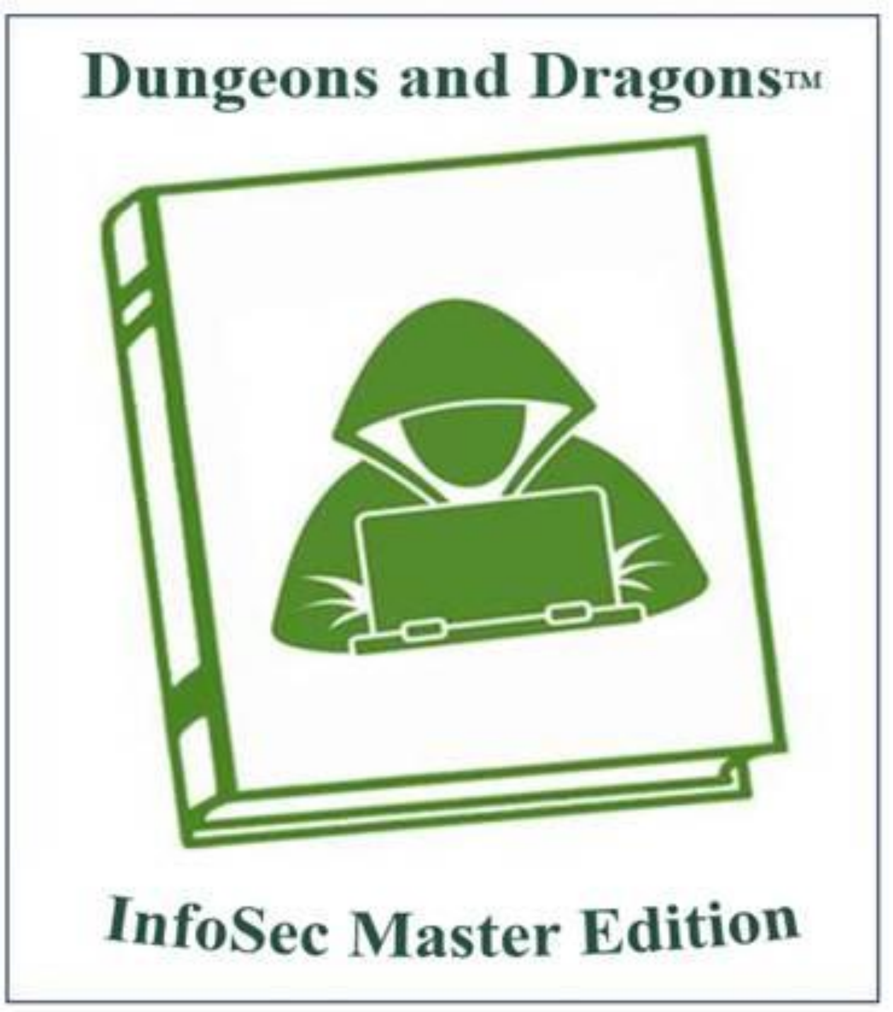
Welcome To The 10th Annual Hacking Conference



The Institute of Internal Auditors
Chicago

ISACA®
Chicago Chapter

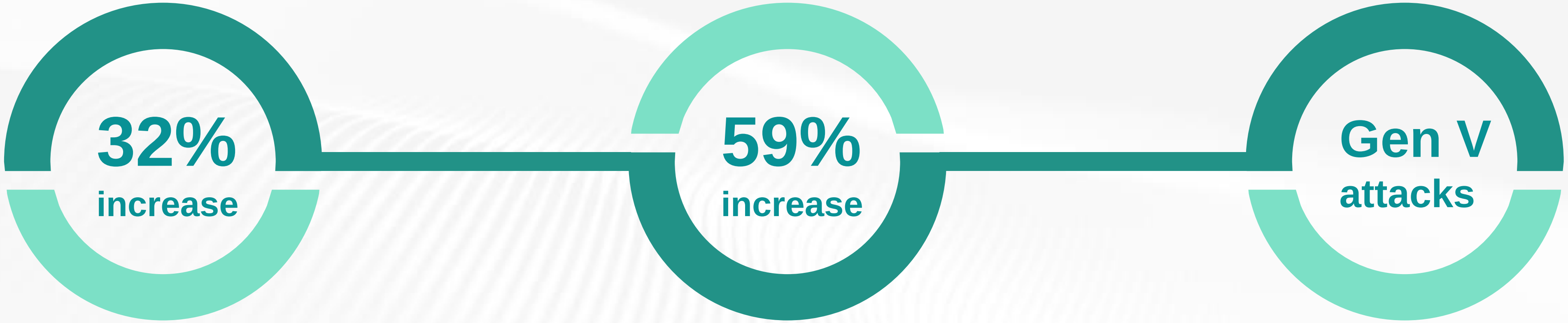
Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session
on the app!

The Institute of
Internal Auditors
Chicago

ISACA
Chicago Chapter

The Threat Landscape Is Growing Exponentially



32%
increase

in global weekly
cyber attacks (YoY)

59%
increase

in ransomware
attacks

Gen V
attacks

at nation
state scale

Security Teams Focus on Detection

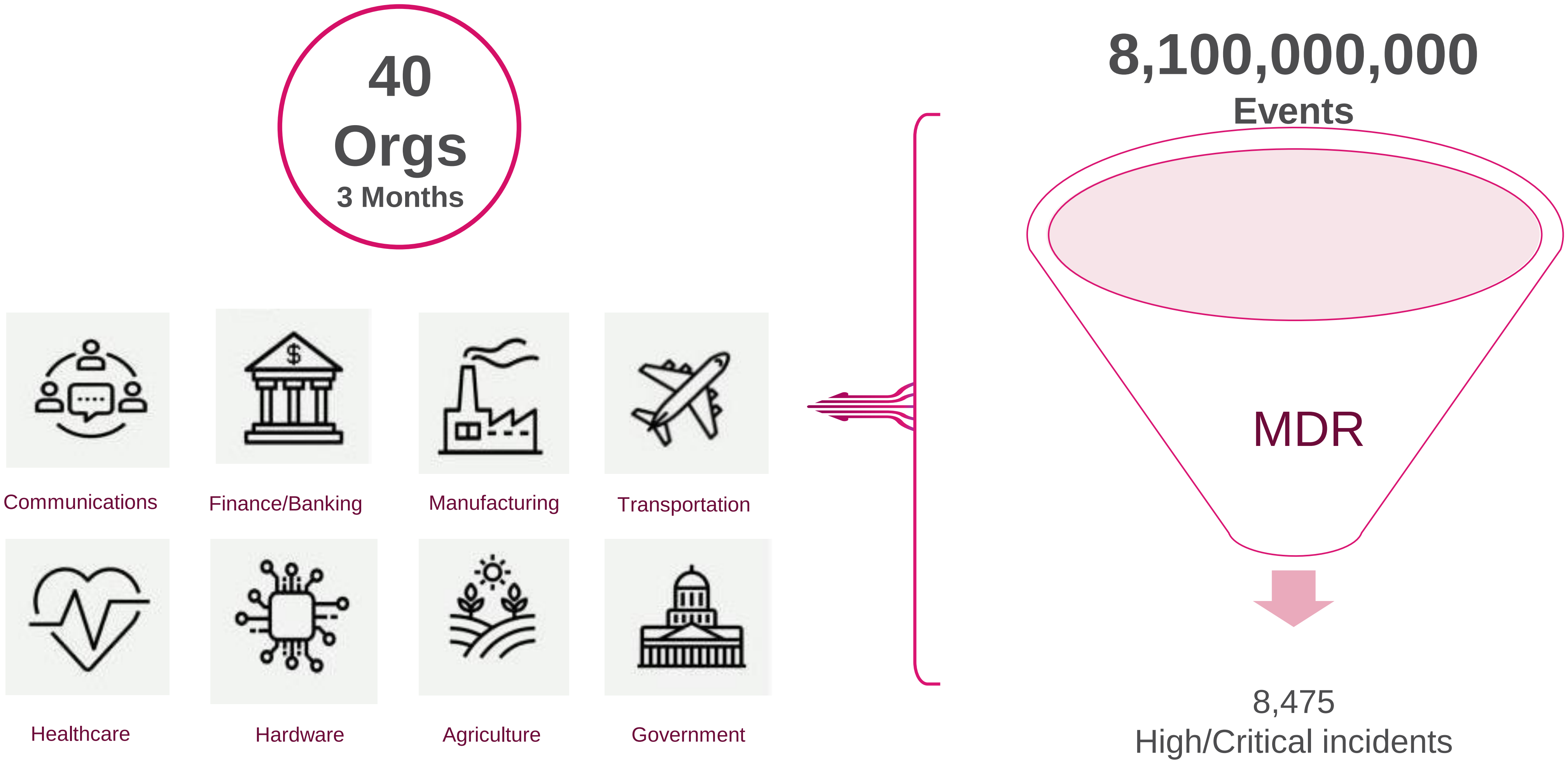
» Endless alerts, false positives

» Multiple tools in siloes

» Narrow attack vector view lacks context

» Cyber experience and skillset shortage

Efficacy of MDR services



40 Orgs

3 Months

Communications

Finance/Banking

Manufacturing

Transportation

Healthcare

Hardware

Agriculture

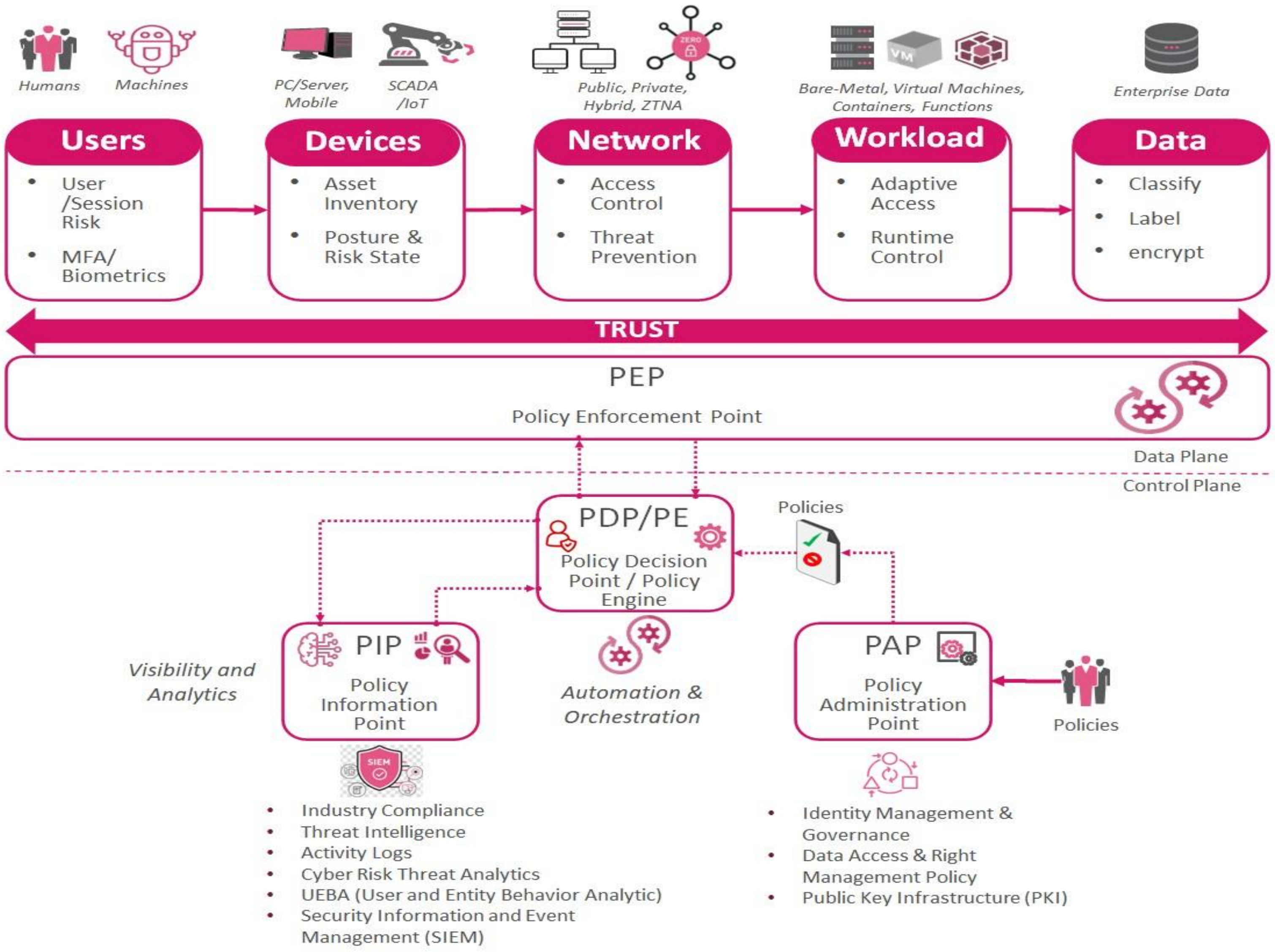
Government

8,100,000,000 Events

MDR

8,475 High/Critical incidents

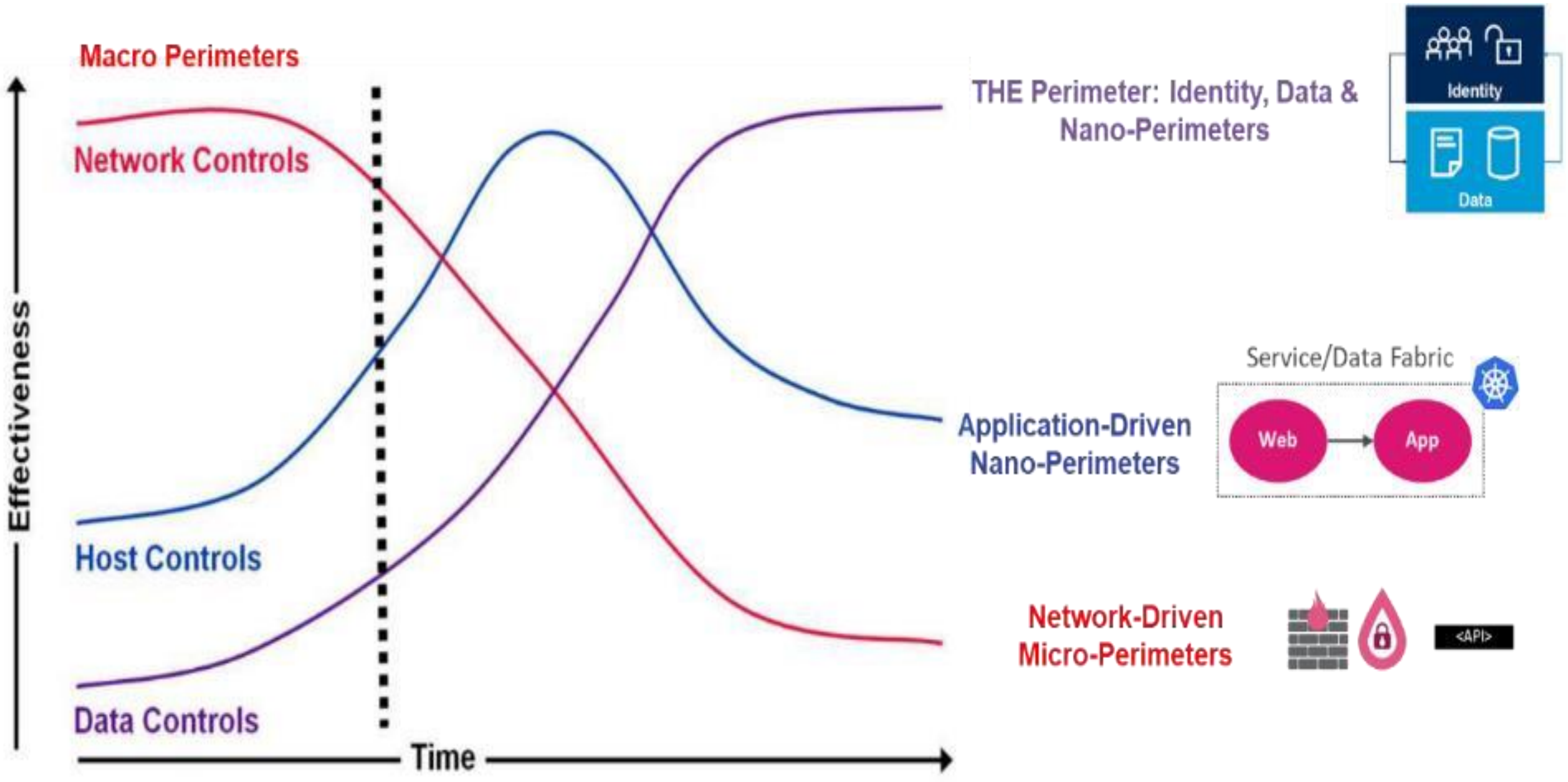
MDR and Zero Trust



- Industry Compliance
- Threat Intelligence
- Activity Logs
- Cyber Risk Threat Analytics
- UEBA (User and Entity Behavior Analytic)
- Security Information and Event Management (SIEM)

- Identity Management & Governance
- Data Access & Right Management Policy
- Public Key Infrastructure (PKI)

Zero Trust Journey



AI in Threat Detection

Classic Machine Learning vs. Deep Learning

Classic Machine Learning

exe

Features definition

Certifier
OS
Compiler info
Metadata
Packer
Writable
Permissions
...etc.

CLASSIFIER ALGORITHM

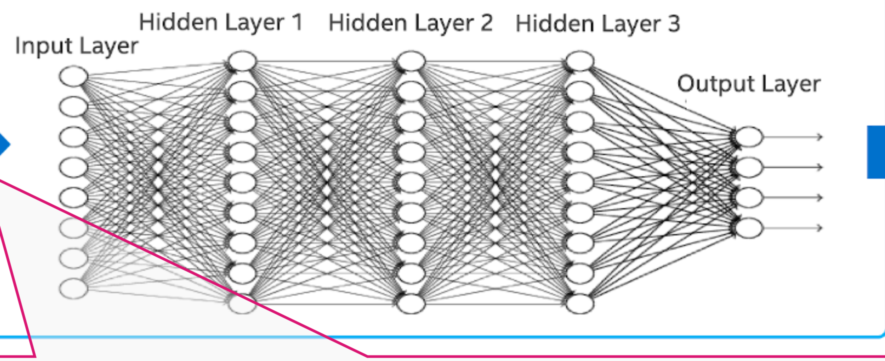
SVM
Random Forest
Decision Trees
...

Malicious

Deep Learning

exe

NEURAL NETWORK



Malicious

Stop Chasing Ghosts or Dragons

All **file bytes** are processed == **30% Better** detection rate
90% Less false positives

CHECK POINT

Ransomware Resilience

*Insurability is Increasingly Dependent On Cyber Hygiene**

Critical Cybersecurity Controls
Multi Factor Authentication (MFA) for VPN & Admin Access
Endpoint Detection & Response (EDR) & Mobile Device Management (MDM)
24/7/365 Monitoring / Alerting (SOC/SIEM)
Vulnerability Management & Process or Protocol for Applying Critical Patches (Patch Management)
Secure Offline Backups (Immutable)
Remote Desktop Protocol (RDP) / SSH is not exposed outside the firewall (Security Assessments)
Privileged Access Management (PAM)
Email Filtering & Validation Process (Security Awareness Training)
End of Life Systems should be replaced
Incident Response Plan (IR) for different types of events (insider threat, ransomware, breach)

**Note: Each insurance carrier has their own specific control requirements that may differ by insured's revenue size & industry class*

Real world examples of MDR in action

North American County Municipality

- 1180 Users
- 2500 IT Assets

Challenge: Needed 24x7x365 Monitoring for compliance

Zero Day Threat: Detected Mimikatz threat
on Exchange server in the middle of the night

- Identified Zero day utilizing Endpoint protection in “detect”
- Responded in 5 minutes to:
  - Kill process,
  - Full forensics sweep on server,
  - Isolated lateral movement,
  - Implemented IPS protections,
  - Called customer to notify,
  - Installed patch,
  - Continued to monitor

North American Very Large City – Department of Health

- 6500 Users, 20+ locations, Primary Hospital
- 15k devices, 50+ external partners, wide range of missions

Challenge: Could not monitor environment without $3-5m in spend to build a 24x7x365 SOC

- High level of security already deployed but could not scale with the noise
- We connect with the customer 2-3 times a week
- **Critical threats lowered from 30 a week to 1-2 a week**
- Authorized software and browser plugins caused significant risk
- Phishing attacks a major threat
- **10k cases per week with 9500 closed automatically**

West European Freight Forwarding Company

- 400 Users
- 500 IT assets

Challenge: Needed 24x7x365 Monitoring for compliance

- Did not have the resources to monitor environment
- Weekly attacks to target freight movements
- Phishing attacks created significant risks (DHL, UPS themed)
- **Lowered number of attacks from 10’s per week to 1-2 a month**

Questions

- How long does it take to implement an MDR solution?
  - 90 days to 6 months

- What is the difference between MDR/SOC/SIEM/SOAR?
  - (SIEM/SOAR) =XDR

- Why is EDR not enough protection for my protection?

Welcome To The 10th Annual Hacking Conference

Remember to check-in to this session on the app!

The Institute of Internal Auditors
Chicago

ISACA®
Chicago Chapter