

# Charlotte AI Agents

Automate time-intensive tasks with mission-ready agents

## Challenges

Security teams are fighting 21st-century adversaries with 20th-century tools. Analysts are buried in alerts, disconnected systems, and manual workflows that slow response and drive burnout.

Threat actors are early and ruthless adopters of AI, using it to accelerate every stage of the kill chain. Cybercriminals and nation-state groups (such as FAMOUS CHOLLIMA) are already applying AI to automate reconnaissance, generate convincing phishing, and scale exploit chaining, compressing breakout time to seconds.

Meanwhile, defenders are stuck with fragmented tools, siloed data, and nonstop alerts. Analysts spend precious minutes stitching together context, assessing triage, and performing manual, swivel-chair work that can be error-prone and inconsistent across analysts — while rigid, rule-based automation can't adapt to new attack patterns or scale expert decision-making.

If teams can't accelerate decisions and execution, they face longer dwell time, longer exposure windows, and higher breach impact. If your defenses are relying on human reaction time, you'll always be playing catch-up.

## Solution

It's time for a new operation model; one built for the AI era. The agentic SOC reimagines security operations with human-led, agent-executed security, where defenders direct AI agents that can reason, decide, and act with expert-level judgment at machine speed. This moves security operations from alert-driven firefighting to proactive, adaptable defense.

CrowdStrike® Charlotte AI™ is the brain of the agentic SOC, helping teams command fleets of agents, from out-of-the-box agents delivered across CrowdStrike Falcon® modules to custom agents built with Charlotte AI AgentWorks. These agents scale expertise and automate time-intensive work across security operations, from data onboarding and detection triage to investigations, threat hunting, and malware analysis.

Unlike brittle, deterministic automation, Charlotte AI agents can reason over complex scenarios, unstructured data, and edge cases and work together as a coordinated system to deliver execution at scale.

## Trained on elite analyst judgment

Charlotte AI agents are trained on the real-world decisions of the elite SOC analysts for CrowdStrike Falcon® Complete managed detection and response.

The result? Charlotte AI's agents go beyond summarization and can reason, decide, and act with expert-informed judgment at scale.

Key benefits

Faster Outcomes Across Security Operations

- Offload time-intensive work to Charlotte AI agents, from triage to risk analysis.
- Reduce toil, accelerate response, and refocus analysts on high-impact work.

Scale Expertise Without Added Headcount

- Charlotte AI's agents inherit the Falcon platform's unified telemetry and shared security context to apply expert-informed judgment.
- Extend your team's impact 24/7 with consistent execution across common SOC workflows.

One Platform to Build, Govern, and Scale Agents

- With Charlotte AI AgentWorks, build, test, and manage agents using natural language.
- Centralize AI adoption to control access, monitor credit usage, and audit agent activity.

Always Under Analyst Control

- Agents operate within defined guardrails with clear explanations and inspectable source data.
- Audit-ready logs and bounded autonomy keep analysts in control of all agent execution.

Get free Charlotte AI credits

Eligible customers can opt in to receive **50 free credits per month**, renewing monthly, to power agent actions across the Falcon platform and experience Charlotte AI and its mission-ready agents.

Charlotte AI agents

Charlotte AI agents deliver outcome-driven automation across the Falcon platform. Agent availability depends on the Falcon modules you license (see table below). Charlotte AI credits power agent actions across Falcon as a single currency for AI usage.

| Agent Name                    | Description                                                                                                                                                                | Required Module            |
|-------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------|
| Detection and Response        |                                                                                                                                                                            |                            |
| Detection Triage Agent        | Analyzes detections, classifies true/false positives, recommends close vs. escalate, and documents reasoning to speed triage                                               | Charlotte AI               |
| Response Agent                | Guides detection investigation by generating/answering analysis questions across Falcon data; documents reasoning to streamline investigations                             | Charlotte AI               |
| Exposure Analysis             |                                                                                                                                                                            |                            |
| Exposure Prioritization Agent | Performs automated CVE triage, analyzes exploitability using native sensor telemetry, maps business impact and attack paths, and generates prioritized remediation actions | Falcon Exposure Management |

| Agent Name                               | Description                                                                                                                                    | Required Module                       |
|------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------|
| <b>Threat Intelligence and Hunting</b>   |                                                                                                                                                |                                       |
| <b>Malware Analysis Agent</b>            | Automates malware analysis (lookups, extraction, comparison), generates YARA rules, and provides attribution and response recommendations      | Falcon Adversary Intelligence Premium |
| <b>Hunt Agent</b>                        | Executes hunting queries at scale and continuously scans for threats, producing clear findings for rapid response                              | Falcon Adversary Intelligence Premium |
| <b>Next-Gen SIEM Analysis</b>            |                                                                                                                                                |                                       |
| <b>Search Analysis Agent</b>             | Uses natural language over event data, explores relationships across complex datasets, and delivers insights without syntax expertise          | Falcon Next-Gen SIEM                  |
| <b>Correlation Rule Generation Agent</b> | Creates new detection rules, optimizes for accuracy, and accelerates consistent detections with less expert dependency                         | Falcon Next-Gen SIEM                  |
| <b>Data Onboarding Agent</b>             | Builds end-to-end next-gen SIEM pipelines from natural language, automates onboarding configuration, and resolves issues to keep data reliable | Falcon Onum                           |
| <b>Query Translation Agent</b>           | Translates Splunk queries into Falcon-native CQL, preserves existing logic, and accelerates investigations without manual rewrites             | Falcon Next-Gen SIEM                  |
| <b>Automation</b>                        |                                                                                                                                                |                                       |
| <b>Data Transformation Agent</b>         | Normalizes data using plain language to streamline workflows without coding                                                                    | Falcon Next-Gen SIEM                  |
| <b>Workflow Generation Agent</b>         | Translates natural language into Falcon Fusion SOAR workflows to automate investigation/response and improve consistency across teams          | Charlotte AI                          |
| <b>Falcon Foundry Agent</b>              | Converts natural language requests into Falcon Foundry app structure/ components to accelerate custom app creation and iteration               | Charlotte AI                          |

[Learn more about Charlotte AI's mission-ready agents](#)

## Forward-Looking Statements

This data sheet may include discussion of unreleased services or features. Any unreleased services or features referenced here are still in development and subject to change. Customers should make their purchase decisions based upon 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/>

