Empowering security superheroes

Applying AI to Detect and Hunt Advanced Attackers

Matt Walmsley

EMEA Director Vectra

matt@vectra.ai

EQUIFAX

The Equifax Data Breach

Majority Staff Report
115th Congress

December 2018

Equifax's Automated Consumer Interview System (ACIS) […] was running a version of **Apache Struts** containing the vulnerability. Equifax did not patch the Apache Struts software […]

The attack lasted for **76 days**. The attackers dropped "web shells" (a web-based backdoor) to obtain remote control over Equifax's network. They **found a file containing unencrypted credentials** (usernames and passwords), enabling the attackers to access sensitive data outside of the ACIS environment. The attackers were able to **use these credentials to access 48 unrelated databases.**

VECTRA

We understand the ways in

Spear phishing email

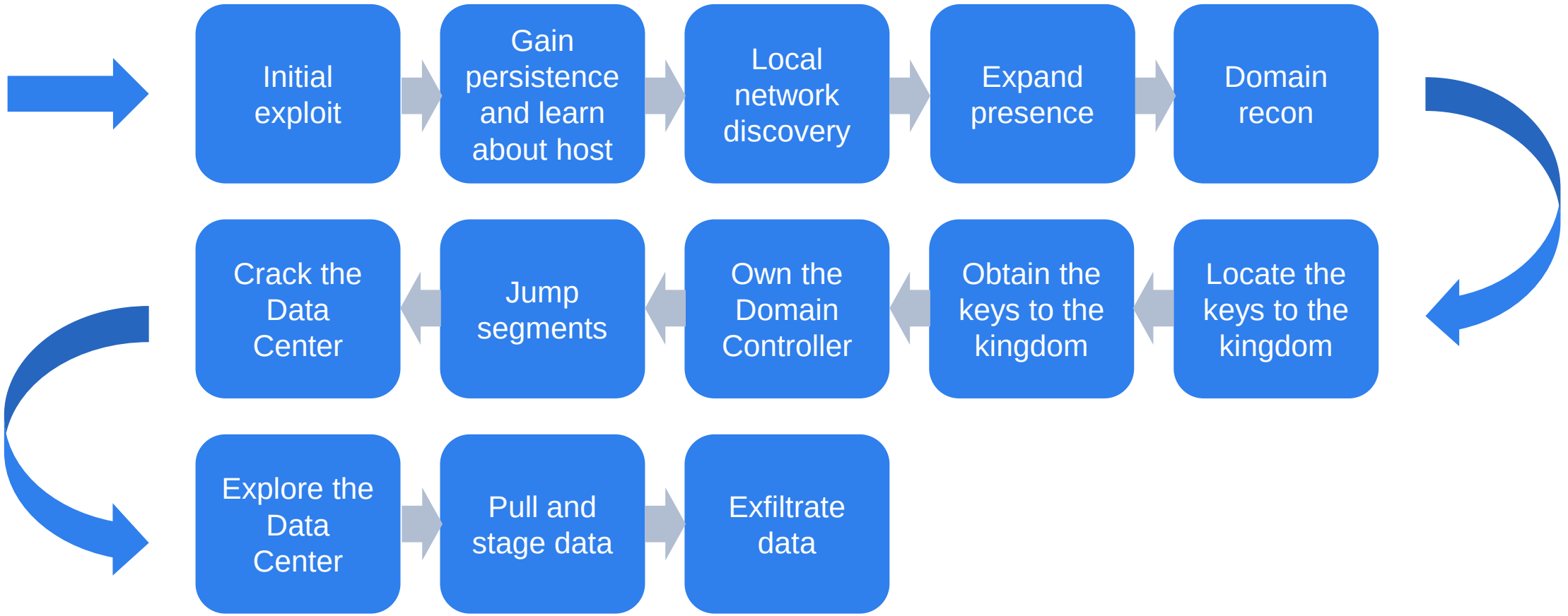
- Already know who to target
- Craft a clever email
- Get them to click

Web server vulnerability exploit

- Identify a vulnerable web property e.g. WordPress or Struts
- Find an exploitable input
- Obtain a shell

VECTRA

A lengthy journey from compromise to breach



Attacker methods

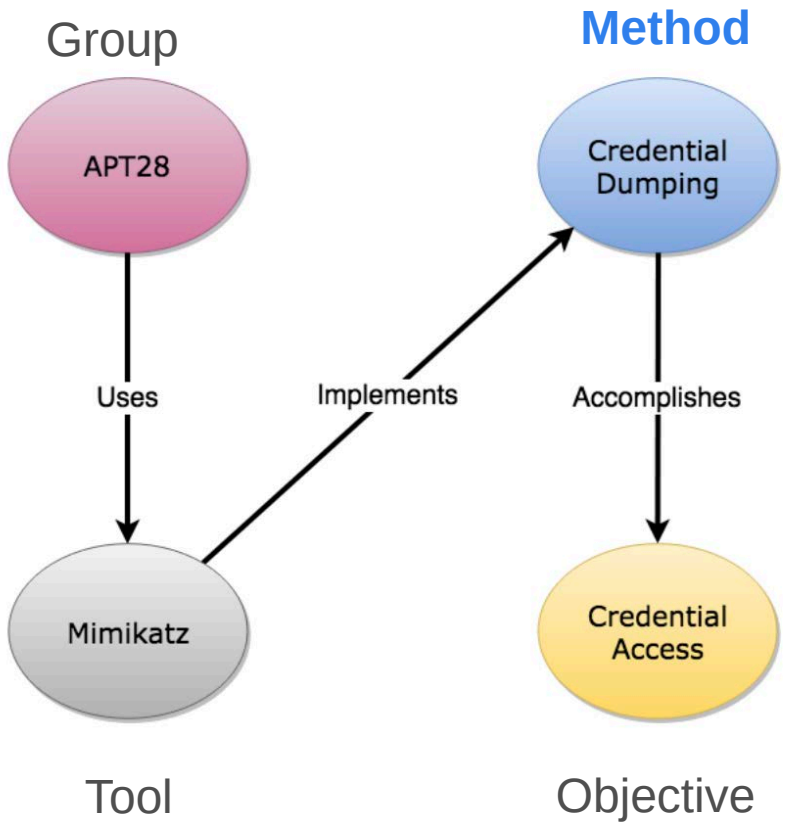
MITRE ATT&CK

- **A**dversarial **T**actics, **T**echniques, **& C**ommon **K**nowledge

- Knowledge base of methods observed in the wild
- Curated from community submissions
- Links to known groups and tools

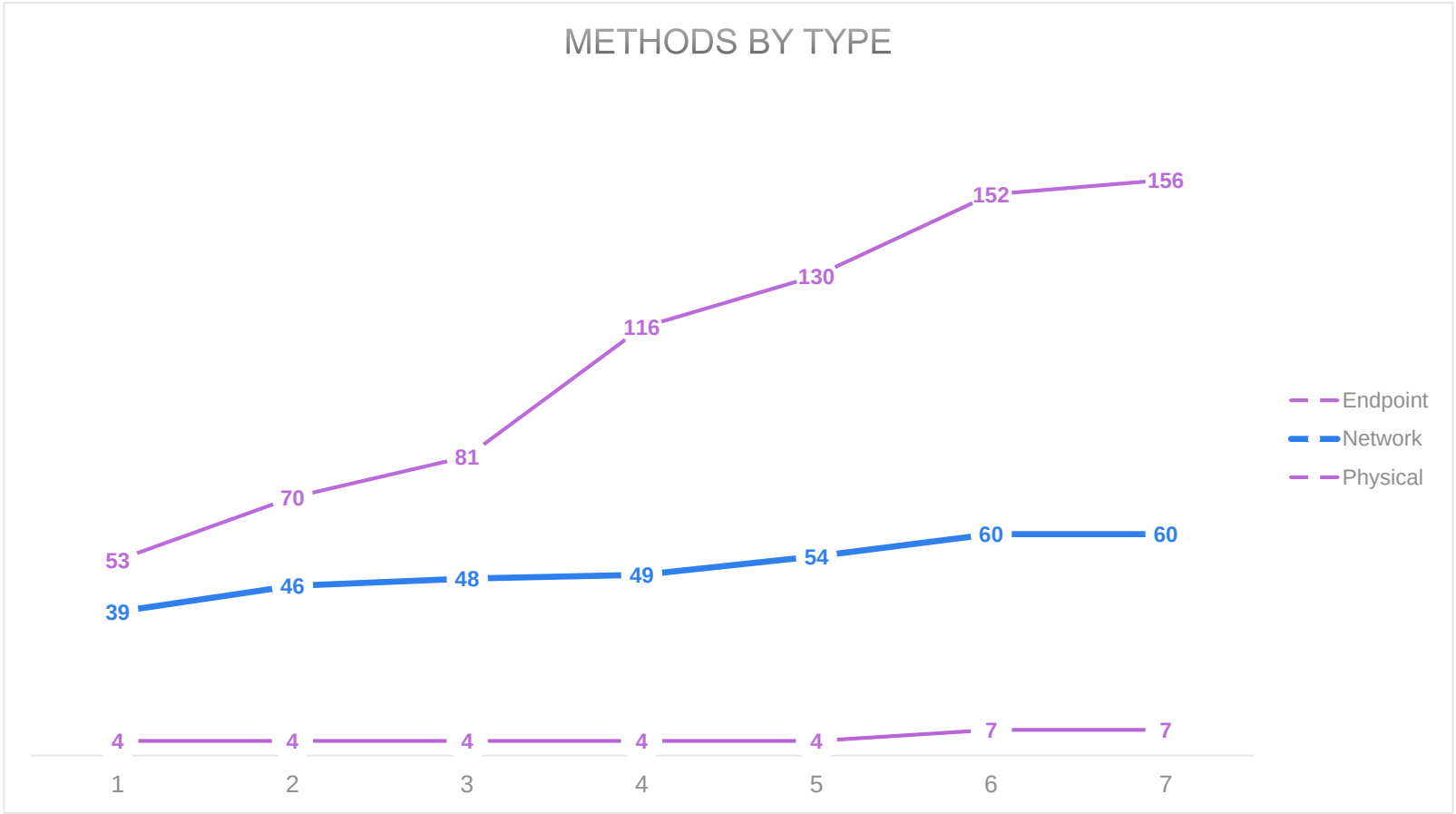
attack.mitre.org

MITRE ATT&CK™



VECTRA®

Methods evolve slowly, especially on the network



May 2015 **ATT&CK Versions** Oct 2018

VECTRA

Detecting attacks using AI

Just looking for anomalies isn’t enough

Unusual ≠ Bad

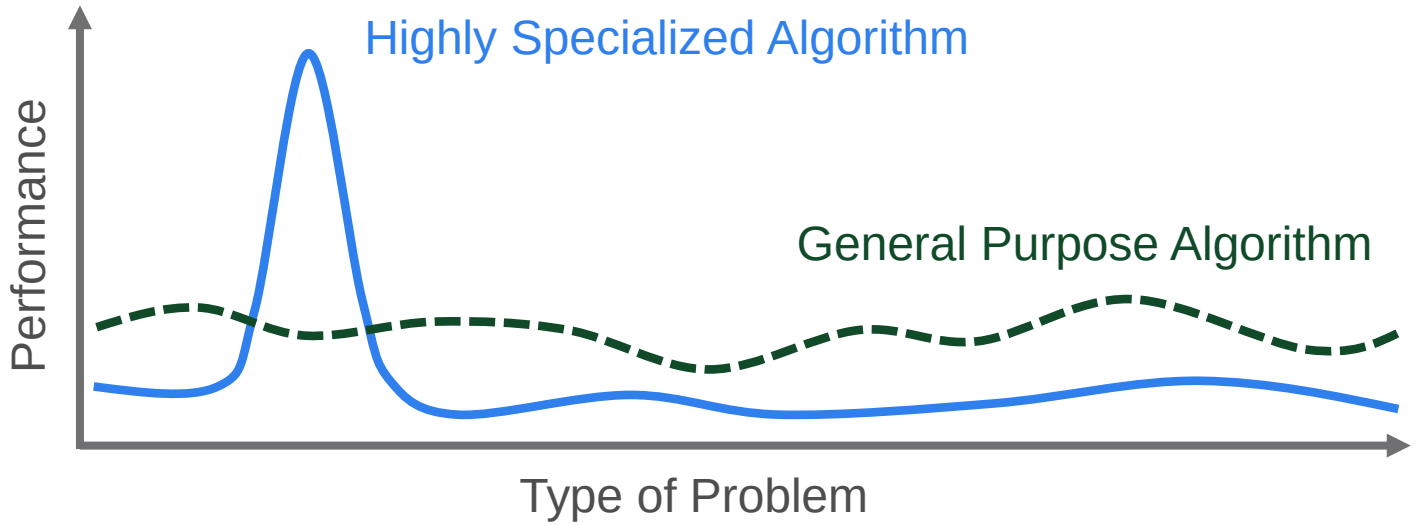
Focus on what attackers must do

Don’t let them hide inside encryption

The “No Free Lunch” theorem

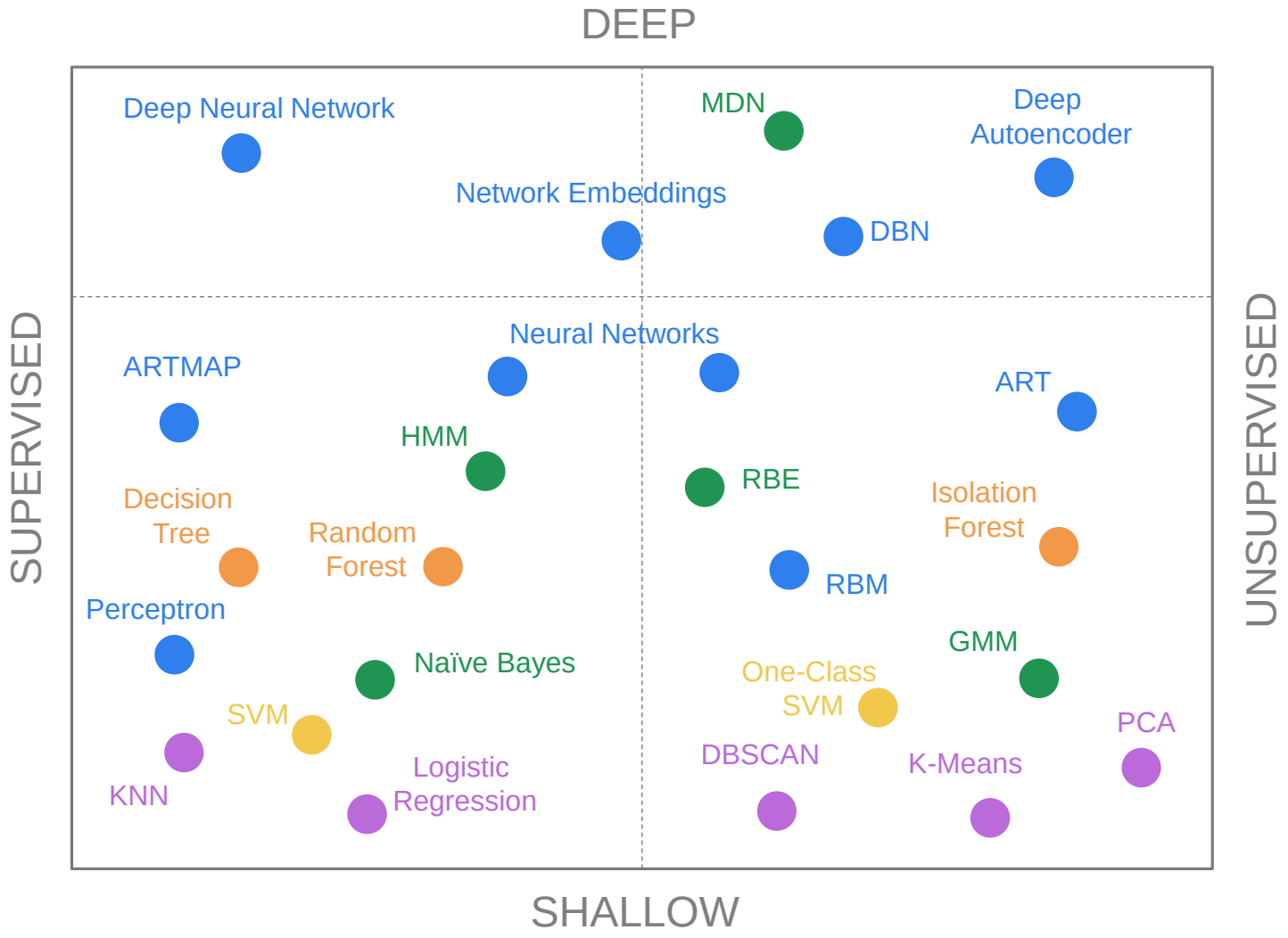
No single algorithm performs best for all problems

Choosing the right algorithm for the problem is critical



VECTRA®

Apply a spectrum of learning approaches

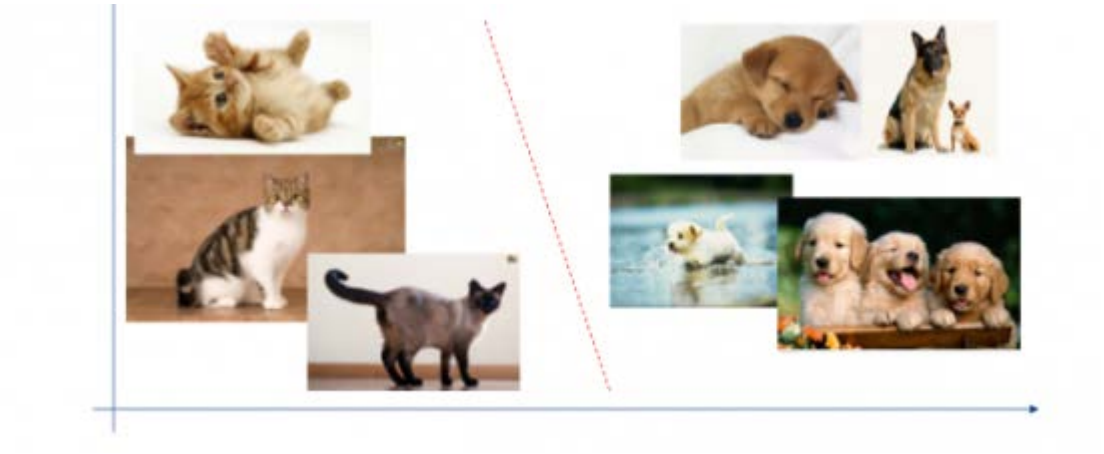


VECTRA

Training approaches

Supervised

Labeled Data Available



Learn to Predict Label from Data

Global threats

Unsupervised

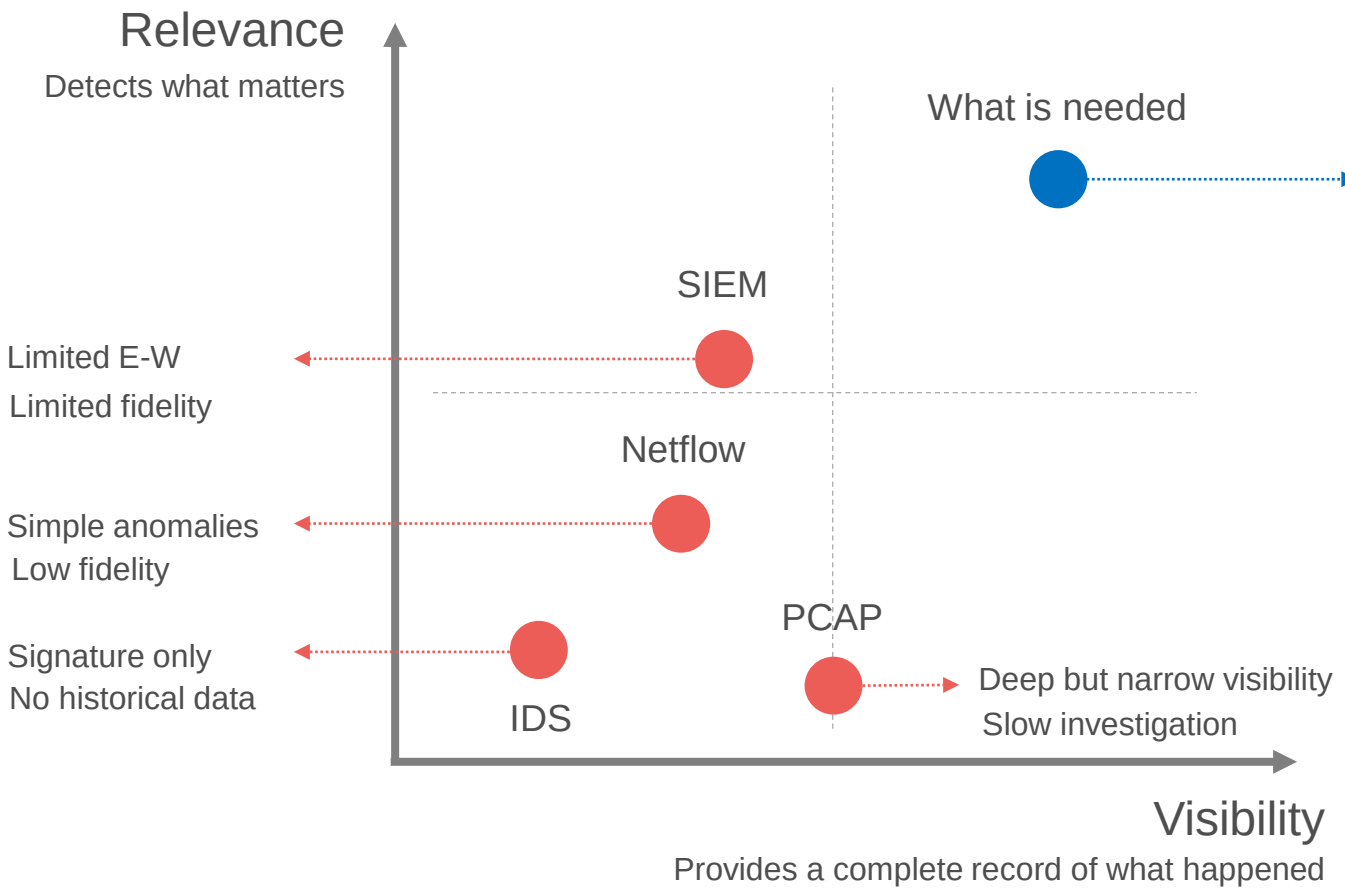
No Labeled Data Available

Discover Structure in the Data

Local threats

VECTRA

Legacy network security is a weak link



Continuous compromise awareness

=

Analysed the right way

AI detections

Smart signatures

Threat intel

▲

The right data

High fidelity

Security enriched

360 deg view

VECTRA®

We need the right data with the right context

Cognito platform

Collects and stores the right network metadata and augments it with machine learning

- High-fidelity
- Security-enriched
- Scalable architecture
- 360° visibility: user, datacenter and cloud
- Real time and historical

VECTRA

Cognito is the ultimate AI-powered network detection and response platform

Cognito Stream

Send security-enriched metadata to data lakes and/or SIEM

Cognito Recall

Investigate and hunt in a cloud-based application

Cognito Detect

Detect and prioritize hidden threats at speed using AI

Cognito platform

The **Cognito** platform collects and stores the right network metadata and enriches it with machine learning

VECTRA

Use AI to detect immutable attacker behaviors

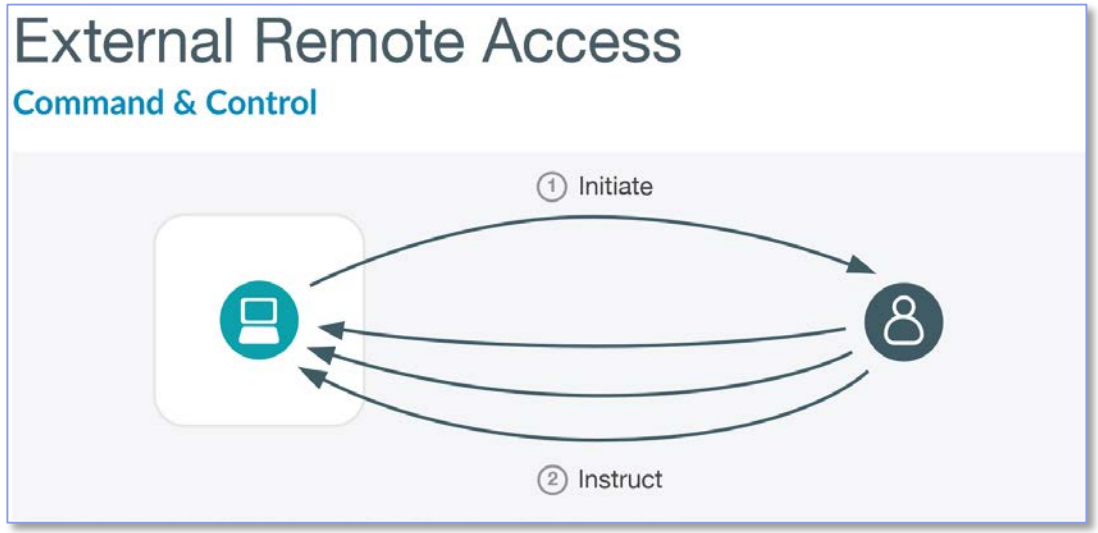
Security Research
Characterise fundamental attacker behaviors

Data Science
AI models to accurately detect behaviors

Attacker Behavior models
High-fidelity, signatureless, and durable detection of methods

VECTRA

Supervised Learning: Classification with Deep Learning

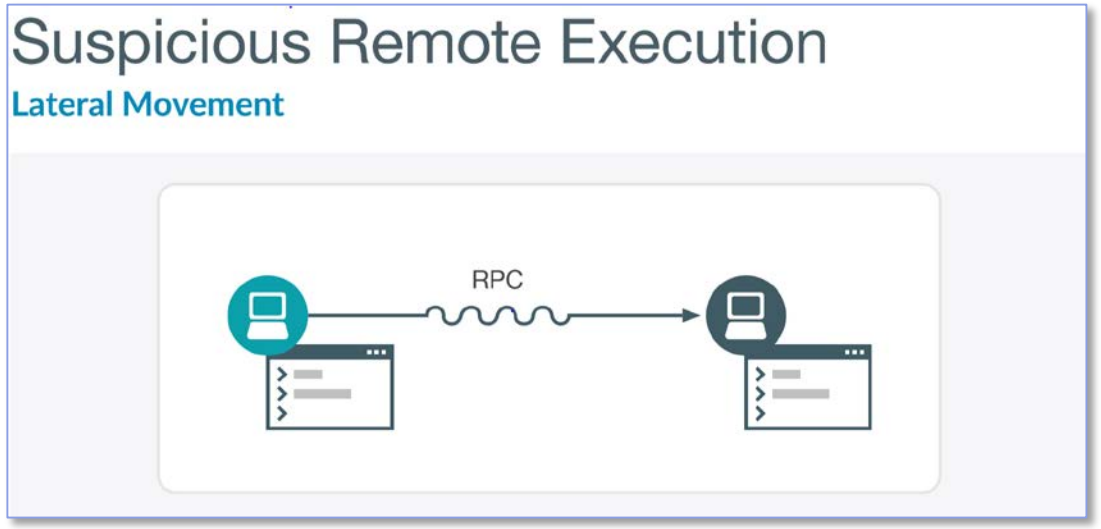


Data: Samples of **Remote Access Tool** traffic and normal traffic.

Features and Separability: Timeseries with traffic statistics at each moment in time; not even close to linearly separable

Model Choice: Not linearly separable? Inputs are timeseries rather than static vectors? Requires a **Recurrent, Deep Neural Network**.

Unsupervised Learning: Custom Novelty Detector



Data: DCE/RPC data for UUIDs performing remote code execution on your network

Features and Constraints: Timeseries of [uuid, src, dst, account] tuples on DCE/RPC

Model Choice: Custom novelty detector anchored on UUIDs to detect unexpected remote execution

VECTRA

Spot attackers throughout 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

VECTRA®

Mapping to the Equifax attack

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

Summary

- Prevention is good, BUT there will always be a way in
- Enterprise remain blind to attackers active inside their network
  - Attacker dwell times too long
- Attacker methods remain stable over time

- **Opportunity to detect attackers using AI**
- **Stop compromise from becoming a breach**
- **Address skills and resource gaps**
  - Automation empowers analysts
  - Reduce barriers to entry into our profession

VECTRA®

Thank you

Join the hunt

vectra.ai