

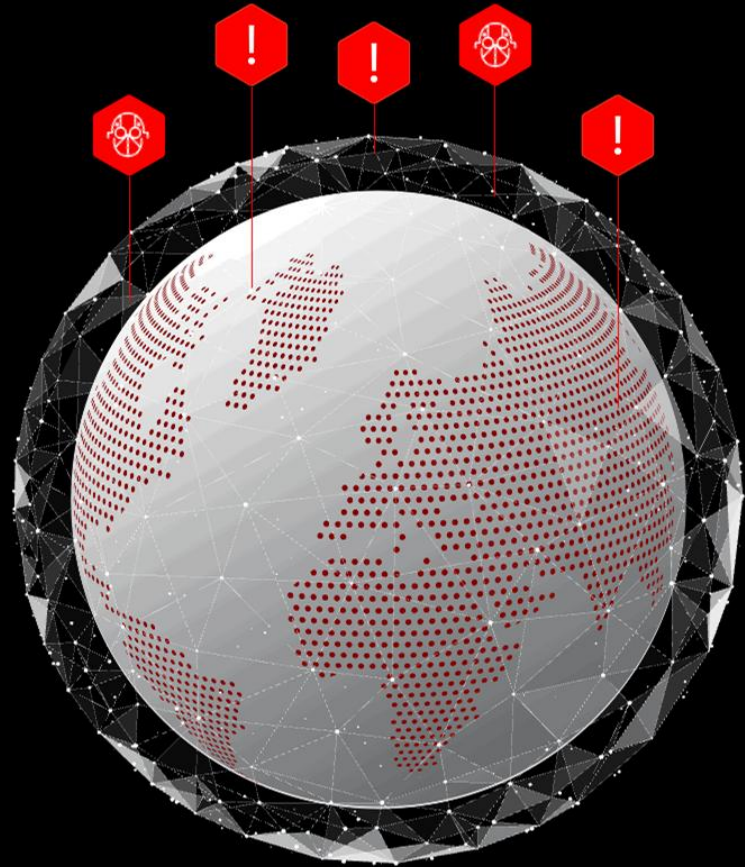
# Smart Defense: How AI Shaping the Future of Cybersecurity

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%**

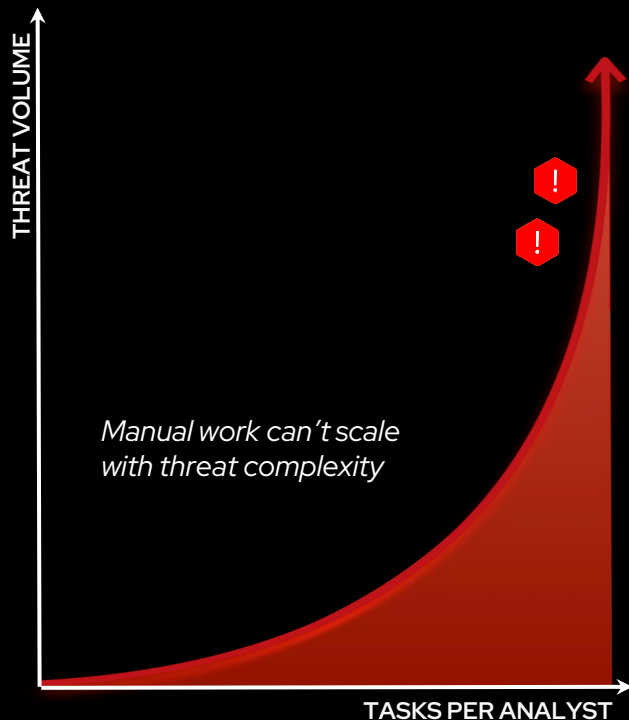
Vishing surge in late 2024

**+442%**



# The Defender's Tipping Point: Unrelenting Labor Pains

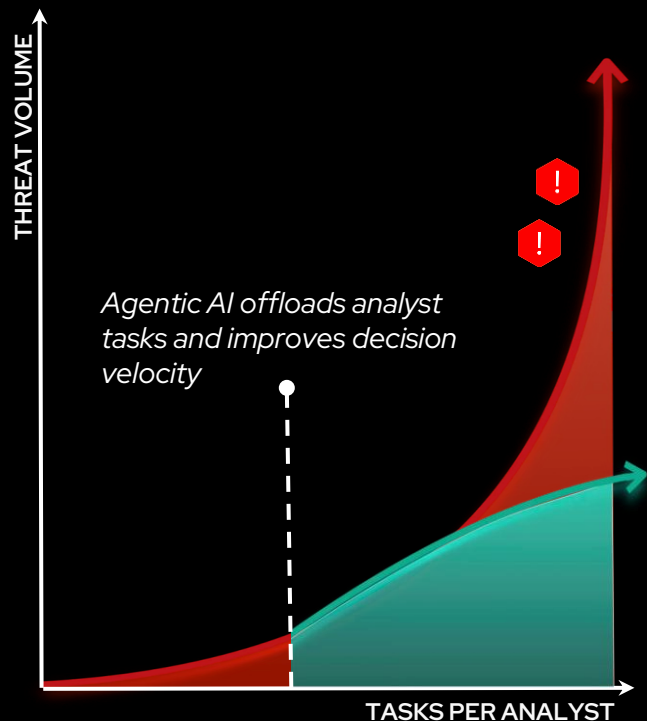
The labor curve is breaking – and so is defender capacity. A new approach is needed to regain control.



- ➔ **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**

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. The alert details include:

- 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

The interface also shows a recommendation to 'Escalate' with a 'Low' verdict confidence and a 'Finished' triage status. An 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...'. A 'Report' button is visible at the bottom right of the explanation section.

# 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. A large, detailed text box is overlaid on the main panel, containing a complex task description and instructions. The background shows various system logs and event feeds.

Get fast answers to plain questions  
**WITH CONVERSATIONAL AI**

The screenshot shows a security dashboard with a search bar at the top containing "Hunt my environment for Scattered Spider". Below the search bar, there is a profile card for the actor "SCATTERED SPIDER" with details such as "Last active: Jan 2024", "Status: Active", "Origin: Unknown", "Hosts: 25", "Target Industries: IT", and "Target Countries: US". Below the profile card, there is a table of detections with columns for Severity, Detect time, Process name, Tags, and Status.

Severity	Detect time	Process name	Tags	Status
High	Jan. 19, 2024 18:02:16	certutil.exe on SE-L...	Tools Co.   Process: certutil...   Status: SE-0...   User name: demo   View...	Assigned   Closed
High	Jan. 19, 2024 18:08:44	UpdateServiceHo...	Defens.   Update...   Status: SE-0...   User name: demo   View...	Assigned   Closed
Medium	Jan. 19, 2024 18:08:44	UpdateServiceHo...	Defens.   Update...   Status: SE-0...   User name: demo   View...	Assigned   Closed
High	Jan. 19, 2024 11:51:45	certutil.exe on SE-L...	Tools Co.   Process: certutil...   Status: SE-0...   User name: demo   View...	Assigned   Reopened

Streamline hands-on investigations  
**WITH EMBEDDED GENAI**

The screenshot displays a network graph visualization on a security dashboard. The graph shows various nodes representing entities like "Backfire\_act01", "cloud", "chrysal", "is", "bank", "maine-mule-ubuntu", "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". The nodes are connected by lines, forming a complex network structure.

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

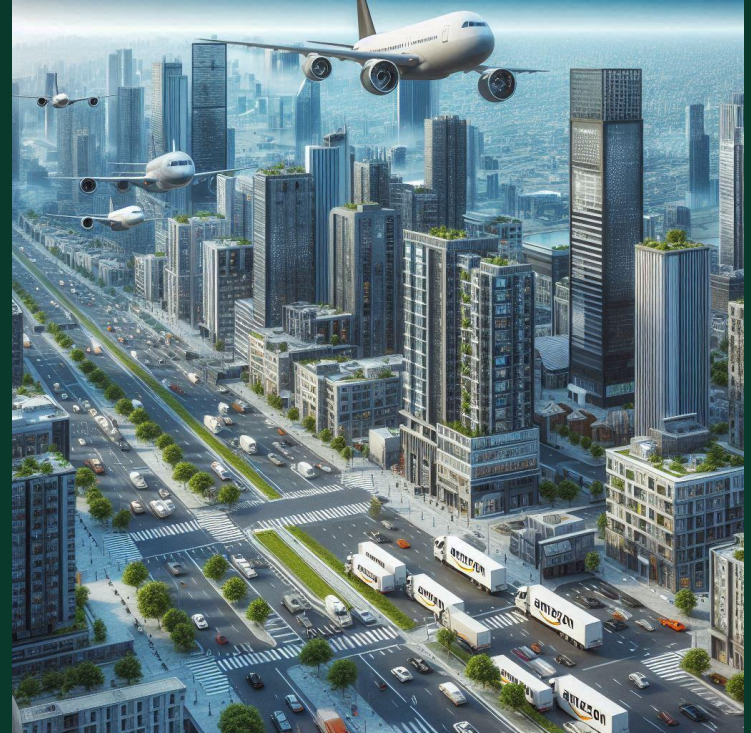
„Network detection and response platforms continuously monitor traffic for anomalies, suspicious patterns and threat indicators, and they complement other threat detection solutions“

„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).“



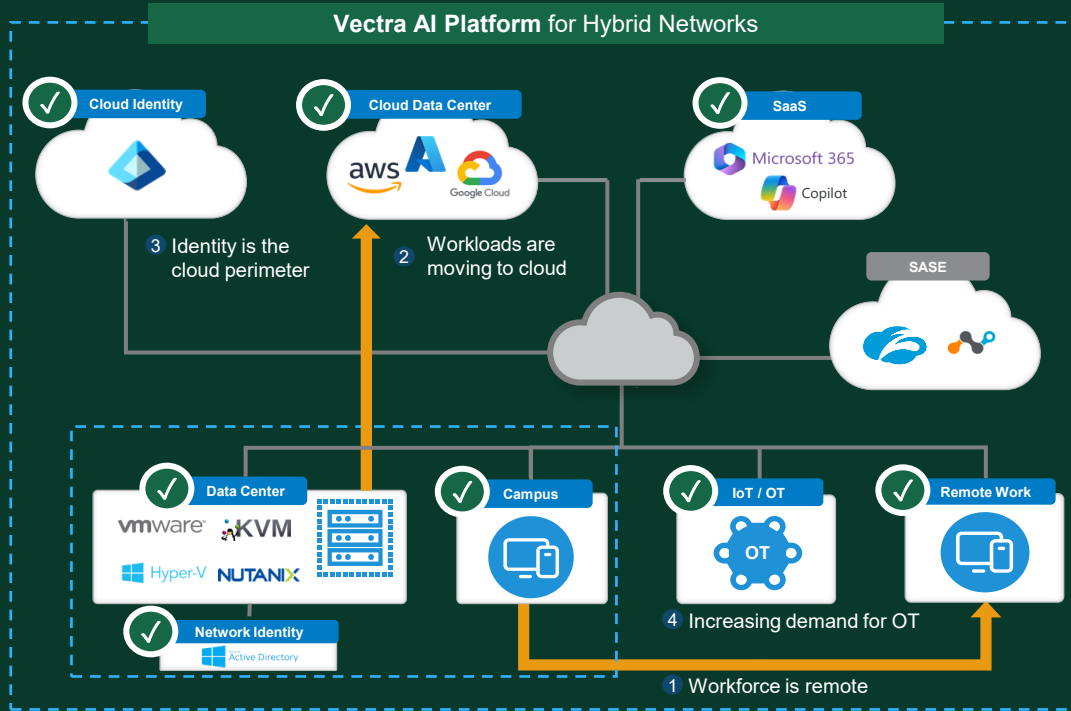
# EVOLUTION TOWARDS MODERN NETWORKS



# EVOLUTION TOWARDS MODERN ATTACKS



# VECTRA AI COVERAGE FOR MODERN NETWORKS

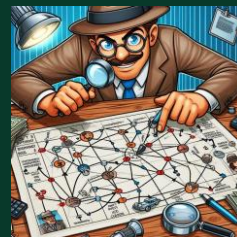


- > Agentless
- > Native coverage
- > Real-time detections
- > Enterprise scale
- > Intuitive SaaS UX
- > Modular design
- > Ecosystem-friendly
- > 24x7x365 MDR

# WHAT VECTRA BRINGS TO THE TABLE



Unified visibility



Correlation of  
detected attacker  
behaviour



Accelerated  
threat detection  
and response



**Vielen Dank**

**Breakout Session:  
14:10 – Reign of AI**