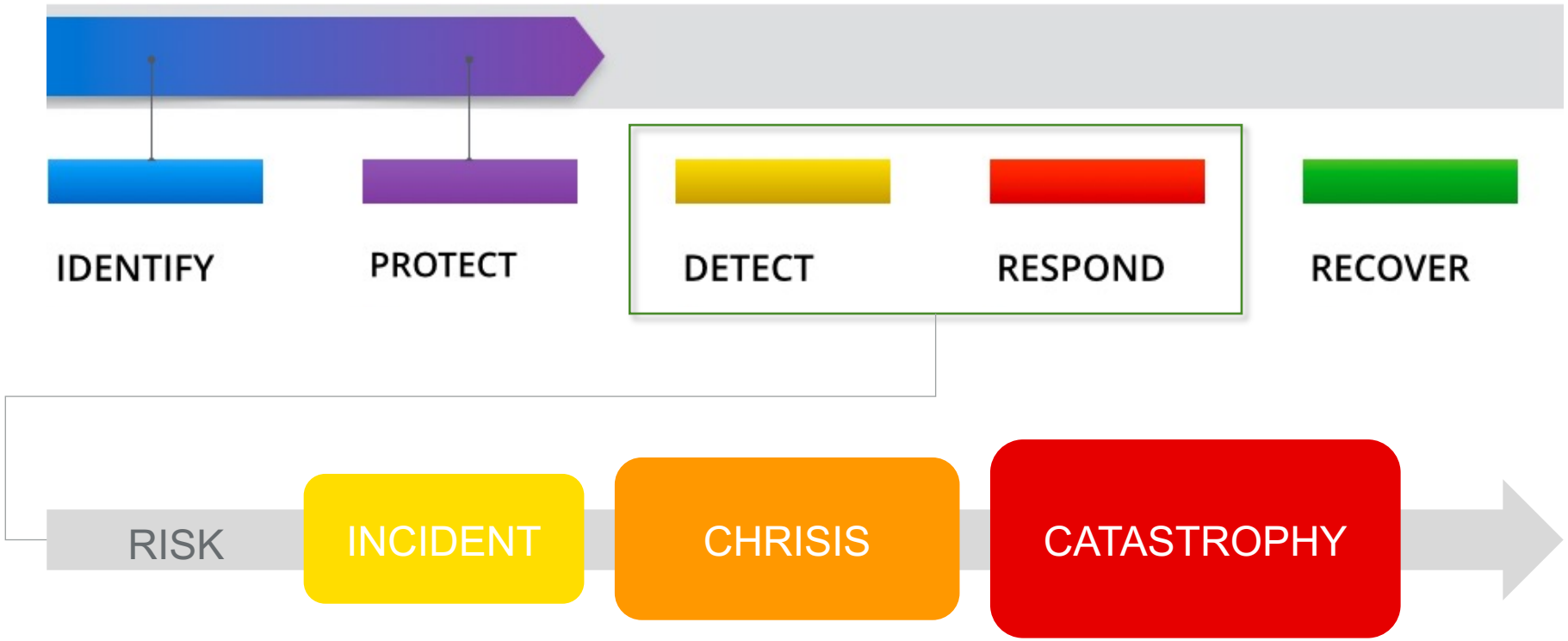
VECTRA®

SECURITY THAT THINKS.®

Attack Signal Intelligence™

Threat Detection and Response for the hybrid enterprise

When Prevention fails, efficient Threat **Detection & Response** is key.



Source: NIST Cyber Security Framework

SANS :

*"While prevention is ideal, **detection** is a must."*

The challenge from an organizations' point of view…

"We don't know if we are being **compromised right now.**

***72%** of security leaders think they may have been breached but don't know it*

"We don't know how to keep pace with **modern attacks.**

***83%** of security leaders think traditional approaches don't work for modern threats*

"We don't know how to prioritize the threats **that matter most.**

79% of security leaders say vendor tools fail to live up to their promise

More attack surface

More evasive attackers

More tools, alerts and noise

The Unknown

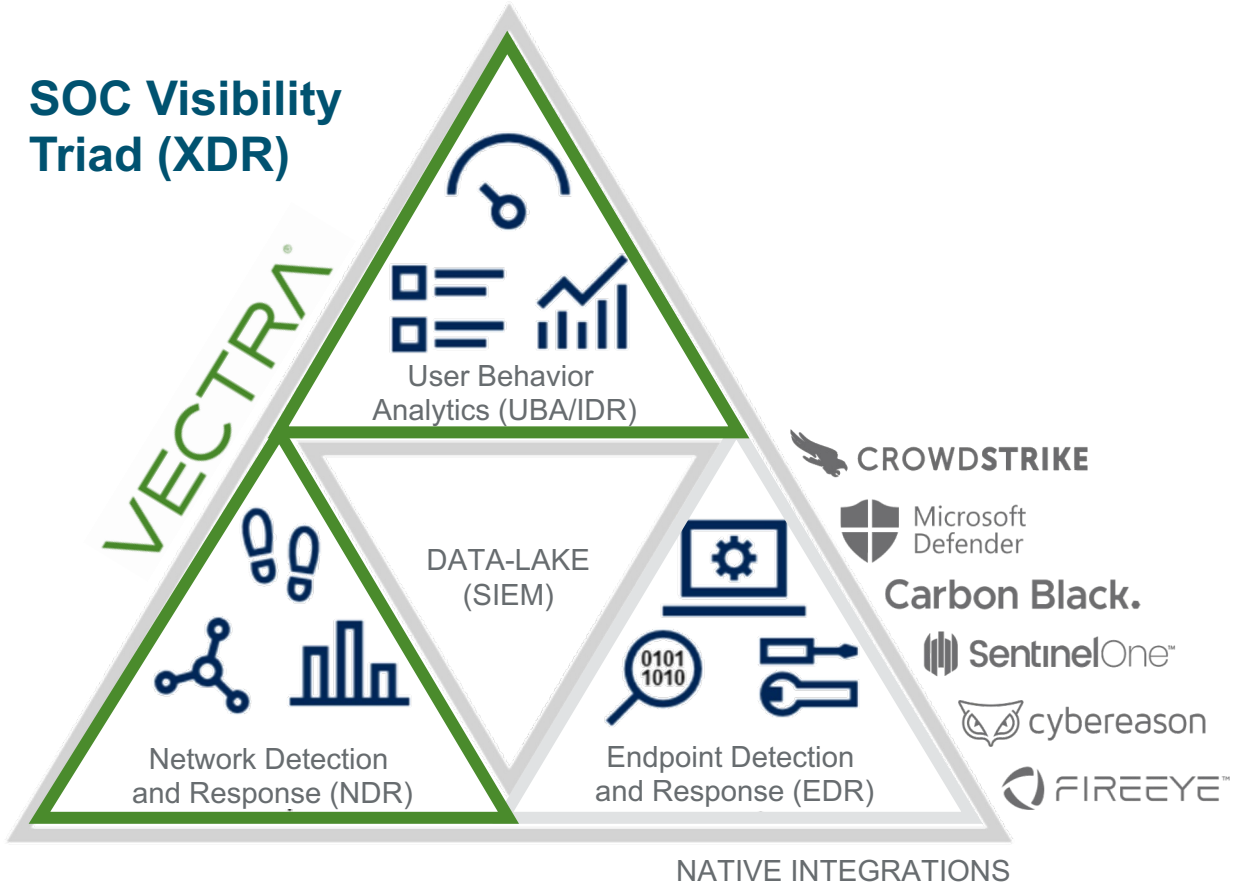
Source: Vectra Research Study | Global : Fit for Purpose or Behind the Curve? - January 2022 - Based on interviews of 1800 IT security decision makers working at organizations with more than 1,000 employees across France, Italy, Spain, Germany, Sweden, Saudi Arabia and the US, and more than 500 employees across the Netherlands and Australia & New Zealand.

Modern SecOps is anchored to the **network**.

Gartner

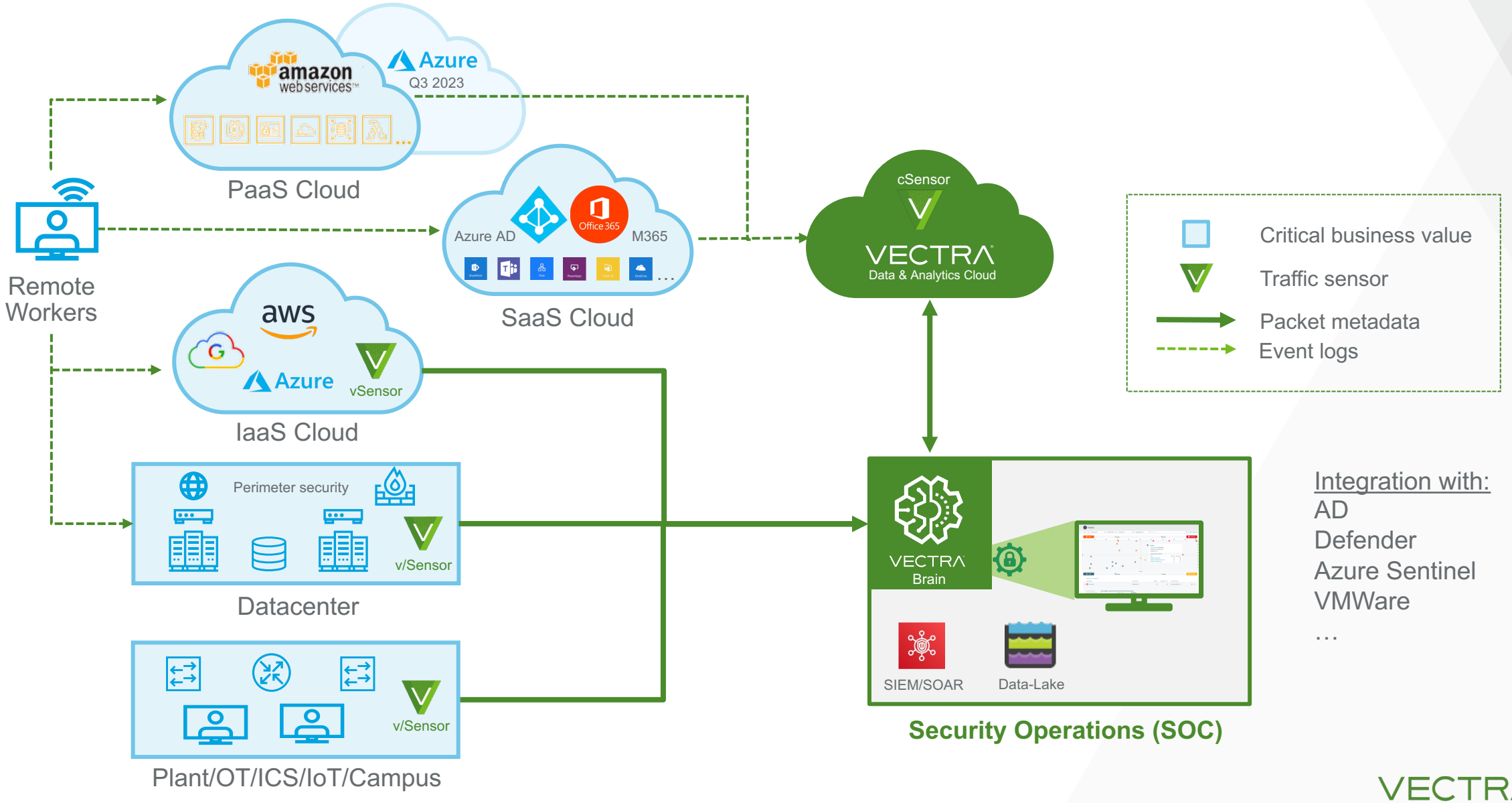
> Network-based technologies enable technical professionals to obtain quick threat visibility across an entire environment without using agents.

Source: Applying Network-Centric Approaches for Threat Detection and Response March, 2019, ID Number: G00373460



How we do it…

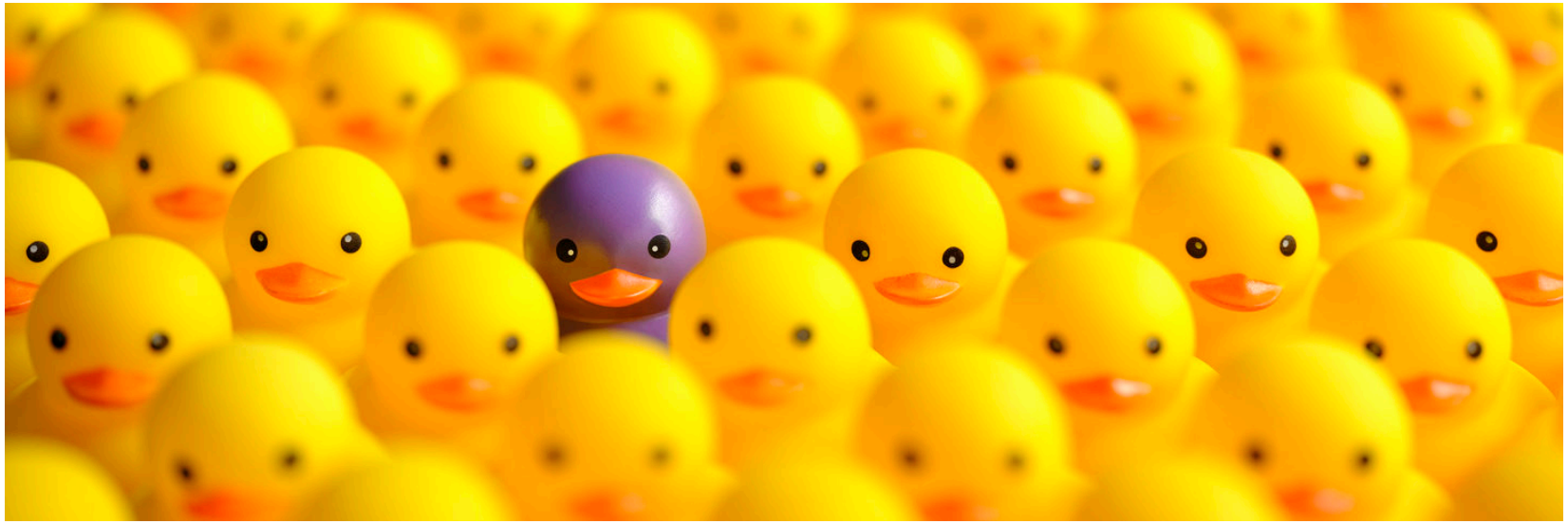
Vectra Hybrid and Multi-cloud platform architecture



Integration with:
AD
Defender
Azure Sentinel
VMWare
…

If only it was this easy…

Different ≠ Bad



Bad ≠ Different

What makes Vectra Attack Signal Intelligence™ unique?

Enable effective detection countermeasures to be developed

Diverse threats

Security Research

Common methods (TTPs)

Slowly evolving set of underlying techniques used to progress attacks

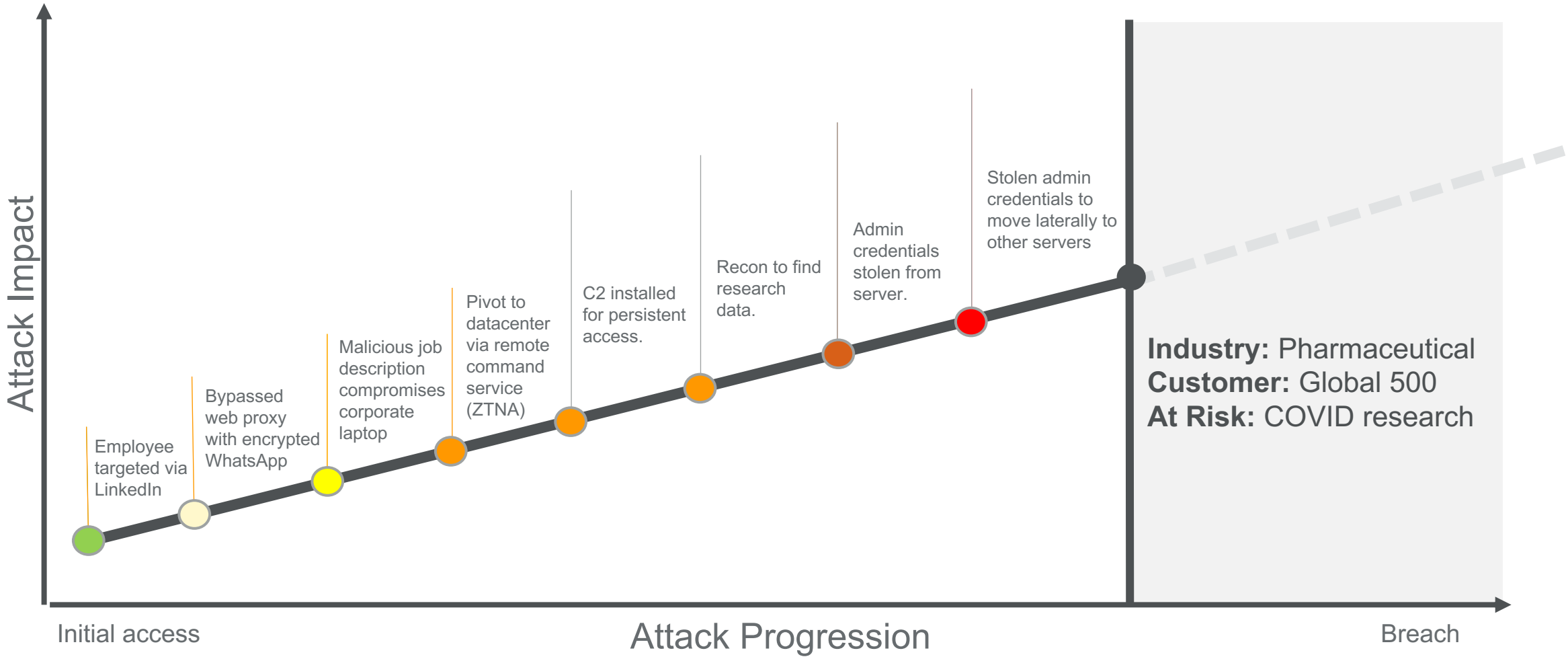
MITRE | ATT&CK®

MITRE | DEFEND™

Which can be **detected** with a durable set of **AI countermeasures**

Nation-state Espionage attack

Actual incident: Attack Signal Intelligence vs Lazarus Group (APT38)

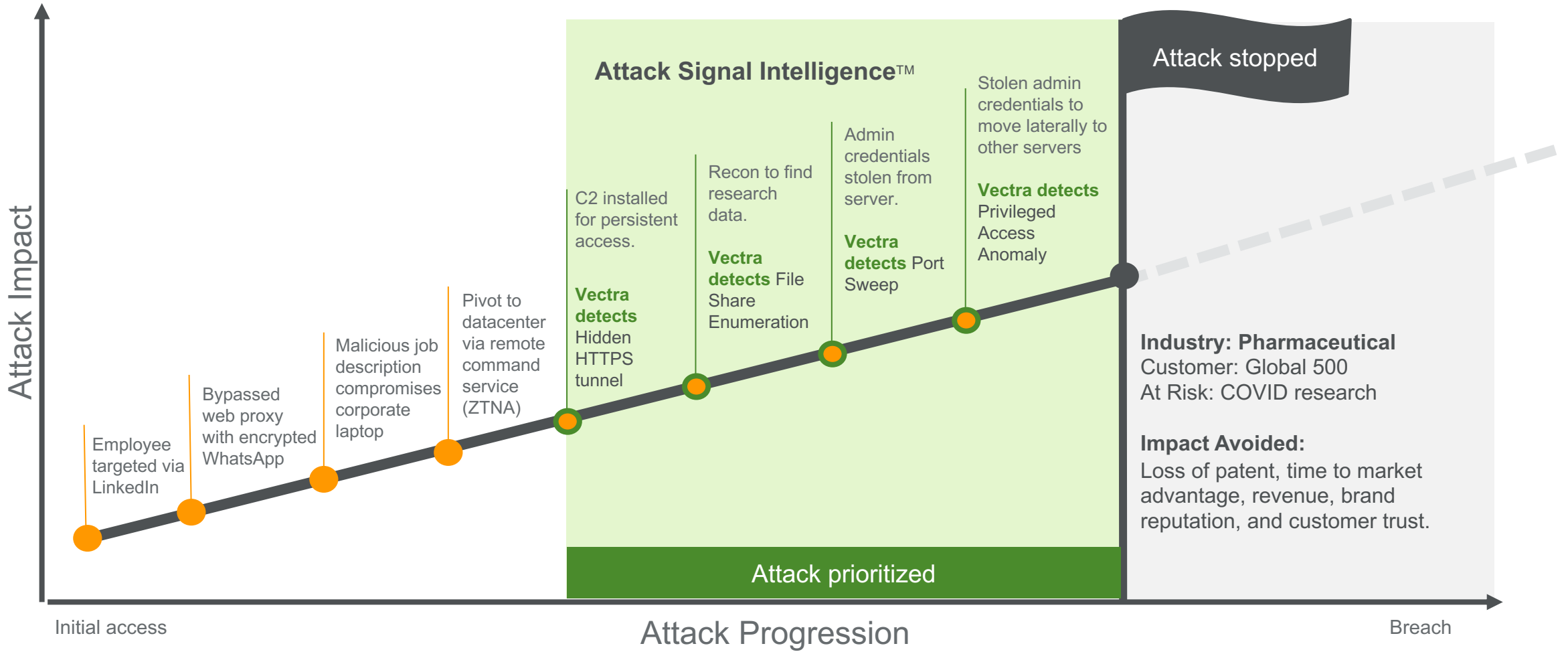


Attacks have an invariable pattern - the **Cyber Kill Chain.**

Finding **attacker behaviors** and **progression** is the key.

Nation-state Espionage attack

Actual incident: Attack Signal Intelligence vs Lazarus Group (APT38)

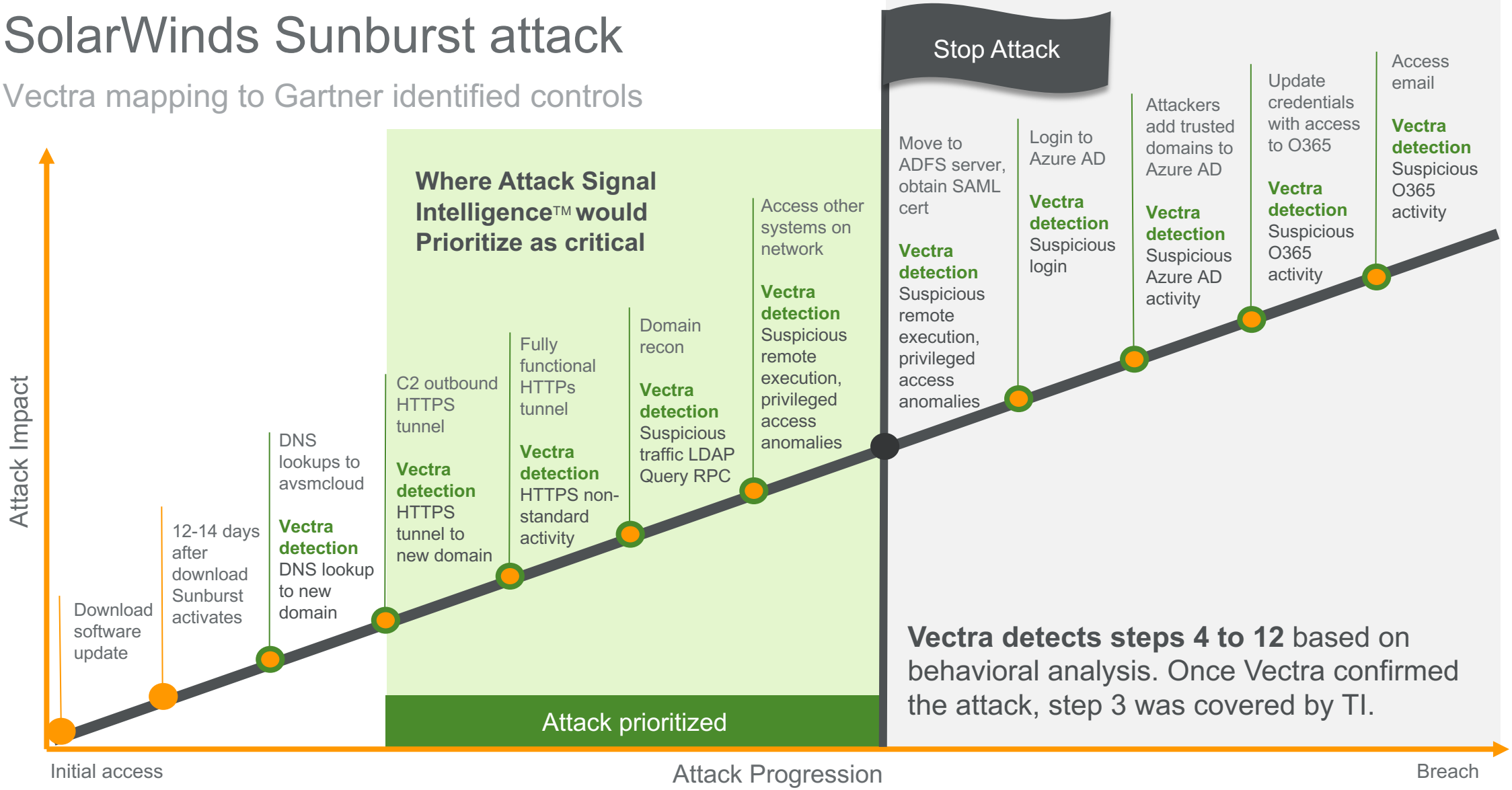


Prevention controls failed throughout - attack progresses

Secure Web Gateway | Email Security | EDR | Firewall | ZT Network Access | AV | IPS

SolarWinds Sunburst attack

Vectra mapping to Gartner identified controls



Vectra detects steps 4 to 12 based on behavioral analysis. Once Vectra confirmed the attack, step 3 was covered by TI.

Source: Gartner 8 controls to Thwart Sunburst and Other Supply Chain Attacks by Thomas Lintemuth, February 19, 2021

Example - SolarWinds Sunburst attack **in Vectra**

srv-sup-orion Threat 82 / Certainty 87

Actions | Tag | Note | Assign | Share

Account Information

Network Account
Name: gwen-adm@corp.example.com
Last Detected: Feb 7th 2022 02:18

Cloud Account
Name: O365:gwen-adm@corp.example.com
Last Detected: Feb 7th 2022 07:48

Show Details

Active Directory Lockdown

Display Name: gwen-adm Gwen Roger Admin
Active Directory Groups: Domain Admins
Password Last Changed: Feb 19th 2021 14:56
Account Status: Enabled

Show Details

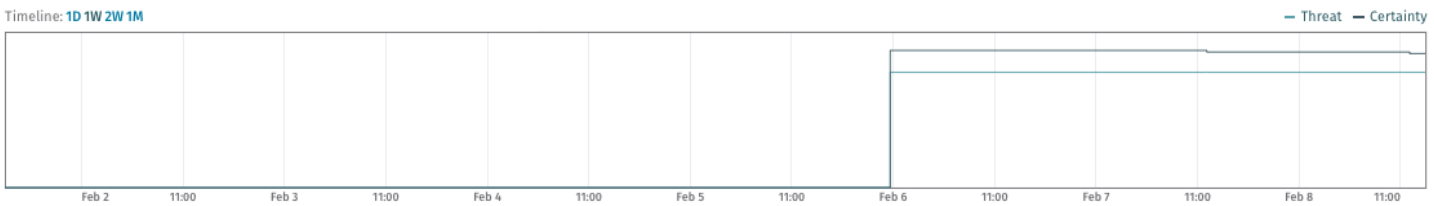
Disable Account

Detection Profile: External Adversary

Active detections are behaviors associated with sophisticated, objective-oriented adversary.

Positive Indicators
Hidden HTTPS Tunnel (C&C)
Privilege Anomaly: Unusual Trio
RPC Recon
Suspicious LDAP Query
Suspicious Remote Execution

Detections | Details



Category: All | Status: All | Contains | Advanced

Expand All | Collapse All

CATEGORY	TYPE	ACCOUNT	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN	
C&C	O365 Suspicious Power Automate Flow Creation	gwen-adm@corp.example.com	80	70	Feb 7th 2022 07:48	Feb 7th 2022 07:48	M365
Recon	O365 Unusual eDiscovery Search	gwen-adm@corp.example.com	40	60	Feb 7th 2022 07:44	Feb 7th 2022 07:44	M365
Exfil	O365 Suspicious Exchange Transport Rule	gwen-adm@corp.example.com	50	60	Feb 7th 2022 07:38	Feb 7th 2022 07:38	M365
C&C	Azure AD Redundant Access Creation	gwen-adm@corp.example.com	40	60	Feb 7th 2022 07:28	Feb 7th 2022 07:28	AzureAD
Lateral	Azure AD Suspicious Operation	gwen-adm@corp.example.com	67	34	Feb 7th 2022 07:18	Feb 7th 2022 07:18	AzureAD
C&C	Azure AD Suspicious Sign-On	gwen-adm@corp.example.com	80	70	Feb 7th 2022 07:08	Feb 7th 2022 07:08	AzureAD
Lateral	Privilege Anomaly: Unusual Trio	gwen-adm@corp.example.com	95	95	Feb 7th 2022 02:18	Feb 7th 2022 02:18	Network
Lateral	Suspicious Remote Execution		20	10	Feb 7th 2022 01:58	Feb 7th 2022 01:58	Network
Recon	RPC Recon		30	63	Feb 7th 2022 00:43	Feb 7th 2022 00:43	Network
Recon	Suspicious LDAP Query		24	25	Feb 7th 2022 00:38	Feb 7th 2022 00:38	Network
C&C	Hidden HTTPS Tunnel		22	64	Feb 6th 2022 22:38	Feb 6th 2022 23:08	Network

The complete kill-chain of attacker methods is automatically correlated into ONE critical incident.

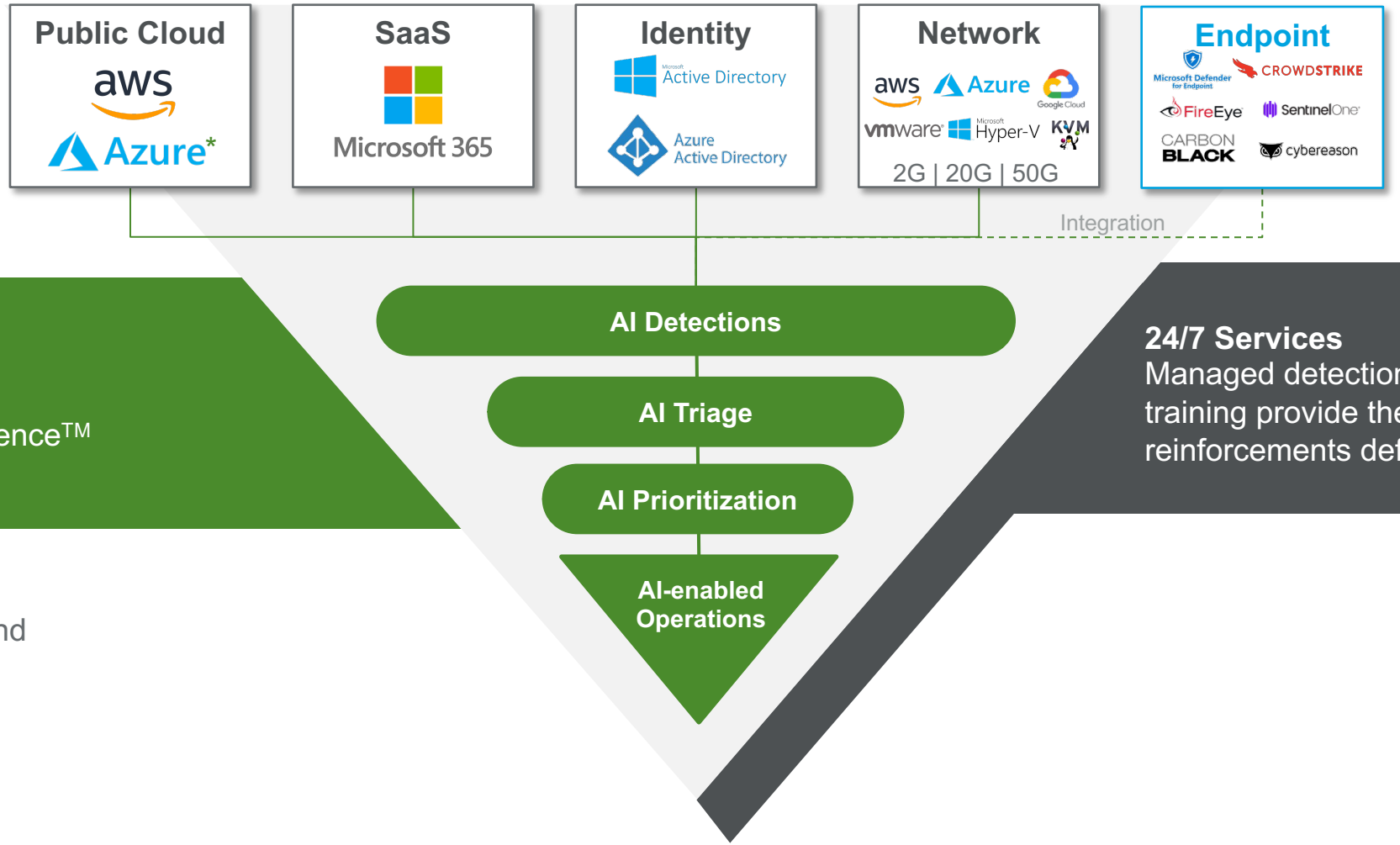
Vectra Erases the **Unknowns.**

The coverage, clarity and control we defenders deserve

Coverage
Know where you are compromised right now

Clarity
Know what to prioritize with Attack Signal Intelligence™

Control
Know how to get ahead and stay ahead of attackers



24/7 Services
Managed detection, response and training provide the skills and reinforcements defenders need

* Early Access Q1 2023


VECTRA®
SECURITY THAT THINKS.®