

Threat Hunting Reloaded: Sichtbarkeit + Kontext = Proaktive Verteidigung

CrowdStrike Charlotte AI +
Vectra.AI Attack Signal Intelligence



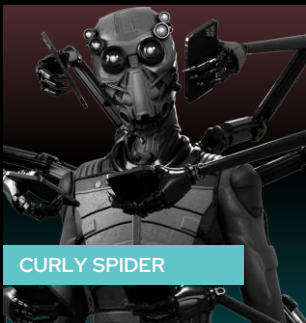
We stop breaches.

Protection that powers you



AI-enabled adversaries are accelerating...

Traditional Defenses
Are Obsolete



CURLY SPIDER

35% increase in “interactive intrusion” techniques

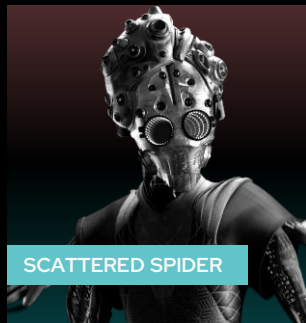
AI Has Weaponized
Deception at Scale



FAMOUS CHOLLIMA

220% increase in AI accelerated human manipulation

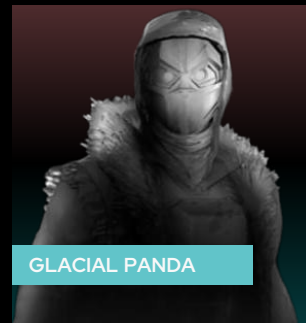
Speed Has Become
the Ultimate Offense



SCATTERED SPIDER

Less than 24 hours: account takeover to ransomware

Fragmentation Gives
Adversaries the Advantage



GLACIAL PANDA

Cross-domain attack 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
DEEP,
UNIFIED CONTEXT**

**TAKE
AUTHORIZED
ACTION**

Security must evolve

Modern attacks demand agentic defense

**ADAPT
ON THE FLY**

**EXPLAIN
AND DOCUMENT
REASONING**

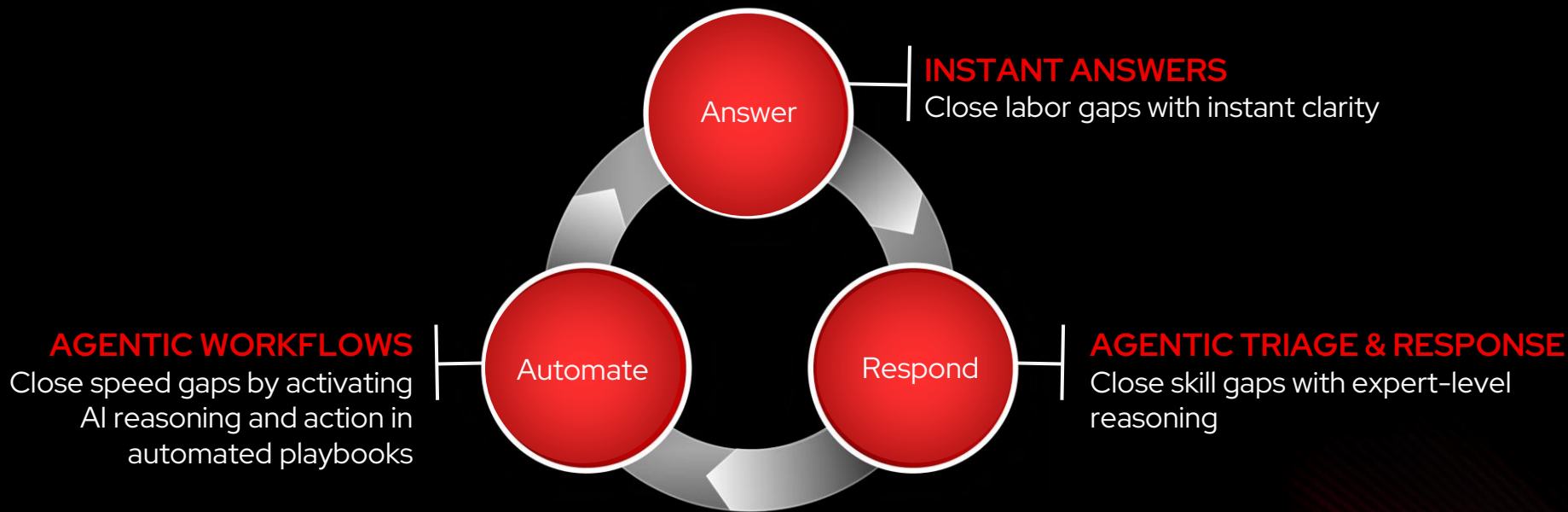
Charlotte AI

The brain of the agentic SOC

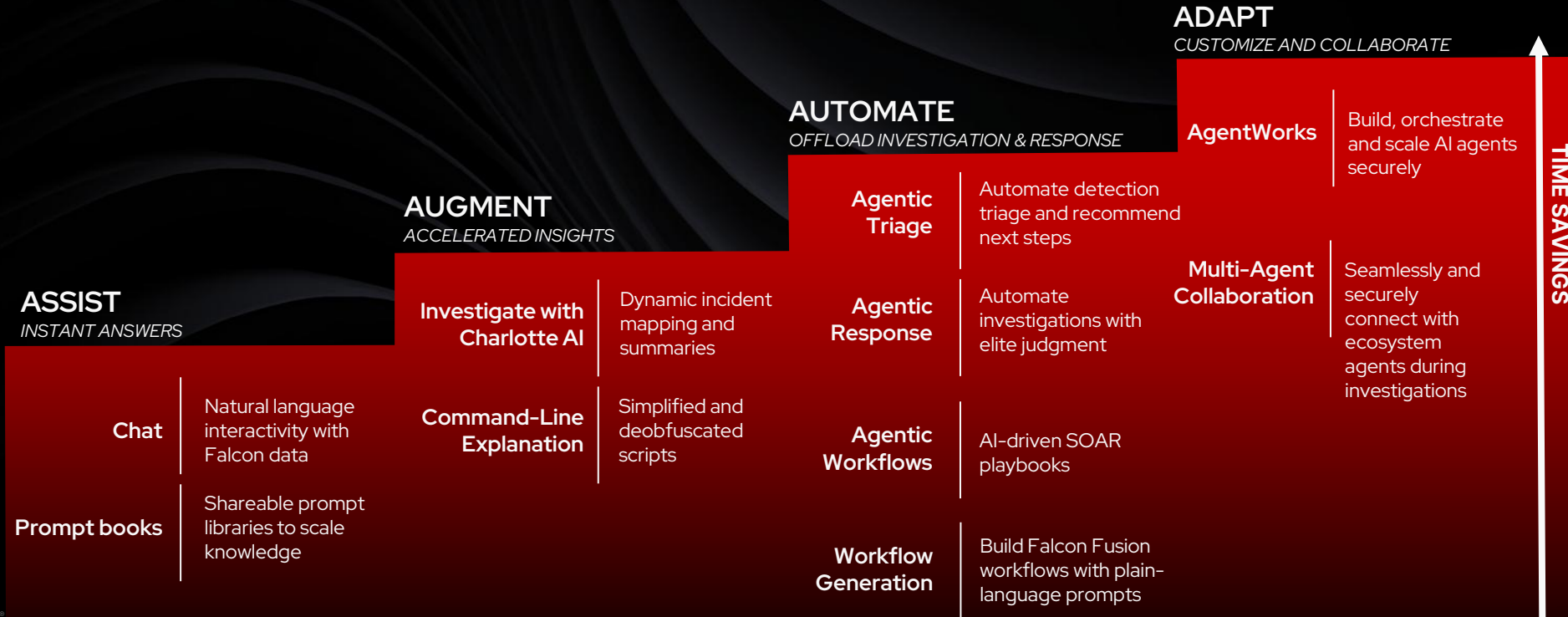


Charlotte AI helps teams close the gaps.

Automate repetitive tasks, accelerate outcomes and free analysts to focus on high-impact work



Accelerate Outcomes and automate high-value work with Charlotte AI



Charlotte AI Agentic Detection Triage

Automatically analyze new detections, obtaining:

- 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

The screenshot displays a security dashboard interface. On the left, a list of detections is shown with columns for 'Assigned to', 'Resolution', and 'Status'. One detection is assigned to 'Salvador Pulido' with a resolution of 'True positive' and a status of 'Closed'. The main panel shows a detailed view of a detection titled 'Suspicious domain replication' on 'Apr. 15, 2025 21:37:11'. The detection is categorized as 'High' severity and occurred on 'Apr. 15, 2025 21:30:11'. The triage section, highlighted with a yellow border, provides the following information:

- 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...
- Action:** Was this triage useful? (thumbs up/down icons)
- Link:** See triage details from Charlotte AI

At the bottom, the 'Status' section shows the detection is assigned to 'Salvador Pulido SE Demo' and is currently 'Closed'. A tag 'true_positive' is visible in a red box.

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 detections. Individual results may vary based on factors such as total alert volume.

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 screenshot displays the 'Agentic response' workflow for a detection on `ip-192-168-43-92.ec2.internal` by `root`. The interface includes a search bar, navigation tabs (Details, Agentic response, Process table, Process tree, Process graph, Events timeline), and a central workspace with a flowchart of investigation steps and questions. A 'Response information' panel on the right shows the generated question and answer.

Investigation Steps:

- Control check if the remote IP address 172.17.0.21 appears on the approved remote access whitelist due to an error?
- Control check for the presence of the string located at "RunCommand", "Content", "id", "Remote", "Access" observed and if the subsequent software emergency on host "ip-192-168-43-92.ec2.internal" due to a...
- Control check the recorded base64 payload for commands compared with known malicious remote shell commands over the interval from 2025-07-10 03:48:04 UTC to 2025-07-10 04:04:04 UTC

Generated Questions:

- Does the cloud audit log indicate any changes in network rule configurations around the time of the payload execution event?
- Do system logs indicate any temporary security monitoring features error?
- Do system event logs record any Firewall process start or stopping?
- Do system audit logs show any use of administrative credentials during the payload execution period?
- Do DNS logs reveal any queries for external domains concurrent with the detection timeline?
- Does the host security log show any unusual processes starting from ip-192-168-43-92 after the remote shell event?
- Do login records indicate any anomalous remote login attempts or log on from ip-192-168-43-92 after the reverse shell event?
- Do audit logs record the creation or modification of any network rules or rule sets on host ip-192-168-43-92 after the reverse shell activity?
- Do host activity log record a denied/rejected host connecting area shell execution?
- Do the unblocklisted script file (RunCommand, Content, id, Remote, Access) have been unblocklisted after a modification from the approved update category?
- Do host audit logs indicate any unanticipated configuration changes during the payload execution period?

Response Information:

Question: Do firewall or security appliance logs indicate any changes in network rule configurations around the time of the payload execution?

Answer: No changes in network rule configurations were found within the 15-minute interval from 2025-07-10 03:48:04 UTC to 2025-07-10 04:04:04 UTC around the payload execution event detected at 2025-07-10 03:56:04 UTC.

Question rationale: This question examines if there were adjustments in network defense mechanisms that might suggest an attempt to bypass security controls, aligning with potential malicious behavior.

Was this response useful? [Feedback icons]

Chain of work:

- Writing COL query
- Running LogScale query

The query filters for events of type `FirewallSetRule`, which indicate changes in firewall or network rule configurations. These events are relevant to identifying any modifications to network rules during the specified 15-minute interval. The `table` function is used to display the relevant fields, including the timestamp of the event (`@timestamp`), the computer name (`ComputerName`), the username associated with the change (`UserName`), the firewall rule details (`FirewallRule`), and the context timestamp (`ContextTimestamp`).

The time filter ensures that only events occurring between 2025-07-10T03:48:04.768Z and 2025-07-10T04:04:04.768Z are retrieved, which aligns with the detection time.

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 of manual effort by a human analyst. 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)

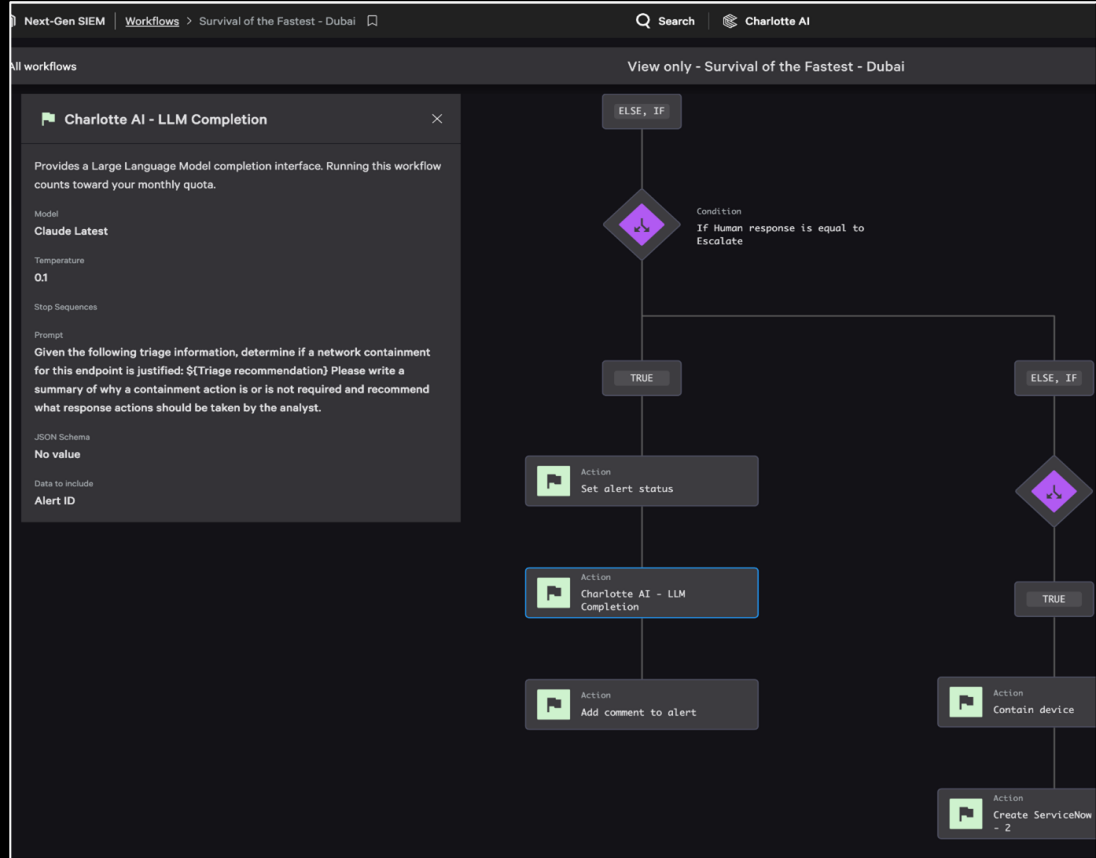
Charlotte AI Agentic Workflows

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



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

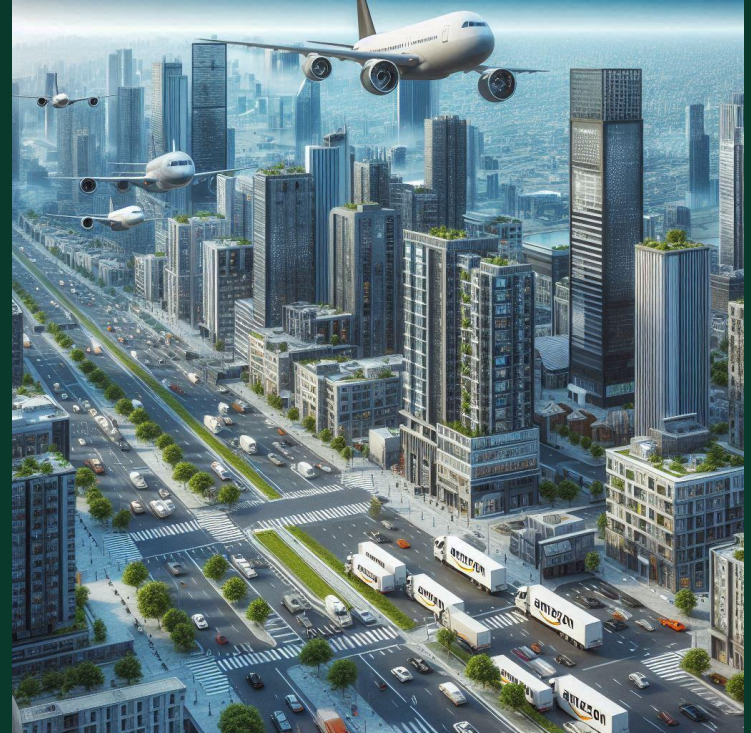
„Network detection and response platforms continuously monitor traffic for anomalies, suspicious patterns and threat indicators, and they complement other threat detection solutions“

„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).“



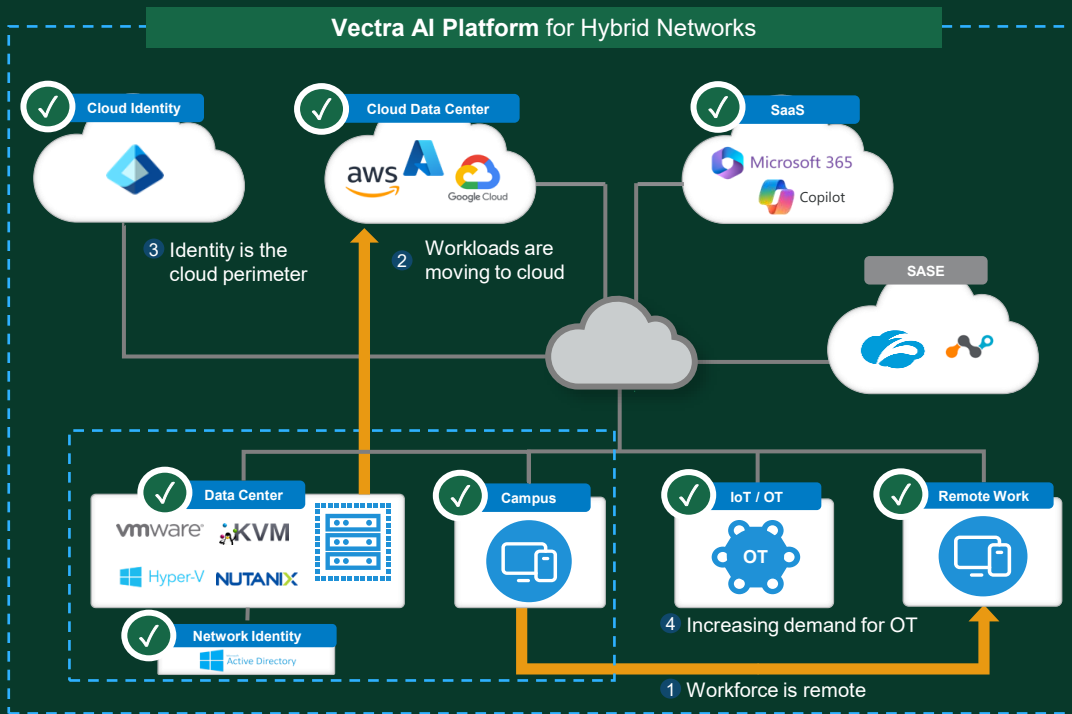
EVOLUTION TOWARDS MODERN NETWORKS



EVOLUTION TOWARDS MODERN ATTACKS



VECTRA AI COVERAGE FOR MODERN NETWORKS

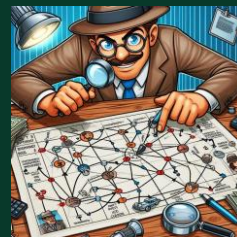


- > Agentless
- > Native coverage
- > Real-time detections
- > Enterprise scale
- > Intuitive SaaS UX
- > Modular design
- > Ecosystem-friendly
- > 24x7x365 MDR

WHAT VECTRA BRINGS TO THE TABLE



Unified visibility



Correlation of
detected attacker
behaviour



Accelerated
threat detection
and response



Vielen Dank