

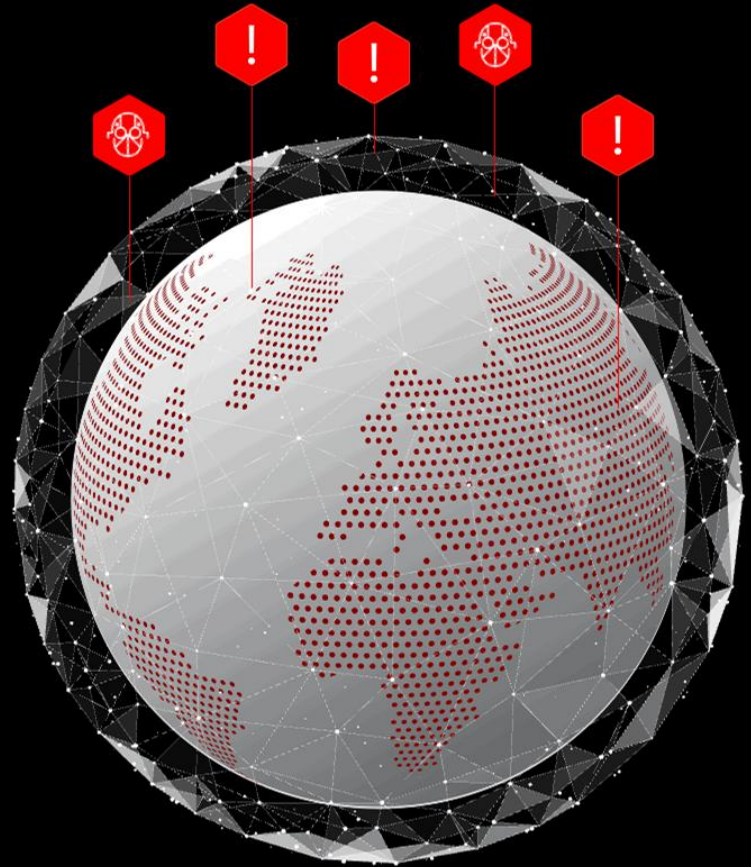
Entspannt digitalisieren: So macht KI Ihre Ämter widerstandsfähig

CrowdStrike Charlotte AI +
Vectra.AI Attack Signal Intelligence



We Stop Breaches

Protection that powers you.



7'0"
6'10"
6'
5'10"
5'8"
5'6"
5'4"
5'2"
5'0"
4'10"

6'8"
6'2"
6'0"
5'10"
5'8"
5'6"
5'4"
5'2"
5'0"
4'10"

AI has supercharged the adversary

From deepfakes to AI-generated profiles, adversaries are scaling deception and disruption with AI

Fastest eCrime breakout time

51 sec

Attacks involve insider threats

40%

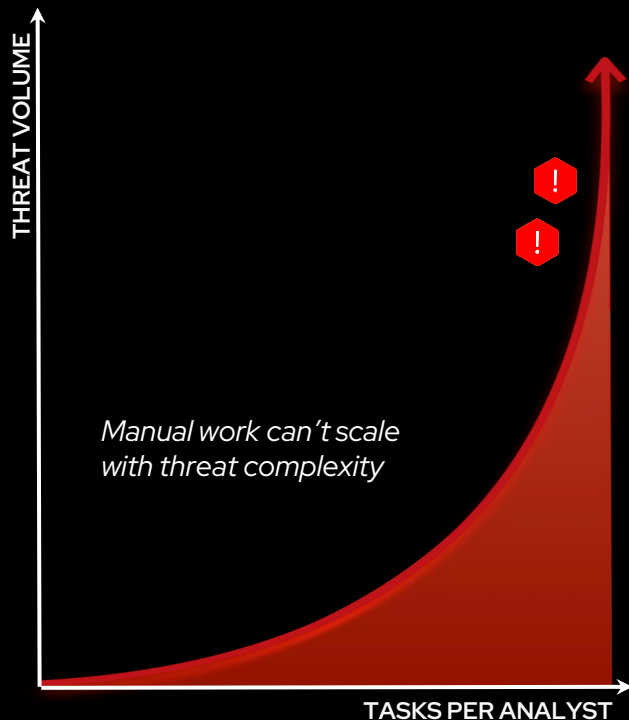
Vishing surge in late 2024

+442%



The Defender's Tipping Point: Unrelenting Labor Pains

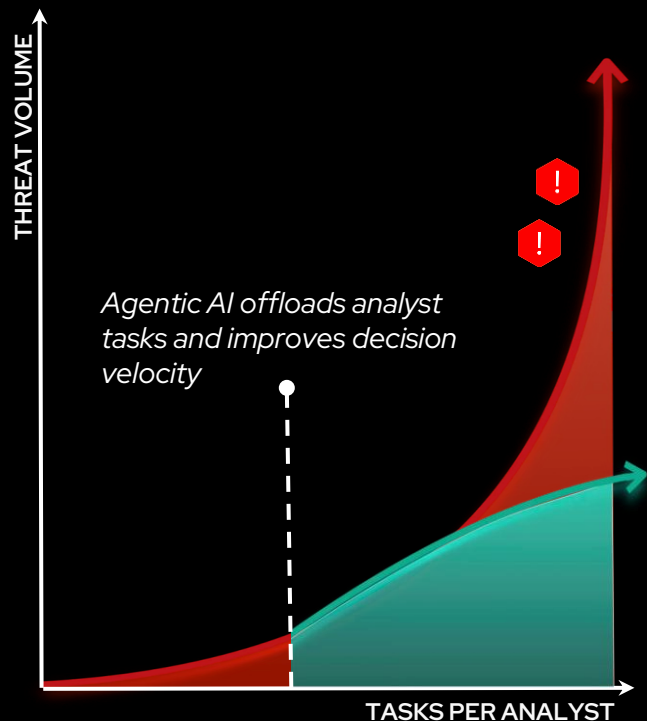
The labor curve is breaking – and so is defender capacity. A new approach is needed to regain control.



- ➔ **OVERWHELMING COMPLEXITY**
Attack surfaces are expanding faster than human teams can handle
- ➔ **ESCALATING BURNOUT**
Repetitive investigations, alert triage, and manual handoffs lead to overload and errors
- ➔ **UNRESOLVED GAPS**
Too many tools, too much noise, not enough time- vulnerabilities fester and threats slip through

A New Foundation: Agentic AI bends the labor curve

Agentic AI transforms operations – cutting complexity, scaling analyst output, and driving real-time response



- ➔ **REDUCE NOISE**
Triage alerts in real time, suppress false positives, and surface only what matters
- ➔ **OFFLOAD OPERATIONAL DRAG**
Alleviate analyst backlogs – from routine to complex tasks– and redirect cognitive load to high-impact work
- ➔ **ACCELERATE RESPONSE**
Execute at machine speed – with analyst-guided or fully autonomous agents

What defenders need- and CrowdStrike delivers

*CrowdStrike surveyed 1,000+ security
leaders on their AI priorities*



Platform-delivered AI. Not another point solution.



Domain-specific Intelligence. Not one-size-fits-all LLMs.



Analyst augmentation. Not replacement.



Built-in value. No hidden costs.



Security by design. Not bolt-on safety.

CrowdStrike

Charlotte AI

Accelerate security workflows with a
purpose-built AI security analyst



CROWDSTRIKE

Charlotte AI



ACCELERATE RESPONSE

Respond in seconds, not cycles. Use state-of-the-art AI - from agentic AI to embedded assistance - to streamline high-friction tasks and accelerate response.



BUILT ON THE INDUSTRY-LEADING PLATFORM

Purpose-built for the modern SOC, Charlotte AI is powered by the industry's richest telemetry and frontline intelligence, driving informed action to stop breaches



ELEVATE EVERYONE

Empowers users across security workflows with superior signal, expert investigation guidance and surfaced insight from Falcon modules.



OPERATE WITH PEACE OF MIND

Automate confidently and stay in control with customer-defined guardrails for autonomy, oversight, role-based access, and auditability.

Charlotte AI: The Rise of the Agentic SOC

With mission-ready agents, operate at adversary speed, with autonomy, precision, and 24/7 operational scale



EXPERT-GRADE PRECISION

>98%

Accuracy in autonomous triage



COMPOUNDING TIME SAVINGS

40+ hours

Avg. analyst hours reclaimed weekly



AUTONOMOUS ACTION

24/7

Drive outcomes around the clock

CHARLOTTE AI DETECTION TRIAGE



Autonomous, cross-domain triage

- Consistently triage with expert-level precision
- Offload manual triage and surface only what matters

CHARLOTTE AI AGENTIC RESPONSE



AI-guided investigations

- Apply the frontline expertise to every investigation
- Accelerate analyst decisions with faster, richer context

CHARLOTTE AI AGENTIC WORKFLOWS



LLM-powered SOAR

- Adapt seamlessly to edge cases and unknowns
- Tailor outputs to fit any team, audience or mission

CHARLOTTE AI

DETECTION TRIAGE

Autonomous, cross-domain triage

- ✓ Expert-level triage across endpoint & identity detections
- ✓ Superior, prioritized signal across domains
- ✓ Accelerates investigations and MTTR

The screenshot displays the CrowdStrike detection triage interface. On the left, a list of alerts is shown with columns for 'Assigned to', 'Resolution', and 'Status'. One alert is highlighted with a 'True positive' resolution and 'Closed' status. The main panel shows a detailed view of a 'Suspicious domain replication' alert, including its name, description, severity (High), start time, and recommendation (Escalate). The interface also shows a 'Triage with Charlotte AI' section with a 'Low' recommendation and 'Finished' status. A 'Status' section at the bottom indicates the alert is assigned to 'Salvador Pulido SE Demo' and is 'Closed'.

Assigned to	Resolution	Status
Unassigned	--	New
Unassigned	--	New
Unassigned	--	New
Unassigned	--	New
Unassigned	--	New
Assigned to Salvador Pu...	True positive	Closed
Unassigned	--	New
Assigned to Salvador PuL...	True positive	Closed
Unassigned	--	New
Unassigned	--	Reopened
Unassigned	--	In progress
Unassigned	--	In progress
Unassigned	--	New
Unassigned	--	New

Suspicious domain replication

Overview

Name: Suspicious domain replication
Detection ID: 5ddb0407bef249c19c7a975f17979a1f1ind:5ddb0407bef249c19c7a975f1797...

Description: katya.jabelita performed domain replication from SPC-DESKTOP-KAT.
[See related activities](#)

Severity: High
Tactic & technique: [Credential Access via DCSync](#)

Start time: Apr. 15, 2025 21:30:11
End time: Apr. 15, 2025 21:30:11

No activity from Falcon Complete message center. [Contact Falcon Complete](#)

Triage with Charlotte AI

Recommendation: Escalate
Escalation priority: 239
Verdict: False positive
Verdict confidence: Low
Triage status: Finished

Explanation: 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...

Was this triage useful? [👍](#) [👎](#) [Report](#)

[See triage details from Charlotte AI](#)

Status

Assigned to: Salvador Pulido SE Demo
Status: Closed

Tags: true_positive

Total comments: 0

From Mission-Ready Operator to Hands-on Assistant

Powered by state-of-the-art foundational models, Charlotte AI turns hours of work into seconds – from mission-critical investigations to fully autonomous operations

Automate complex tasks
WITH AGENTIC AI

The screenshot displays a security dashboard with a central panel titled "powerShell.exe on SE-0-JS-WTKVM by jsmith". To the left, a sidebar contains a list of tasks, with one task highlighted in a red box. The main panel shows a detailed view of the task, including a timeline of events and a list of related tasks. The interface is dark-themed and includes various navigation and search options.

Get fast answers to plain questions
WITH CONVERSATIONAL AI

The screenshot shows a security dashboard with a conversational AI interface. The main panel is titled "Hunt my environment for Scattered Spider" and displays a profile for the actor "SCATTERED SPIDER". The profile includes a profile picture, a status of "Active", and various attributes such as "Last active", "First activity", "IP", "Actor type", "Motivation", and "Community identifiers". Below the profile, there is a table of detections with columns for "Severity", "Detection time", "Process name", "File name", "Process ID", "User name", "Process ID", "Assigned", and "Status".

Severity	Detection time	Process name	File name	Process ID	User name	Process ID	Assigned	Status	
High	Jan. 19, 2024 18:02:16	PowerShell.exe	certutil.exe on SE-L...	Com...	certu...	SE-0...	demo	Closed	
High	Jan. 19, 2024 18:08:44	UpdateServiceHo...	Defen...	Updat...	SE-0...	demo	Closed	Closed	
Medium	Jan. 19, 2024 18:08:44	UpdateServiceHo...	Defen...	Updat...	SE-0...	demo	Closed	Closed	
High	Jan. 19, 2024 11:51:45	PowerShell.exe	certutil.exe on SE-L...	Com...	certu...	SE-0...	demo	Closed	Reopened

Streamline hands-on investigations
WITH EMBEDDED GENAI

The screenshot displays a security dashboard with a network graph visualization. The graph shows a complex network of nodes and edges, representing a cloud attack on a container. The nodes are labeled with various entities such as "SCATTERED SPIDER", "Backfire_act01", "Backfire_act02", "Backfire_act03", "Backfire_act04", "Backfire_act05", "Backfire_act06", "Backfire_act07", "Backfire_act08", "Backfire_act09", "Backfire_act10", "Backfire_act11", "Backfire_act12", "Backfire_act13", "Backfire_act14", "Backfire_act15", "Backfire_act16", "Backfire_act17", "Backfire_act18", "Backfire_act19", "Backfire_act20", "Backfire_act21", "Backfire_act22", "Backfire_act23", "Backfire_act24", "Backfire_act25", "Backfire_act26", "Backfire_act27", "Backfire_act28", "Backfire_act29", "Backfire_act30", "Backfire_act31", "Backfire_act32", "Backfire_act33", "Backfire_act34", "Backfire_act35", "Backfire_act36", "Backfire_act37", "Backfire_act38", "Backfire_act39", "Backfire_act40", "Backfire_act41", "Backfire_act42", "Backfire_act43", "Backfire_act44", "Backfire_act45", "Backfire_act46", "Backfire_act47", "Backfire_act48", "Backfire_act49", "Backfire_act50", "Backfire_act51", "Backfire_act52", "Backfire_act53", "Backfire_act54", "Backfire_act55", "Backfire_act56", "Backfire_act57", "Backfire_act58", "Backfire_act59", "Backfire_act60", "Backfire_act61", "Backfire_act62", "Backfire_act63", "Backfire_act64", "Backfire_act65", "Backfire_act66", "Backfire_act67", "Backfire_act68", "Backfire_act69", "Backfire_act70", "Backfire_act71", "Backfire_act72", "Backfire_act73", "Backfire_act74", "Backfire_act75", "Backfire_act76", "Backfire_act77", "Backfire_act78", "Backfire_act79", "Backfire_act80", "Backfire_act81", "Backfire_act82", "Backfire_act83", "Backfire_act84", "Backfire_act85", "Backfire_act86", "Backfire_act87", "Backfire_act88", "Backfire_act89", "Backfire_act90", "Backfire_act91", "Backfire_act92", "Backfire_act93", "Backfire_act94", "Backfire_act95", "Backfire_act96", "Backfire_act97", "Backfire_act98", "Backfire_act99", "Backfire_act100". The graph is dark-themed and includes various navigation and search options.

VECTRA®

HOW TO
PROTECT
MODERN
NETWORKS



INTRODUCTION TO VECTRA AI / TEAM ALPINE

Customer First, Partner Centric

- + Founded 2011, Privately held
- + Headquartered in San Jose, CA
- + 580+ employees
- + 113 countries
- + 3 Global SOCs
- + >1800 customers

AI Driven

- + Research + Data Science + Engineering
- + 150+ AI-driven attacker behavior models
- + 35 patents in AI-driven threat detection
- + Most referenced vendor in MITRE D3FEND (11)
- + Cover >90% of MITRE ATT&CK techniques



Kim Rehage
Team Alpine



Michael Buchner
Team Alpine



Jo Wegener
Team Alpine



David Solar
Team Alpine



Aurélien Hess
Team Alpine



GARTNER MAGIC QUADRANT FOR NDR 2025

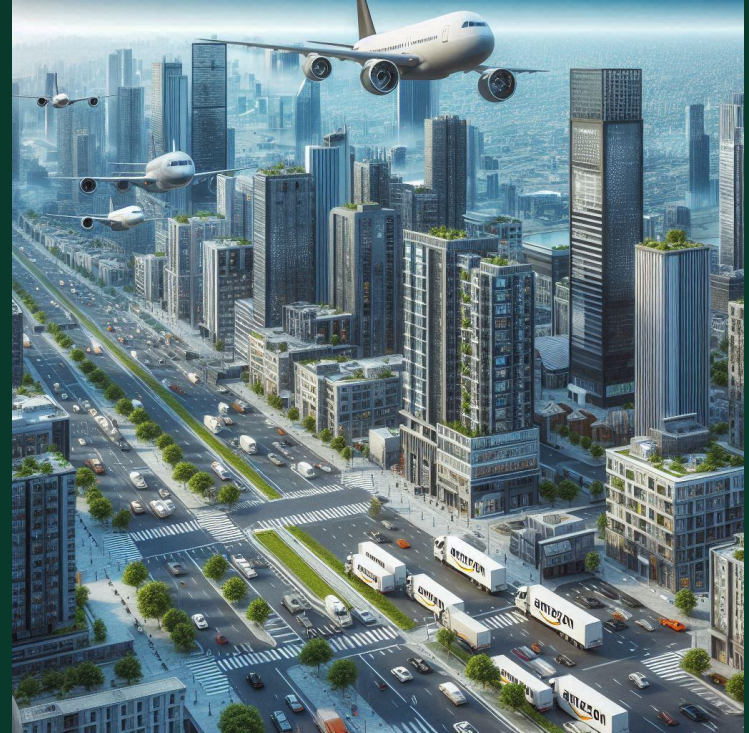
„Network detection and response platforms continuously monitor traffic for anomalies, suspicious patterns and threat indicators, and they complement other threat detection solutions“

„Organizations rely on NDR to detect and contain postbreach activity such as ransomware, insider threats and lateral movements. NDR complements other technologies that primarily trigger alerts based on rules and signatures by building heuristic models of normal network behavior and detecting anomalies“

„NDR is commonly used as a complementary detection and response technology as part of a broader arsenal of security operation center (SOC) tools. These include security orchestration, automation and response (SOAR), security information and event management (SIEM), endpoint detection and response (EDR), and other detection technologies, but also services such as managed detection and response (MDR).“



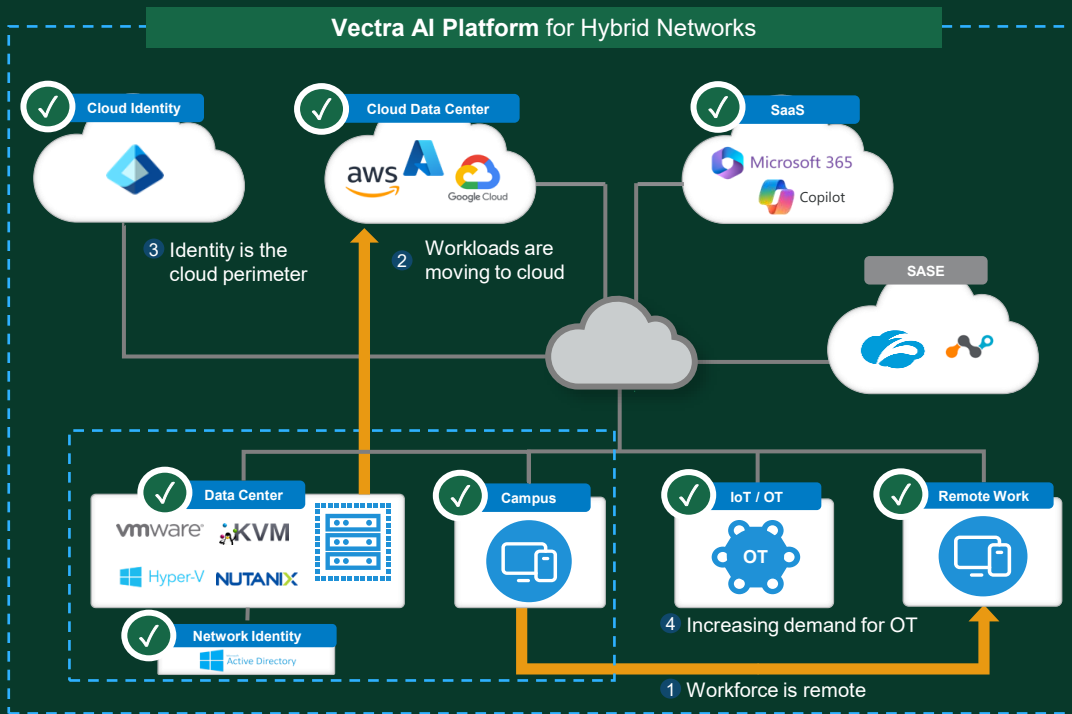
EVOLUTION TOWARDS MODERN NETWORKS



EVOLUTION TOWARDS MODERN ATTACKS



VECTRA AI COVERAGE FOR MODERN NETWORKS

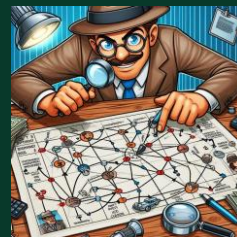


- > Agentless
- > Native coverage
- > Real-time detections
- > Enterprise scale
- > Intuitive SaaS UX
- > Modular design
- > Ecosystem-friendly
- > 24x7x365 MDR

WHAT VECTRA BRINGS TO THE TABLE



Unified visibility



Correlation of
detected attacker
behaviour



Accelerated
threat detection
and response