Arm your SOC with Vectra AI Instant Investigations

Perform investigations regardless of skill-level with the Vectra AI Platform

Vectra AI-driven Attack Signal Intelligence™ provides the lighted pathways to serve as a quick start guide for modern SOC teams to investigate the most critical and urgent threats with little to no effort through automated controls. SOC teams will have access to the powerful signal of the Vectra AI Platform to streamline threat hunting and investigation on any incident across the data center network and hybrid cloud.

Instant Investigation is a necessity for modern SOC teams. With the Vectra AI Platform, security teams can get a jump start during investigations and turn the tables on attackers before an incident becomes a breach, regardless of where an attack originates and moves within the hybrid cloud.

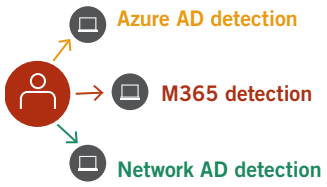
Key Benefits

- **Contextualized threat activity:** Use Instant Investigation to access all activity from hosts and accounts in real-time regardless of domain.
- **Improved SOC efficiency:** Improve overall workflow with integrated hybrid attack investigation and response for faster and more accurate threat hunting and investigation with speed.
- **Keep pace with evolving attacks:** Erase concerns around skills shortage and overworked SOC analysts by leveraging Instant Investigations through AI-driven detection models that reduce detection latency time.

Vectra AI Platform Investigation Stack

AI-Driven Prioritization

Focus on urgent



Ranks events by business impact and unifies visibility

Instant Investigation

Zero-query investigation

SaaS Application History	
SalesForce	UserLogin
Zscaler	UserLogin
AWS	Failure
Azure	UserLogin

Azure AD History
Change Federated Trust
Disable MFA
Modify Service Principle
Install OAuth Application

Microsoft 365 History
DownloadFile
Create InboxRule
eDiscoverySearch
Start PowerAutomate

Answers to the top questions to stop a threat

Advanced Investigation

Seamless pivot to full logs and fast response

M365 Logs		
User	**Operation**	**Details**
jane@biz.ai	Create InboxRule	Hide all emails
jane@biz.ai	Create InboxRule	Move to RSS
tom@biz.ai	Create InboxRule	Forward to @protomail
rob@biz.ai	Create InboxRule	Spam

Complete view of M365 and Azure AD data

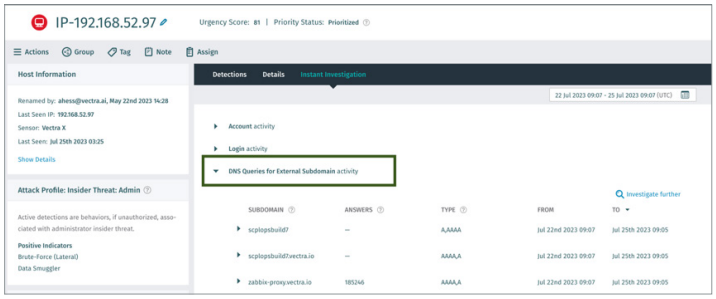
Easily investigation impact and hunt

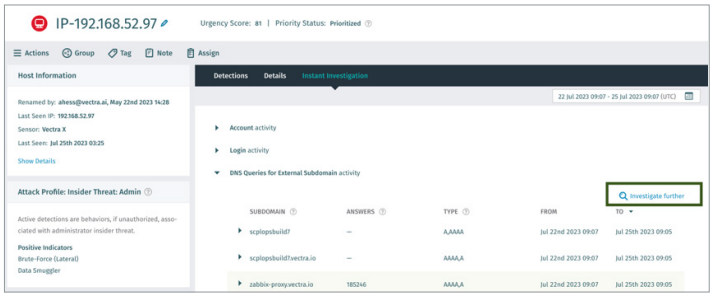
With an average of about 6 days for SOC teams to resolve a security alert — detection, investigation and response latency can mean catastrophe for an organization.

Only the Vectra AI Platform can provide the intelligent controls that enable Instant Investigation — so your SOC can move at the speed and scale of hybrid attackers. Instant Investigation eliminates the guesswork for SOC analysts with contextualized threat activity for faster, more accurate threat hunting, investigation and response.

1: 2023 Verizon Data Breach Investigation Report (DBIR)

How it works

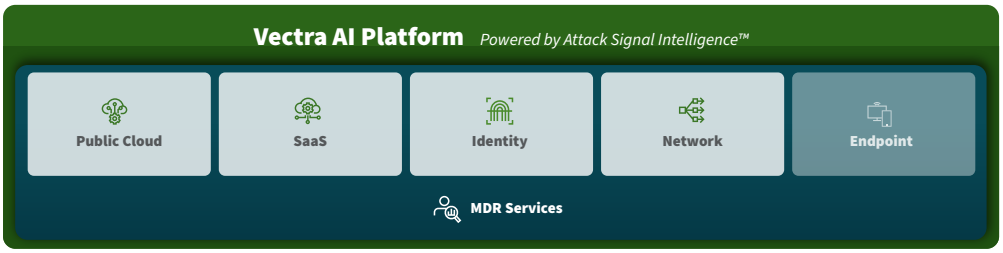




- **Automatic incident priorities:** Get AI-driven detection activity within a single pane of glass.
- **Zero query searches:** No need to craft searches for threat investigations and hunting.
- **Guided next steps:** Within the platform, quickly move from Instant Investigation to Advanced Investigation for the most critical and urgent threats.

Technical Requirements

- **Coverage:** Utilize a TDIR solution (such as the Vectra AI Platform), that unifies and consolidates attack telemetry across the entire hybrid cloud attack surface including identity, public cloud, SaaS and data center networks. In simplest terms, perform instant investigations on any threat across your hybrid cloud environment.
- **Clarity:** Integrated, real-time AI-driven attack signal to automate threat detection, triage and prioritization across your hybrid cloud domains. Shift from event-centric threat detection to entity-centric attack signal for higher-fidelity alerts on hosts and accounts under attack, removing the need to triage hundreds if not thousands of threat events per day. With a TDIR solution, SOC teams can differentiate between benign and malicious true positives, saving valuable time and resources.
- **Control:** Arm SOC analysts by removing as much deployment complexity upfront to prevent further investigation and response latency in analyst workflows, while placing full context and control at their fingertips. In addition, leverage co-managed services to add more reinforcements to SOC teams when talent resources are scarce or have limited access to the expertise needed for threat hunting.



The Vectra AI Platform enables SOC teams to instantly investigate threats across the hybrid cloud to combat attackers in real-time. The Vectra AI Platform truly streamlines threat hunting and investigations with Vectra AI-driven Attack Signal Intelligence. Security teams are provided with the necessary and actionable intelligence to safeguard their data center network, identity, public cloud and SaaS with zero queries in an instant — reducing the mean time to respond, so they can stop attackers in their tracks.

About Vectra AI

Vectra AI is the leader and pioneer in AI-driven Attack Signal Intelligence. Only Vectra AI natively delivers hybrid attack telemetry across public cloud, SaaS, identity, and networks in a single platform. The Vectra AI Platform with Attack Signal Intelligence empowers security teams to rapidly prioritize, investigate and respond to the most advanced and urgent cyber-attacks to their hybrid environment. Vectra AI has 35 patents in AI-driven threat detection and is the most referenced vendor by MITRE D3FEND. Organizations worldwide rely on the Vectra AI Platform and MDR services to move at the speed and scale of hybrid attackers. For more information, visit www.vectra.ai.

For more information please contact us:
Email: info@vectra.ai | vectra.ai