



# Charlotte AI

*Leading Cybersecurity in the AI Era*

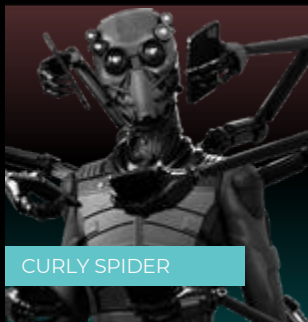
Salvador Polido Celestino

Sr. Regional Sales Engineer - CrowdStrike



# AI-enabled adversaries are accelerating...

Traditional Defenses  
Are Obsolete



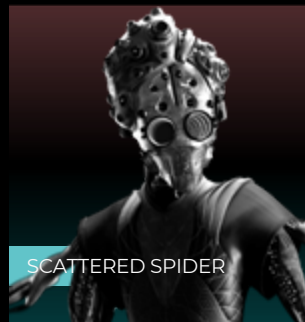
35% increase in "interactive  
intrusion" techniques

AI Has Weaponized  
Deception at Scale



720% increase in AI  
accelerated human  
manipulation

Speed Has Become  
the Ultimate Offense



less than 24 hours: account  
takeover to ransomware

Fragmentation Gives  
Adversaries the  
Advantage



Cross-domain attacks are the  
norm: siloed tools cannot  
detect

...intensifying the gaps between security teams and  
adversaries



RESPOND  
AT MACHINE SPEED

APPLY REASONING  
AT SCALE

OPERATE WITH  
D.E.P.,  
UNIFIED CONTEXT

TAKE  
AUTHORIZED  
ACTION

# Security must evolve

Modern attacks demand agentic defense

ADAPT  
ON THE FLY

EXPLAIN  
AND DOCUMENT  
BE A SON IN O

# Charlotte AI

The brain of the  
agentic SOC



# Accelerate Outcomes and automate high-value work

with Charlotte AI



## AUGMENT ACCELERATED INSIGHTS

## ASSIST INSTANT ANSWERS

Chat	Natural language interactivity with Falcon data
Prompt books	Shareable prompt libraries to scale knowledge

Investigate with Charlotte AI	Dynamic incident mapping and summaries
Command-Line Explanation	Simplified and deobfuscated scripts

## AUTOMATE OFFLOAD INVESTIGATION & RESPONSE

Agentic Triage	Automate detection triage and recommend next steps	AgentWorks	Build, orchestrate and scale AI agents securely
Agentic Response	Automate investigation with elite judgment	Multi-Agent Collaboration	Seamlessly and securely connect with ecosystem agents during investigation
Agentic Workflows	AI-driven SOAR playbooks		
Workflow Generation	Build Falcon Fusion workflows with plain- language prompts		

TIME SAVINGS



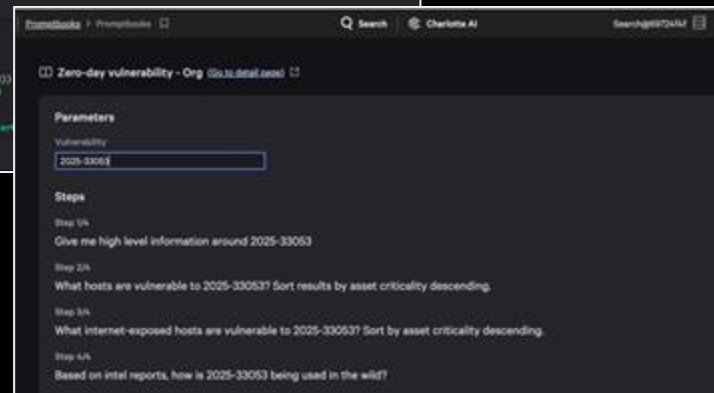
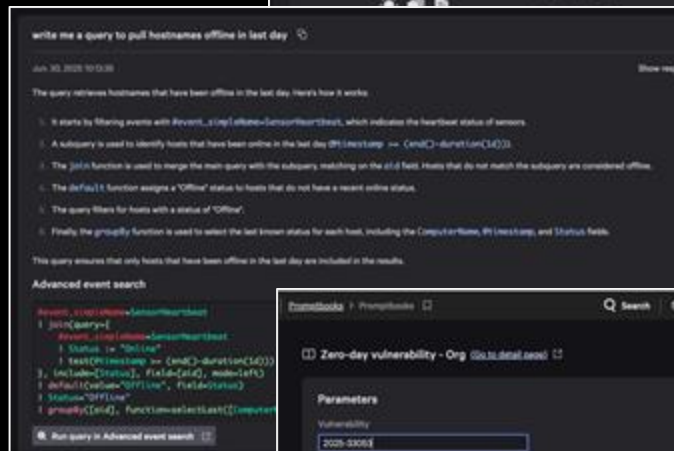
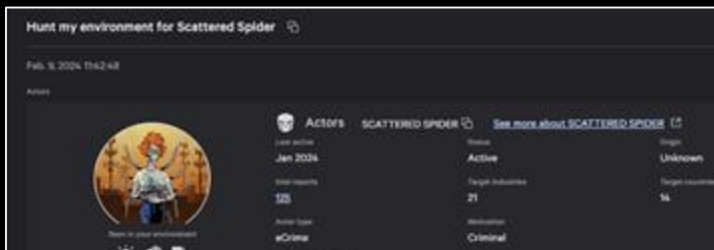
# Charlotte AI Conversational AI

Get fast answers to plain-language questions:

- Answer questions with actual Falcon platform data
- Generate summaries, analyze cross-module insights, and ask follow-up questions
- Create reusable prompt collections to standardize workflows

Why it matters:

- Querydata intuitively
- Accelerate Falcon onboarding
- Get traceable, auditable answers



# Charlotte AI Agentic Detection Triage

Automatically analyze new detections,  
to obtain to g:

- Triage verdict+confidence level
- Clear explanation
- Next-step recommendation

Why it matters:

- Save 5+ minutes per detection
- Apply the expertise of Falcon Complete
- Prioritize real threats
- Triage analysis does not consume Charlotte AI credits

*Time savings represents the amount of time an analyst would have spent triaging detections but can now use that time for other skilled work while Charlotte triages the based on factors such as total alert volume.*

The screenshot displays the CrowdStrike Falcon console interface. At the top, there are filters for 'Assign...', 'Resolution', and 'Status'. Below this is a table of detections. The first detection is 'Suspicious domain replication', which is assigned to 'Unassigned' and has a status of 'New'. The detailed view of this detection shows the following information:

- Name:** Suspicious domain replication
- Description ID:** 568b0407b624c19c7a875f797a1f1e5d5d804c7b624c19c7a875f797...
- Description:** katya.isabella performed domain replication from SPC-DESKTOP-KAT.
- Severity:** High
- Tools & technique:** Credential Access via DCsync
- Start time:** Apr. 15, 2025 21:38:11
- End time:** Apr. 15, 2025 21:38:11

Below the detection details, there is a section titled 'Triage with Charlotte AI'. This section provides a recommendation of 'Escalate', a triage priority of '239', and a verdict of 'False positive'. It also includes a triage status of 'Finished' and a triage confidence of 'Low'. The explanation states: 'The detection labeled as "Suspicious domain replication" was identified as a false positive. This detection was triggered because a user executed a domain replication request, which is often associated with the DCsync technique under the Credential Access tactic in the MITRE ATT&CK framework. The DCsync...'. There is a 'Report' button and a link to 'See triage details from Charlotte AI'.

At the bottom, there is a 'Status' section showing the detection is assigned to 'Salvador Pulido SE Demo' and has a status of 'Closed'. The triage tag is 'true\_positive'.



# Charlotte AI Agentic Response

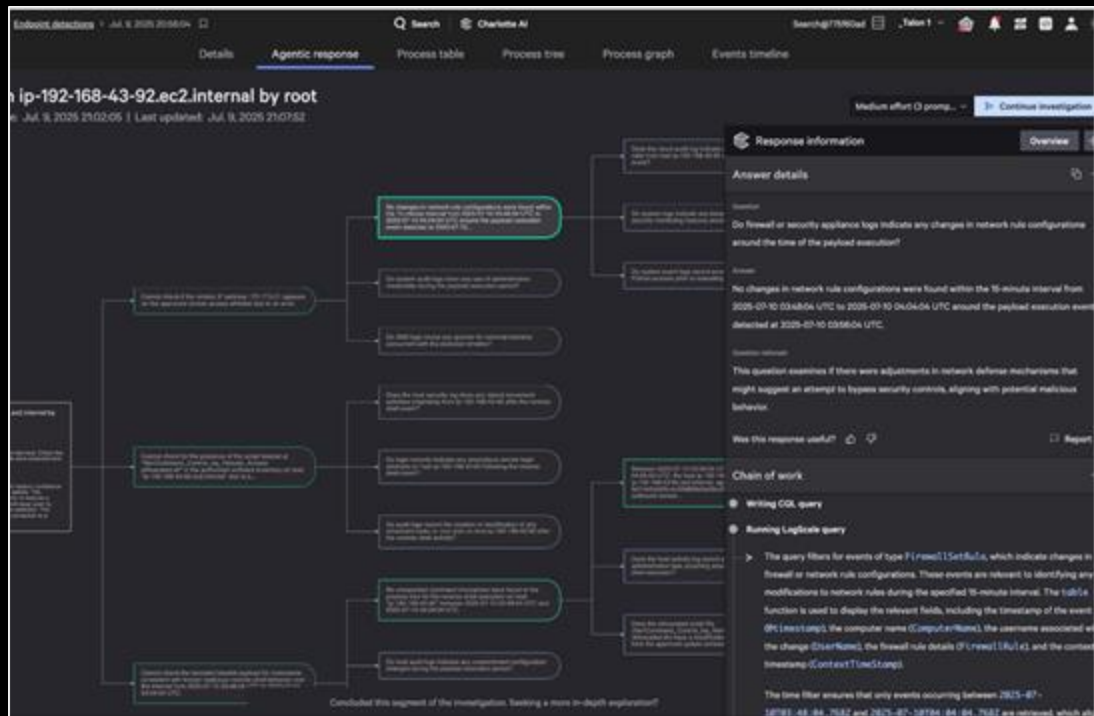
## Autonomously investigate detections:

- Generates analysis questions and answers them
- Explains rationale for each question
- User-activated through the Detection Details view (manual) or via Falcon Fusion SOAR workflows (automated)

## Why it matters:

- Save 10+ minutes per credit spent
- Apply the latest insights from Falcon Complete Next-Gen MDR at scale with consistency

*The time savings of more than 10 minutes per investigation is an estimate based on Agentic Response's ability to automate tasks that would otherwise require more than 10 minutes. This should not be interpreted as a guarantee that this will lead to a 10 minute reduction in the total investigation time or mean time to respond (MTTR).*





- **Visualize connections:** Map users, devices, and activity linked to an incident to assemble the full scope of an attack
- **Streamline documentation:** Auto-generate incident summaries for documentation and handoff

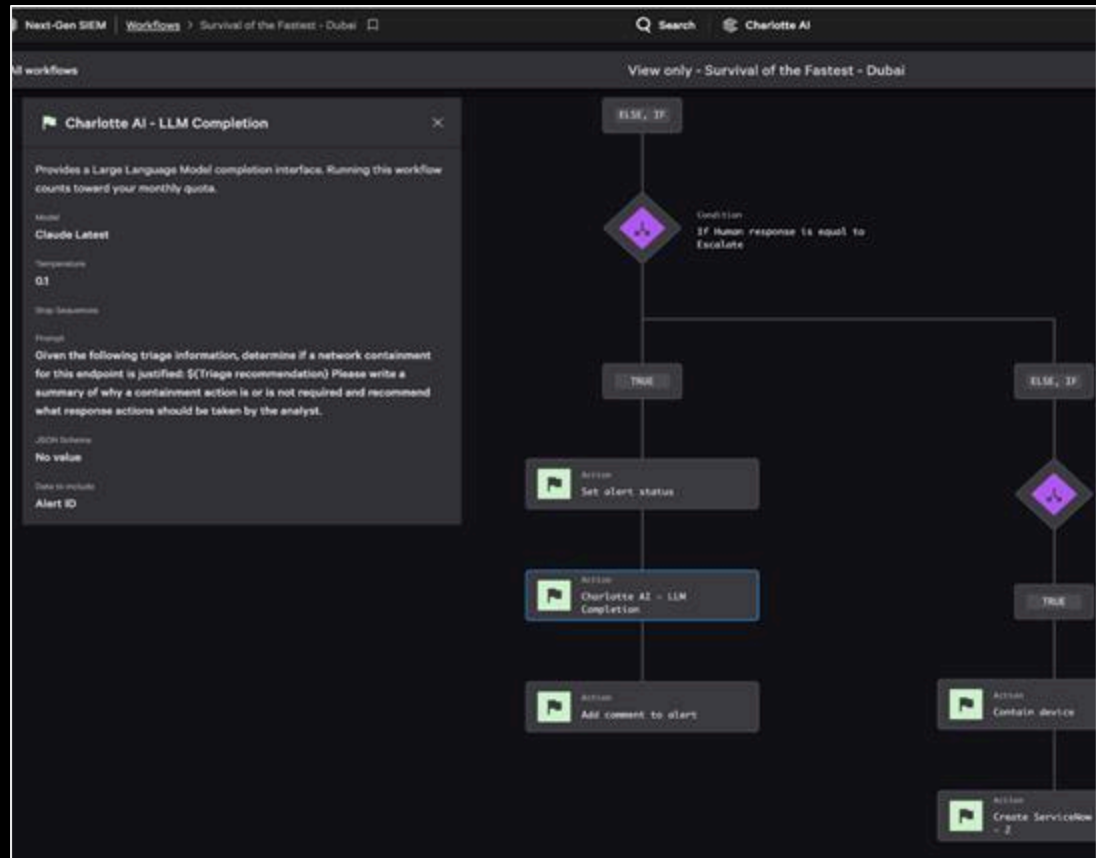
# Charlotte AI Agentic Workflows

## Customize AI-powered playbooks:

- Bring AI models into Falcon Fusion SOAR workflows to analyze 1st/3rd party data
- Use natural language to direct model analysis
- Configure automated actions based on AI reasoning

## Why it matters:

- Create adaptable, automated response
- Generate audience-ready outputs
- Use cutting-edge models —no extra infrastructure or agreements



We stop  
breaches.

*Protection that powers you*



Thank you