Mitigate the Risk from Privilege Identity Attacks with the Vectra AI Platform

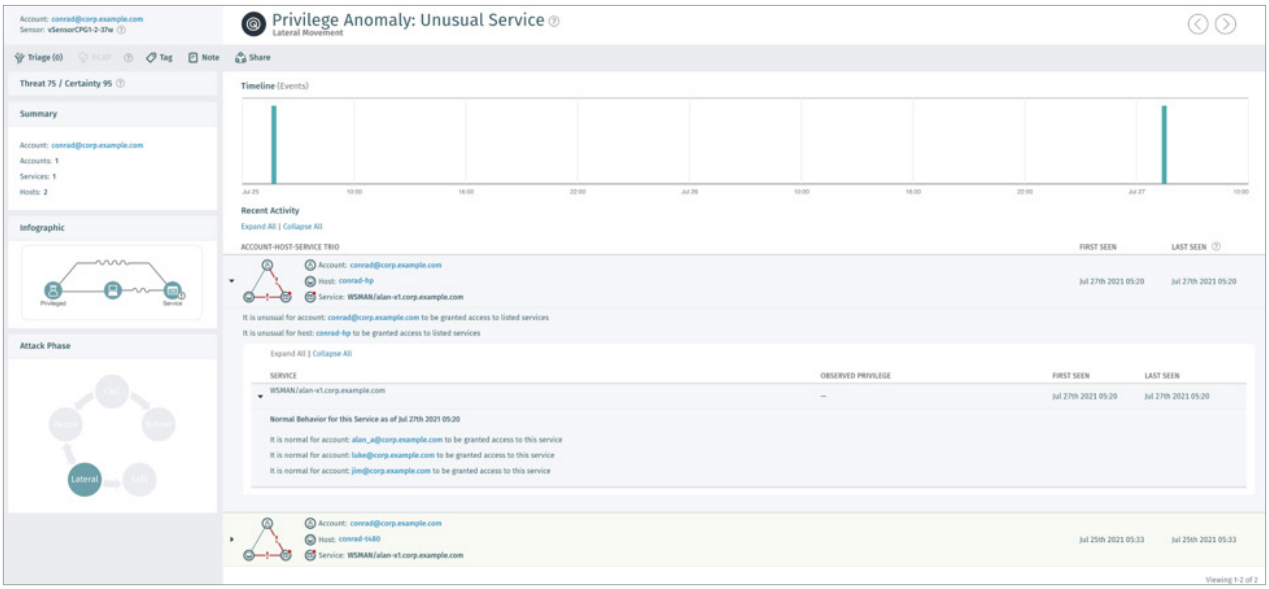
Vectra AI spots privilege abuse with unmatched signal clarity for your XDR.

Vectra AI Attack Signal Intelligence™ exposes the complete narrative of any attacker trying to abuse privilege. SOC teams use the Vectra AI Platform to investigate and respond to any type of misuse or unauthorized access across today's hybrid attack surfaces — public cloud, SaaS, identity, and data center networks. Vectra AI ensures that your team never misses an escalation action or unsanctioned access, so attackers never reach their target.

Privilege misuse is a top cybersecurity threat today that often results in expensive losses and can even cripple businesses. It's also one of the most popular attack vectors among threat actors, and when successfully carried out, provides free access to an enterprise's underbelly, often without raising any alarms until damage is already done. With the Vectra AI Platform, organizations can achieve enterprise-scale privilege visibility in real-time.

Key Benefits

- Real-time AI-driven detection for any privileged service access by attackers.
- Unique visibility into all privilege identity behaviors across the hybrid cloud, highlighting any instance of attacker abuse.
- Zero-Trust hybrid cloud visibility including data center network, Azure AD and public cloud that focuses on behavior, not static configurations.
- Full hybrid cloud coverage that does not require any additional hardware or manual adjustments.



With over 80% of attacks involving stolen identities[1], Vectra's Privilege Access Analytics provides the critical alerting to see attackers before they achieve their objectives.

Only the Vectra AI Platform can provide your SOC team with an accurate understanding of privilege access incidents with the full context of attacker behaviors across your public cloud, SaaS, identity and data center network. Thus, reducing detection latency and the mean time to respond (MTTR) without the need to dive down a deep rabbit hole during investigation. SOC analysts know exactly who and what abused an identity along with a timestamp, so they can stop attackers in their tracks.

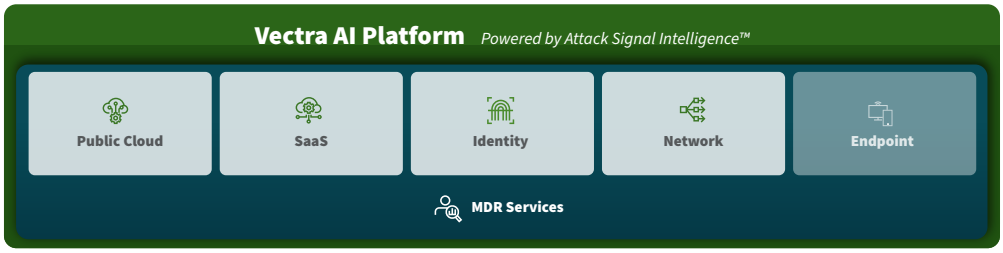
1: 2023 Verizon Data Breach Investigation Report (DBIR)

How it works

- Privilege-aware AI detections find attackers the moment they abuse privilege within your hybrid cloud.
- Comprehensive visibility and threat coverage for every identity, service and machine within an easy-to-use interface.
- Automatically see the privilege of every user in your environment without complex queries or additional tools.

Technical Requirements

- **Coverage:** Rapid technology advancements and high user expectations mean that new systems and applications are constantly being added to IT ecosystems, while new privileged accounts are being constantly created to manage them. Organizations need a Threat Detection Investigation and Response (TDIR) solution, such as the Vectra AI Platform to provide consolidated and unified attack telemetry coverage for all privileged accounts across the hybrid cloud.
- **Clarity:** AI-driven signal clarity for the highest threat signal clarity with entity-centric TDIR is required to move at the speed of privileged access attackers. Without these necessary insights, it is nearly impossible to not only identify, but prioritize which compromised accounts to spend efforts on to combat the threat. The Vectra AI Platform harnesses Vectra AI-driven Attack Signal Intelligence to provide the best-in-class AI-driven security in real-time, empowering organizations to be more resilient to exploits so they can achieve their business objectives.
- **Control:** Cybersecurity solutions should enable an easier workflow for SOC teams. Modern TDIR solutions for hybrid cloud require intelligent control with AI-enabled operations to detect the most urgent and critical threats for teams to act and respond accordingly. The Vectra AI Platform is the only solution that empowers SOC teams to be able to take the best course of action through AI-enabled investigation, hunting and response.



The Vectra AI Platform enables SOC teams to see and stop attackers abusing privilege across the hybrid cloud. The Vectra AI Platform Privilege Access Analytics identifies attacks that are too often overlooked by legacy tools. By thinking like an attacker and developing long-live environment baselines, Vectra AI Attack Signal Intelligence detects subtle signs of privilege abuse without flagging every new connection. These alerts provide teams with actionable intelligence to safeguard their network and cloud identities — keeping their organizations secure.

Learn more about the Vectra AI Platform

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

© 2023 Vectra AI, Inc. All rights reserved. Vectra, the Vectra AI logo, and Security that thinks are registered trademarks and the Vectra Threat Labs , Threat Certainty Index and Attack Signal Intelligence are trademarks of Vectra AI. Other brand, product and service names are trademarks, registered trademarks or service marks of their respective holders. Version: **091223**