

Charlotte Agentic SOAR

Accelerate security operations with AI-powered automation

In today's SOC, every second matters. Analysts are buried in alerts, overwhelmed by false positives, and swiveling across too many tools, while adversaries move at machine speed. In 2025, the fastest recorded eCrime breakout time was a mere 27 seconds, according to the CrowdStrike 2026 Global Threat Report. To keep pace, teams need more than automation. They need intelligence that can reason, coordinate, and act — quickly, consistently, and under control.

CrowdStrike® Charlotte Agentic SOAR brings AI-driven agents and automation together in a unified response layer across the CrowdStrike Falcon® platform. Charlotte Agentic SOAR combines the precision and predictability of deterministic automation with the flexibility and adaptability of intelligent agents that operate with shared context, reason through complex situations, and coordinate actions in real time. Together, they amplify human expertise, accelerate response, and enable security teams to stop AI-accelerated adversaries.

Charlotte Agentic SOAR includes:

- A workflow engine to coordinate actions and agents, unifying response across tools
- CrowdStrike® Charlotte AI™ first-party agents to scale elite analyst judgment with autonomous reasoning and adaptive, context-aware decision-making
- Charlotte AI AgentWorks for building, testing, and managing custom agents in plain language
- Unified case management to streamline investigations in a single command center
- CrowdStrike Falcon® Foundry to build AI-powered security apps and extend automation across the SOC

Key benefits

- Unify threat detection, investigation, and response across the Falcon platform
- Reduce manual work to improve speed, consistency, and accuracy
- Accelerate response with an expanding ecosystem of agents, integrations, and actions
- Maximize analyst impact with AI agents and adaptive, agentic workflows

Key capabilities

Build Agentic Workflows with Confidence

Charlotte Agentic SOAR modernizes how security teams collaborate, automate, and respond. Analysts can build and run workflows that combine deterministic automation with adaptive AI agents, all within a single, unified experience.

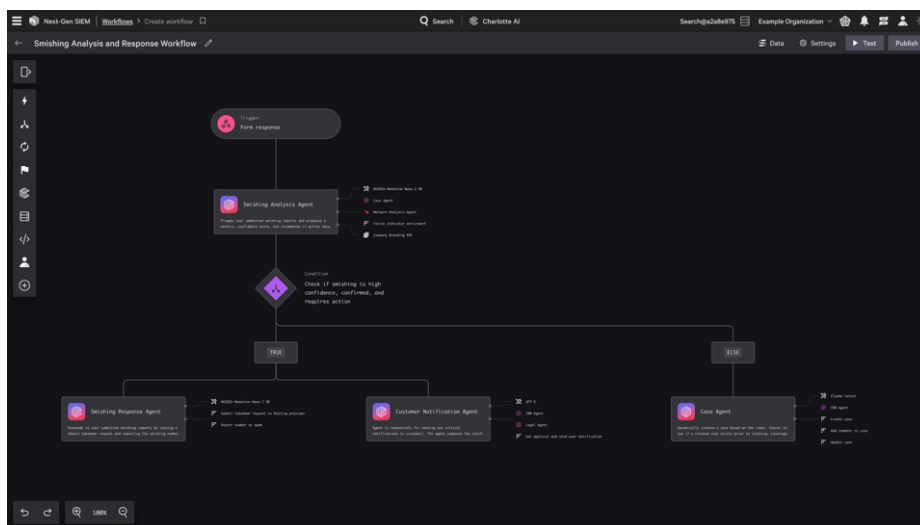


Figure 1. Charlotte Agentic SOAR combines deterministic structure with agentic reasoning in a single interface.

Charlotte Agentic SOAR by the numbers:

- 160+ out-of-the-box playbooks
- 4,500+ third-party workflow actions
- 290+ third-party integrations
- 220+ workflow triggers
- 10+ out-of-the-box agents

- **Unite deterministic and agentic automation:** Blend deterministic workflows for repeatable, well-defined tasks with agentic workflows that can reason through ambiguity or complexity. Automate routine actions like alert notifications, enrichment, and containment, while agents handle nuanced tasks such as cross-domain correlation, context-driven escalation, and decision support.
- **Design smarter, faster workflows:** Build automation in minutes with an intuitive visual builder: Choose a trigger, set conditions, and configure actions. With Charlotte AI's Workflow Generation Agent, teams can describe what they want in plain language and have workflows generated for them — reducing setup time, lowering the barrier for less technical users, and freeing analysts for higher-value work.
- **Orchestrate human-agent collaboration:** Coordinate multiple agents that share context and collaborate in real time. Use out-of-the-box agents for common security tasks, or create custom agents in Charlotte AI AgentWorks with no code. Analysts stay in control through human-in-the-loop oversight, approving key steps, supervising execution, and ensuring actions align with policy and intent.

Streamline Investigation and Response with Native Case Management

Case Management, a native capability of the Falcon platform, transforms how analysts investigate and resolve incidents, transforming static recordkeeping with an intelligent command center for the SOC. It centralizes alerts, context, and actions into a single workspace so analysts can move seamlessly from detection to resolution without switching tools.

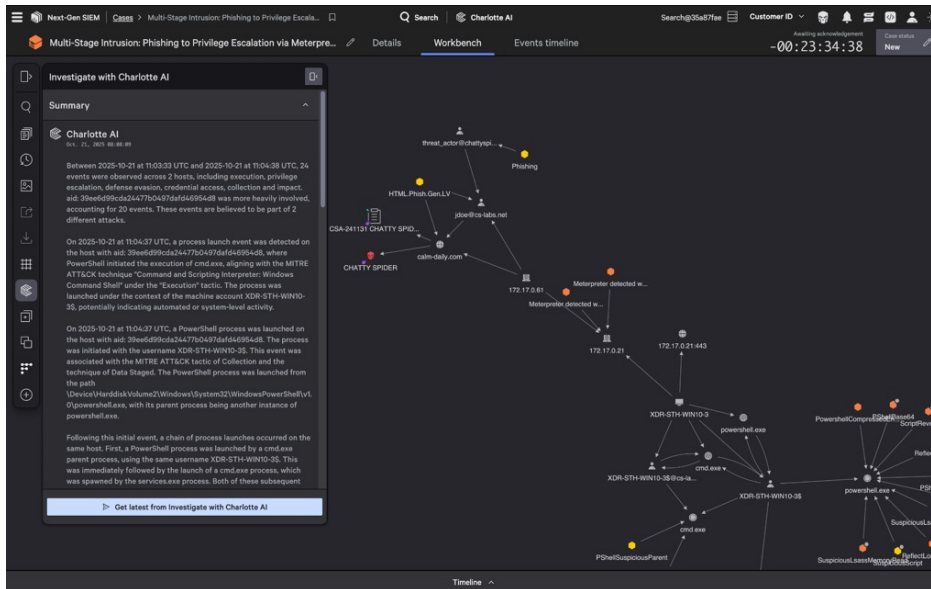


Figure 2. Case Management, integrated with Charlotte Agentic SOAR, centralizes investigations for a more collaborative response.

- Drive cohesive, case-centric response:** Establish a single source of truth for every investigation. Automatically create cases from detections, or manually open cases to centralize evidence, context, and response actions. Track ownership, SLAs, and progress to improve collaboration, accountability, and shift handoffs. Built-in visualizations and Charlotte AI-powered insights help analysts understand relationships, summarize findings, and take informed, decisive action faster.
- Automate end-to-end case resolution:** Reduce manual work and accelerate response. Charlotte Agentic SOAR can auto-create cases, enrich them with context, trigger investigation workflows, and execute containment or remediation actions across Falcon modules and third-party tools while maintaining human oversight and control. Bi-directional integrations with IT ticketing systems (e.g., ServiceNow) enable coordinated handoffs across SecOps and IT.
- Improve SOC performance with actionable metrics:** Get complete visibility into operational performance. Track SLA adherence, ownership, and case resolution times. Use workflow execution metrics to identify bottlenecks and optimize automation. SOC leaders get a real-time view into efficiency, collaboration, and performance trends to continuously strengthen readiness and balance team workloads.

Unify and Scale Security with a Connected Ecosystem

Modern security automation requires a broad, reliable integration ecosystem. Charlotte Agentic SOAR extends the Falcon platform's reach by unifying integrations, playbooks, workflow actions, and agents across the security stack so teams can detect, investigate, and respond faster from a single operational view.

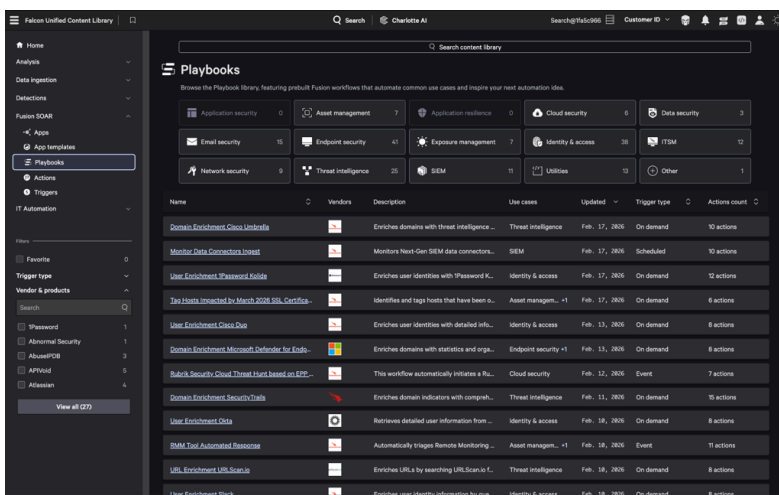


Figure 3. Charlotte Agentic SOAR unifies integrations and playbooks across the security, IT, and AI ecosystems to accelerate automation and unify the SOC.

- Accelerate automation with a unified content library:** The Content Library consolidates integrations, playbooks, and workflow actions across the Falcon platform, with SOAR content in one place. Filter by vendor or use case to quickly discover and deploy the content you need. Built-in technical details and documentation speed implementation, expand coverage across new use cases, and help teams realize value faster.
- Expand and customize with Falcon Foundry:** Falcon Foundry extends Charlotte Agentic SOAR with low-code development tools and AI-powered guidance. The Foundry App Generation Agent uses natural language to generate templates and connect to APIs so teams can quickly build, customize, and scale integrations across their environment.
- Connect agents across the security ecosystem:** With support for the Model Context Protocol (MCP), Charlotte Agentic SOAR enables agents to collaborate across your ecosystem with shared context. Use first-party and third-party agents from Charlotte AI AgentWorks or connect external AI systems to build intelligent, adaptive workflows. The result is a more unified SOC, powered by agent-to-agent and human-to-agent collaboration.

Redefining investigation and response for the agentic SOAR era

Charlotte Agentic SOAR is the orchestration layer for the agentic SOC, uniting automation, intelligent agents, and human oversight in one platform. With no-code workflow creation, AI-assisted case management, and an ecosystem of integrations and agents, SOC teams can triage, investigate, and respond faster while staying in complete control.

Charlotte Agentic SOAR Capability Overview

	Charlotte Agentic SOAR Essentials <i>Available to Falcon Insight XDR customers via the Charlotte AI free-credit promotion¹</i>	Charlotte Agentic SOAR <i>Available as a standalone offering or included with Falcon Next-Gen SIEM²</i>
Real-time response actions on the endpoint (e.g., network isolation, quarantine, etc.)	✓	✓
Workflow and Case Management		
Workflows	✓ (Fair-use limits apply)	✓ (Fair-use limits apply)
Third-party Integrations	Limited to utility and ITSM connectors — varies by licensed modules	✓
Case Management	Limited to Falcon data only	✓
Case and Data Retention	✓	✓
Agentic and Generative AI		
Charlotte AI credits required. Credits are available through an opt-in promotion or can be purchased with the Charlotte AI module. Falcon Next-Gen SIEM customers may also be eligible for additional free credits based on paid data ingestion. All credits roll into a single shared pool that can be used across Charlotte AI features on the Falcon platform.		
Chat <i>(via the Charlotte AI module or Global Navigation in the UI)</i>	✓ Limited to 50 Charlotte AI credits	✓
Charlotte AI Agents <i>(agents are based on a user's licensed Falcon modules)</i>	✓ Limited to 50 Charlotte AI credits	✓ Includes Charlotte AI's Detection Triage Agent and Response Agent
Charlotte AI AgentWorks <i>(e.g., agent building, agent testing, performance management)</i>	✓ Limited to 50 Charlotte AI credits	✓

1. The Charlotte AI free-credit promotion is available for eligible customers to opt in directly from the Falcon console. This promotion provides access to Charlotte AI-powered chat, agents, and embedded GenAI features across Falcon modules. Customers receive 50 Charlotte AI credits, renewing monthly.
2. Credit allotment for Falcon Next-Gen SIEM customers is based on paid data ingestion.

Embedded GenAI Features <i>(e.g., Workbench incident analysis and summarization, command-line analysis)</i>	✓ Limited to 50 Charlotte AI credits	✓
LLM Inference in Workflows <i>(via the "LLM-Completion" workflow action)</i>	✓ Limited to 50 Charlotte AI credits	✓
Third-party Connectors and Bi-directional MCP Access		✓

Falcon Foundry		
Custom App Creation	✓	✓
App Execution <i>(consumes credits)</i>	✓ Limited to 50 Charlotte AI credits	✓

Free trial

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/>

