REAL WORLD ATTACK SIMULATION RESULTS

Close Microsoft Threat Detection, Investigation and Response Gaps With Vectra AI

With modern cyberattacks, different doesn't always mean malicious, and normal doesn't always mean benign. Learn how security teams can go beyond the basics to reinforce their hybrid / multi-cloud defense.

VECTRA® Integrity360
your security in mind

Modern attackers no longer need to hack their way in, they try to log in.

According to the *Microsoft Digital Defense Report 2024*, Microsoft customers face over 600 million cybercriminal and nation-state attacks daily. If left undetected, these attacks could lead to costly business disruptions, ransomware incidents, and theft of high-value data. Attackers only need to be right once. The question is: can security teams rely solely on native security solutions to stay safe? **Unfortunately the answer is no.**

To effectively defend against today's attack – defenders need to:

1. **ASSUME BREACH**

   see and stop attackers who are moving seamlessly in the environment and across the network, Active Directory, Entra ID, M365, Azure, and Copilot for M365.

2. **RELY ON AI DETECTIONS**

   because different doesn't always mean malicious, and normal doesn't always mean benign.

3. **HAVE RELIABLE PRIORITIZATION**

   so you don't miss an attack and can take swift actions on urgent and real threats.

Here, we reveal real attack simulations and red team results on multi-cloud and hybrid cloud environments. You'll discover:

How attackers were able to bypass native defenses.

How security teams detected and stopped them before damage occurred.

How Vectra AI reinforces defenses for hybrid / multi cloud security.

Vectra AI's 360° coverage for the Microsoft ecosystem

We fill gaps to complement native solutions

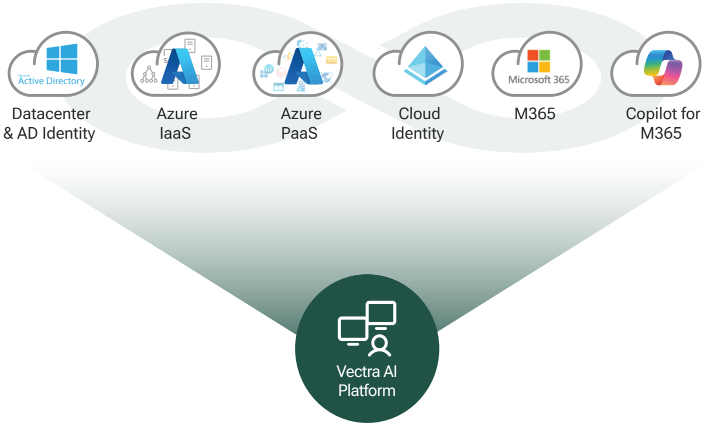
DEFENDER XDR + SENTINEL OFFERS:

Baseline threat intel and anomaly detection

Posture management

Endpoint coverage

Logs that enable customized workflows



Vectra AI extends visibility and value by providing:

Comprehensive threat coverage:

- Detect attacks Defender misses by securing Network, Active Directory, Entra ID, M365, Copilot and Azure against hidden threats.

Credential attack visibility:

- Gain visibility at every stage of identity attacks.

Hybrid-Cloud protection

- Protect hybrid services for Azure organizations that have data center workloads.

Connect the dots:

- AI correlates attacker behaviors across domains, prioritizing the most urgent risks across the Microsoft ecosystem.

Accelerated investigation:

- Vectra's enriched metadata and logs add context beyond what's available in a SIEM for deeper threat hunting and investigation.

MXDR:

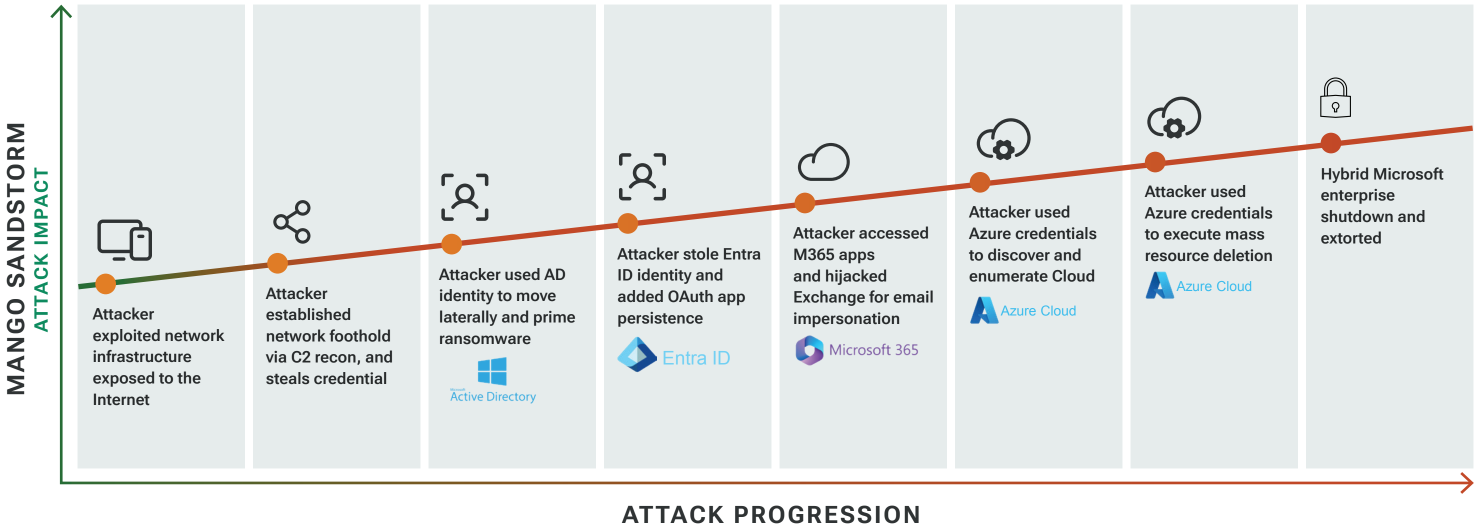
- Vectra's 24/7 MXDR hybrid attack experts alleviate the operational burden in threat detection and response.

Table of Contents

The Microsoft threat Surface is huge

Spanning across Active Directory, Microsoft Entra ID, M365 and Azure

Attackers can **move across different Microsoft attack surface seamlessly–** targeting critical resources and data.

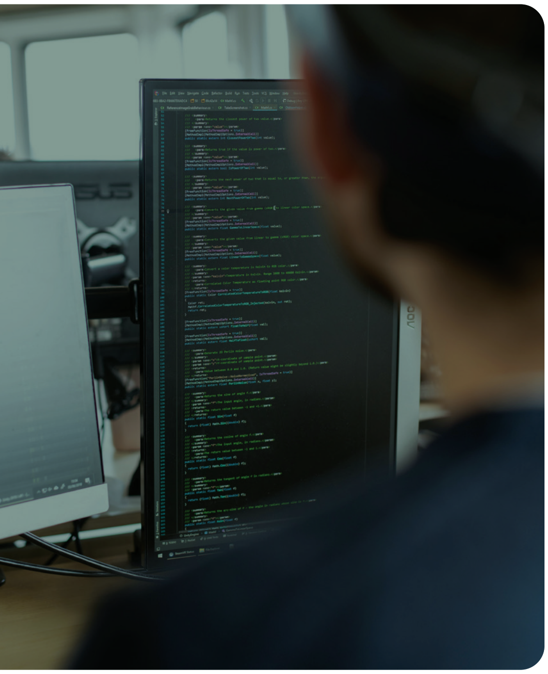


1. Attacker exploited network infrastructure exposed to the Internet
2. Attacker established network foothold via C2 recon, and steals credential
3. Attacker used AD identity to move laterally and prime ransomware
4. Attacker stole Entra ID identity and added OAuth app persistence
5. Attacker accessed M365 apps and hijacked Exchange for email impersonation
6. Attacker used Azure credentials to discover and enumerate Cloud
7. Attacker used Azure credentials to execute mass resource deletion
8. Hybrid Microsoft enterprise shutdown and extorted

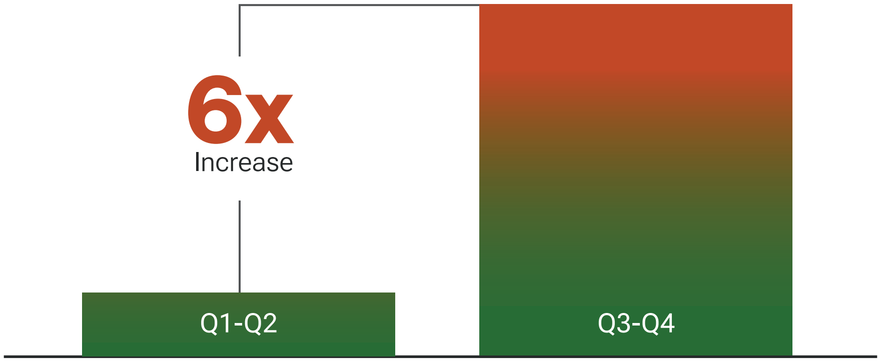
- **Prevention fails and native solutions fail to detect such attacks**
- **Attackers can start the attack at any of the above attack surfaces**

2024 attack trends from Vectra MDR

Microsoft security helps but does not fully solve the problem



Malicious Identity Attacks 2024*



- Vectra MDR finds that customers with premium licenses (E5) continue to have fewer incidents.
- However, 57% of E5 customers had a validated compromise stopped by Vectra AI.
- 6X increase in malicious identity attacks.

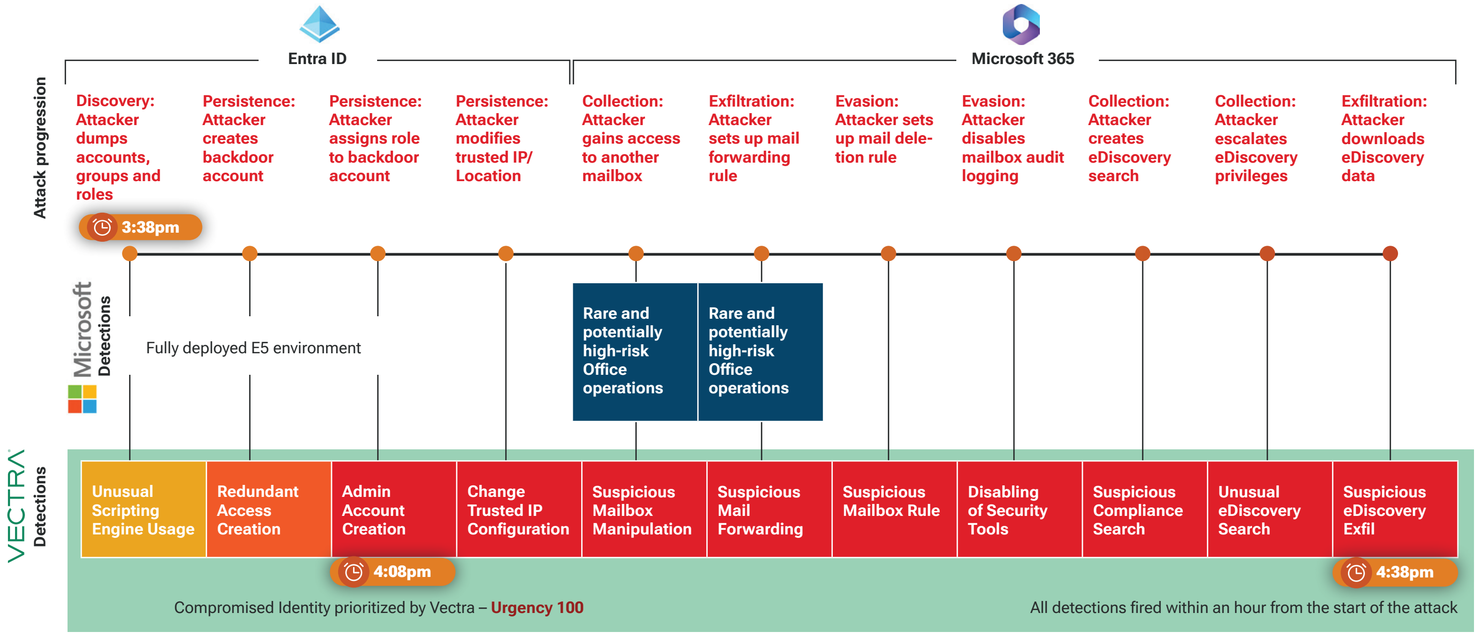
> “Vectra AI covers not only the basics, but with the detection models, it really looks at the identities traversing through Microsoft Azure and Office 365, and that gives us a complete picture.”
>
> **FABIAN HEIZ**
> CISO at Coop

* Source: Vectra AI MDR Analysis October 2024

ATTACK SIMULATION RESULT #1:

Ransomware attack by Scattered Spider

Vectra AI extends value of E5 by finding 11x additional attacker technique



Entra ID

Microsoft 365

Attack progression

Discovery: Attacker dumps accounts, groups and roles

Persistence: Attacker creates backdoor account

Persistence: Attacker assigns role to backdoor account

Persistence: Attacker modifies trusted IP/ Location

Collection: Attacker gains access to another mailbox

Exfiltration: Attacker sets up mail forwarding rule

Evasion: Attacker sets up mail deletion rule

Evasion: Attacker disables mailbox audit logging

Collection: Attacker creates eDiscovery search

Collection: Attacker escalates eDiscovery privileges

Exfiltration: Attacker downloads eDiscovery data

3:38pm

Microsoft Detections

Fully deployed E5 environment

Rare and potentially high-risk Office operations

Rare and potentially high-risk Office operations

VECTRA Detections

Unusual Scripting Engine Usage

Redundant Access Creation

Admin Account Creation

Change Trusted IP Configuration

Suspicious Mailbox Manipulation

Suspicious Mail Forwarding

Suspicious Mailbox Rule

Disabling of Security Tools

Suspicious Compliance Search

Unusual eDiscovery Search

Suspicious eDiscovery Exfil

4:08pm

4:38pm

Compromised Identity prioritized by Vectra – **Urgency 100**

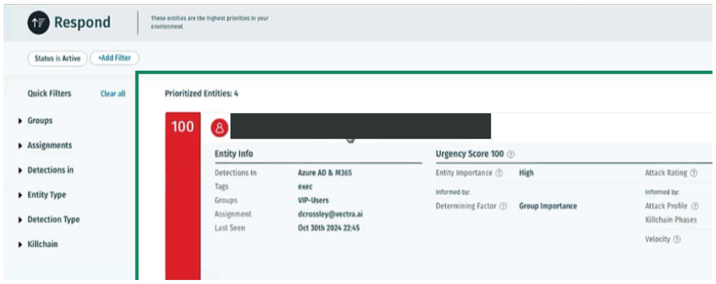
All detections fired within an hour from the start of the attack

- Defender XDR detected **1 technique** with low priority
- Vectra AI provided more assurance by detecting **11 techniques**, with AI prioritization and actionable insights
- Besides Scattered Spider, Vectra AI also covers attack techniques associated with: APT28, APT29, APT33, Ke3chang, LAPSUS$, Magic Hound, FIN4, Chimera, Fox Kitten, Kimsuky, Silent Librarian, C0027, SolarWinds Compromise, and unknown attackers

In a ransomware attack by Scattered Spider, Vectra AI finds 11x more attacker techniques than E5, with better clarity and less effort

VECTRA

Vectra AI prioritized incidents, connected the dots between attack surfaces, and provided detailed alert context:



Prioritized Entities: 4

[redacted]

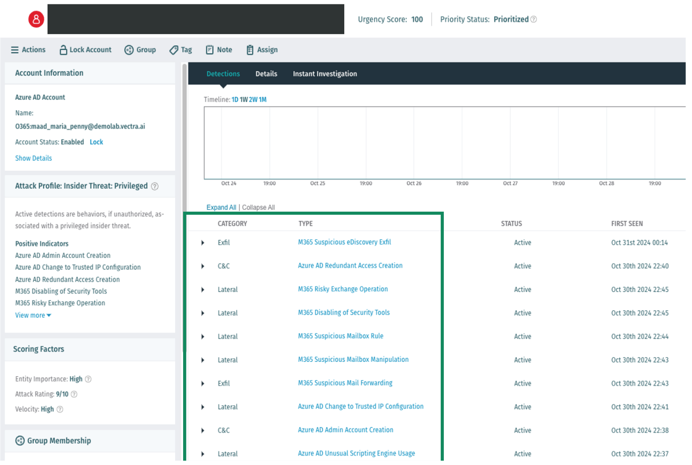
Entity Info

Detections In	Azure AD & M365
Tags	exec
Groups	VIP-Users
Assignment	dcrossley@vectra.ai
Last Seen	Oct 30th 2024 22:45

Urgency Score 100

Entity Importance: High
Informed by:
Determining Factor: Group Importance

Attack Rating
Informed by:
Attack Profile
Killchain Phases
Velocity



[redacted]

Urgency Score: 100 | Priority Status: Prioritized

Account Information

Azure AD Account
Name:
O365:maad_maria_penny@demolab.vectra.ai
Account Status: Enabled Lock
Show Details

Attack Profile: Insider Threat: Privileged

Active detections are behaviors, if unauthorized, associated with a privileged insider threat.

Positive Indicators
Azure AD Admin Account Creation
Azure AD Change to Trusted IP Configuration
Azure AD Redundant Access Creation
M365 Disabling of Security Tools
M365 Risky Exchange Operation
View more

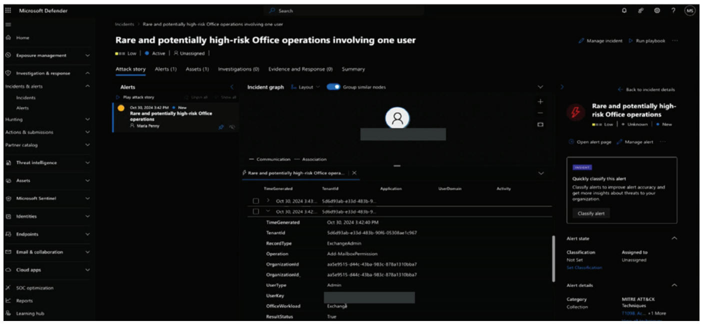
Scoring Factors

Entity Importance: High
Attack Rating: 9/10
Velocity: High

CATEGORY	TYPE	STATUS	FIRST SEEN
Exfil	M365 Suspicious eDiscovery Exfil	Active	Oct 31st 2024 00:14
C&C	Azure AD Redundant Access Creation	Active	Oct 30th 2024 22:40
Lateral	M365 Risky Exchange Operation	Active	Oct 30th 2024 22:45
Lateral	M365 Disabling of Security Tools	Active	Oct 30th 2024 22:45
Lateral	M365 Suspicious Mailbox Rule	Active	Oct 30th 2024 22:44
Lateral	M365 Suspicious Mailbox Manipulation	Active	Oct 30th 2024 22:43
Exfil	M365 Suspicious Mail Forwarding	Active	Oct 30th 2024 22:43
Lateral	Azure AD Change to Trusted IP Configuration	Active	Oct 30th 2024 22:41
C&C	Azure AD Admin Account Creation	Active	Oct 30th 2024 22:38
Lateral	Azure AD Unusual Scripting Engine Usage	Active	Oct 30th 2024 22:37

Microsoft

Microsoft generated one low severity alert with limited actionable insights on attacker behaviors before and after:



Incidents > Rare and potentially high-risk Office operations involving one user

Rare and potentially high-risk Office operations involving one user

Low | Active | Unassigned |

Oct 30, 2024 3:42 PM • New
Rare and potentially high-risk Office operations
Maria Penny

[redacted]

Rare and potentially high-risk Office opera...

TimeGenerated	TenantId	Application	UserDomain	Activity
Oct 30, 2024 3:43...	5d6d93ab-e33d-483b-9...			
Oct 30, 2024 3:42...	5d6d93ab-e33d-483b-9...			

TimeGenerated	Oct 30, 2024 3:42:40 PM
TenantId	5d6d93ab-e33d-483b-90f6-05308ae1c967
RecordType	ExchangeAdmin
Operation	Add-MailboxPermission
OrganizationId	aa5e9515-d44c-43ba-983c-878a1310bba7
OrganizationId_	aa5e9515-d44c-43ba-983c-878a1310bba7
UserType	Admin
UserKey	[redacted]
OfficeWorkload	Exchange
ResultStatus	True

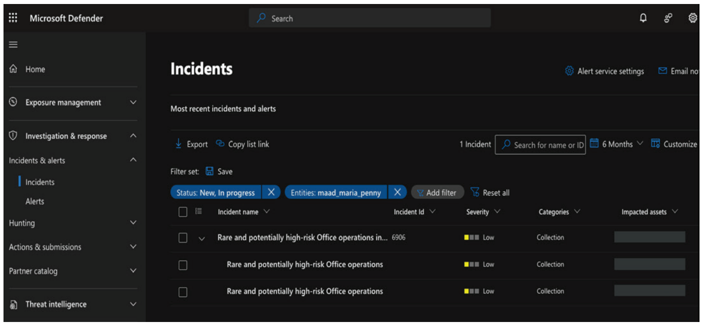
Rare and potentially high-risk Office operations

Low | Unknown | New

INSIGHT
Quickly classify this alert
Classify alerts to improve alert accuracy and get more insights about threats to your organization.

Alert state
Classification: Not Set
Set Classification
Assigned to: Unassigned

Alert details
Category: Collection
MITRE ATT&CK Techniques: T1098: Ac... +1 More



Incidents

Most recent incidents and alerts

1 Incident

Status: New, In progress | Entities: maad_maria_penny

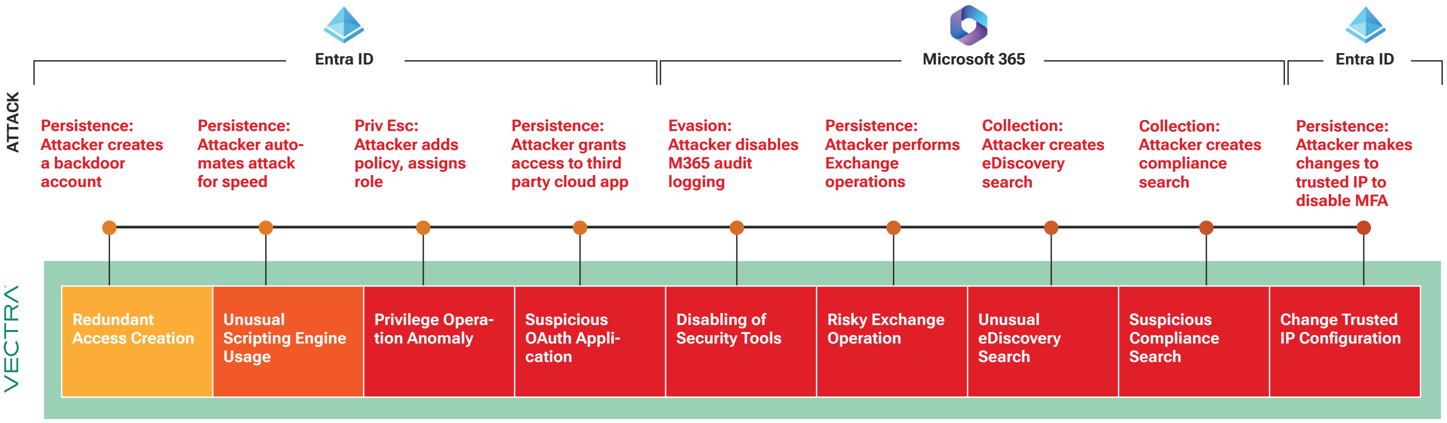
Incident name	Incident Id	Severity	Categories	Impacted assets
Rare and potentially high-risk Office operations in...	6906	Low	Collection	[redacted]
Rare and potentially high-risk Office operations		Low	Collection	[redacted]
Rare and potentially high-risk Office operations		Low	Collection	[redacted]

ATTACK SIMULATION RESULT #2:

Ransomware attack with Fortune 500 finance customer

In a ransomware attack simulation with a Fortune 500 customer, Vectra AI finds 9 attacker techniques that E5 missed

Scattered Spider compromised a user and gained legitimate access to the account



Entra ID

ATTACK	VECTRA
Persistence: Attacker creates a backdoor account	Redundant Access Creation
Persistence: Attacker automates attack for speed	Unusual Scripting Engine Usage
Priv Esc: Attacker adds policy, assigns role	Privilege Operation Anomaly
Persistence: Attacker grants access to third party cloud app	Suspicious OAuth Application

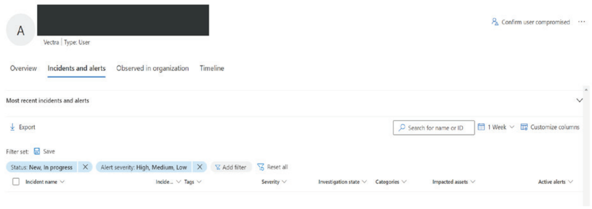
Microsoft 365

ATTACK	VECTRA
Evasion: Attacker disables M365 audit logging	Disabling of Security Tools
Persistence: Attacker performs Exchange operations	Risky Exchange Operation
Collection: Attacker creates eDiscovery search	Unusual eDiscovery Search
Collection: Attacker creates compliance search	Suspicious Compliance Search

Entra ID

ATTACK	VECTRA
Persistence: Attacker makes changes to trusted IP to disable MFA	Change Trusted IP Configuration

Microsoft 0 DETECTIONS (Fully deployed E5 environment)



A [redacted]
Vectra | Type: User

Confirm user compromised ···

Overview | Incidents and alerts | Observed in organization | Timeline

Most recent incidents and alerts

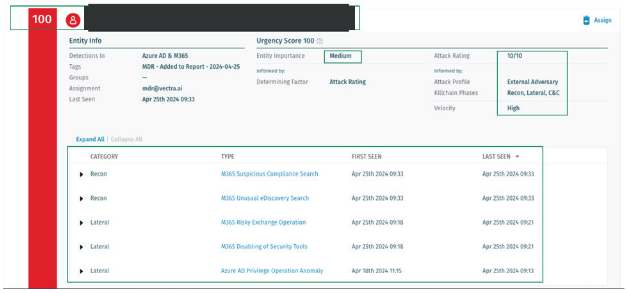
Export | Search for name or ID | 1 Week | Customize columns

Filter set: Save

Status: New, In progress ✕ | Alert severity: High, Medium, Low ✕ | Add filter | Reset all

□ Incident name	Incide...	Tags	Severity	Investigation state	Categories	Impacted assets	Active alerts

VECTRA 9 DETECTIONS



100 [redacted]

Assign

Entity Info

Detections In	Azure AD & M365
Tags	MDR - Added to Report - 2024-04-25
Groups	—
Assignment	mdr@vectra.ai
Last Seen	Apr 25th 2024 09:33

Urgency Score 100

Entity Importance	Medium
Informed by:	
Determining Factor	Attack Rating

Attack Rating	10/10
Informed by:	
Attack Profile	External Adversary
Killchain Phases	Recon, Lateral, C&C
Velocity	High

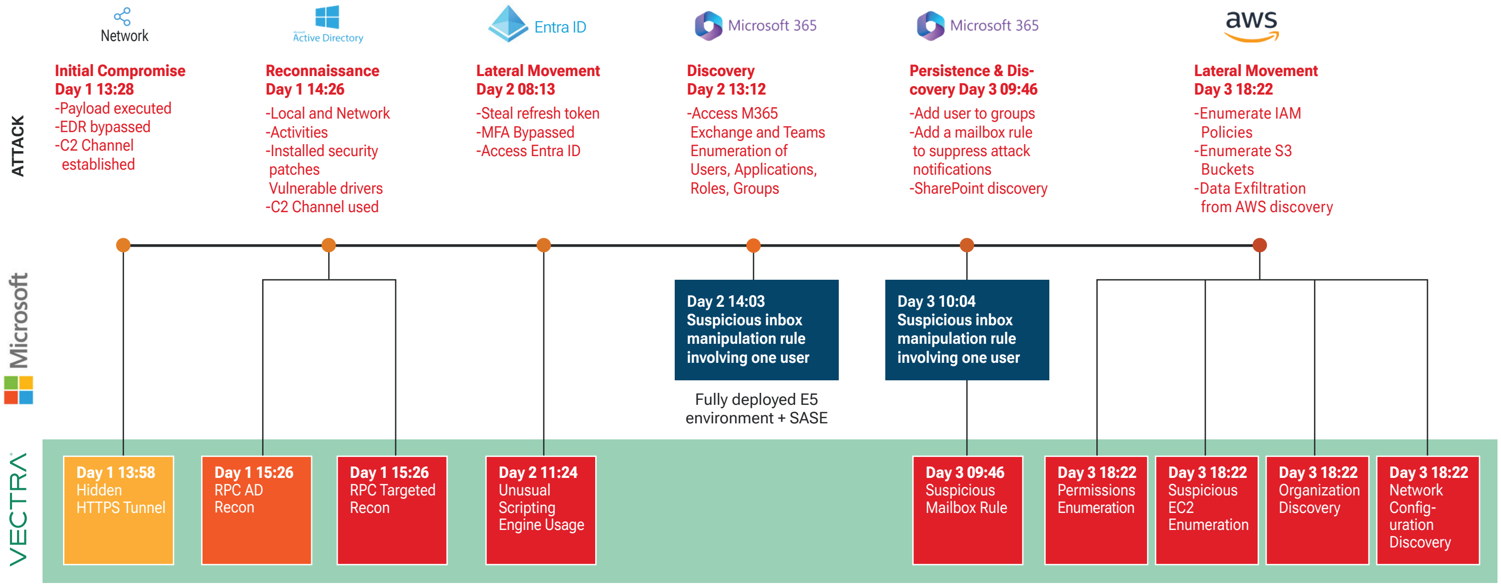
Expand All | Collapse All

CATEGORY	TYPE	FIRST SEEN	LAST SEEN
Recon	M365 Suspicious Compliance Search	Apr 25th 2024 09:33	Apr 25th 2024 09:33
Recon	M365 Unusual eDiscovery Search	Apr 25th 2024 09:33	Apr 25th 2024 09:33
Lateral	M365 Risky Exchange Operation	Apr 25th 2024 09:18	Apr 25th 2024 09:21
Lateral	M365 Disabling of Security Tools	Apr 25th 2024 09:18	Apr 25th 2024 09:21
Lateral	Azure AD Privilege Operation Anomaly	Apr 18th 2024 11:15	Apr 25th 2024 09:13

ATTACK SIMULATION RESULT #3:

Network to cloud attack with large insurance group

In a network-to-cloud offensive security assessment at a large insurance group, Vectra AI extended E5 visibility to find attacker techniques across 5 domains



ATTACK

Network

Initial Compromise
Day 1 13:28
-Payload executed
-EDR bypassed
-C2 Channel established

Active Directory

Reconnaissance
Day 1 14:26
-Local and Network
-Activities
-Installed security patches
Vulnerable drivers
-C2 Channel used

Entra ID

Lateral Movement
Day 2 08:13
-Steal refresh token
-MFA Bypassed
-Access Entra ID

Microsoft 365

Discovery
Day 2 13:12
-Access M365 Exchange and Teams Enumeration of Users, Applications, Roles, Groups

Microsoft 365

Persistence & Discovery Day 3 09:46
-Add user to groups
-Add a mailbox rule to suppress attack notifications
-SharePoint discovery

aws

Lateral Movement
Day 3 18:22
-Enumerate IAM Policies
-Enumerate S3 Buckets
-Data Exfiltration from AWS discovery

Microsoft

Day 2 14:03
Suspicious inbox manipulation rule involving one user

Fully deployed E5 environment + SASE

Day 3 10:04
Suspicious inbox manipulation rule involving one user

VECTRA

Day 1 13:58
Hidden HTTPS Tunnel

Day 1 15:26
RPC AD Recon

Day 1 15:26
RPC Targeted Recon

Day 2 11:24
Unusual Scripting Engine Usage

Day 3 09:46
Suspicious Mailbox Rule

Day 3 18:22
Permissions Enumeration

Day 3 18:22
Suspicious EC2 Enumeration

Day 3 18:22
Organization Discovery

Day 3 18:22
Network Configuration Discovery

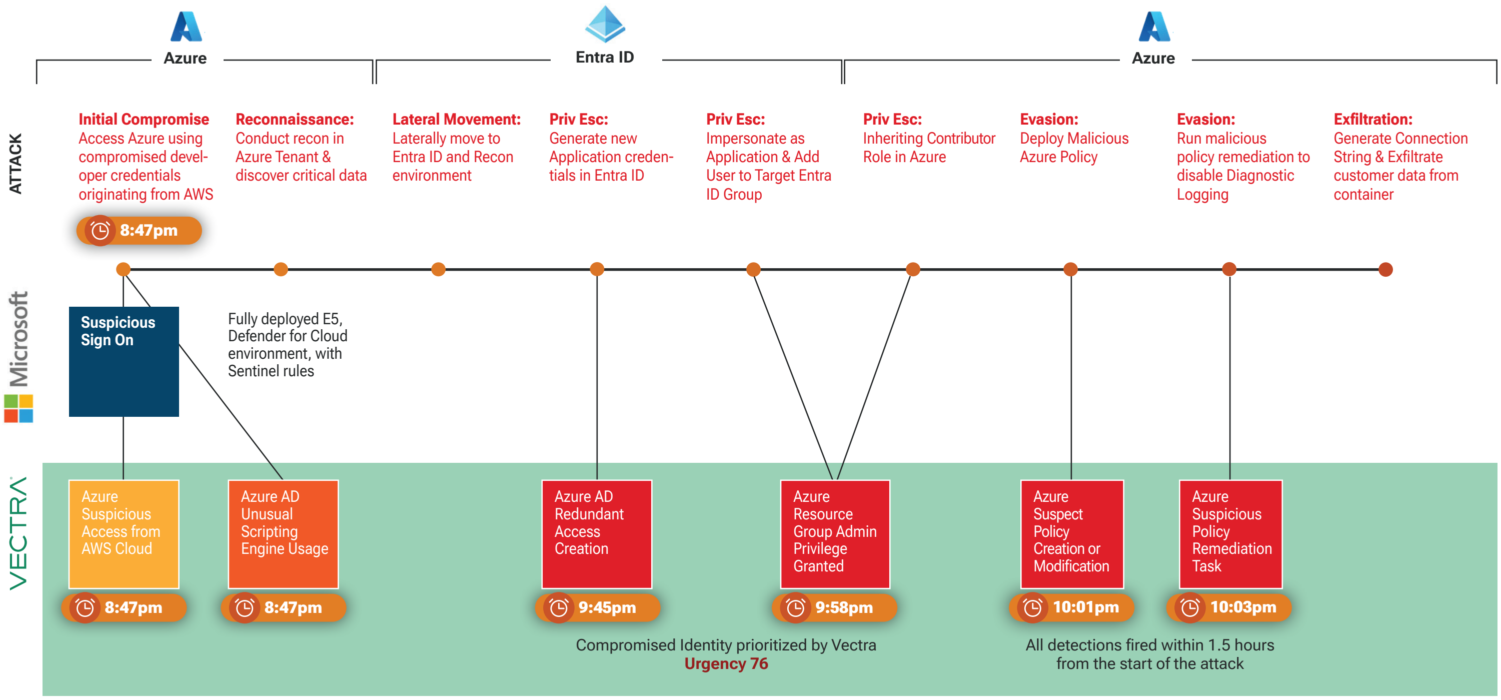
- Defender XDR identified **2 techniques** with low priorities
- Vectra prioritized the attack with **9 techniques** detected across **5 domains**
- Initial Vectra AI detection within 30 minutes of initial compromise, 24 hours before initial Microsoft Detection

ATTACK SIMULATION RESULT #4:

Multi-Cloud Attack Targeting Azure and Entra ID - Large global fintech

Vectra AI extends value of E5 by finding 5 additional attacker technique

Attacker compromised an Azure identity and gained legitimate access to the organization



Initial Compromise Access Azure using compromised developer credentials originating from AWS — 8:47pm

Reconnaissance: Conduct recon in Azure Tenant & discover critical data

Lateral Movement: Laterally move to Entra ID and Recon environment

Priv Esc: Generate new Application credentials in Entra ID

Priv Esc: Impersonate as Application & Add User to Target Entra ID Group

Priv Esc: Inheriting Contributor Role in Azure

Evasion: Deploy Malicious Azure Policy

Evasion: Run malicious policy remediation to disable Diagnostic Logging

Exfiltration: Generate Connection String & Exfiltrate customer data from container

Suspicious Sign On

Fully deployed E5, Defender for Cloud environment, with Sentinel rules

Azure Suspicious Access from AWS Cloud — 8:47pm

Azure AD Unusual Scripting Engine Usage — 8:47pm

Azure AD Redundant Access Creation — 9:45pm

Azure Resource Group Admin Privilege Granted — 9:58pm

Azure Suspect Policy Creation or Modification — 10:01pm

Azure Suspicious Policy Remediation Task — 10:03pm

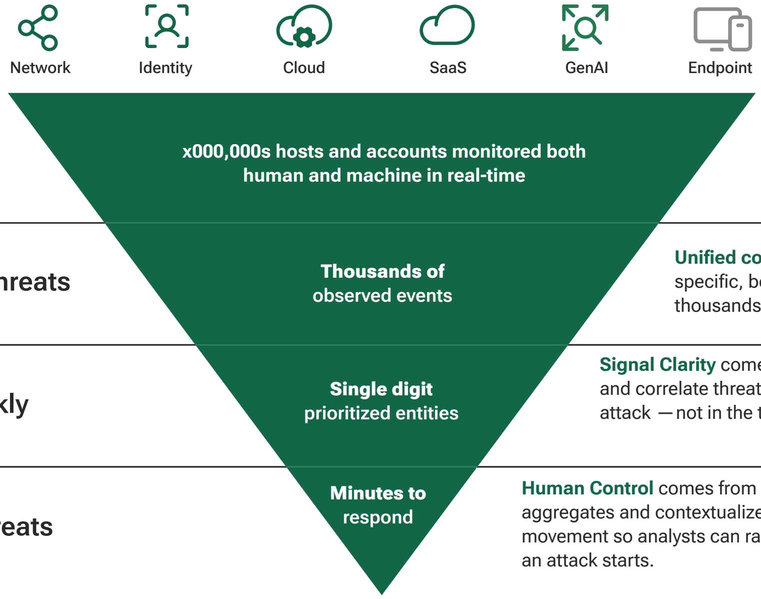
Compromised Identity prioritized by Vectra **Urgency 76**

All detections fired within 1.5 hours from the start of the attack

- Defender XDR identified **1 technique** but **suspicious sign on can be evaded by attacker** (e.g. using VPN to log in from same country)
- Vectra prioritized the attack with **6 techniques** detected, **connecting the dots** across Azure and Entra ID

How Vectra AI reinforce hybrid / multi-cloud security

Attack Signal Intelligence – AI to find and stop attackers. Our approach delivers the most accurate attack signal intelligence for the SOC.



Network Identity Cloud SaaS GenAI Endpoint

x000,000s hosts and accounts monitored both human and machine in real-time

We integrate visibility to hundreds of thousands of hosts and accounts—both human and machine—across network, identity, cloud, M365, Copilot with endpoint and email on the roadmap.

1. **Coverage** to find threats

Thousands of observed events

Unified coverage comes from our pre-built, domain specific, behavior-based AI detections – observing thousands of potential threat events.

2. **Clarity** to act quickly

Single digit prioritized entities

Signal Clarity comes from our ability to automatically triage and correlate threat events to prioritize and alert on entities under attack —not in the thousands, but in the single digits per day.

3. **Control** to stop threats

Minutes to respond

Human Control comes from our Instant investigations that automatically aggregates and contextualizes hybrid-attacker progression and lateral movement so analysts can rapidly and confidently respond minutes after an attack starts.

1. Coverage to find threats

VECTRA AI'S 170+ ADVANCED MACHINE LEARNING MODELS ACROSS NETWORK IDENTITY AND CLOUD CONTINUOUSLY LEARN AND ADAPT TO EVER-EVOLVING ATTACKER BEHAVIORS

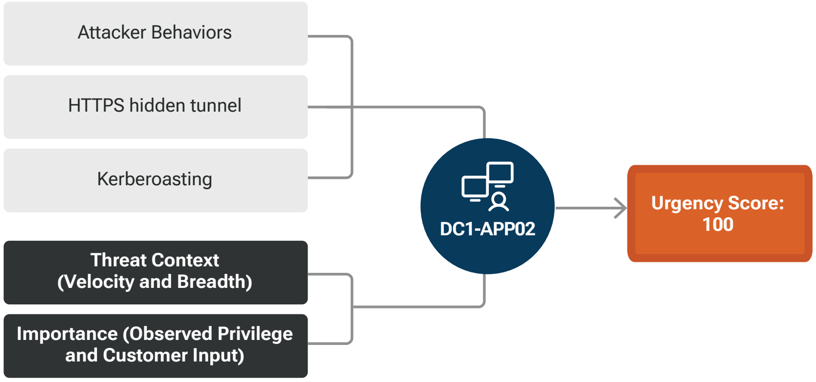
Access	Persist	Command & Control	Escalate & Evade	Recon & Discover	Lateral Movement	Exfiltration & disruption
New host	MFA disabled	Hidden HTTPS tunnel	New host	Kerberoasting (x4)	Privilege access anomaly (x6)	Smash and grab
Suspected compromise access	Trusted IP change	Hidden DNS tunnel	Log disabling attempt	Internal darknet scan	Suspected remote exec	Ransomware file activity
Brute-force attempt / success	Admin account creation	Hidden HTTP tunnel	Disabling security tools	Port scan	Suspicious remote desktop	Data gathering
Disabled account	Account manipulation	Hidden ICMP tunnel	Suspicious mailbox rule	Port sweep	Suspicious admin	Data smuggler
TOR Activity	Redundant access	Multi-homed fronted tunnel	Log disabling attempt	SMB account scan	Shell knocker	Hidden tunnel exfill (x4)
Unusual scripting engine	Device/factor registration	Suspicious relay	Suspect privilege operation	Kerberos account scan	Automated replication	Botnet abuse
Suspicious OAuthApp	Logging disabled	Suspect domain activity	Suspect privilege manipulate	Kerberos brute-sweep	Brute-force	Crypto mining
Suspicious sign-on	User hijacking	Malware update	Suspect console pivot	File share enumeration	SMB Brute force	External teams access
Suspicious sign-on with MFA fail	ECS hijacking	Peer-to-peer	Suspect cred access EC2	Suspicious LDAP query	Kerberos brute force	Ransomware SharePoint activity
Suspicious teams app	Suspect login profile manipulation	Suspicious HTTP	Suspect cred access SSM	RDP Recon	SQL injection activity	Suspicious SharePoint download
Suspicious copilot access	Security tools disabled	Stealth HTTP post	Suspect cred access ECS	RPC recon	Internal stage loader	Suspicious SharePoint sharing
Suspicious CSP access	SSM hijacking	TOR activity	Suspect cred access Lambda	RPC targeted recon	Suspicious active directory	Exfil before termination
Suspicious credential usage	Suspect policy manipulation	Novel external port	Diagnostic logging disabled	Unusual eDiscovery search	NovelAdmin protocol	Suspicious mailbox forwarding
Root credential usage	Suspicious app service action	Threat intel match	Subscription admin abuse (x4)	Unusual compliance search	NovelAdmin share access	eDiscovery Exfil
TOR activity	Managed identity abuse	Vectra threat intel match	TVM/ARC DSC execution	Suspect eDiscovery activity	ICMP internal tunnel	Power automate activity (x3)
Suspicious CSP access	Suspicious policy (x3)		Suspect key vault privilege granted	User permission enumeration	Risky exchange op	Ransomware S3 activity
TOR activity	Suspect app service (x3)		Privilege anomaly: root scope	EC2 enumeration	Internal spear phishing	Suspect public S3 charge
	Anonymous app service webjob		Privilege anomaly: Management group scope	S3 enumeration	File poisoning	Suspect public EBS charge
			Suspicious VM serial console usage	Suspect escalation recon	Mailbox manipulation	Suspect public EC2 charge
				Organization discovery	DLL hijacking	Suspect public RDS charge
				Suspicious Copilot access	Privilege operations anomaly	Suspect external access grant
				Azure credential dump	Suspicious runbook usage (x2)	Suspicious disk download
				Suspect key vault cred dump	Suspicious RunCommand execution (x3)	Cryptomining
				Suspect key vault enumeration	Suspicious extension (x3)	Suspect public change (x2)
						Suspect mass resource delete

🟩 Data center network & identity, IaaS, IoT/OT
🟦 Identity:Azure AD (Entra ID)
🟧 SAAS: Microsoft 365
🟪 GenAir:Copilot for M365
🟦 PaaS: AWS
🟩 PaaS: Azure

Vectra provides coverage for what attacks do before and after the sign-in, with visibility into living-off-the-land tactics that allow teams to stop attackers before damage.

2. Clarity to act quickly

AI PRIORITIZATION AND CORRELATION CONNECT THE DOTS AND FIND WHAT'S URGENT


Attacker Behaviors
HTTPS hidden tunnel
Kerberoasting
Threat Context (Velocity and Breadth)
Importance (Observed Privilege and Customer Input)
DC1-APP02
Urgency Score: 100

CONNECTING THE DOTS::

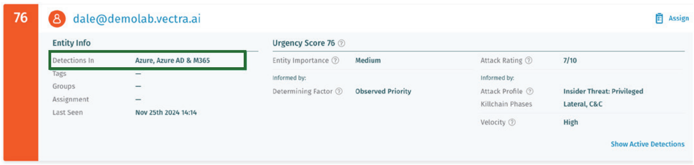
Scores based on behavior and context

Considers and learns what's important

Connects activity **across domains**

Automatically resolves benign activity

CONNECTS ACTIVITY ACROSS DOMAINS



76 dale@demolab.vectra.ai Assign

Entity Info

Detections In	Azure, Azure AD & M365
Tags	—
Groups	—
Assignment	—
Last Seen	Nov 25th 2024 14:14

Urgency Score 76

Entity Importance: Medium

Informed by:

Determining Factor: Observed Priority

Attack Rating: 7/10

Informed by:

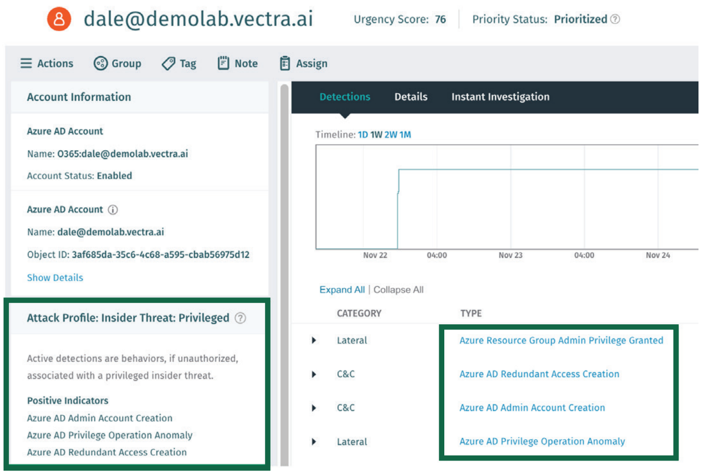
Attack Profile: Insider Threat: Privileged

Killchain Phases: Lateral, C&C

Velocity: High

Show Active Detections

PROVIDES CONTEXT ON ATTACKER BEHAVIORS



dale@demolab.vectra.ai Urgency Score: 76 | Priority Status: Prioritized

Account Information

Azure AD Account

Name: O365:dale@demolab.vectra.ai

Account Status: Enabled

Azure AD Account

Name: dale@demolab.vectra.ai

Object ID: 3af685da-35c6-4c68-a595-cbab56975d12

Show Details

Attack Profile: Insider Threat: Privileged

Active detections are behaviors, if unauthorized, associated with a privileged insider threat.

Positive Indicators

Azure AD Admin Account Creation

Azure AD Privilege Operation Anomaly

Azure AD Redundant Access Creation

Timeline: 1D 1W 2W 1M

Expand All | Collapse All

CATEGORY	TYPE
Lateral	Azure Resource Group Admin Privilege Granted
C&C	Azure AD Redundant Access Creation
C&C	Azure AD Admin Account Creation
Lateral	Azure AD Privilege Operation Anomaly

3. Control to stop threats

Active posture monitoring

Vectra AI enables teams to shift left by identifying security gaps across networks, identities, cloud services, and GenAI tools like Microsoft Copilot for M365. We actively monitor over 20 AI-enhanced data streams and hundreds of attributes to find how attackers could bypass control in your environment in a future attack with the context to reduce your attack surface.

Accelerated investigations and intuitive threat hunting

Vectra AI instantly delivers answers to analysts' top questions from metadata across network, cloud, and identity in every case — without the need to write a single query. When deeper investigation is required, teams have access to all 20 data streams with integrated context, accelerating the path to identifying threats.

Comprehensive response capabilities

Vectra AI's native integrations with EDR, AD and Entra ID allow security analysts to manually or automatically take the right action at the right time to stop an attacker wherever they are in the environment.

Integration with Microsoft Sentinel

Vectra AI natively integrates with Microsoft Sentinel, enhancing existing workflows, removing the need to manage custom analytics while maximizing time.

MXDR to alleviate operational burden

Vectra's 24/7 MXDR hybrid attack experts alleviate your operational burden in threat detection and response.

Uncover your gaps in Microsoft environments: Offensive security test

Here are three tools / services that allow your team to uncover gaps across your Microsoft environment:

1

Uncover network / network-to-cloud gaps

Vectra's Offensive Security Service uses certified experts and trusted tools like Cobalt Strike and Outflank to deliver seamless, controlled assessments. The team validates attack signals, identifies vulnerabilities, and provides actionable insights to address network or network-to-cloud security gaps, enabling informed decision-making.

2

Uncover identity gaps

MAAD-AF is an open-source tool for testing Microsoft 365 and Entra ID security through adversary emulation. It helps security teams replicate attacker tactics, and identify gaps in existing identity detection and response capabilities.

3

Uncover cloud gaps

Halberd, a free open-source multi-cloud security testing tool, helps security teams test their defenses against attack techniques across Microsoft 365, Microsoft Entra ID (formerly Azure AD), Microsoft Azure and AWS—all in one platform through adversary emulation.

Schedule an Offensive Security Test with Vectra AI

See Vectra AI in Action

About Vectra AI

Vectra AI, Inc. is the cybersecurity AI company that stops attacks others can't. The Vectra AI Platform delivers integrated signal across public cloud, SaaS, identity, and data center networks in a single platform. Vectra AI's patented Attack Signal Intelligence empowers security teams to rapidly detect, prioritize, investigate and stop the most advanced hybrid cyber-attacks. With 35 patents in AI-driven detection and the most vendor references in 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.