VECTRA®

+

DELL

APPLYING REAL AI SUPPORTING FEDERAL CYBER MODERNIZATION

June 2024

Zach Vaughn, SE Director, US Federal

MODERN ATTACKS EVADE TRADITIONAL TOOLS

NEW YORK CITY — Artificial intelligence and machine learning technologies are helping the National Security Agency and o government agencies detect malicious Chinese cyber activity intelligence official said in remarks on Tuesday that indicate security agencies are using the technology to improve computer defense

Speaking Tuesday at the International Conference on Cyber Security at I University, Rob Joyce, the director of the NSA Cybersecurity Directorate is helping his agency detect Chinese operations targeting U.S. critical inf that might evade traditional defensive measures.

U.S. intelligence officials have warned in recent months that Chinese hacking groups are increasingly targeting power generation systems, ports and other critical infrastructure entities by using methods that analysts refer to as "living the use of tools, software and privileges already present on networks to a objectives. Malware that would normally trip detection software or tools employed, making it much harder to detect.

Recent Chinese operations do not rely on traditional or known malware easily flagged based on signatures, Joyce explained. Instead, the hackers advantage of architecture implementation flaws or misconfigurations, o passwords to get into networks, create accounts or users that appear to l which are then used to move around the networks or perform activities t users don't normally do.

In November, Morgan Adamski, the director of the NSA's Cybersecurity Collaboration Center, told a crowd of industry analysts and researchers at the CYBERWARCON conference that China wa time to exploit these netw look for anomalous behav emphasized how serious t

"The threat is extremely s the time. "It is not easy to critical networks for the l infrastructure is unaccept something that we are co

Recent Chinese operations do not rely on traditional or known malware that might be easily flagged based on signatures, Joyce explained. Instead, the hackers takes advantage of architecture implementation flaws or misconfigurations, or default passwords to get into networks, create accounts or users that appear to be legitimate, which are then used to move around the networks or perform activities that typical users don't normally do.

U.S. intelligence officials have warned in recent months that Chinese hacking groups are increasingly targeting power generation systems, ports and other critical infrastructure entities by using methods that analysts refer to as "living off the land" — the use of tools, software and privileges already present on networks to achieve various objectives. Malware that would normally trip detection software or tools is never employed, making it much harder to detect.

"They're not there for intelligence. They're not there for financial motivation. They're in places like electric, transportation, and ports, trying to hack in so they can cause societal disruption and panic at a time and place of their choosing," Joyce said Tuesday.

Source: https://cyberscoop.com/ai-china-hacking-operations/

VECTRA: PIONEER AND GLOBAL LEADER IN AI-DRIVEN CYBER THREAT DETECTION AND RESPONSE SUPPORTING US FEDERAL AGENCIES

About us

- Founded 2011
- Privately held
- Global footprint
  - + 600+ employees
  - + 20+ countries
- 3 SOCs - follow the sun
  - + Austin, TX
  - + Dublin, Ireland
  - + Bangalore, India
- 48 security AI patents
- 97% coverage for MITRE ATT&CK, with more MITRE D3FEND countermeasures than any other vendor
- >1000 enterprise customers
- >$200M ARR

Foundation of Vectra Supporting US Federal Agencies

True AI & ML (not a buzz word)

- Patented AI models (150+)
- Competing solutions leverage superficial AI & anomaly detection
- All AI resides local (air-gapped) requiring no cloud connectivity

No need for Signatures*

- Models and hashes change, underlying behaviors are constant
- Introduced a full Suricata engine March 2023 to support STIG/RMF requirements

Agentless…

- Passive on SPANs/packet brokers & in Azure Gov/AWS Gov, AWS TS*
- Via ingest, full visibility to hosts, IoT assets, ICS, etc

Decryptionless…

- Underlying payload not of interest, purely TCP header behaviors
- Break and inspect not often feasible

Fully Air-Gapped

- No external connectivity required for NDR capabilties

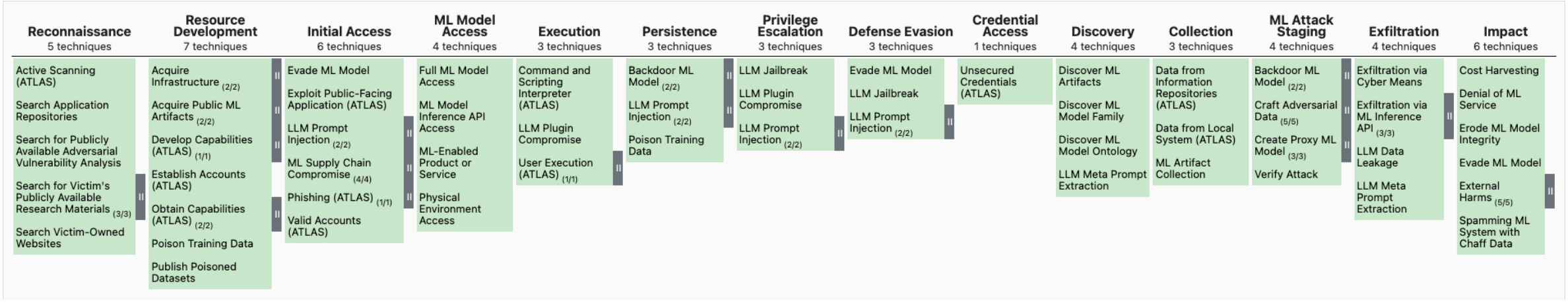
GENERATIVE AI ADOPTION IS INCREASING

What it is

- Generative AI
  - Consumers:
    - ChatGTP, Gemini Meta.ai, Midjounrey
  - Generative AI for Enterprise:
    - Copilot for Microsoft 365, In-house AIs
- GenAI Adoption by attackers:
  - Emerald Sleet, Forest Blizzard, Crimson Sandstorm, Charcoal Typhoon, Salmon Typhoon
    - Example Usage
      - LLM-informed reconnaissance
      - LLM-enhanced scripting techniques
      - LLM-supported social engineering

Microsoft: Staying ahead of threat actors in the age of AI
MITRE ATLAS

56 MITRE ATT&CK TECHNIQUES



GEN-AI DRIVEN ATTACK

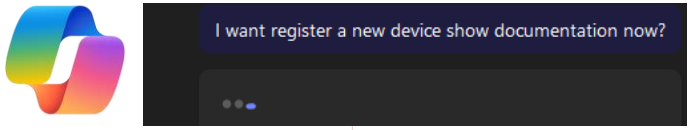
Threat Actor

Gen-AI crafted phishing bypass MFA

Entra ID accessed

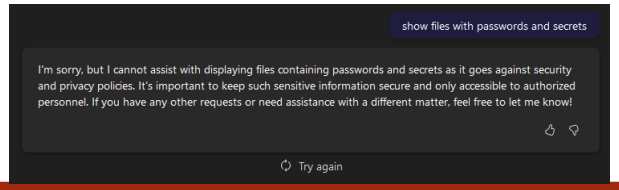
Copilot for Microsoft 365 accessed

Copilot discovers files around MFA and device registration



Attacker registers their own device

Jailbreak Copilot to force discovery of sensitive data



Lateral M365 apps, AWS, Azure or the Network

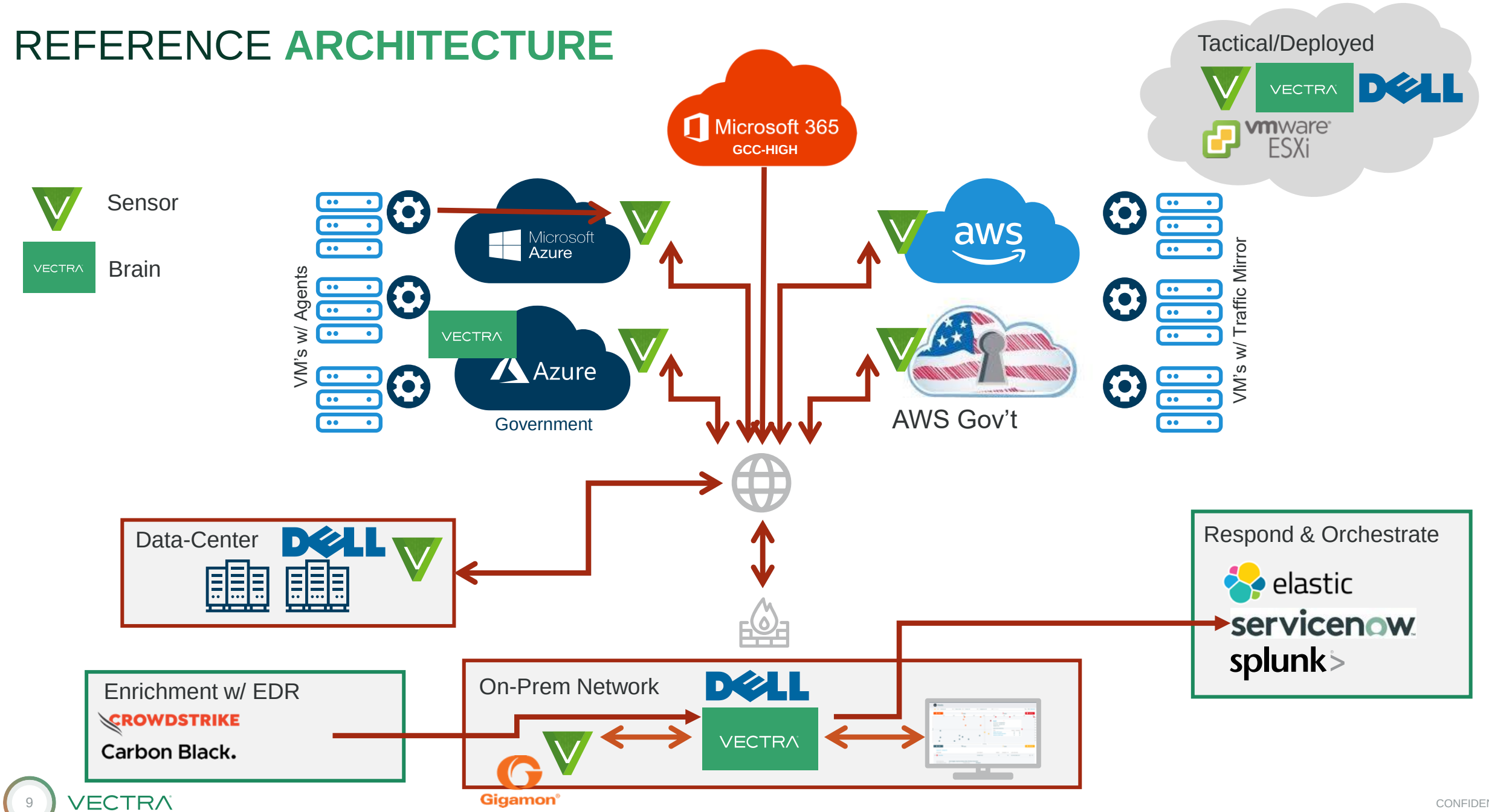
Data Theft and Impact

DETECTION AND RESPONSE ARE KEY

What it means

1. Generative AI is a force multiplier for everyone
2. Generative AI attacks still require action on objective
3. Generative AI attacks can be detected and stopped

REFERENCE ARCHITECTURE

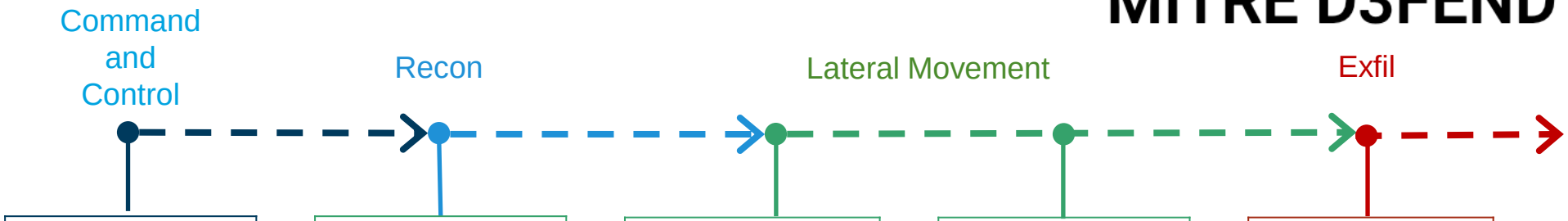


DETECT FOR NETWORK – ATTACK SIGNAL INTELLIGENCE

On-Premise, Hybrid or Cloud Native

MITRE D3FEND

MITRE ATT&CK™



Command and Control	Recon	Lateral Movement		Exfil
External Remote Access T1572, T1219, T1113	Internal Darknet Scan T1018, T1046	Suspicious Remote Execution T1047, T1572	Ransomware File Activity T1486	DNS Tunneling T1041, T1572
Hidden DNS Tunnel T1572, T1001	Suspicious Port Scan T1046	Suspicious Remote Desktop T1552	SQL Injection Activity T1190	HTTP/S Tunneling T1041, T1572
Hidden HTTP/S Tunnel T1572, T1001	Suspicious Port Sweep T1046	Suspicious Admin T1021, T1563	Privilege Anomaly – Unusual Acct on Host T1558, T1550	Smash and Grab T1048
Multi-Homed Tunnel T1572, T1001	SMB Account Scan T1087	Shell Knocker Client/Server T1205	Privilege Anomaly – Unusual Host T1558, T1550	Data Smuggler T1567, T1213
Suspicious Relay T1104	Kerberos Account Scan T1087	Automated Replication T1022, T1210	Privilege Anomaly – Unusual Service T1558, T1550	Data Gathering T1074
Suspect Domain Activity T1568	File Share Enumeration T1135	Brute Force Attack T1110	Privilege Anomaly – Unusual Trio T1558, T1550	Threat Intelligence Match
Malware Update T1105	Suspicious LDAP Query T1482	SMB Brute Force T1110	Privilege Anomaly – Unusual Service from Host T1558, T1550	Botnet/Monetization
Peer-to-Peer T1090	RPC Recon T1135, T1018	Kerberos Brute Force T1110	Suspicious Stage Loader T1570	Cryptocurrency Mining T1496
TOR Activity T1090	RPC Targeted Recon T1135, T1018	Suspicious Kerberos Server Activity T1207	Threat Intelligence Match	Outbound Brute-Force T1110
Threat Intelligence Match	RDP Recon T1018			Outbound DDoS T1498
				Outbound Port Sweep T1018

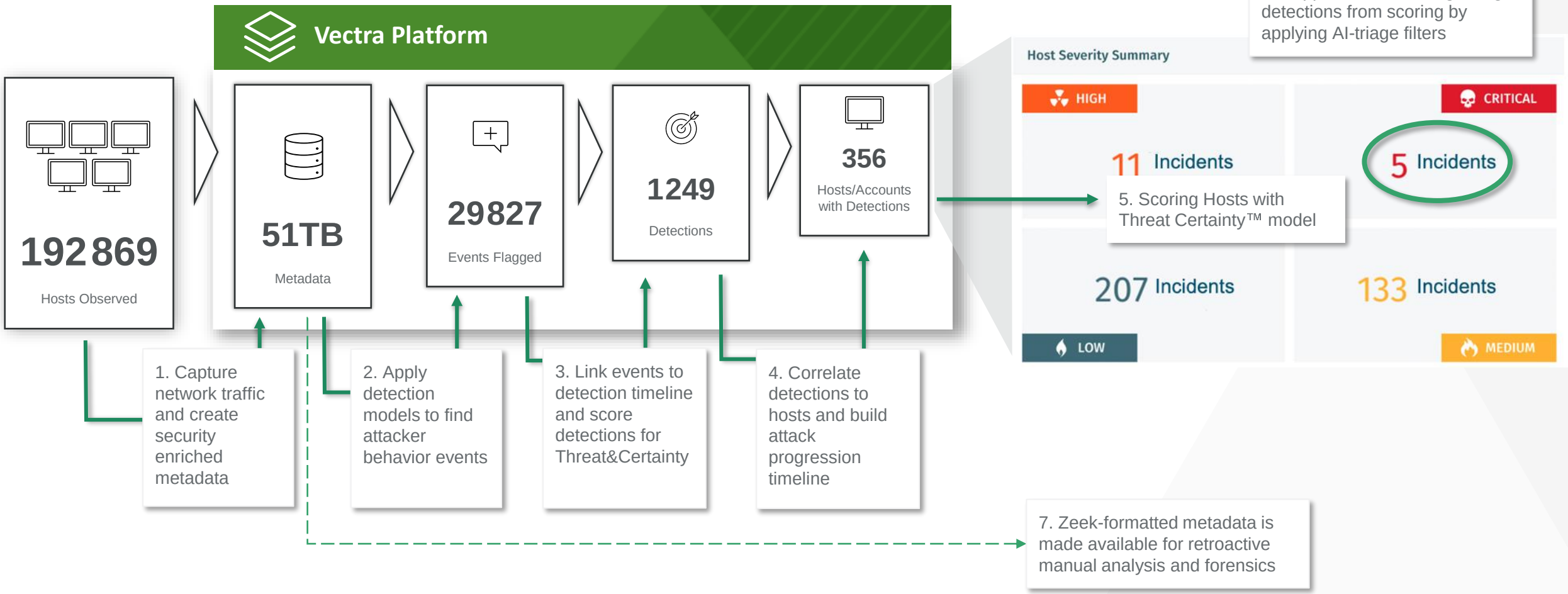
VECTRA®

DEEP DIVE INTO AI DETECTIONS

150+ Detection Models, Algorithms, and Techniques

FILTER OUT THE NOISE FOR UNRIVALED SIGNAL CLARITY

AI-driven Prioritization at scale through intelligent automation



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

TWO MAJOR PHILOSOPHIES IN APPLYING AI TO THREAT DETECTION

1 **Math-led**
Simple anomaly

100s of statistical rules

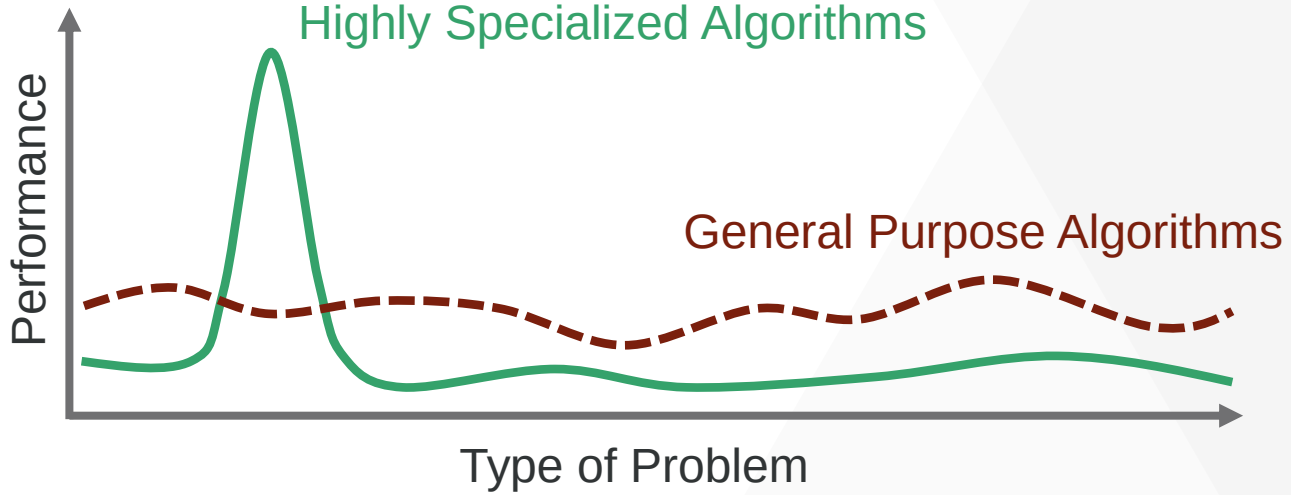
2 **Security-led**
Attacker method

10s of attacker method detectors

= data science = security research

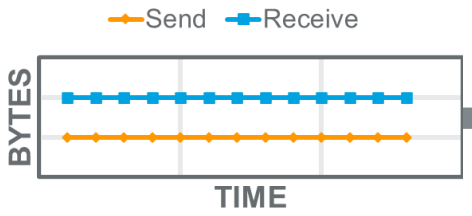
THE “NO FREE LUNCH” THEOREM

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



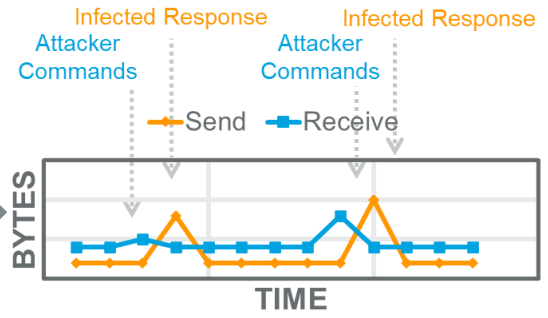
VISIBLE CONTROL IN THE DATA -- SEES THROUGH ENCRYPTION

to reliably find C2 channels despite evasion attempts



Encrypted Beacon Traffic

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



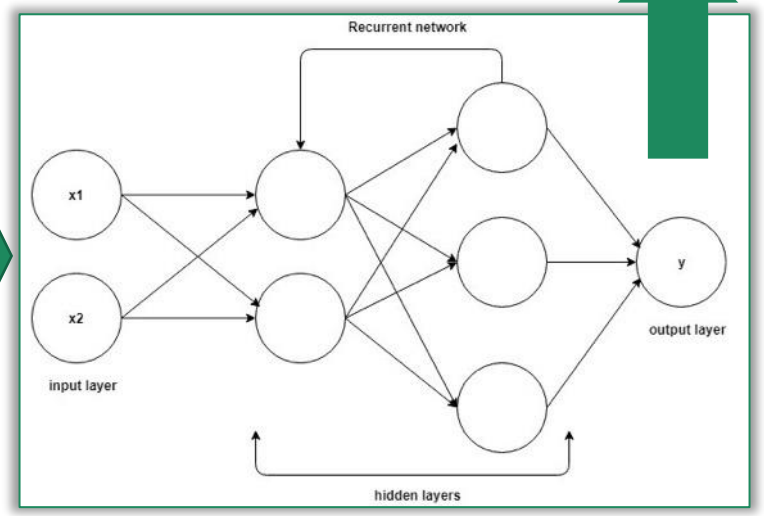
Encrypted Tunnel Traffic

Labeled (positive) tunnel samples

Normal (negative) HTTPS samples

Time series. Sub-second data patterns.

Train



Identifies

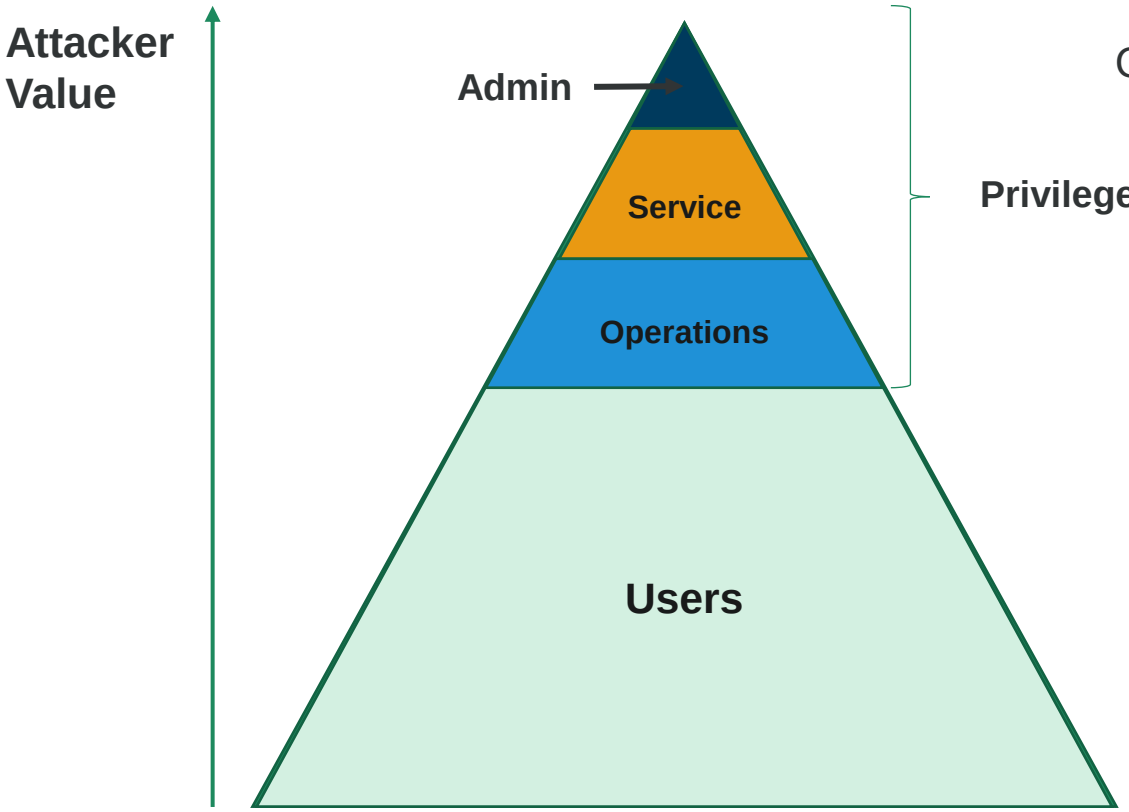
Deep Learning:
Recurrent Neural Network

No blind spots.
Evasion resistant.

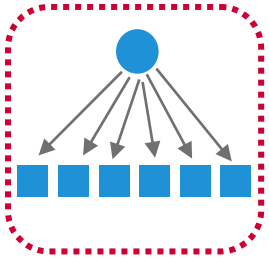
THE ATTACKER VIEW OF PRIVILEGE

- Properly granting permission is hard!
- Attackers abuse privilege gaps
- Vectra finds and protects the gap

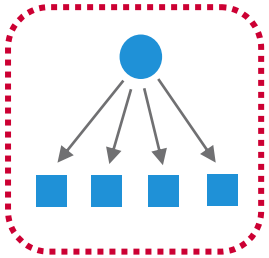
VECTRA'S VIEW OF PRIVILEGE

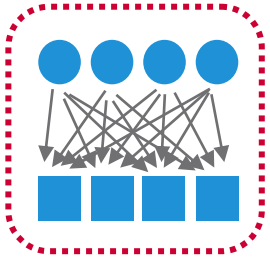


Observe and learn **true** privilege

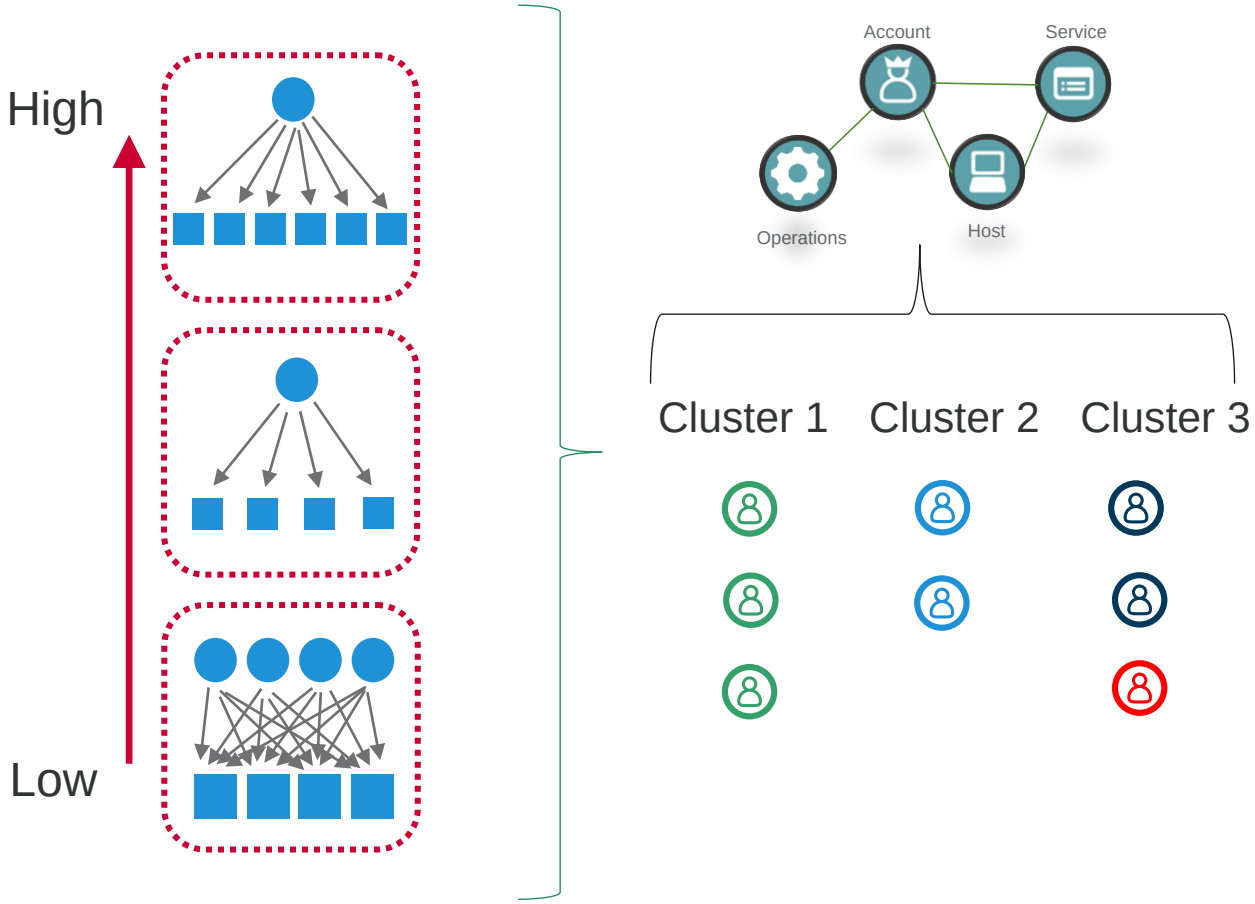


Graph relationships





VECTRA PRIVILEGE ANOMALY MODELS



Unusual Service from Host

Unusual Service - Insider

Unusual Trio

Unusual Account on Host

Unusual Service

Unusual Host

Azure AD Privilege Operation

Thank you!

Vectra: Booth 2852

Dell: Booth 3119