WHAT CAN YOU DO WITH THE COGNITO™ PLATFORM?

Cognito is the ultimate AI-powered cyberattack-detection and threat-hunting platform.

The Cognito platform uses AI to detect attackers in real time and enrich threat investigations with a conclusive chain of forensic evidence.

DETECT CYBERATTACKS WITH COGNITO DETECT™

The most powerful way to find and stop attackers in real time.

- **Detect** unknown and hidden threats in user and IoT devices.
- **Identify** threats in the cloud and data center workloads.
- **Reduce** the security operations workload by 32x.
- **Perform** intrusion detection without signatures or reputation lists.

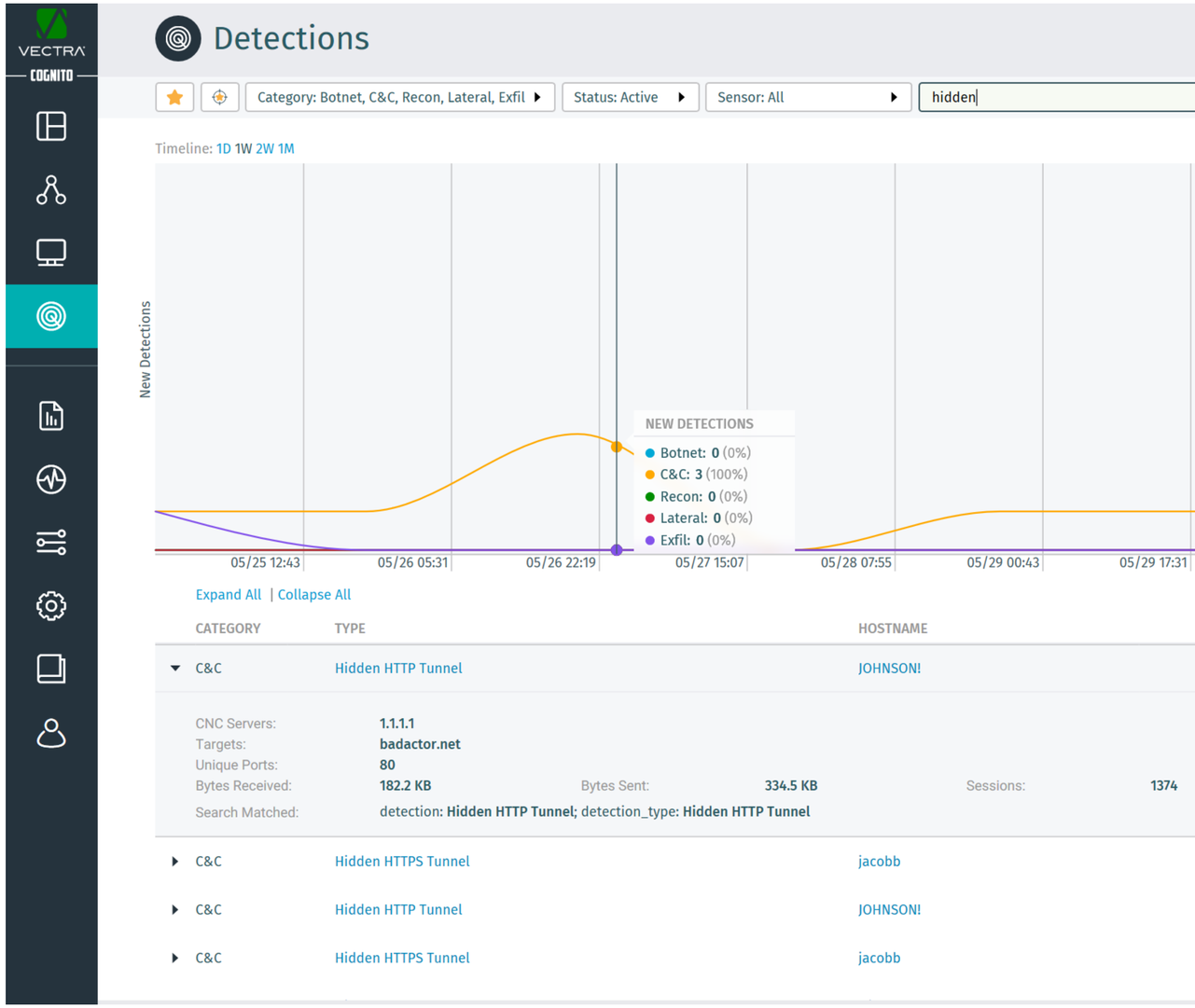
VECTRA

DETECT UNKNOWN AND HIDDEN THREATS

- **Expose** cyberattacker behaviors in encrypted traffic – without requiring decryption.
- **Identify** hidden tunnels in HTTP, HTTPS and DNS traffic that evade security enforcement points.
- **Detect** external remote access communication and customized/unknown remote access tools.

> *"Vectra detects things you wouldn't normally see."*

Sean Michael O'Connor
Assistant CIO,
Worcester Polytechnic Institute



The Cognito Hidden Tunnel Detection

VECTRA

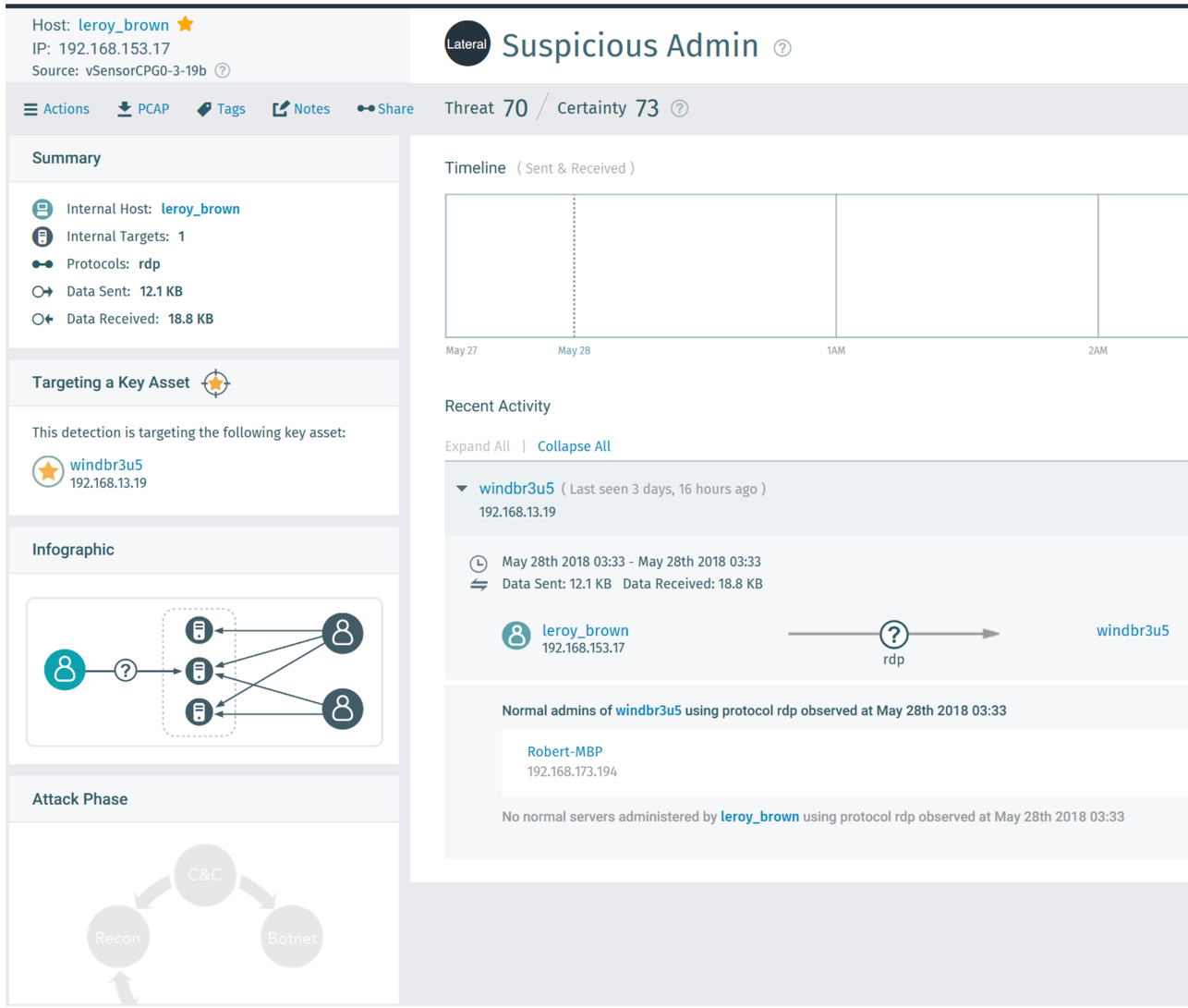
DETECT THREATS IN THE CLOUD AND DATA CENTER WORKLOADS

- **Gain visibility** into virtual environments and learn the dynamics of change, even as hosts and workloads are added, deleted or moved.
- **Automatically learn** administrative access models, including who manages specific servers and from where.
- **Detect abuse** of admin credentials and protocols, use of rootkits, hidden tunnels and backdoors, and data accumulation or exfiltration.

> *"Vectra fills a big cybersecurity void in the public cloud."*

Beau Canada
Vice President of Information Security,
Ticketmaster

VECTRA



The Cognito Suspicious Admin Detection

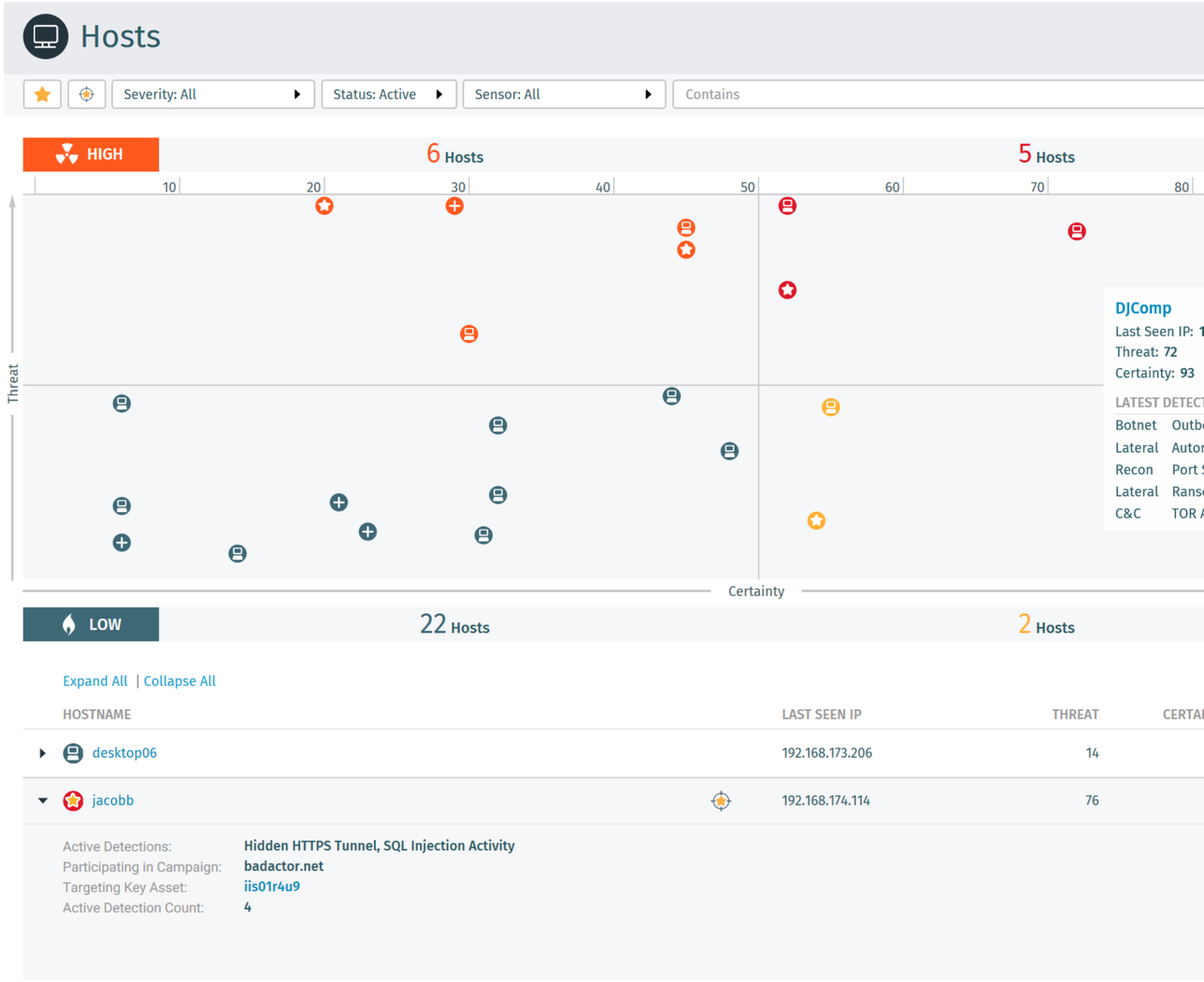
REDUCE THE SECURITY OPERATIONS WORKLOAD

- **Automatically** roll-up a chain of related events into a single incident as a starting point for deeper investigations or immediate action.
- **Enable** security operations teams to easily share consistent information on demand or on a set schedule.
- **Drive** dynamic response rules and automatically trigger responses from other security enforcement points.

“With Vectra, we cut threat investigation times from days to minutes.”

Daniel Basile
Executive Director Security operations center,
Texas A&M University System

VECTRA



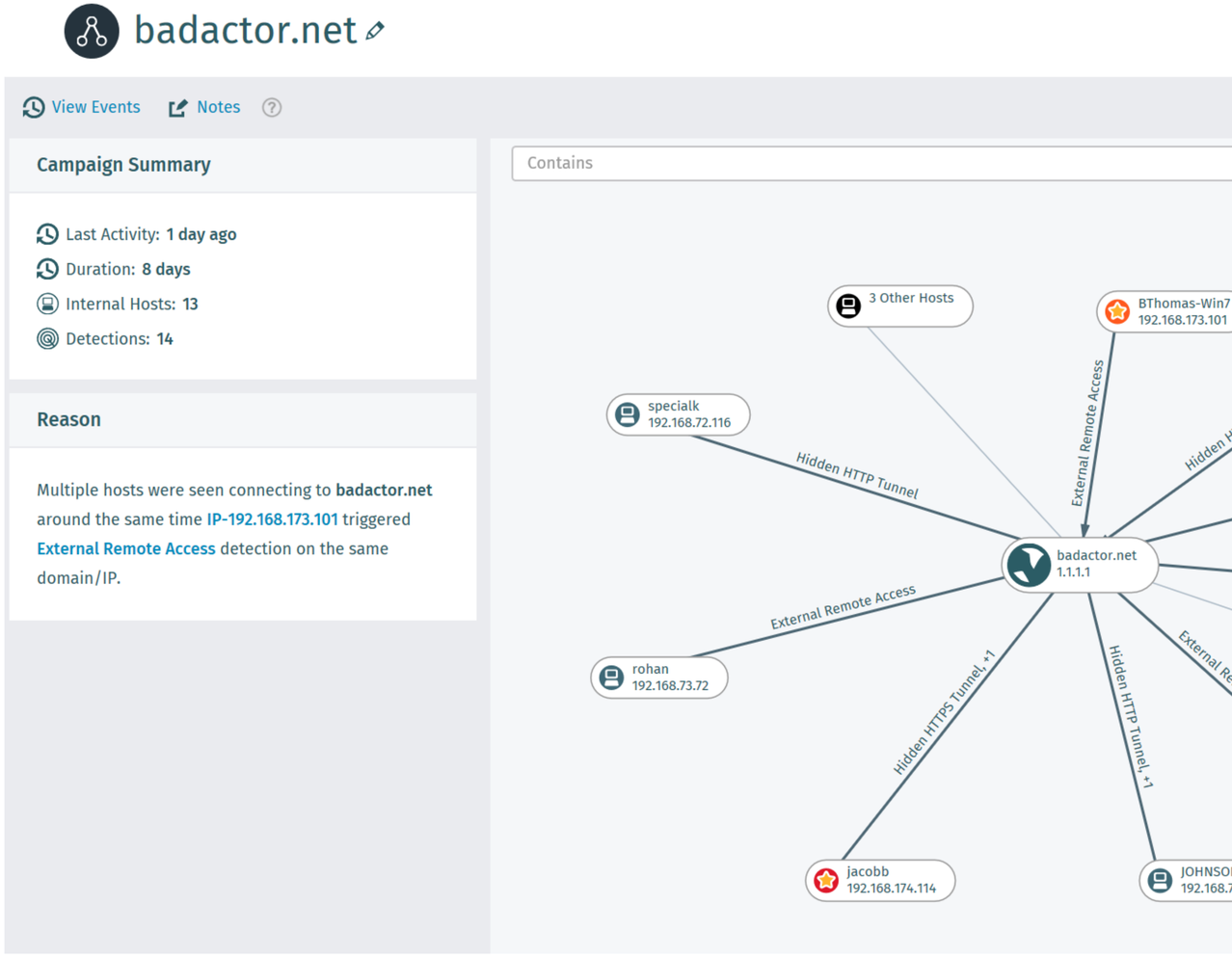
The Threat Certainty Index in Cognito Detect

PERFORM INTRUSION DETECTION

- **Detect** known and unknown attackers that evade existing security enforcement points.
- Enterprise-wide **visibility** into internal reconnaissance and lateral movement that typically spreads unchecked in a cyberattack.
- **Identify** devices or workloads at the center of an attack to stop in-progress threats and avert data loss.

> *"Vectra identifies threats that other 'industry-standard' tools miss."*

Rob Caputo
Principal CS Technology,
IT advisory firm



Synthesized view of an entire attack campaign in Cognito

VECTRA

HUNT FOR THREATS WITH COGNITO RECALL™

The most efficient way to hunt for threats.

- **AI-assisted** threat hunting.
- Conduct conclusive, in-depth threat **investigation**.
- Perform **retrospective** threat hunting.
- Enterprise-wide **visibility** into hidden threats.

“Cognito Recall is a dramatic leap forward in AI-assisted threat hunting and incident investigation.”

Mark Rodman
Head of Information Security Operations,
The Stars Group (PokerStars).

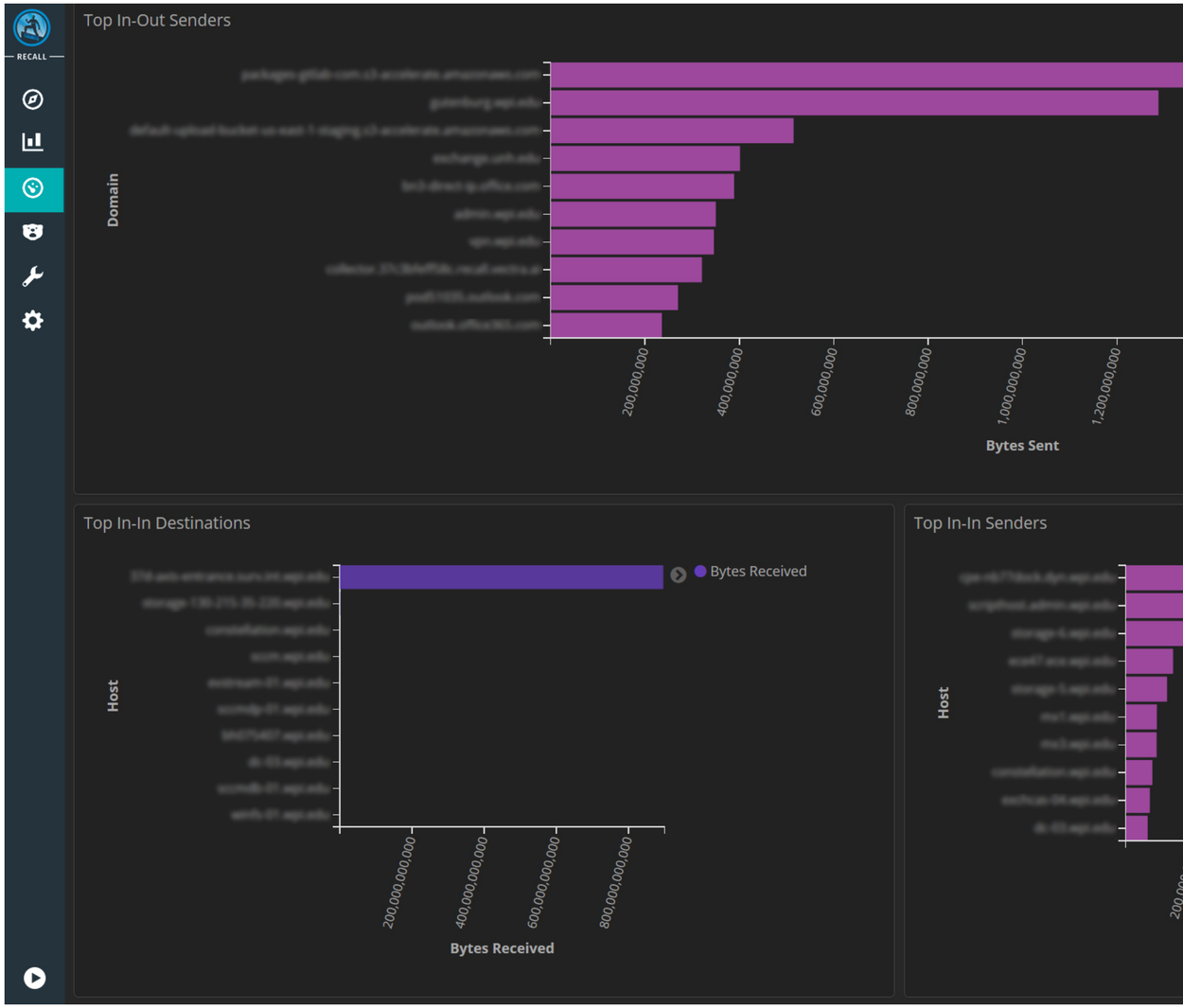
VECTRA

THREAT HUNTING: LOOKING FOR ACTIVE THREATS

- **Always-learning** behavioral models provide a logical starting point to perform AI-assisted threat hunting.
- **Use** threat-hunting techniques to investigate indicators of compromise and historic anomalies.
- **Leverage** a high-fidelity data source for threat hunting – enriched metadata – which requires far less storage space.

> *"Vectra makes threat hunting more efficient."*

Liam Fu
Head of Information Security,
Shop Direct



Track all outbound and inbound communication from host devices

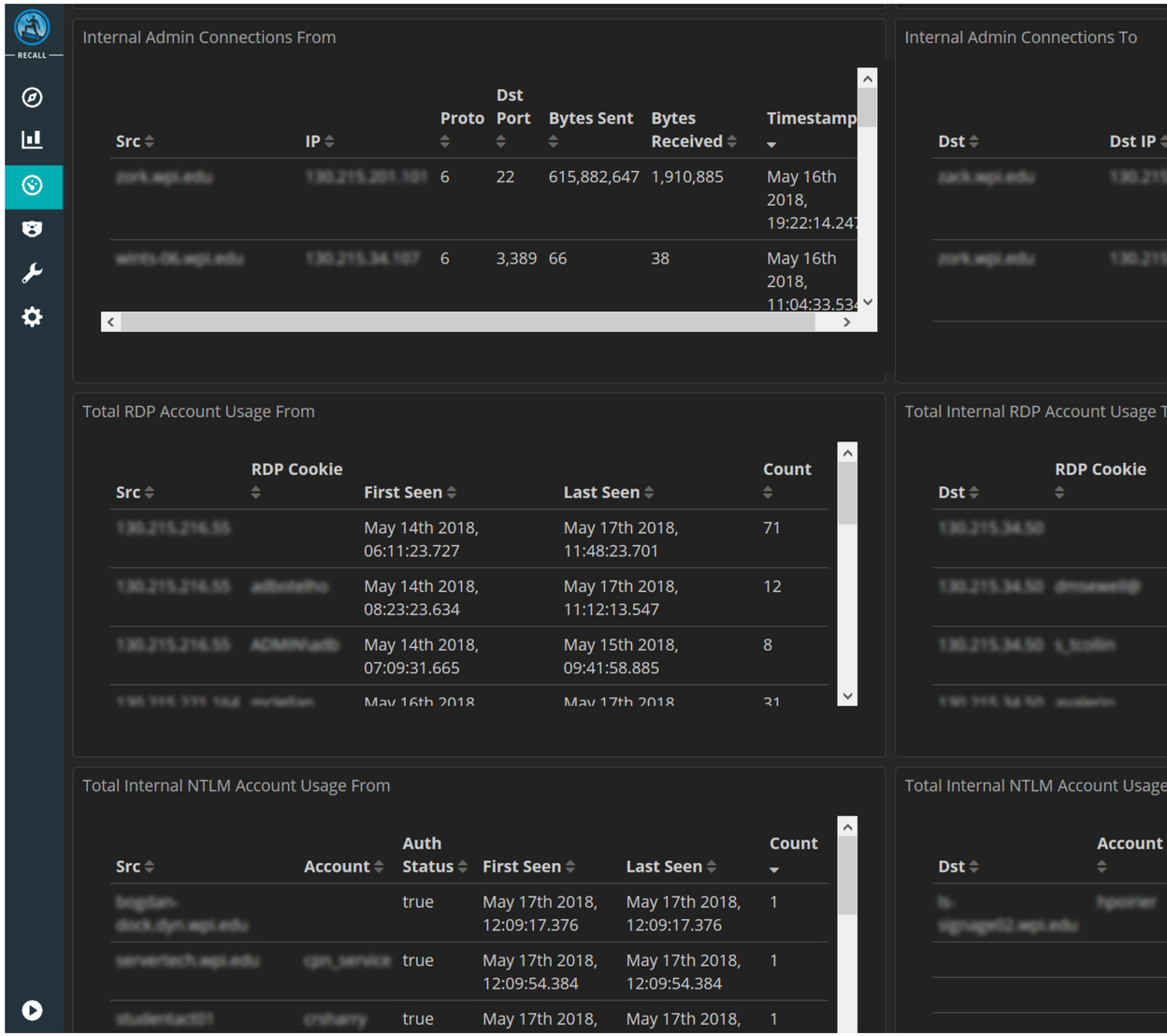
VECTRA

IN-DEPTH THREAT INVESTIGATION: FIND OUT WHAT HAPPENED

- **Discover** common threads between entities uncovered through automated threat detection.
- **Deep-dive** into incidents triggered by Cognito Detect and other security tools to gain context from threat activity.
- **Find** all devices accessed by compromised credentials and identify files involved in exfiltration.

“Vectra dramatically reduces the time we spend on threat investigations.”

Jojo Maalouf
IT Security Manager,
Hydro Ottawa



Details that enhance account-based investigations

VECTRA

RETROSPECTIVE THREAT HUNTING: REEVALUATE THE PAST

- **Metadata is stored** for a limitless period of time for search and analysis in future investigations.
- **Intelligently investigate** any device or workload activity over time, regardless of IP address changes.
- **All network metadata** is associated with devices, workloads and host names, not just IP addresses.
- **Deep protocol visibility**, not just connectivity, accelerates analysis and investigation.

“Vectra provides context to make fast, informed decisions.”

Dave Buffo
Senior Security Administrator,
Tri-State Generation and Transmission Association

Identify anomalous behaviors

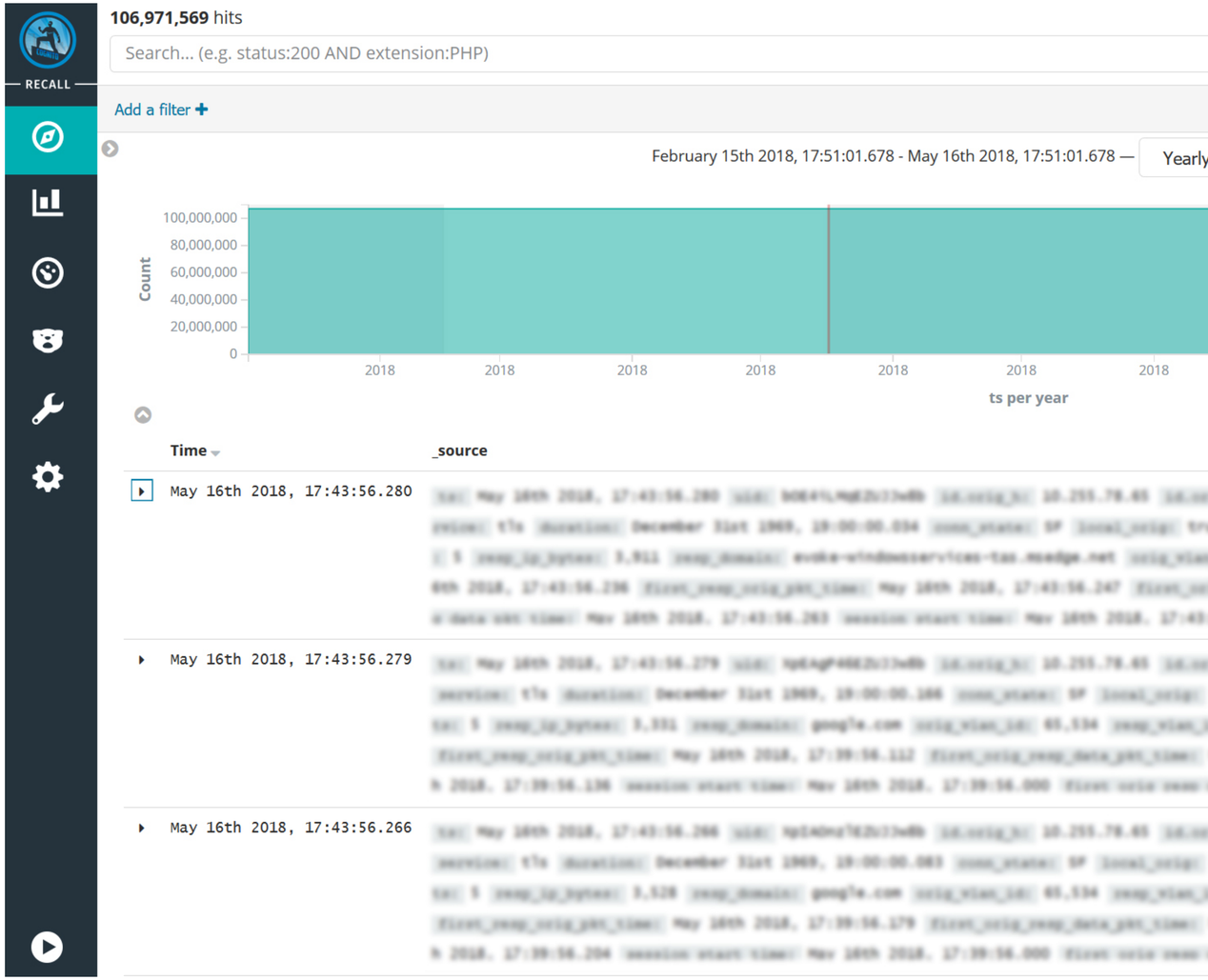
VECTRA

ENTERPRISE-WIDE VISIBILITY

- **Get conclusive**, actionable attack details and statistics about network activity and device behavior.
- **Collect and store** rich network metadata, relevant logs and cloud events for incident investigations.
- **High-fidelity visibility** into attacker behaviors in cloud and data center workloads and user and IoT devices.
- Cloud-powered **limitless scale** enables you to store and search rich metadata for as long as you need it.

“Vectra detects threats across the entire attack surface.”

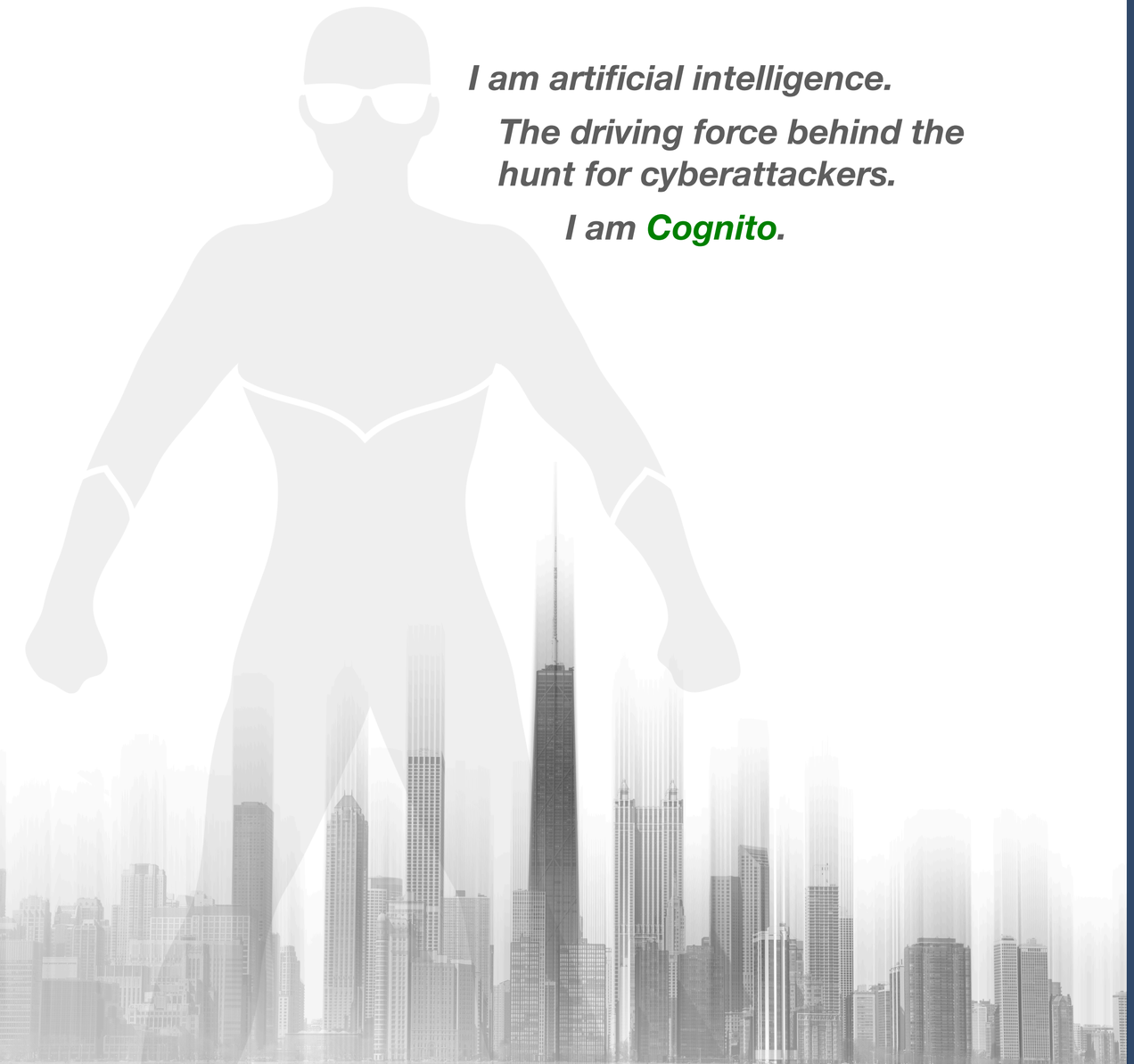
Enterprise Management Associates
A leading industry analysis and consulting firm



Full metadata search capabilities and limitless data storage

VECTRA

VECTRA®



I am artificial intelligence.

The driving force behind the hunt for cyberattackers.

*I am **Cognito**.*

COGNITO

IS THE ULTIMATE AI-POWERED CYBERATTACK-DETECTION AND THREAT-HUNTING PLATFORM

The Cognito platform from Vectra uses AI to detect attackers in real time and enrich threat investigations with a conclusive chain of forensic evidence.

Download our white paper to learn how to augment security operations centers with artificial intelligence.

GET THE WHITE PAPER