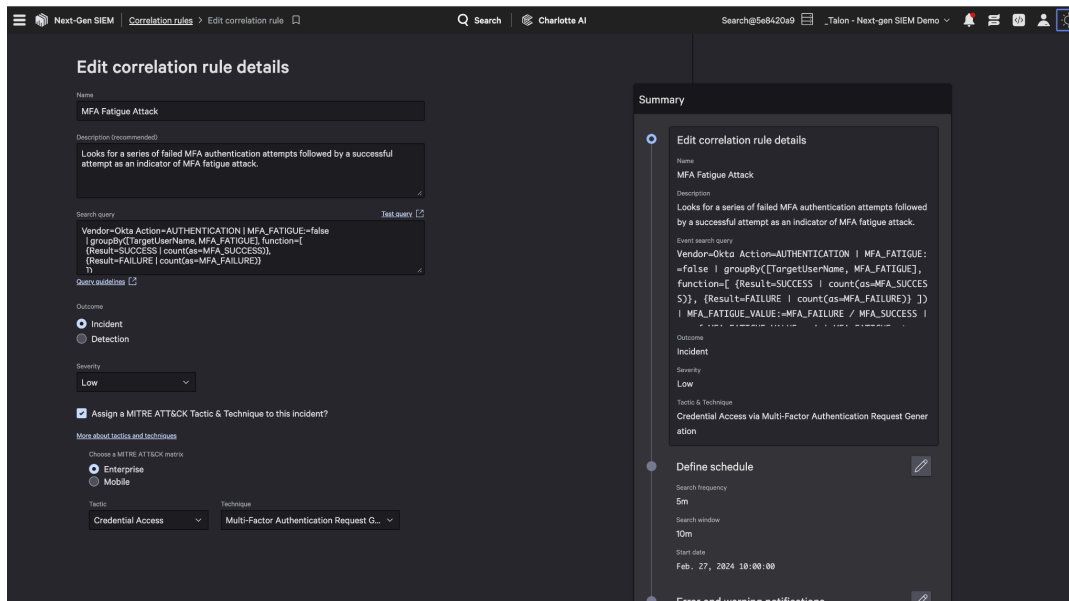


Figure 8. Falcon Next-Gen SIEM correlation rules are flexible and use the same common language used across all third-party data

Legacy SIEMs burden security teams with complex and unwieldy lists of correlation rules, often developed years or even decades ago. These rules create a flood of false positives, forcing specialized detection engineers to waste time tuning and maintaining them. Overwhelmed, many organizations turn to managed security service providers (MSSPs) with mixed results.

Falcon Next-Gen SIEM cuts through the pitfalls of outdated correlation rules. It delivers laser-accurate detection for both Falcon telemetry – including endpoint, cloud and identity data – and third-party logs. Crafted by experts with industry-leading adversary research, Falcon Next-Gen SIEM out-of-the-box correlation rules align with MITRE ATT&CK, helping detect attack techniques across the cyber kill chain. Teams can easily customize rules with a unified language for search, parsing and dashboards.

Identify Anomalous User Behavior

Falcon Next-Gen SIEM + Falcon Identity Protection

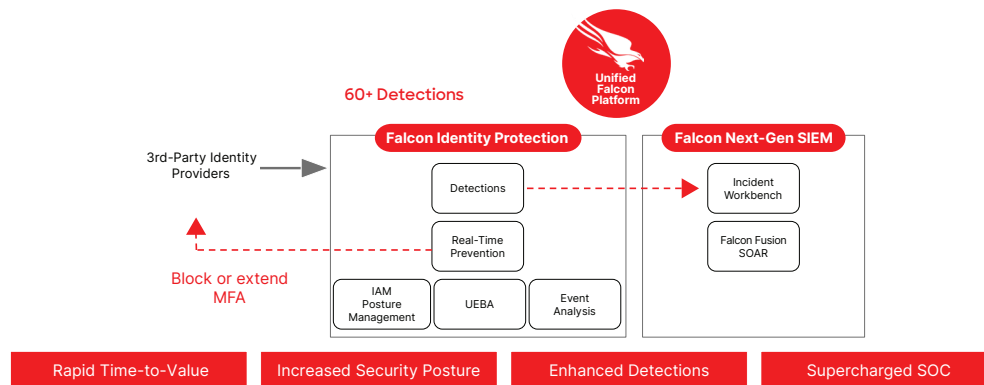


Figure 9. CrowdStrike Falcon® Identity Protection provides additional context to detect and investigate identity-based attacks and real-time prevention capabilities

User and entity behavior analytics (UEBA) has emerged as a key capability for security teams to detect anomalous behavior that could indicate attacker activity by leveraging ML and advanced analytics to identify suspicious behaviors that deviate from the norm. However, standalone UEBA solutions or those added on top of a separate SIEM typically lack the context analysts need, generate noisy false positives or suffer significant delays in alerting.

The Falcon platform unifies endpoint and identity security with a single agent and console for immediate time-to-value. With CrowdStrike Falcon® Identity Protection, organizations can instantly respond to threats with automated actions, investigating and mitigating risks in real time. The Falcon agent collects, examines and forwards user events to the Falcon platform for cloud-based analysis. Falcon Identity Protection automatically builds user and entity behavioral baselines, creating a profile of normal activity and behaviors with advanced AI/ML. Falcon's AI-driven analytics provide deeper insights into user and entity behavior, ensuring accurate threat identification and reducing false positives. Proactive prevention policies enforced at the endpoint, such as blocking users or prompting for multifactor authentication, mitigate risks and reduce the number of detections that analysts must manually investigate, thereby alleviating analyst fatigue.

Monitor with Live Dashboards

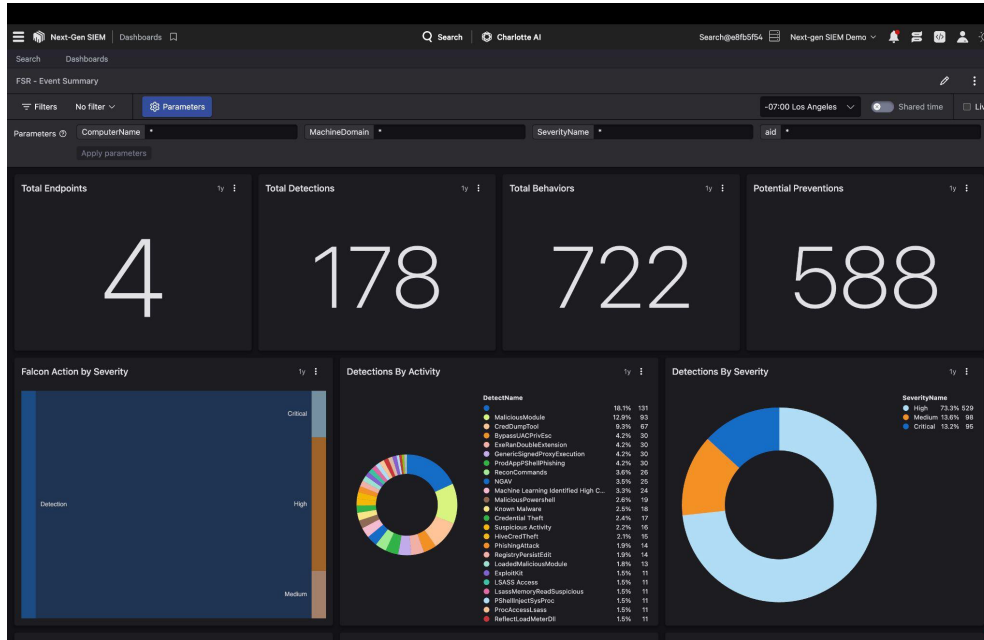


Figure 10. Aggregate and visualize your data with the intuitive dashboard builder in Falcon Next-Gen SIEM

Intuitive, visual dashboards allow your team to instantly understand large amounts of data in real time, at a glance, for security monitoring. Dashboards can be set to automatically update, ensuring teams always see the latest and greatest information, and incident responders can quickly pivot from charts to detailed search results with a single click.

Creating dashboards to meet your specific requirements can easily be done by running a query with Advanced Event Search in Falcon Next-Gen SIEM. In seconds, results can be turned into a table, graph, chart or other visualization that best highlights needed information. Powerful filters, customizable drag-and-drop widgets and contextual notes all help ensure each user gets the data they need in the way they want it.

This flexibility ensures that each team member can quickly access relevant information, minimizing the time required to identify and remediate security issues.

Investigate Incidents with a Modern Analyst Experience

To stop modern adversaries, SOC teams must move from manual, slow searches to AI-assisted investigations that put all event details and threat context at your fingertips, provide a clear picture of an attack in an elegant yet powerful visual graph, and summarize incidents in plain language with generative AI. The Falcon platform redefines the analyst experience with AI-driven features and cutting-edge workflow automation, streamlining and accelerating every step of incident response.

Unify Alerts in One Console

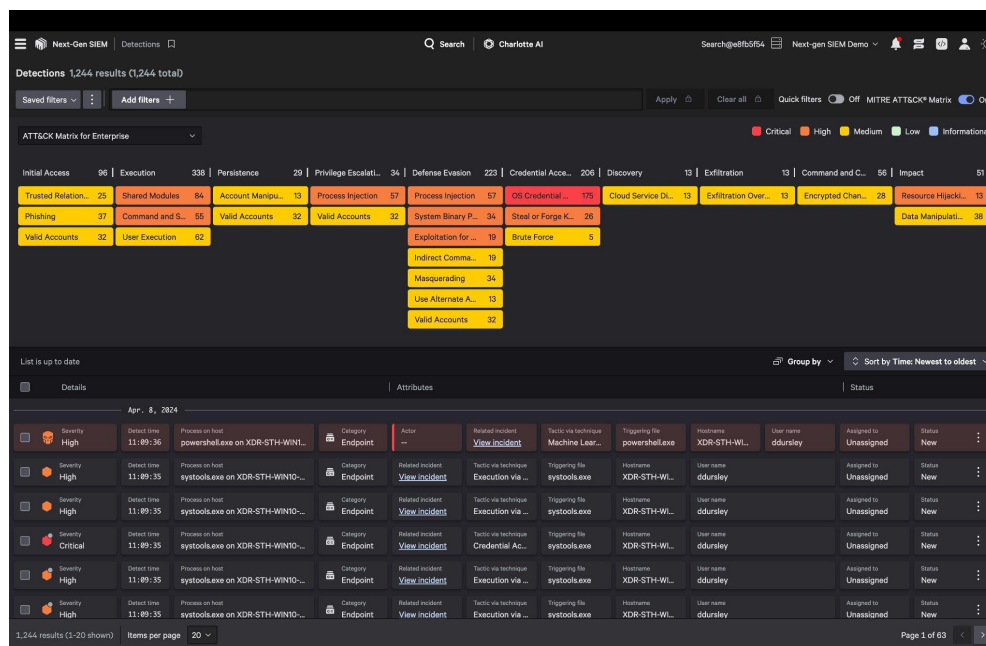


Figure 11. Crafted by CrowdStrike experts with industry-leading adversary research, out-of-the-box correlation rules align with MITRE ATT&CK

Falcon Next-Gen SIEM provides a single view for all detections, integrating Falcon-originated alerts with third-party alerts on one screen. Analysts can intelligently correlate events across multiple data sources into incidents and swiftly prioritize triage and analysis. Teams can also use CrowdStrike Falcon® Fusion SOAR workflows to automatically close noisy alerts. Analysts benefit from flexible filtering options, including severity, log source, tags and more, and can visualize the tactics and techniques used at each stage of an attack with a MITRE ATT&CK heatmap.

Investigate with Full Context

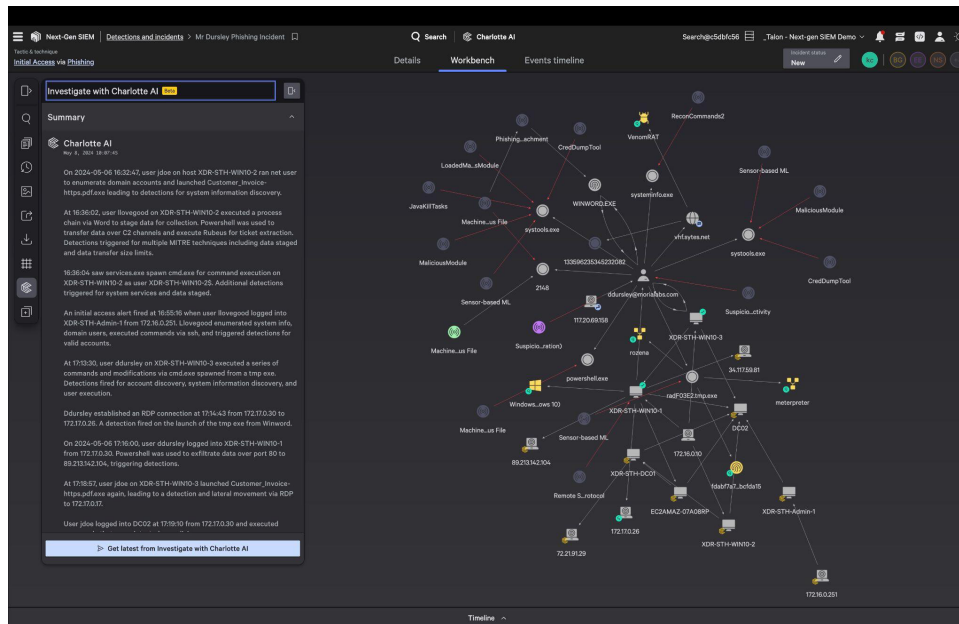


Figure 12. The Incident Workbench enhances investigation with incident visualization and expedites response with on-demand workflow automation

The Incident Workbench in the Falcon platform offers an interactive graph view for investigations with full context and actionable insights. Analysts can visualize relationships between assets, users and other entities as well as processes and executions, allowing them to explore and search alerts from multiple sources and time frames. Additional nodes or entities can be added or hidden by further traversing the graph, and entities are automatically enriched with sandbox results and threat intelligence attribution, providing investigative insights for every incident. Analysts can also run workflows, enrich incidents with threat context, and view full execution details from the Incident Workbench.

The Incident Details view reveals the IOAs, users, hosts, IP addresses and processes associated with the incident, as well as the correlation rule that triggered the incident. An Events Timeline displays the sequence of events across data sources so your analysts can determine the scope and impact to swiftly take action.

Collaborate on Cases in Real Time

The Falcon platform enables real-time collaboration, allowing analysts to update statuses, assign tasks and share notes for incidents or individual entities. Analysts can tag and notify additional team members to join the investigation, seeing changes to the incident graph in real time. Full version control provides transparency and the ability to restore previous versions, ensuring a comprehensive and coordinated response to threats.

Uplevel Analysts with Charlotte AI

CrowdStrike® Charlotte AI™, CrowdStrike's GenAI security assistant, enhances the analyst experience by enabling users of all skill levels to surface insights from their modules and take action across their environment using simple, plain-language queries. From authoring scripts to summarizing thousands of threat intelligence reports to assisting users across investigations with answers to pressing questions, Charlotte AI enables security teams to unlock greater insight from the Falcon platform and compress hours of work into just minutes or seconds. Charlotte AI also enables users to automate incident creation and summarization, surfacing suggested details to append to cases, saving hours of manual work.

Respond at Machine Speed to Fight Adversaries Gaining Speed and Sophistication

Resolve Incidents Faster and Force-Multiply Your Team with Falcon Fusion SOAR

Security teams are overwhelmed with countless false positives, repetitive tasks and the inefficiencies of “swivel chair” caused by a multitude of tools in the SOC. They need cutting-edge solutions to outpace adversaries that are becoming increasingly fast and sophisticated.

Falcon Fusion SOAR revolutionizes security operation by drastically reducing mean time to respond (MTTR) with its intuitive workflow automation and seamless security and IT orchestration. Falcon Next-Gen SIEM customers can immediately benefit from Falcon Fusion SOAR, as it is included at no additional cost.

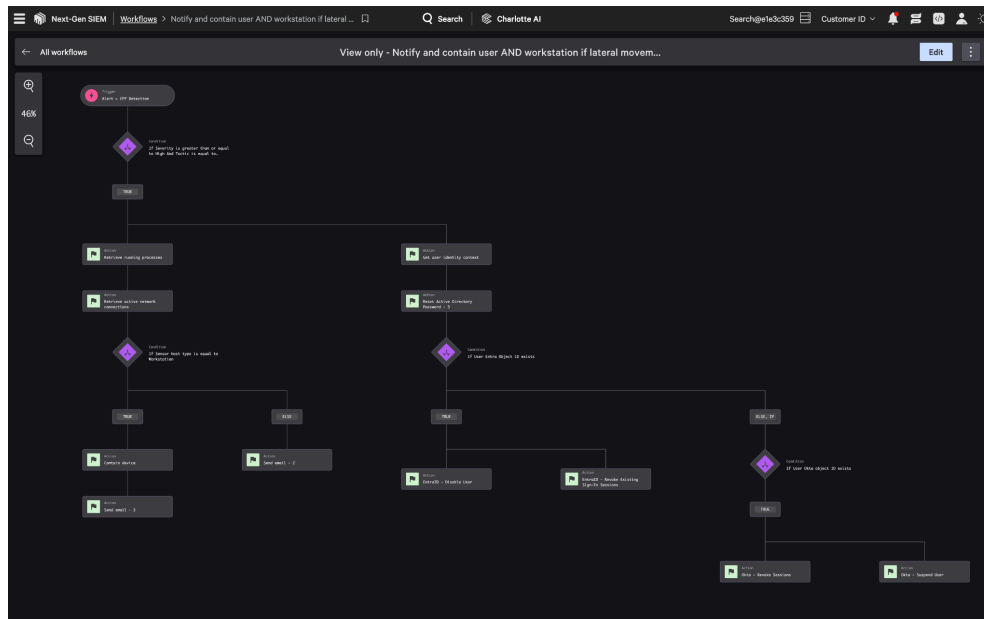


Figure 13. Falcon Fusion SOAR lets you quickly build workflows by choosing the trigger, defining the conditions and configuring actions

Falcon Fusion SOAR resolves incidents faster with no-code workflow automation. Purpose-built for the Falcon platform, Falcon Fusion SOAR helps automate any security use case, with the ability to take actions from the endpoint to the firewall. Teams can supercharge security orchestration, automation and response, so they can outpace adversaries with speed, efficiency and accuracy.

With real-time access to high-fidelity CrowdStrike and third-party data, native query and write functionality, and seamless integration across CrowdStrike modules and third-party tools, Falcon Fusion SOAR dramatically reduces time to respond, freeing up teams to focus on high-impact operations.

Falcon Fusion SOAR empowers teams to codify consistent response processes and eliminate repetitive tasks with easy-to-build workflows. With over 125 Falcon platform actions, more than 200 third-party actions and 50+ pre-built playbooks, security teams can get a head start to easily build workflows, with the ability to customize and extend Falcon Fusion SOAR even further to access additional actions. The visual builder enables analysts to build workflows by simply selecting the event trigger, defining the conditions and configuring actions across Falcon and third-party data. Falcon Fusion SOAR supports complex workflows by leveraging branching and conditional logic, loops, polling and pagination to create detailed and customized responses to specific threats.

Falcon Fusion SOAR orchestrates response across the SOC to stop adversaries in their tracks. Tight integration with the Falcon agent lets analysts drive any endpoint action. They can contain fast-moving attacks through native integration with the Falcon agent for rapid response and recovery. Analysts can contain or isolate hosts, kill processes, clear session tokens, reset user passwords and send files to sandbox environments.

An expanding set of integrations lets your team seamlessly connect tools and coordinate tasks, striking the perfect balance between machine-driven automation and human decision-making. Actions can be executed in series or parallel, with branching conditional logic and loops to evaluate and address every entity involved in an incident. All of these integrations and custom actions can be managed from the SOAR content library, which allows you to easily browse, discover and bookmark content from different vendors and for various use cases. This flexibility allows for comprehensive and adaptable incident management.

Falcon Fusion SOAR natively integrates with Falcon Next-Gen-SIEM to enable bidirectional read/write capabilities, run searches as part of workflows and utilize output for subsequent steps, ensuring a seamless and efficient response process. To further enhance threat detection and response, Falcon Fusion SOAR sends email notifications when a detection is created – these can be CrowdStrike detections, correlation rules and third-party detections.

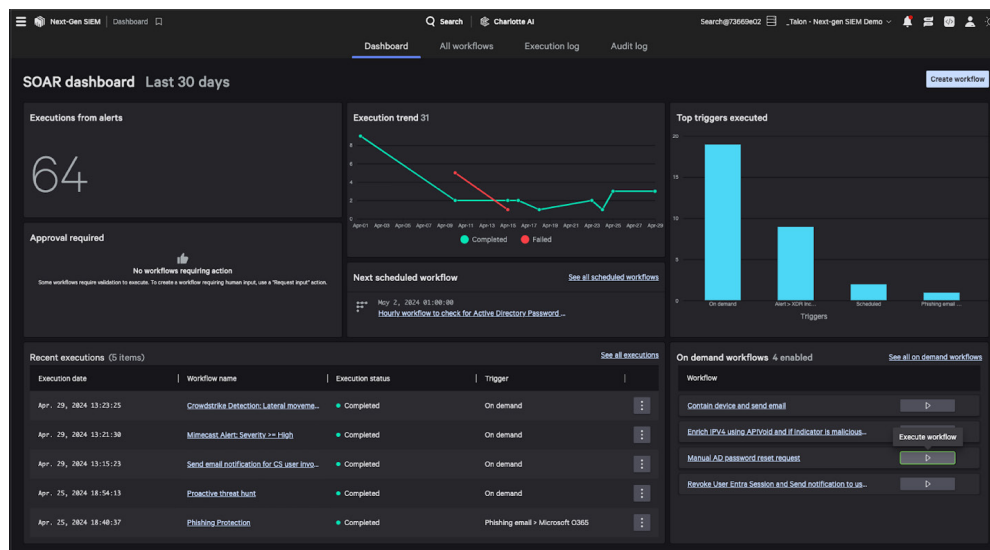


Figure 14. Continuously measure and monitor SOAR KPIs to improve your security posture with the new metrics dashboard in Falcon Fusion SOAR

Additionally, a SOAR dashboard provides critical insights into team performance and workflow automation trends, displaying executed workflows, triggers, related detections and more. By monitoring these key performance indicators (KPIs), organizations can continually assess and improve their workflow automation strategies. This data-driven approach helps teams identify areas for improvement and offers quick workflow troubleshooting to optimize your incident response efforts.

With no-code workflow automation that's built into the Falcon platform and available to all CrowdStrike customers, Falcon Fusion SOAR boosts SOC productivity, enhances collaboration and empowers your team to punch above their weight to save you time and safeguard your organizations from fast-moving adversaries.

Create Custom Apps with Falcon Foundry to Extend the Power of Falcon Next-Gen SIEM

CrowdStrike Falcon® Foundry allows teams to easily build custom applications to extend the Falcon platform and add custom content to Falcon Next-Gen SIEM. With access to modern low-code and no-code app development tools and the same CrowdStrike data and infrastructure, your team can build custom apps to solve the toughest cybersecurity challenges. When building a custom app with Falcon Foundry, security engineers can leverage the visual app builder to select their desired data source or define new ones, define their app logic, create a friendly app interface and determine user permissions. The applications can then be released and installed for security teams to use in fighting the adversaries.

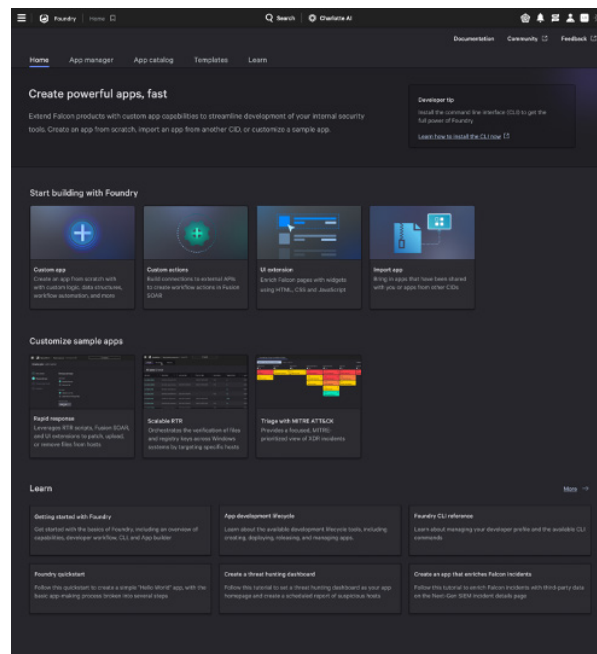


Figure 15. Falcon Foundry lets you build custom applications including actions in third-party tools

Falcon Foundry provides the ability to integrate with third-party HTTP-based APIs to import data that can enrich Falcon Next-Gen SIEM detections and incidents or create custom actions that expand the orchestration capabilities of Falcon Fusion SOAR. Additionally, Falcon Foundry enables security teams to create UI extensions, which display in key areas such as the detections page or the Incident Workbench, to provide analysts with easy access to additional information or custom remediation directly from the UI, accelerating investigations and reducing the need to pivot into other tools.

Hunt with Blazing-Fast Search

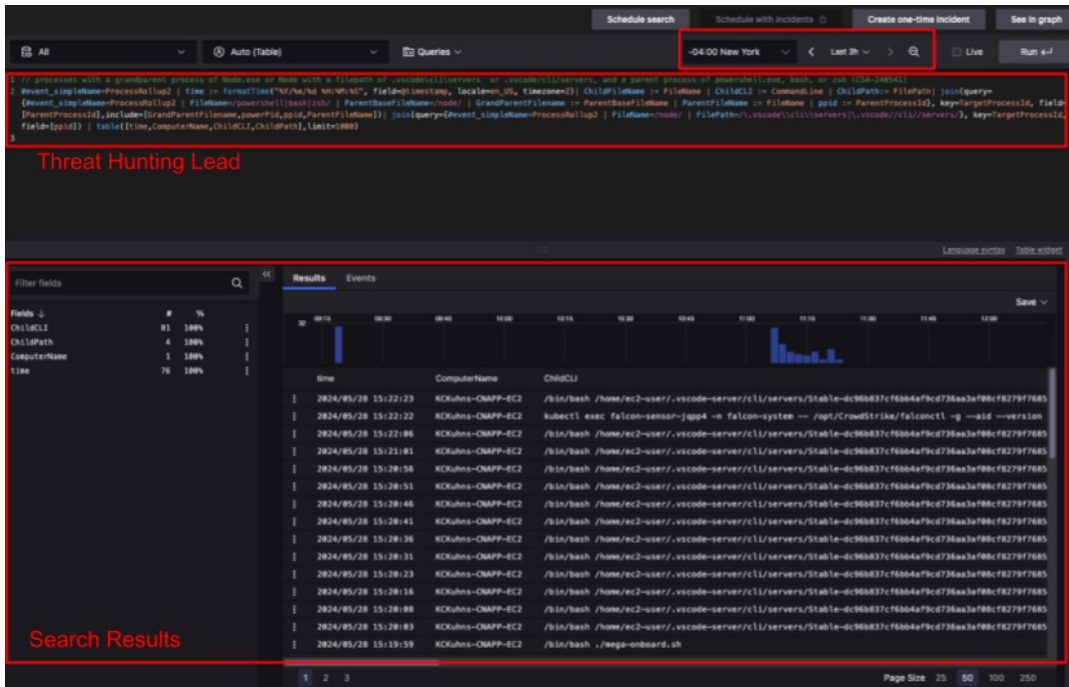
Index-Free Architecture Delivers up to 150x Faster Speed

Falcon Next-Gen SIEM is built for speed and scale, leveraging a cloud-native, index-free architecture. The power of the cloud makes storage fast, flexible, cost-efficient and convenient. Falcon Next-Gen SIEM stores data in buckets labeled with information to let its internal search engine know if sought-after data could be in them. Bloom filters and tags help the search engine avoid scanning irrelevant data for matches, reducing the amount of data to be searched by up to 100x or more.

The easy-to-learn and mature CrowdStrike Query Language helps analysts quickly extract valuable insights with advanced features like filtering, aggregation, advanced joins and regex support. Threat hunters can quickly scan all events with free-text search and easily add threat intelligence or custom content to searches through lookup files. Falcon Next-Gen SIEM takes threat hunting and searching to the next level with its powerful query language, scalability and search performance that's up to 150 times faster than legacy SIEMs.

Proactively Identify Emerging Threats with Adversary-led Intelligence

Adversaries rapidly evolve their tactics to evade detection. Continuous threat hunting based on the latest threat intelligence is critical to stop the most advanced threats. To meet this need, Falcon Next-Gen SIEM features an integrated hunting workflow with CrowdStrike's industry-leading threat intelligence. By leveraging one-click hunting leads powered by Falcon Adversary Intelligence Premium, security teams can quickly and efficiently identify even the most sophisticated adversarial tactics.



The screenshot displays the Falcon Next-Gen SIEM interface. At the top, there's a navigation bar with options like 'Schedule search', 'Schedule with incidents', 'Create one-time incident', and 'See in graph'. Below this, a query editor shows a complex query for threat hunting. A red box highlights the query text, with the label 'Threat Hunting Lead' overlaid in red. The query is a KQL statement designed to find processes with specific characteristics, such as being a grandparent process of a process with a certain name, and having specific command-line arguments.

Below the query editor, the 'Results' section is visible, showing a table of search results. A red box highlights this section, with the label 'Search Results' overlaid in red. The table has columns for 'time', 'ComputerName', and 'CmdLine'. The results show multiple instances of processes running on 'KICuhs-ONAPP-EC2' with various command-line arguments, including paths to system directories and specific tools like 'falcon-sensor-jpp04'.

Figure 16. One-click hunting leads let you seamlessly pivot from threat intelligence reports to search in Falcon Next-Gen SIEM

As CrowdStrike's threat intelligence team identifies new adversarial tactics, its threat hunting experts continuously publish new pre-built hunting leads. Using one-click actions, security teams can activate these leads to instantly pinpoint signs of malicious activity while avoiding costly upfront threat research. The pre-built hunting leads can be shared among SOC team members, modified and saved within Falcon Next-Gen SIEM to maximize operational effectiveness and enhance the team's capability to defeat adversaries. While immediately increasing the security team's productivity in finding threats, it also accelerates the team's ability to proactively adjust security controls as threats evolve.

Get 24/7 Security from the Experts

Managed Detection and Response

CrowdStrike Falcon® Complete Next-Gen MDR sets a new benchmark for managed detection and response (MDR). Leveraging the power of the Falcon platform, Falcon Complete Next-Gen MDR combines advanced technology with expert-led detection, investigation and response to provide unmatched protection around-the-clock against sophisticated threats.

Falcon Complete Next-Gen MDR expands MDR operations beyond native endpoint, identity and cloud security telemetry, incorporating critical third-party data from Falcon Next-Gen SIEM and revolutionary AI capabilities for rich attack context and rapid response. Falcon Complete Next-Gen MDR complements CrowdStrike's community of service partners to accelerate next-gen SIEM adoption and SOC transformation services.

Service Partners Simplify Implementation

CrowdStrike partners with leading global system integrators (GSIs) around the world to help you migrate, implement and operationalize Falcon Next-Gen SIEM. GSIs act as trusted advisors, guiding organizations to ensure deployments are optimized for maximum effectiveness and minimal complexity. Services can include:

- SIEM migration
 - Data ingestion
 - Custom detections and dashboards
 - Customized threat hunting
 - Custom SOAR playbook development
 - Executive and operations reporting
-

Conclusion

By leveraging the power of AI and automation, Falcon Next-Gen SIEM accelerates threat detection and response, enabling organizations to transform their security operations and stop the breach. With CrowdStrike, security teams can consolidate on a single platform and streamline workflows with a modern analyst experience so they can slash complexity and costs.

See Falcon Next-Gen
SIEM in action →

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.

