

Falcon Next-Gen SIEM: Detections

High-confidence detections built for how security teams actually work

Modern adversaries are moving faster than ever, with AI-enabled attacks increasing by 89% year-over-year in 2025,¹ dramatically accelerating the scale and speed of cyber threats. Security teams must rapidly detect threats and continuously expand coverage to keep pace with emerging tactics. Yet building and maintaining effective detections remains resource-intensive, leaving many organizations with gaps in coverage and delayed visibility into evolving threats.

Detections you can trust — without the complexity

CrowdStrike Falcon® Next-Gen SIEM transforms detection from a manual, resource-intensive process into a streamlined, intelligence-driven capability. Built on CrowdStrike's expertise and continuously updated threat intelligence, the CrowdStrike Falcon® platform delivers high-confidence detections that surface real threats while reducing noise. By combining curated detection logic, behavioral analytics, and rich context, security teams can accelerate investigations and focus on what matters most — stopping threats.

The Falcon platform consolidates CrowdStrike and third-party data, presenting detections in a unified view that enables streamlined analysis and response across the environment. Teams can start immediately with pre-built detections and easily create and customize their own to fit their environment. This approach reduces the effort required to build and maintain detections while improving coverage, lowering false positives, and enabling teams to act with greater speed and confidence.

Key benefits

- Surface high-confidence alerts across CrowdStrike and third-party data
- Understand and close detection gaps with MITRE ATT&CK®-mapped coverage
- Accelerate detection creation and optimization with AI-powered assistance
- Leverage automation to streamline alert triage and reduce manual effort
- Extend coverage for emerging threats with adversary-driven detections

¹ CrowdStrike 2026 Global Threat Report

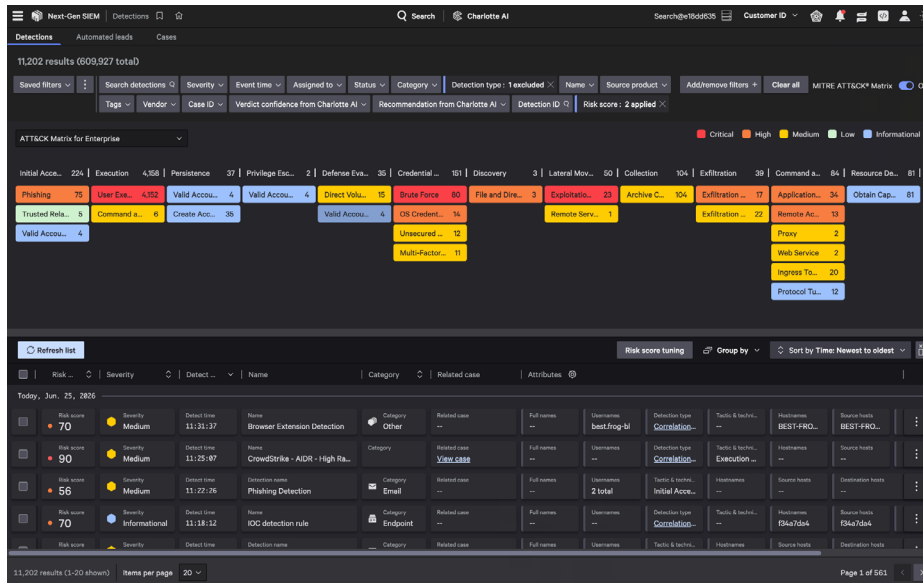


Figure 1. Falcon Next-Gen SIEM surfaces high-confidence detections in a unified view, giving analysts the context they need to investigate efficiently and respond with speed.

Key capabilities

Get Started Fast with Production-Ready Detections

Falcon Next-Gen SIEM enables teams to move from data ingestion to actionable detections quickly. With pre-built detection content and clear visibility into their detection coverage, organizations can quickly identify and close gaps without extensive setup or tuning.

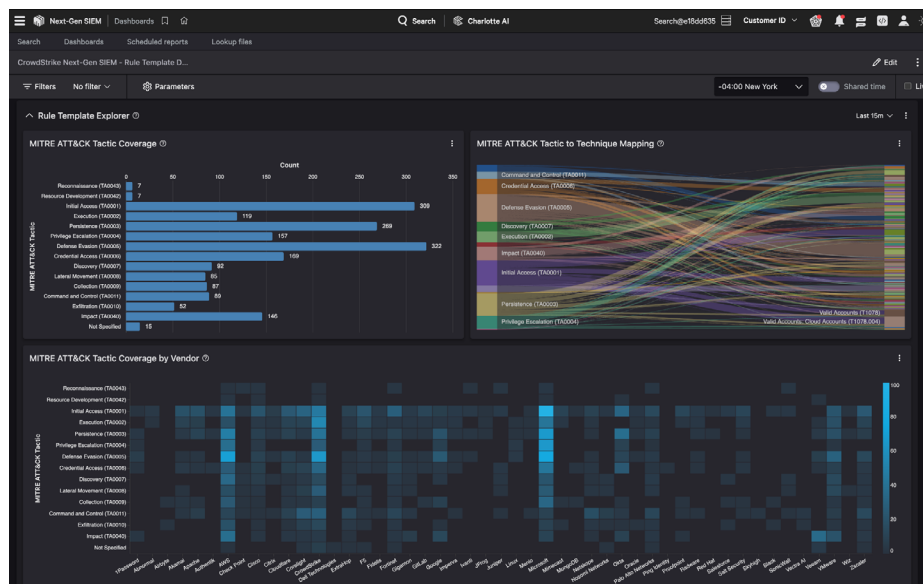


Figure 2. Production-ready detections, MITRE ATT&CK coverage visibility, and risk-based prioritization enable teams to strengthen detection coverage and streamline alert triage from Day One.

Bring clarity to detection across your entire environment

Modern attacks span endpoints, identities, and cloud environments, overwhelming teams with fragmented alerts and noise. Falcon Next-Gen SIEM combines ready-to-use content, intelligent correlation, and continuous updates to surface real threats and enable faster, more confident response.



- **Out-of-the-box detection content:** Leverage expert-built detections from CrowdStrike, backed by world-class threat intelligence and insights from CrowdStrike Falcon® Complete managed detection and response (MDR) and CrowdStrike Falcon® Adversary OverWatch™ threat hunters, continuously updated to reflect real-world attacker behavior and emerging threats, reducing the need for manual rule creation and maintenance.
- **Detection coverage visibility:** Assess gaps and understand detection coverage across MITRE ATT&CK to ensure critical techniques are monitored.
- **Streamlined alert triage:** Use risk scoring and threat intelligence enrichment to prioritize detections and focus on what matters most, then apply CrowdStrike Falcon® Fusion workflows in the Falcon platform to automate triage and response with speed and consistency.

Gain Comprehensive Detection Coverage Across the Attack Lifecycle

Falcon Next-Gen SIEM delivers a layered approach to detection coverage to identify attacks as they happen. Sensor coverage provides real-time detection and prevention across endpoints, identities, and cloud workloads. Real-time detections surface threats immediately across both CrowdStrike and third-party data, while scheduled detections uncover patterns and anomalies that emerge over time. Together, these approaches provide comprehensive coverage through a combination of CrowdStrike-developed and customizable detection logic.

Real-Time Detections				
	CrowdStrike Data	Third-Party Data	CrowdStrike-Managed	Customizable
Falcon Sensor Rules Power immediate, high-confidence detections at the endpoint to rapidly identify and stop threats, with broad coverage across known attacker behaviors.	✓		✓	✓
Automated Leads Complement Falcon sensor detections by identifying and filtering environment-specific anomalies, correlating subtle signals unique to your organization to surface stealthy threats earlier.	✓		✓	
Falcon Platform IOAs Deliver CrowdStrike expert-built detections that are continuously updated and proactively pushed in response to emerging threats, without requiring manual effort.	✓	✓	✓	
Real-Time Correlation Rules Analyze streaming data in near real time to connect signals across sources and detect threats as they unfold.	✓	✓		✓
Third-Party Detections Ingest and unify external alerts within Falcon Next-Gen SIEM to enable centralized visibility and streamlined investigation across the security stack.		✓		✓

Scheduled Detections				
	CrowdStrike Data	Third-Party Data	CrowdStrike-Managed	Customizable
Correlation Rules Correlate activity across multiple data sources over extended time windows to detect broader attack patterns beyond real-time visibility. CrowdStrike's expert-built library of over 1,400 correlation rule templates accelerates detection creation and customization.	✓	✓		✓ 1,400+ Templates Available to Deploy
Behavioral Rules Link events through behavioral patterns over time using the correlate() function to uncover complex attack sequences that would otherwise go undetected. CrowdStrike provides over 60 expert-built behavioral rule templates to accelerate detection creation and investigation.	✓	✓		✓ 60+ Templates Available to Deploy

Stay Ahead of Emerging Threats with CrowdStrike-Managed Detections

Emerging threats often require security teams to rapidly create, deploy, and maintain new detection content, creating operational burden and delaying protection. Falcon Platform IOAs eliminate this challenge by automatically delivering CrowdStrike-managed detections informed by the latest adversary activity, helping organizations detect emerging threats faster while reducing detection engineering effort.

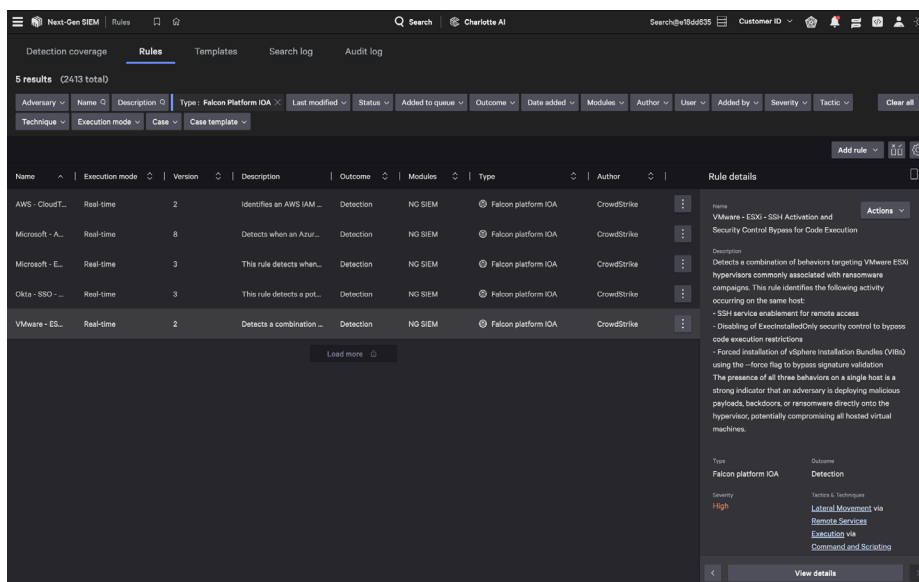


Figure 3. Stay ahead of emerging threats with Falcon Platform IOAs and the Emerging Threats dashboard, combining automatically updated detections with curated hunting content and investigation guidance.

- **Adversary-driven detections built from frontline expertise:** CrowdStrike detection engineers work alongside Falcon Complete, Falcon Adversary OverWatch, and the CrowdStrike threat intelligence and incident response teams to rapidly transform newly observed attacker behaviors — like novel intrusions or new tactics, techniques, and procedures (TTPs) in the wild — into high-fidelity detections that provide coverage before a threat is widely known.
- **Automatically delivered and continuously maintained:** Falcon Platform IOAs are automatically enabled and continuously updated by CrowdStrike, helping organizations quickly respond to emerging threats without managing detection content themselves.
- **Emerging Threats dashboard for deeper visibility:** Access curated retrospective hunting content, rule templates, and investigation guidance to better understand, hunt for, and respond to newly emerging threats.

Create and Customize Detections with Ease

When customization is required, Falcon Next-Gen SIEM provides flexible and intuitive tools that support both novice users and advanced detection engineers, reducing complexity while maintaining full control.

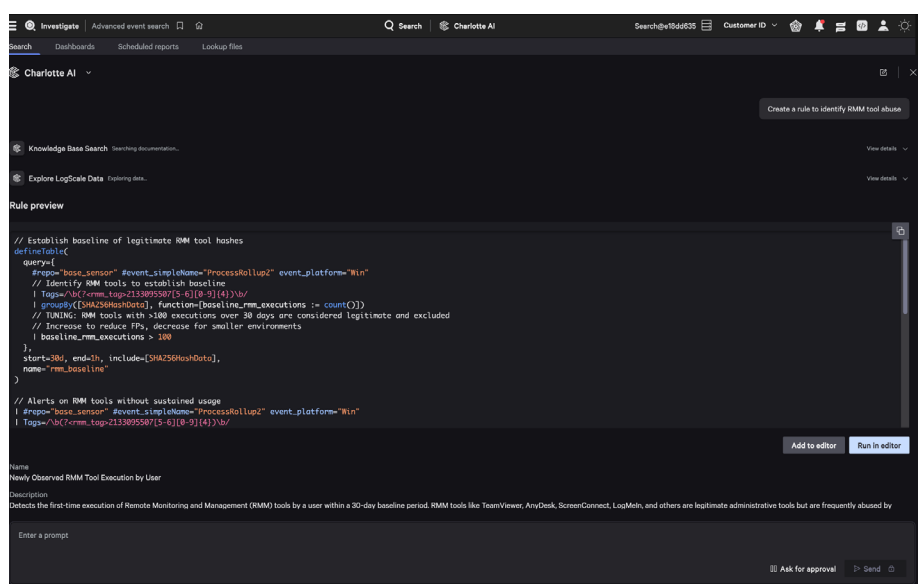


Figure 4. Create and customize detections with intuitive authoring tools, AI-powered rule generation, and detection-as-code workflows that simplify development without sacrificing flexibility.

- **Intuitive rule creation with version control:** Build and refine detections using an intuitive query builder with built-in versioning to track changes, test updates, and maintain consistency over time.
- **Detection-as-code support via API:** Create, manage, and deploy detections programmatically using APIs to support detection-as-code workflows and integrate with existing development pipelines.
- **AI-powered rule generation:** Leverage CrowdStrike's Rule Generation Agent powered by CrowdStrike Charlotte AI™ to generate, refine, and optimize detection logic, helping teams create high-quality rules faster.

Simplify Daily Operations with Intelligent Detections

Falcon Next-Gen SIEM brings together CrowdStrike and third-party detections in a unified platform, combining expert-built content, easy-to-create custom detections, and intelligent correlation to surface real threats across your environment. With risk-based prioritization, enriched context, and automation, analysts can cut through alert noise, quickly adapt detections to their environment and evolving threats, and respond with greater speed and confidence and less manual effort.

Schedule a Demo



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/>

Follow us: [Blog](#) | [X](#) | [LinkedIn](#) | [Facebook](#) | [Instagram](#)

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