VECTRA®
SECURITY THAT THINKS

Identify & Neutralize the Insider: Vectra AI Detection & Metadata Traffic Analysis

Hybrid and Multi-cloud Threat Detection and Response
with AI-driven Attack Signal Intelligence™

Zachary Vaughn| Director, Federal Security Engineering | zvaughn@Vectra.ai | 202-288-2098

Agenda

- Introduction
- Background on Vectra AI: Why, What and How
- Let’s talk about AI
- Uncovering a novel Insider Threat
- Taking Things Further
- Q & A

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

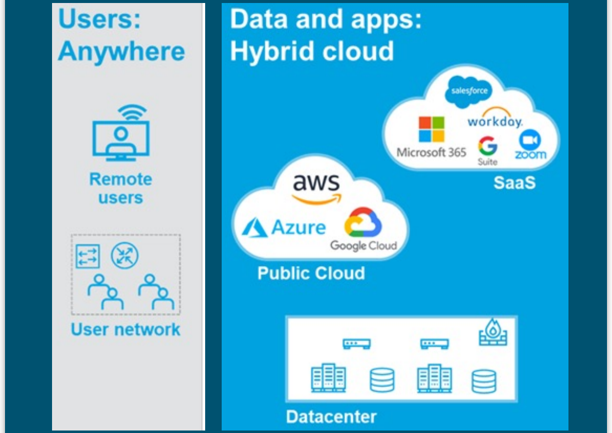
spiral of more

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

More SOC unknowns

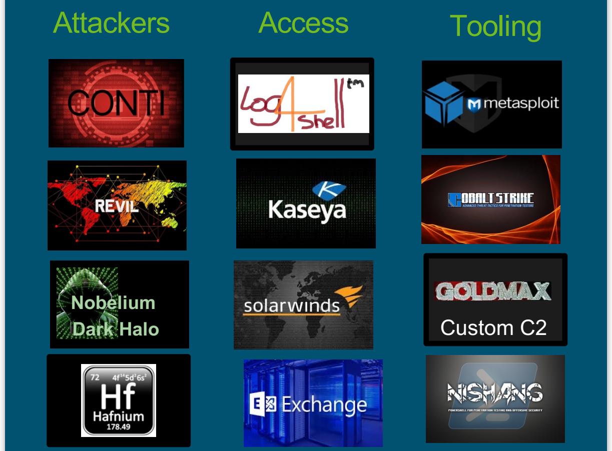
The “we don’t knows” of hybrid threat detection and response

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]

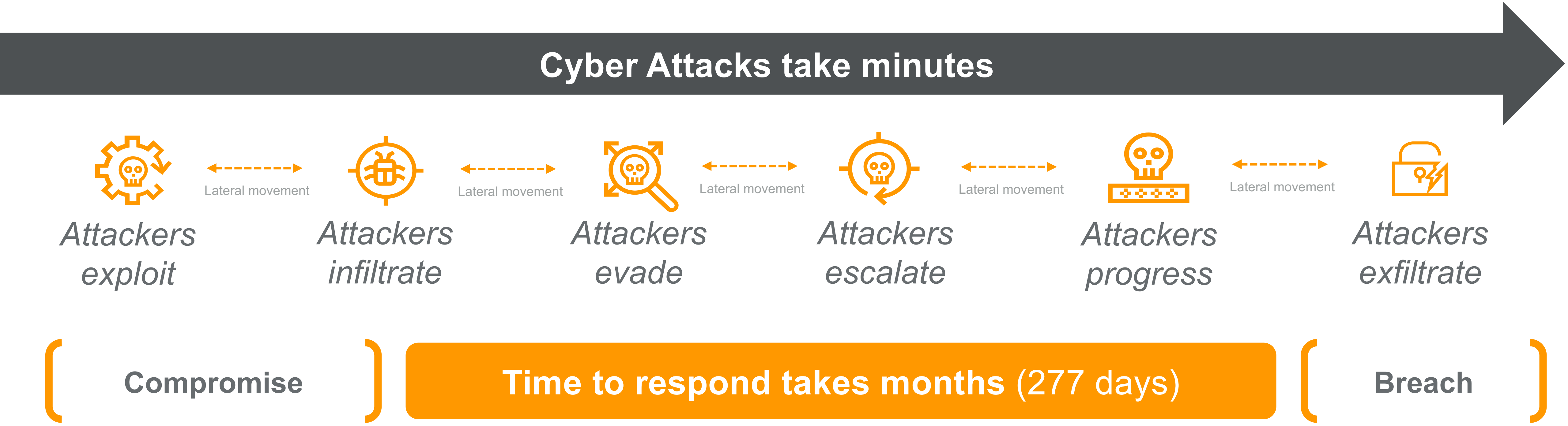
45% Cloud-based breaches [3]

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

More SOC latency, inefficiency

When cyber-attacks take minutes, response shouldn't take months



Cyber Attacks take minutes

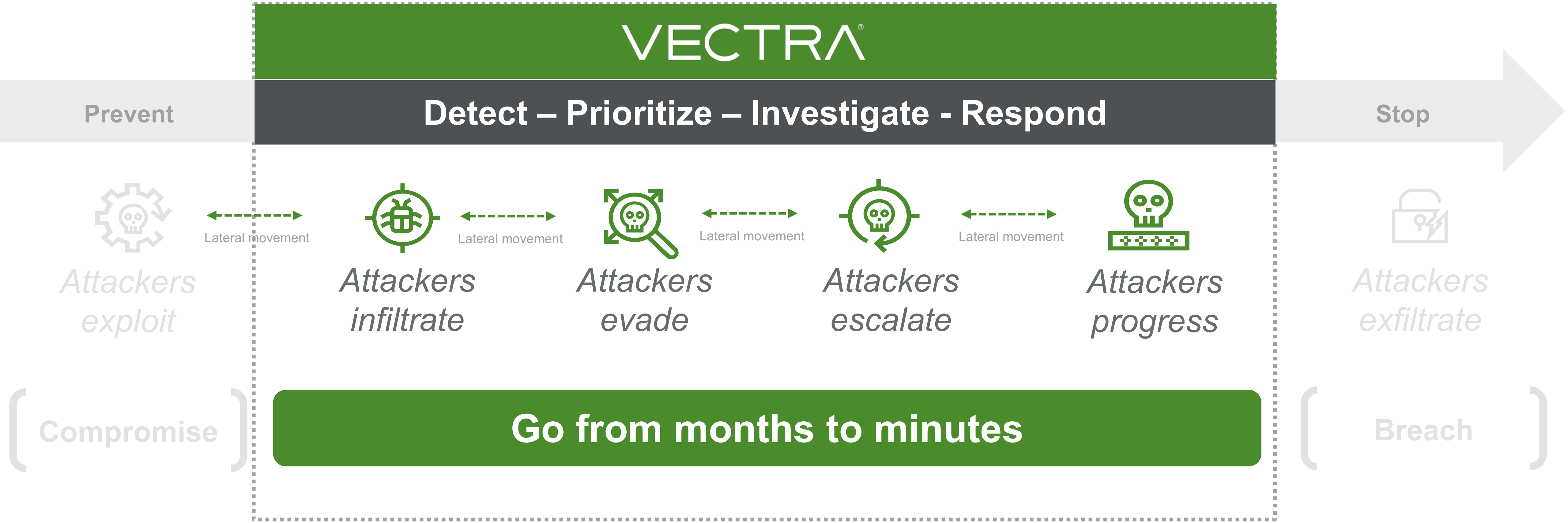
Attackers exploit ← Lateral movement → *Attackers infiltrate* ← Lateral movement → *Attackers evade* ← Lateral movement → *Attackers escalate* ← Lateral movement → *Attackers progress* ← Lateral movement → *Attackers exfiltrate*

[**Compromise**] **Time to respond takes months** (277 days) [**Breach**]

Source: IBM Security Cost of a Data Breach 2022

Vectra solves for the unknowns

Remove latency, improve SOC efficiency



VECTRA

Prevent

Detect – Prioritize – Investigate - Respond

Stop

Go from months to minutes

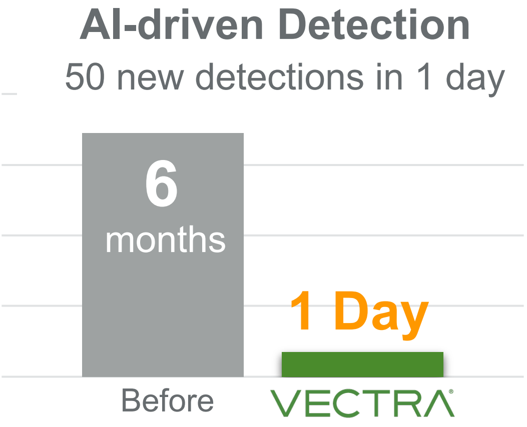
“Prevention is ideal, but Detection and Response is a must” - SANS

Vectra delivers SOC Efficiency

Case Study: Financial Services

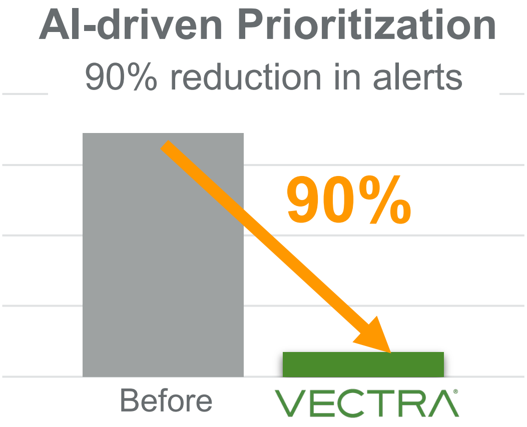
Blackstone

> *“**Vectra’s platform** has helped us strengthen our cybersecurity defense capabilities and has made our firmwide cybersecurity program **more efficient**.”*
>
> – Kevin Kennedy
> Senior Vice President, Cybersecurity



AI-driven Detection

50 new detections in 1 day



AI-driven Prioritization

90% reduction in alerts

“The signal-to-noise ratio from low fidelity to high fidelity is all done basically upstream by Vectra”

SOC efficiency gains:

- Automate and improve quality of threat detections over native tools
- Less detection engineering time, more MITRE coverage
- Higher fidelity, more accurate events in case management
- Faster MTTD, MTTI, MTTR measurement and metrics

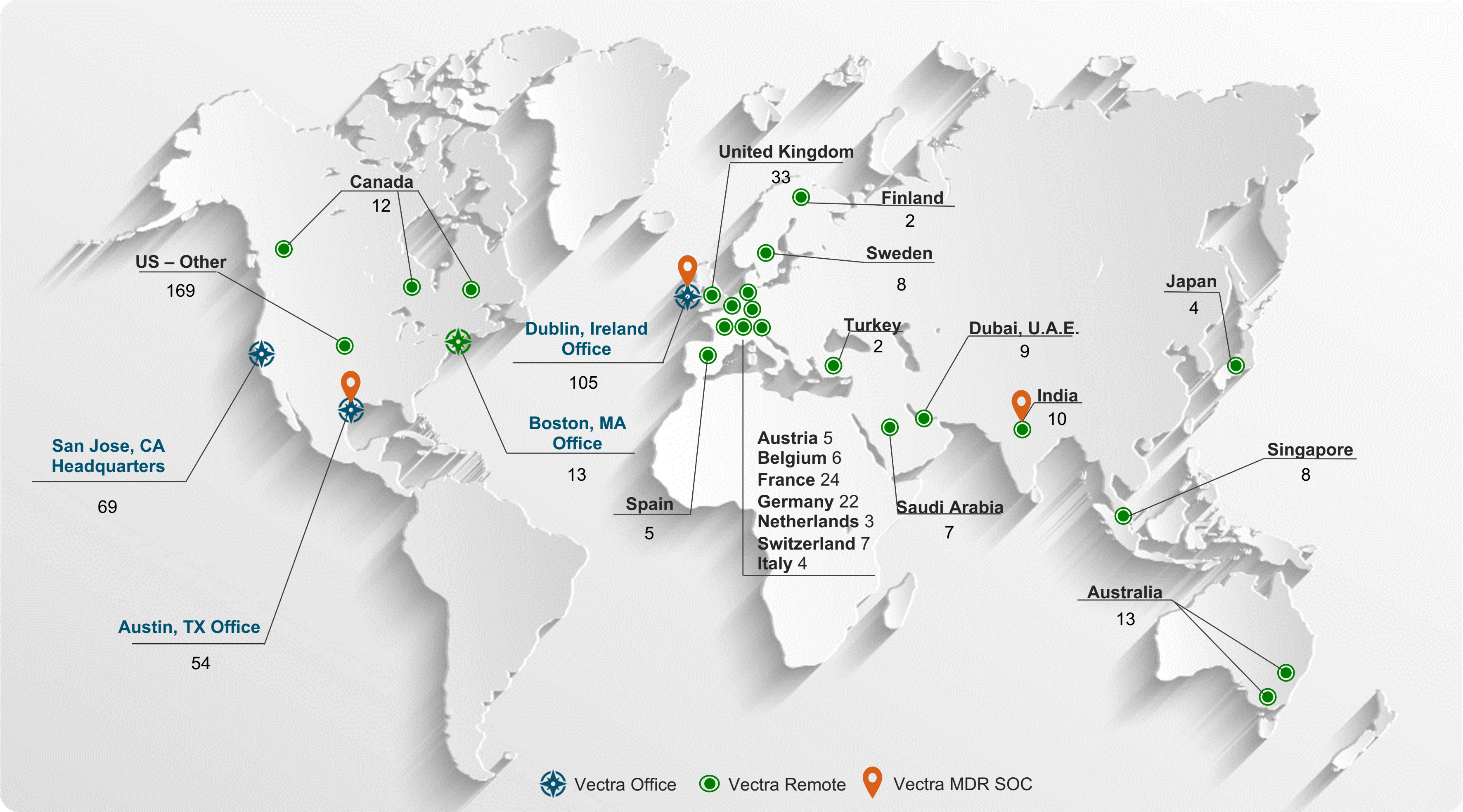
Source: Case Study: Vectra helps Blackstone reduce threat detections on O365 by over 50x - https://content.vectra.ai/hubfs/downloadable-assets/CaseStudy_Blackstone.pdf

About Us, Our Customers & Partners

Optional slides

Vectra is the AI-driven partner you can trust

The pioneer and global leader in AI-driven cyber threat detection and response



About us

- Founded 2011
- Privately held
- Global footprint
  - + 600+ employees
  - + 20+ countries
- 3 SOCs - follow the sun
  - + Austin, TX
  - + Dublin, Ireland
  - + Bangalore, India
- 12 security AI patents
- 97% coverage for MITRE ATT&CK, with more MITRE D3FEND countermeasures than any other vendor
- >1000 enterprise customers
- >$100M ARR

UNDER ARMOUR · MITSUBISHI ELECTRIC *Changes for the Better* · KRONOS · SANOFI · Orange Cyberdefense · A.S. Watson Group A member of CK Hutchison Holdings · TEXAS A&M UNIVERSITY 1876

Vectra: Supporting Federal Customers

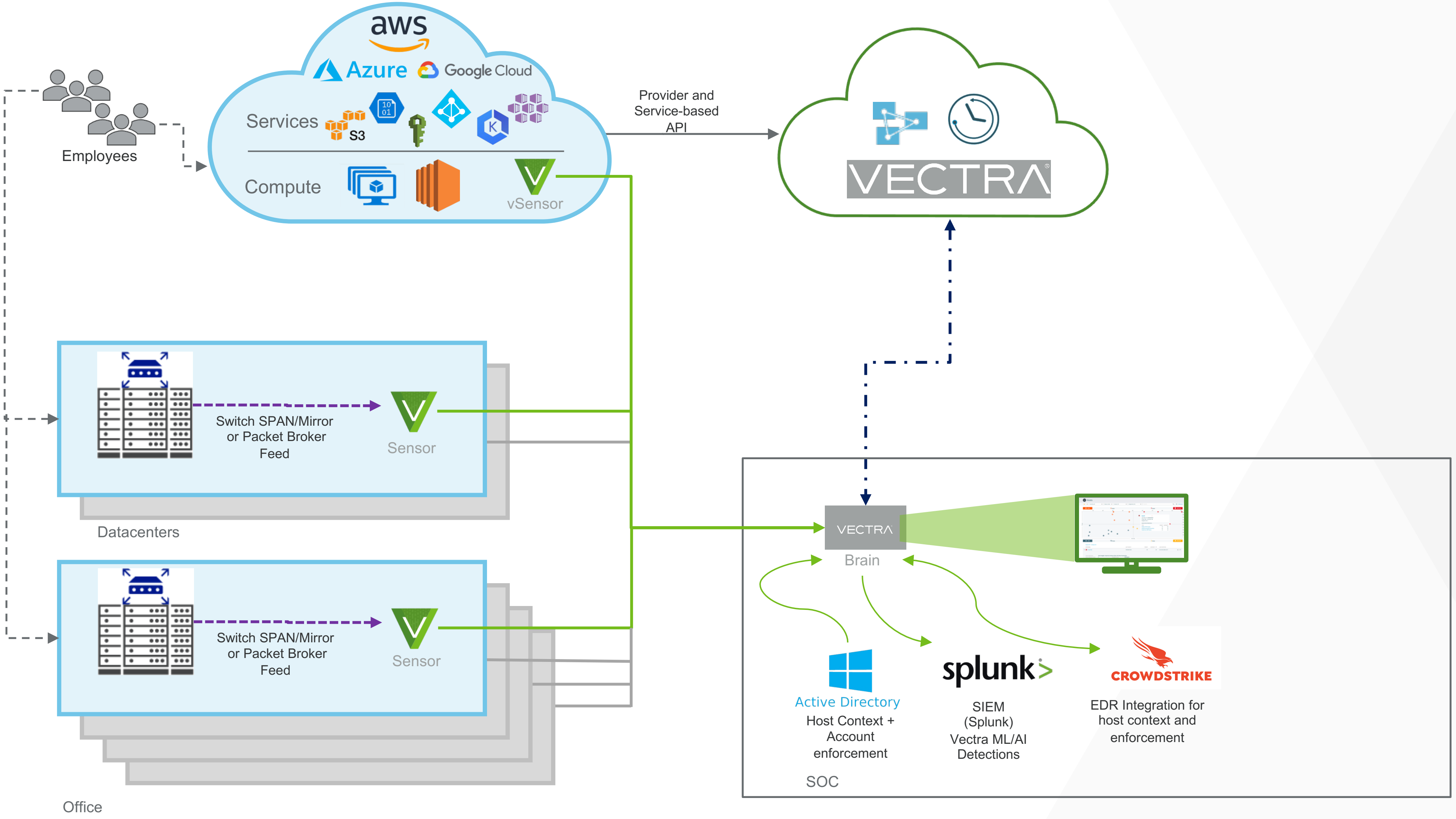
Our Partners

A broad ecosystem of alliance, integration, and services partners

Microsoft	aws	IBM Security	DELL		KPMG
CROWDSTRIKE	servicenow	splunk>	CORTEX BY PALO ALTO NETWORKS	zscaler	Capgemini
SentinelOne	vmware	SURICATA	LogRhythm	FIREEYE	Orange Cyberdefense
cybereason	paloalto NETWORKS	SWIMLANE	Siemplify now part of Google Cloud	ArcSight	wipro
vmware Carbon Black	CHECK POINT	FORTINET	JUNIPer NETWORKS	Jira Software	

Attack Signal Intelligence™

Introduction to Vectra Attack Signal Intelligence

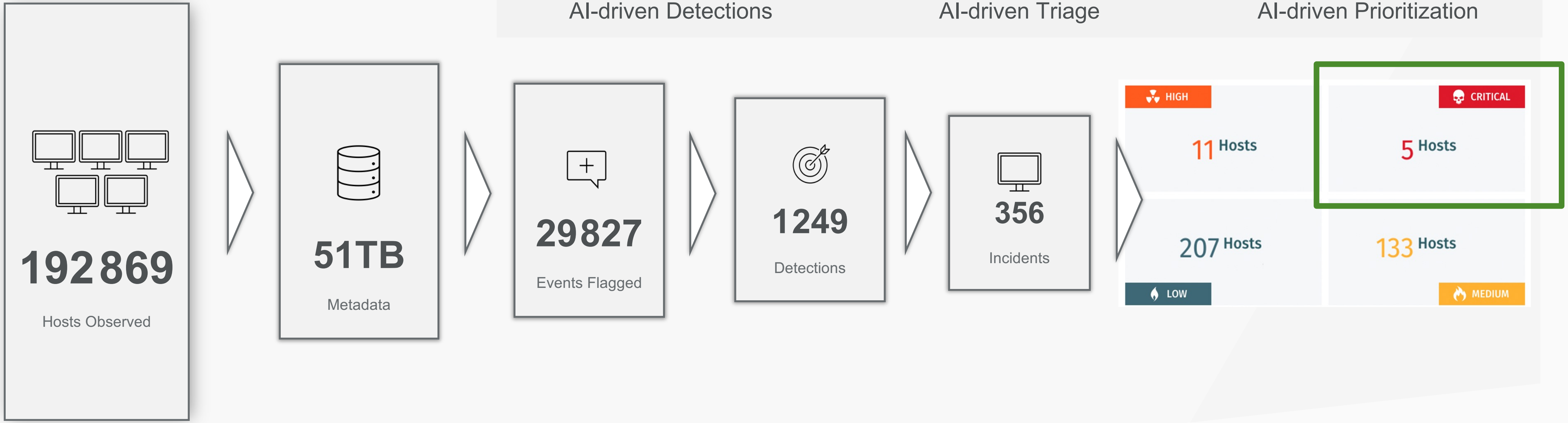


VECTRA
SECURITY THAT THINKS.®

Only Vectra filters out the noise, prioritizes real threats

Attack Signal Intelligence - game changing signal clarity for NDR

Collect	Analyze		Prioritize
	Think like an attacker	Know what is malicious	Focus on what is urgent
	AI-driven Detections	AI-driven Triage	AI-driven Prioritization



192869
Hosts Observed

51TB
Metadata

29827
Events Flagged

1249
Detections

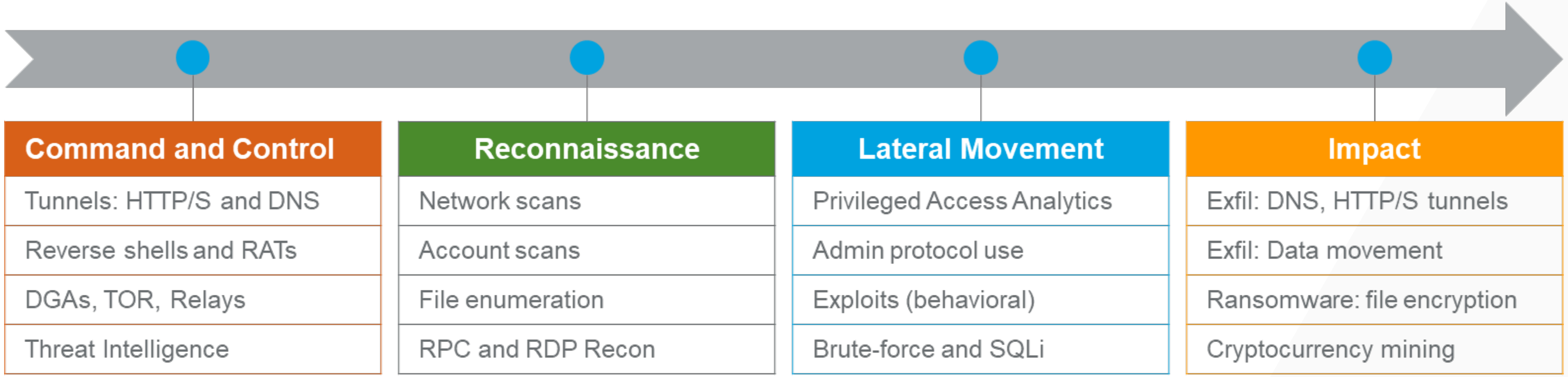
356
Incidents

VECTRA
SECURITY THAT THINKS.®

2. Analyze metadata for attacker behaviors

150+ ready-built attacker behavior models, +97% coverage of Mitre ATT&CK*

- Threat actors have 1000’s of tools and tactics, but behaves similarly
  1. They establish a control mechanism into the compromised environment (C2)
  2. They snoop around to map out the compromised environment (Recon)
  3. They move laterally inside the compromised environment (Lateral movement)
  4. They steal, encrypt, alter and destroy (Impact)

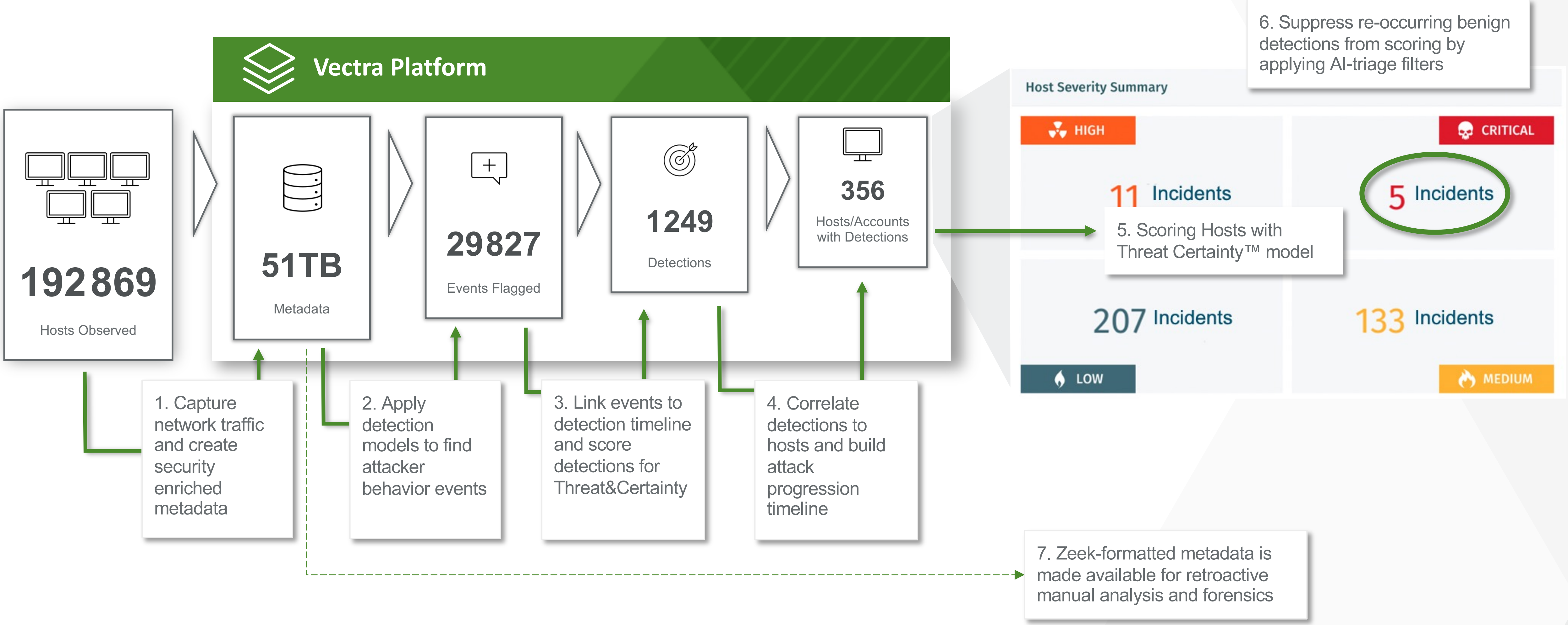


Command and Control	Reconnaissance	Lateral Movement	Impact
Tunnels: HTTP/S and DNS	Network scans	Privileged Access Analytics	Exfil: DNS, HTTP/S tunnels
Reverse shells and RATs	Account scans	Admin protocol use	Exfil: Data movement
DGAs, TOR, Relays	File enumeration	Exploits (behavioral)	Ransomware: file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

* Source: https://support.vectra.ai/s/article/KB-VS-1158

3. 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

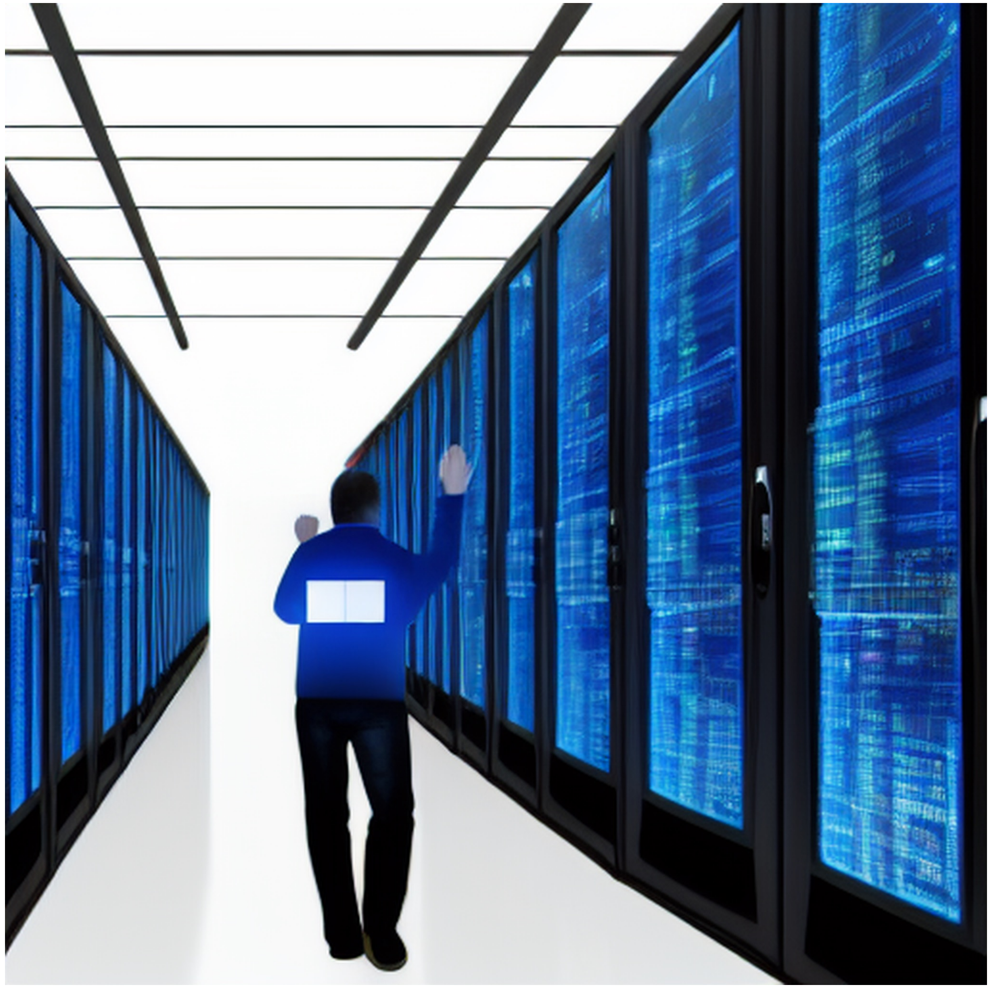
Source: Customer environment in a large multinational enterprise, during a 30 day period

VECTRA
SECURITY THAT THINKS.®

AI = a (short) Buzzword

Skepticism is thoroughly encouraged

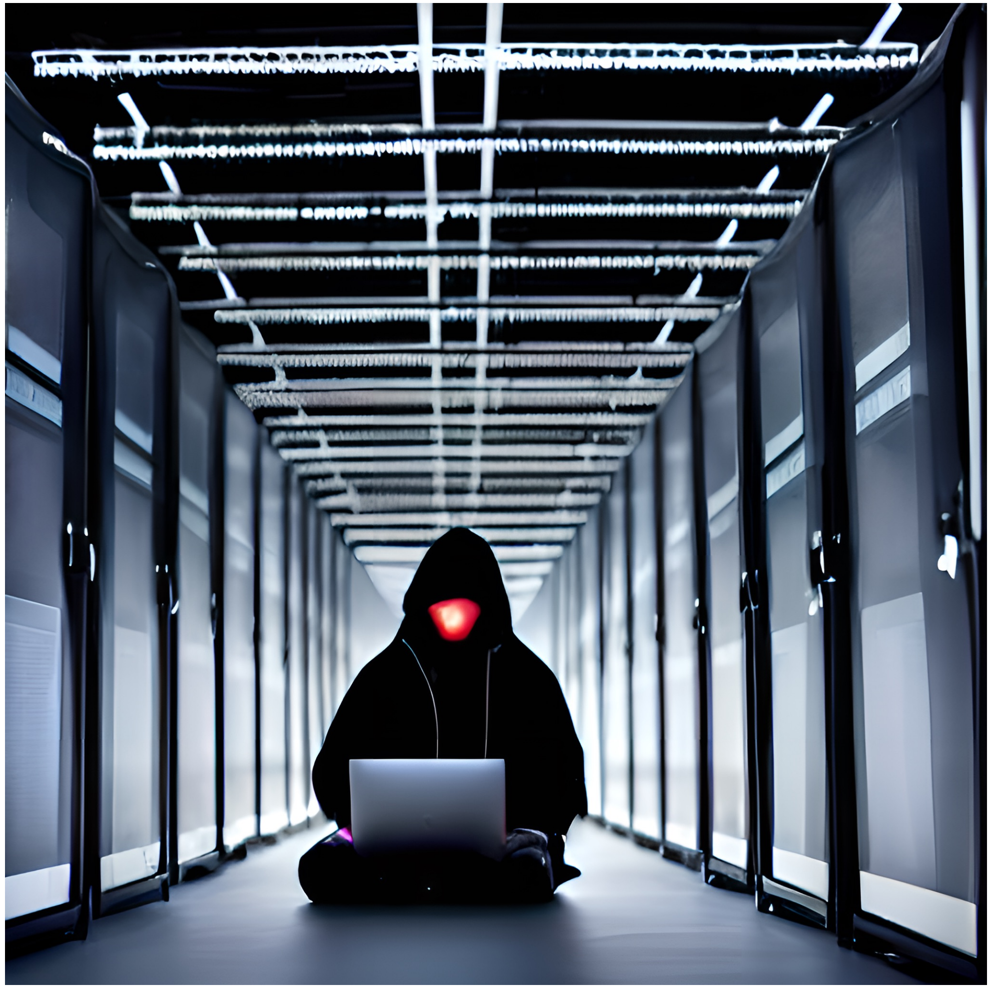
Input / Signal is important…



“hacker in a datacenter”

Steps: 20, Sampler: Euler a, CFG scale: 7,
Seed: 1147051768, Size: 512x512

Input / Signal is important…

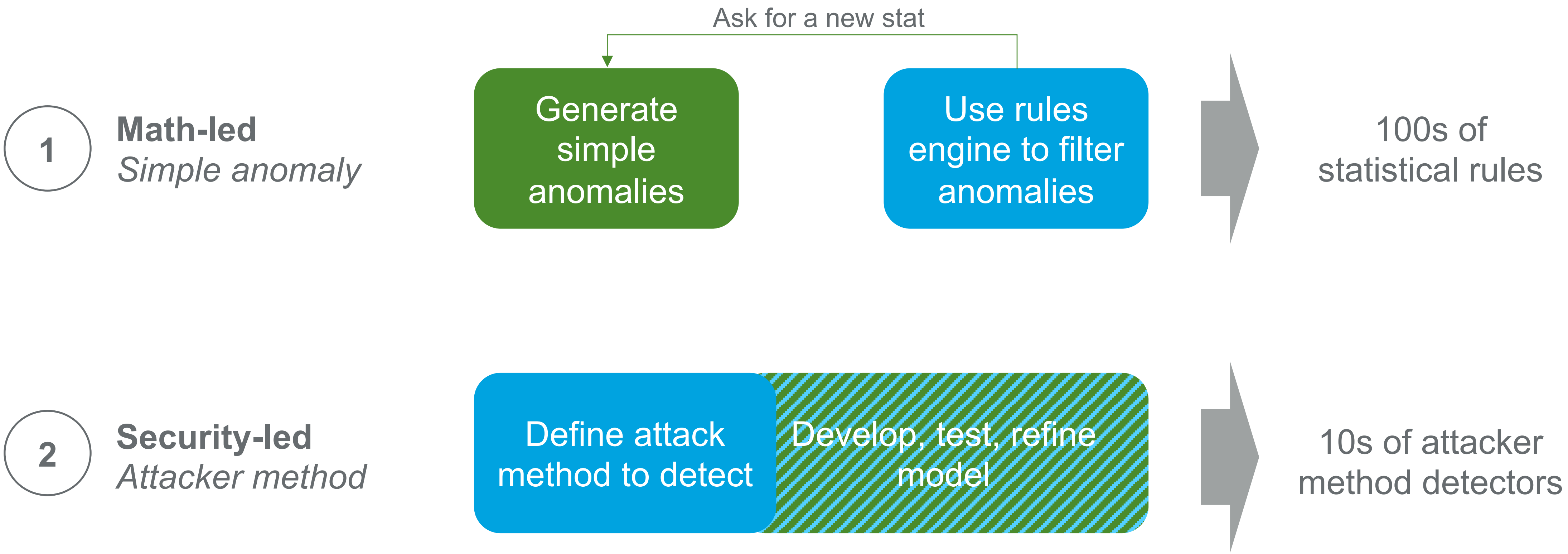


((((dark)))) ((figure sitting on the floor)), (wearing a hooded jacket), in a glowing data center typing on an open (laptop), (((wires everywhere))) connected to rows of server computers, 8k, high resolution, ((high focus)), extreme detail, extreme focus, eerie lighting, hard edges, disturbing, frightening

Negative prompt: ugly, deformed, [[[[[bright light]]]]], unrealistic, skewed perspective, awkward limbs, [[[[blurry]]]], [fuzzy], diffuse, soft edges, round corners, bulging, (((logo))), cloudy, calming, ((((peaceful)))), nice, [[glowing edges]], color, incomplete hands, incomplete limbs, incomplete objects, strange objects, strange looking

Steps: 90, Sampler: Euler a, CFG scale: 7,
Seed: 3308590029, Size: 512x512

Two major philosophies in applying AI to threat detection



Ask for a new stat

1 **Math-led**
Simple anomaly

Generate simple anomalies

Use rules engine to filter anomalies

100s of statistical rules

2 **Security-led**
Attacker method

Define attack method to detect

Develop, test, refine model

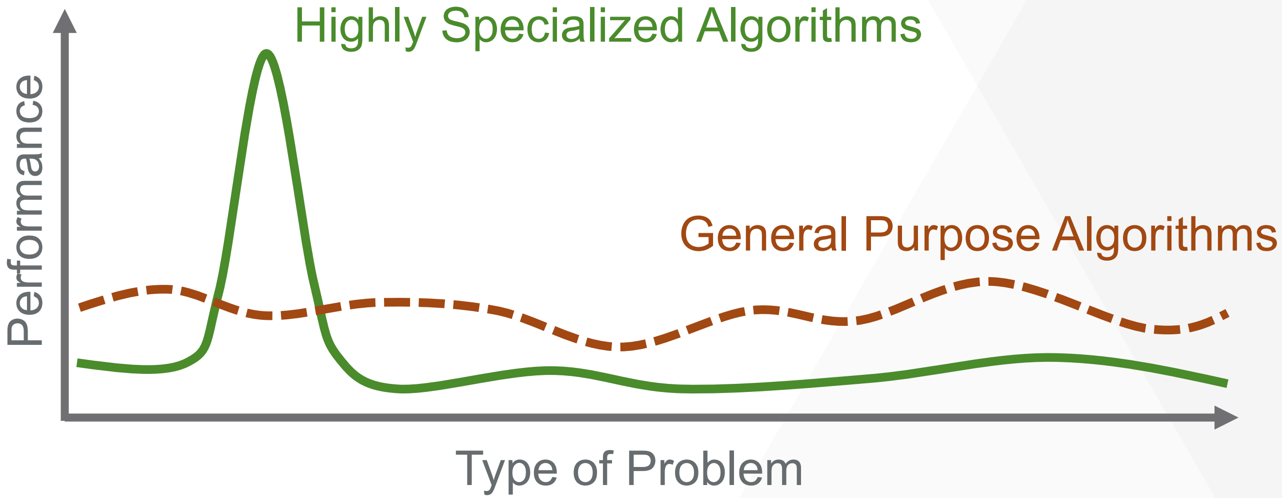
10s of attacker method detectors

🟩 = data science 🟦 = security research

VECTRA® SECURITY THAT THINKS.®

The “No Free Lunch” theorem

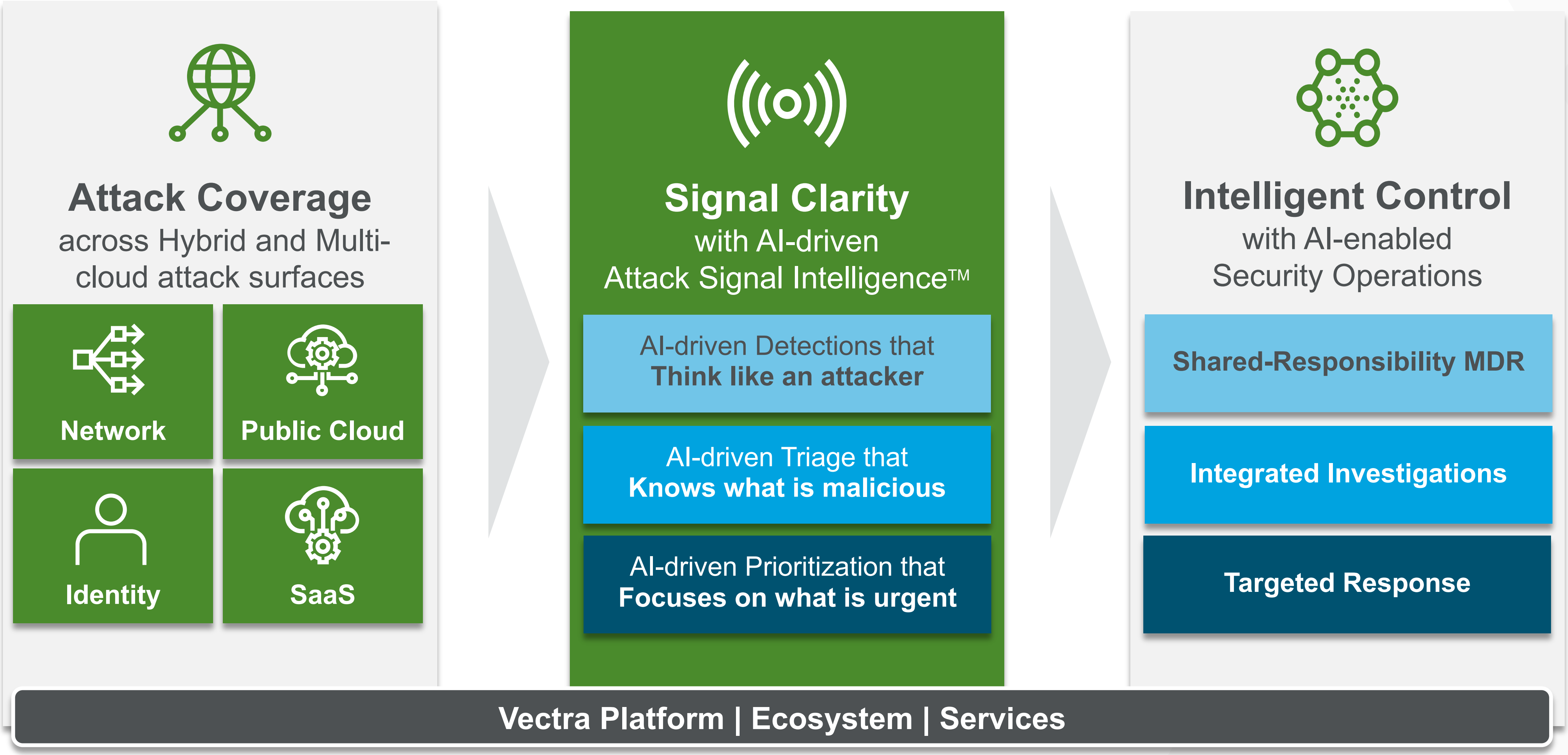
- Supervised – Global learning
  - Deep learning / neural networks
  - Natural language processing
  - Statistical modeling
- Unsupervised – Local learning
  - Clustering
  - Outlier detection
  - Graph analysis



VECTRA
SECURITY THAT THINKS.

AI-driven signal clarity is our core

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



Attack Coverage

across Hybrid and Multi-cloud attack surfaces

- Network
- Public Cloud
- Identity
- SaaS

Signal Clarity

with AI-driven Attack Signal Intelligence™

- AI-driven Detections that **Think like an attacker**
- AI-driven Triage that **Knows what is malicious**
- AI-driven Prioritization that **Focuses on what is urgent**

Intelligent Control

with AI-enabled Security Operations

- **Shared-Responsibility MDR**
- **Integrated Investigations**
- **Targeted Response**

Vectra Platform | Ecosystem | Services

Only Vectra Security AI is optimized to detect attacker methods

With Attack Signal Intelligence^{TM} behavior-based, AI-driven Detection

1

Analyze **attacker methods**

MITRE | ATT&CK®

Per-domain analysis enables deep coverage

2

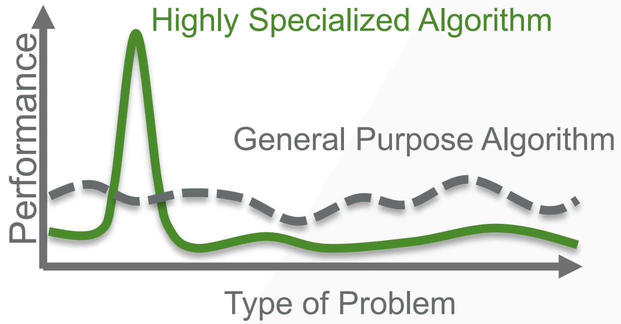
Define **countermeasures**

MITRE | D3FEND™

Define techniques to detect attack methods

3

Use the **optimal ML** approach for each



Security-led approach to AI

Powered by cutting-edge ML

Outcome: more coverage and clarity, less noise

vs simple anomaly-based detection

What makes Vectra Security AI unique

How our Attack Signal Intelligence™ stands apart

Sees through encryption

Finds attackers without forcing decryption using the power of recurrent neural networks and deep learning

Learns account privilege

Zeroes in on credential attacks by automatically discovering and focusing on accounts most useful to attackers.

Analyzes in many dimensions

Sees real threats in a sea of "different" by considering feature interactions in a multi-dimensional space.

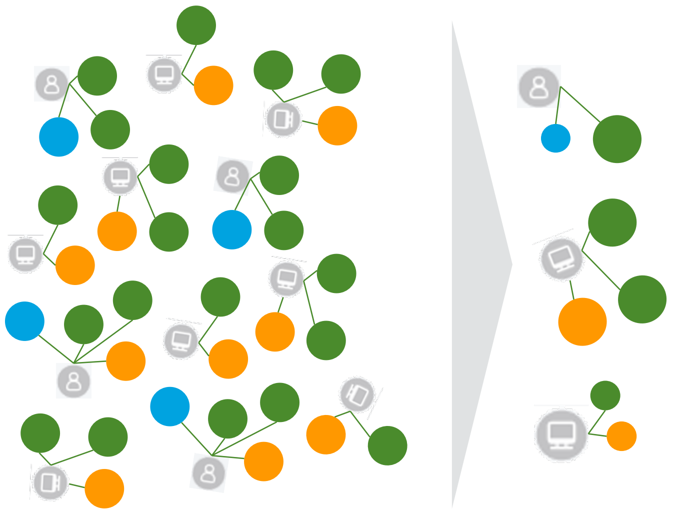
Sees attack progression

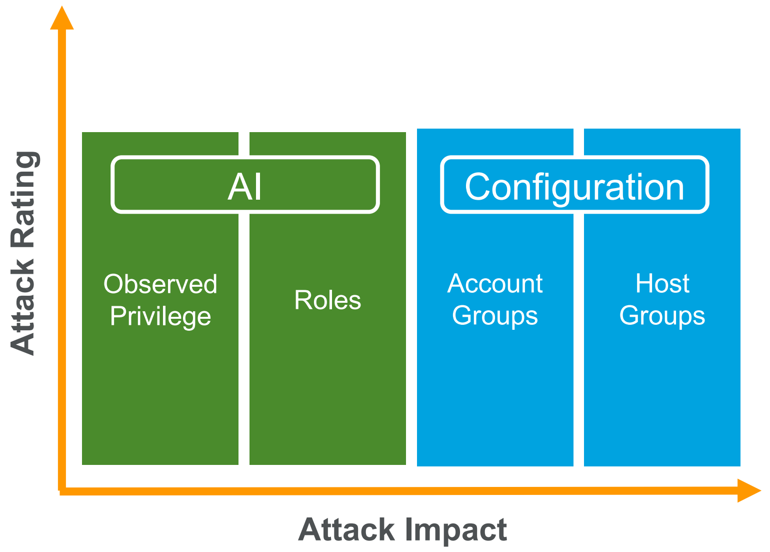
Focuses on what attackers do/use to hide and progress , e.g., M365 Power Automate or AWS admin API calls.

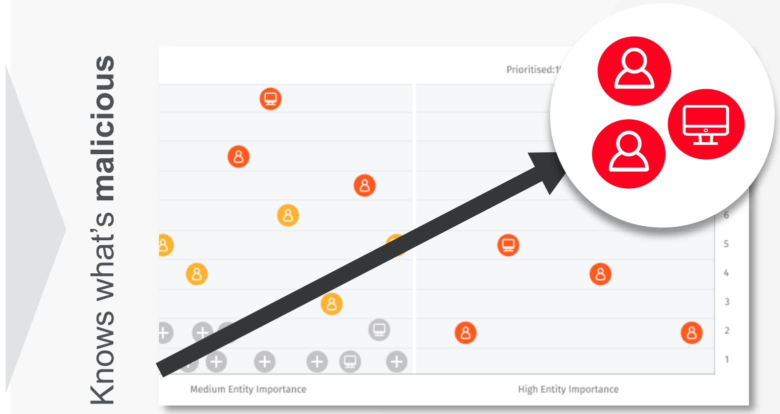
Vectra AI-driven Attack Signal IntelligenceTM

AI that Filters out the noise, prioritizes real threats

Think like an attacker	Know what is malicious & important	Focus on what is urgent
AI-driven Detections	AI-driven Triage	AI-driven Prioritization







Knows what's **important**

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
SECURITY THAT THINKS.®

How AI Differentiates Vectra's Approach

- True AI & ML
  - Patented AI models (150+) of supervised and unsupervised algorithms

- Natively Signatureless*…
  - Models and hashes change, underlying behaviors are constant
  - *Full Suricata engine available as of March 2023

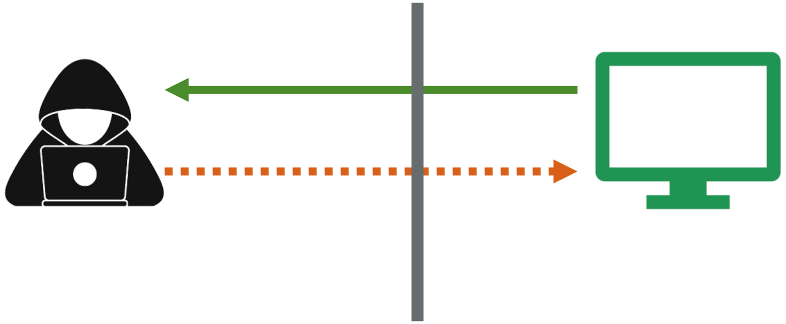
- Agentless…
  - Passive on SPANs/packet brokers & in Azure/AWS Gov, and C2E (in process)

- Decryptionless…
  - Underlying payload not of interest, purely TCP header behaviors

AI Challenges

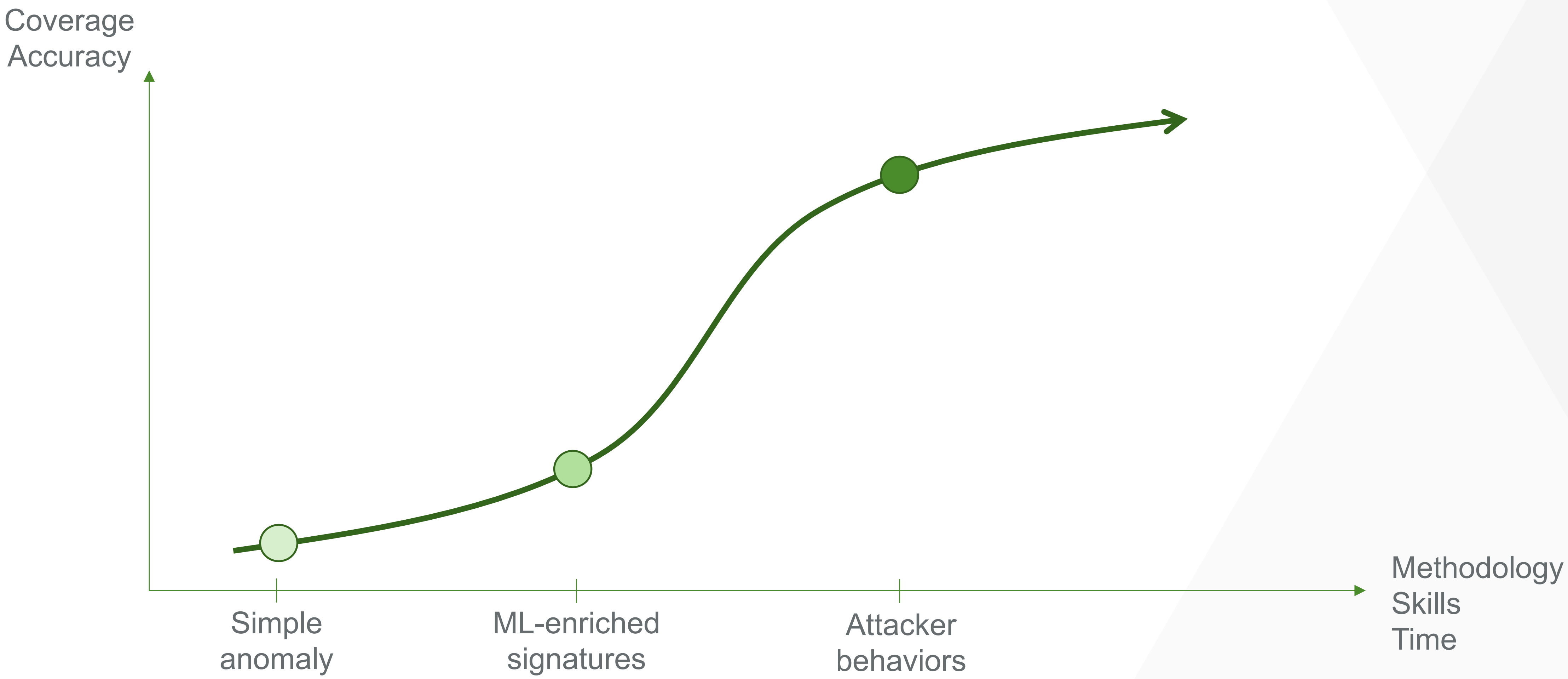
Challenge: Detect an HTTPS Tunnel

Core to every APT attack is their C2



- Designed to evade detection
- Attackers constantly evolve
- Benign networks constantly change

Perspective on approaches



Challenge: Detect an HTTPS Tunnel

Durability
Accuracy
Sophistication

	Example	Notes
AI model	HTTPS Tunnel detector	Directly detect behavior of interest in an accurate way
ML-enhanced signatures	SSL beaconing to rare destination	Approximation of tunnel -> FP and FN problems
Simple anomalies + static IoCs	Unusual HTTPS connection count	FP: user browses more FN: tunnel conns low relative to user

Vectra Hidden HTTPS Tunnel Model

1000s of labeled tunnel samples
- Many tools
- Many uses

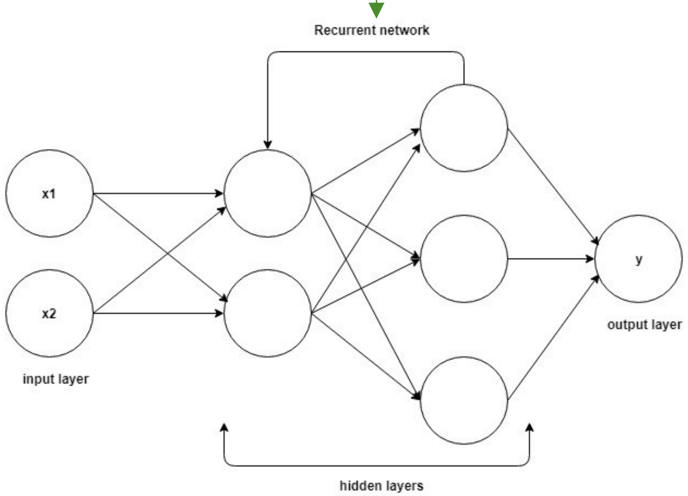
Normal HTTPS traffic from dozens of customers

Time series data. Sub-second data transfer patterns.

Unique to Vectra. Not in Zeek.

Train

If the answer is incorrect, the system is told to retrain.



Deep Learning:
LSTM Recurrent Neural Network

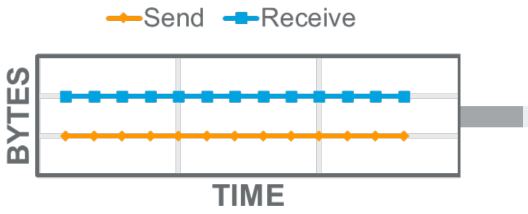
The output layer determines the answer.

Example: This is a muffin.

Directly detects behavior of tunneling.
No whitelists.
No blind spots.

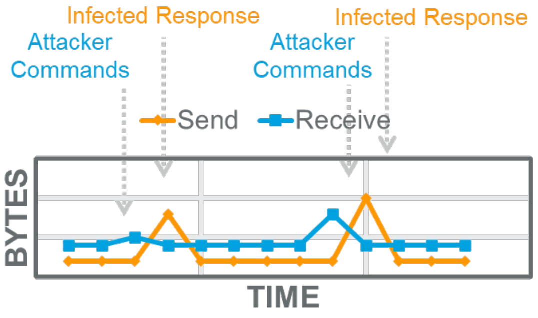
Visible Control in the data -- Sees through encryption

to reliably find C2 channels despite evasion attempts



Encrypted Beacon Traffic

Challenge: choosing the <0.1% of beacons that show C2 tunnel behavior



Encrypted Tunnel Traffic

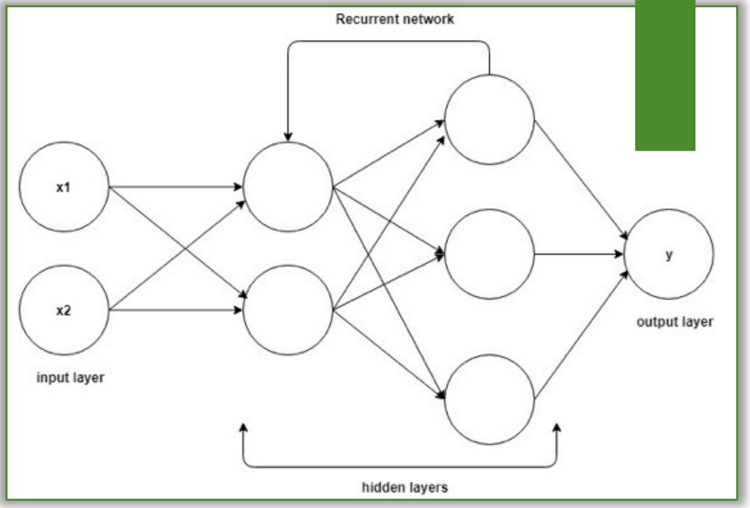
Identifies

Labeled (positive) tunnel samples

Normal (negative) HTTPS samples

Time series.
Sub-second
data patterns.

Train

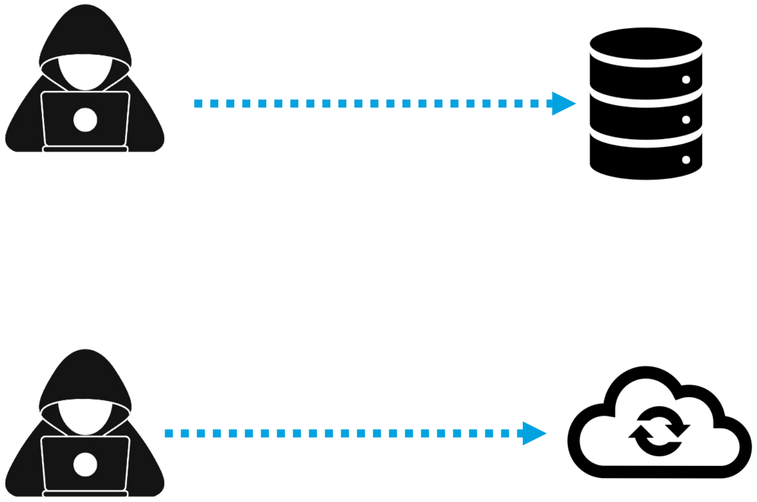


Deep Learning:
Recurrent Neural Network

No blind spots.
Evasion resistant.

Challenge: Detecting the abuse of privilege credentials

Privilege accounts are high priorities for attacker



- Access to both **network** and **cloud**
- By definition, actions are allowed to happen
- Abnormal ***is*** normal

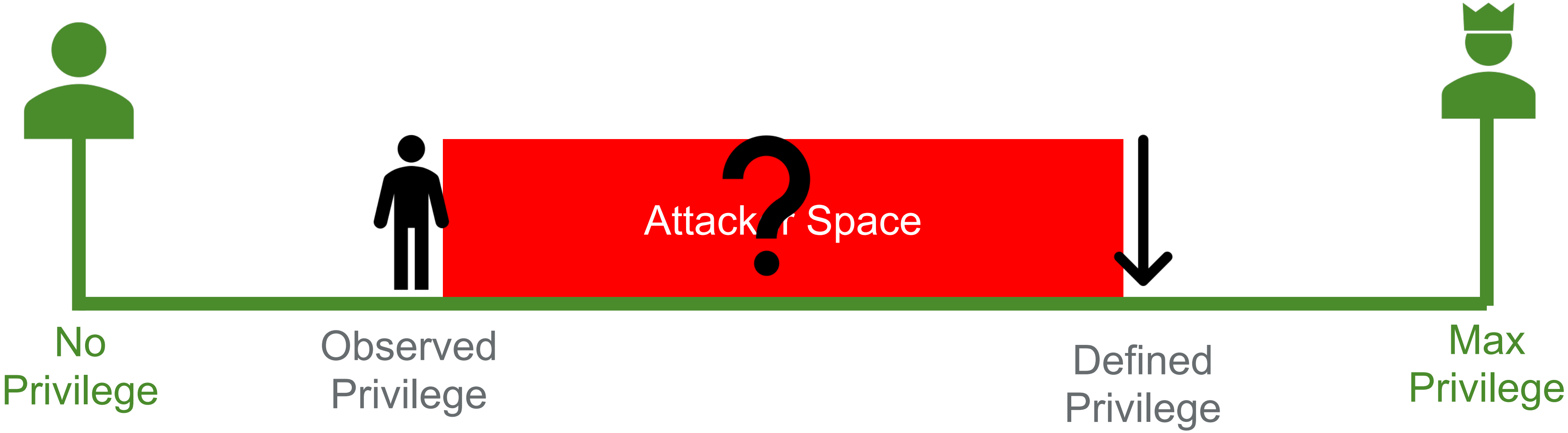
Perspective on approaches

Durability
Accuracy
Sophistication

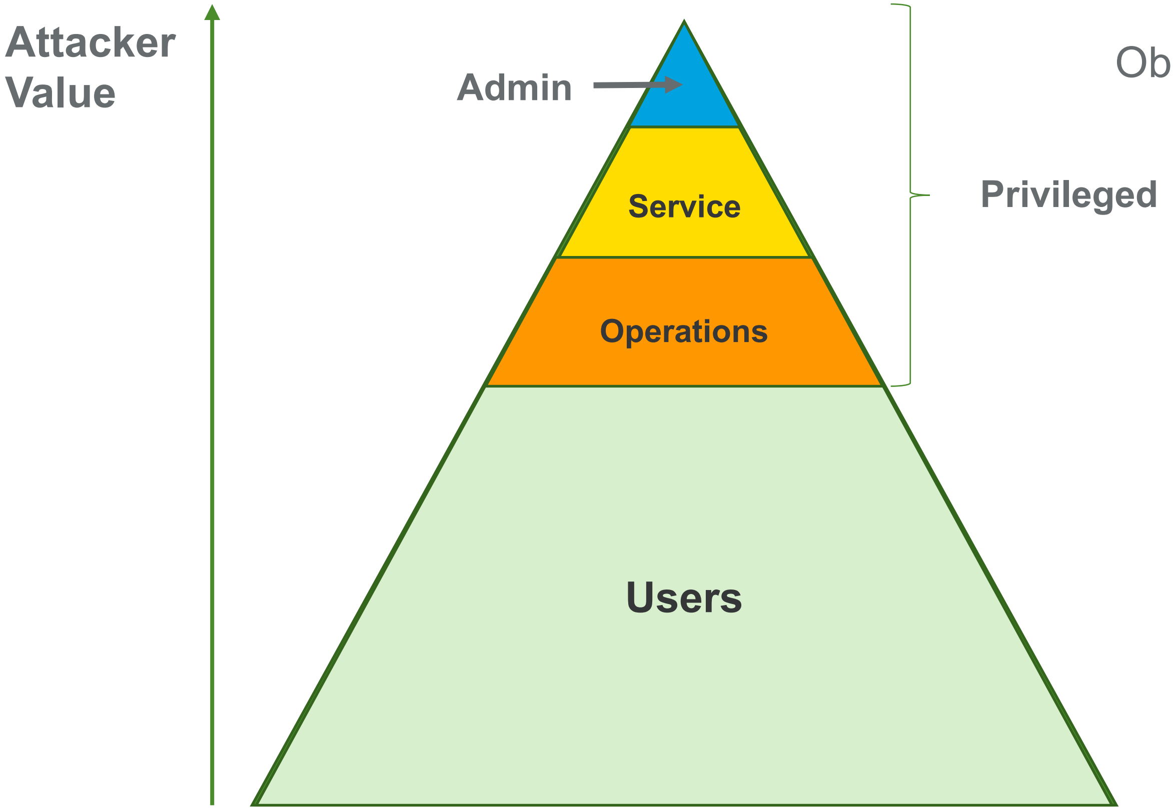
	Example	Notes
AI model	Privilege aware anomaly	Detect **how** attackers abuse credentials
“Rare” access	First access if it is used by less than 5 others	FP: New functionality FN: Attacker access to common service
First access	First time an account accesses something	FP: New functionality in org FN: Access on different host

The attacker view of privilege

- Properly permissioning users is hard!
- Attacker abuse privilege gaps
- Vectra finds and protects the gap

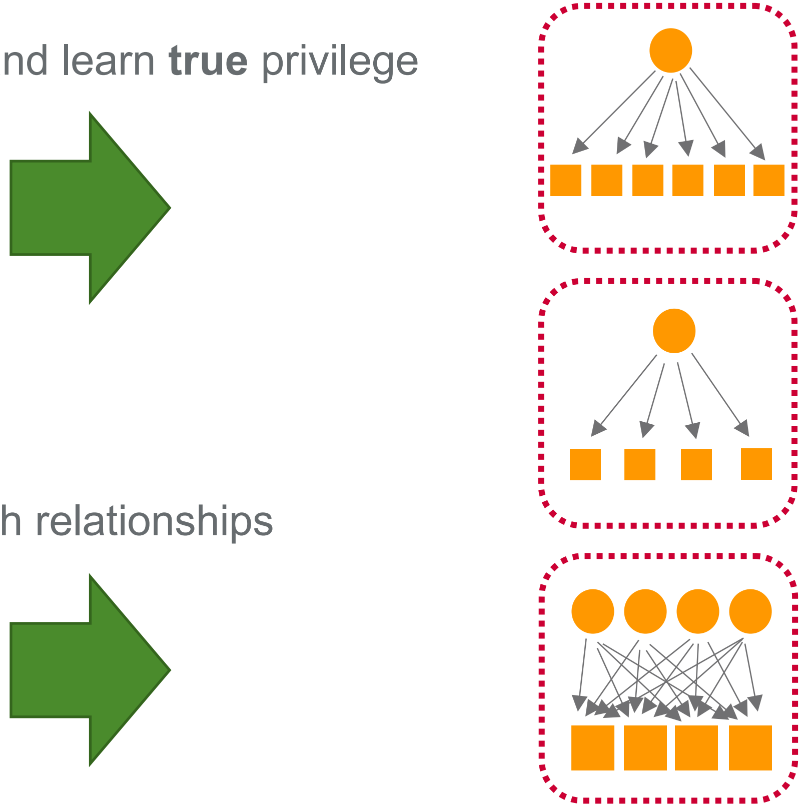


Vectra’s view of privilege

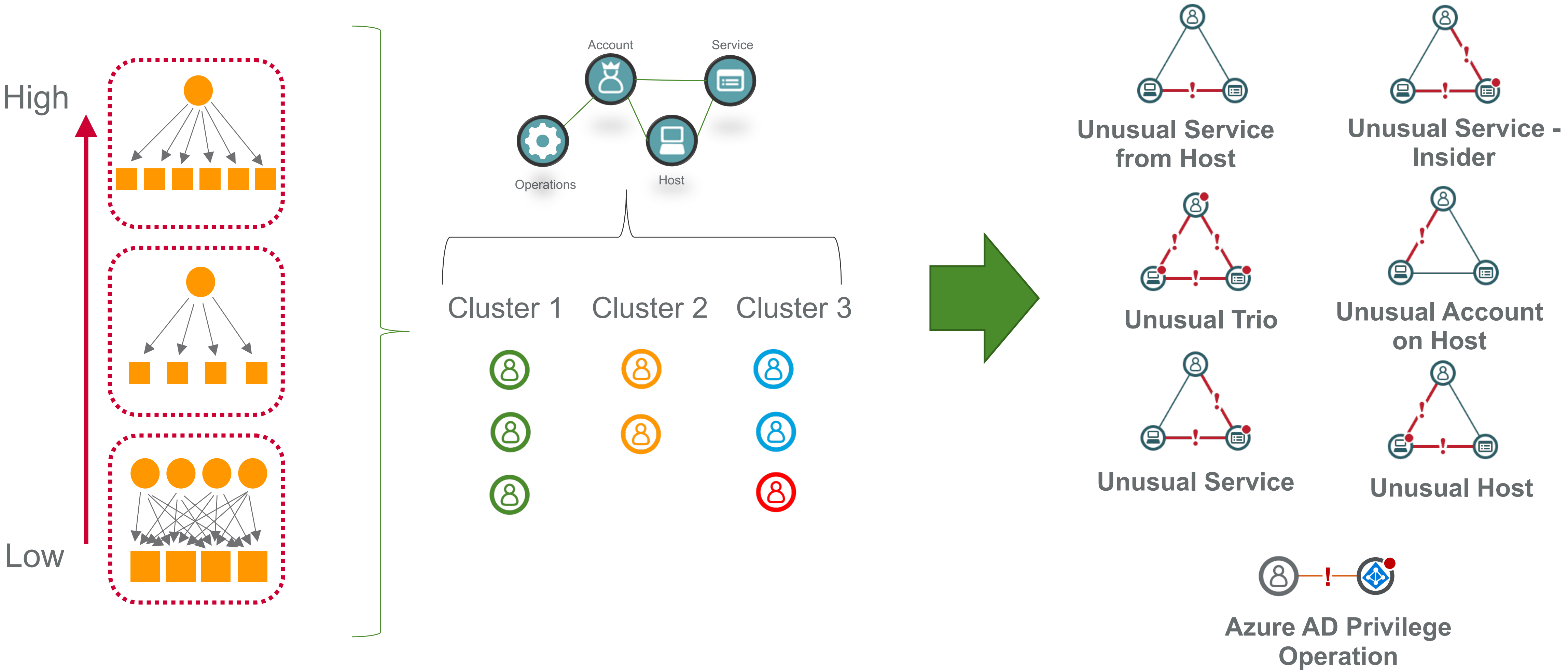


Observe and learn **true** privilege

Graph relationships



Vectra Privilege Anomaly Models



High

Low

Account

Service

Operations

Host

Cluster 1

Cluster 2

Cluster 3

Unusual Service from Host

Unusual Service - Insider

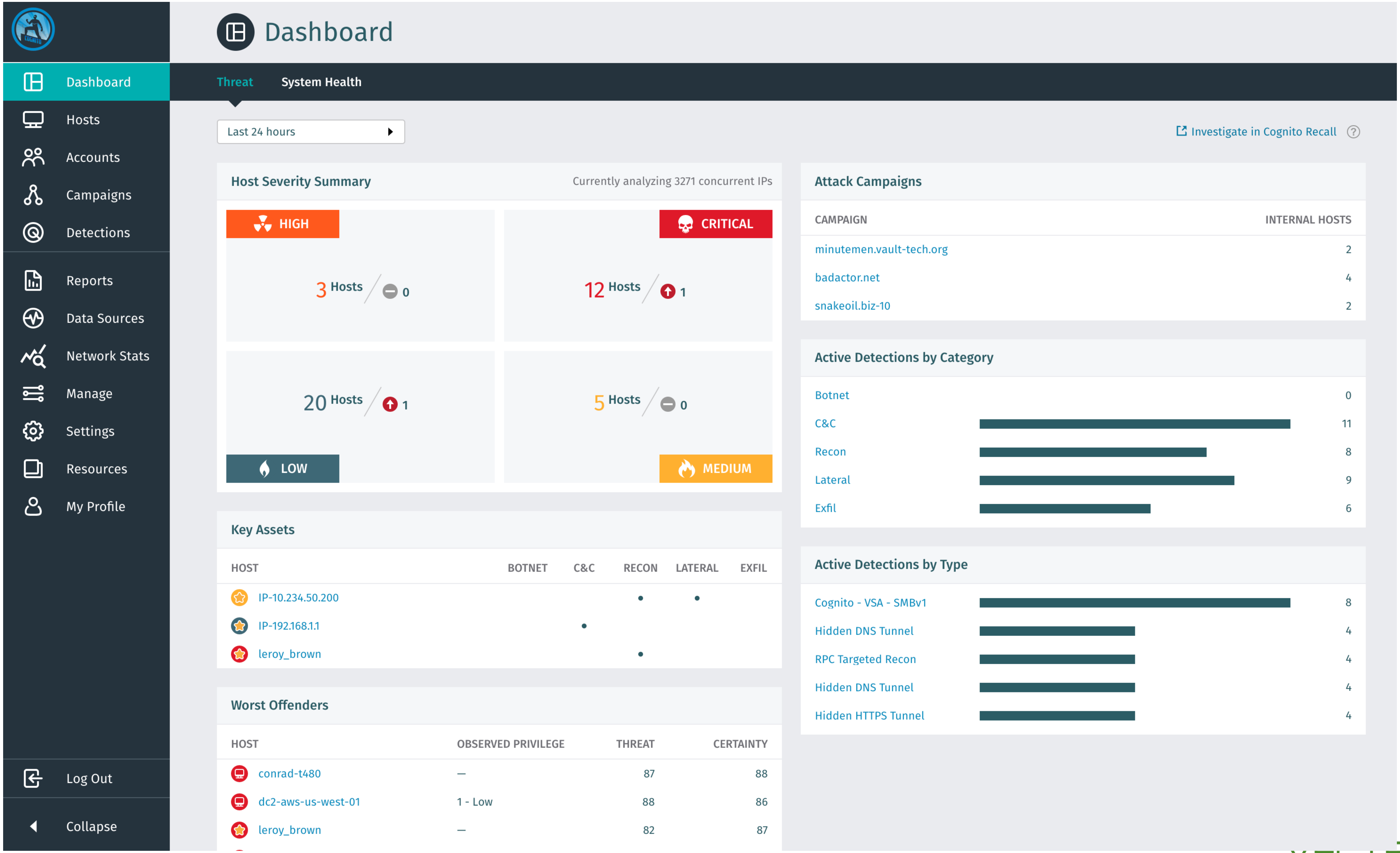
Unusual Trio

Unusual Account on Host

Unusual Service

Unusual Host

Azure AD Privilege Operation



Dashboard

Host Severity Summary

Currently analyzing 3271 concurrent IPs

HIGH 3 Hosts / 0	CRITICAL 12 Hosts / 1
20 Hosts / 1 LOW	5 Hosts / 0 MEDIUM

Attack Campaigns

CAMPAIGN	INTERNAL HOSTS
minutemen.vault-tech.org	2
badactor.net	4
snakeoil.biz-10	2

Active Detections by Category

Botnet	0
C&C	11
Recon	8
Lateral	9
Exfil	6

Key Assets

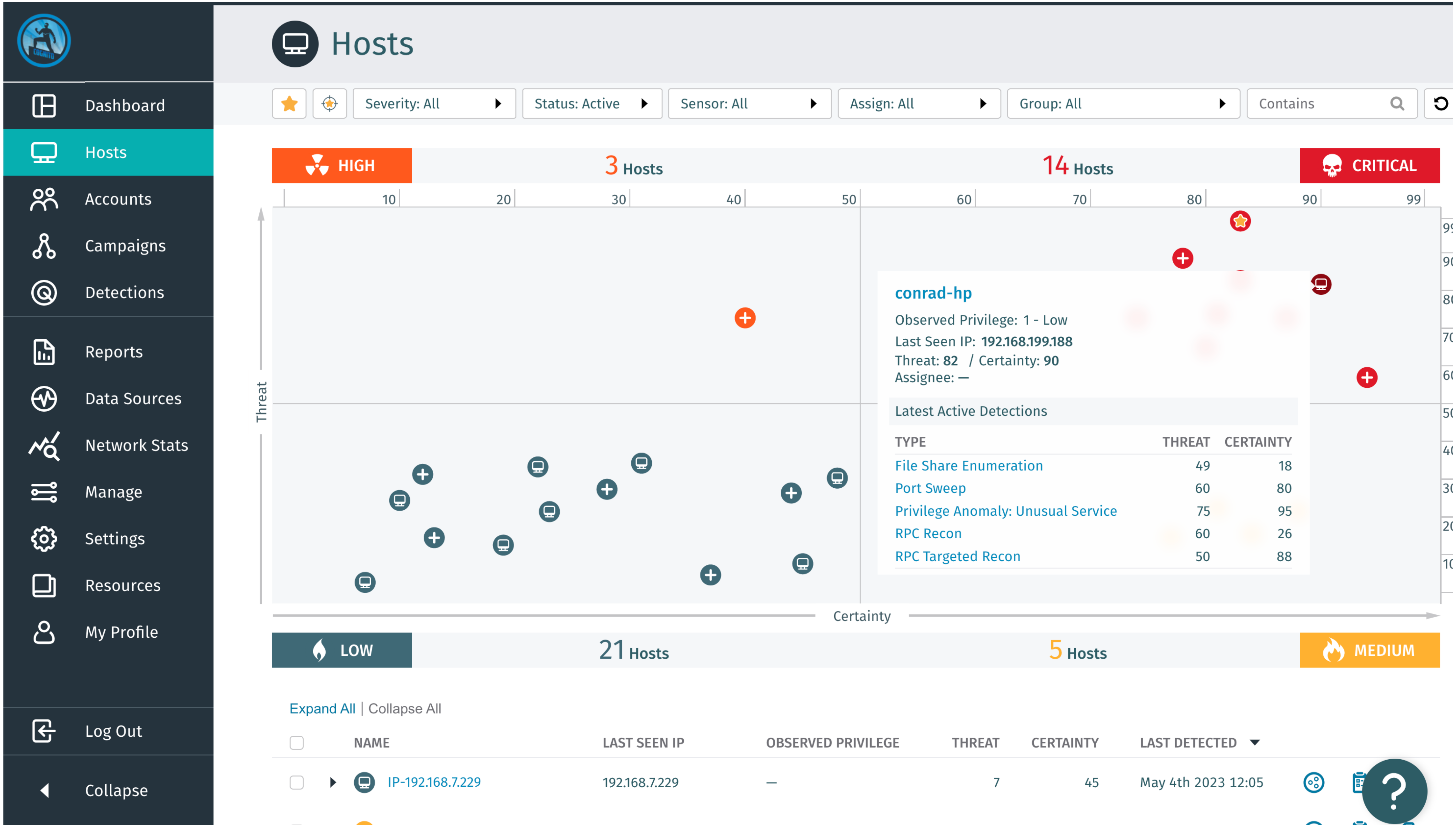
HOST	BOTNET	C&C	RECON	LATERAL	EXFIL
IP-10.234.50.200			•	•	
IP-192.168.1.1		•			
leroy_brown			•		

Active Detections by Type

Cognito - VSA - SMBv1	8
Hidden DNS Tunnel	4
RPC Targeted Recon	4
Hidden DNS Tunnel	4
Hidden HTTPS Tunnel	4

Worst Offenders

HOST	OBSERVED PRIVILEGE	THREAT	CERTAINTY
conrad-t480	—	87	88
dc2-aws-us-west-01	1 - Low	88	86
leroy_brown	—	82	87



conrad-hp

Observed Privilege: 1 - Low
Last Seen IP: **192.168.199.188**
Threat: **82** / Certainty: **90**
Assignee: —

Latest Active Detections

TYPE	THREAT	CERTAINTY
File Share Enumeration	49	18
Port Sweep	60	80
Privilege Anomaly: Unusual Service	75	95
RPC Recon	60	26
RPC Targeted Recon	50	88

Expand All | Collapse All

□	NAME	LAST SEEN IP	OBSERVED PRIVILEGE	THREAT	CERTAINTY	LAST DETECTED
□	IP-192.168.7.229	192.168.7.229	—	7	45	May 4th 2023 12:05

Attack Signal Intelligence at work

Finding and Stopping the Insider

Problem Statement

Inability to detect the unknown with legacy signature or "ML enabled" capabilities

Solution Statement

Vectra's AI approach coupled with the integrated Suricata engine allow for detection of sophisticated nation states, insider, and threat actors while maintaining required GRC mandates

Make the unknown… known

Disclaimer / Rules of Engagement

1. During this activity, no systems will be harmed or compromised.

2. The Vectra team will not access any files or systems outside the boundaries of the target hosts and cloud workload.

3. No manipulation, alteration, deletion, or encryption of any systems will be executed within this exercise.

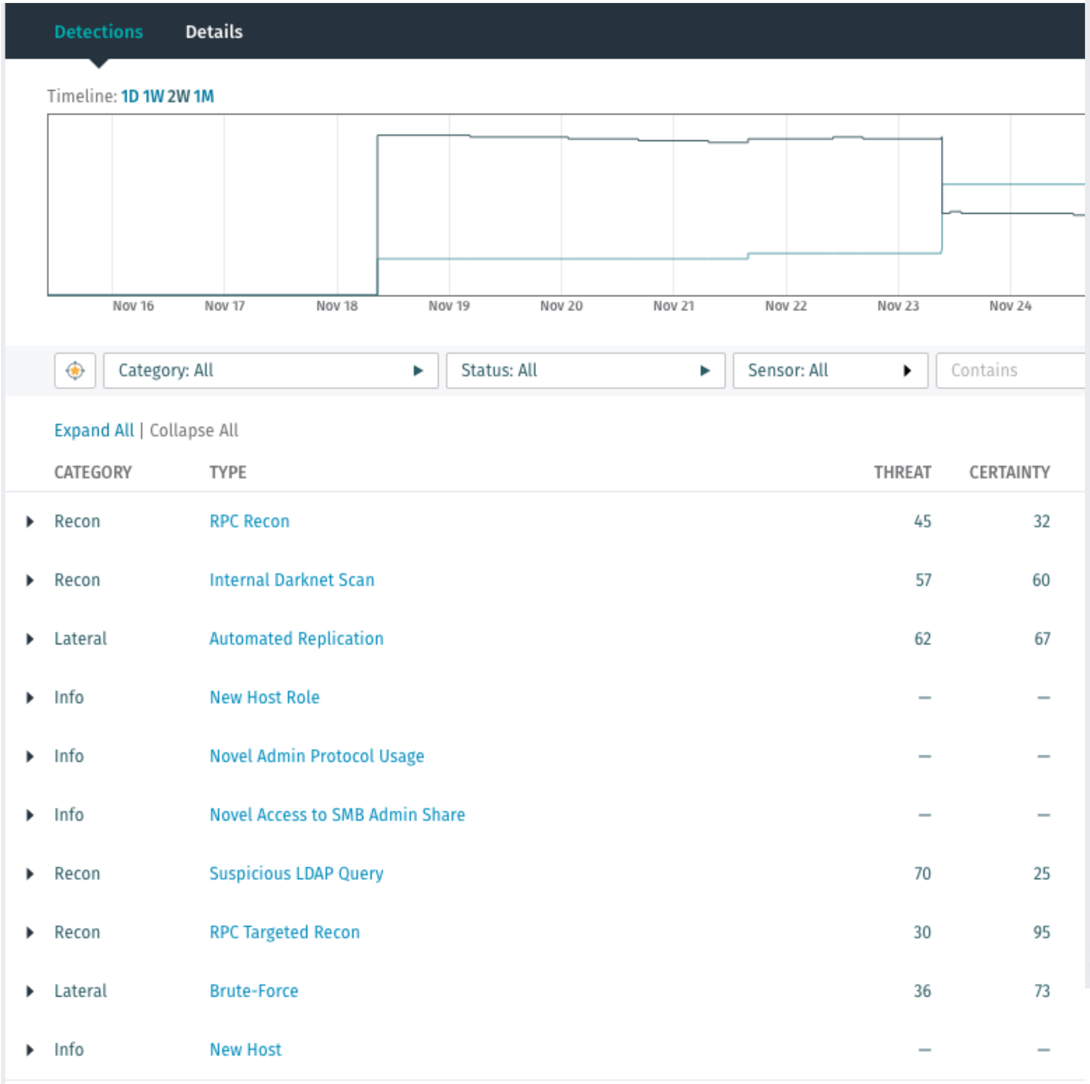
4. At all times, the GDIT leads will have full visibility to the actions of the exercise and the ability to stop the simulation.

5. Any and all activities related to this exercise will only be discussed within the GDIT Team and the Vectra National Security team. No information derived from this exercise will be discussed, transmitted or other outside a pre-defined list of members of both teams. Any communication outside these predefined boundaries must be approved by both parties.

Goals

- Perform behavioral actions to simulate an insider threat
- Show the value of applying AI to security to detect real-time threats
- Distinguish Vectra against traditional Intrusion Detection / Intrusion Prevention systems
  - Identify behaviors faster than existing tools
  - Identify behaviors other tools do not

identifiedsystem01

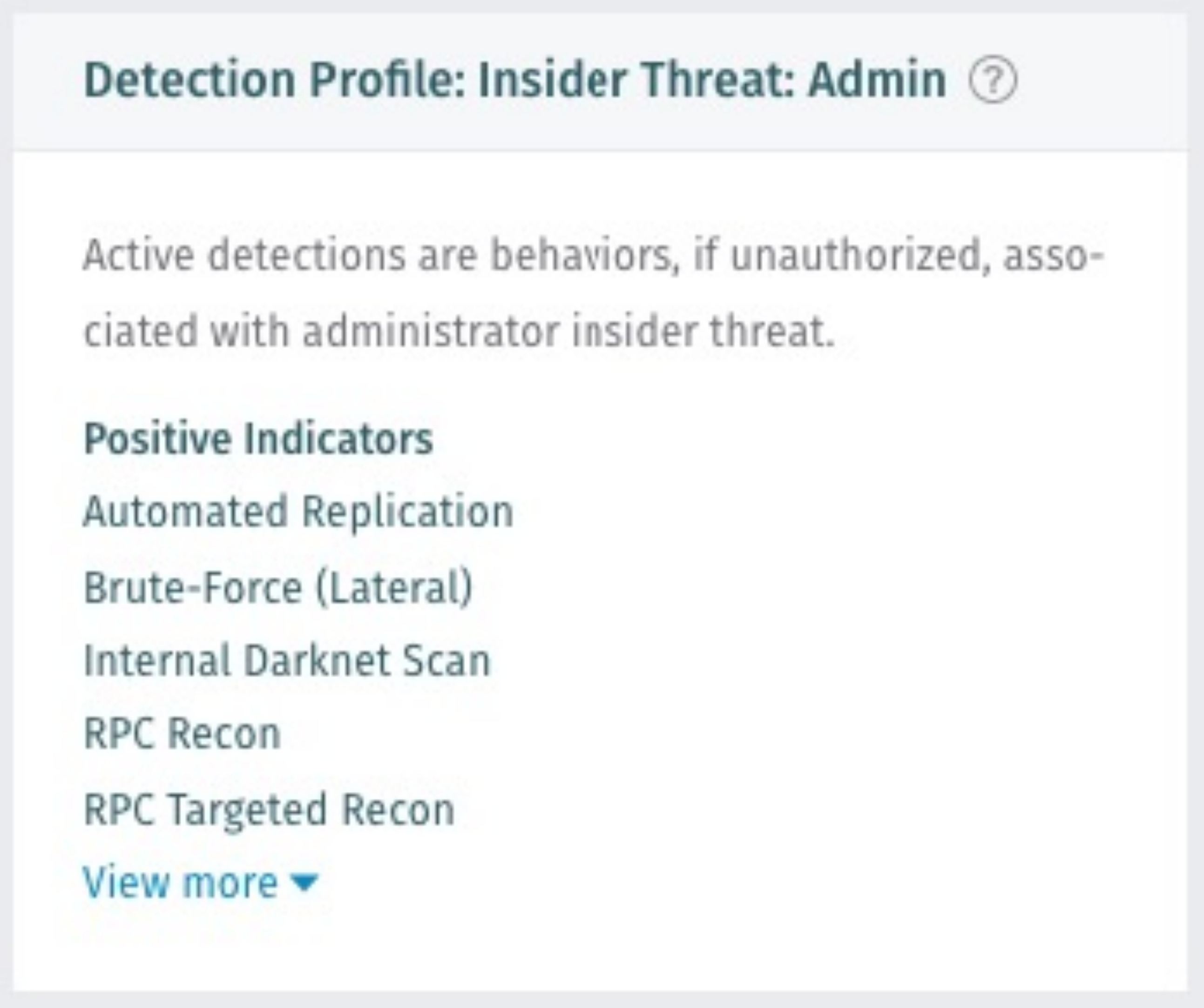


Timeline: 1D 1W 2W 1M

Category: All ▶ | Status: All ▶ | Sensor: All ▶ | Contains

Expand All | Collapse All

CATEGORY	TYPE	THREAT	CERTAINTY
▸ Recon	RPC Recon	45	32
▸ Recon	Internal Darknet Scan	57	60
▸ Lateral	Automated Replication	62	67
▸ Info	New Host Role	–	–
▸ Info	Novel Admin Protocol Usage	–	–
▸ Info	Novel Access to SMB Admin Share	–	–
▸ Recon	Suspicious LDAP Query	70	25
▸ Recon	RPC Targeted Recon	30	95
▸ Lateral	Brute-Force	36	73
▸ Info	New Host	–	–



Detection Profile: Insider Threat: Admin ?

Active detections are behaviors, if unauthorized, associated with administrator insider threat.

Positive Indicators

Automated Replication

Brute-Force (Lateral)

Internal Darknet Scan

RPC Recon

RPC Targeted Recon

View more ▾

Vulnerability Discovery

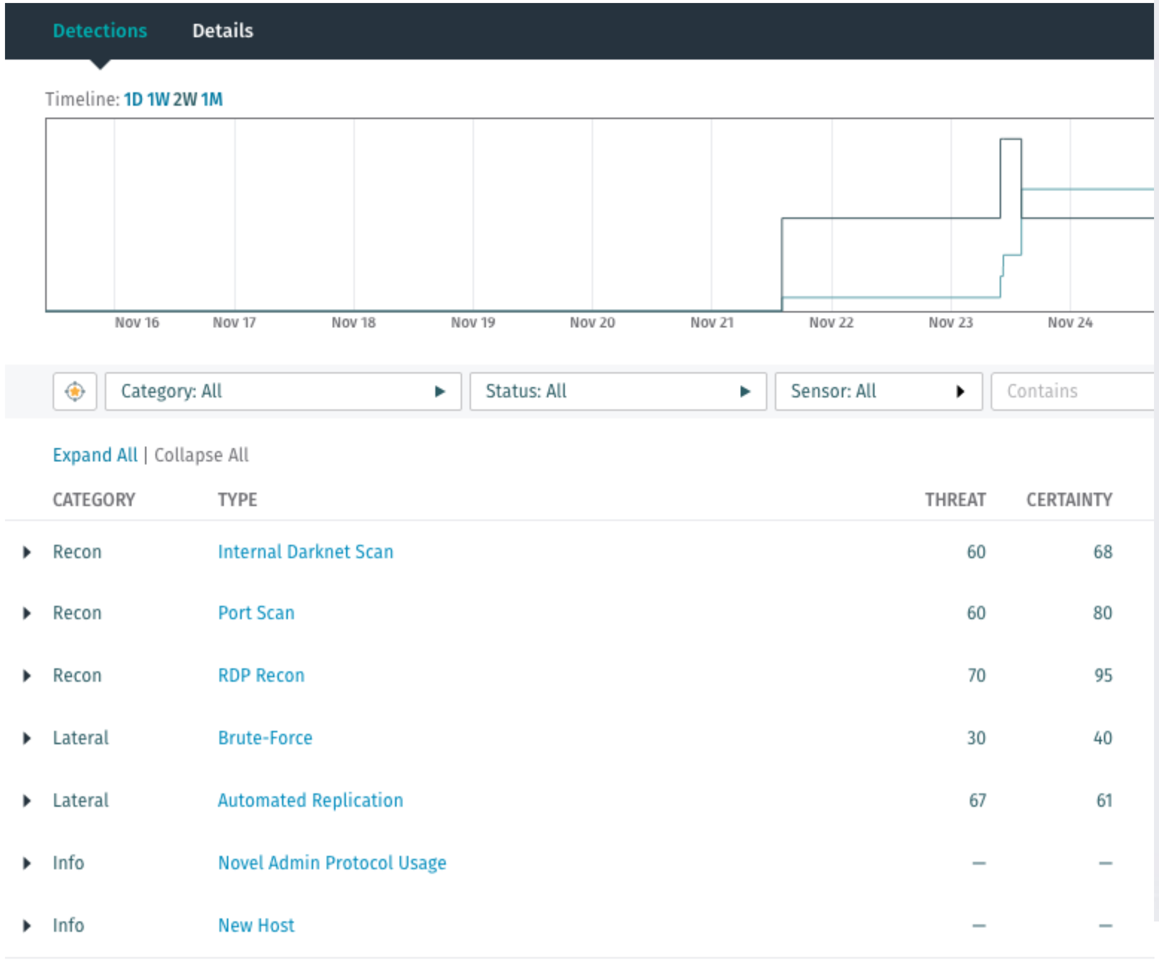
General Behavioral Profile

- Discovery, Reconnaissance, Lateral movement, and/or Exploitation
- NOT PRESENT: External, persistent Command and Control and/or Data Exfiltration

Possible Root Causes

- An adversary that has yet to exhibit the full range of malicious behaviors, or a limited scope penetration testing activity
- Vulnerability discovery and management infrastructure behaviors observed

identifiedsystem02

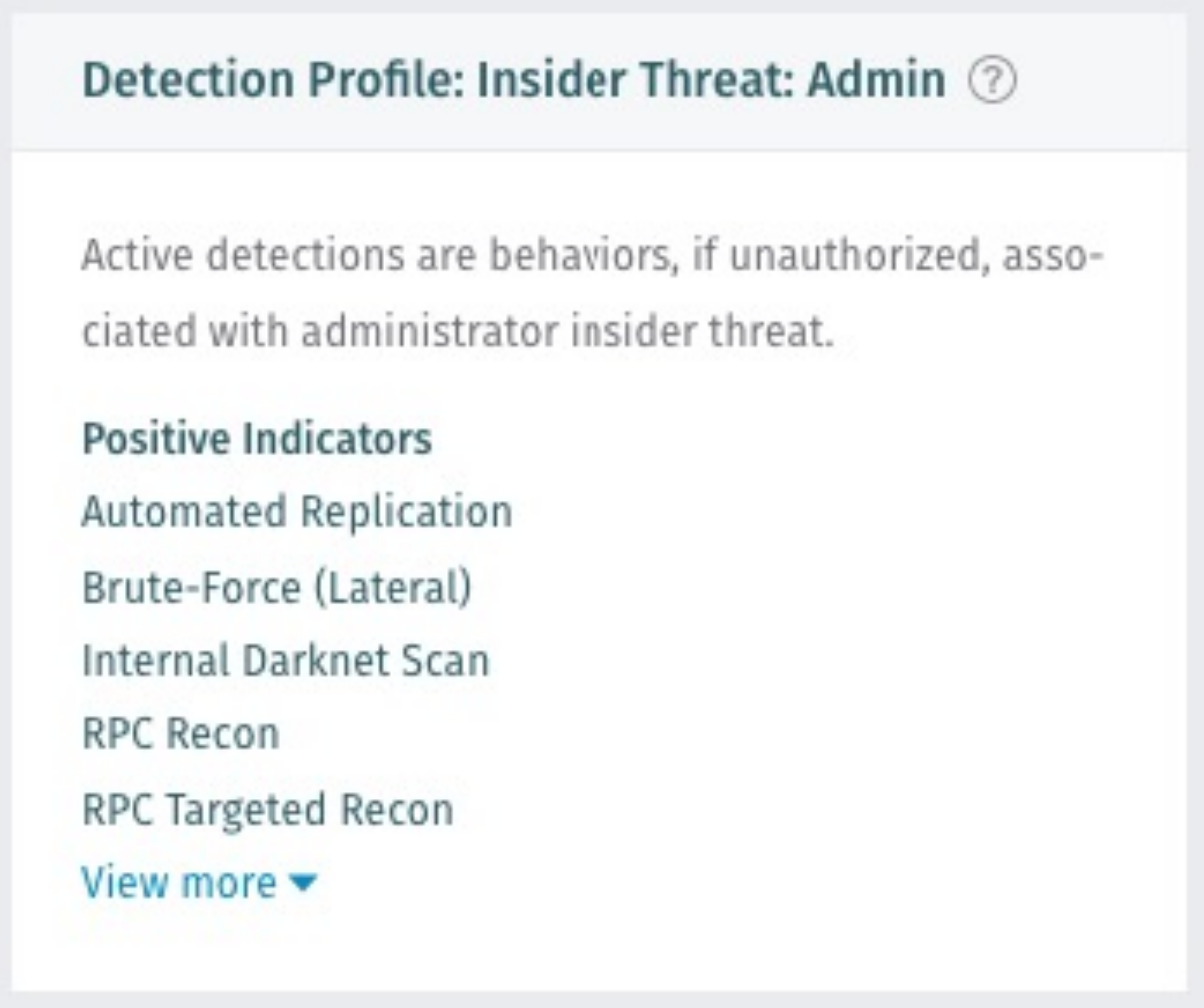


Category: All

Status: All

Sensor: All

CATEGORY	TYPE	THREAT	CERTAINTY
Recon	Internal Darknet Scan	60	68
Recon	Port Scan	60	80
Recon	RDP Recon	70	95
Lateral	Brute-Force	30	40
Lateral	Automated Replication	67	61
Info	Novel Admin Protocol Usage	–	–
Info	New Host	–	–



Detection Profile: Insider Threat: Admin ?

Active detections are behaviors, if unauthorized, associated with administrator insider threat.

Positive Indicators

Automated Replication

Brute-Force (Lateral)

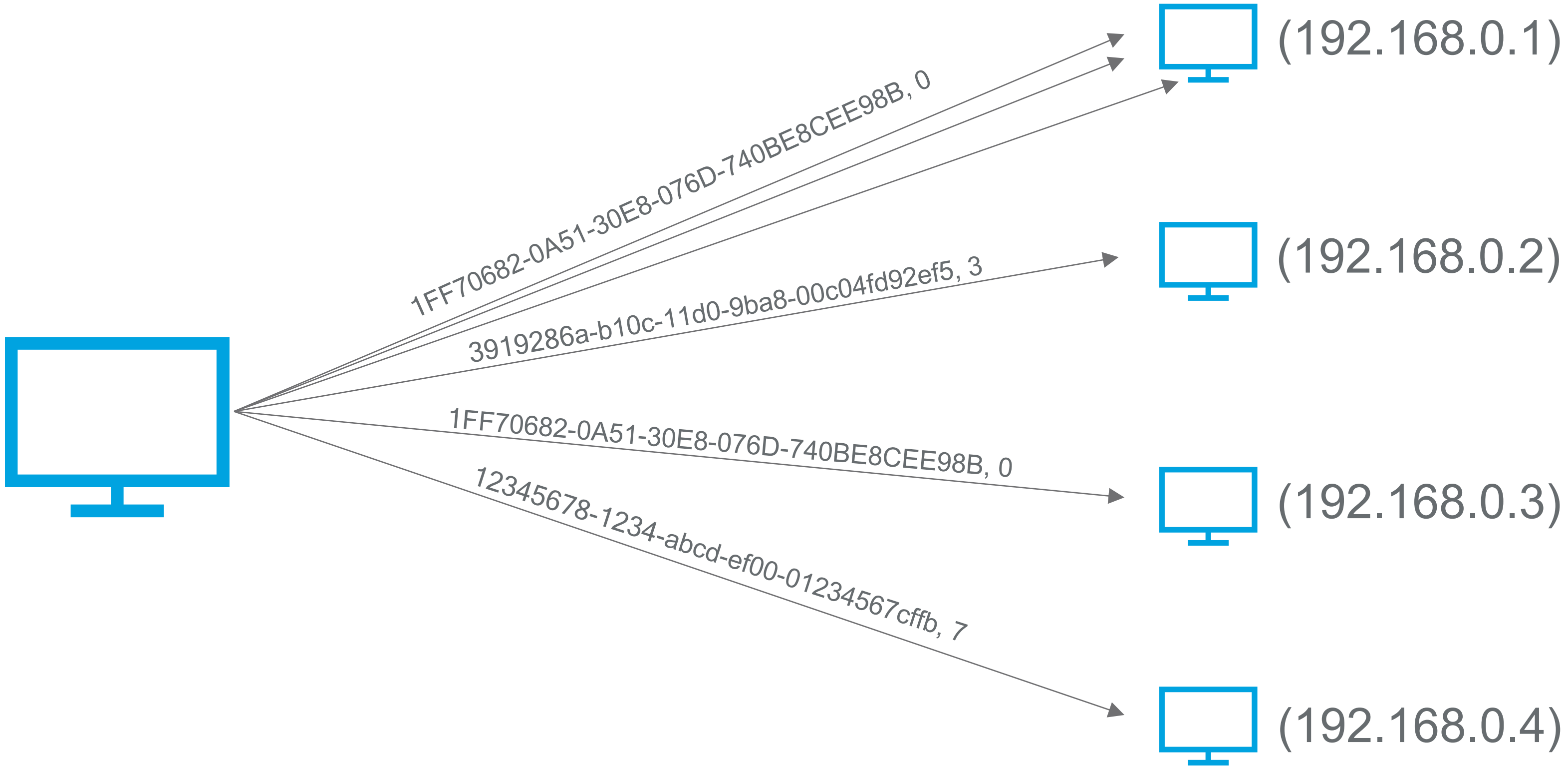
Internal Darknet Scan

RPC Recon

RPC Targeted Recon

Detection Detail: RPC Recon

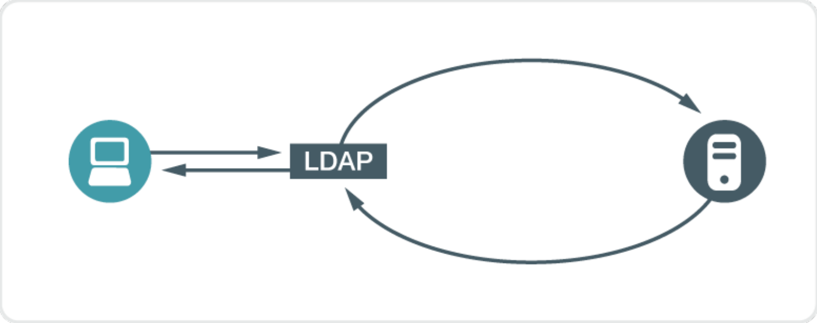
- Is the breadth of RPC activity on this host session abnormal?
  - Is it reaching out to far more than we expect given what was learned during the learning period?


1FF70682-0A51-30E8-076D-740BE8CEE98B, 0
(192.168.0.1)
3919286a-b10c-11d0-9ba8-00c04fd92ef5, 3
(192.168.0.2)
1FF70682-0A51-30E8-076D-740BE8CEE98B, 0
(192.168.0.3)
12345678-1234-abcd-ef00-01234567cffb, 7
(192.168.0.4)

Detection Detail: Suspicious LDAP Query

- A primary goal of an attacker is to elevate privileges or find existing credentials. Using existing credentials is desired but the attacker must first find the accounts they are interested in.

- Suspicious LDAP Query is designed to identify when an internal host is querying Active Directory using the LDAP protocol in a manner that appears like reconnaissance behavior.



Insider Threat: Admin

General Behavioral Profile

- Technically sophisticated, objective-oriented activities
- Advanced discovery and lateral movement techniques
- NOT PRESENT: External Command and Control and/or Data Exfiltration

Possible Root Causes

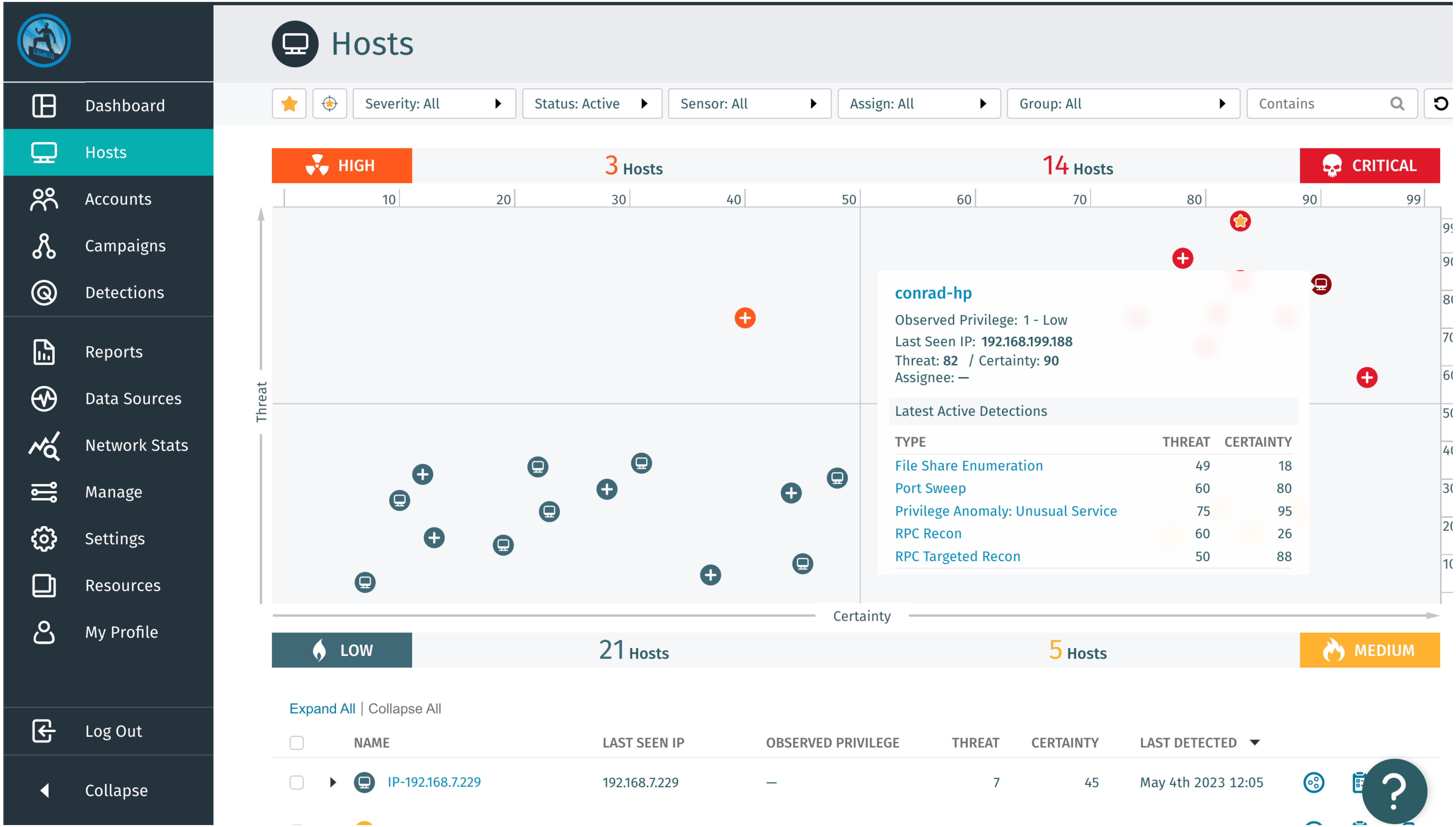
- Technically sophisticated insider threat with local network access
- Emerging External Adversary with an out-of-band communication
- An Admin has begun performing authorized activities that were previously unknown to the system

Summing It Up

- The Vectra System detected, labeled, and exposed behavior from a technically sophisticated actor.
- The operations included reconnaissance, lateral movement, and exfiltration
- In day-to-day operations, analysts working with the detections Vectra provided would stop the threat well before the exfiltration stage

But, What If…?

APR
$1.00 U.K. 40p
#32
MARVEL® COMICS GROUP
APPROVED BY THE COMICS CODE AUTHORITY
WHAT IF THE AVENGERS HAD BECOME PAWNS OF KORVAC?
FEATURING THE MOST AWESOME COLLECTION OF COSMIC BEINGS EVER UNITED TOGETHER IN COMMON CAUSE!



Hosts

Severity: All | Status: Active | Sensor: All | Assign: All | Group: All | Contains

3 Hosts

14 Hosts

21 Hosts

5 Hosts

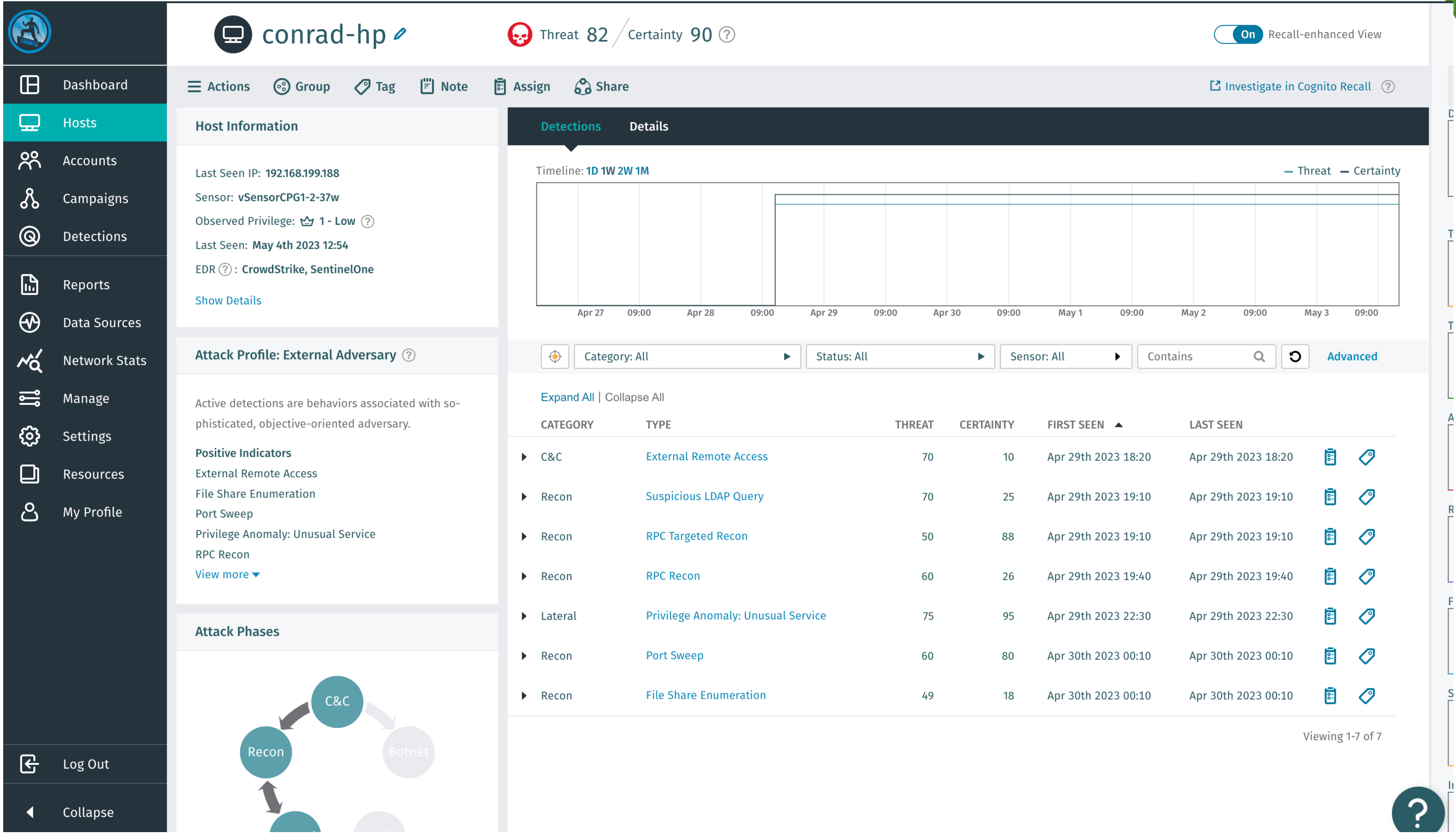
conrad-hp

Observed Privilege: 1 - Low
Last Seen IP: **192.168.199.188**
Threat: **82** / Certainty: **90**
Assignee: —

Latest Active Detections

TYPE	THREAT	CERTAINTY
File Share Enumeration	49	18
Port Sweep	60	80
Privilege Anomaly: Unusual Service	75	95
RPC Recon	60	26
RPC Targeted Recon	50	88

☐	NAME	LAST SEEN IP	OBSERVED PRIVILEGE	THREAT	CERTAINTY	LAST DETECTED
☐	IP-192.168.7.229	192.168.7.229	—	7	45	May 4th 2023 12:05



conrad-hp

Threat 82 / Certainty 90

Host Information

Last Seen IP: 192.168.199.188

Sensor: vSensorCPG1-2-37w

Observed Privilege: 1 - Low

Last Seen: May 4th 2023 12:54

EDR: CrowdStrike, SentinelOne

Show Details

Attack Profile: External Adversary

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

Positive Indicators

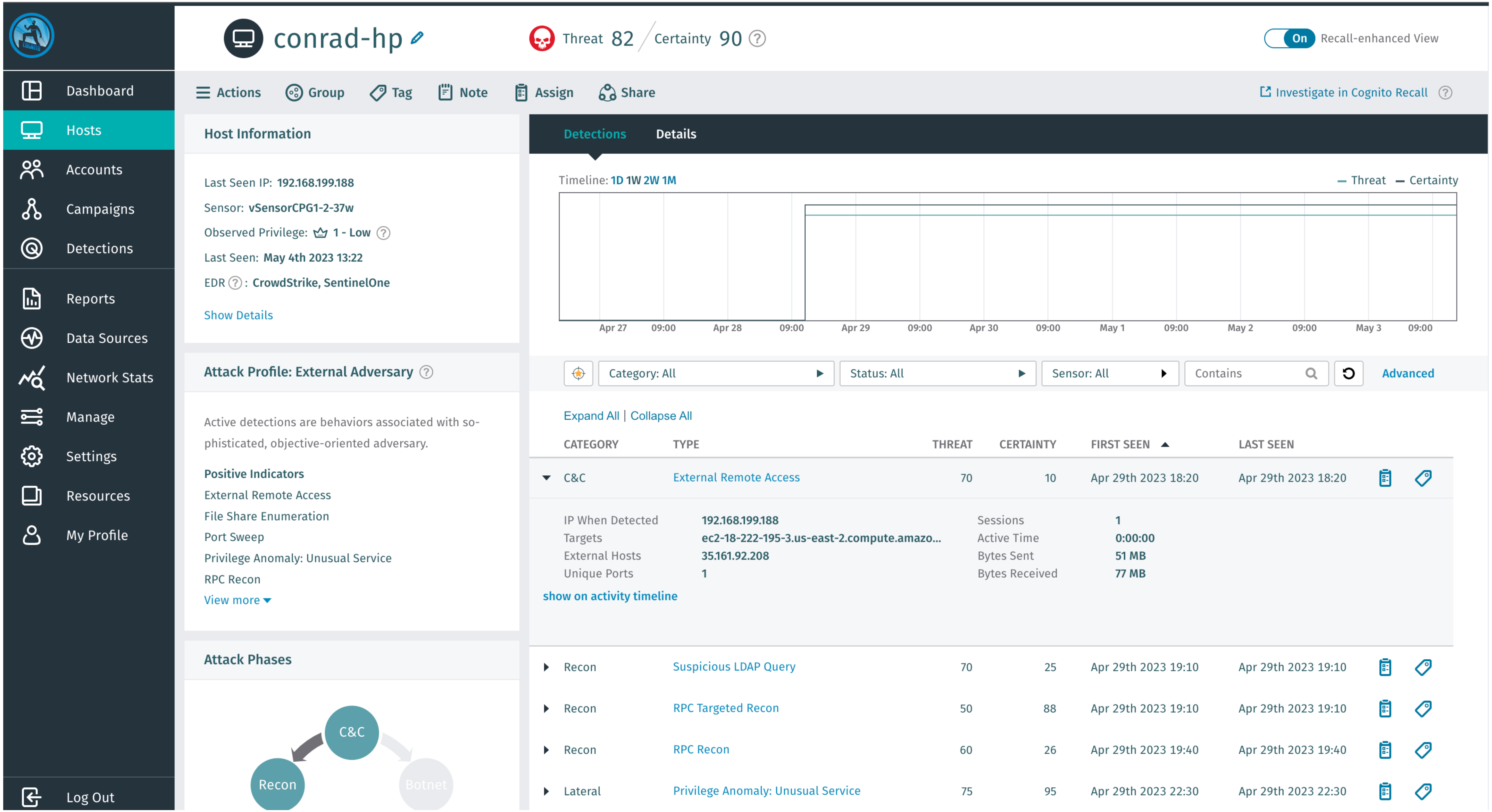
External Remote Access
File Share Enumeration
Port Sweep
Privilege Anomaly: Unusual Service
RPC Recon
View more

Attack Phases

CATEGORY	TYPE	THREAT	CERTAINTY	FIRST SEEN ▲	LAST SEEN
C&C	External Remote Access	70	10	Apr 29th 2023 18:20	Apr 29th 2023 18:20
Recon	Suspicious LDAP Query	70	25	Apr 29th 2023 19:10	Apr 29th 2023 19:10
Recon	RPC Targeted Recon	50	88	Apr 29th 2023 19:10	Apr 29th 2023 19:10
Recon	RPC Recon	60	26	Apr 29th 2023 19:40	Apr 29th 2023 19:40
Lateral	Privilege Anomaly: Unusual Service	75	95	Apr 29th 2023 22:30	Apr 29th 2023 22:30
Recon	Port Sweep	60	80	Apr 30th 2023 00:10	Apr 30th 2023 00:10
Recon	File Share Enumeration	49	18	Apr 30th 2023 00:10	Apr 30th 2023 00:10

Viewing 1-7 of 7

VECTRA
SECURITY THAT THINKS.®



conrad-hp

Threat 82 / Certainty 90

Host Information

Last Seen IP: **192.168.199.188**

Sensor: **vSensorCPG1-2-37w**

Observed Privilege: **1 - Low**

Last Seen: **May 4th 2023 13:22**

EDR: **CrowdStrike, SentinelOne**

Show Details

Attack Profile: External Adversary

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

Positive Indicators

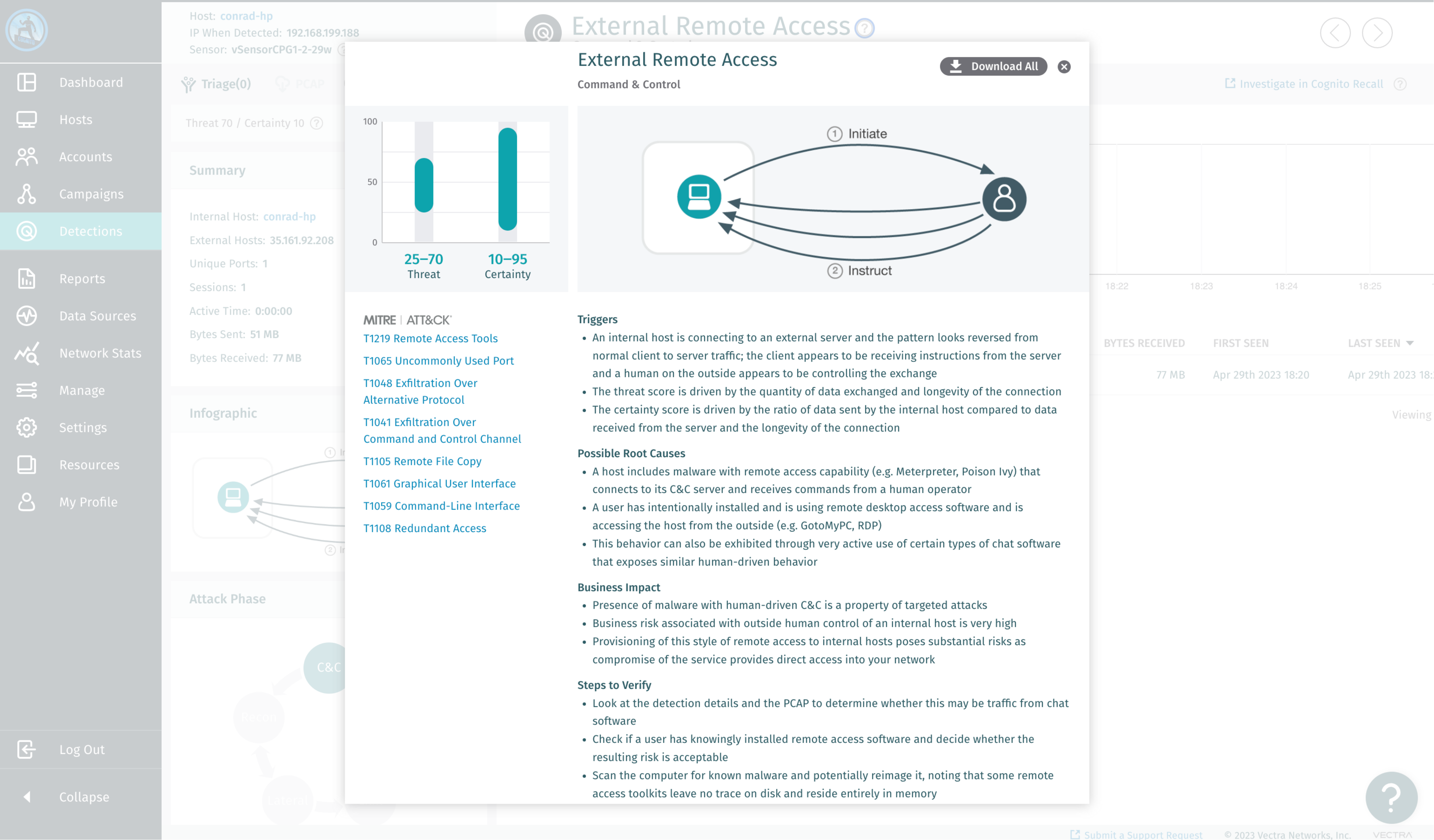
External Remote Access
File Share Enumeration
Port Sweep
Privilege Anomaly: Unusual Service
RPC Recon
View more

Attack Phases

CATEGORY	TYPE	THREAT	CERTAINTY	FIRST SEEN	LAST SEEN
C&C	External Remote Access	70	10	Apr 29th 2023 18:20	Apr 29th 2023 18:20
Recon	Suspicious LDAP Query	70	25	Apr 29th 2023 19:10	Apr 29th 2023 19:10
Recon	RPC Targeted Recon	50	88	Apr 29th 2023 19:10	Apr 29th 2023 19:10
Recon	RPC Recon	60	26	Apr 29th 2023 19:40	Apr 29th 2023 19:40
Lateral	Privilege Anomaly: Unusual Service	75	95	Apr 29th 2023 22:30	Apr 29th 2023 22:30

IP When Detected	192.168.199.188	Sessions	1
Targets	ec2-18-222-195-3.us-east-2.compute.amazo...	Active Time	0:00:00
External Hosts	35.161.92.208	Bytes Sent	51 MB
Unique Ports	1	Bytes Received	77 MB

show on activity timeline



Host: conrad-hp
IP When Detected: 192.168.199.188
Sensor: vSensorCPG1-2-29w

External Remote Access

Threat 70 / Certainty 10

Summary

Internal Host: conrad-hp
External Hosts: 35.161.92.208
Unique Ports: 1
Sessions: 1
Active Time: 0:00:00
Bytes Sent: 51 MB
Bytes Received: 77 MB

Infographic

Attack Phase

BYTES RECEIVED	FIRST SEEN	LAST SEEN
77 MB	Apr 29th 2023 18:20	Apr 29th 2023 18:

External Remote Access

Command & Control

25–70 Threat
10–95 Certainty

MITRE | ATT&CK
- T1219 Remote Access Tools
- T1065 Uncommonly Used Port
- T1048 Exfiltration Over Alternative Protocol
- T1041 Exfiltration Over Command and Control Channel
- T1105 Remote File Copy
- T1061 Graphical User Interface
- T1059 Command-Line Interface
- T1108 Redundant Access

Triggers
- An internal host is connecting to an external server and the pattern looks reversed from normal client to server traffic; the client appears to be receiving instructions from the server and a human on the outside appears to be controlling the exchange
- The threat score is driven by the quantity of data exchanged and longevity of the connection
- The certainty score is driven by the ratio of data sent by the internal host compared to data received from the server and the longevity of the connection

Possible Root Causes
- A host includes malware with remote access capability (e.g. Meterpreter, Poison Ivy) that connects to its C&C server and receives commands from a human operator
- A user has intentionally installed and is using remote desktop access software and is accessing the host from the outside (e.g. GotoMyPC, RDP)
- This behavior can also be exhibited through very active use of certain types of chat software that exposes similar human-driven behavior

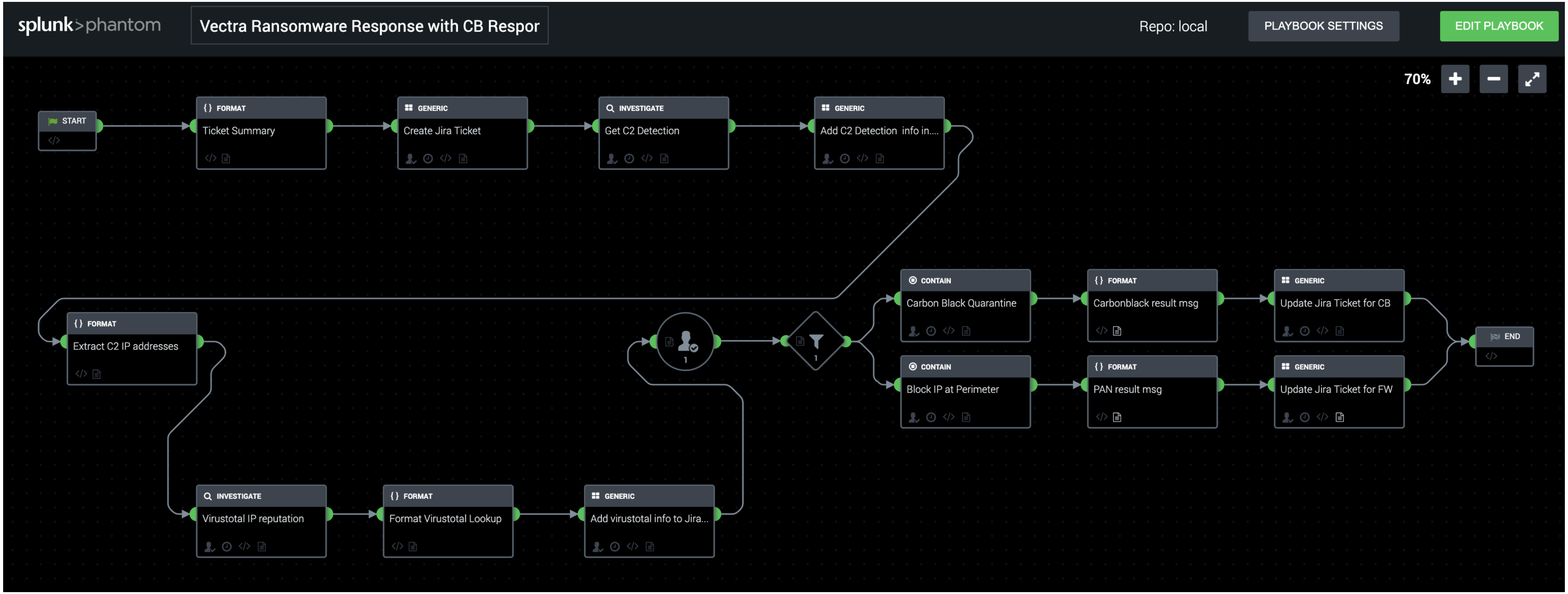
Business Impact
- Presence of malware with human-driven C&C is a property of targeted attacks
- Business risk associated with outside human control of an internal host is very high
- Provisioning of this style of remote access to internal hosts poses substantial risks as compromise of the service provides direct access into your network

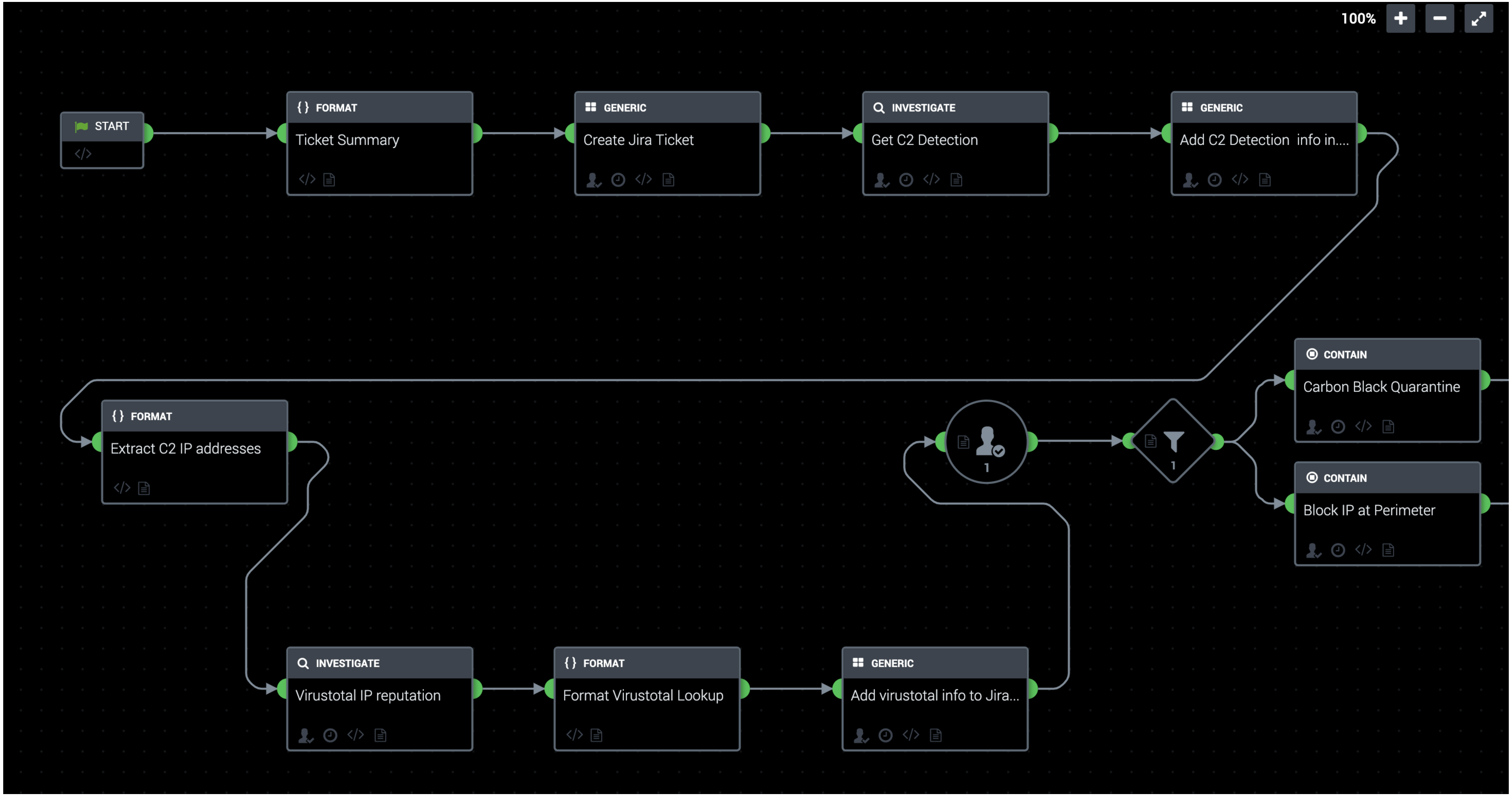
Steps to Verify
- Look at the detection details and the PCAP to determine whether this may be traffic from chat software
- Check if a user has knowingly installed remote access software and decide whether the resulting risk is acceptable
- Scan the computer for known malware and potentially reimage it, noting that some remote access toolkits leave no trace on disk and reside entirely in memory

© 2023 Vectra Networks, Inc.

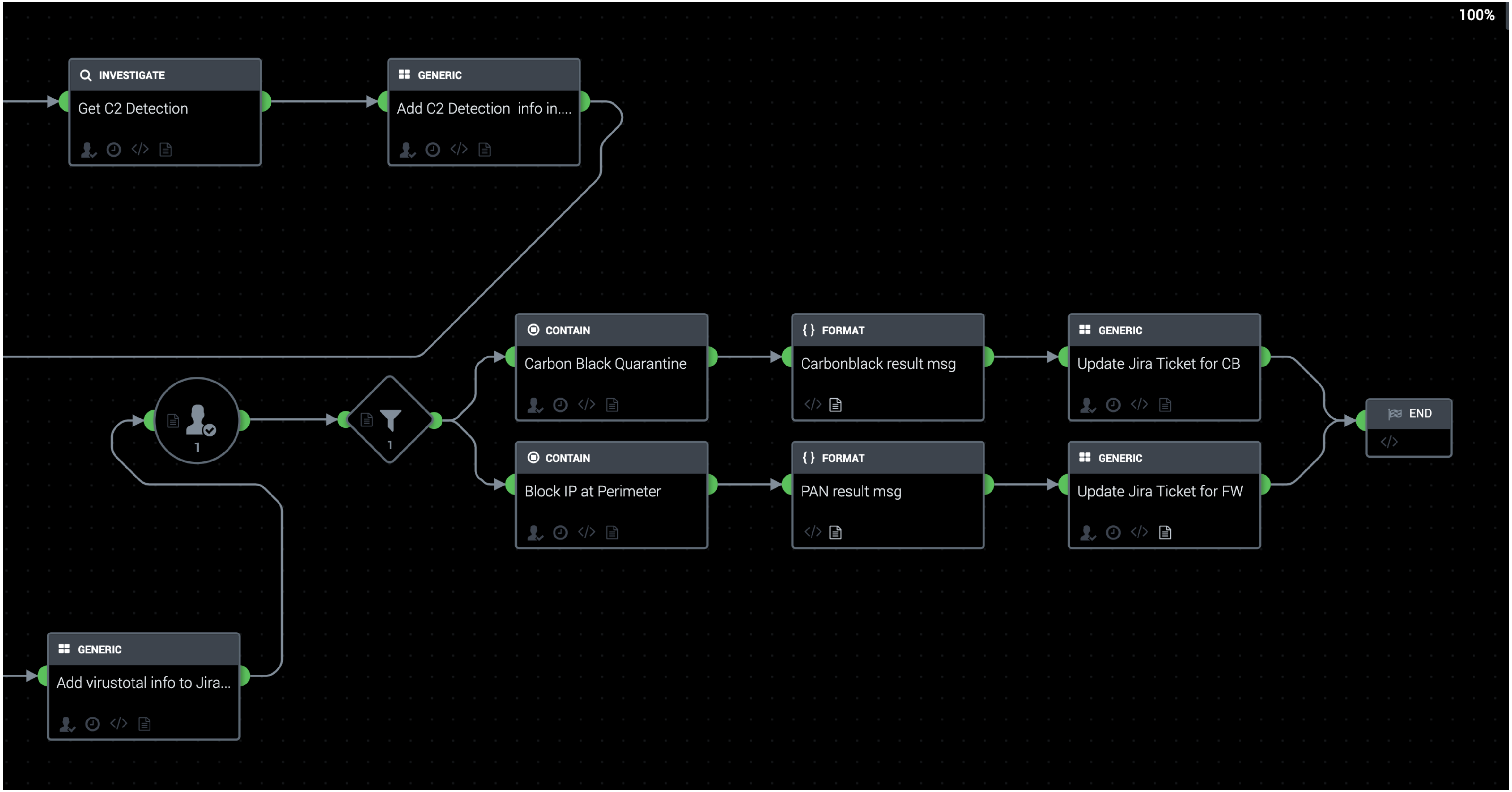
But, What If…?

MARVEL COMICS
WHAT IF...
SPIDER-MAN
HAD KEPT HIS SIX ARMS?
$1.25 US
$1.50 CAN
42
OCT
UK 85p
APPROVED BY THE COMICS CODE AUTHORITY
30TH ANNIVERSARY
1962 1992
THE AMAZING SPIDER-MAN

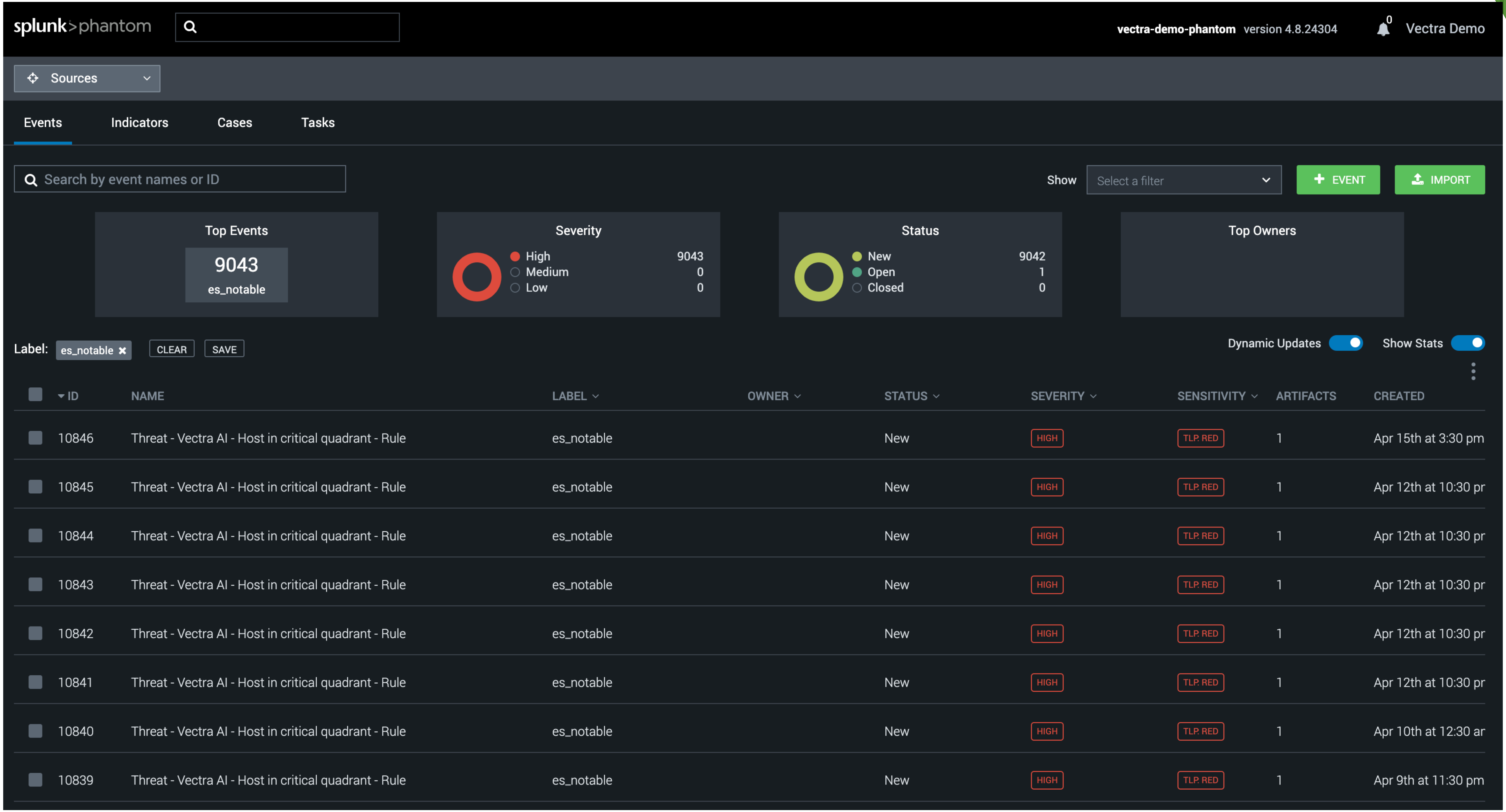

splunk>phantom
Vectra Ransomware Response with CB Respor
Repo: local
PLAYBOOK SETTINGS
EDIT PLAYBOOK
70%
START
FORMAT
Ticket Summary
GENERIC
Create Jira Ticket
INVESTIGATE
Get C2 Detection
GENERIC
Add C2 Detection info in....
FORMAT
Extract C2 IP addresses
1
1
CONTAIN
Carbon Black Quarantine
FORMAT
Carbonblack result msg
GENERIC
Update Jira Ticket for CB
CONTAIN
Block IP at Perimeter
FORMAT
PAN result msg
GENERIC
Update Jira Ticket for FW
END
INVESTIGATE
Virustotal IP reputation
FORMAT
Format Virustotal Lookup
GENERIC
Add virustotal info to Jira...



VECTRA
SECURITY THAT THINKS.®



VECTRA
SECURITY THAT THINKS.®



splunk>phantom

vectra-demo-phantom version 4.8.24304

Vectra Demo

Sources

Events | Indicators | Cases | Tasks

Search by event names or ID

Show: Select a filter

+ EVENT

IMPORT

Top Events

9043
es_notable

Severity

● High	9043
○ Medium	0
○ Low	0

Status

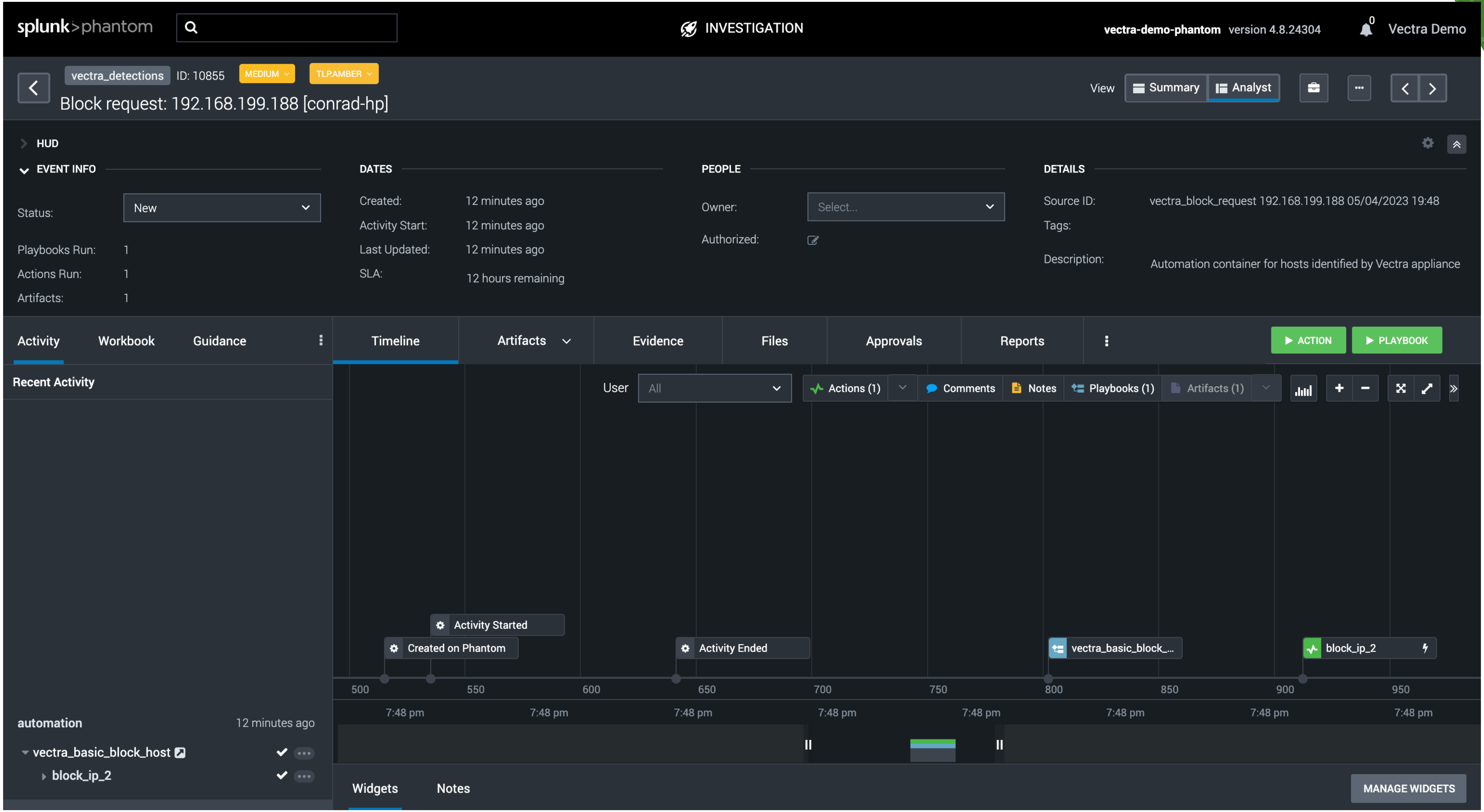
● New	9042
● Open	1
○ Closed	0

Top Owners

Label: es_notable ✖ CLEAR SAVE

Dynamic Updates ● Show Stats ●

□	ID	NAME	LABEL	OWNER	STATUS	SEVERITY	SENSITIVITY	ARTIFACTS	CREATED
□	10846	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 15th at 3:30 pm
□	10845	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 12th at 10:30 pr
□	10844	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 12th at 10:30 pr
□	10843	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 12th at 10:30 pr
□	10842	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 12th at 10:30 pr
□	10841	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 12th at 10:30 pr
□	10840	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 10th at 12:30 ar
□	10839	Threat - Vectra AI - Host in critical quadrant - Rule	es_notable		New	HIGH	TLP: RED	1	Apr 9th at 11:30 pm



splunk>phantom

INVESTIGATION

vectra-demo-phantom version 4.8.24304

Vectra Demo

vectra_detections ID: 10855 MEDIUM TLP:AMBER

Block request: 192.168.199.188 [conrad-hp]

View Summary Analyst

HUD

EVENT INFO

Status: New

Playbooks Run: 1

Actions Run: 1

Artifacts: 1

DATES

Created: 12 minutes ago

Activity Start: 12 minutes ago

Last Updated: 12 minutes ago

SLA: 12 hours remaining

PEOPLE

Owner: Select...

Authorized:

DETAILS

Source ID: vectra_block_request 192.168.199.188 05/04/2023 19:48

Tags:

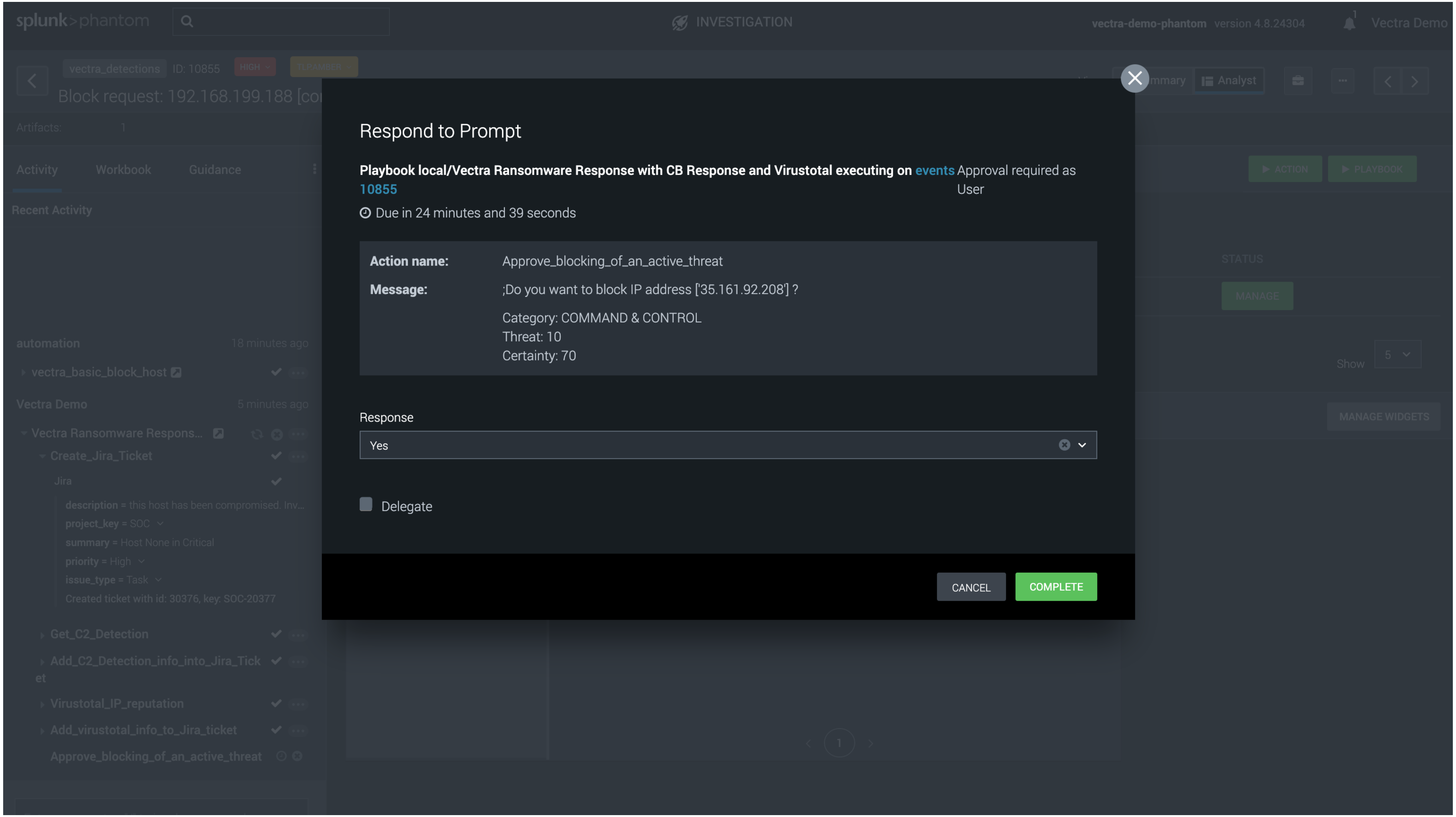
Description: Automation container for hosts identified by Vectra appliance

automation 12 minutes ago

vectra_basic_block_host ✓

block_ip_2 ✓

VECTRA
SECURITY THAT THINKS.®



automation 18 minutes ago

- vectra_basic_block_host ✓

Vectra Demo 5 minutes ago

- Vectra Ransomware Respons...
  - Create_Jira_Ticket ✓
    - Jira ✓
      - description = this host has been compromised. Inv...
      - project_key = SOC
      - summary = Host None in Critical
      - priority = High
      - issue_type = Task
      - Created ticket with id: 30376, key: SOC-20377
  - Get_C2_Detection ✓
  - Add_C2_Detection_info_into_Jira_Ticket ✓
  - Virustotal_IP_reputation ✓
  - Add_virustotal_info_to_Jira_ticket ✓
  - Approve_blocking_of_an_active_threat

Respond to Prompt

Playbook local/Vectra Ransomware Response with CB Response and Virustotal executing on events 10855 Approval required as User

Due in 24 minutes and 39 seconds

Action name: Approve_blocking_of_an_active_threat

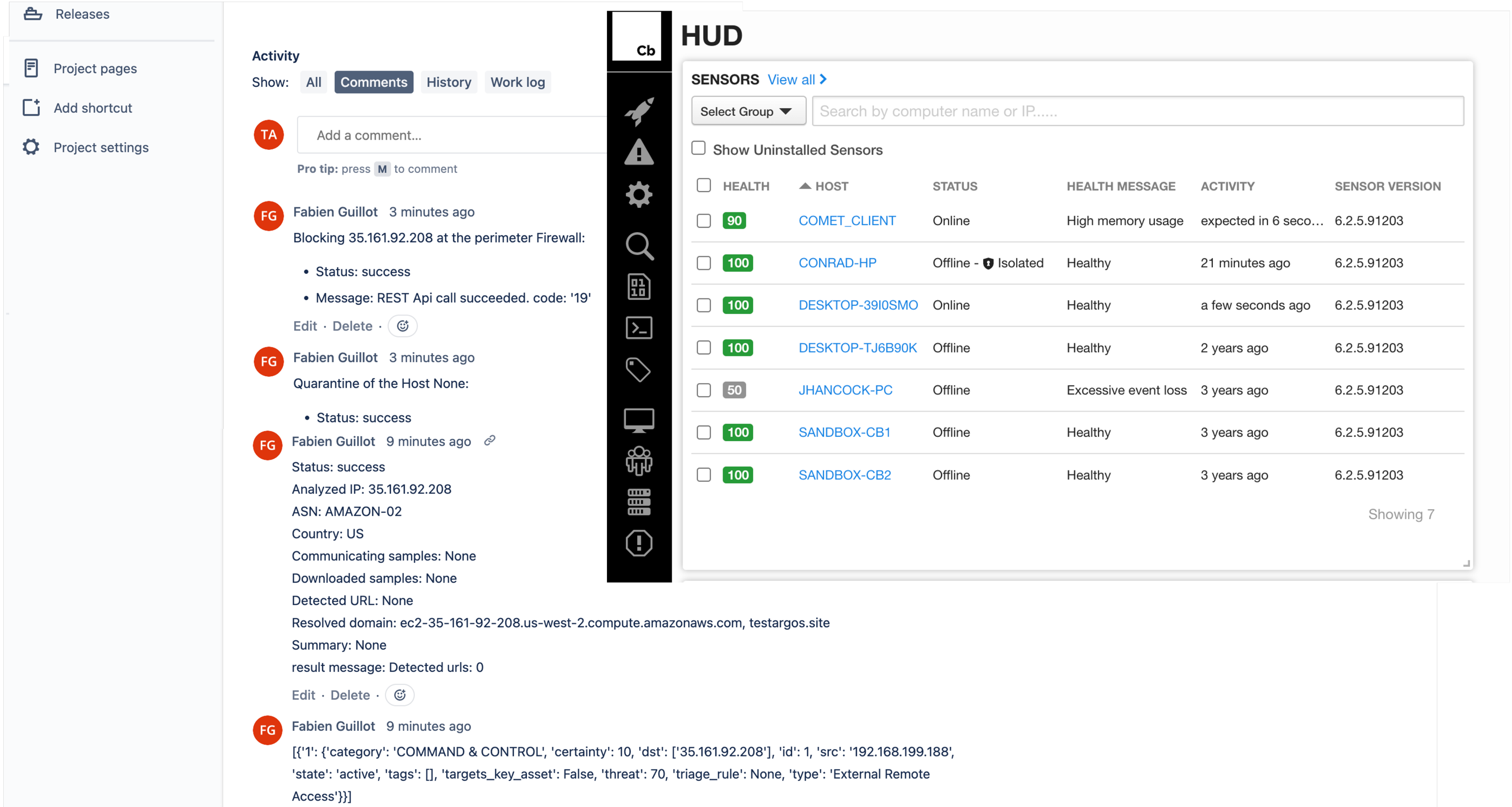
Message: ;Do you want to block IP address ['35.161.92.208'] ?

Category: COMMAND & CONTROL
Threat: 10
Certainty: 70

Response: Yes

□ Delegate

CANCEL COMPLETE



Activity

Show: All **Comments** History Work log

TA Add a comment...

Pro tip: press M to comment

FG Fabien Guillot 3 minutes ago

Blocking 35.161.92.208 at the perimeter Firewall:

- Status: success
- Message: REST Api call succeeded. code: '19'

Edit · Delete ·

FG Fabien Guillot 3 minutes ago

Quarantine of the Host None:

- Status: success

FG Fabien Guillot 9 minutes ago

Status: success
Analyzed IP: 35.161.92.208
ASN: AMAZON-02
Country: US
Communicating samples: None
Downloaded samples: None
Detected URL: None
Resolved domain: ec2-35-161-92-208.us-west-2.compute.amazonaws.com, testargos.site
Summary: None
result message: Detected urls: 0

Edit · Delete ·

FG Fabien Guillot 9 minutes ago

```
[{'1': {'category': 'COMMAND & CONTROL', 'certainty': 10, 'dst': ['35.161.92.208'], 'id': 1, 'src': '192.168.199.188',
'state': 'active', 'tags': [], 'targets_key_asset': False, 'threat': 70, 'triage_rule': None, 'type': 'External Remote
Access'}}]
```

Cb

HUD

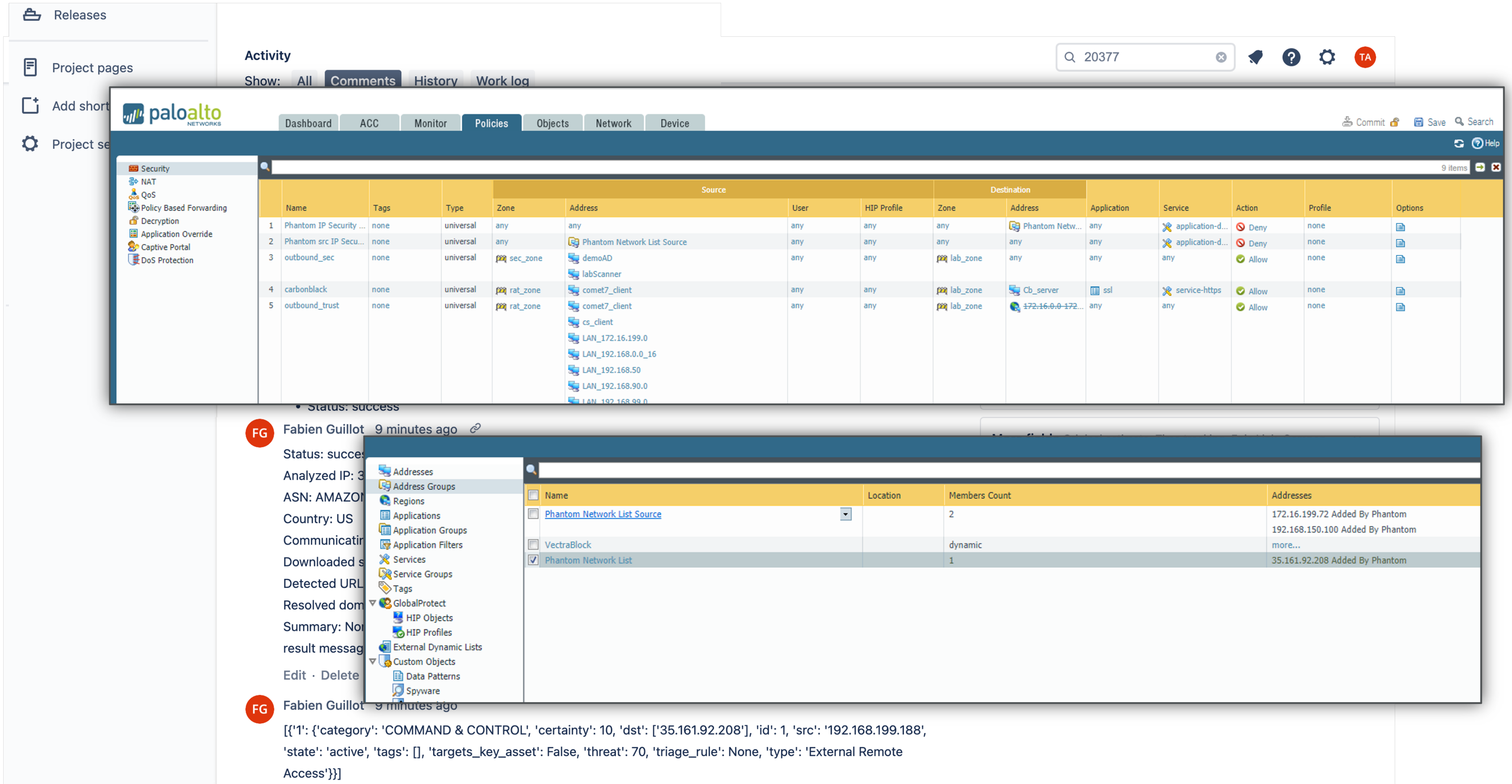
SENSORS View all >

Select Group ▼ | Search by computer name or IP......

□ Show Uninstalled Sensors

□	HEALTH	▲ HOST	STATUS	HEALTH MESSAGE	ACTIVITY	SENSOR VERSION
□	90	COMET_CLIENT	Online	High memory usage	expected in 6 seco…	6.2.5.91203
□	100	CONRAD-HP	Offline - Isolated	Healthy	21 minutes ago	6.2.5.91203
□	100	DESKTOP-39I0SMO	Online	Healthy	a few seconds ago	6.2.5.91203
□	100	DESKTOP-TJ6B90K	Offline	Healthy	2 years ago	6.2.5.91203
□	50	JHANCOCK-PC	Offline	Excessive event loss	3 years ago	6.2.5.91203
□	100	SANDBOX-CB1	Offline	Healthy	3 years ago	6.2.5.91203
□	100	SANDBOX-CB2	Offline	Healthy	3 years ago	6.2.5.91203

Showing 7



				Source				Destination						
	Name	Tags	Type	Zone	Address	User	HIP Profile	Zone	Address	Application	Service	Action	Profile	Options
1	Phantom IP Security ...	none	universal	any	any	any	any	any	Phantom Netw...	any	application-d...	Deny	none	🗎
2	Phantom src IP Secu...	none	universal	any	Phantom Network List Source	any	any	any	any	any	application-d...	Deny	none	🗎
3	outbound_sec	none	universal	sec_zone	demoAD labScanner	any	any	lab_zone	any	any	any	Allow	none	🗎
4	carbonblack	none	universal	rat_zone	comet7_client	any	any	lab_zone	Cb_server	ssl	service-https	Allow	none	🗎
5	outbound_trust	none	universal	rat_zone	comet7_client cs_client LAN_172.16.199.0 LAN_192.168.0.0_16 LAN_192.168.50 LAN_192.168.90.0 LAN_192.168.99.0	any	any	lab_zone	~~172.16.0.0-172...~~	any	any	Allow	none	🗎

- Status: success

Fabien Guillot 9 minutes ago

Status: succe

Analyzed IP: 3

ASN: AMAZO

Country: US

Communicati

Downloaded s

Detected URL

Resolved dom

Summary: No

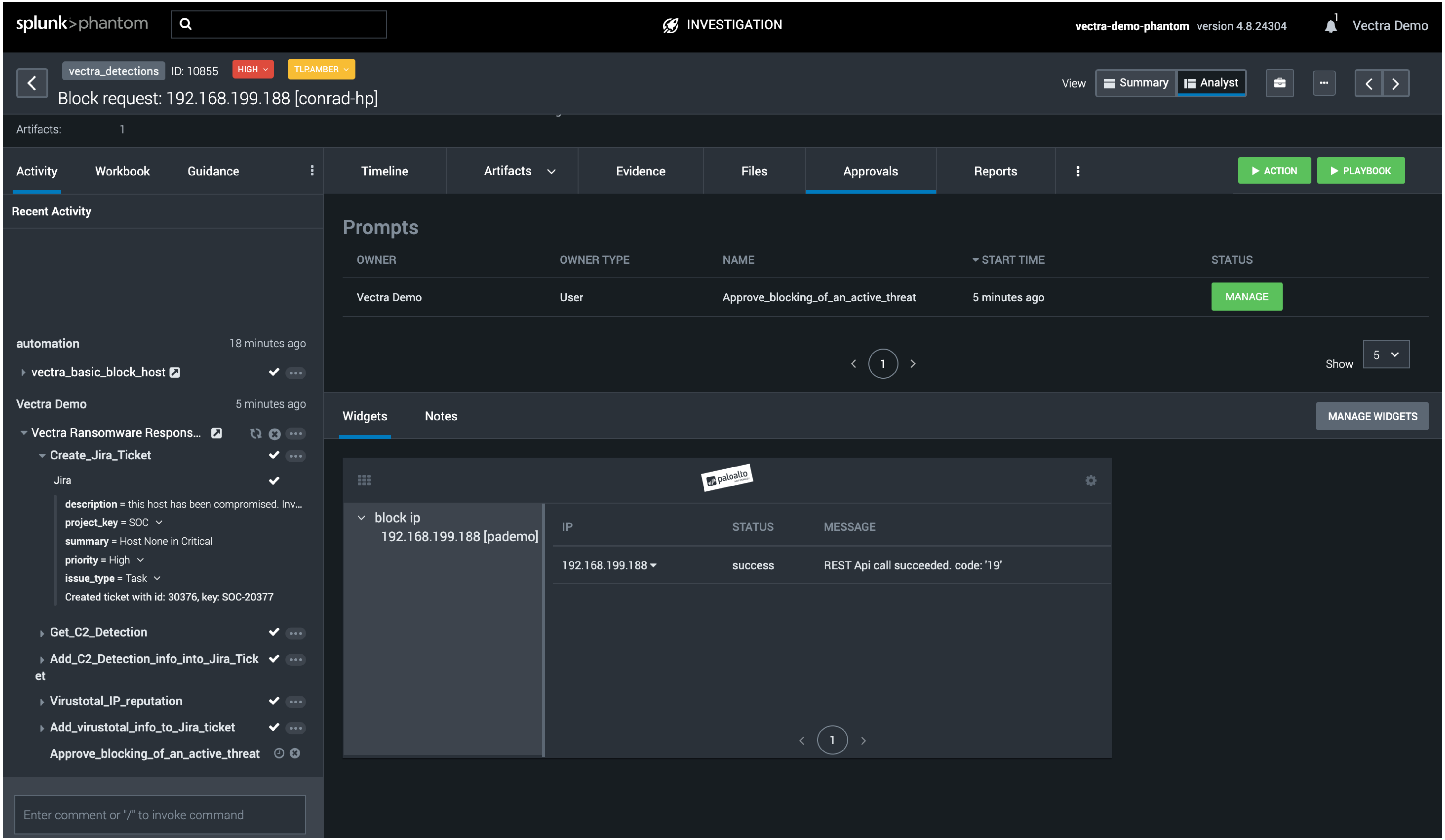
result messag

Edit · Delete

	Name	Location	Members Count	Addresses
□	Phantom Network List Source		2	172.16.199.72 Added By Phantom 192.168.150.100 Added By Phantom
□	VectraBlock		dynamic	more...
☑	Phantom Network List		1	35.161.92.208 Added By Phantom

Fabien Guillot 9 minutes ago

```
[{'1': {'category': 'COMMAND & CONTROL', 'certainty': 10, 'dst': ['35.161.92.208'], 'id': 1, 'src': '192.168.199.188',
'state': 'active', 'tags': [], 'targets_key_asset': False, 'threat': 70, 'triage_rule': None, 'type': 'External Remote
Access'}}]
```



Block request: 192.168.199.188 [conrad-hp]

automation 18 minutes ago

- vectra_basic_block_host ✓

Vectra Demo 5 minutes ago

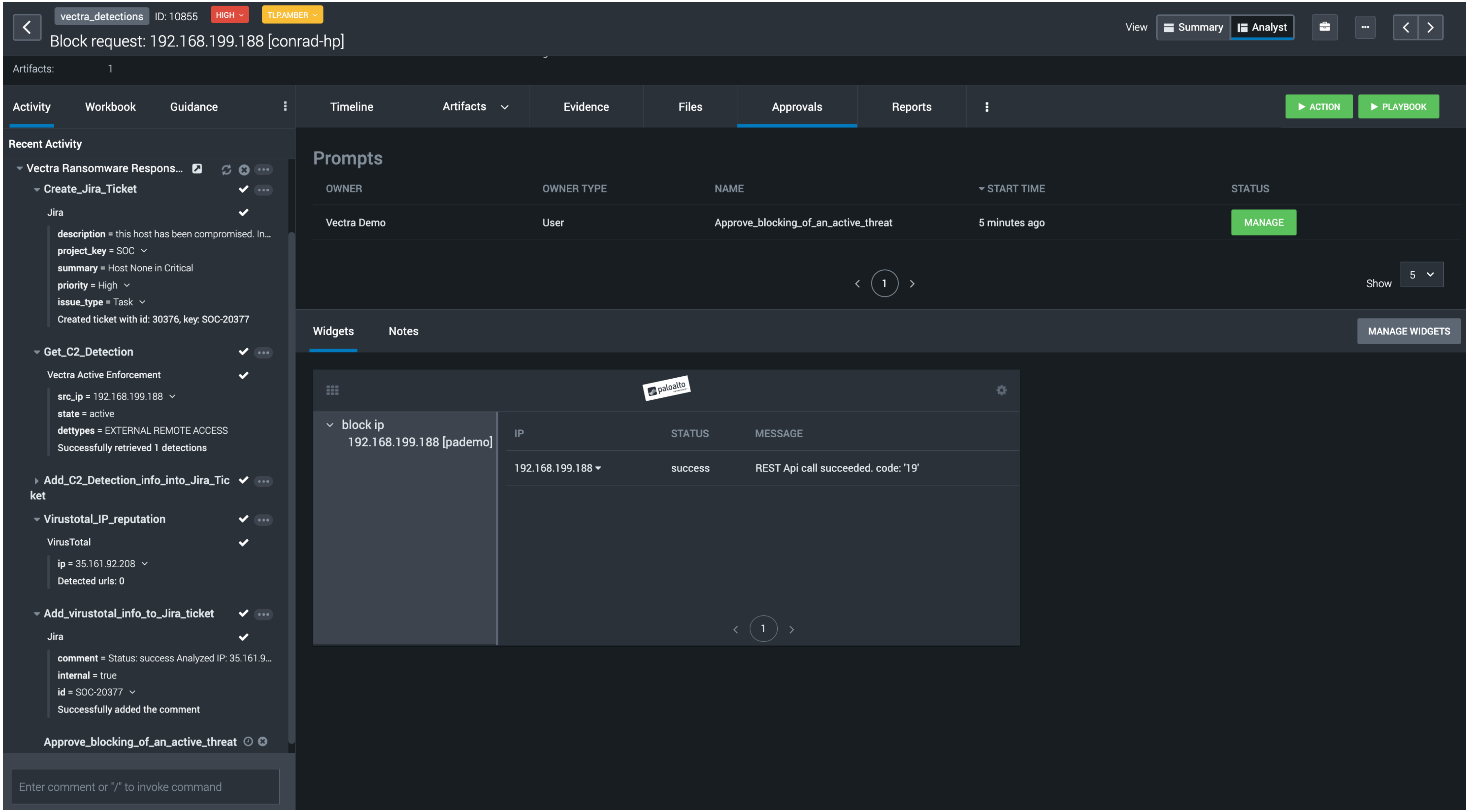
- Vectra Ransomware Respons...
  - Create_Jira_Ticket ✓
    - Jira ✓
      - **description** = this host has been compromised. Inv...
      - **project_key** = SOC
      - **summary** = Host None in Critical
      - **priority** = High
      - **issue_type** = Task
      - Created ticket with id: 30376, key: SOC-20377
  - Get_C2_Detection ✓
  - Add_C2_Detection_info_into_Jira_Ticket ✓
  - Virustotal_IP_reputation ✓
  - Add_virustotal_info_to_Jira_ticket ✓
  - Approve_blocking_of_an_active_threat

Prompts

OWNER	OWNER TYPE	NAME	START TIME	STATUS
Vectra Demo	User	Approve_blocking_of_an_active_threat	5 minutes ago	MANAGE

block ip
192.168.199.188 [pademo]

IP	STATUS	MESSAGE
192.168.199.188	success	REST Api call succeeded. code: '19'



Block request: 192.168.199.188 [conrad-hp]

Artifacts: 1

Recent Activity

- Vectra Ransomware Respons...
  - Create_Jira_Ticket ✓
    - Jira ✓
      - **description** = this host has been compromised. In...
      - **project_key** = SOC
      - **summary** = Host None in Critical
      - **priority** = High
      - **issue_type** = Task
      - Created ticket with id: 30376, key: SOC-20377
  - Get_C2_Detection ✓
    - Vectra Active Enforcement ✓
      - **src_ip** = 192.168.199.188
      - **state** = active
      - **dettypes** = EXTERNAL REMOTE ACCESS
      - Successfully retrieved 1 detections
  - Add_C2_Detection_info_into_Jira_Ticket ✓
  - Virustotal_IP_reputation ✓
    - VirusTotal ✓
      - **ip** = 35.161.92.208
      - Detected urls: 0
  - Add_virustotal_info_to_Jira_ticket ✓
    - Jira ✓
      - **comment** = Status: success Analyzed IP: 35.161.9...
      - **internal** = true
      - **id** = SOC-20377
      - Successfully added the comment
  - Approve_blocking_of_an_active_threat

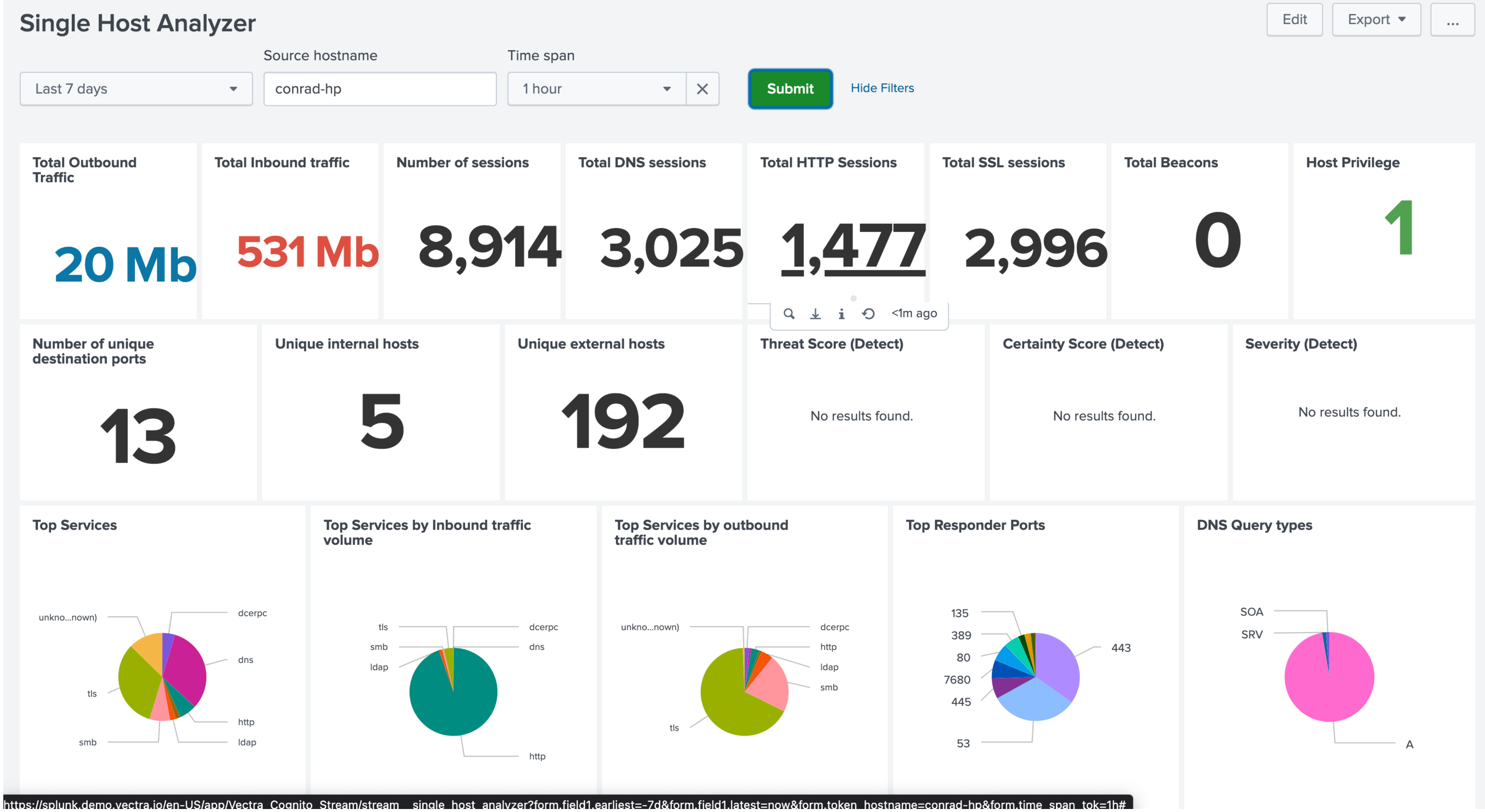
Enter comment or "/" to invoke command

Prompts

OWNER	OWNER TYPE	NAME	START TIME	STATUS
Vectra Demo	User	Approve_blocking_of_an_active_threat	5 minutes ago	MANAGE

block ip
192.168.199.188 [pademo]

IP	STATUS	MESSAGE
192.168.199.188	success	REST Api call succeeded. code: '19'



Single Host Analyzer

Edit | Export ▾ | ...

Last 7 days ▾

Source hostname: conrad-hp

Time span: 1 hour ▾ ✕

Submit | Hide Filters

Total Outbound Traffic	Total Inbound traffic	Number of sessions	Total DNS sessions	Total HTTP Sessions	Total SSL sessions	Total Beacons	Host Privilege
20 Mb	531 Mb	8,914	3,025	1,477	2,996	0	1

<1m ago

Number of unique destination ports	Unique internal hosts	Unique external hosts	Threat Score (Detect)	Certainty Score (Detect)	Severity (Detect)
13	5	192	No results found.	No results found.	No results found.

Top Services

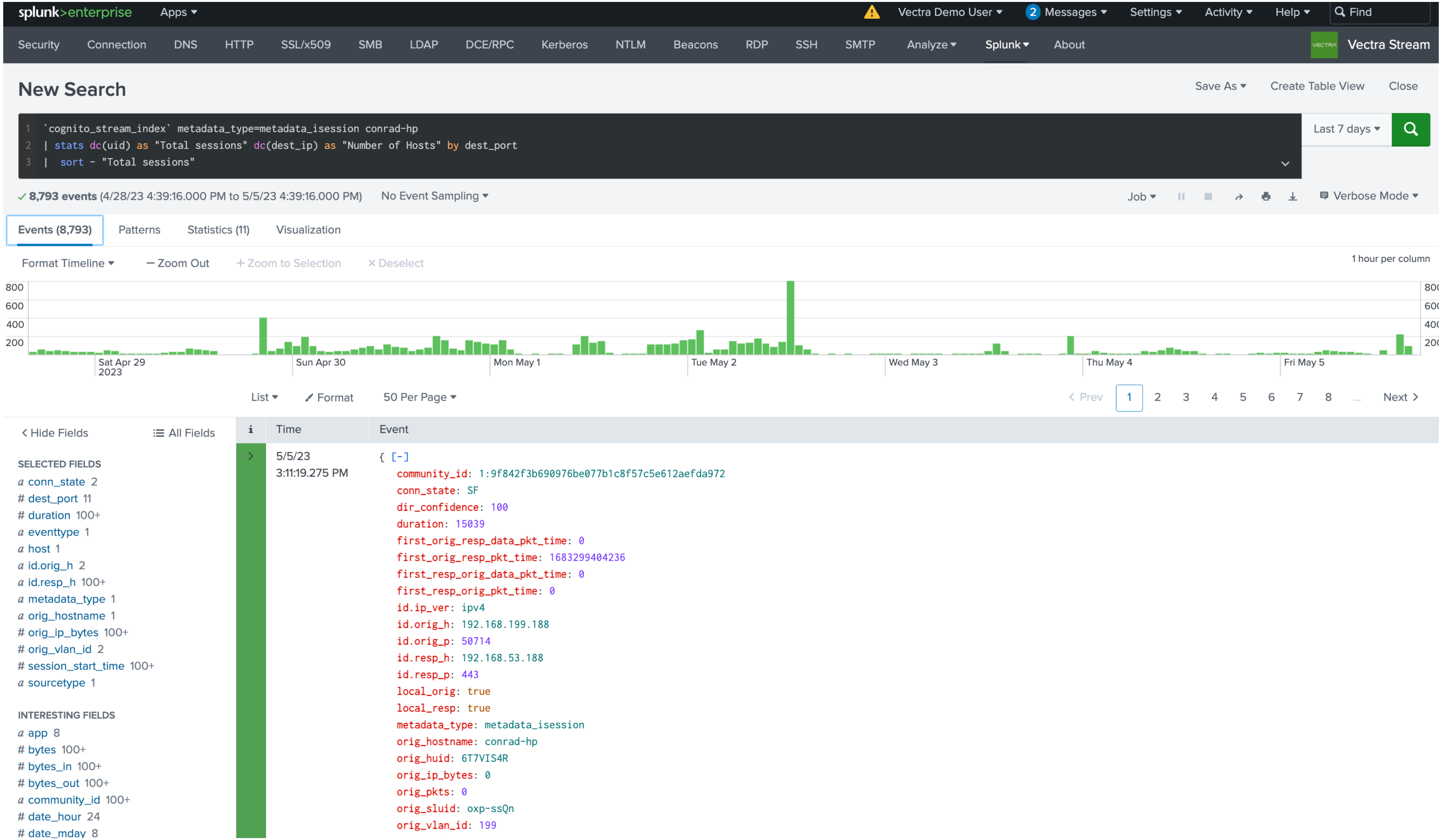
Top Services by Inbound traffic volume

Top Services by outbound traffic volume

Top Responder Ports

DNS Query types

https://splunk.demo.vectra.io/en-US/app/Vectra_Cognito_Stream/stream__single_host_analyzer?form.field1.earliest=-7d&form.field1.latest=now&form.token_hostname=conrad-hp&form.time_span_tok=1h#



New Search

```
`cognito_stream_index` metadata_type=metadata_isession conrad-hp
| stats dc(uid) as "Total sessions" dc(dest_ip) as "Number of Hosts" by dest_port
|  sort - "Total sessions"
```

✓ **8,793 events** (4/28/23 4:39:16.000 PM to 5/5/23 4:39:16.000 PM)   No Event Sampling

Events (8,793)

SELECTED FIELDS

a	conn_state	2
#	dest_port	11
#	duration	100+
a	eventtype	1
a	host	1
a	id.orig_h	2
a	id.resp_h	100+
a	metadata_type	1
a	orig_hostname	1
#	orig_ip_bytes	100+
#	orig_vlan_id	2
#	session_start_time	100+
a	sourcetype	1

INTERESTING FIELDS

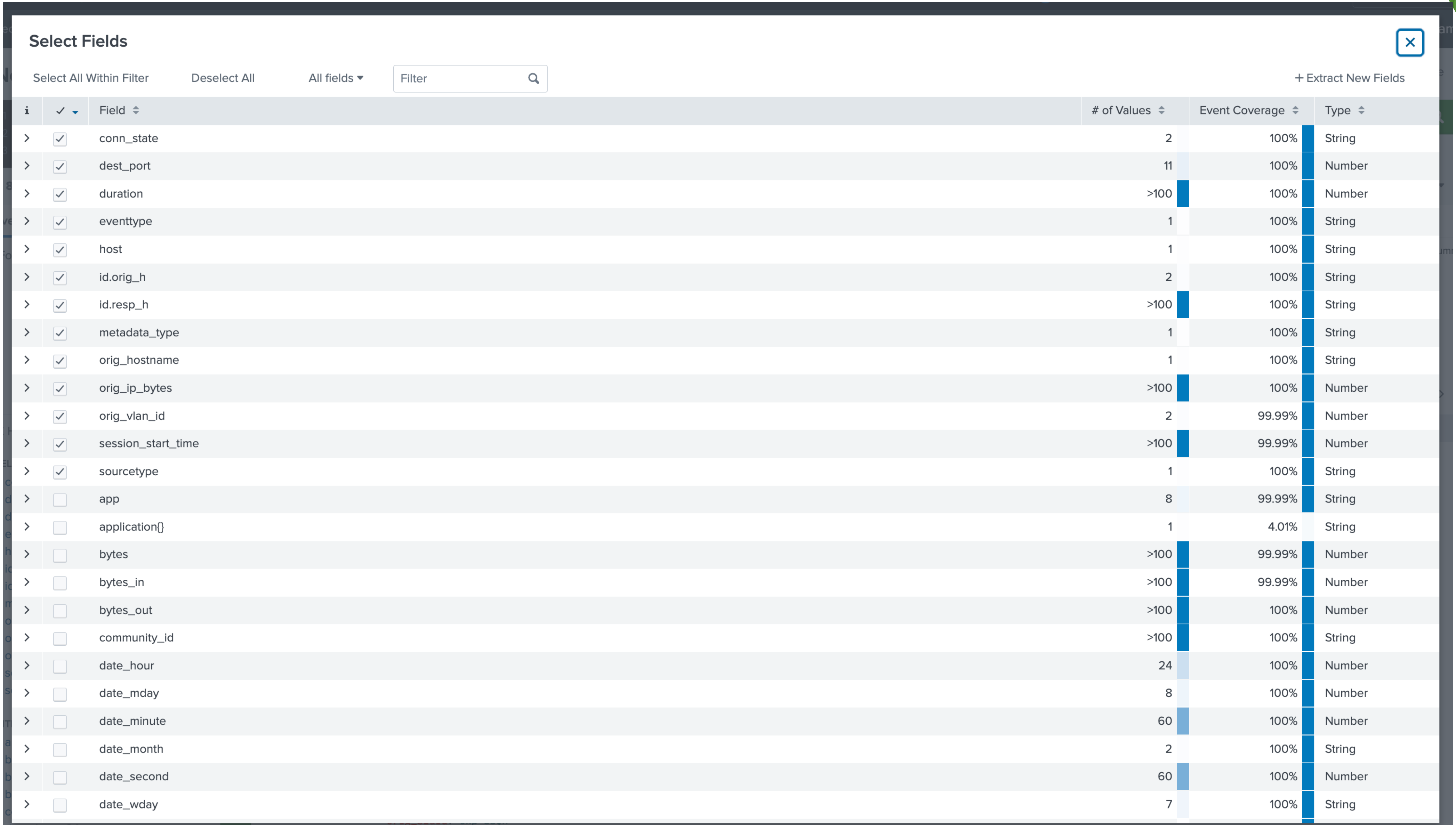
a	app	8
#	bytes	100+
#	bytes_in	100+
#	bytes_out	100+
a	community_id	100+
#	date_hour	24
#	date_mday	8

i	Time	Event
>	5/5/23 3:11:19.275 PM	see below

```
{ [-]
   community_id: 1:9f842f3b690976be077b1c8f57c5e612aefda972
   conn_state: SF
   dir_confidence: 100
   duration: 15039
   first_orig_resp_data_pkt_time: 0
   first_orig_resp_pkt_time: 1683299404236
   first_resp_orig_data_pkt_time: 0
   first_resp_orig_pkt_time: 0
   id.ip_ver: ipv4
   id.orig_h: 192.168.199.188
   id.orig_p: 50714
   id.resp_h: 192.168.53.188
   id.resp_p: 443
   local_orig: true
   local_resp: true
   metadata_type: metadata_isession
   orig_hostname: conrad-hp
   orig_huid: 6T7VIS4R
   orig_ip_bytes: 0
   orig_pkts: 0
   orig_sluid: oxp-ssQn
   orig_vlan_id: 199
```

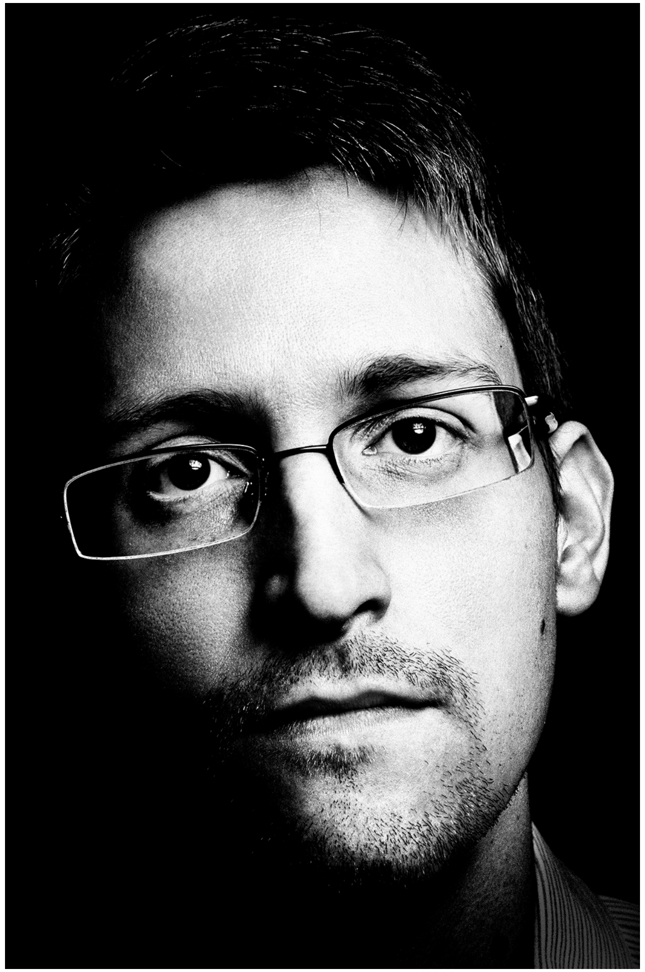
splunk>

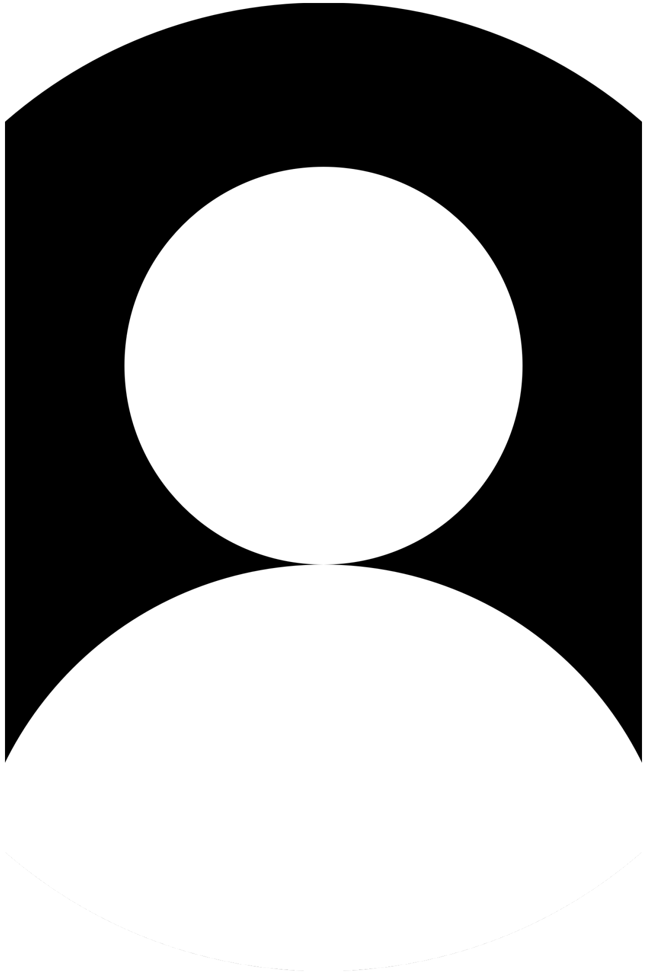
VECTRA
SECURITY THAT THINKS.



Select Fields

i	✓	Field	# of Values	Event Coverage	Type
›	☑	conn_state	2	100%	String
›	☑	dest_port	11	100%	Number
›	☑	duration	>100	100%	Number
›	☑	eventtype	1	100%	String
›	☑	host	1	100%	String
›	☑	id.orig_h	2	100%	String
›	☑	id.resp_h	>100	100%	String
›	☑	metadata_type	1	100%	String
›	☑	orig_hostname	1	100%	String
›	☑	orig_ip_bytes	>100	100%	Number
›	☑	orig_vlan_id	2	99.99%	Number
›	☑	session_start_time	>100	99.99%	Number
›	☑	sourcetype	1	100%	String
›	□	app	8	99.99%	String
›	□	application{}	1	4.01%	String
›	□	bytes	>100	99.99%	Number
›	□	bytes_in	>100	99.99%	Number
›	□	bytes_out	>100	100%	Number
›	□	community_id	>100	100%	String
›	□	date_hour	24	100%	Number
›	□	date_mday	8	100%	Number
›	□	date_minute	60	100%	Number
›	□	date_month	2	100%	String
›	□	date_second	60	100%	Number
›	□	date_wday	7	100%	String





VECTRA®

SECURITY THAT THINKS.®