VECTRA®

Customer Guide

WHY MIGRATE TO THE VECTRA AI PLATFORM

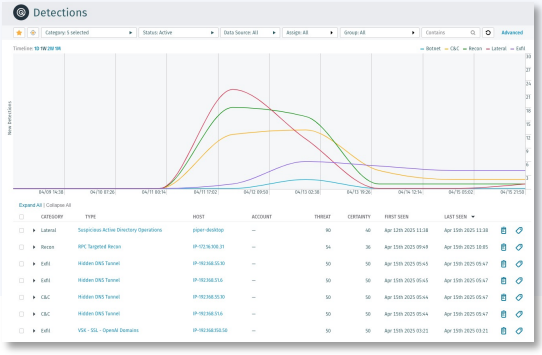
with Respond UX (RUX)

Updated Q1 2025

REASON #1: **SIGNAL CLARITY**

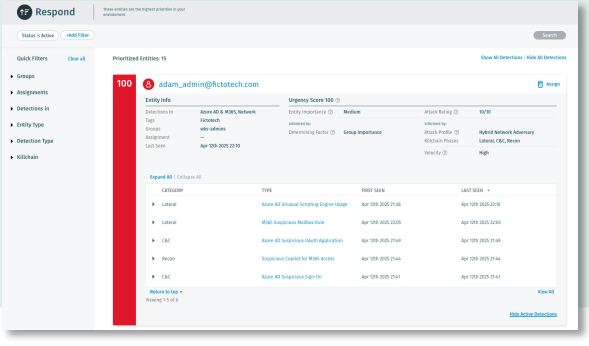
Vectra AI's RUX prioritization engine brings clear, actionable signals to analysts.

CHALLENGES WITH QUADRANT UX



- Too much information with no clear direction on where to begin investigations
- Lacks prioritization of the most urgent threats
- Detections don't tell the complete modern attack story

WHY RESPOND UX



- Clear AI-driven prioritization and triage of urgent threats
- Bite-size information for quicker analysis
- Security analyst workflow is supported by the platform

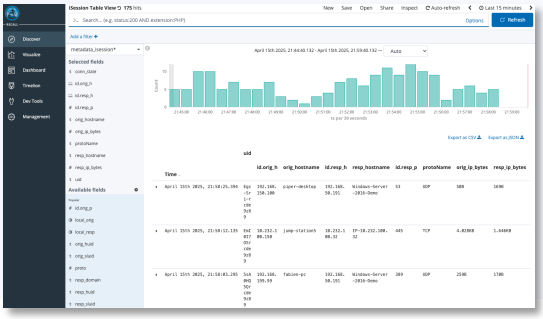
"With Vectra in place, the light started to turn on. Its automation and filtering capabilities allowed us to focus on the most important threats, which made our team more efficient and effective in our response."

Globe Telecom
Telecom & Communications

REASON #2: **INTELLIGENT CONTROL**

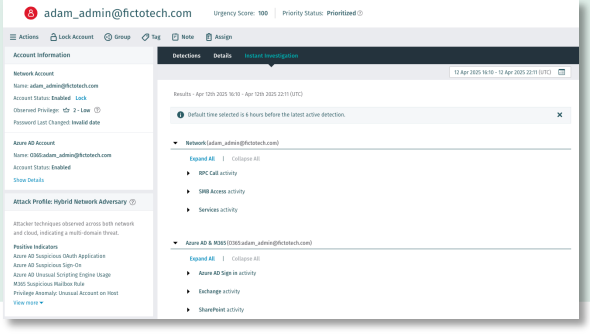
Vectra AI's RUX allows analysts to monitor, investigate, and respond to alerts within a single pane of glass.

CHALLENGES WITH QUADRANT UX



- Need to pivot to Vectra Recall for further investigation
- Workflow is overwhelming with no clear direction on where to start
- Unclear connection to the surfaced threat that needed further investigation

WHY RESPOND UX



- Pre-built queries via Instant Investigations for prioritized threat
- Single screen, not need for pivoting
- Seamless workflow from monitoring to investigation to response, accelerating MTTR

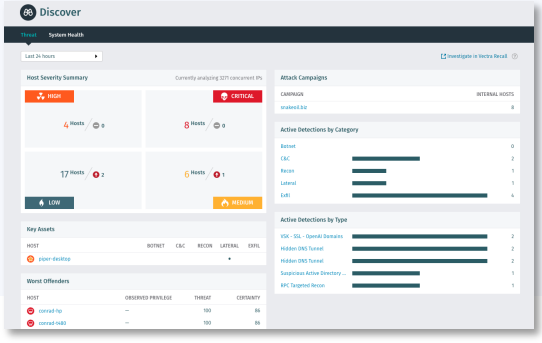
"We realized that the ease of use and automation of Vectra, combined with its high efficiency, will save us time, give us greater understanding of the context of each attack, and facilitate faster reactions to eliminate threats."

mLeasing
Finance

REASON #3: **MODERN NETWORK COVERAGE**

Vectra AI's RUX covers the entire modern network with multi-domain support.

CHALLENGES WITH QUADRANT UX



- Need to pivot to Vectra Recall for further investigation
- Workflow is overwhelming with no clear direction on where to start
- Unclear connection to the surfaced threat that needed further investigation

WHY RESPOND UX

- Multi-domain coverage for modern networks
- Datacenters, identities, cloud servers, applications

"Vectra AI not only covers the basics, but with detection models, it really looks at the identity traversing through Microsoft Entra ID and Microsoft 365. That gives us a complete picture."

Coop
Supermarkets

VECTRA®

FEATURE LEVEL COMPARISONS

ATTACK COVERAGE

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) provides customers attack coverage with AI Detections that identify unknown threats across networks, identity, and cloud in real-time.

WHY RUX FOR **ATTACK COVERAGE:**

- **RUX tells the entire modern attack story with full coverage across the modern network**. While attack coverage is comprehensive for QUX, it lacks the entire modern network story without cloud detection for Azure.
- **RUX unifies all entities (hosts and accounts) under a single module.** Because of how QUX is deployed and implemented, hosts and accounts are separated into two views that add cognitive load to manual analysis.

FEATURE LEVEL COMPARISON:

Attack Surface Coverage		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
AI Detections for Public Cloud (Azure)[1]	No	Yes
Unified visibility across all attack surfaces	Limited	Yes
Unified visibility of entities (hosts and accounts)	No	Yes

1) For a comprehensive list of detections, please see the appendix.

SIGNAL CLARITY

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) gives customers signal clarity with AI Assistants that automatically triage and correlate threat events to prioritize single entities under attack.

WHY RUX FOR **SIGNAL CLARITY:**

- **RUX utilizes Vectra's AI Assistants to cut the noise**. With AI-powered prioritization, triage, and stitching, RUX streamlines threat detection and investigation for customers while QUX cannot pull all data and information together for an integrated signal.
  - AI Prioritization: highlights what's most critical and urgent – factoring in how observed behaviors map to real attacks, considering attack velocity, breadth, and the privileges of the affected accounts and hosts.
  - AI Triage: distinguishes true from false, malicious from benign – surfacing only high-relevance threats based on deviations from normal behavior

FEATURE LEVEL COMPARISON:

Signal Clarity		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
AI Prioritization	No	Yes
AI Triage for Network	Yes	Yes
AI Triage for Azure AD	No	Yes
AI Triage for AWS	No	Yes
AI Triage for M365	No	Yes
AI Triage for Azure	No	Yes
Single prioritized list of incidents across attack surfaces	No	Yes
Ability to customize prioritization score	No	Yes
Ability to customize prioritization thresholds	No	Yes
Ability to filter prioritized entities by attack surface	No	Yes
Ability to filter prioritized entities by detection type	No	Yes
Ability to filter prioritized entities by entity type	No	Yes
Ability to view all scoring factors without having to click into the entity	No	Yes
Ability to view detection summary without having to click into the entity	No	Yes
Easy access for remote and distributed teams	No	Yes
Network metadata based custom models	Requires Vectra Recall	No

INTELLIGENT CONTROL – DISCOVER

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) puts defenders in control with the context needed to discover where vulnerabilities exist that attackers may exploit.

WHY RUX FOR **DISCOVERY:**

- **RUX enables security professionals to enforce a proactive threat defense security program with dynamic snapshots on system and threat surface health.** Discover Dashboards are critical to offering security engineers and architects visibility into deployments across the modern network, gathering information on potential gaps in coverage and/or compliance issues.

FEATURE LEVEL COMPARISON:

Discover Dashboards		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
Threat Summary dashboard	No	Yes
Azure dashboard	No	Yes
Azure AD dashboard	No	Yes
Copilot M365 dashboard	No	Yes
Network dashboard	No	Yes
System Health dashboard	Yes	Yes

INTELLIGENT CONTROL – HUNT

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) puts defenders in control with the context needed to hunt for attackers in their environment.

WHY RUX FOR **THREAT HUNTING:**

> **RUX's Hunt dashboard is more intuitive than QUX's equivalent.** QUX's equivalent of the Hunt dashboard lacks the ability to discover threat trends and attacker patterns within the environment across the entire modern network due to limitations in the design of the visualization.

FEATURE LEVEL COMPARISON:

Threat Hunting		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
Hunt dashboard	No	Yes
Hosts dashboard	Yes	No

INTELLIGENT CONTROL – INVESTIGATE

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) puts defenders in control with the context needed to rapidly investigate attacks in progress.

WHY RUX FOR **INVESTIGATIONS:**

- **RUX offers the metadata that is critical to investigations.** QUX can ingest metadata for investigations at an additional cost while RUX has it available out-of-the box.
- **Investigations can span across the entire modern network.** Investigations in QUX are limited to network data while RUX can pull in information from datacenters, identity, and cloud.

FEATURE LEVEL COMPARISON:

Investigation		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
AI-enriched Zeek metadata across 16 different streams	Only with Recall	Yes
Micro-PCAP for network detections	Yes	Yes
Instant Investigations for network hosts	No	Yes
Instant investigation for network accounts	No	Yes
Instant Investigations for AzureAD and M365 accounts	No	Yes
Instant investigations for AWS accounts	No	Yes
Network metadata integrated into the UI	No	Yes
AWS, Azure AD, M365 metadata integrated in the UI	No	Yes
Ability to filter, sort, download the metadata from the UI	Network only with Recall	Yes, across all attack surfaces
Advanced search on detections	Yes	Yes
Dashboards using network metadata	Network only with Recall	Yes

INTELLIGENT CONTROL – RESPOND

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) puts defenders in control with the controls needed to stop attacks early in their progression.

WHY RUX FOR **RESPONSE:**

- **RUX supports the full scope of responding to threats.** While QUX can utilize limited native response actions and integrated response actions (e.g. endpoint host lockdown on natively supported integrations), users miss out on response and remediation actions available through Vectra's Managed Services. Vectra's Managed Services can integrate with a portfolio of 100+ security technologies, enabling customers to enact response across their entire modern network.

FEATURE LEVEL COMPARISON:

Response		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
AD Account Lockdown	Yes	Yes
Azure AD Account Lockdown	No	Yes
Endpoint Host Lockdown for all natively-supported EDRs *Crowdstrike, Microsoft Defender, SentinelOne, Cybereason, Carbon Black, FireEye HX*	Yes	Yes
Managed response and remediation	Limited	Yes
CORTEX XSOAR App	Yes	Yes
ServiceNow App	ITSM and SIR	ITSM and SIR
Custom Response Integrations: Firewall, NAC, etc.	Vectra Automated Response (VAR) Integrations or Custom-built on API v2	Vectra Automated Response (VAR) Integrations or Custom-built on API v3

INTELLIGENT CONTROL – REPORTING

QUX vs RUX

The Vectra AI Platform with Respond UX (RUX) puts defenders in control with the context needed to report on overall security posture and operational efficiency.

WHY RUX FOR **REPORTING:**

- **RUX offers out-of-the-box reporting for all members on the security team.** Reporting on RUX has curated reports for security executives, security analysts, and security architects or engineers while QUX only has reports available for security architects/engineers to assess the network system.
- **RUX's reporting allows executives to align the Vectra system with their overarching security program.** The Executive Overview report highlights security posture and operational efficiency, enabling security executives to justify investments in Vectra and assess security risk and management.

FEATURE LEVEL COMPARISON:

Reporting		
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
Executive Overview report	No	Yes
Attack Signal report	No	Yes
Asset inventory report	Yes	Yes
Operational metrics report	Yes	Yes
Host severity report	Yes	No
Active Posture for Network, Identity, and Copilot for M365	No	Yes

INTELLIGENT CONTROL – TECH INTEGRATIONS

QUX vs RUX

> The Vectra AI Platform with Quadrant UX (QUX) and Respond UX (UX) puts defenders in control of third-party data and information with technical integrations available natively and externally via API.

Native Integrations	Current solution	New: Vectra AI Platform
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
rDNS	Yes	Yes
Windows event log ingestion	Yes	Yes
ZScaler Private Access (ZPA) ingestion	Yes	Yes
DHCP ingestion	Yes	Yes

External Integrations	Current solution	New: Vectra AI Platform
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
API support	Token-based	OAuth-2 based
Event-based API support	No	Yes
Splunk TA and App support	Yes	Yes
IBM QRadar and QROC support	Yes	Yes
Syslog based integration with SIEM	Yes (syslog from Brain)	Yes - external syslog converter
Custom Integrations* built on API	Custom-developed on API v2	Must be re-built for API v3
Splunk SIEM and SOAR	Yes	Yes
IBM QRadar	Yes	Yes
Microsoft Sentinel	Yes	Yes
Palo Alto Networks SOAR	Yes	Yes
ServiceNow SOAR and ITSM	Yes	Yes
Google SecOps SIEM and SOAR	Yes	Yes

INTELLIGENT CONTROL – ADMINISTRATION

QUX vs RUX

> The Vectra AI Platform with Quadrant UX (QUX) and Respond UX (UX) puts defenders in control of the platform with administrative capabilities meant to increase efficiency and streamline workflows.

Core Capabilities	Current solution	New: Vectra AI Platform
Analyst Experience	**Quadrant UX (Appliance)**	**Respond UX (SaaS)**
Internal IP definition	Yes	Yes
Support for physical, virtual or cloud network sensors	Yes	Yes
Triage filters	Yes	Yes
Host groups	Yes	Yes
Account groups	Yes	Yes
Vectra threat feed	Yes	Yes
Custom threat feed	Yes	Yes
VCenter integration	Yes	Yes
Proxy support	Yes	Yes
Granular RBAC	Yes	Yes
Vectra defined roles	Yes	Yes
Custom roles	Yes	No
Selective PCAP	Yes	Yes
Configurable time zone	Yes	Yes
Internal IP definition	Yes	Yes
Support for physical, virtual or cloud network sensors	Yes	Yes
Triage filters	Yes	Yes
Host groups	Yes	Yes
Account groups	Yes	Yes
Authentication	Local, SAML, Radius, Tacacs, LDAP	Local and SAML
Dynamic Groups	Yes	Yes

PACKAGING

QUX vs RUX

The Vectra AI Platform offers three different packages with varying levels of customer support and metadata to cater to customer environments.

Package	**Vectra AI - Essential** (Quadrant UX)	**Vectra AI – Standard** (Respond UX)	**Vectra AI – Complete** (Respond UX)
SaaS Delivery	✗	✓	✓
Integrated Metadata – 3 days	✗	✓	✓
Integrated Metadata – 14 days	✗	⛶	✓
Integrated Metadata – 30 days	✗	⛶	⛶
Premium Support	⛶	⛶	✓
Premium MDR	⛶	✗	✓
Standard MDR	⛶	⛶	✗
Premium MXDR	✗	✗	⛶
Services	⛶	⛶	⛶
Stream	⛶	⛶	⛶
Match	⛶	⛶*	⛶
Recall	⛶	✗	✗

Disclaimer: This document is for informational purposes only and is subject to change. For items marked “Roadmap Target” we are providing our best estimate. As market conditions, customer requirements, and product priorities shift, the delivery of said items may also shift. We are committed to keeping this document as up to date as possible.

VECTRA®

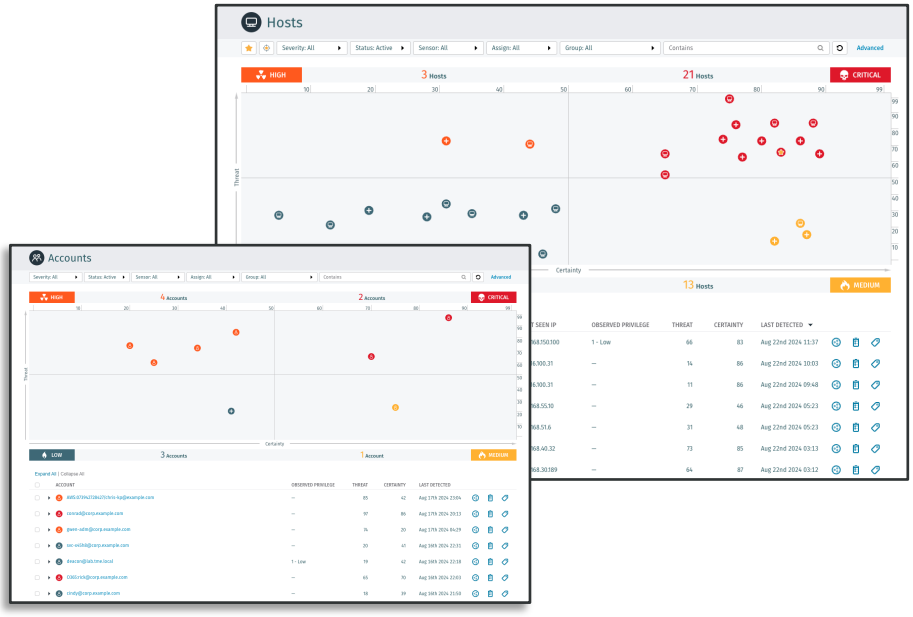
INTERFACE COMPARISON

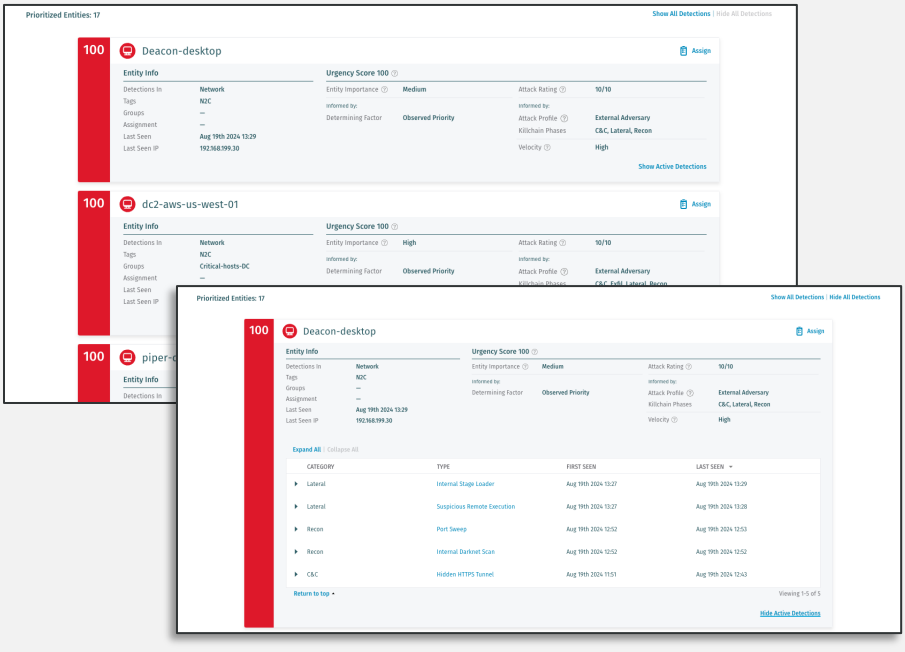
ATTACK COVERAGE

Quadrant UX

Host and Accounts Quadrants

Prioritized hosts and accounts separated by two different quadrant views.





Respond UX

Respond Console

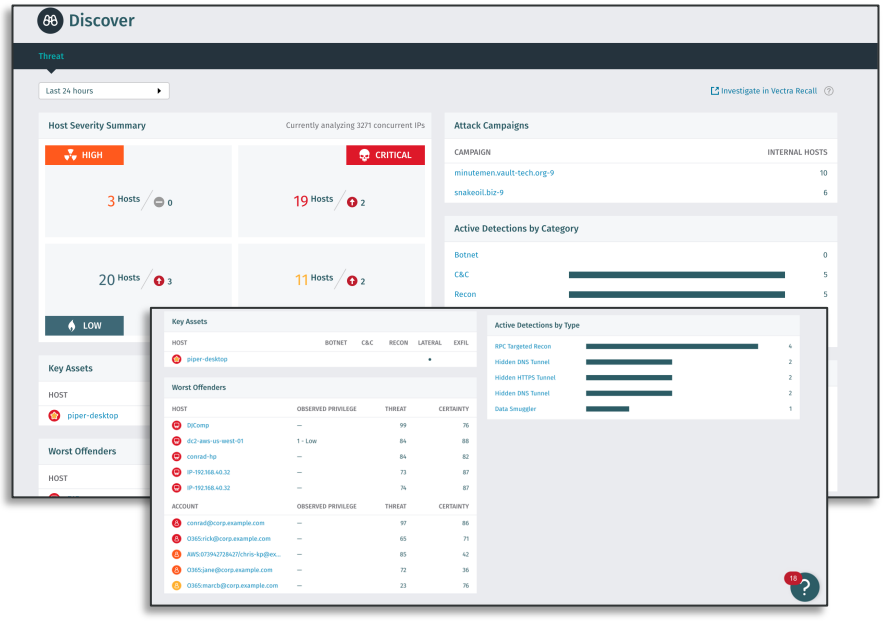
Unified list of hosts and accounts organized under an entity with snapshot view of correlated detections.

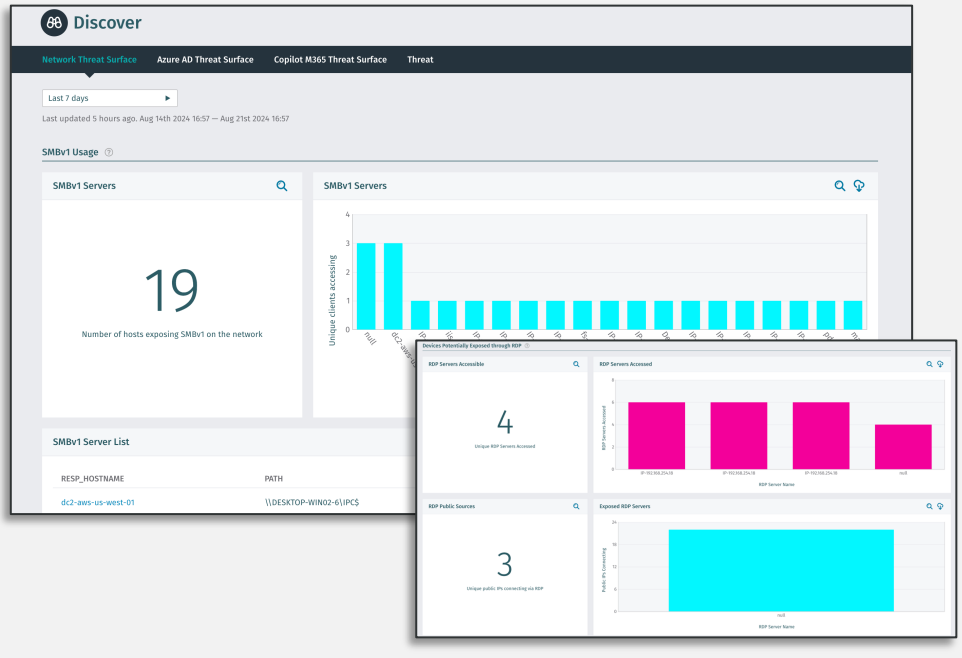
DISCOVER DASHBOARDS

Quadrant UX

Discover Dashboard

Snapshot of information from Host and Account quadrants.





Respond UX

Discover Dashboards

Shows security posture dynamically for datacenter, cloud, and identity along with system health.

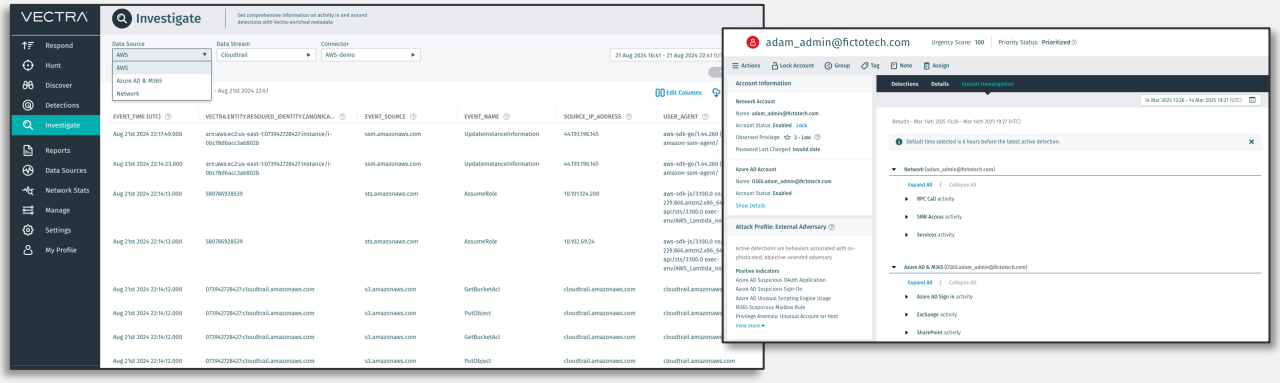
INVESTIGATIONS AND THREAT HUNTING

Quadrant UX

Investigations and Hunt consoles are **unavailable** in QUX.

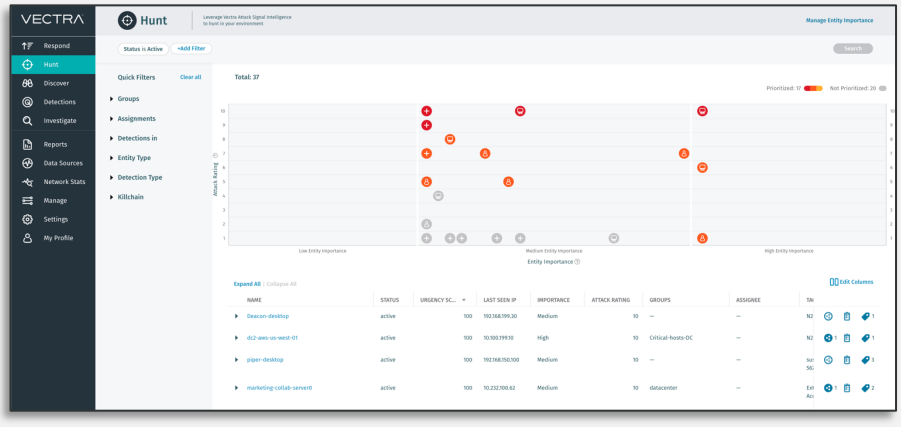
Respond UX *Investigations Module*

Advanced Investigations console with intuitive query-building. Single-click pivot from Instant Investigations.



Respond UX *Hunt Module*

Visualized overview of threats across the entire environment.



VECTRA®

DETECTIONS

ATTACK COVERAGE – **NETWORK AND AWS DETECTIONS**

These detections are available on QUX and RUX.

Network Detections

Command & Control

External Remote Access
ICMP Tunnel
Hidden Tunnel
Hidden DNS Tunnel
Hidden HTTP Tunnel
Hidden HTTPS Tunnel
Malware Update
Multi-home Fronted Tunnel
Peer-to-Peer
Stealth HTTP Post
Suspect Domain Activity
Suspicious HTTP
Suspicious Relay
TOR Activity
Threat Intelligence Match
Vectra Threat Intelligence Match

Exfiltration

Data Gathering
Data Smuggler
Hidden DNS Tunnel
Hidden HTTP Tunnel
Hidden HTTPS Tunnel
ICMP Tunnel
Smash and Grab
Threat Intelligence Match

Botnet Activity

Brute-Force
Cryptocurrency Mining
Outbound DoS
Outbound Port Sweep

Reconnaissance

File Share Enumeration
Internal Darknet Scan
Kerberoasting: Weak Cipher Request
Kerberoasting: SPN Sweep
Kerberos Account Scan
Kerberos Brute-Sweep
RDP Recon
RPC Recon
RPC Targeted Recon
SMB Account Scan
Suspicious LDAP Query
Suspicious Port Scan
Suspicious Port Sweep

Lateral Movement

Automated Replication
Brute-Force
ICMP Tunnel: Client
ICMP Tunnel: Server
Kerberoasting: Targeted Weak Cipher Response
Privilege Anomaly: Unusual Account on Host
Privilege Anomaly: Unusual Host
Privilege Anomaly: Unusual Service
Privilege Anomaly: Unusual Service – Insider
Privilege Anomaly: Unusual Service from Host
Privilege Anomaly: Unusual Trio
Ransomware File Activity
SMB Brute-Force
Shell Knocker Client
Shell Knocker Server
SQL Injection Activity
Stage Loader
Suspicious Active Directory Operations
Suspicious Admin
Suspicious Remote Desktop
Suspicious Remote Execution
Threat Intelligence Match

AWS Detections

Command & Control

AWS Root Credential Usage
AWS Suspicious Credential Usage
AWS TOR Activity

Exfiltration

AWS Suspect External Access Granting
AWS Suspect Public AMI Change
AWS Suspect Public EBS Change
AWS Suspect Public RDS Change
AWS Suspect Public EC2 Change
AWS Suspect Public S3 Change

Botnet Activity

AWS Cryptomining
AWS Suspect Traffic Mirror Creation

Reconnaissance

AWS External Network Discovery
AWS Network Configuration Discovery
AWS Organization Discovery
AWS S3 Enumeration
AWS Suspect Credential Access from EC2
AWS Suspect Credential Access from ECS
AWS Suspect Credential Access from SSM
AWS Suspect Discovery from EC2 Instance
AWS Suspect Escalation Reconnaissance
AWS Suspicious C2 Enumeration
AWS User Permissions Enumeration

Lateral Movement

AWS ECR Hijacking
AWS Lambda Hijacking
AWS Logging Disabled
AWS Ransomware S3 Activity
AWS Security Tools Disabled
AWS Suspect Admin Privilege Granting
AWS Suspect Console Pivot
AWS Suspect Login Profile Manipulation
AWS Suspect Organization Exit
AWS Suspect Privilege Escalation
AWS Suspect Region Activity
AWS User Hijacking

ATTACK COVERAGE – **M365 AND AZURE AD DETECTIONS**

These detections are available on QUX and RUX.

M365 Detections

Command & Control

M365 Power Automate HTTP Flow Creation
M365 Suspicious Power Automate Flow Creation

Exfiltration

M365 eDiscovery Exfil
M365 Exfiltration Before Termination
M365 Suspicious Download Activity
M365 Suspicious Exchange Transport Rule
M365 Suspicious Mail Forwarding
M365 Suspect Power Automate Activity
M365 Suspicious Sharing Activity

Reconnaissance

M365 Suspicious Compliance Search
M365 Suspicious Copilot for M365 Access
M365 Unusual eDiscovery Search
M365 Suspect eDiscovery Usage

Lateral Movement

M365 Attacker Tool: Ruler
M365 Disabling of Security Tools
M365 DLL Hijacking Activity
M365 External Teams Access
M365 Internal Spearphishing
M365 Log Disabling Attempt
M365 Malware Stage: Upload
M365 Ransomware
M365 Risky Exchange Operation
M365 Phishing Simulation Configuration Change
M365 SecOps Mailbox Change
M365 Suspicious Teams Application
M365 Suspicious Mailbox Manipulation
M365 Suspicious Mailbox Rule Creation

Azure AD Detections

Command & Control

Azure AD Admin Account Creation
Azure AD Cross Tenant Access Change
Azure AD Domain Settings Modified
Azure AD Login From Suspicious Location
Azure AD MFA-Failed Suspicious Sign-On
Azure AD New Certification Authority Registered
Azure AD New Partner Added to Organization
Azure AD Redundant Access Creation
Azure AD Suspicious OAuth Application
Azure AD Suspicious Sign-On
Azure AD Suspicious Access from Cloud Provider
Azure AD Suspected Compromised Access
Azure AD TOR Activity

Lateral Movement

Azure AD Successful Brute-Force
Azure AD Successful Brute-Force – Failed Login
Azure AD Suspicious Device Registration
Azure AD Suspicious Factor Registration
Azure AD Change to Trusted IP Configuration
Azure AD MFA Disabled
Azure AD Newly Created Admin Account
Azure AD Privilege Operation Anomaly
Azure AD Unusual Scripting Engine Usage

ATTACK COVERAGE – **PUBLIC CLOUD** DETECTIONS

Public Cloud (Azure) detections are **only** available on the Respond UX.

Azure Detections		
Command & Control	**Botnet Activity**	**Lateral Movement**
Azure Suspicious Access from AWS Cloud Azure Suspicious Access from GCP Cloud Azure Suspicious Hybrid Machine Extension Installation Azure Suspicious Hybrid Machine Run Command Execution Azure Suspicious VM Extension Installation Azure Suspicious VM Run Command Execution Azure Suspicious VM Scale Set Extension Installation Azure Suspicious VM Scale Set Run Command Execution Azure Suspicious VM Automation Test Azure Suspicious Hybrid Automation Test Azure Suspicious Automation Staged Azure Suspicious VM Automation Execution Azure Suspicious Hybrid Automation Execution Azure TOR Activity	Azure Cryptomining **Exfiltration** Azure Suspect Public Storage Account Change Azure Suspicious Disk Download Azure Suspicious Key Vault Extraction **Reconnaissance** Azure Suspect Credential Dump Azure Suspect Key Vault Enumeration	Azure Anomalous App Service WebJob Activity Azure Diagnostic Logging Disabled Azure Managed Identity Anomaly Azure Mass Resource Deletion Azure Privilege Anomaly: Management Group Score Azure Privilege Anomaly: Root Scope Azure Resource Group Admin Privilege Granting Azure Resource Group Admin Role Unassigned Azure Subscription Admin Privilege Granting Azure Subscription Admin Role Unassigned Azure Suspect App Service Deployment Activity Azure Suspect Key Vault Privilege Granting Azure Suspicious App Service Creation or Modification Azure Suspicious App Service Credential Download Azure Suspicious App Service Deployment Configuration Download Azure Suspicious Automation DSC Execution Azure Suspicious Policy Assignment Azure Suspicious Policy Creation or Modification Azure Suspicious Remediation Task Azure Suspicious Serial Console Usage