VECTRA®
Security that thinks®

Applying AI to automate threat detection and empower threat hunting

WOUTER SPIERENBURG
SR SALES ENGINEER

You + AI =
Security that thinks®

VECTRA®

“We’re the world leader in applying AI to detect and hunt for cyberattackers”

What is AI?

I propose to consider the question, 'Can machines think?

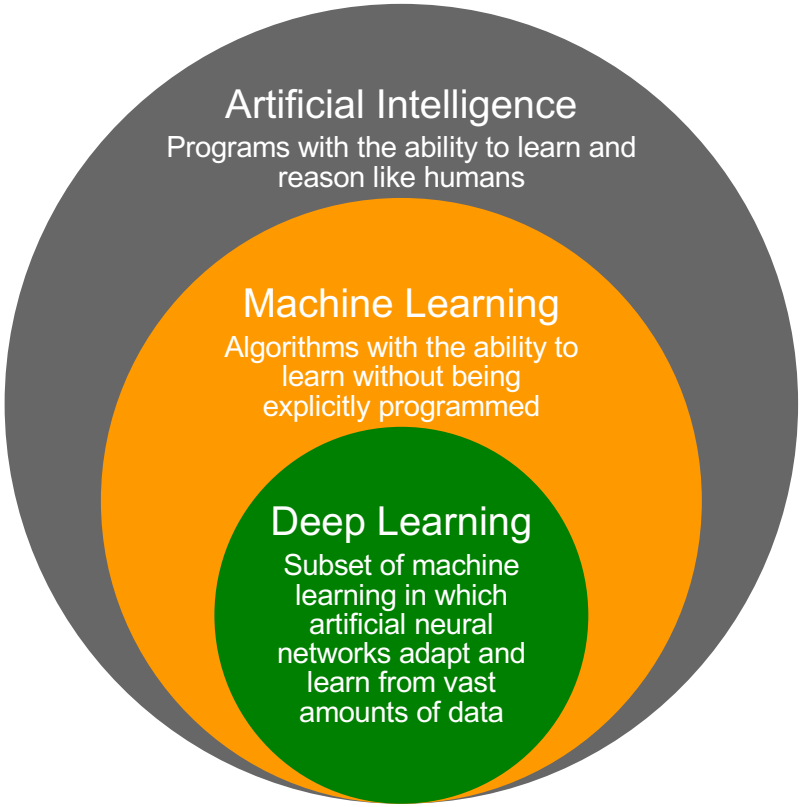
The Turing test….

“if a computer could fool people into thinking that they were interacting with another person, rather than a machine, then it could be classified as possessing artificial intelligence”

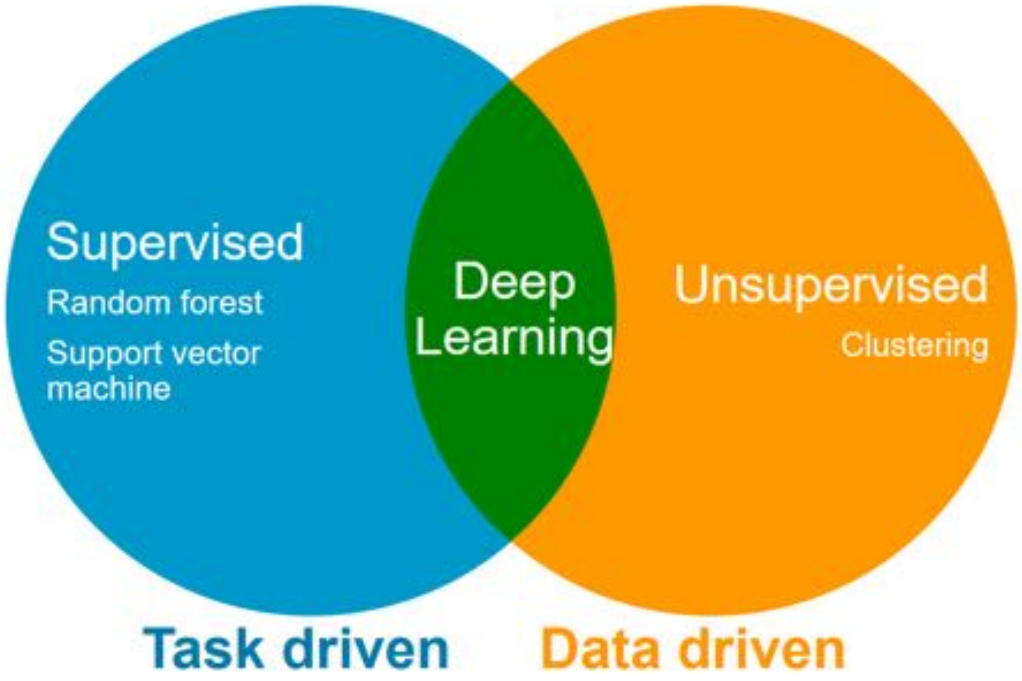
Essentially can a machine do in part the function of a role occupied by a human?

Alan Mathison Turing OBE FRS

What makes a machine intelligent?

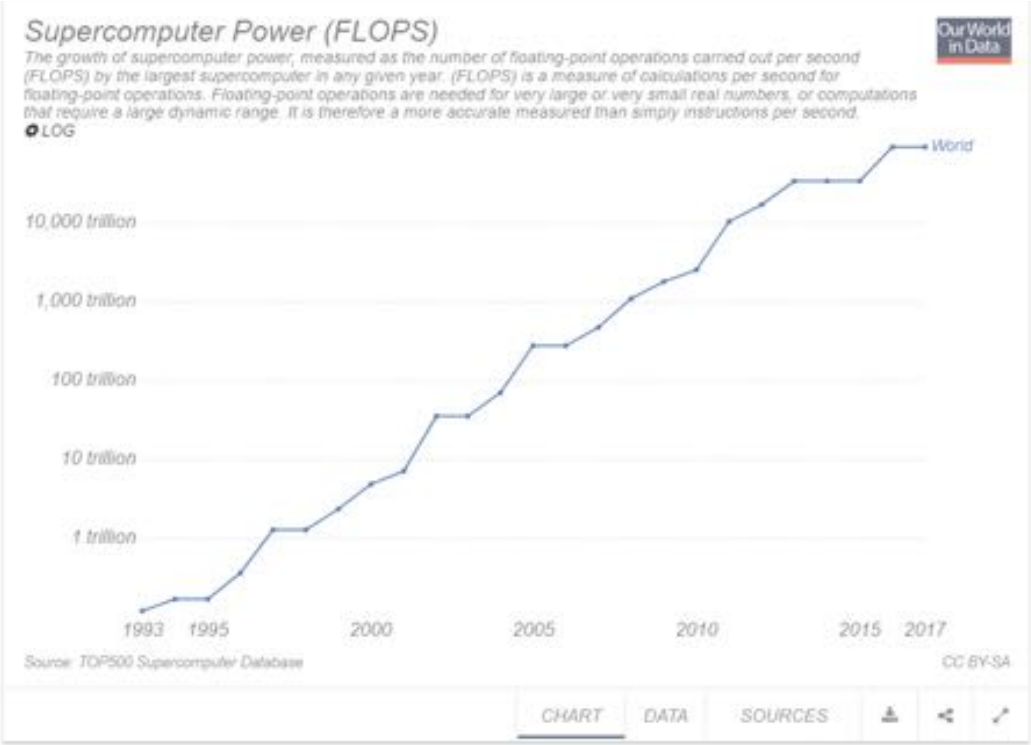


Types of Machine learning



AI/ML and Data Science has been here for a while so why now for Information Security?

Exponentially increasing computational capacity over time (computations per second) – Koomey, Berard, Sanchez, and Wong (2011)[4]



Industries that underwent radical transformation..

1930s — 1950s

Telephone central office

Automotive manufacturing

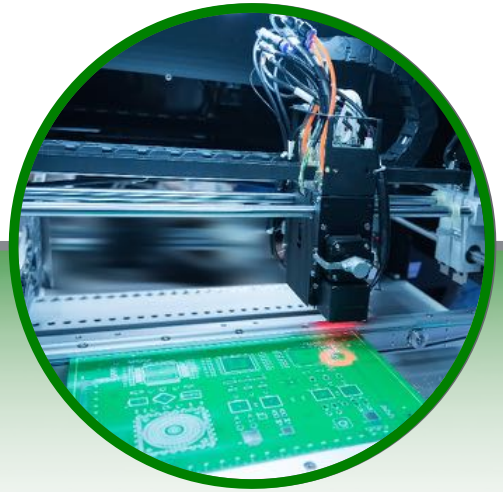
Electronics manufacturing

From one perspective this would have felt like AI but was in reality electrical automation

Today

Telephone central office

Automotive manufacturing

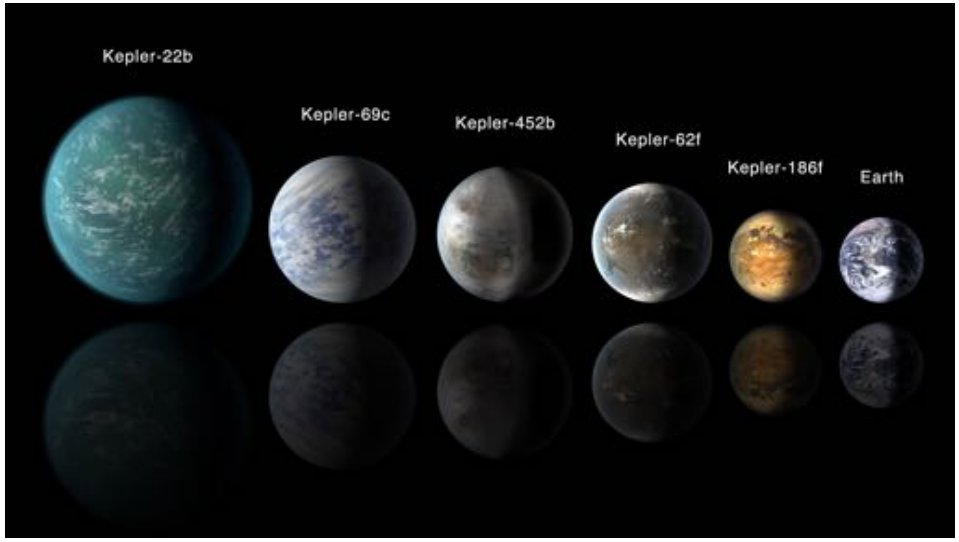


Electronics manufacturing

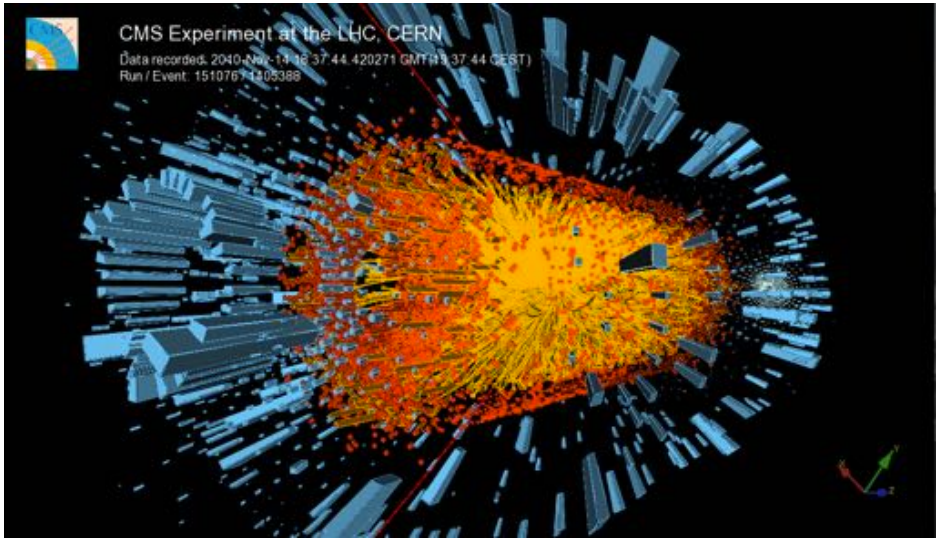
Good use cases for AI

- Big data set and looking for a needle in a haystack…..

Exoplanets



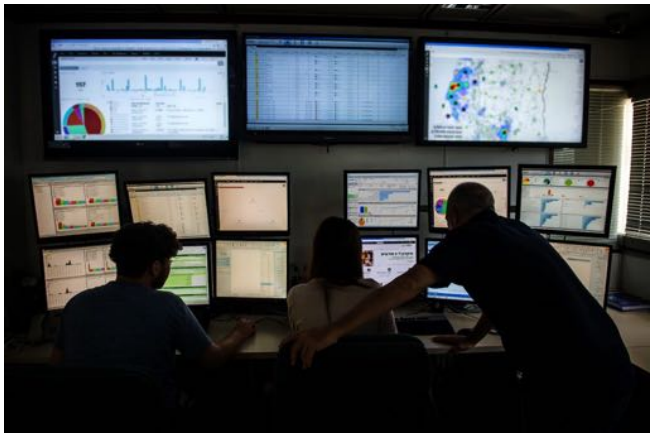
Sub atomic particles



……what about Cyber?

Where can you apply AI in the context of Cyber Security?

Endpoint



SIEM

Network

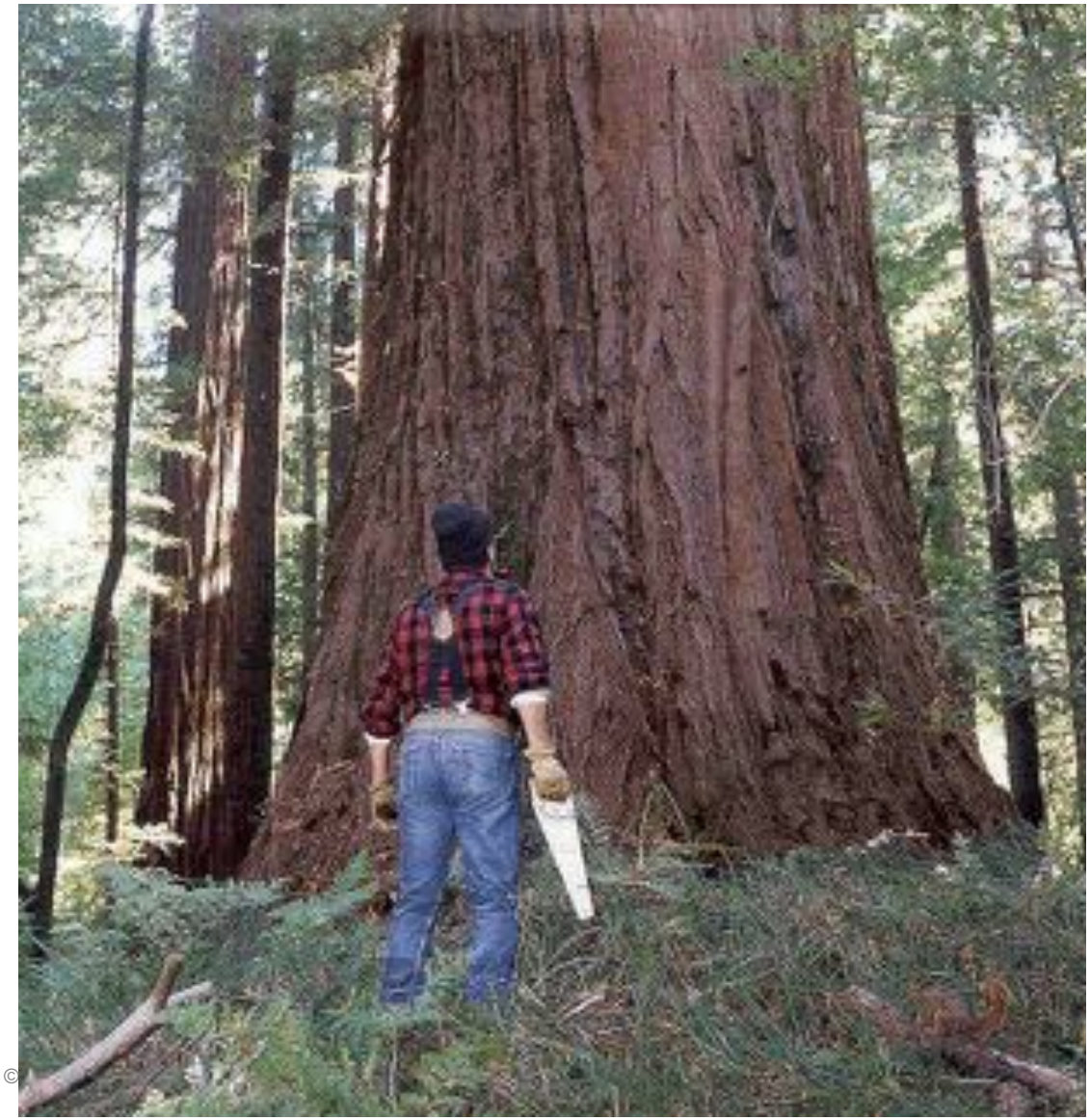
The right tool for the job

Machine learning is about making decisions based on the amount and type of information you have.

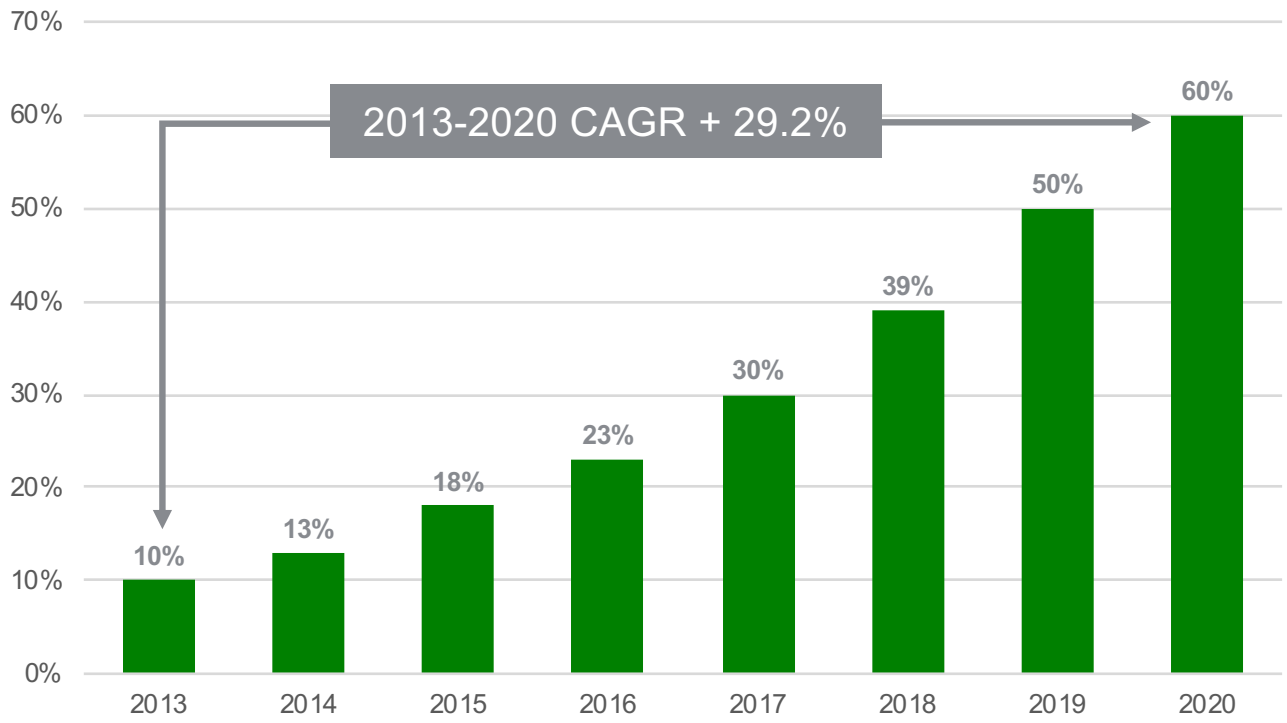
Each algorithm solves a different problem.

The network presents a wonderful opportunity as a primary data source

Very hard for the threat actor to hide in the network



Enterprise security budget shifting to detection and response



% of IT security budget dedicated to detection and response

VECTRA

Source: Gartner, CS Communications Infrastructure Team, Credit Suisse Research

Two detection and response challenges – time and talent

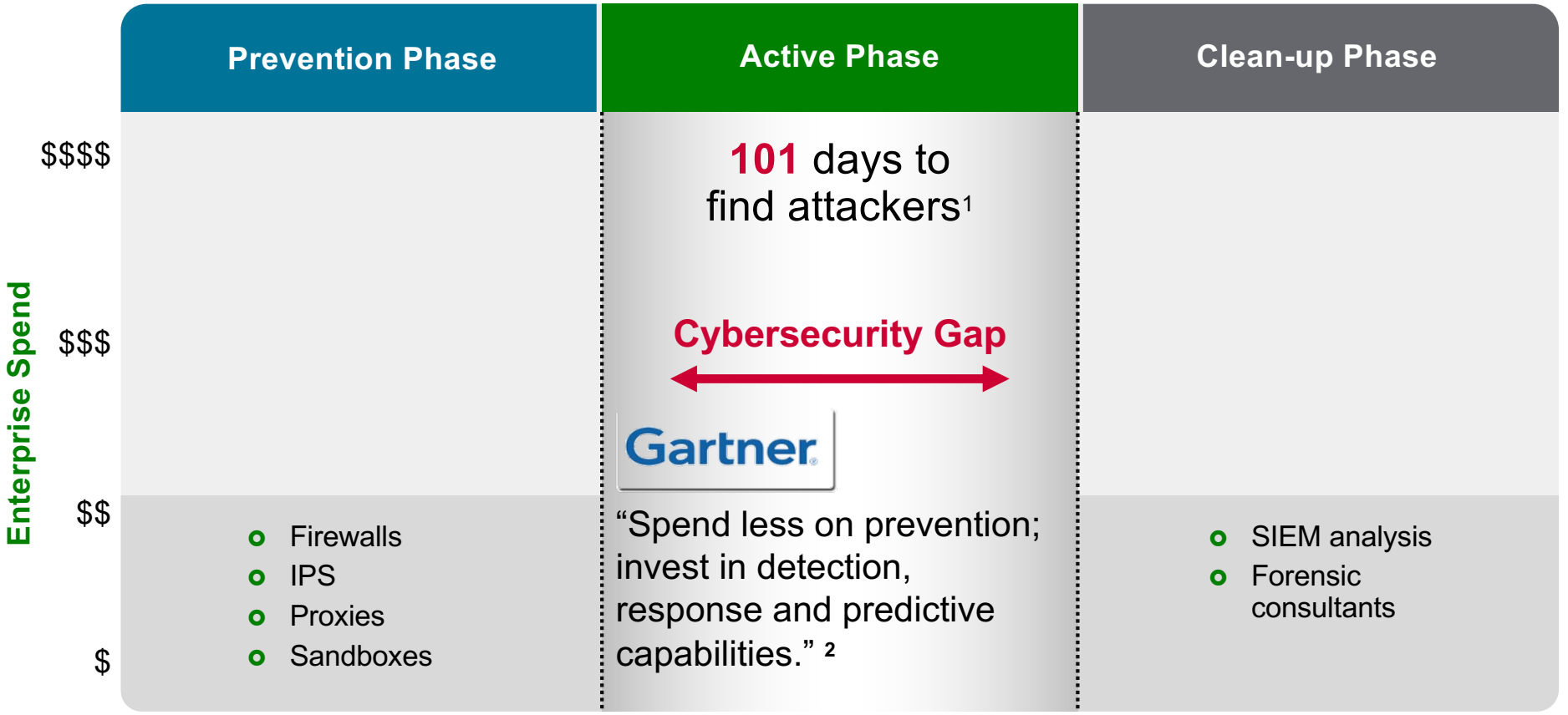
“What we need is speed, speed, speed.”

– Admiral Mike Rodgers

“Unfilled Cybersecurity jobs to hit 3.5 million by 2021”

– CSO Online

Enterprises are blind to attacks despite massive investment



[1] Source: M-Trends 2018

[2] Designing an Adaptive Security Architecture for Protection from Advanced Attacks, 12 February 2014, ID G00259490

Cognito Detect – It's all about detecting attacker behaviors

Security Research
Characterize fundamental attacker behaviors

Data Science
ML models to accurately detect behaviors

10 Patents Awarded
20+ Patents Pending

Attacker Behavior models
High-fidelity, signatureless detection

Command and Control	Reconnaissance	Lateral Movement	Exfiltration
Advanced C2: human control	Network sweeps and scans	Stolen accounts	Data movement
Botnet C2	Advanced: AD, RPC, shares	Exploits	Methods, e.g. tunnels
		Backdoors	

Detects attacker behaviors across the kill chain

Command and Control
External Remote Access
Hidden DNS Tunnel
Hidden HTTP/S Tunnel
Suspicious Relay
Suspect Domain Activity
Malware Update
Peer-to-Peer
Pulling Instructions
Suspicious HTTP
Stealth HTTP Post
TOR Activity
Threat Intel Match

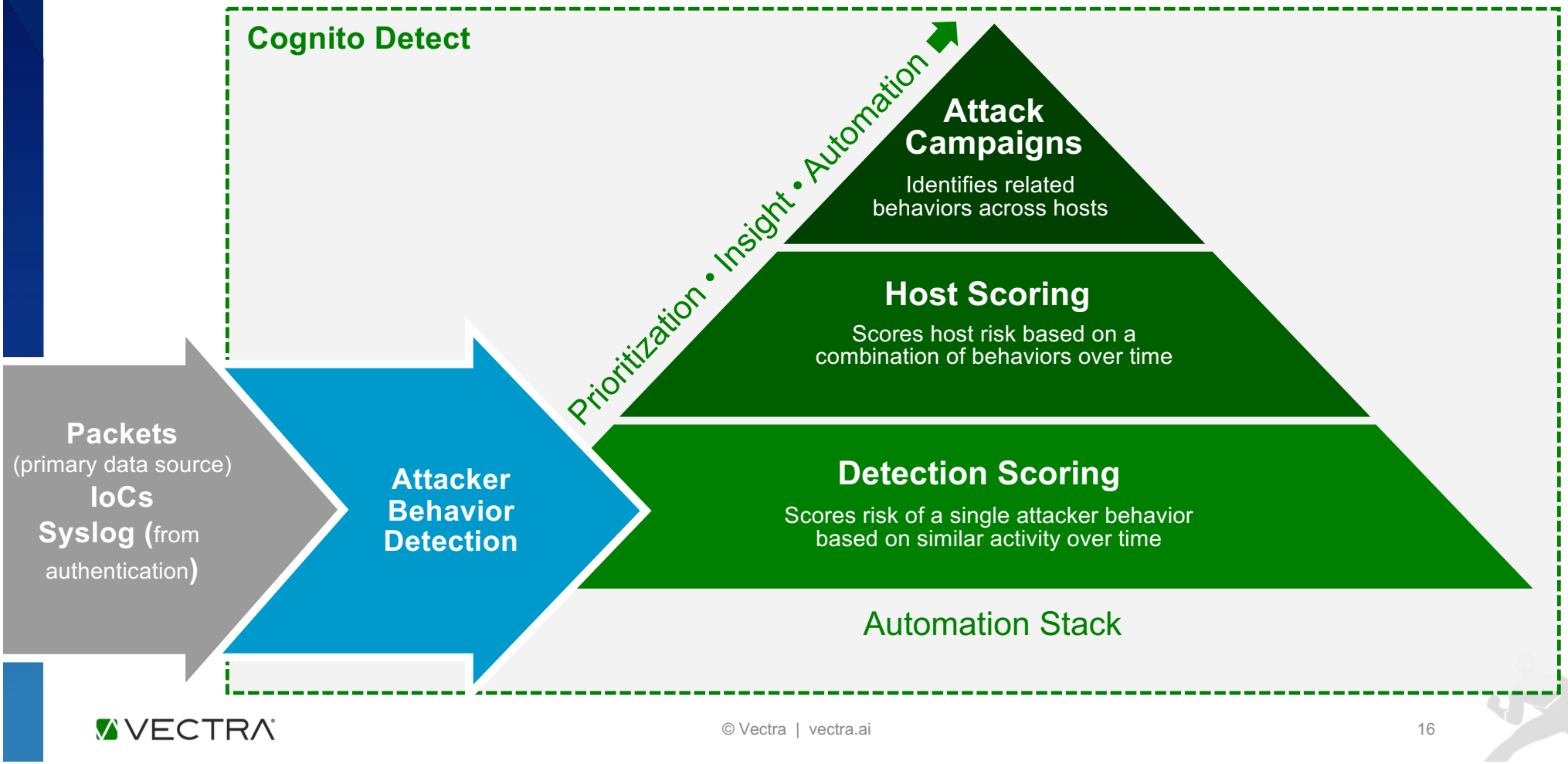
Reconnaissance
Internal Darknet Scan
Port Scan
Port Sweep
SMB Account Scan
Kerberos Account Scan
File Share Enum
Suspicious LDAP Query
RDP Recon
RPC Recon

Lateral Movement
Suspicious Remote Exec
Suspicious Remote Desktop
Suspicious Admin
Shell Knocker
Automated Replication
Brute-Force Attack
SMB Brute-Force
Kerberos Brute Force
Suspicious Kerberos Client
Suspicious Kerberos Account
Kerberos Server Activity
Ransomware File Activity
SQL Injection Activity

Exfiltration
Data Smuggler
Smash and Grab
Hidden DNS Tunnel
Hidden HTTP/S Tunnel

Botnet Monetization
Abnormal Web or Ad Activity
Cryptocurrency Mining
Brute-Force Attack
Outbound DoS
Outbound Port Sweep
Outbound Spam

Automated hunting for attacker behaviors



Vectra is the only visionary

in the Gartner 2018 Magic Quadrant for Intrusion Detection and Prevention Systems

All statements in this report attributable to Gartner represent Vectra's interpretation of data, research opinion or viewpoints published as part of a syndicated subscription service by Gartner, Inc., and have not been reviewed by Gartner. Each Gartner publication speaks as of its original publication date (and not as of the date of this presentation. The opinions expressed in Gartner publications are not representations of fact, and are subject to change without notice.

Gartner

Figure 1. Magic Quadrant for Intrusion Detection and Prevention Systems

Source: Gartner (January 2018)

Source: Gartner Magic Quadrant for Intrusion Detection and Prevention Systems January, 2018. ID Number: G00324914

InformationWeek DARKReading

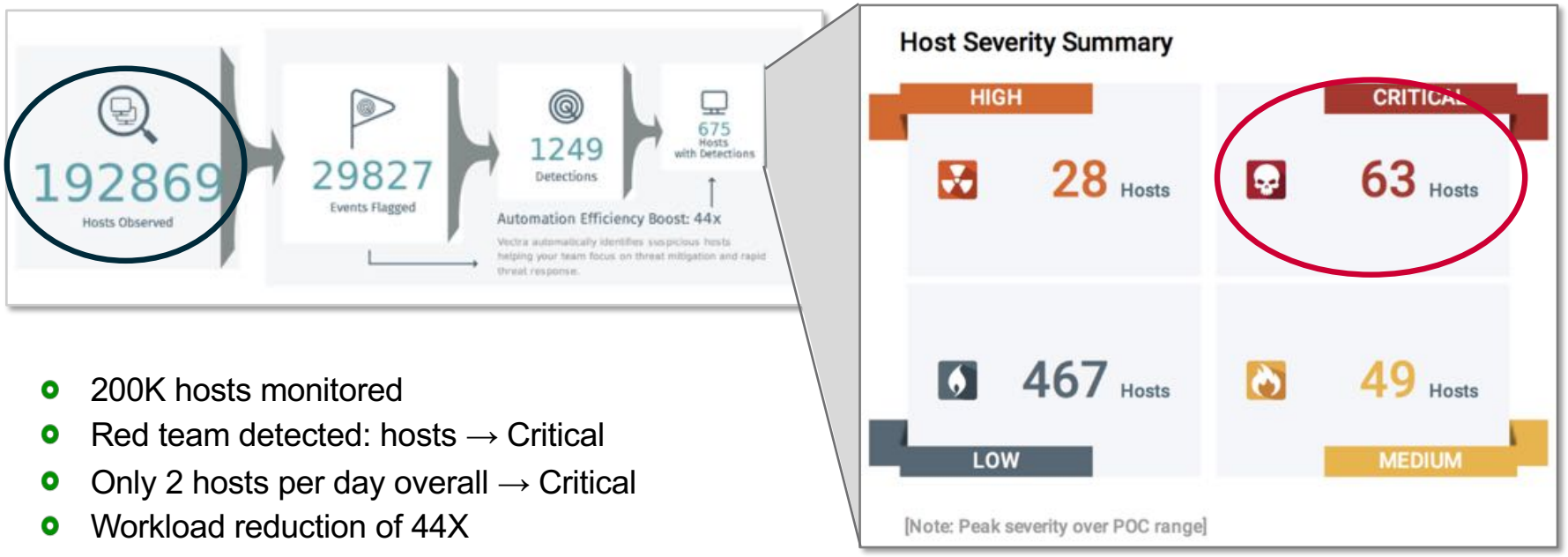
Best of black hat Awards

VECTRA
Security that thinks®

"We chose Vectra as the winner because it prioritizes threats and reduces attacker dwell time with a lightweight solution."

– Tim Wilson
Editor in Chief, Dark Reading, 2016

Cognito Detect reduced workload by 44X in 30-day eval



- 200K hosts monitored
- Red team detected: hosts → Critical
- Only 2 hosts per day overall → Critical
- Workload reduction of 44X

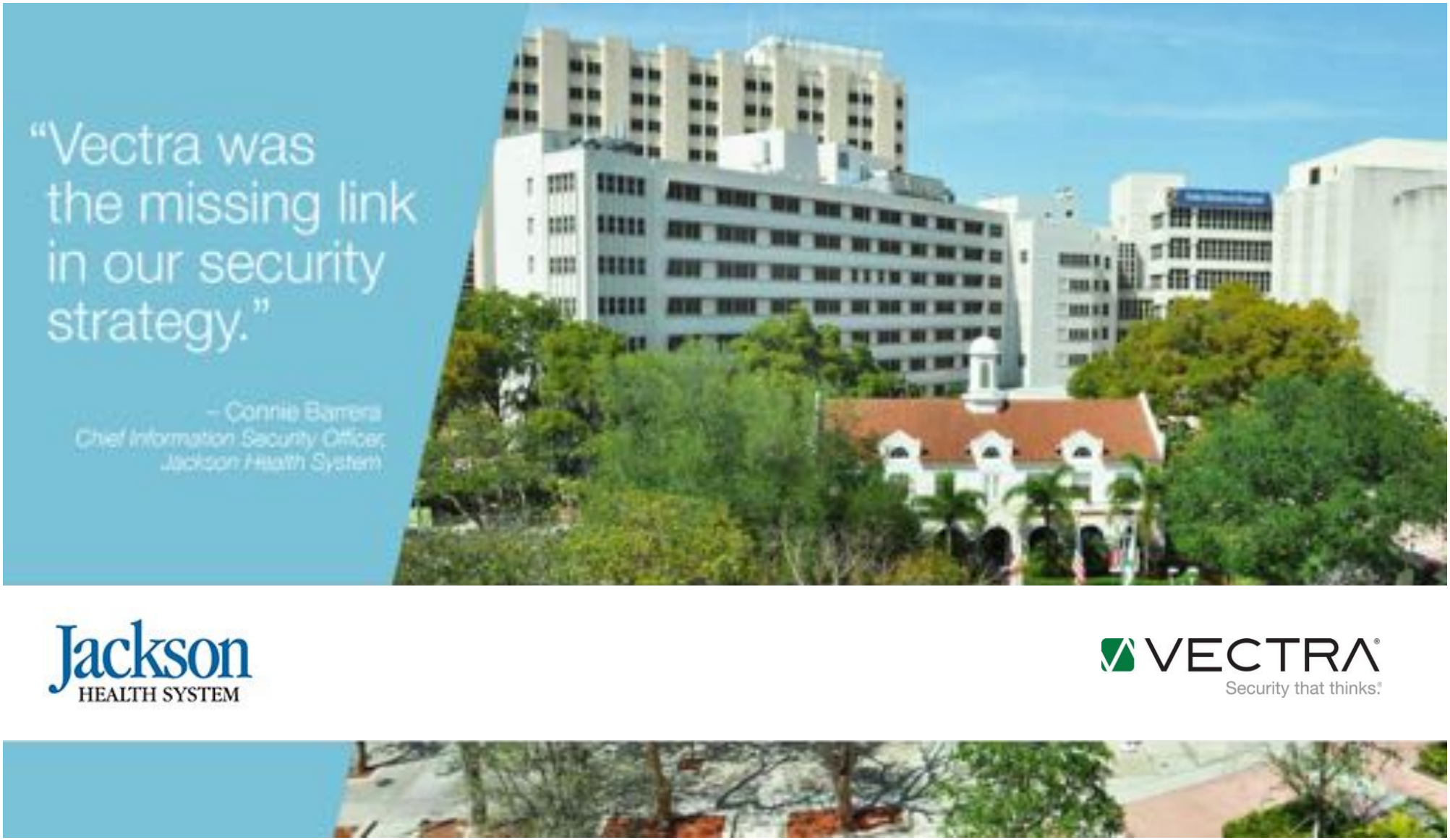
Cognito separates high-fidelity signal from the daily noise

"Vectra provides automated detections with context so security analysts have information to make fast, informed decisions."

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

TRI-STATE
Generation and Transmission Association, Inc.

VECTRA
Security that thinks®



Jackson HEALTH SYSTEM

VECTRA
Security that thinks®

"Vectra is threat detection on steroids."

– Duane Smith
Chief Information Security Officer
Tribune Media Group

Tribune Media

VECTRA
Security that thinks®

“Our security team always knows what is going, where an attack is happening, and the necessary steps to remediate the threat.”

– Markus Müller-Fehrenbach
Head of IT infrastructure and operations,
Vetropak holdings

vetropack

VECTRA
Security that thinks®

“Vectra is helping us reduce business risk.”

– Liam Fu
Head of Information Security, Shop Direct

SHOP DIRECT

VECTRA
Security that thinks®

Coop selected the Cognito AI platform from Vectra as an innovative approach to increasing cybersecurity operational efficiency and efficacy.

coop

VECTRA
Security that thinks®

"Cognito Recall represents a dramatic leap forward in AI-assisted threat hunting and incident investigation."

– Mark Rodman
Head of Information Security Operations, Stars Group

THE STARS GROUP

VECTRA
Security that thinks®

"Deploying Vectra Cognito has significantly improved our visibility of advanced threat scenarios without having to commit high level of resources."

– Nuno Andrade
CISO,
RSA Group

RSA

VECTRA
Security that thinks®


VECTRA®
Security that thinks®