VECTRA®

AI/ML XDR

Detect and Respond in Real-Time

Kelly Ross – Account Exec
kross@vectra.ai
210-601-5297

Steve Hill – Security Engineer
steve.hill@vectra.ai
571-969-4531

BOTTOM LINE UP FRONT (BLUF):

Vectra’s pioneering AI/ML, real-time cyber threat detection and response platform

- DCO surface area too large for traditional methods to be successful on their own.
- Security via Compliance hampering DCO and giving adversaries the advantage
  - Volt Typhoon operating for 5 years+
- Vectra brings benefits of AI/ML to threat detection/threat hunting
  - **Real-Time Visibility and Alerting** across Hybrid Cloud, Enterprise, DDIL and Tactical
  - Reduces altert noise by up to 85% vs signature-based products
  - Speeds decision making and response
  - Integrates and operates at **enterprise scale**
- USG, NGA, NAVY, SOCOM moved to rapid procurement to fill this gap

About Vectra:

- **Founded 2010** ; HQ San Jose, CA
    - 2000+ customers; IC, DoD, Civilian, Sis
- Easily overlay AI based security to address critical blind spot
    - **REAL TIME THREAT DETECTION and E/W VISIBILITY**
    - **Automating threat hunting** with contextualization and prioritization of threats
    - **AI User Behavior Analytics** – Identify insider threat/privilege mis-use or escalation
    - **Reduces alert noise by up to 85%** vs signature-based products

VECTRA®

THE PROBLEM STATEMENT

Finding the needle amongst needles

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

DISA RECOGNIZES THE NEED/OPPORTUNITY

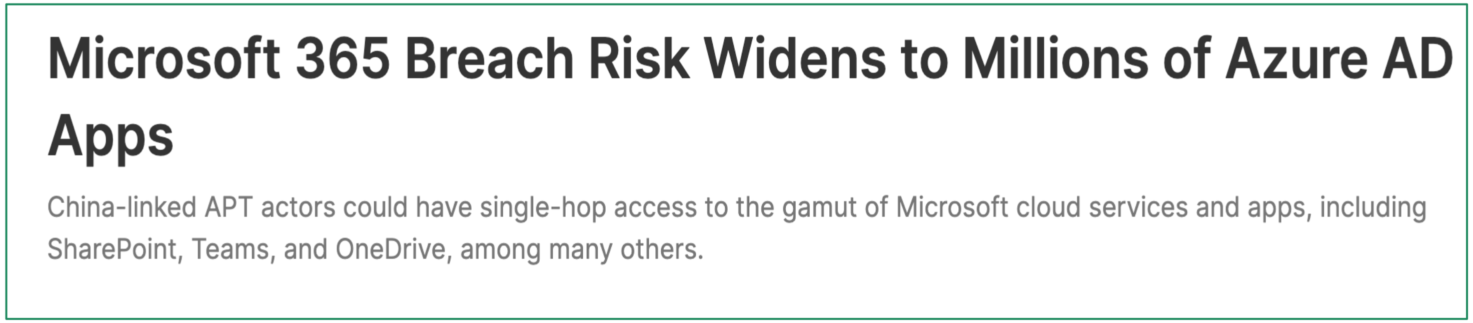
Recent RFI

The purpose of this RFI is to enhance DISA’s Defensive Cyber Operations (DCO) using Artificial Intelligence (AI) and Machine Learning (ML)…

As cyber threats proliferate – both in terms of numbers and sophistication – the ability of DISA to successfully perform the defensive cyber operations becomes more and more challenging. To overcome these challenges, DISA is interested in exploring the potential of applying commercial AI/ML models, tools, services, and best practices to augment and enhance its current DCO capabilities and methods.

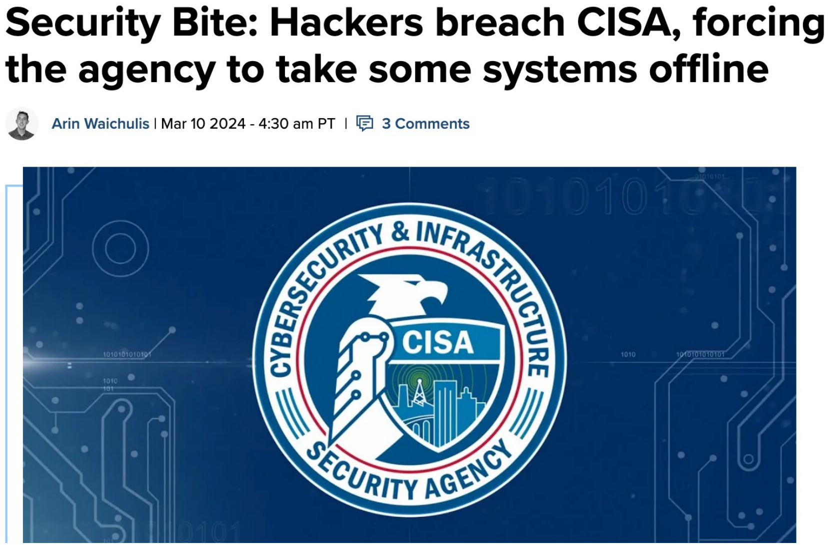
Source: DISA EM

EVERYONE IS UNDER SIEGE; NO ONE IS IMMUNE



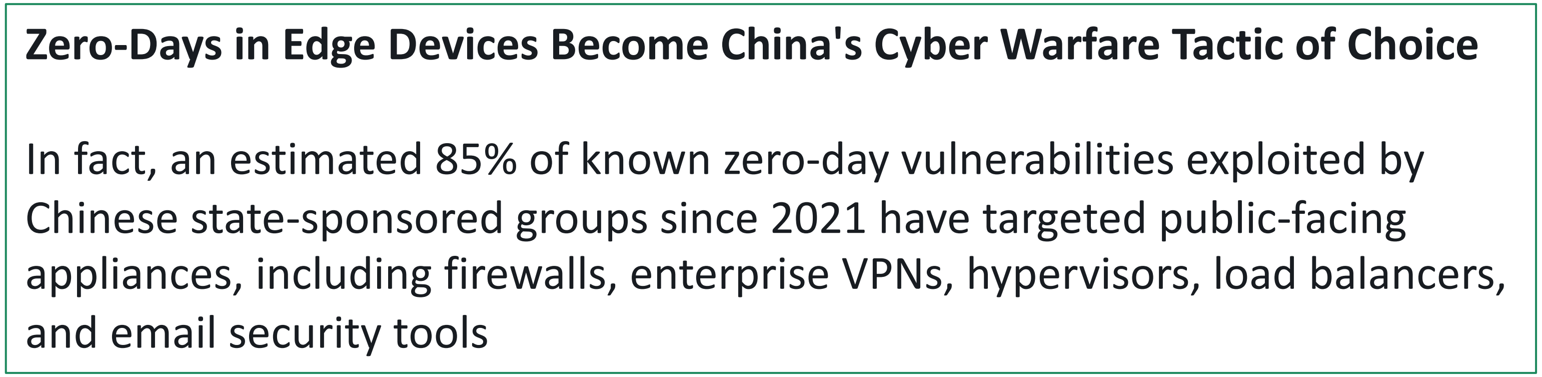
Microsoft 365 Breach Risk Widens to Millions of Azure AD Apps

China-linked APT actors could have single-hop access to the gamut of Microsoft cloud services and apps, including SharePoint, Teams, and OneDrive, among many others.



Security Bite: Hackers breach CISA, forcing the agency to take some systems offline

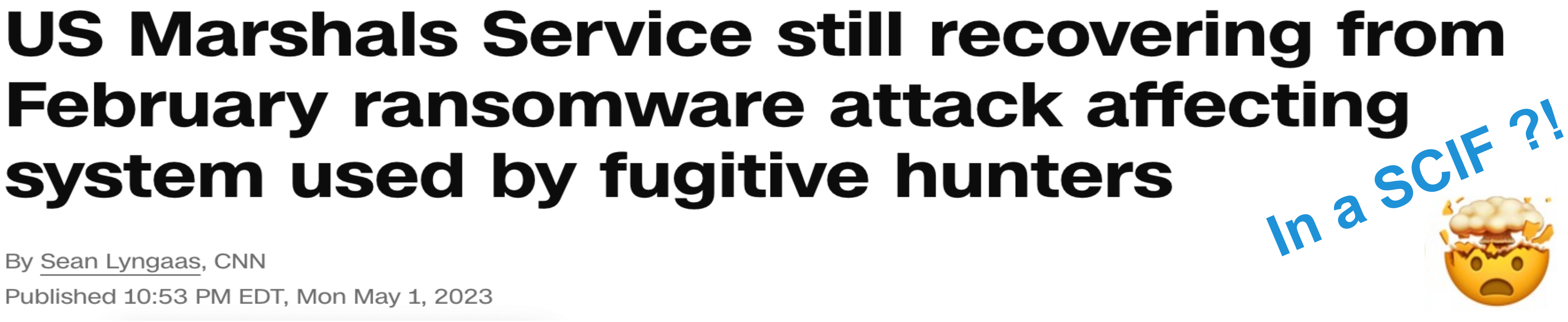
Arin Waichulis | Mar 10 2024 - 4:30 am PT | 3 Comments



Zero-Days in Edge Devices Become China's Cyber Warfare Tactic of Choice

In fact, an estimated 85% of known zero-day vulnerabilities exploited by Chinese state-sponsored groups since 2021 have targeted public-facing appliances, including firewalls, enterprise VPNs, hypervisors, load balancers, and email security tools

MORE ATTACKS IN MORE AUSTERE ENVIRONMENTS



US Marshals Service still recovering from February ransomware attack affecting system used by fugitive hunters

By Sean Lyngaas, CNN

Published 10:53 PM EDT, Mon May 1, 2023

In a SCIF ?! 🤯

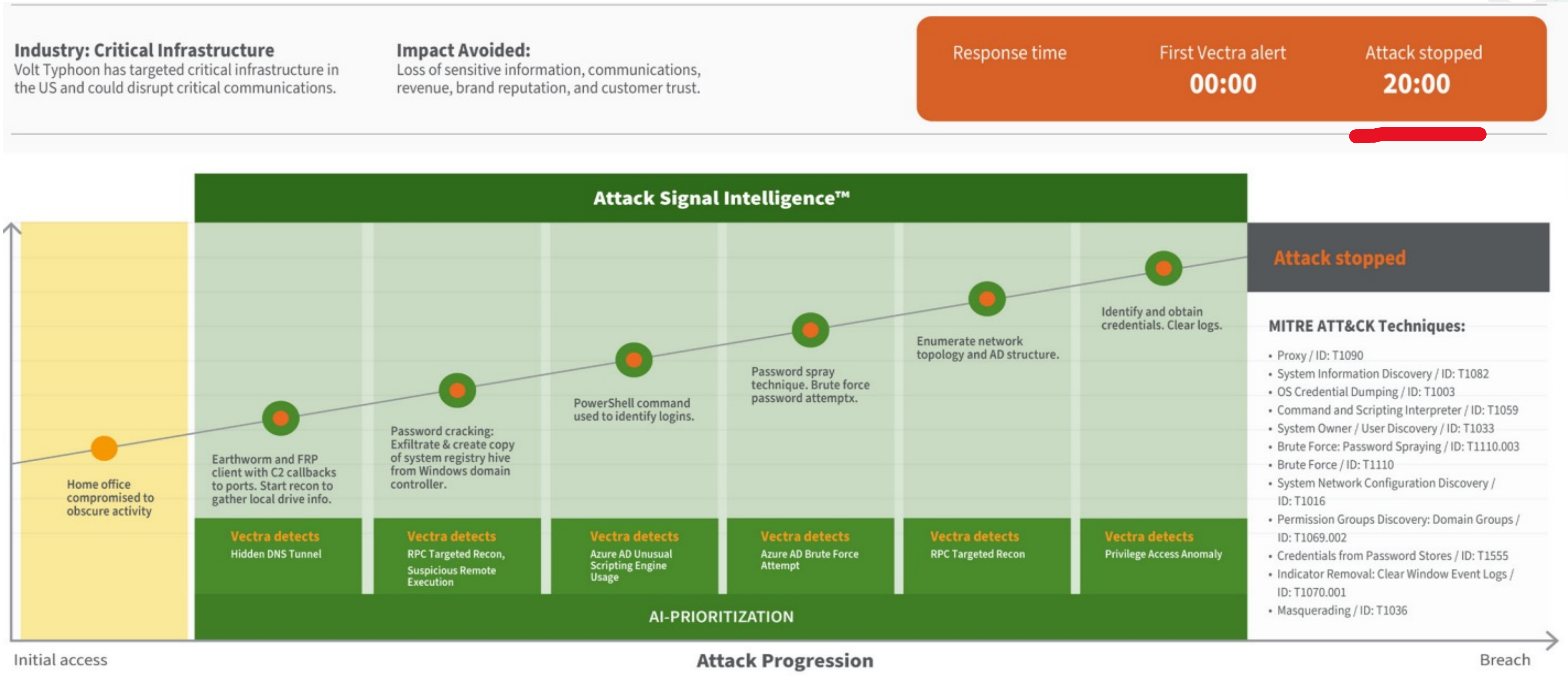
Volt Typhoon, one congressional official said, was essentially “a ticking time bomb” that could give China the power to interrupt or slow American military deployments or resupply operations by cutting off power, water and communications to U.S. military bases.

Source - NY Times

Operating since 2019 ?! 😱

STOP THE INTRUDER BY UNDERSTANDING THE INTRUDER

Drastically Reduce Mean Time to Remediate



Industry: Critical Infrastructure
Volt Typhoon has targeted critical infrastructure in the US and could disrupt critical communications.

Impact Avoided:
Loss of sensitive information, communications, revenue, brand reputation, and customer trust.

Response time	First Vectra alert	Attack stopped
	00:00	20:00

Attack Signal Intelligence™

- Home office compromised to obscure activity
- Earthworm and FRP client with C2 callbacks to ports. Start recon to gather local drive info. — **Vectra detects** Hidden DNS Tunnel
- Password cracking: Exfiltrate & create copy of system registry hive from Windows domain controller. — **Vectra detects** RPC Targeted Recon, Suspicious Remote Execution
- PowerShell command used to identify logins. — **Vectra detects** Azure AD Unusual Scripting Engine Usage
- Password spray technique. Brute force password attemptx. — **Vectra detects** Azure AD Brute Force Attempt
- Enumerate network topology and AD structure. — **Vectra detects** RPC Targeted Recon
- Identify and obtain credentials. Clear logs. — **Vectra detects** Privilege Access Anomaly

AI-PRIORITIZATION

Attack stopped

MITRE ATT&CK Techniques:

- Proxy / ID: T1090
- System Information Discovery / ID: T1082
- OS Credential Dumping / ID: T1003
- Command and Scripting Interpreter / ID: T1059
- System Owner / User Discovery / ID: T1033
- Brute Force: Password Spraying / ID: T1110.003
- Brute Force / ID: T1110
- System Network Configuration Discovery / ID: T1016
- Permission Groups Discovery: Domain Groups / ID: T1069.002
- Credentials from Password Stores / ID: T1555
- Indicator Removal: Clear Window Event Logs / ID: T1070.001
- Masquerading / ID: T1036

VECTRA®

STRETCH GOALS IN DCO

The 1-10-60 Framework

THE 1-10-60 RULE/FRAMEWORK

Achieve cyber resiliency

- Introduced by Dmitri Alperovitch, the founder of Crowd Strike

- Detect Threats within the first minute
  - Most DCO architectures are reliant on logs and post incident damage control
  - Requires **real-time** detection capabilities lacking in most DCO architectures

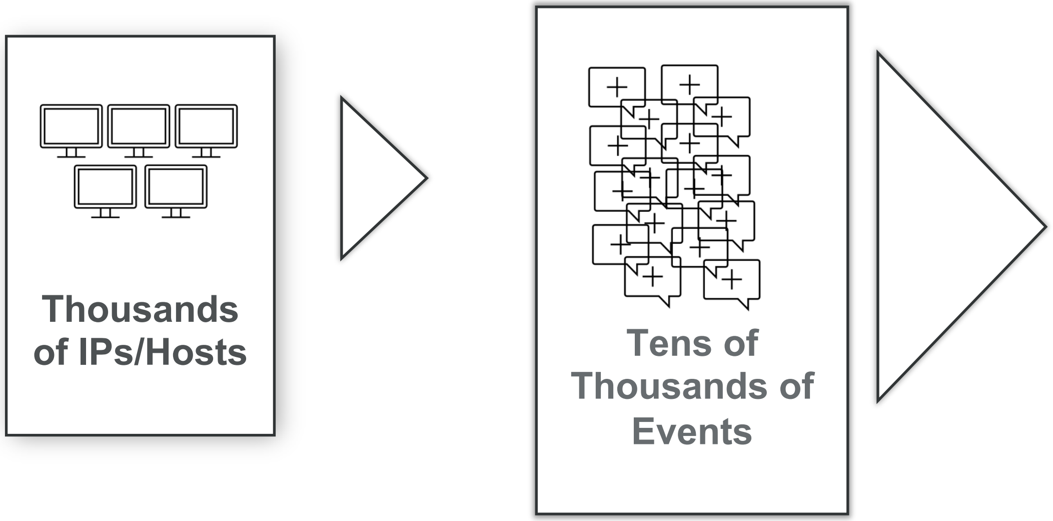
- Understand the nature of the threat within 10 minutes
  - Typically requires correlation across multiple tools/systems
  - Signature based systems are playing catchup

- Respond to the threat within 60 mins
  - Requires correlation, prioritization and certainty
  - Fully contextualized threat intelligence to understand the behavior and potential impact

Average breakout time of cyber attack is less than 60 mins

ALERT OVERLOAD = REDUCED SIEM VALUE

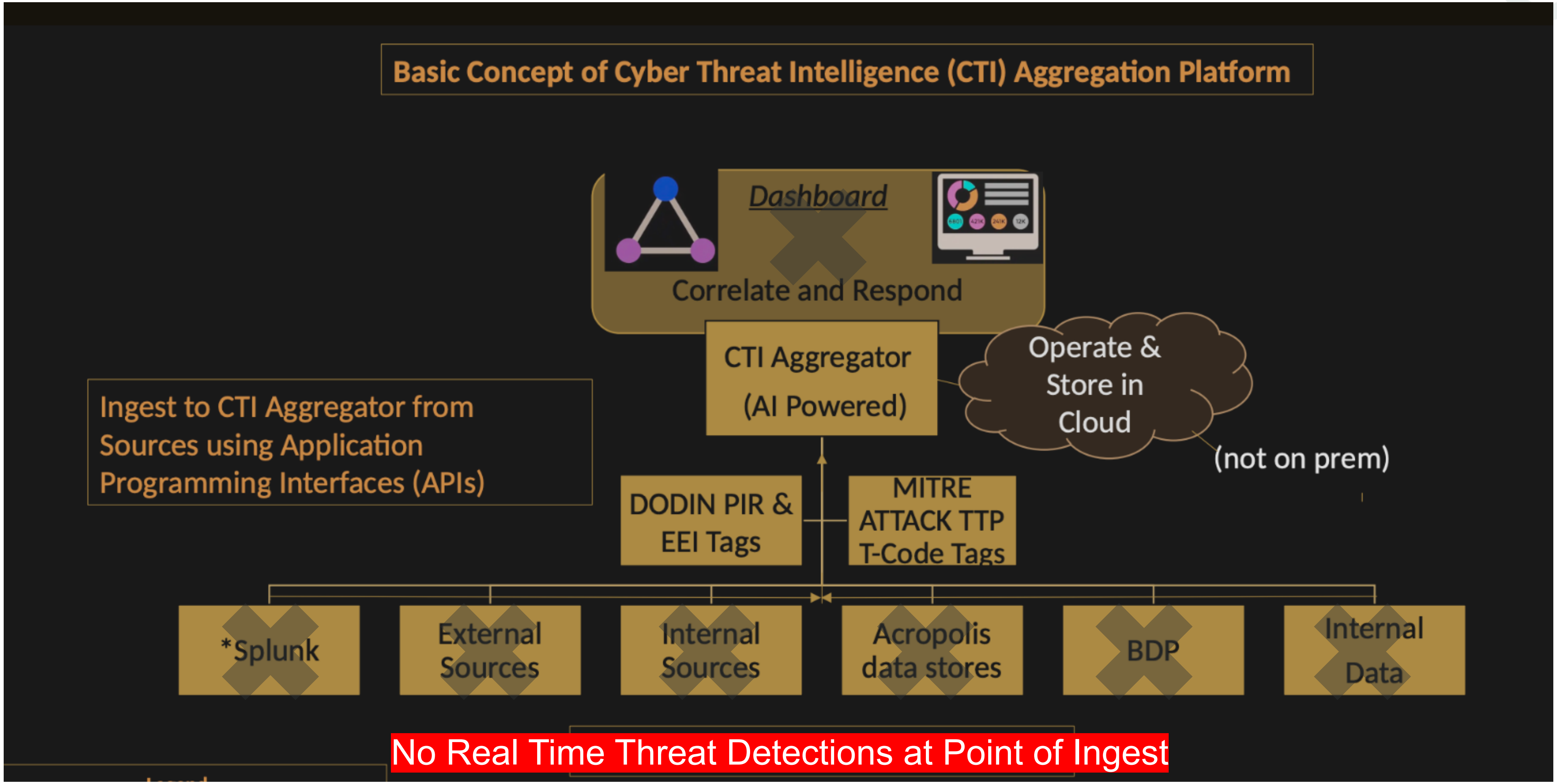
Legacy sensors and signature-based alerting



Thousands of IPs/Hosts

Tens of Thousands of Events

BLIND SPOTS IN THREAT DETECTION = DAMAGE CONTROL



Basic Concept of Cyber Threat Intelligence (CTI) Aggregation Platform

Dashboard

Correlate and Respond

CTI Aggregator

(AI Powered)

Operate & Store in Cloud

(not on prem)

Ingest to CTI Aggregator from Sources using Application Programming Interfaces (APIs)

DODIN PIR & EEI Tags

MITRE ATTACK TTP T-Code Tags

*Splunk

External Sources

Internal Sources

Acropolis data stores

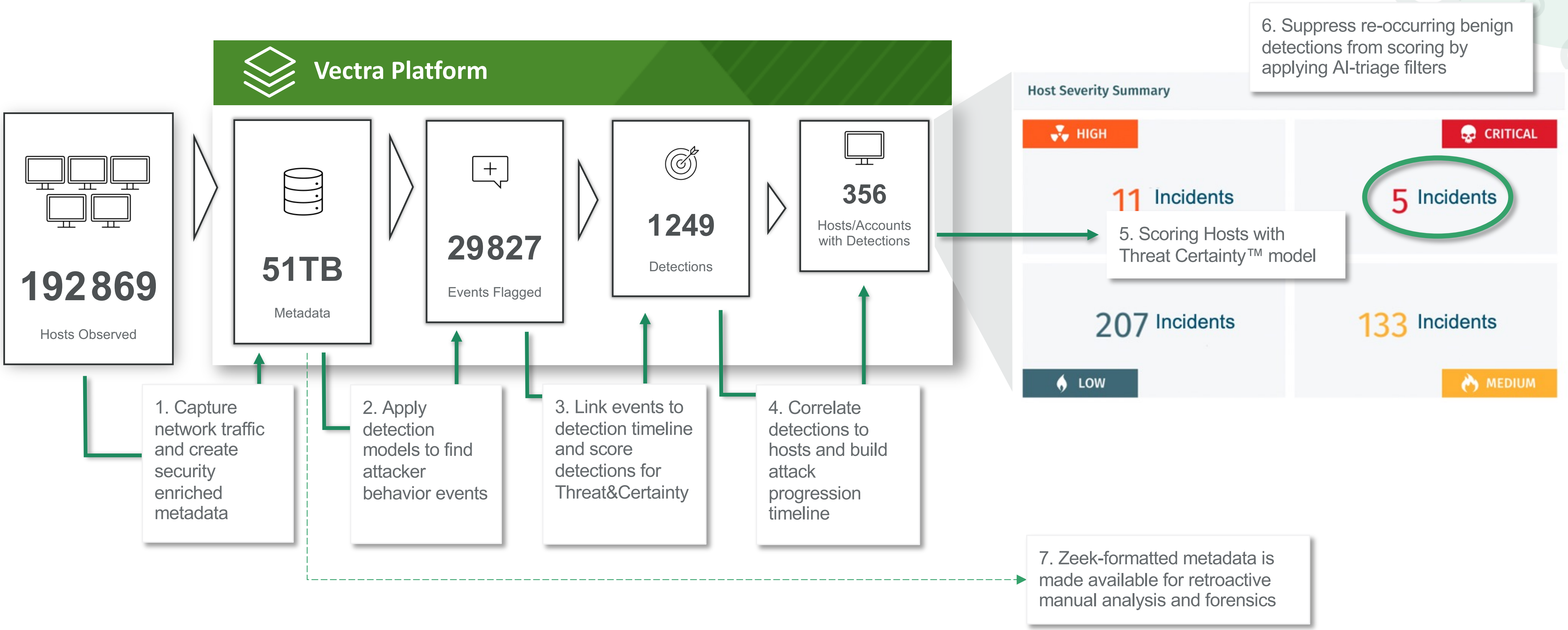
BDP

Internal Data

No Real Time Threat Detections at Point of Ingest

FILTER OUT THE NOISE FOR UNRIVALED SIGNAL CLARITY

AI-driven Prioritization at scale through intelligent automation



1. Capture network traffic and create security enriched metadata

2. Apply detection models to find attacker behavior events

3. Link events to detection timeline and score detections for Threat&Certainty

4. Correlate detections to hosts and build attack progression timeline

5. Scoring Hosts with Threat Certainty™ model

6. Suppress re-occurring benign detections from scoring by applying AI-triage filters

7. Zeek-formatted metadata is made available for retroactive manual analysis and forensics

Source: Customer environment in a large multinational enterprise, during a 30 day period

CORRELATED ACTIONABLE EVENT DATA

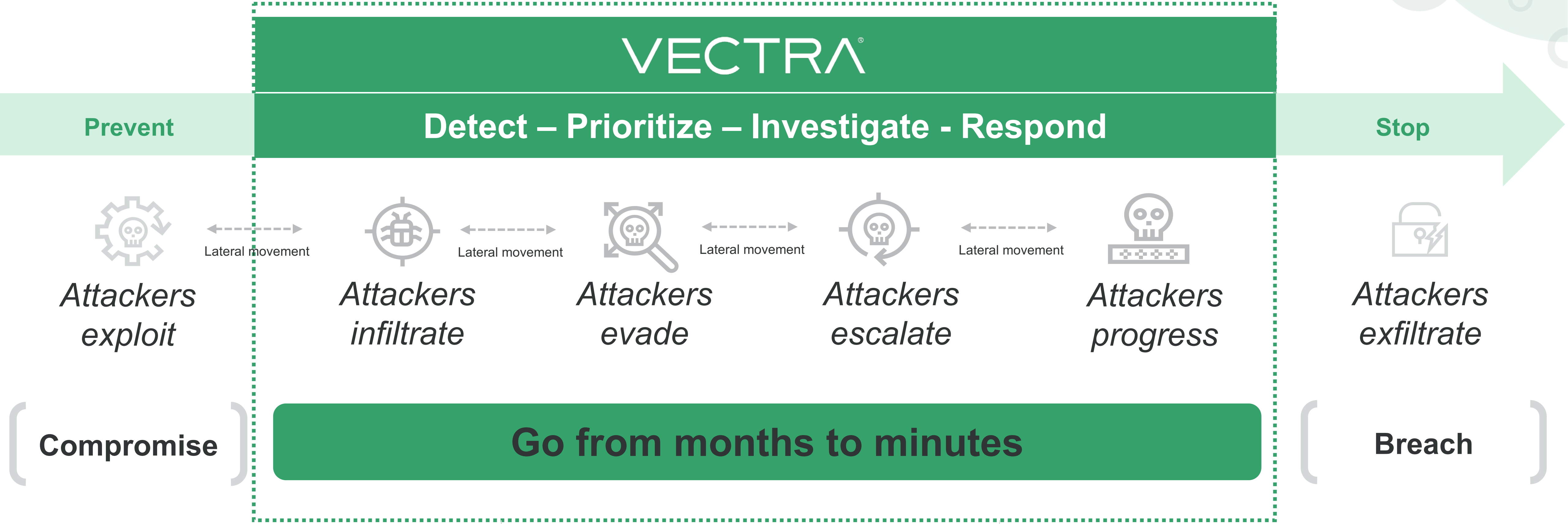
Reduce alert overload – Reduce MTTR – Reduce Dwell Time

SAMPLE EVENT LOG

```
<13>Jul 9 07:54:46 vectranetworks.vectra.test vectra_cef -: CEF:0|Vectra
Networks|X Series|4.2| smb_brute_force|SMB Brute-Force|7|externalId=9481
cat=LATERAL MOVEMENT dvc=10.97.41.41 dvchost=10.97.41.41
shost=hostname123.example.com src=10.125.64.136 flexNumber1Label=threat
flexNumber1=70 flexNumber2Label=certainty flexNumber2=59 cs4Label=Vectra
Event URL cs4=https:// www.Qradar.test/paths/resources1.ext cs5Label=triaged
cs5=False dst=10.160.0.145 dhost= proto= dpt=445 out=None in=None
start=1531119062000 end=1531119099000
```

MAKING **1-10-60** A REALITY

Detect threats in **Real Time**



VECTRA

Prevent

Detect – Prioritize – Investigate - Respond

Stop

Attackers exploit

Lateral movement

Attackers infiltrate

Lateral movement

Attackers evade

Lateral movement

Attackers escalate

Lateral movement

Attackers progress

Attackers exfiltrate

Compromise

Go from months to minutes

Breach

197%
Improved visibility into actual threats

85%
Reduction in alerts

60 days to 4 hours
Reduce mean time to remediation

VECTRA®

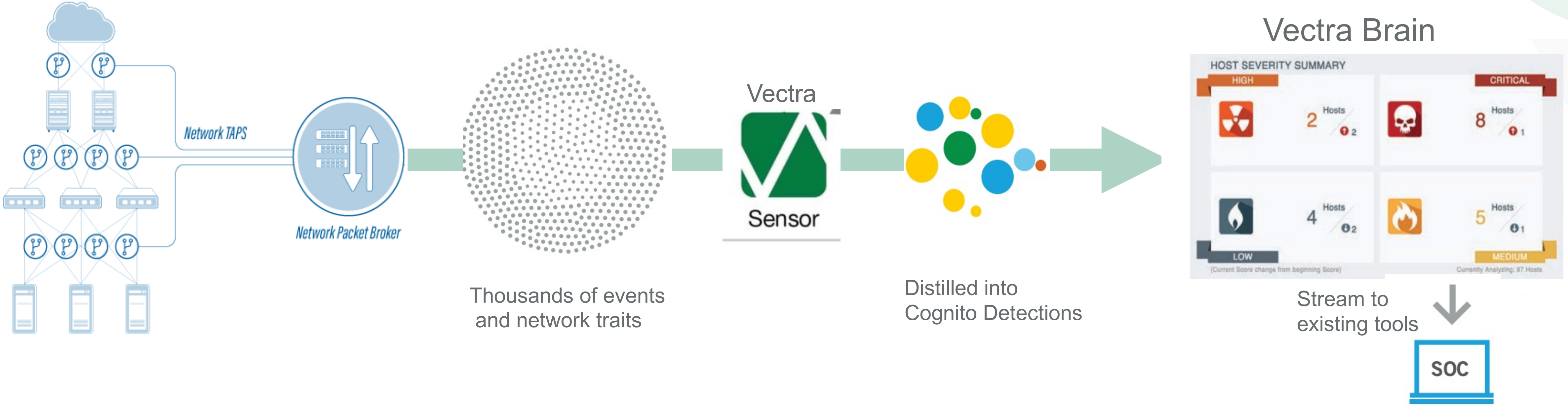
AI behind Vectra AI

Key Takeaways from Vectra's Approach

True AI & ML

- **Natively Signatureless*…**
  - **Models and hashes change, underlying behaviors are constant**
  - **Can utilize Suricata signatures to drive prioritization**
- **Agentless…**
  - **Passive on SPANs/packet brokers & in Azure/AWS Gov**
- **Decryptionless…**
  - **Underlying payload not necessary to detect, purely TCP header behaviors**

VECTRA: PLATFORM WALK THROUGH



Vectra Brain

HOST SEVERITY SUMMARY

HIGH 2 Hosts ↑2

CRITICAL 8 Hosts ↑1

LOW 4 Hosts ↓2

MEDIUM 5 Hosts ↓1

(Current Score change from beginning Score)

Currently Analyzing: 87 Hosts

Thousands of events and network traits

Distilled into Cognito Detections

Stream to existing tools

1. Capture

Capture relevant data everywhere without agents.

2. Enrich

Pair security research and data science to enrich the data.

3. Apply

Flexibly apply data to your use case.

FINDING ATTACK SIGNAL IS OUR DNA

Over a decade of innovation in using AI to find attack signal in data

Security research to understand how **attackers** think + **Data** that reveals attacks + **AI models** custom-developed for each attack type + **Real-time analytics** at enterprise scale + Automated **feedback** loop

35 Patents

150+ models spanning neural networks, unsupervised, novelty

12 MITRE References

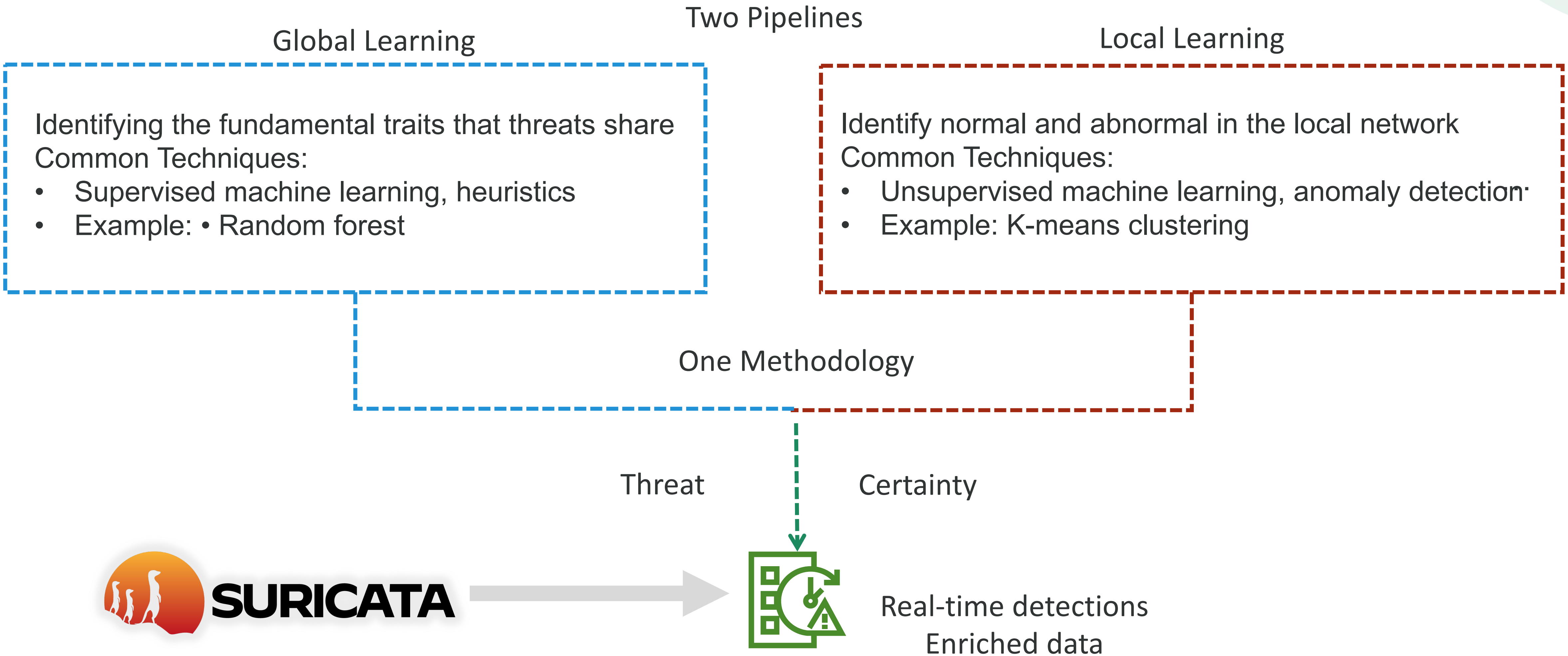
Most patent references of any security vendor

Network Effect

Continuous feedback from 1,000+ customers

AI-driven Attack Signal Intelligence TM

Vectra AI Difference: Two pipelines. One methodology.



Two Pipelines

Global Learning

Identifying the fundamental traits that threats share
Common Techniques:

- Supervised machine learning, heuristics
- Example: • Random forest

Local Learning

Identify normal and abnormal in the local network
Common Techniques:

- Unsupervised machine learning, anomaly detection
- Example: K-means clustering

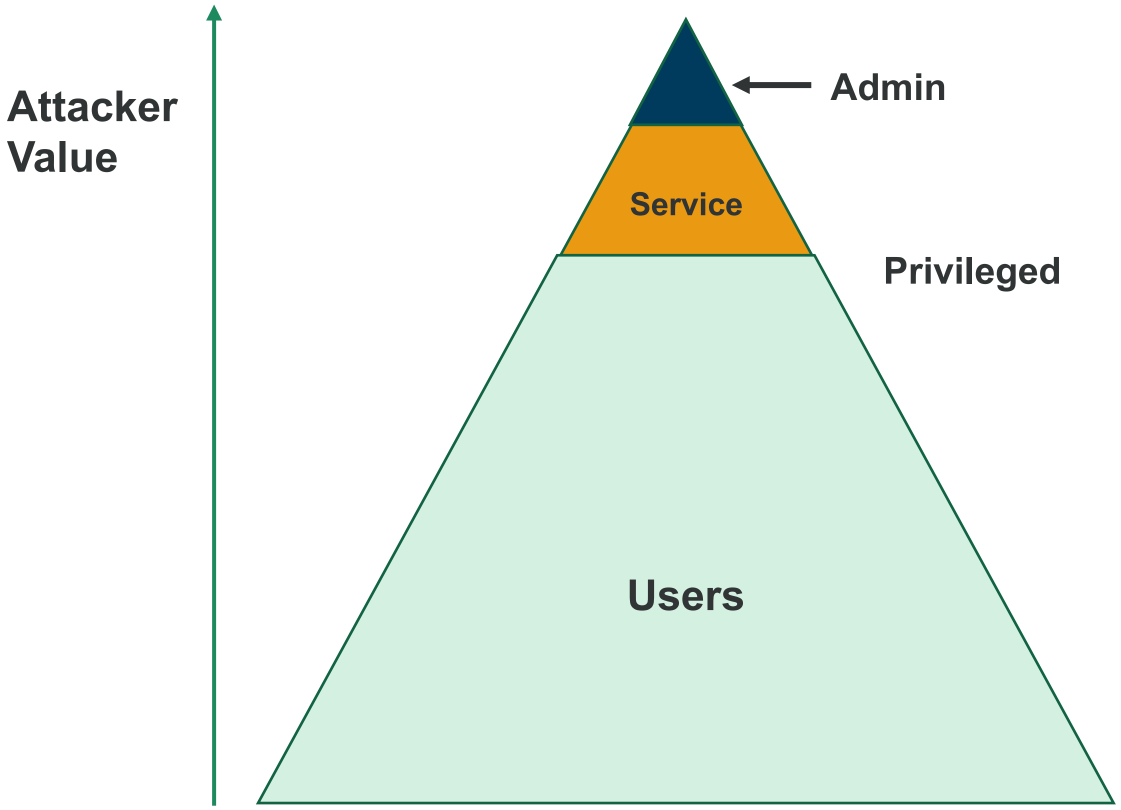
One Methodology

Threat

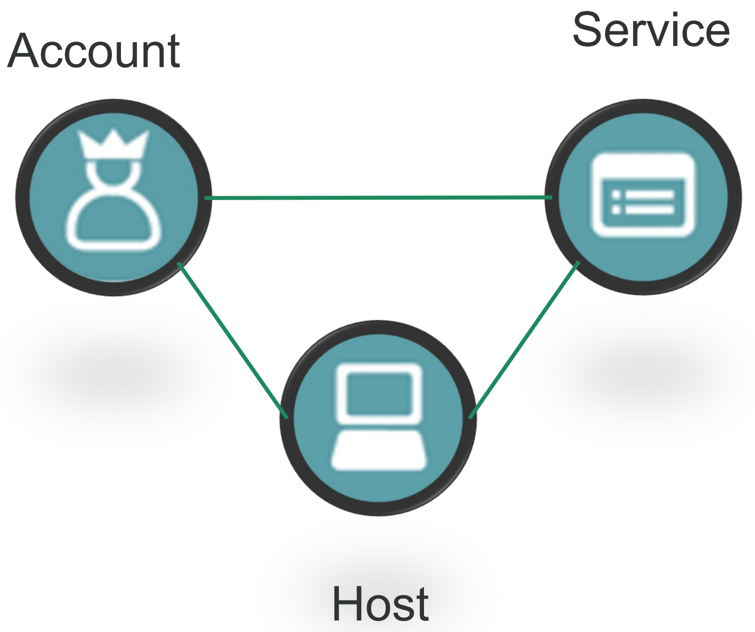
Certainty

Real-time detections
Enriched data

CONTEXTULIZING ACCESS CONTROL



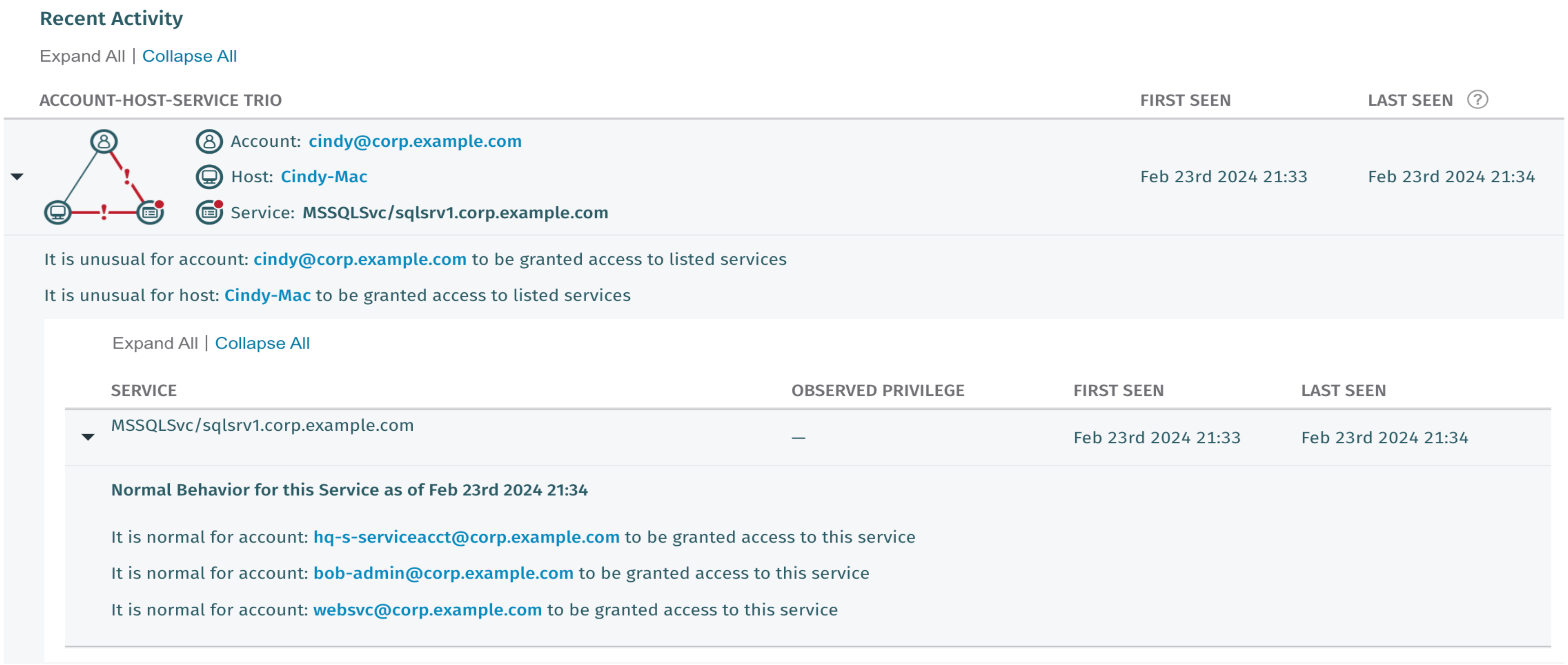
The admin with medium observed privilege that starts to access unusual high-privilege services will set off alarm bells in PAA. In a granted-privilege universe, this activity would be authorized.



- Map relationships
- Observe and learn privilege
- Detect useful anomalies

ACCELERATE ZERO TRUST FOR PRIVILEGED ACCOUNTS

85% of attacks use stolen accounts – stop them now



Recent Activity

Expand All | Collapse All

ACCOUNT-HOST-SERVICE TRIO	FIRST SEEN	LAST SEEN ?
Account: cindy@corp.example.com Host: Cindy-Mac Service: MSSQLSvc/sqlsrv1.corp.example.com	Feb 23rd 2024 21:33	Feb 23rd 2024 21:34

It is unusual for account: cindy@corp.example.com to be granted access to listed services

It is unusual for host: Cindy-Mac to be granted access to listed services

Expand All | Collapse All

SERVICE	OBSERVED PRIVILEGE	FIRST SEEN	LAST SEEN
MSSQLSvc/sqlsrv1.corp.example.com	—	Feb 23rd 2024 21:33	Feb 23rd 2024 21:34

Normal Behavior for this Service as of Feb 23rd 2024 21:34

It is normal for account: hq-s-serviceacct@corp.example.com to be granted access to this service

It is normal for account: bob-admin@corp.example.com to be granted access to this service

It is normal for account: websvc@corp.example.com to be granted access to this service

VECTRA®

ENHANCE DCO WITH AI/ML

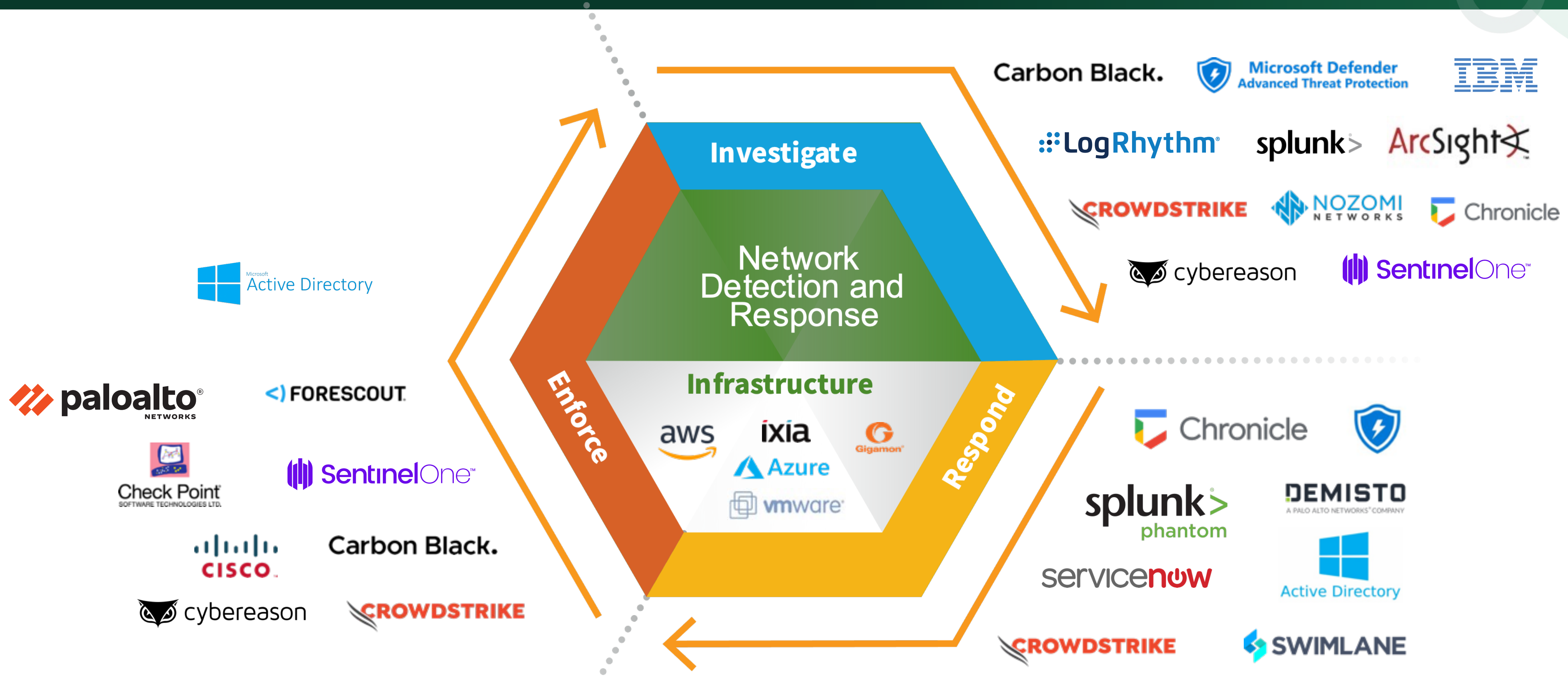
Ease of deployment and Integration

INCREASE DCO EFFICIENCY

- Align to the 1-10-60 framework
  - Close the MTTR gaps between 24/7 and non-24/7 DCO teams
  - Make DCO more efficient and effective

- Improve Red Team’s positive impact on security capability and posture
  - Track red team/pen testing campaigns
  - Demonstrate ability to thwart malicious advesarial campaigns

INTEGRATES WITH SECURITY ECHOSYSTEM



Native integrations including EDR, SIEMs and orchestration tools

Open Robust API for customizable integrations

VECTRA®

RECAP

RECAP

Visibility across cloud, DC, and network

- Includes SaaS apps, IaaS, data center, enterprise network, and IoT devices

Identify threats targeting users and hosts, not just detections

- 34x reduction in workload for Tier 1 analysts
- Automate response to network & endpoints

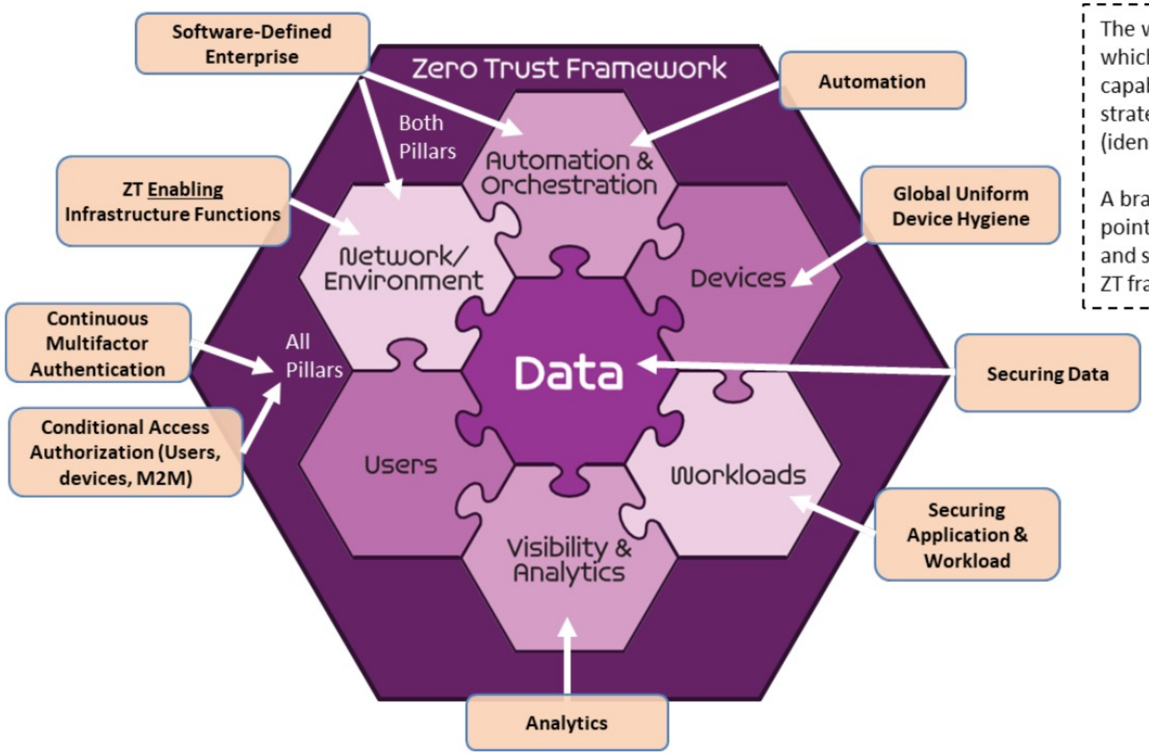
Ultra high signal-noise ratio to focus on what matters

- Identify attacker behavior, not signature or anomaly-based detections
- Even when the traffic is encrypted

VECTRA®

Vectra Maps to DoD Zero Trust Principles

Direct correlation to security disciplines


Software-Defined Enterprise
Zero Trust Framework
Automation
Both Pillars
Automation & Orchestration
ZT Enabling Infrastructure Functions
Global Uniform Device Hygiene
Network/ Environment
Devices
Continuous Multifactor Authentication
All Pillars
Data
Securing Data
Conditional Access Authorization (Users, devices, M2M)
Users
Workloads
Securing Application & Workload
Visibility & Analytics
Analytics

The white arrows show which ZT aggregated capability acts on a group of strategic resources (identified as ZT Pillars).

A branch of capabilities may point to more than one pillar and some point to the entire ZT framework.

4. Data
4.4 Data Monitoring and Sensing

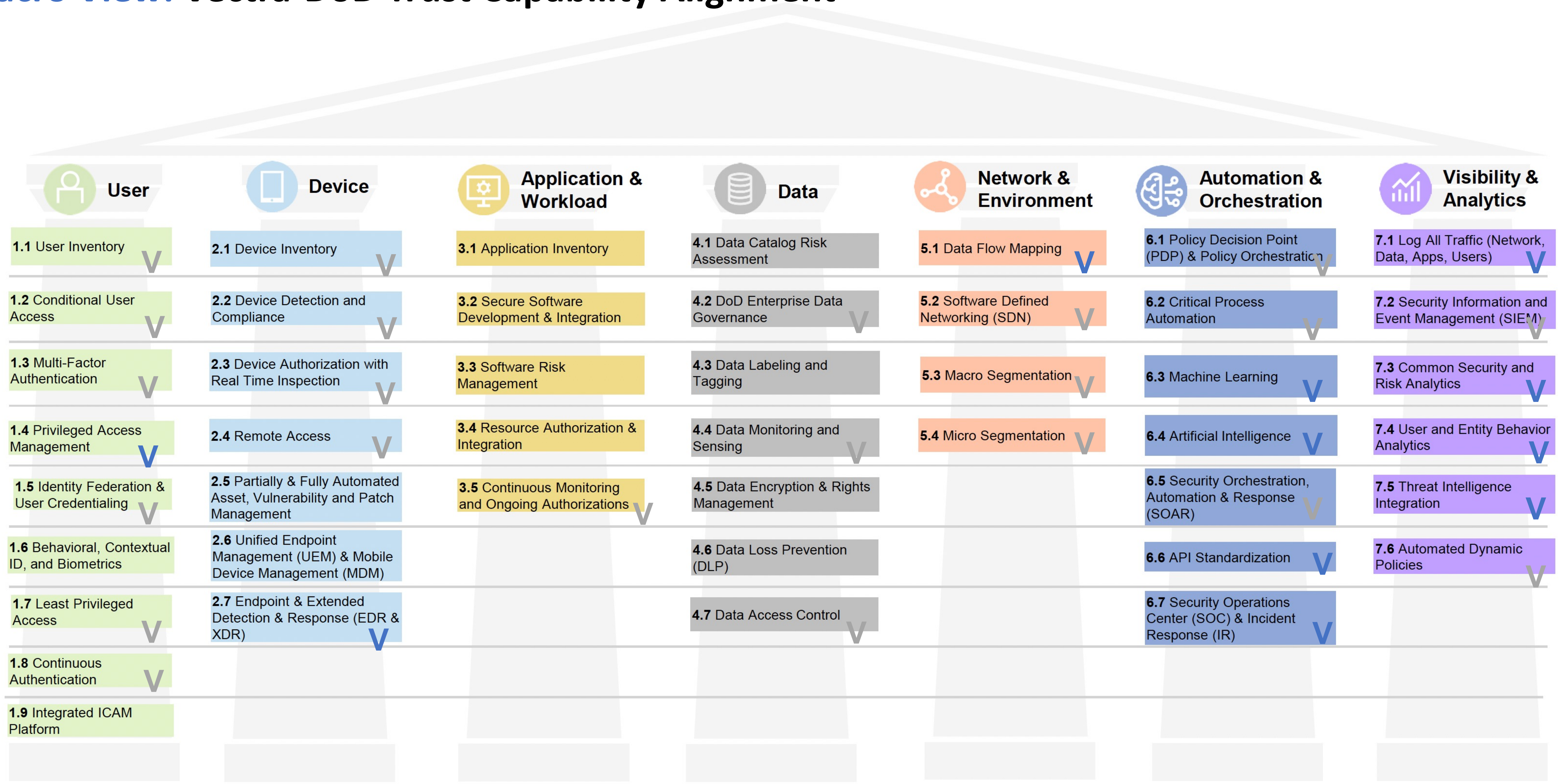
6. Automation & Orchestration
6.3 Machine Learning
6.4 Artificial Intelligence
6.7 Security Operations Center (SOC) & Incident Response (IR)

7. Visibility & Analytics
7.3 Common Security and Risk Analytics
7.4 User and Entity Behavior Analytics
7.5 Threat Intelligence Integration

ZT of the Future
We Support On-Prem Networks Today
We Support Cloud Today
We Support Hybrid Cloud Today
We Support Multi Cloud Today

ZT ARCHITECTURE

Macro View: Vectra-DoD Trust Capability Alignment



User

- **1.1** User Inventory V
- **1.2** Conditional User Access V
- **1.3** Multi-Factor Authentication V
- **1.4** Privileged Access Management V
- **1.5** Identity Federation & User Credentialing V
- **1.6** Behavioral, Contextual ID, and Biometrics
- **1.7** Least Privileged Access V
- **1.8** Continuous Authentication V
- **1.9** Integrated ICAM Platform

Device

- **2.1** Device Inventory V
- **2.2** Device Detection and Compliance V
- **2.3** Device Authorization with Real Time Inspection V
- **2.4** Remote Access V
- **2.5** Partially & Fully Automated Asset, Vulnerability and Patch Management
- **2.6** Unified Endpoint Management (UEM) & Mobile Device Management (MDM)
- **2.7** Endpoint & Extended Detection & Response (EDR & XDR) V

Application & Workload

- **3.1** Application Inventory
- **3.2** Secure Software Development & Integration
- **3.3** Software Risk Management
- **3.4** Resource Authorization & Integration
- **3.5** Continuous Monitoring and Ongoing Authorizations V

Data

- **4.1** Data Catalog Risk Assessment
- **4.2** DoD Enterprise Data Governance V
- **4.3** Data Labeling and Tagging
- **4.4** Data Monitoring and Sensing V
- **4.5** Data Encryption & Rights Management
- **4.6** Data Loss Prevention (DLP)
- **4.7** Data Access Control V

Network & Environment

- **5.1** Data Flow Mapping V
- **5.2** Software Defined Networking (SDN) V
- **5.3** Macro Segmentation V
- **5.4** Micro Segmentation V

Automation & Orchestration

- **6.1** Policy Decision Point (PDP) & Policy Orchestration V
- **6.2** Critical Process Automation V
- **6.3** Machine Learning V
- **6.4** Artificial Intelligence V
- **6.5** Security Orchestration, Automation & Response (SOAR) V
- **6.6** API Standardization V
- **6.7** Security Operations Center (SOC) & Incident Response (IR) V

Visibility & Analytics

- **7.1** Log All Traffic (Network, Data, Apps, Users) V
- **7.2** Security Information and Event Management (SIEM) V
- **7.3** Common Security and Risk Analytics V
- **7.4** User and Entity Behavior Analytics V
- **7.5** Threat Intelligence Integration V
- **7.6** Automated Dynamic Policies V

Vectra Meets

Vectra Supports/Integrated