VECTRA®
SECURITY THAT THINKS.®

Cyberattacks are not an act of black magic!

React or Negotiate!!

15 June 2023
Rudi Jager, Security Engineer
Marcel Kosters, Security Engineer

VECTRA®
The Netherlands

Paul Tel
Country Manager

Albert Oostindie
Account Manager

Viktor Rekker
Account Manager

Mart-Jan de Vries
Account Manager

Jennie Rogers
Marketing Manager

Tomi Tarpio
Partner Manager

Rudi Jager
Security Engineer

Marcel Kosters
Security Engineer

The one constant in security is MORE

Spiral of more

- More Remote Users
- More Cloud Services
- More Cloud Vulnerabilities
- More Account Compromise
- More Network Devices
- More Lateral Movement

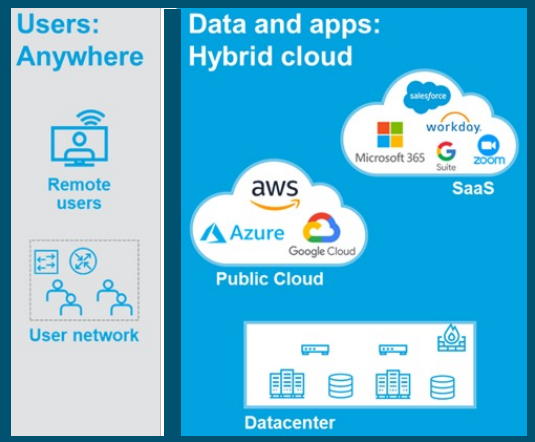
spiral of more

- More Attack Surface
- More Evasive Attackers
- More Blind Spots
- More Attacker Exploits
- More Alert Triage
- More Analyst Workload

More SOC unknowns

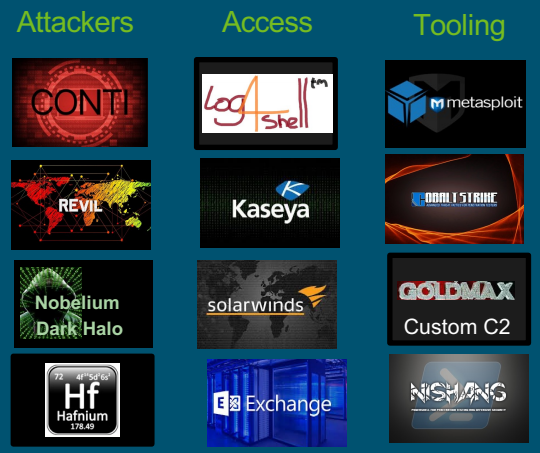
The “we don’t knows” of hybrid threat detection and response

More Attack Surface



We don’t know where we are compromised - right now

More Evasive Attacker Methods



We don’t know how to keep pace with modern threats

More People & Skills Needed

3.4M Cybersecurity workforce gap [2]

7/10 Analysts are burnt out [3]

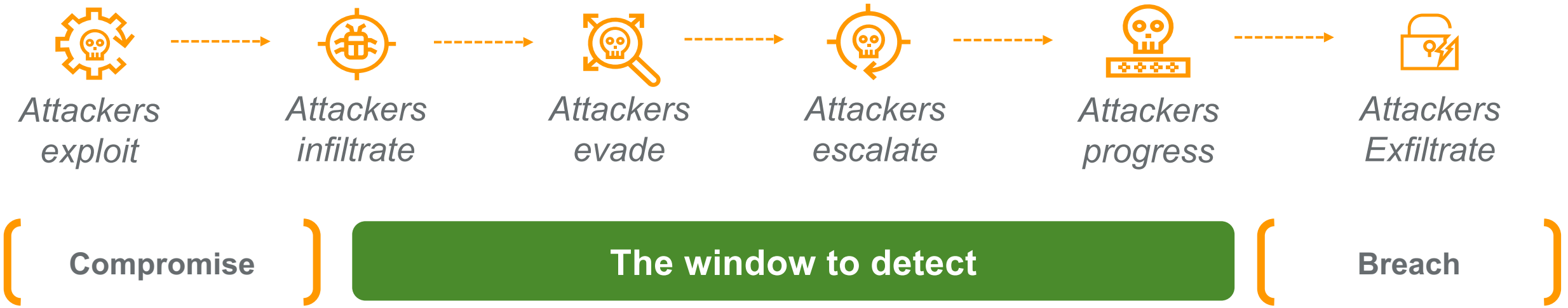
45% Cloud-based breaches [3]

We don’t know what threats are real – what alerts matter

[1] Vectra Research Study December 2022 | [2] (ISC)2 Research 2022 | [3] IBM Security Research 2022 | [4] Vectra sponsored research: Enterprise Strategy Group study The Evolving Role of NDR, October 2022

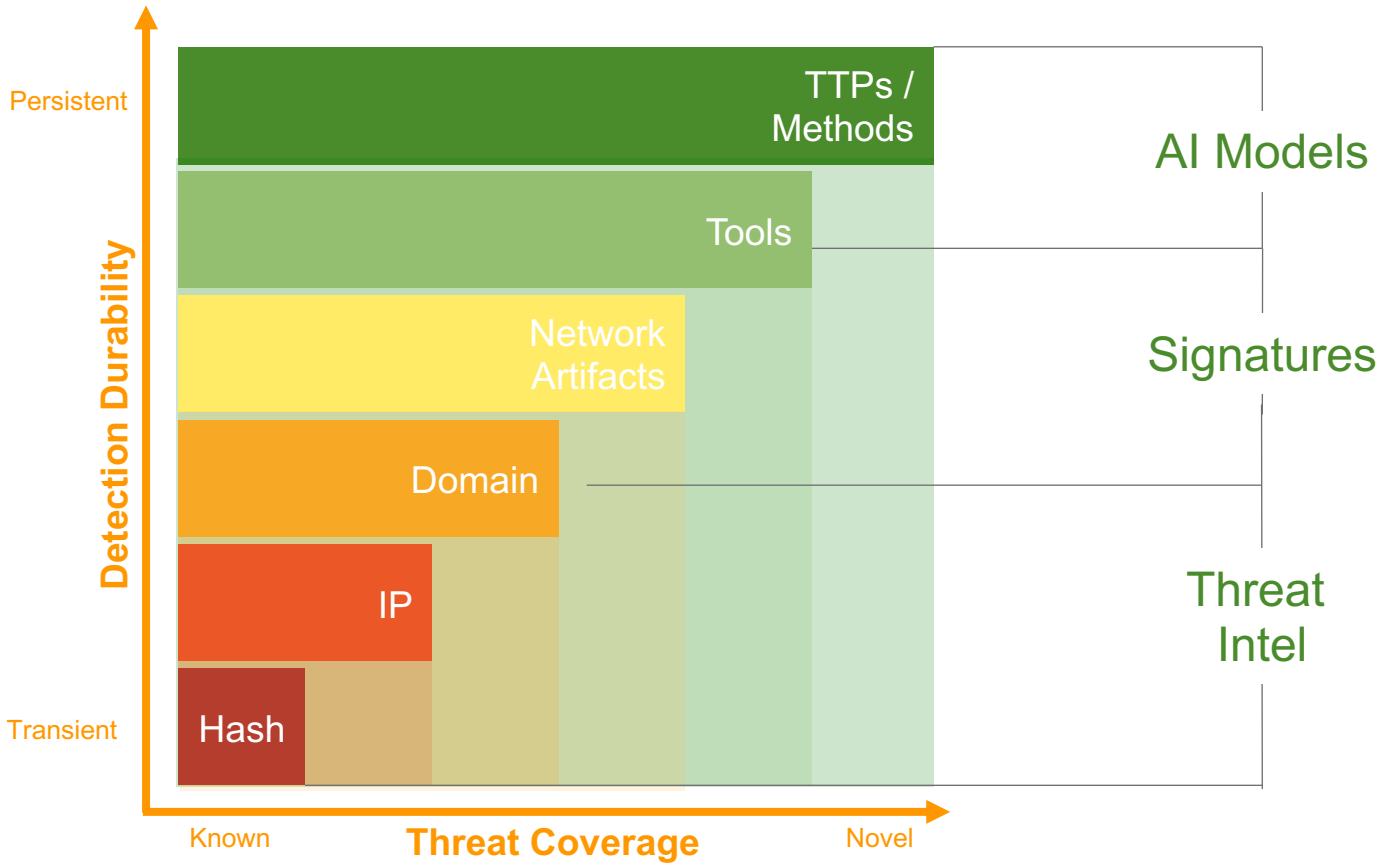
VECTRA SECURITY THAT THINKS®

Attacks have an invariable pattern: the Cyber Kill Chain.



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

Vectra: Methodology
Erase the Unknown



AI Models

- Coverage of novel and known attacks
- Much more difficult and expensive to evade
- Detect Attacks over Encryption

Signatures

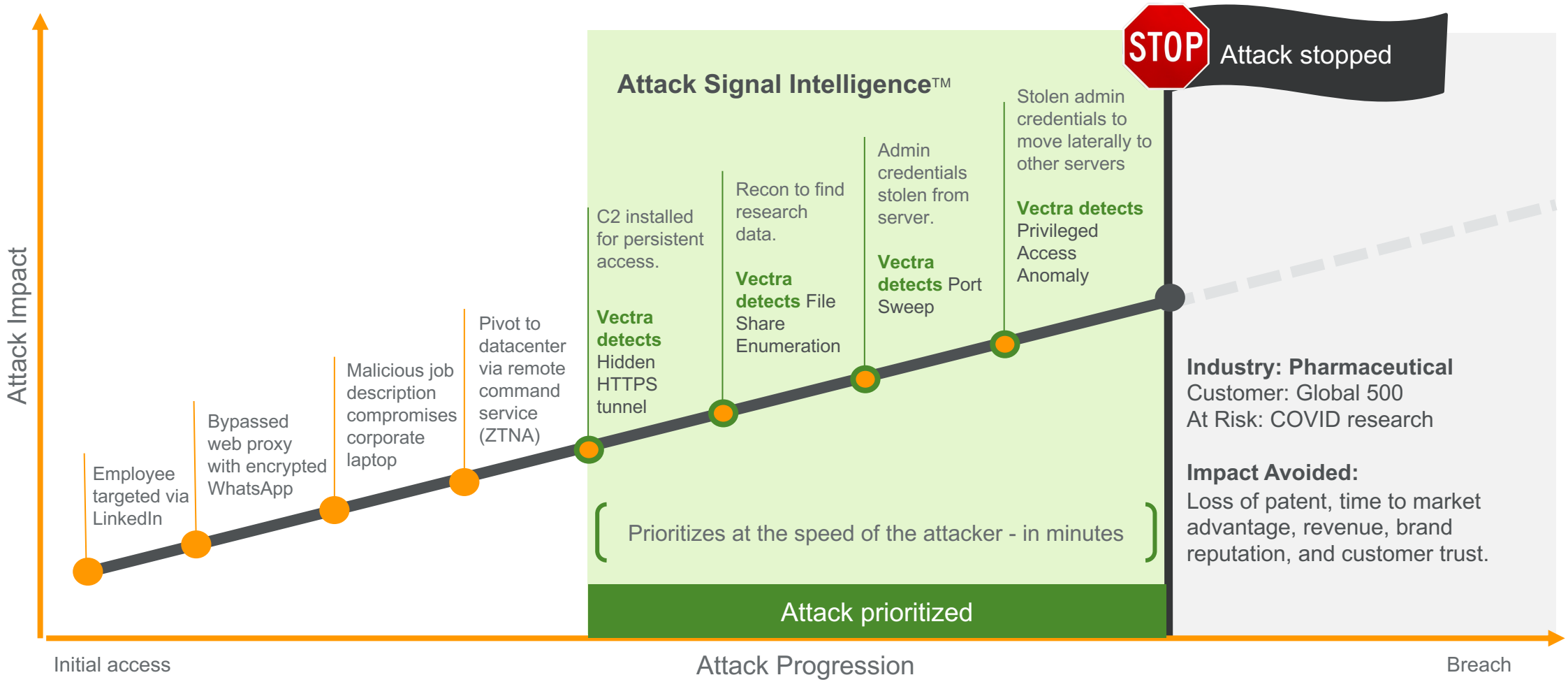
- Match known patterns
- Inexpensive to develop
- Label threats for attribution

Threat Intel

- Match known IOC's
- Easily automated
- Very inexpensive to develop

Network Attack

Actual incident: Lazarus Group

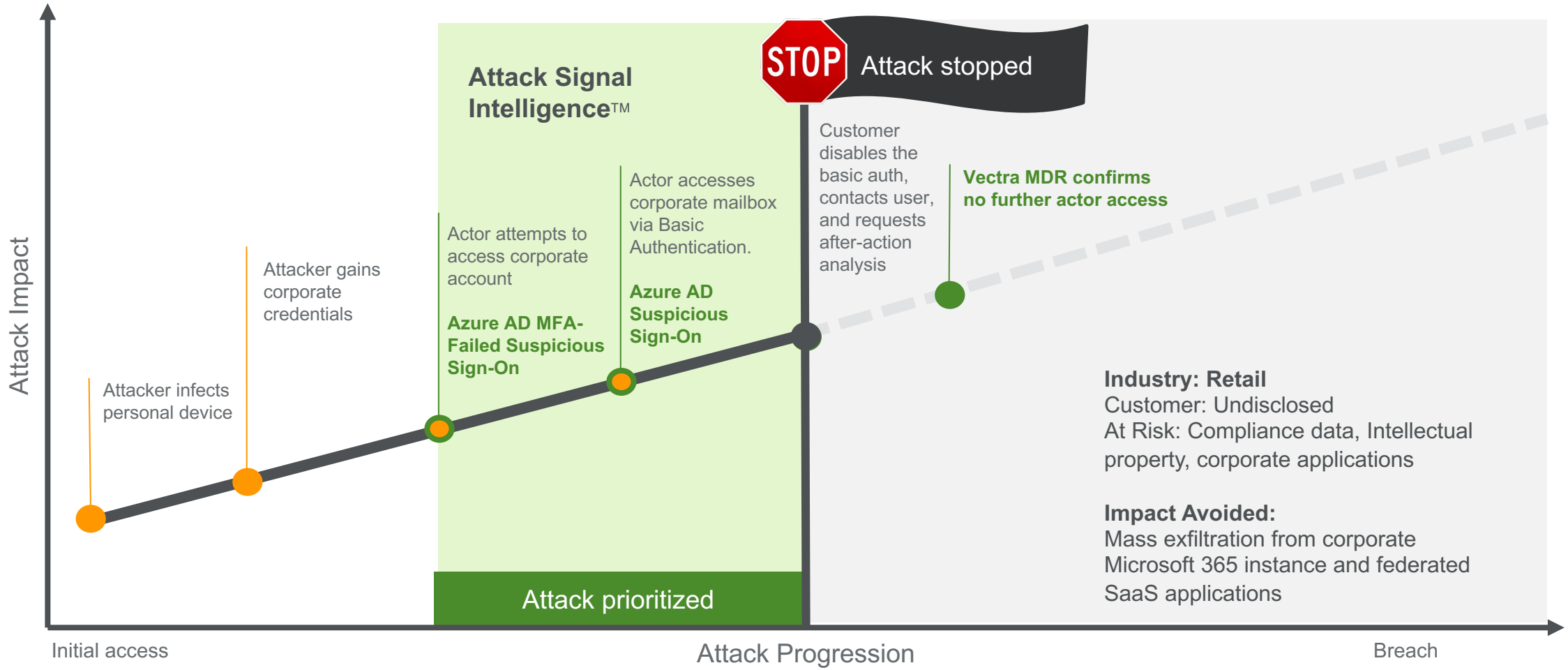


Prevention controls failed throughout - attack progresses

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

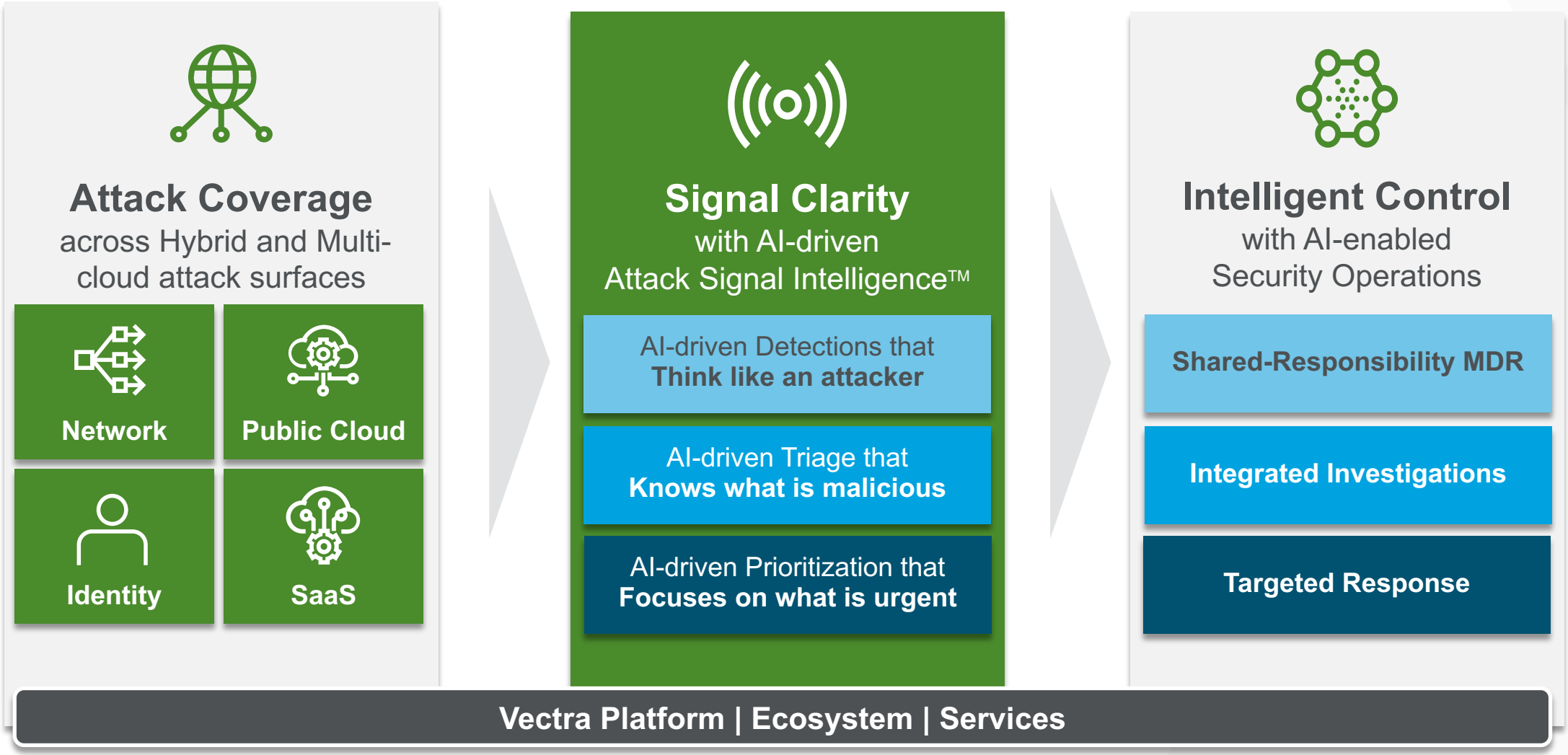
Personal device to Corporate cloud attack

Actual incident: Vectra MDR Analysts stop cloud attack originating from a personal device



AI-driven signal clarity is our core

Prioritize threats in places EDR can't and in ways legacy IDS and SIEM won't.



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**

Improve detection instead of negotiating

Remove latency, improve SOC efficiency

"Prevention is ideal, but Detection and Response is a must" - SANS

Vectra: Threat Detection & Response For Hybrid & Multi-cloud

Sees in places EDR can't go. Looks in ways legacy IDS and SIEM don't