VECTRA®
SECURITY THAT THINKS

Vectra AI Platform

The integrated signal for your XDR @Cybers Security Summit

Miika Ruotsalainen – Vectra Ai
+358443457178 - mruotsalainen@vectra.ai

CONFIDENTAIL

The problem

The defenders’ dilemma: a vicious spiral of more

More advanced hybrid attacker methods

More detection tools and rules

More hybrid attack volume & variety

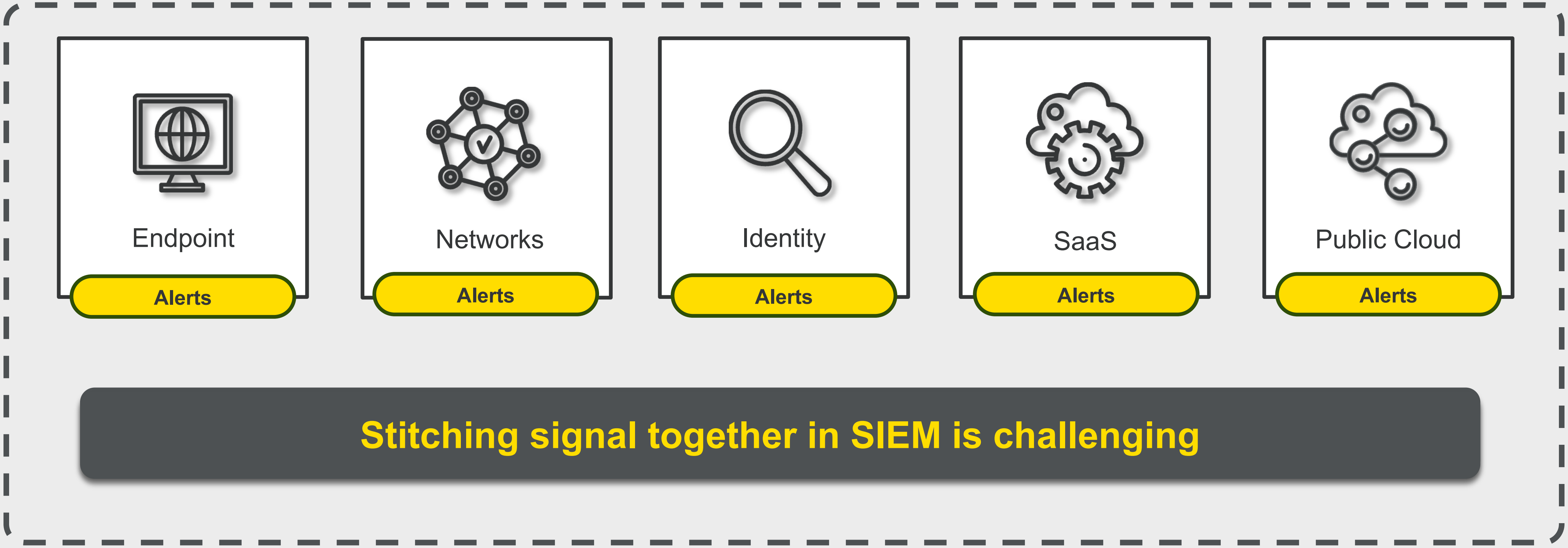
More complexity, maintenance, cost

More hybrid attack surface

More skills gaps, workload, burnout

Before Vectra AI, customers’ attack signal was siloed & hidden

Negatively impacting Cyber Resilience, SOC effectiveness and Time to detect and respond



Endpoint

Alerts

Networks

Alerts

Identity

Alerts

SaaS

Alerts

Public Cloud

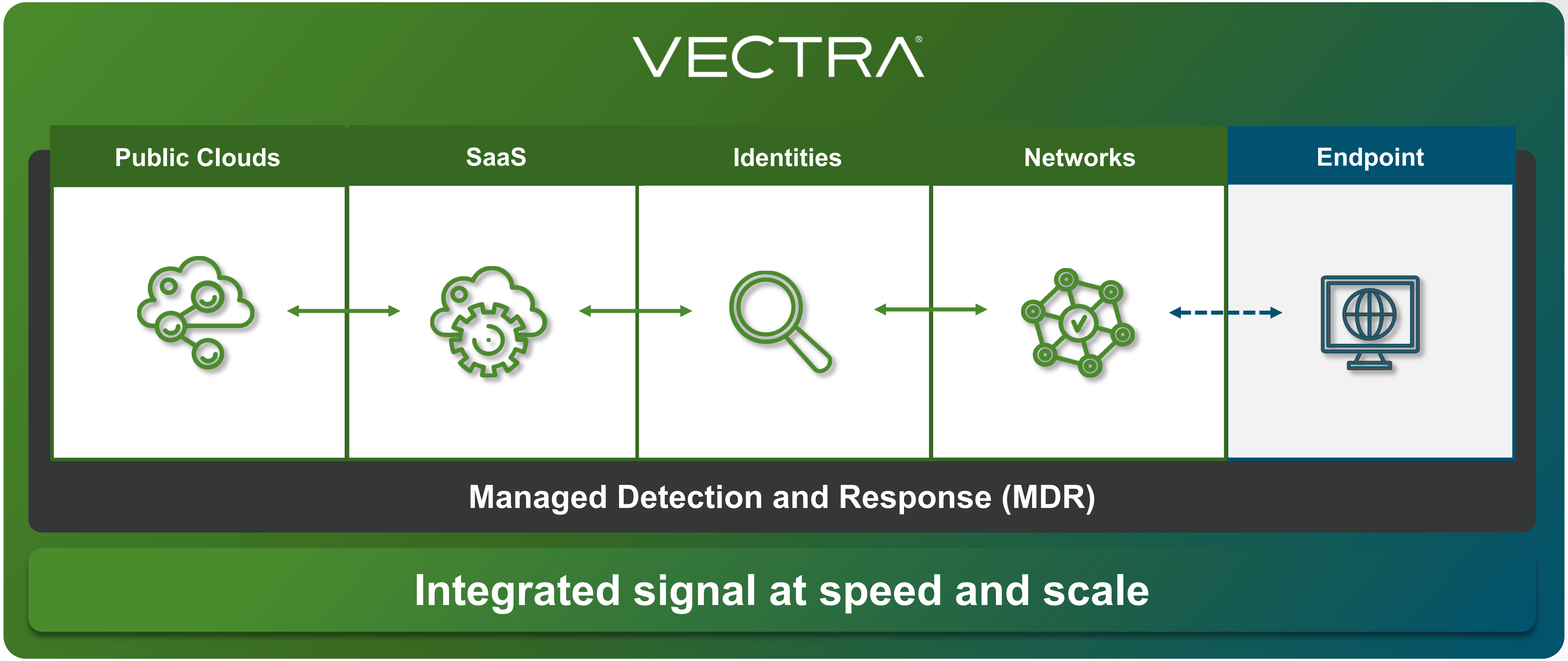
Alerts

Stitching signal together in SIEM is challenging

Source: Vectra AI: State of Threat Detection 2023 Report | The Defender’s Dilemma

With Vectra AI, customers' attack signal is integrated & visible

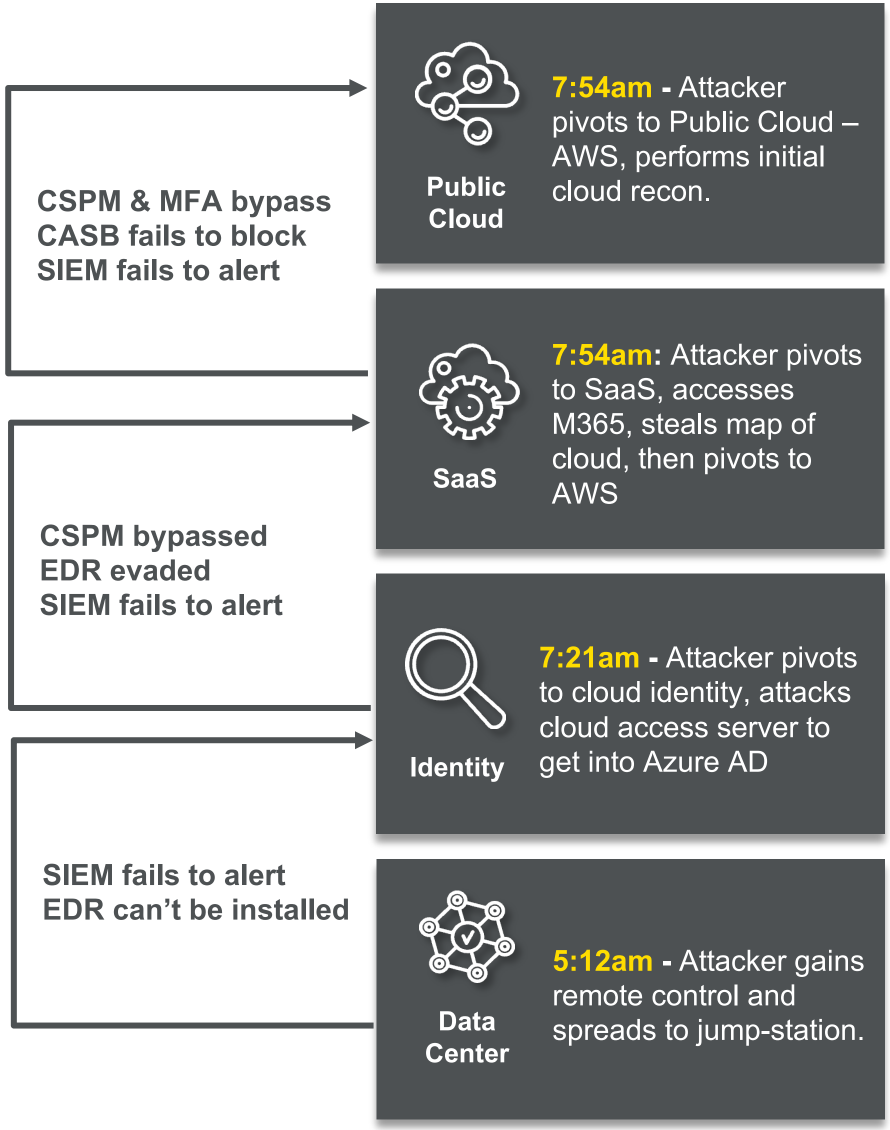
Cyber resilience through effective early hybrid attack detection and response



Managed Detection and Response (MDR)

Integrated signal at speed and scale

Vectra AI integrated signal finds attacks others can’t



CSPM & MFA bypass
CASB fails to block
SIEM fails to alert

Public Cloud — **7:54am** - Attacker pivots to Public Cloud – AWS, performs initial cloud recon.

CSPM bypassed
EDR evaded
SIEM fails to alert

SaaS — **7:54am:** Attacker pivots to SaaS, accesses M365, steals map of cloud, then pivots to AWS

Identity — **7:21am** - Attacker pivots to cloud identity, attacks cloud access server to get into Azure AD

SIEM fails to alert
EDR can’t be installed

Data Center — **5:12am** - Attacker gains remote control and spreads to jump-station.

Vectra AI detects: AWS Sign-in, AWS Organization Discovery, AWS User Permission Enumeration

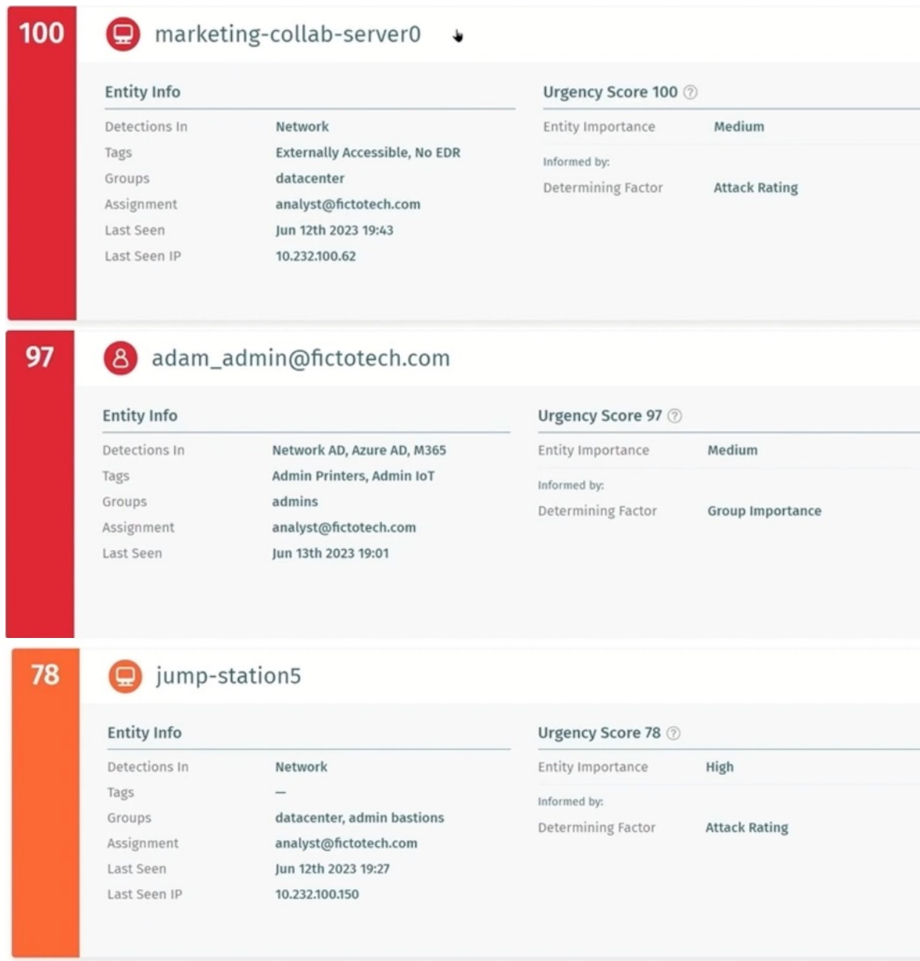
Vectra AI detects: AAD Suspicious Sign-on, M365 Suspicious Email Rule, AAD Risky OAuth Application

Vectra AI detects: Suspicious Remote Execution, Privileged Anomaly, Unusual Account on Host

Vectra AI detects: Suspicious Remote Execution

Vectra AI detects: Port Scan, Port Sweep, Suspicious LDAP, RPC Recon

Vectra AI detects: HTTPS Hidden tunnel



100 marketing-collab-server0

Entity Info		Urgency Score 100	
Detections In	Network	Entity Importance	Medium
Tags	Externally Accessible, No EDR	Informed by:	
Groups	datacenter	Determining Factor	Attack Rating
Assignment	analyst@fictotech.com		
Last Seen	Jun 12th 2023 19:43		
Last Seen IP	10.232.100.62		

97 adam_admin@fictotech.com

Entity Info		Urgency Score 97	
Detections In	Network AD, Azure AD, M365	Entity Importance	Medium
Tags	Admin Printers, Admin IoT	Informed by:	
Groups	admins	Determining Factor	Group Importance
Assignment	analyst@fictotech.com		
Last Seen	Jun 13th 2023 19:01		

78 jump-station5

Entity Info		Urgency Score 78	
Detections In	Network	Entity Importance	High
Tags	—	Informed by:	
Groups	datacenter, admin bastions	Determining Factor	Attack Rating
Assignment	analyst@fictotech.com		
Last Seen	Jun 12th 2023 19:27		
Last Seen IP	10.232.100.150		

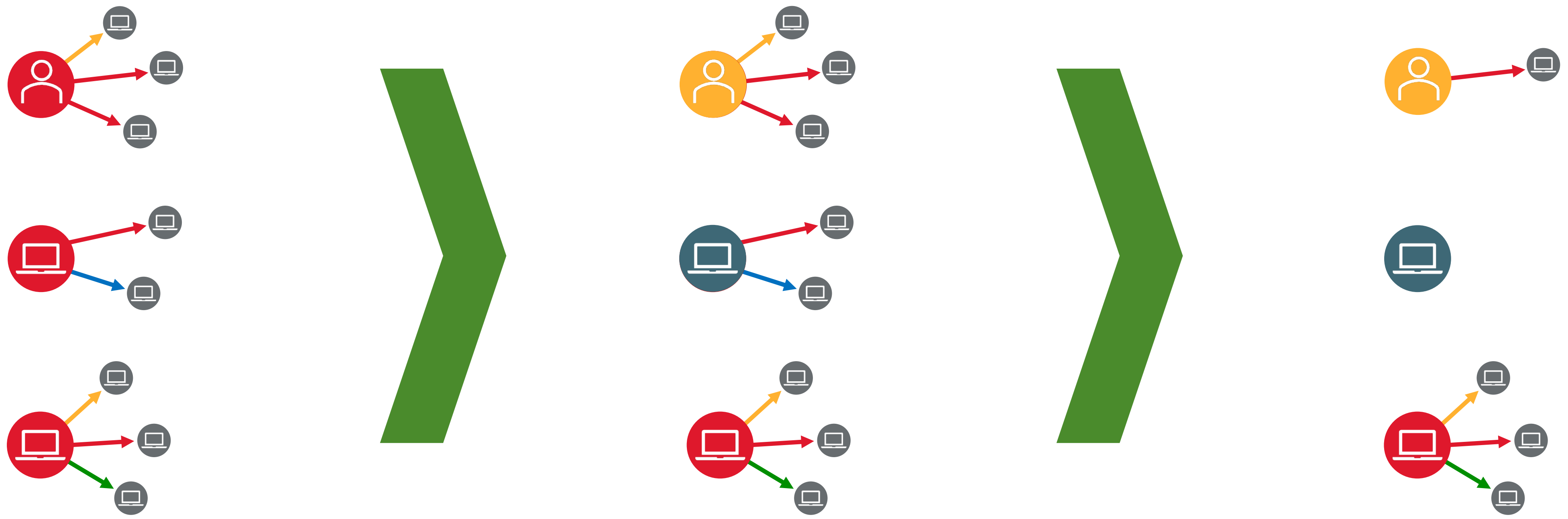
VECTRA
SECURITY THAT THINKS.®

Vectra's AI detection and prioritization stack

AI-Driven Detection
Think like an attacker

AI-Driven Triage
Know what's malicious

AI-Driven Prioritization
Focus on urgent



Finds and correlates attack behaviors

Automates the investigation of benign activity

Ranks events by business impact and unifies visibility

Vectra's unique approach

VECTRA
SECURITY THAT THINKS.®

Only Vectra AI-driven Detections think like an attacker

Real-time, behavior-based detections across the cyber kill chain

Attack Progression →

Access	Persist	Command & Control	Escalate & Evade	Recon & Discover	Lateral Movement	Exfiltration & Disruption
🟩 New Host	🟦 MFA Disabled	🟩 Hidden HTTPS Tunnel	🟩 New Host Role	🟩 Kerberoasting (x2)	🟩 Privilege Access Anomaly (x6)	🟩 Smash and Grab
🟦 Suspected Compromise Access	🟦 Trusted IP Change	🟩 Hidden DNS Tunnel	🟨 Log Disabling Attempt	🟩 Internal Darknet Scan	🟩 Suspicious 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	🟩 Multi-homed Fronted Tunnel	🟨 Suspicious Mailbox Rule	🟩 Port Sweep	🟩 Suspicious Admin	🟩 Data Smuggler
🟦 TOR Activity	🟦 Redundant Access	🟩 Suspicious Relay	🟨 Log Disabling Attempt	🟩 SMB Account Scan	🟩 Shell Knocker	🟩 Hidden DNS Tunnel Exfil
🟦 Unusual Scripting Engine	🟧 Logging Disabled	🟩 Suspect Domain Activity	🟧 Suspect Privilege Escalation	🟩 Kerberos Account Scan	🟩 Automated Replication	🟩 Hidden HTTP/S Tunnel Exfil
🟦 Suspicious OAuth App	🟧 User Hijacking	🟩 Malware Update	🟧 Suspect Privilege Manipulate	🟩 Kerberos Brute-Sweep	🟩 Brute-Force	🟩 Botnet Abuse Behaviors
🟦 Suspicious Sign-On	🟧 ECS Hijacking	🟩 Peer-to-Peer	🟧 Suspect Console Pivot	🟩 File Share Enumeration	🟩 SMB Brute-Force	🟩 Crypto mining
🟦 Suspicious Sign-On with MFA Fail	🟧 Suspect Login Profile Manipulation	🟩 Suspicious HTTP	🟧 Suspect Cred Access EC2	🟩 Suspicious LDAP Query	🟩 Kerberos Brute Force	🟨 External Teams Access
🟦 Suspicious Teams App	🟧 Security Tools Disabled	🟩 Stealth HTTP Post	🟧 Suspect Cred Access SSM	🟩 RDP Recon	🟩 SQL Injection Activity	🟨 Ransomware SharePoint Activity
🟧 Suspicious Credential Usage	🟧 SSM Hijacking	🟩 TOR Activity	🟧 Suspect Cred Access ECS	🟩 RPC Recon	🟩 Internal Stage Loader	🟨 Suspicious SharePoint Download
🟧 Root Credential Usage		🟩 Novel External Port	🟧 Suspect Cred Access Lambda	🟩 RPC Targeted Recon	🟩 Suspicious Active Directory	🟨 Suspicious SharePoint Sharing
🟧 TOR Activity		🟩 Threat Intel Match		🟨 Unusual eDiscovery Search	🟩 Novel Admin Protocol	🟨 Exfil Before Termination
		🟩 Vectra Threat Intel Match		🟨 Unusual Compliance Search	🟩 Novel Admin Share Access	🟨 Suspicious Mailbox Forwarding
				🟨 Suspect eDiscovery Activity	🟦 Risky Exchange Op	🟨 eDiscovery Exfil
				🟧 User Permission Enumeration	🟦 Internal Spear phishing	🟨 Power Automate Activity (x3)
				🟧 EC2 Enumeration	🟦 File Poisoning	🟧 Ransomware S3 Activity
				🟧 S3 Enumeration	🟦 Mailbox Manipulation	🟧 Suspect Public S3 Change
				🟧 Suspect Escalation Recon	🟦 DLL Hijacking	🟧 Suspect Public EBS Change
				🟧 Organization Discovery	🟦 Privilege Operation Anomaly	🟧 Suspect Public EC2 Change
						🟧 Suspect Public RDS Change
						🟧 Suspect External Access Grant

🟩 Hybrid Network and Identity
🟦 Identity: Azure AD
🟧 Public Cloud: AWS
🟨 SaaS: Microsoft 365

Vectra's unique approach

VECTRA
SECURITY THAT THINKS.®

Integrated signal no matter your pane of glass

Vectra AI Platform ecosystem

Vectra AI

Vectra AI as your primary pane of glass.

Integrated signal across:

- Network (NDR)
- Identity (IDR for Azure AD)
- SaaS (CDR for M365)
- Public Cloud (CDR for AWS)
- Endpoint (EDR)

CROWDSTRIKE
Microsoft Defender for Endpoint
SentinelOne
cybereason
VMware Carbon Black
Trellix

SIEM / SOAR

SIEM / SOAR as your primary pane of glass

Enrich with Vectra AI signal for:

- Network (NDR)
- Identity (IDR for Azure AD)
- SaaS (CDR for M365)
- Public Cloud (CDR for AWS)

splunk>
IBM Security
Microsoft
Siemplify now part of Google Cloud
CORTEX BY PALO ALTO NETWORKS
SWIMLANE
LogRhythm

EDR

EDR as your primary pane of glass:

Enrich with Vectra AI signal for:

- Network (NDR)
- Identity (IDR for Azure AD)
- SaaS (CDR for M365)
- Public Cloud (CDR for AWS)

CROWDSTRIKE
Microsoft Defender for Endpoint
SentinelOne
cybereason
paloalto NETWORKS
Trellix

Thank you

Miika Ruotsalainen – +358443457178 - mruotsalainen@vectra.ai