RESEARCH BRIEF

Reducing Noise, Elevating Threats: A Data-Driven Look at SOC Efficiency

A data-driven analysis on alert volume, threat prioritization, and SOC optimization.

VECTRA®

Fact: Security teams are overwhelmed by thousands of alerts

The reality is that only a small fraction of those thousands of alerts are real, actionable threats. According to the 2024 State of Threat Detection report by Vectra AI, security professionals receive 3,832 alerts per day. Of those thousands of alerts, analysts are only able to review 38% of them. As a result, 71% of SOC practitioners worry every week that they'll miss a real attack.

In this report, Vectra AI analyzed behavioral signals across our RUX Platform and MDR/MXDR customers to explore threat trends and the vitality of noise reduction in the modern SOC.

Key Takeaway: Better signal clarity starts with smarter threat visibility and prioritization where it counts.

Observation 1

Detections are seldom threats.

Vectra MDR Customers

Vectra AI ingested and analyzed over 1.1 million behavioral signals across our MDR and MXDR customers. From this vast dataset, fewer than 300 were elevated to **confirmed malicious threats** over a three-month period, illustrating how Vectra's AI filters out 99.98% of noise before it even reaches analysts.

Vectra Respond UX Customers

Of the 1,728,135 detections triggered in US-based Vectra AI customers using the Respond UX, only 9,139 entities were prioritized across 131 customers within a 1-month period. That is less than 70 prioritized entities per month per customer. This is 0.53% of the total number of detections over a 1-month period.

VECTRA'S AI AGENTS FILTER OUT

99.98%

of noise before it even reaches analysts

Key Takeaway:

Tool selection should focus on platforms that reduce the volume-to-value gap, not just those that add detection feeds.

Observation 2

Insider threats are on the rise.

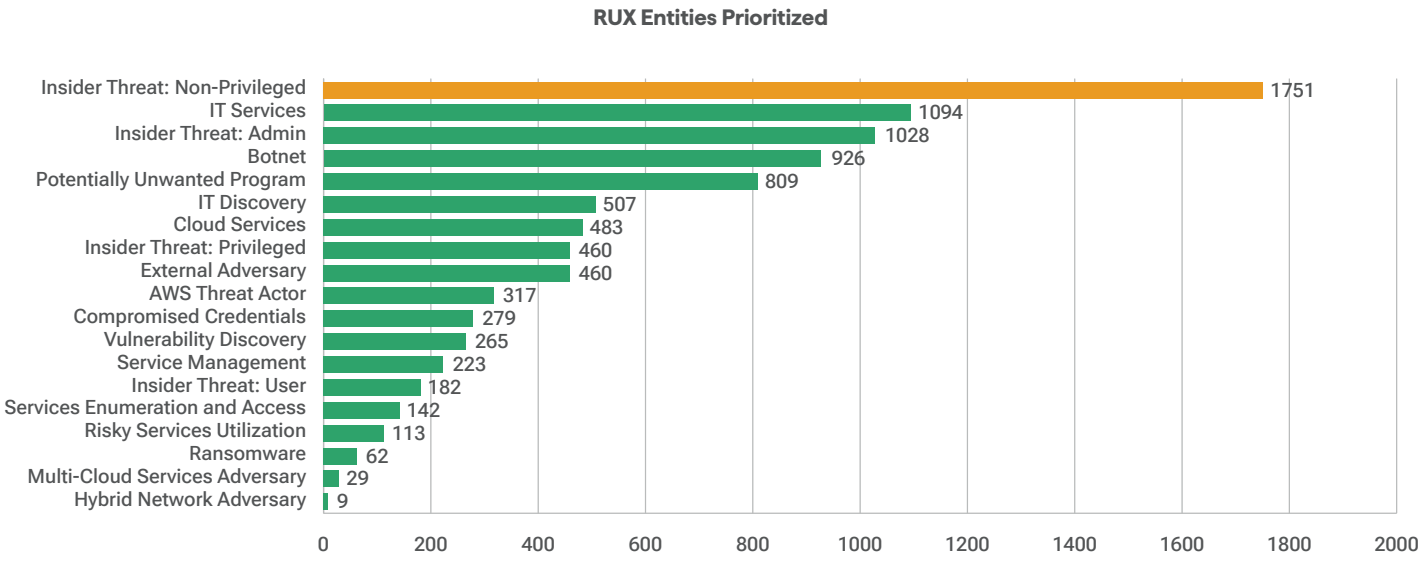
Vectra Respond UX Customers

Of the 9,139 entities prioritized for RUX customers in the US, 19.2% were Non-Privileged Insider Threats, which is the most prevalent attacker profile during the reported period. Non-privileged insider threats come from two possible root causes:

- An emerging external adversary targeting data resources
- An identity was compromised and is using additional privileges and access not previously observed

Of the 9,139 entities prioritized for RUX customers in the US, 38% of prioritized threats linked to insider behaviors, often via non-privileged and admin identities.

Figure 3: Number of entities prioritized by attack profile



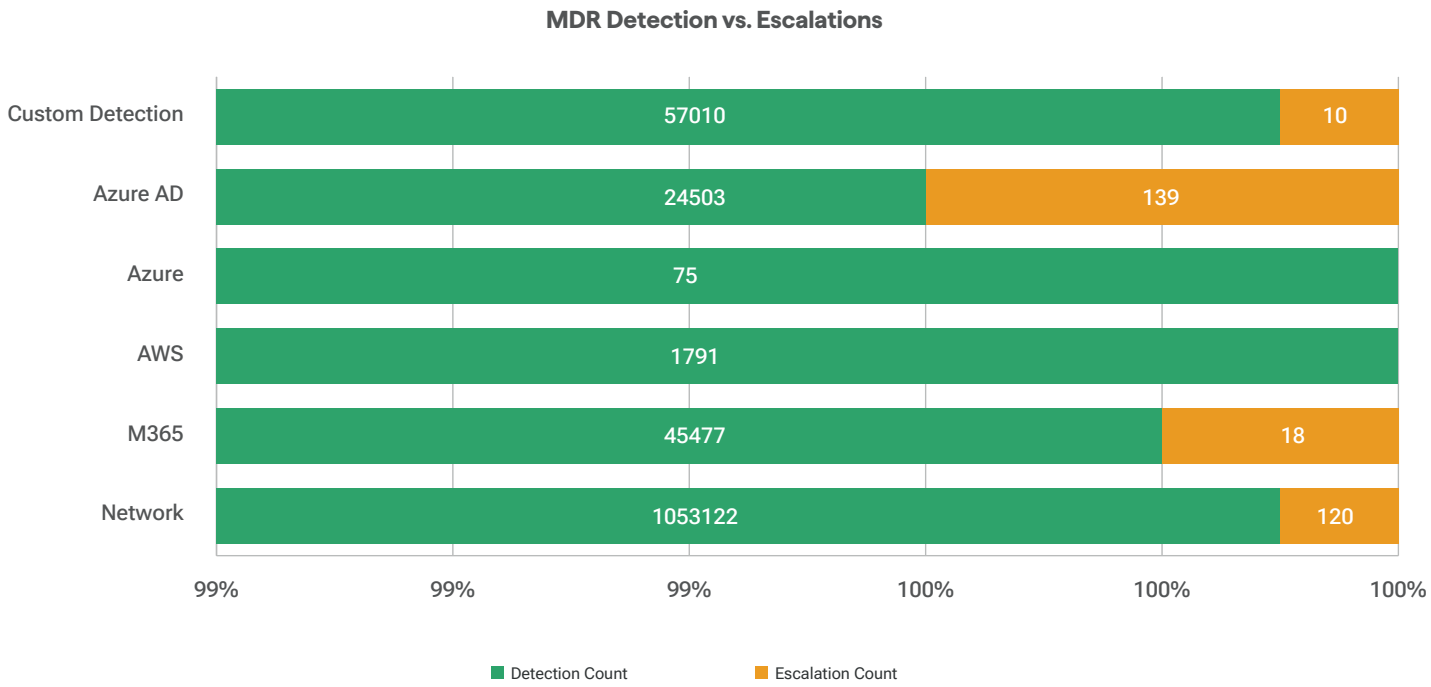
Source: Vectra RUX Entities — February 3-March 3, 2025

This chart displays the distribution of prioritized threat entities in RUX across various attack profiles.

Vectra MDR Customers

For Vectra MDR and MXDR customers, of the 287 true positives escalated, 48% of the cases were for attacks originating from Azure AD. Specifically, 65 of the escalations were for Azure AD Suspicious Sign-On detections. This accounts for 23% of the total malicious true positives escalated during this time period.

Figure 4: Malicious true positive escalations by the Vectra MDR team by attack surface.



Source: Vectra MDR Escalations — January-March 2025

This chart compares MDR customer detection volume to escalation frequency across six attack surfaces, highlighting Azure AD and M365 as high-signal contributors.

Key Takeaway:

User and identity misuse is bound to happen, so focus on TDIR strategies and technologies that permeate the modern network and highlight user and identity misuse, not just perimeter behaviors.

Observation 3

Custom detections matter.

Custom detections in Vectra AI are tailored rules created to surface threats specific to an organization's unique environment or risk profile. They extend platform coverage beyond standard models to detect high-priority behaviors that matter most to each customer.

Vectra MDR Customers

Custom detections accounted for 4.8% of MDR and MXDR detections with 10 confirmed malicious true positives.

Vectra Respond UX Customers

For RUX customers, custom detections accounted for 6.6% of the detections.

CUSTOM DETECTIONS ACCOUNT FOR:

4.8% of MDR escalations

6.6% of RUX detections

Key Takeaway:

In both RUX and MDR/MXDR data, custom detections provide visibility into organization-specific risks. TDIR platforms should support flexible tuning and services to align detections with unique attacker behaviors.

Recommendations for SOC Teams and Security Buyers

1. Prioritize Tools That Minimize Alert Noise and Maximize Threat Precision

Select detection platforms that correlate, triage, and prioritize detections to surface only high-confidence, actionable threats. With less than 1% of alerts proving malicious, reducing alert fatigue is essential to SOC efficiency and optimization.

2. Invest in Pervasive Threat Detection

With nearly half of true positives linked to Azure AD and a significant portion tied to insider misuse, security solutions must provide deep visibility into behaviors within the modern network, not just endpoint. TDIR capabilities that follow attacker movement across user, credential, and network access layers are no longer optional – it's a requirement.

3. Automate Prioritization Without Losing Context

Implement tools that use AI and machine learning to automate the prioritization of entities, helping analysts cut through overwhelming volumes of alerts while preserving investigation context. Solutions that can distill millions of raw detections into a few dozen meaningful entities can dramatically improve detection-to-response speed and reduce risk.

4. Prioritize Platforms That Support Custom Detection Tuning

Organizations face unique threats, and custom detections, though limited in volume, consistently uncover true positives. Buyers should prioritize TDIR platforms with flexible detection customization both within the technology and in available consulting services to align with their specific risk profiles.

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that protects modern networks from modern attacks. When modern cyber attackers bypass existing controls, evade detection and gain access to customers' data center, campus, remote work, identity, cloud, and IoT/OT environments, the Vectra AI Platform sees their every move, connects the dots in real-time, and stops them from becoming breaches. With 35 patents in AI security and the most vendor references in MITRE D3FEND, organizations worldwide rely on Vectra AI to see and stop attacks their other tools can't.
For more information, visit www.vectra.ai.

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