VECTRA

Vectra AI Coverage

Challenge: Modern networks, modern attacks

Modern Networks are hybrid, complex, and always changing and so are modern attacks

- Identities sprawling both new and old, network and cloud-based
- Accounts logging on and off both human and machine
- People moving to and from corporate offices, campuses to home offices and remote locations
- Workloads moving to and from on-premises to cloud
- Devices showing up on the network both managed and unmanaged, with agents and without
- Applications sanctioned and unsanctioned interacting with people, devices, APIs, data.
- Data constantly moving to and from and in-between data centers, clouds, devices

Protecting modern networks from modern attacks is challenging:

Attack Surface is Expanding

The days of the network being narrowly defined as on-premises data centers and campuses are long over. Today, the network is a highly complex, interconnected web spanning data centers, campuses, remote workers, clouds, identities, and IoT/OT.

Attackers don't Operate in Siloes

A modern attack is a dynamic, multi-phase intrusion targeting an expansive multi-domain attack surface. Modern attackers are savvy, stealthy, adaptive, innovative and fast – embracing AI and automation to be more efficient and effective at their job.

Attackers Bypass Legacy Controls

Relying heavily or solely on traditional protection and controls is not enough to stop today's modern attackers.

Vectra AI Detection Coverage for the modern network.

Vectra AI reduces attack exposure with native coverage integrated across:

Network

Shore up defenses with Vectra AI Detections for Network and close intrusion and endpoint detection gaps.

Vectra AI Detections for Network surface attackers in your infrastructure moving laterally both east-west and north-south across data centers, campuses, remote work, cloud and OT environments.

Key Differentiators:

- Detection without decryption: Unlike other tools that introduce operational burden, latency, and risk by needing to decrypt to detect, we see through encryption to detect threats.
- Advanced C2 Coverage: AI Detections for the most advanced attacker methods of establishing command and control (C2) early in the cyber kill chain.
- Signature and threat intel ingestion: Ingest signatures and threat intel feeds to make your attack signal stronger, and threat hunting and investigations faster.

Identity

Strengthen defenses with Vectra AI Detections for Identity and know when attackers compromise accounts, abuse privilege.

Vectra AI Detections for Identity surface attackers compromising and escalating privileges for both human and machine accounts across Active Directory, Microsoft Entra ID, Microsoft 365, AWS and Azure.

Key Differentiators:

- Privilege Access Analytics (PAA). Our patented graph-based AI algorithm monitors interactions between accounts, services and hosts to detect attacker abuse of privileges.
- Entity Attribution. We attribute detections to hosts, devices, and accounts — human and machine — saving a ton of manual work and tool pivoting for analysts.
- Native Tool Reinforcement. Real-time detection of living-off-the-land and zero-day attack techniques, covering every stage of the attack.

Cloud

Fortify defenses with Vectra AI Detections for Cloud and detect attacker behaviors other tools can't.

Vectra AI Detections for Cloud surface multi-cloud attacks spanning your AWS, Microsoft Azure, Microsoft 365, and Microsoft Copilot for M365 environments.

Key Differentiators:

- Multi-cloud coverage. AI detections across all stages of an attack for AWS, Microsoft Azure, Microsoft 365, and Microsoft Copilot for M365.
- Native Tool Reinforcement. Over 100 AI detections for Microsoft environments and over 40 AI detections for AWS.
- Entity Attribution. Our cloud attribution technology leverages AI/ML to analyze over a dozen artifacts to confidently attribute attacks to a specific entity.

Vectra AI for Network Coverage

Data Center: Detects misuse of command and control by detecting hidden tunnels (e.g. Hidden HTTP, Hidden HTTPs, Hidden DNS, SQL injection attempts, Suspect Domain Activity (SPA), and more.

Campus: Detects against modern network attackers that bypass existing permitter controls e.g. EDR, SIEM, SOAR, IDS/IPS, PCAP, CWPP, Firewalls, and more.

OT: Detects attacks targeting critical infrastructure and resources through compromised IT, Internet Connected OT assets, and/or compromised 3rd party technician equipment with malware, known IoC's (Surricata) and more.

Remote Work: Detects misuse of network traffic from both North-South and East-West for more effective network security posture.

Cloud Networks: Detects attacks utilizing lift-and-shift methods from On-Premises to IaaS (Amazon Web Services-AWS, Microsoft Azure, and Google Cloud Platform - GCP) and vice versa.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
Privilege Anomaly: Unusual Account on Host	Suspicious Active Directory Operations	Privilege Anomaly: Unusual Account on Host	Privilege Anomaly: Unusual Account on Host	Privilege Anomaly: Unusual Account on Host	Brute-Force	External Remote Access	Automated Replication	Data Gathering	External Remote Access	Data Smuggler	Cryptocurrency Mining
Privilege Anomaly: Unusual Host	Vectra Threat Intelligence Match	Privilege Anomaly: Unusual Host	Privilege Anomaly: Unusual Host	Privilege Anomaly: Unusual Host	Kerberoasting: SPN Sweep	File Share Enumeration	Internal Darknet Scan	Data Smuggler	Hidden DNS Tunnel	Malware Update	Outbound DoS
Privilege Anomaly: Unusual Service		Privilege Anomaly: Unusual Service	Privilege Anomaly: Unusual Service	Privilege Anomaly: Unusual Service	Kerberoasting: Targeted Weak Cipher Response	Hidden DNS Tunnel	Stage Loader	External Remote Access	Hidden HTTP Tunnel	Smash and Grab	Ransomware File Activity
Privilege Anomaly: Unusual Service - Insider		Privilege Anomaly: Unusual Service - Insider	Privilege Anomaly: Unusual Service - Insider	Privilege Anomaly: Unusual Service - Insider	Kerberoasting: Weak Cipher Request	Hidden HTTP Tunnel	Suspicious Admin	File Share Enumeration	Hidden HTTPS Tunnel	Vectra Threat Intelligence Match	
Privilege Anomaly: Unusual Service from Host		Privilege Anomaly: Unusual Service from Host	Privilege Anomaly: Unusual Service from Host	Privilege Anomaly: Unusual Service from Host	Kerberos Account Scan	Hidden HTTPS Tunnel	Suspicious Port Scan	Hidden DNS Tunnel	ICMP Tunnel		
Privilege Anomaly: Unusual Trio		Privilege Anomaly: Unusual Trio	Privilege Anomaly: Unusual Trio	Privilege Anomaly: Unusual Trio	Kerberos Brute-Sweep	Internal Darknet Scan	Suspicious Port Sweep	Hidden HTTP Tunnel	ICMP Tunnel: Client		
SQL Injection Activity		Shell Knocker Client	Suspicious Active Directory Operations	Shell Knocker Client	Outbound Port Sweep	Kerberoasting: SPN Sweep	Suspicious Remote Desktop Protocol	Hidden HTTPS Tunnel	ICMP Tunnel: Server		
Shell Knocker Server		Shell Knocker Server	Suspicious Admin	Shell Knocker Server	Privilege Anomaly: Unusual Account on Host	Kerberoasting: Weak Cipher Request	Suspicious Remote Execution	Multi-home Fronted Tunnel	Malware Update		
Suspicious Active Directory Operations		Suspicious Active Directory Operations	Suspicious Remote Desktop Protocol	Suspicious Active Directory Operations	Privilege Anomaly: Unusual Host	Kerberos Account Scan		Smash and Grab	Multi-home Fronted Tunnel		
Suspicious Admin		Suspicious Admin	Suspicious Remote Execution	Suspicious Admin	Privilege Anomaly: Unusual Service	Kerberos Brute-Sweep			Peer-To-Peer		
Suspicious Remote Desktop Protocol		Suspicious Remote Desktop Protocol		Suspicious Remote Desktop Protocol	Privilege Anomaly: Unusual Service - Insider	Multi-home Fronted Tunnel			Shell Knocker Client		
Suspicious Remote Execution		Suspicious Remote Execution		Suspicious Remote Execution	Privilege Anomaly: Unusual Service from Host	Outbound Port Sweep			Shell Knocker Server		
					Privilege Anomaly: Unusual Trio	Privilege Anomaly: Unusual Account on Host			Stealth HTTP Post		
					SMB Brute-Force	Privilege Anomaly: Unusual Host			Suspect DNS Activity		
					Suspicious Admin	Privilege Anomaly: Unusual Service			Suspect Domain Activity		
					Suspicious Remote Desktop Protocol	Privilege Anomaly: Unusual Service - Insider			Suspect HTTP Activity		
					Suspicious Remote Execution	Privilege Anomaly: Unusual Service from Host			Suspect HTTPS Activity		
						Privilege Anomaly: Unusual Trio			Suspect TCP Activity		
						RDP Recon			Suspicious Active Directory Operations		
						RPC Recon			Suspicious HTTP		
						RPC Targeted Recon			Suspicious Relay		
						SMB Account Scan			TOR Activity		
						SMB Brute-Force			Vectra Threat Intelligence Match		
						Suspicious Active Directory Operations					
						Suspicious LDAP Query					
						Suspicious Port Scan					
						Suspicious Port Sweep					

Vectra AI for Cloud Coverage

AWS: Detect attacks threatening control plane and resources, such as S3, EC2, Lambdas and more.

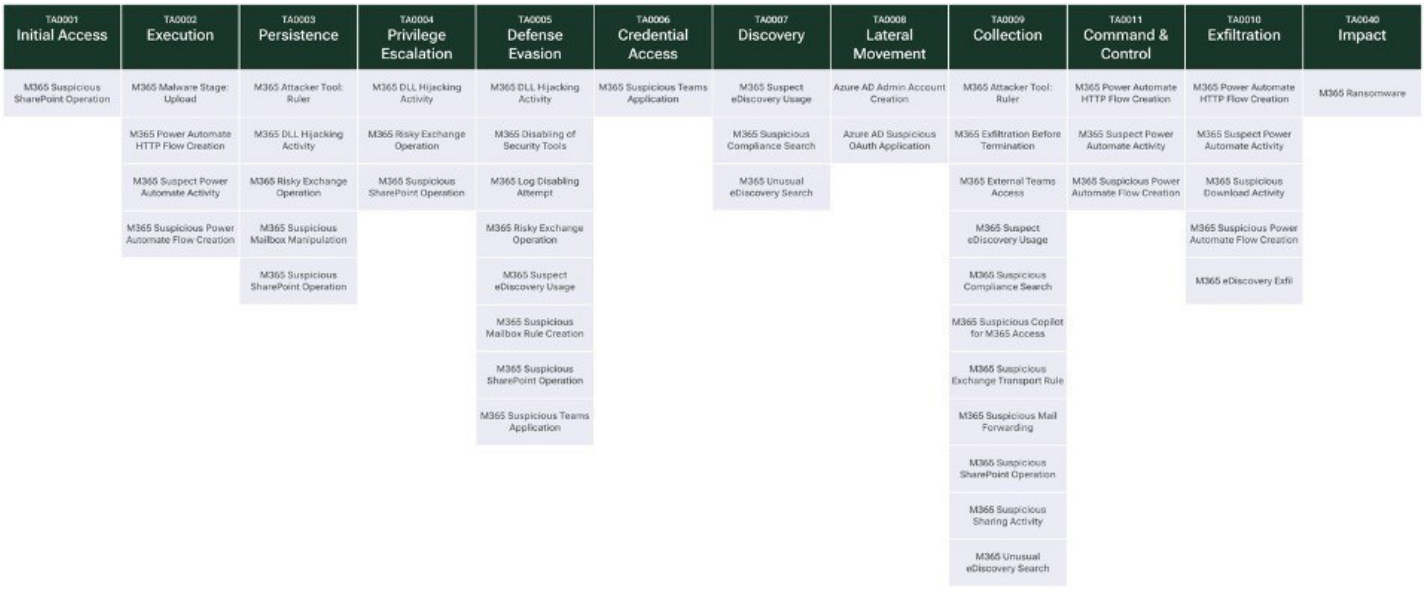
TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
AWS Root Credential Usage		AWS ECR Hijacking	AWS Root Credential Usage	AWS Logging Disabled	AWS Suspect Credential Access from EC2	AWS Network Configuration Discovery		AWS Suspect Public EBS Change	AWS TOR Activity	AWS Suspect Public AMI Change	AWS Cryptomining
AWS Suspect Admin Privilege Granting		AWS Lambda Hijacking	AWS Suspect Admin Privilege Granting	AWS Root Credential Usage	AWS Suspect Credential Access from ECS	AWS Organization Discovery		AWS Suspect Public EC2 Change		AWS Suspect Public EBS Change	AWS Ransomware S3 Activity
AWS Suspect External Access Granting		AWS Root Credential Usage	AWS Suspect External Access Granting	AWS Security Tools Disabled	AWS Suspect Credential Access from SSM	AWS S3 Enumeration		AWS Suspect Public S3 Change		AWS Suspect Public EC2 Change	
AWS Suspicious Credential Usage		AWS Suspect Admin Privilege Granting	AWS Suspicious Credential Usage	AWS Suspect Admin Privilege Granting	AWS Suspect Discovery From EC2 Instance	AWS Suspect Console Pivot				AWS Suspect Public RDS Change	
		AWS Suspect External Access Granting		AWS Suspect External Access Granting	AWS Suspect Traffic Mirror Creation	AWS Suspect Discovery From EC2 Instance				AWS Suspect Public S3 Change	
		AWS Suspect Login Profile Manipulation		AWS Suspect Organization Exit		AWS Suspect Escalation Reconnaissance					
		AWS Suspect Privilege Escalation		AWS Suspect Public EC2 Change		AWS Suspect Traffic Mirror Creation					
		AWS Suspect Region Activity		AWS Suspicious Credential Usage		AWS Suspicious EC2 Enumeration					
		AWS Suspicious Credential Usage				AWS User Permissions Enumeration					
		AWS User Hijacking									

Microsoft Azure: Detect Azure attacks, providing hybrid visibility into critical infrastructure, control plane and resources, such as policies, App Service, automation accounts, and more.

TA0043 Recon	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
Azure Suspect Key Vault Enumeration	Azure Suspicious Access from AWS Cloud	Azure Suspicious Automation DSC Execution	Azure Anomalous App Service WebJob Activity	Azure Anomalous App Service WebJob Activity	Azure Anomalous App Service WebJob Activity	Azure Suspect Credential Dump		Azure Managed Identity Anomaly	Azure Suspect Public Storage Account Change	Azure Suspicious Automation DSC Execution	Azure Suspicious Disk Download	Azure Cryptomining
	Azure Suspicious Access from GCP Cloud	Azure Suspicious Hybrid Machine Extension Installation	Azure Privilege Anomaly: Management Group Scope	Azure Privilege Anomaly: Management Group Scope	Azure Diagnostic Logging Disabled	Azure Suspicious App Service Credential Download		Azure Suspicious Automation Staged	Azure Suspicious Disk Download	Azure Suspicious Automation Staged		Azure Mass Resource Deletion
		Azure Suspicious Hybrid Machine Run Command Execution	Azure Privilege Anomaly: Root Scope	Azure Privilege Anomaly: Root Scope	Azure Mass Resource Deletion	Azure Suspicious App Service Deployment Configuration Download		Azure Suspicious Hybrid Automation Execution		Azure Suspicious Hybrid Automation Test		Azure Resource Group Admin Role Unassigned
		Azure Suspicious Policy Creation or Modification	Azure Resource Group Admin Privilege Granting	Azure Resource Group Admin Privilege Granting	Azure Privilege Anomaly: Management Group Scope	Azure Suspicious Key Vault Extraction		Azure Suspicious VM Automation Execution		Azure Suspicious VM Automation Test		Azure Subscription Admin Role Unassigned
		Azure Suspicious Policy Remediation Task	Azure Subscription Admin Privilege Granting	Azure Subscription Admin Privilege Granting	Azure Privilege Anomaly: Root Scope					Azure TOR Activity		
		Azure Suspicious Serial Console Usage	Azure Suspect App Service Deployment Activity	Azure Suspect App Service Deployment Activity	Azure Resource Group Admin Privilege Granting							
		Azure Suspicious VM Extension Installation	Azure Suspect Key Vault Privilege Granting	Azure Suspect Key Vault Privilege Granting	Azure Subscription Admin Privilege Granting							
		Azure Suspicious VM Run Command Execution	Azure Suspicious Access from AWS Cloud	Azure Suspicious Access from AWS Cloud	Azure Suspect App Service Deployment Activity							
		Azure Suspicious VM Scale Set Extension Installation	Azure Suspicious Access from GCP Cloud	Azure Suspicious Access from GCP Cloud	Azure Suspect Key Vault Privilege Granting							
		Azure Suspicious VM Scale Set Run Command Execution	Azure Suspicious App Service Creation or Modification	Azure Suspicious App Service Creation or Modification	Azure Suspect Public Storage Account Change							
			Azure Suspicious Automation DSC Execution	Azure Suspicious Hybrid Machine Extension Installation	Azure Suspicious Access from AWS Cloud							
			Azure Suspicious Automation Staged	Azure Suspicious Policy Assignment	Azure Suspicious Access from GCP Cloud							
			Azure Suspicious Hybrid Automation Test	Azure Suspicious Policy Creation or Modification	Azure Suspicious App Service Creation or Modification							
			Azure Suspicious Hybrid Machine Extension Installation	Azure Suspicious Policy Remediation Task								
			Azure Suspicious Policy Assignment	Azure Suspicious VM Extension Installation								
			Azure Suspicious Policy Creation or Modification	Azure Suspicious VM Scale Set Extension Installation								
			Azure Suspicious Policy Remediation Task									
			Azure Suspicious VM Automation Test									
			Azure Suspicious VM Extension Installation									
			Azure Suspicious VM Scale Set Extension Installation									

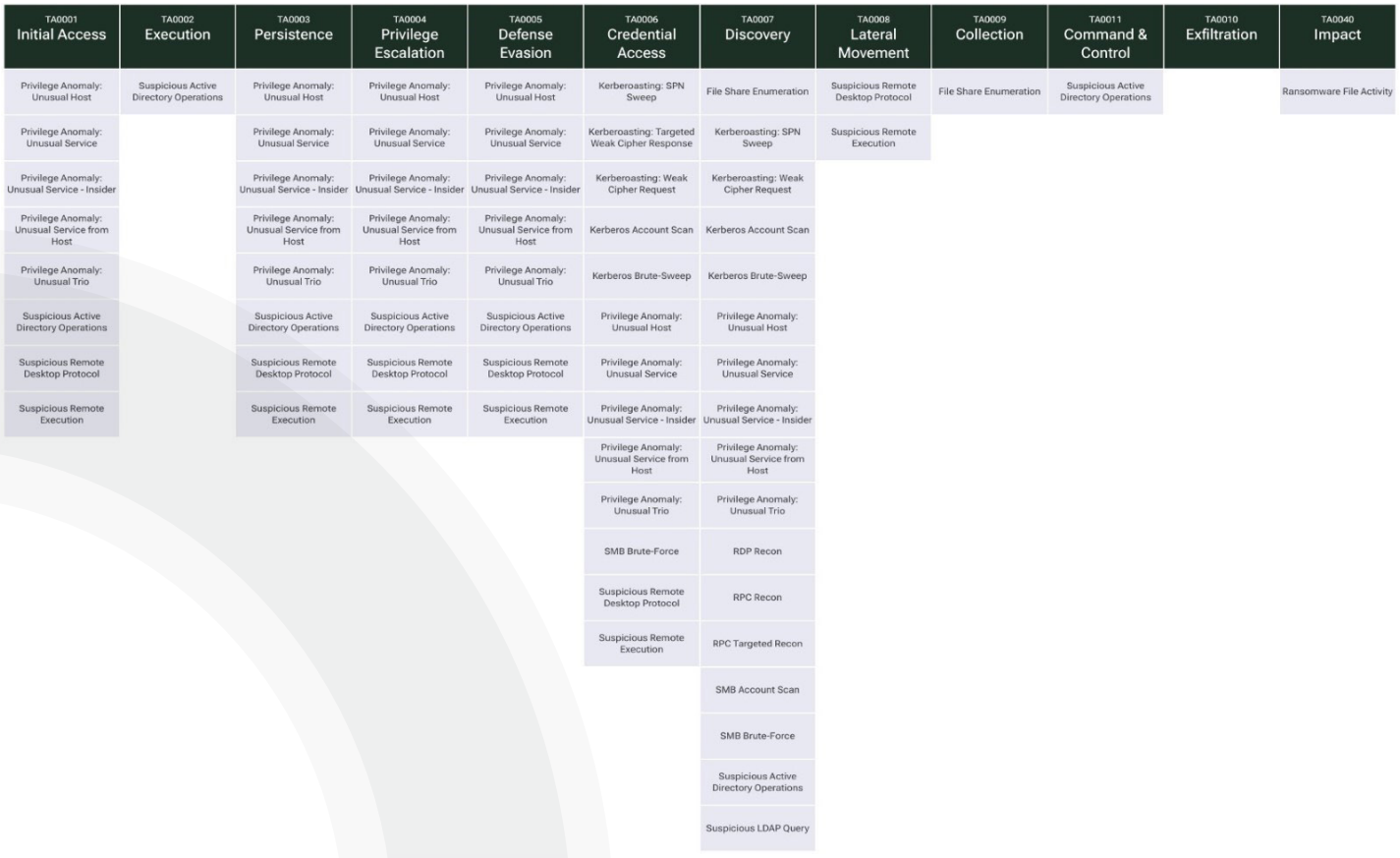
Microsoft M365: Detect living-off-the-land attacks across Microsoft 365, including Teams, Exchange, OneDrive, eDiscovery, Power Automate, and SharePoint, ensuring full threat monitoring of critical business data.

Microsoft Copilot for 365: Detect attackers using Microsoft's Gen AI to accelerate data discovery and steal high-value information.



Vectra AI for Identity Coverage

Active Directory: Detect credential attacks involving zero-day techniques and privileged credential abuse for lateral movement, including Kerberoasting, brute force, and protocol abuse of RDP, SSH, NTLM, LDAP, DCERPC, SMB, and more.



Microsoft Entra ID: Detect initial access to Microsoft Entra ID credentials and track attackers' next move, including cloud privilege abuse, new device registrations, and backdoor creation.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
Azure AD Login From Suspicious Location	Azure AD Unusual Scripting Engine Usage	Azure AD Login From Suspicious Location	Azure AD Login From Suspicious Location	Azure AD Admin Account Creation	Azure AD Admin Account Creation	Azure AD Newly Created Admin Account	Azure AD Admin Account Creation		Azure AD Suspicious Access from Cloud Provider		
Azure AD MFA Disabled		Azure AD MFA Disabled	Azure AD MFA Disabled	Azure AD Change to Trusted IP Configuration	Azure AD MFA Disabled		Azure AD Suspicious OAuth Application		Azure AD TOR Activity		
Azure AD MFA-Failed Suspicious Sign-On		Azure AD MFA-Failed Suspicious Sign-On	Azure AD MFA-Failed Suspicious Sign-On	Azure AD Login From Suspicious Location	Azure AD Successful Brute-Force						
Azure AD New Partner Added to Organization		Azure AD Newly Created Admin Account	Azure AD Newly Created Admin Account	Azure AD MFA Disabled	Azure AD Suspicious Factor Registration						
Azure AD Newly Created Admin Account		Azure AD Privilege Operation Anomaly	Azure AD Privilege Operation Anomaly	Azure AD MFA-Failed Suspicious Sign-On	Azure AD Suspicious OAuth Application						
Azure AD Privilege Operation Anomaly		Azure AD Redundant Access Creation	Azure AD Suspected Compromised Access	Azure AD Newly Created Admin Account							
Azure AD Suspected Compromised Access		Azure AD Suspected Compromised Access	Azure AD Suspicious Access from Cloud Provider	Azure AD Privilege Operation Anomaly							
Azure AD Suspicious Access from Cloud Provider		Azure AD Suspicious Access from Cloud Provider	Azure AD Suspicious Sign-on	Azure AD Suspected Compromised Access							
Azure AD Suspicious Sign-on		Azure AD Suspicious Device Registration		Azure AD Suspicious Access from Cloud Provider							
		Azure AD Suspicious Factor Registration		Azure AD Suspicious Factor Registration							
		Azure AD Suspicious Sign-on		Azure AD Suspicious OAuth Application							
				Azure AD Suspicious Sign-on							

Microsoft 365: Detect living-off-the-land attacks across Microsoft 365, including Teams, Exchange, OneDrive, eDiscovery, Power Automate, SharePoint, and more.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
M365 Suspicious SharePoint Operation	M365 Malware Stage: Upload	M365 Attacker Tool: Ruler	M365 DLL Hijacking Activity	M365 DLL Hijacking Activity	M365 Suspicious Teams Application	M365 Suspect eDiscovery Usage	Azure AD Admin Account Creation	M365 Attacker Tool: Ruler	M365 Power Automate HTTP Flow Creation	M365 Power Automate HTTP Flow Creation	M365 Ransomware
	M365 Power Automate HTTP Flow Creation	M365 DLL Hijacking Activity	M365 Risky Exchange Operation	M365 Disabling of Security Tools		M365 Suspicious Compliance Search	Azure AD Suspicious OAuth Application	M365 Exfiltration Before Termination	M365 Suspect Power Automate Activity	M365 Suspect Power Automate Activity	
	M365 Suspect Power Automate Activity	M365 Risky Exchange Operation	M365 Suspicious SharePoint Operation	M365 Log Disabling Attempt		M365 Unusual eDiscovery Search		M365 External Teams Access	M365 Suspicious Power Automate Flow Creation	M365 Suspicious Download Activity	
	M365 Suspicious Power Automate Flow Creation	M365 Suspicious Mailbox Manipulation		M365 Risky Exchange Operation				M365 Suspect eDiscovery Usage		M365 Suspicious Power Automate Flow Creation	
		M365 Suspicious SharePoint Operation		M365 Suspect eDiscovery Usage				M365 Suspicious Compliance Search		M365 eDiscovery Exfil	
				M365 Suspicious Mailbox Rule Creation				M365 Suspicious Copilot for M365 Access			
				M365 Suspicious SharePoint Operation				M365 Suspicious Exchange Transport Rule			
				M365 Suspicious Teams Application				M365 Suspicious Mail Forwarding			
								M365 Suspicious SharePoint Operation			
								M365 Suspicious Sharing Activity			
								M365 Unusual eDiscovery Search			

Azure: Detect Azure cloud identity attacks with visibility into critical infrastructure and resources, such as policies, App Service, automation accounts, and more.

TA0043 Recon	TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
Azure Suspect Key Vault Enumeration	Azure Suspicious Access from AWS Cloud	Azure Suspicious Automation DSC Execution	Azure Anomalous App Service WebJob Activity	Azure Anomalous App Service WebJob Activity	Azure Anomalous App Service WebJob Activity	Azure Suspect Credential Dump		Azure Managed Identity Anomaly	Azure Suspect Public Storage Account Change	Azure Suspicious Automation DSC Execution	Azure Suspicious Disk Download	Azure Cryptomining
	Azure Suspicious Access from GCP Cloud	Azure Suspicious Hybrid Machine Extension Installation	Azure Privilege Anomaly: Management Group Scope	Azure Privilege Anomaly: Management Group Scope	Azure Diagnostic Logging Disabled	Azure Suspicious App Service Credential Download		Azure Suspicious Automation Staged	Azure Suspicious Disk Download	Azure Suspicious Automation Staged		Azure Mass Resource Deletion
		Azure Suspicious Hybrid Machine Run Command Execution	Azure Privilege Anomaly: Root Scope	Azure Privilege Anomaly: Root Scope	Azure Mass Resource Deletion	Azure Suspicious App Service Deployment Configuration Download		Azure Suspicious Hybrid Automation Execution		Azure Suspicious Hybrid Automation Test		Azure Resource Group Admin Role Unassigned
		Azure Suspicious Policy Creation or Modification	Azure Resource Group Admin Privilege Granting	Azure Resource Group Admin Privilege Granting	Azure Privilege Anomaly: Management Group Scope	Azure Suspicious Key Vault Extraction		Azure Suspicious VM Automation Execution		Azure Suspicious VM Automation Test		Azure Subscription Admin Role Unassigned
		Azure Suspicious Policy Remediation Task	Azure Subscription Admin Privilege Granting	Azure Subscription Admin Privilege Granting	Azure Privilege Anomaly: Root Scope					Azure TOR Activity		
		Azure Suspicious Serial Console Usage	Azure Suspect App Service Deployment Activity	Azure Suspect App Service Deployment Activity	Azure Resource Group Admin Privilege Granting							
		Azure Suspicious VM Extension Installation	Azure Suspect Key Vault Privilege Granting	Azure Suspect Key Vault Privilege Granting	Azure Subscription Admin Privilege Granting							
		Azure Suspicious VM Run Command Execution	Azure Suspicious Access from AWS Cloud	Azure Suspicious Access from AWS Cloud	Azure Suspect App Service Deployment Activity							
		Azure Suspicious VM Scale Set Extension Installation	Azure Suspicious Access from GCP Cloud	Azure Suspicious Access from GCP Cloud	Azure Suspect Key Vault Privilege Granting							
		Azure Suspicious VM Scale Set Run Command Execution	Azure Suspicious App Service Creation or Modification	Azure Suspicious App Service Creation or Modification	Azure Suspect Public Storage Account Change							
			Azure Suspicious Automation DSC Execution	Azure Suspicious Hybrid Machine Extension Installation	Azure Suspicious Access from AWS Cloud							
			Azure Suspicious Automation Staged	Azure Suspicious Policy Assignment	Azure Suspicious Access from GCP Cloud							
			Azure Suspicious Hybrid Automation Test	Azure Suspicious Policy Creation or Modification	Azure Suspicious App Service Creation or Modification							
			Azure Suspicious Hybrid Machine Extension Installation	Azure Suspicious Policy Remediation Task								
			Azure Suspicious Policy Assignment	Azure Suspicious VM Extension Installation								
			Azure Suspicious Policy Creation or Modification	Azure Suspicious VM Scale Set Extension Installation								
			Azure Suspicious Policy Remediation Task									
			Azure Suspicious VM Automation Test									
			Azure Suspicious VM Extension Installation									
			Azure Suspicious VM Scale Set Extension Installation									

AWS: Detect AWS cloud identity attacks with visibility into S3, EC2, Lambdas and more.

TA0001 Initial Access	TA0002 Execution	TA0003 Persistence	TA0004 Privilege Escalation	TA0005 Defense Evasion	TA0006 Credential Access	TA0007 Discovery	TA0008 Lateral Movement	TA0009 Collection	TA0011 Command & Control	TA0010 Exfiltration	TA0040 Impact
AWS Root Credential Usage		AWS ECR Hijacking	AWS Root Credential Usage	AWS Logging Disabled	AWS Suspect Credential Access from EC2	AWS Network Configuration Discovery		AWS Suspect Public EBS Change	AWS TOR Activity	AWS Suspect Public AMI Change	AWS Cryptomining
AWS Suspect Admin Privilege Granting		AWS Lambda Hijacking	AWS Suspect Admin Privilege Granting	AWS Root Credential Usage	AWS Suspect Credential Access from ECS	AWS Organization Discovery		AWS Suspect Public EC2 Change		AWS Suspect Public EBS Change	AWS Ransomware S3 Activity
AWS Suspect External Access Granting		AWS Root Credential Usage	AWS Suspect External Access Granting	AWS Security Tools Disabled	AWS Suspect Credential Access from SSM	AWS S3 Enumeration		AWS Suspect Public S3 Change		AWS Suspect Public EC2 Change	
AWS Suspicious Credential Usage		AWS Suspect Admin Privilege Granting	AWS Suspicious Credential Usage	AWS Suspect Admin Privilege Granting	AWS Suspect Discovery From EC2 Instance	AWS Suspect Console Pivot				AWS Suspect Public RDS Change	
		AWS Suspect External Access Granting		AWS Suspect External Access Granting	AWS Suspect Traffic Mirror Creation	AWS Suspect Discovery From EC2 Instance				AWS Suspect Public S3 Change	
		AWS Suspect Login Profile Manipulation		AWS Suspect Organization Exit		AWS Suspect Escalation Reconnaissance					
		AWS Suspect Privilege Escalation		AWS Suspect Public EC2 Change		AWS Suspect Traffic Mirror Creation					
		AWS Suspect Region Activity		AWS Suspicious Credential Usage		AWS Suspicious EC2 Enumeration					
		AWS Suspicious Credential Usage				AWS User Permissions Enumeration					
		AWS User Hijacking									

Vectra AI provides

Attack Signal

- **Behavior-based Analytics.** Unlike anomaly-based tools that use AI to detect what is different, our AI is behavior-based detecting ever-evolving and emerging attacker methods.
- **Privilege Access Analytics (PAA).** Our patented graph-based AI algorithm monitors interactions between accounts, services and hosts to detect attacker abuse of privileges.
- **Advanced C2 Coverage:** AI Detections for the most advanced attacker methods of establishing command and control (C2) early in the cyber kill chain.
- **Signature Optimization.** We don't suggest you throw your signatures away – ingest them to make your attack signal stronger, and threat hunting and investigations faster.

Analyst Speed

- **Detection without decryption.** Unlike other tools that introduce operational burden, latency, and risk by needing to decrypt to detect, we see through encryption to detect threats.
- **Network Identity attribution.** We attribute detections to both hosts and Active Directory accounts whether they be human or machine saving a ton of manual work and chair swivelling and tool pivoting for analysts.
- **Security-enriched metadata.** Get deep context on every detection whether it be in our user interface or sent to the SIEM or data lake of your choice.
- **User Experience.** We strive for function over flash with a user interface that is simple to learn, manage, use for any analyst of any skill level.

Operational Scale

- **No agents.** Get immediate detection coverage where endpoint agents cannot be deployed.
- **Time to signal.** Deploy in days if not hours, get actionable network attack signal in minutes.
- **Flexibility.** Go on-premises, air gapped, SaaS, or hybrid with unmatched scale up to 300,000 IPs
- **Customization.** Integrate with your processes and tools with the Vectra Automated Response framework
- **Managed Services Support.** Leverage our MDR team to assist with 24/7 monitoring or to supplement your threat hunting, detection, investigation, and response program.

Visit our website **Get started**

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.

VECTRA

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