VECTRA®

Network Detection and Response

Russian state-sponsored cybercriminals exploiting VMware vulnerability

Average number of records stolen in a breach

- **2010-2014 = 400M**
- **2015-2020 = 1.4 billion**

Phishing campaign threatens coronavirus vaccine supply chain

Suspicious email aimed to get users to give up Office 365 credentials

Data of 27 Million Texas Drivers Compromised in Breach
Gov Info Security

Why?

CISA Warns Public About Online Holiday Shopping Scams
Security Magazine

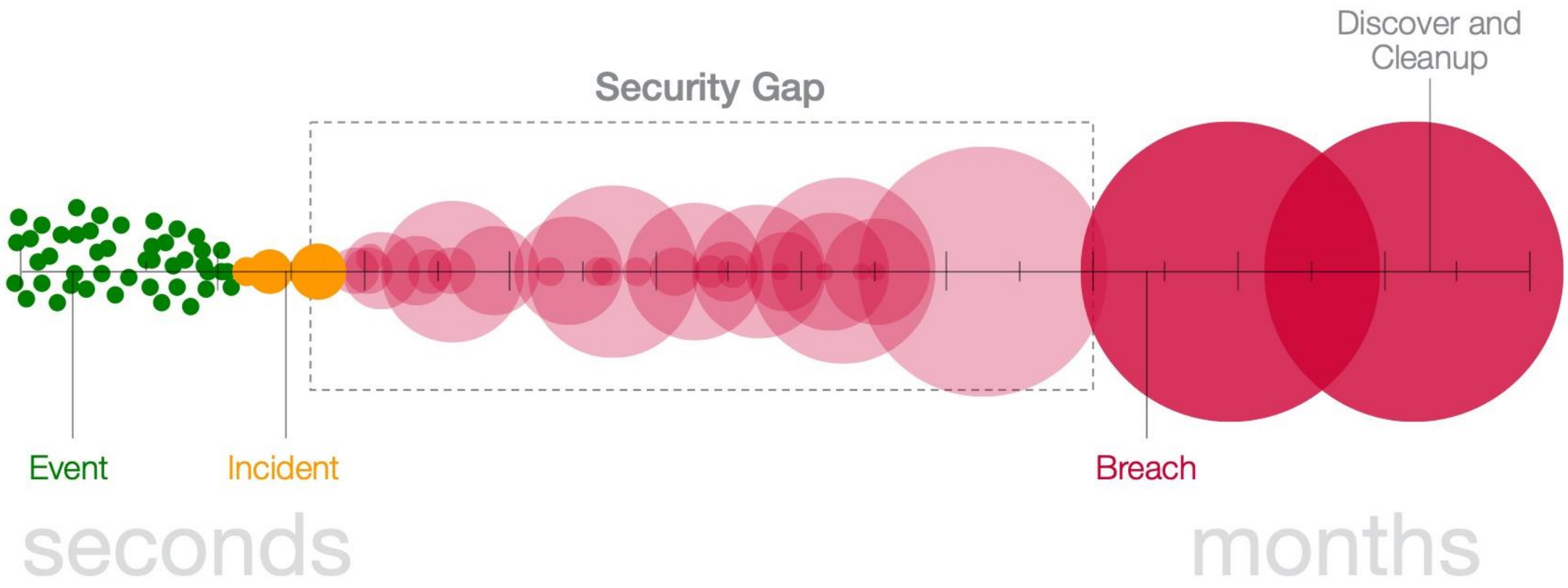
Europol Warns of COVID-19 Vaccine Crime Gangs
Latest Warning About Online Fraudsters, Supply Chain Threats

U.S. Treasury, Commerce Depts. Hacked Through SolarWinds Compromise

Cost of a breach in 2020: $3.86M
- Ponemon institute

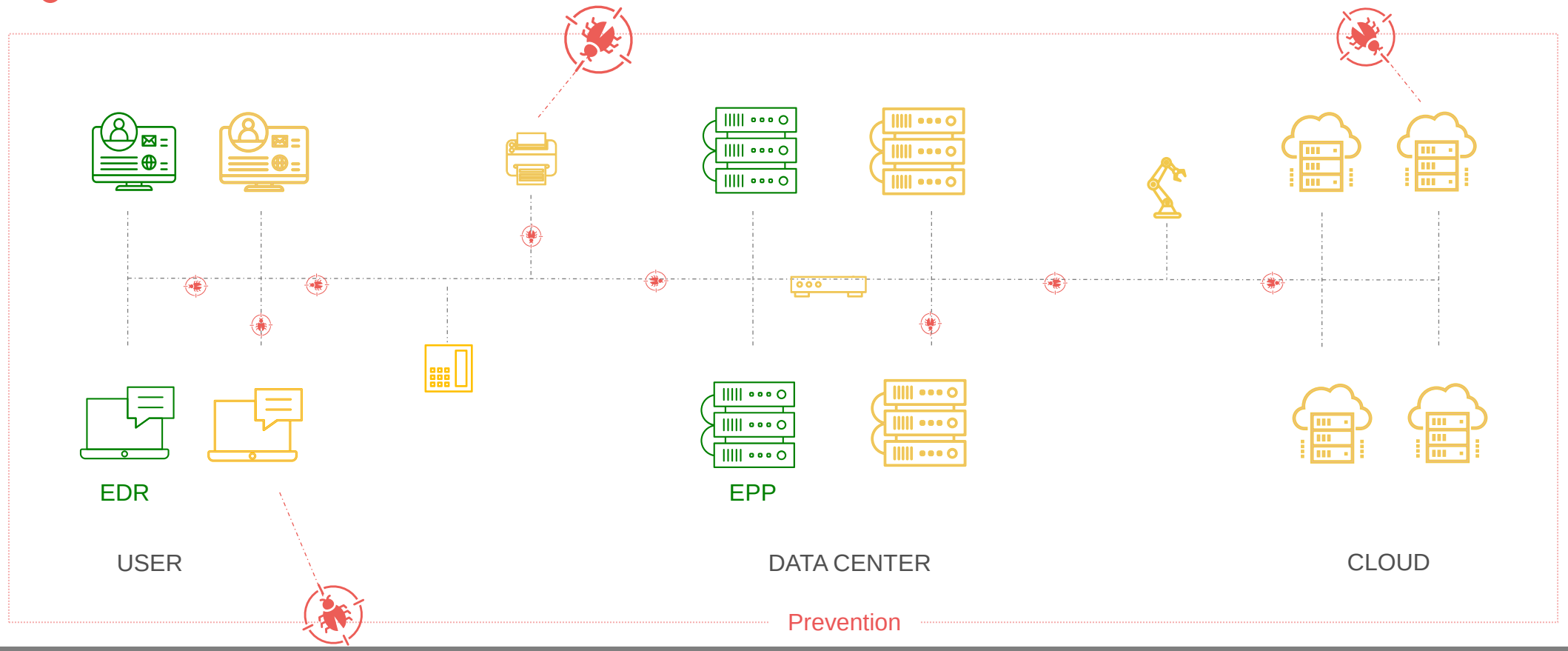
Phishing Campaign Targets 200M Microsoft 365 Accounts

Detection stops incidents from becoming breaches.



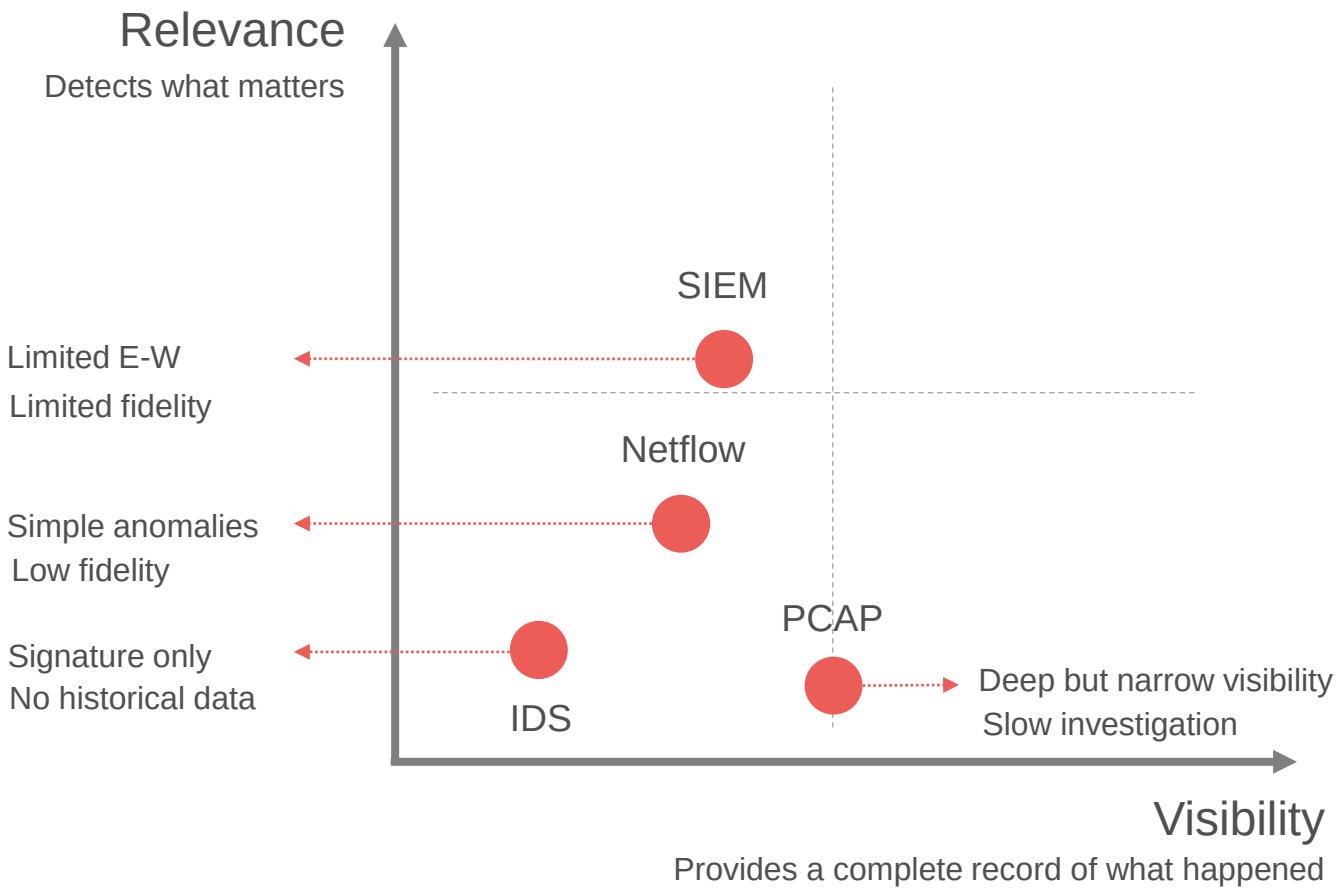
VECTRA

There is a security gap



Only the Network provides full coverage

Legacy network security is the weak link

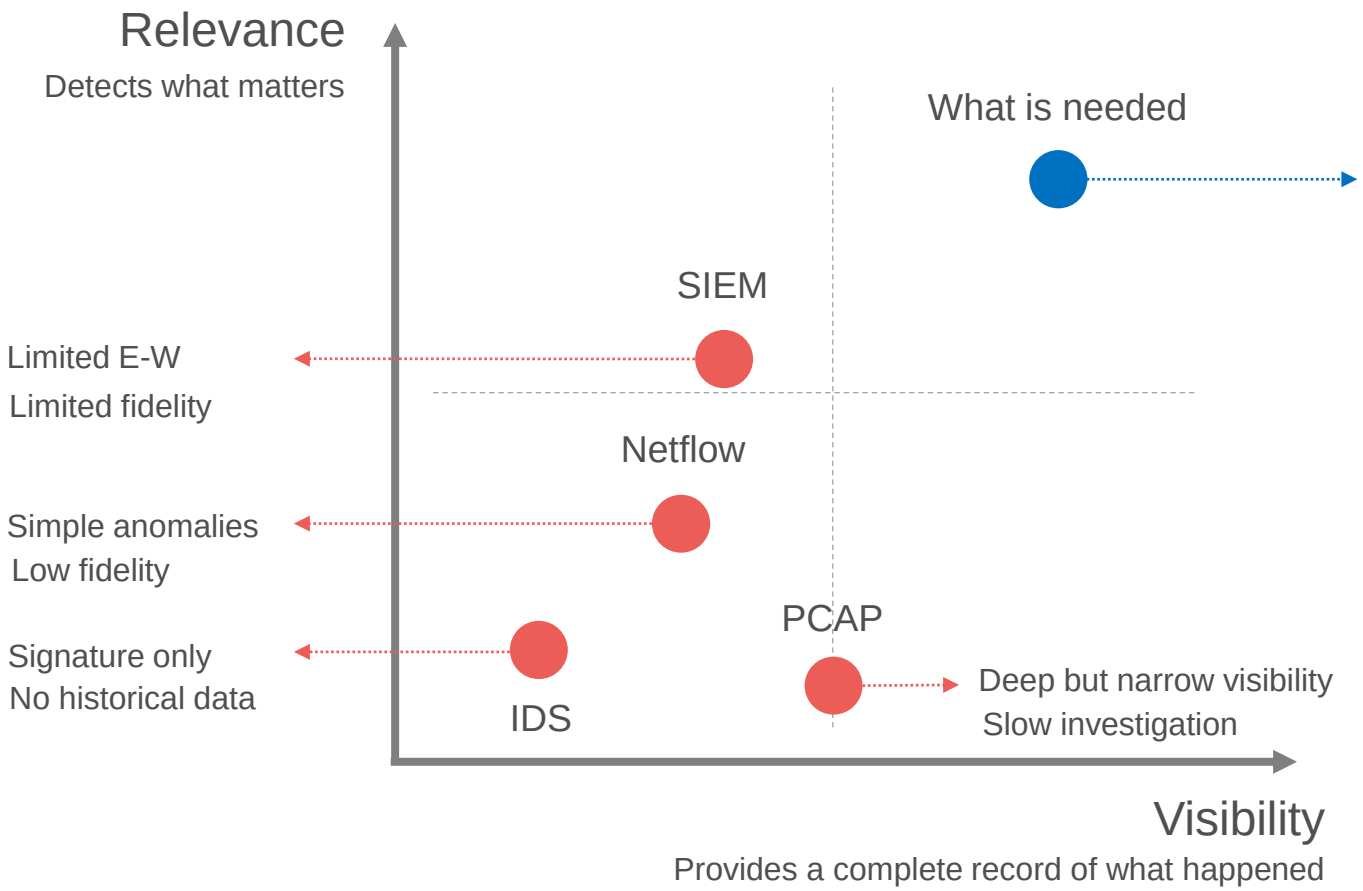


Resulting Challenges

- Too many blind spots – no visibility
- Attackers remain hidden for months
- Drowning in irrelevant alerts
- Time and resources

VECTRA

Legacy network security is the weak link



Continuous compromise awareness

=

Analyzed the right way

AI detections

Smart signatures

Threat intel

▲

The right data

High fidelity

Security enriched

360 deg view

VECTRA

How do we make this a reality?

1 Capture the right data everywhere without agents.

- Sensors deployed across cloud, data center and enterprise
- Custom flow engine extracts relevant metadata from traffic or logs
- Ingest external data sources

Public Cloud

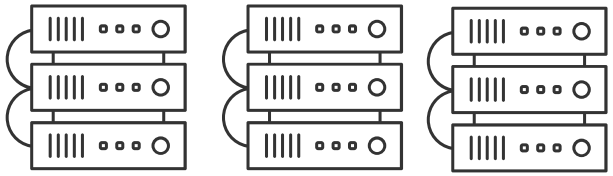
Microsoft Azure

amazon web services

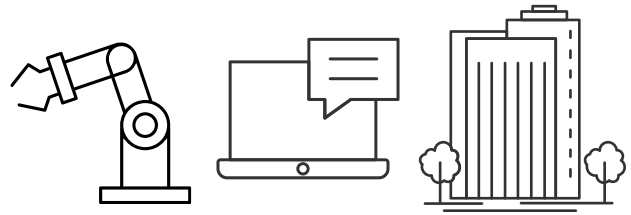
Office 365

Google Cloud

Data Center



Managed and Unmanaged Devices

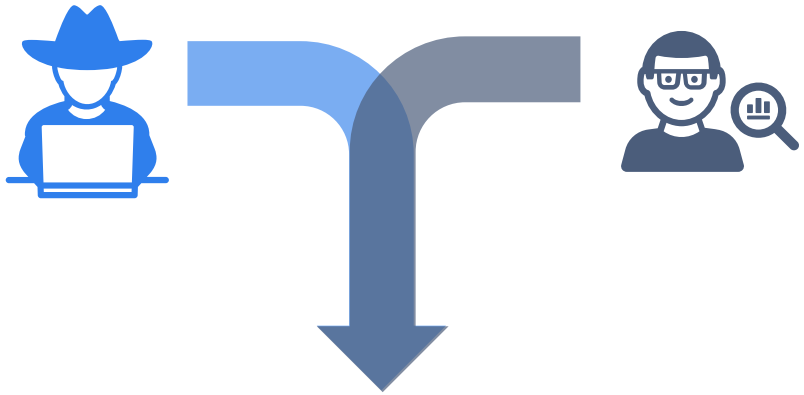


2 Detect attacker behaviors, not anomalies

Identify patterns matching techniques and procedures, rather than flagging anomalous behavior.

Security Research

Fundamental attacker behaviors sourced from securing the world's most sensitive assets



Data Science

Team of **PhD data scientists** who codify behaviors across unsupervised, supervised and deep learning models

Security Analyst in Software

Complete coverage of the MITRE ATT&CK

Security enrichments

Automate Tier-1 activities

3 Surface threats in real time.

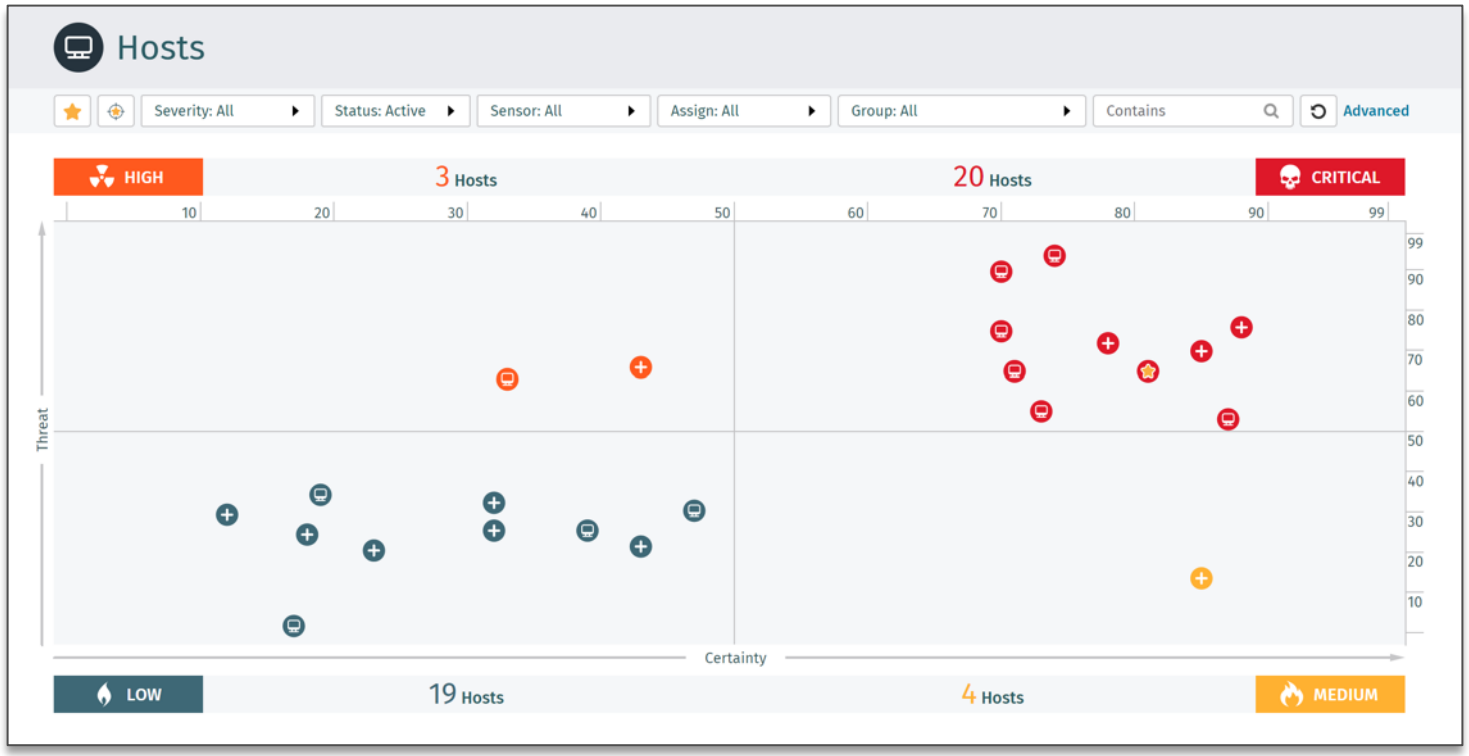
Show meaningful alerts and map them to the cyber kill-chain and ATT&CK framework.

Command and Control	Reconnaissance	Lateral Movement	Impact
Tunnels: HTTP/S and DNS	Network scans	Privileged Access Analytics	Exfil: DNS, HTTP/S tunnels
Reverse shells and RATs	Account scans	Admin protocol use	Exfil: Data movement
DGAs, TOR, Relays	File enumeration	Exploits (behavioral)	Ransomware: file encryption
Threat Intelligence	RPC and RDP Recon	Brute-force and SQLi	Cryptocurrency mining

VECTRA®

4 Correlate and prioritize alerts.

Ultra high signal-noise ratio to focus on what matters.



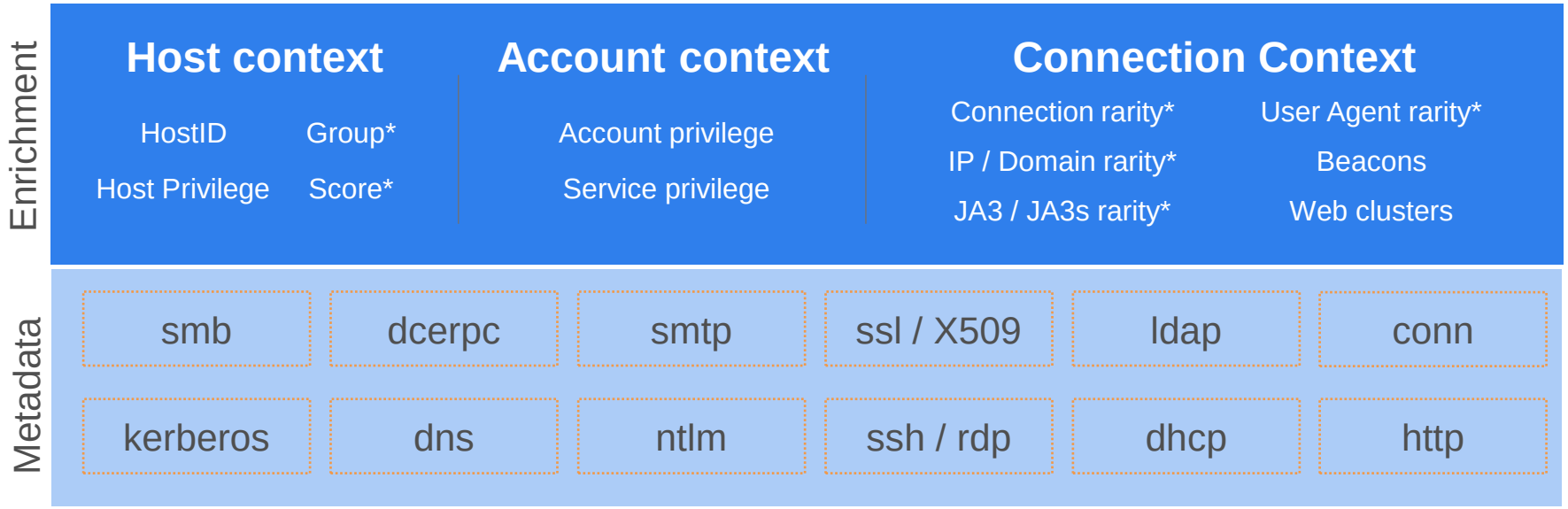
Host & Accounts

Unified view

Clear prioritization

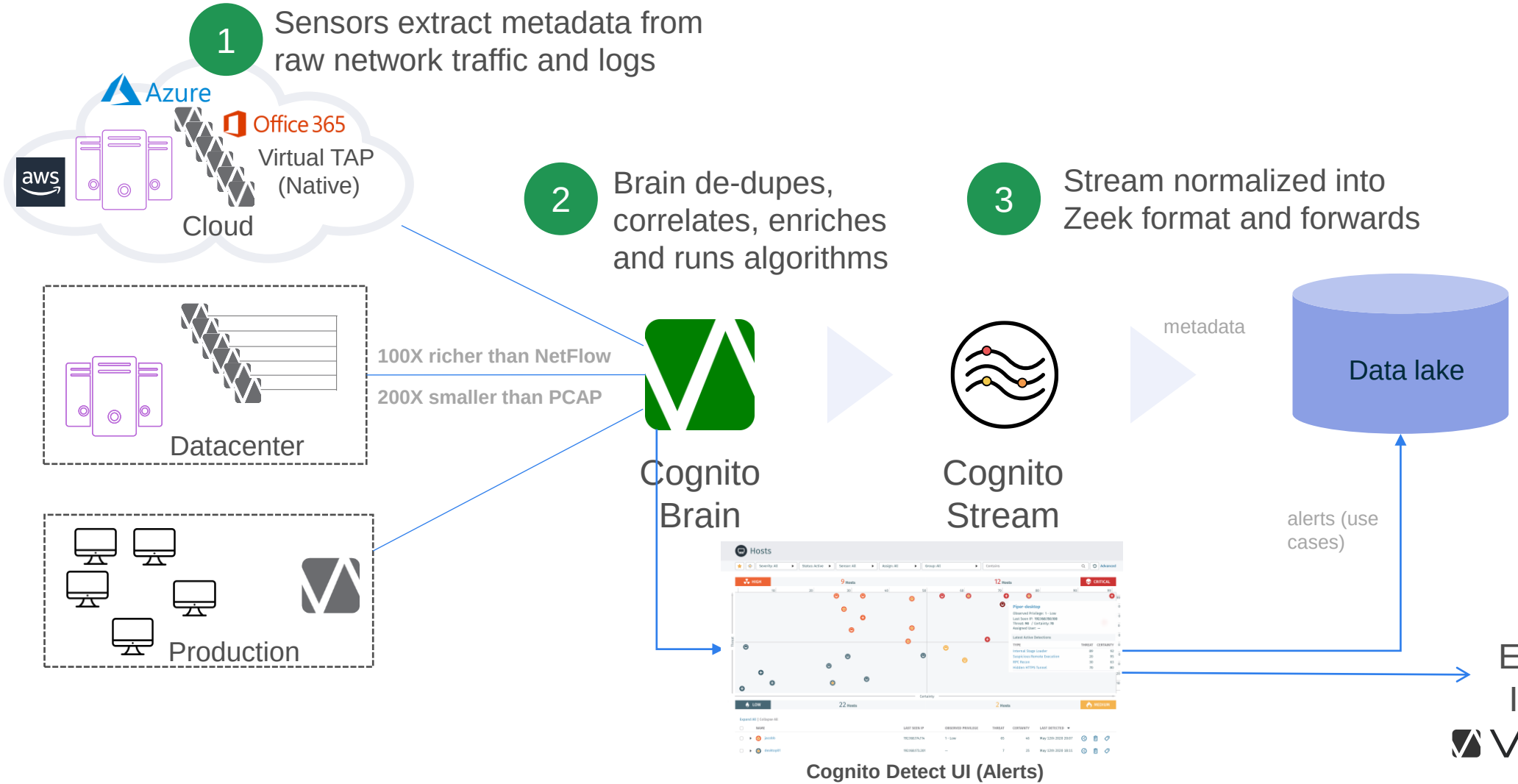
5 Investigate using rich Zeek-formatted metadata.

Easier and faster investigation using data 100x richer than Netflow and 200x smaller than full pcap

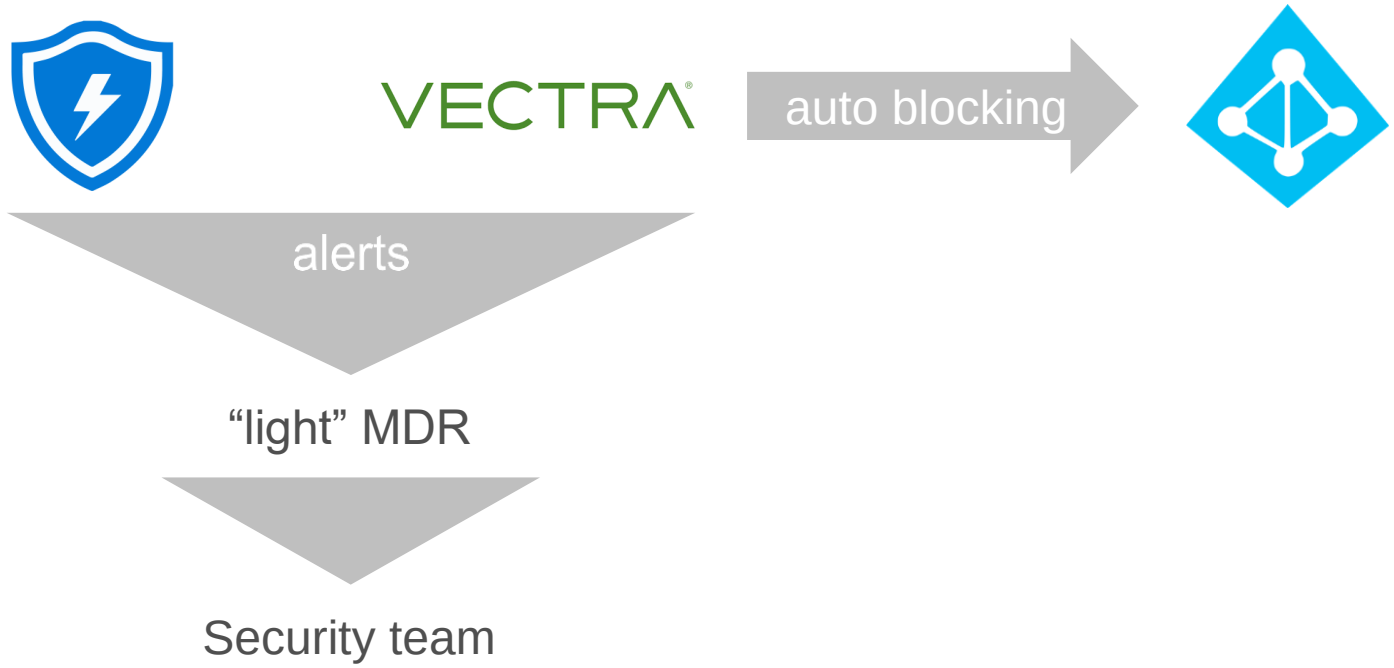


VECTRA

Vectra Deployment

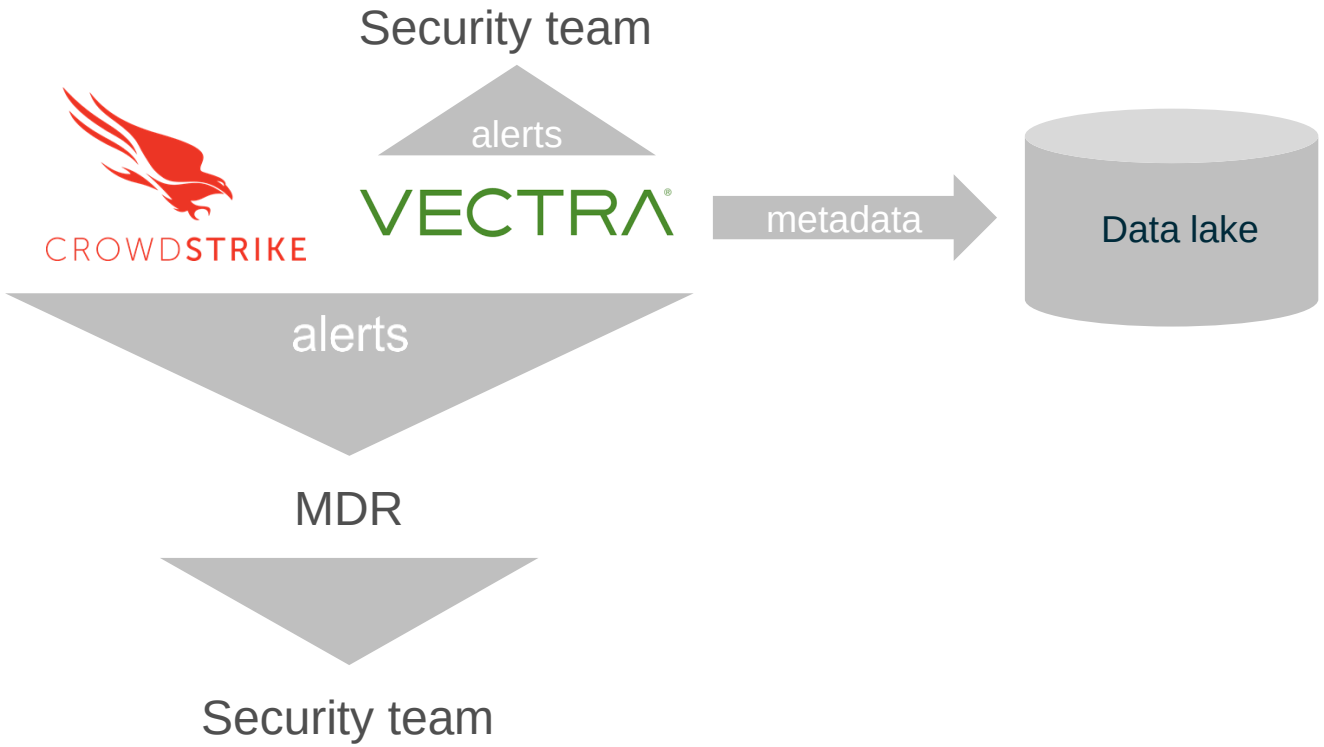


Case study 1: private hospital



Case study 2: Kantonsspital

Case study 3: Private Hospital group



Q&A

ahess@vectra.ai