AI-Enabled Threat Discovery and the Post-Compromise Detection Gap

Why security teams need behavioral detection when Anthropic Mythos and similar tools compress attacker timelines

Executive Summary

- Anthropic Mythos and similar tools compress the time between initial access and operational impact from days or weeks to hours.
- Prevention remains important, but perimeter and signature-based controls are not designed to reliably detect what an attacker does after authenticated access is established.
- Vectra AI closes that gap by detecting behavioral evidence of compromise across network and identity activity after authentication.

What Anthropic Mythos and similar tools change

- Accelerates discovery of vulnerable paths, trust relationships, and privileged identities.
- Reduces defender dwell time for correlation and manual investigation.
- Makes post-compromise visibility the decisive factor in stopping mission impact.

Where the current stack stops

- Proxy, IPS, and endpoint tools are strongest at known-bad content, exploits, and artifacts.
- They are weaker at recognizing whether a valid account, host, or service is behaving like an attacker.
- That gap matters most after authenticated access is obtained inside trusted environments.

What Vectra AI adds for security teams

Behavioral detection

- Reconnaissance
- Lateral movement
- Credential abuse
- Privilege escalation

Network + identity context

- Legitimate protocols
- Service account misuse
- Privileged anomalies
- Attack prioritization

Fast, additive deployment

- Deploy alongside current tools
- Scale from focused scope
- Lower analyst noise
- Flexible expansion path

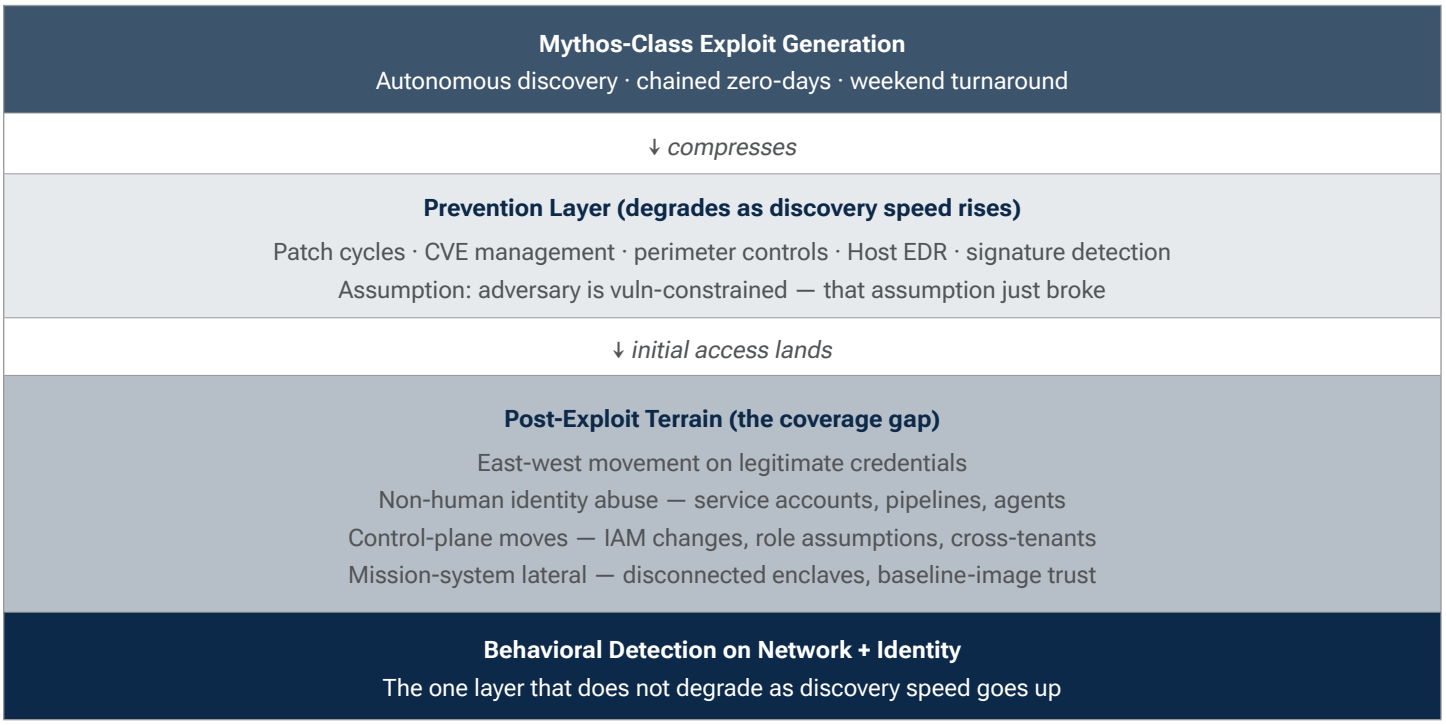

Figure 1 — Mythos-class exploit generation compresses the prevention layer and exposes the post-exploit terrain that signature stacks cannot see.

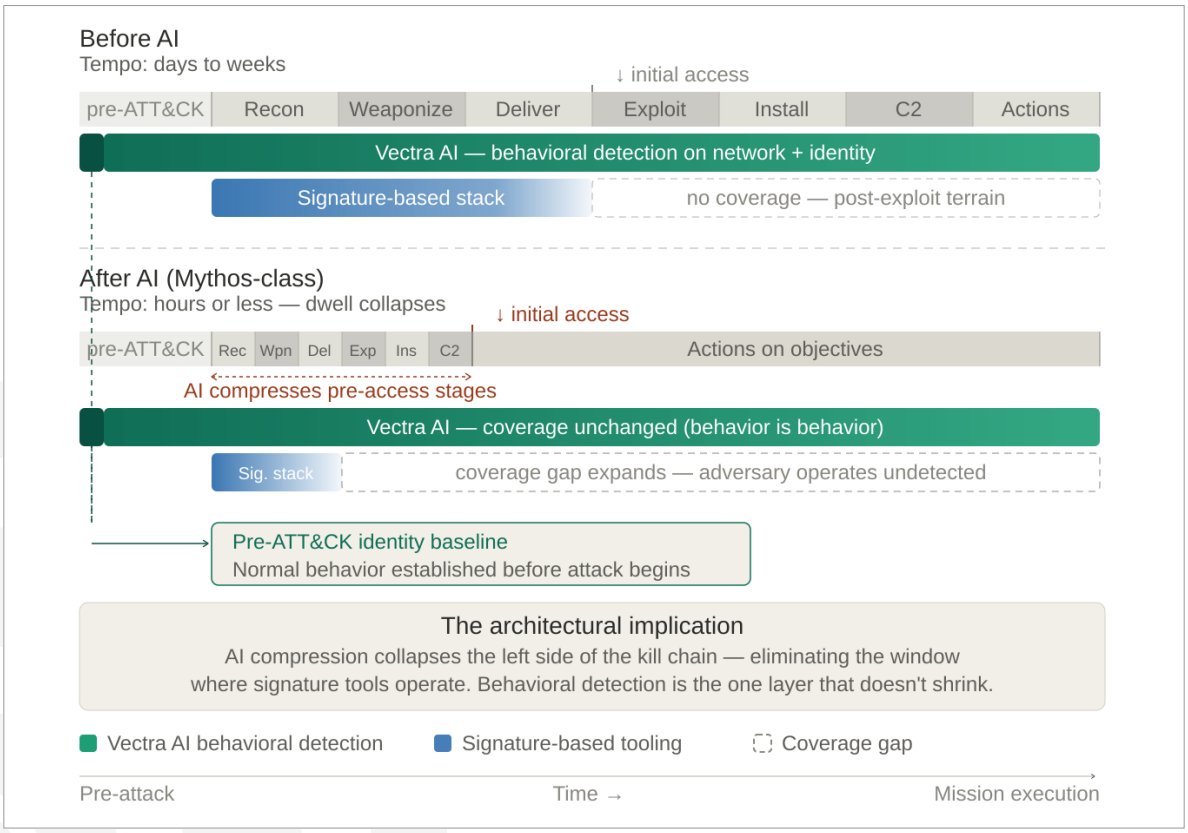

Figure 2 — Detection coverage mapped against the MITRE ATT&CK kill chain. AI acceleration compresses pre-access stages, collapsing the window where signature-based tools operate. Vectra AI behavioral detection is the one layer whose coverage does not shrink.

Customer proof points

Global Beauty Retailer

Global beauty retailer eliminated critical blind spots by detecting 100% of red-team and real attacker behaviors in real time,including identifying the first compromised account during a smishing attack that would have otherwise gone unnoticed.

Learn more

Telecom & Communication Services

Globe Telecom closed critical visibility gaps by uncovering threats across network traffic, lateral movement, and legacy systems that cannot support agents, enabling a complete view of attacker activity across the environment.

Learn more

Supermarkets

Coop gained complete visibility across network and identity, enabling confident detection of real threats while reducing noise by 98% and saving over 55,000 hours of investigation time.

Learn more

Speed & Ease of Deployment

- Fast to deploy and easy to scale across enterprise and priority environments.
- Designed to complement existing investments rather than force architectural reset.

Bottom Line

- Vectra AI strengthens the current security stack, especially post-compromise.
- It improves visibility into lateral movement, identity misuse, and mission-relevant attack behavior.
- It offers a practical, low-friction path to measurable security value.

About Vectra AI

Vectra AI delivers modern network observability, signal, and control at AI speed, giving organizations real-time visibility into their network, clear insight into which behaviors matter, and the ability to act before risk becomes impact. By connecting on-premises, multi-cloud, identity, SaaS, IoT/OT, edge, and AI activity, Vectra AI helps organizations reduce exposure, accelerate detection and response, and continuously improve security posture. With over a decade of AI and ML innovation with 39 patents and a Leader in the 2025-2026 Gartner® Magic Quadrant™ for Network Detection and Response, Vectra AI empowers security teams to stay ahead of emerging cyberattacks, increase operational efficiency, and prove resilient in an increasingly complex, AI-driven world. For more information, visit www.vectra.ai.

VECTRA AI

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