

The State of Artificial Intelligence in Security and Risk Management

Jeremy D'Hoinne
@jeremydhoinne

© 2020 Gartner, Inc. and/or its affiliates. All rights reserved. Gartner is a registered trademark of Gartner, Inc. and its affiliates. This publication may not be reproduced or distributed in any form without Gartner's prior written permission. It consists of the opinions of Gartner's research organization, which should not be construed as statements of fact. While the information contained in this publication has been obtained from sources believed to be reliable, Gartner disclaims all warranties as to the accuracy, completeness or adequacy of such information. Although Gartner research may address legal and financial issues, Gartner does not provide legal or investment advice and its research should not be construed or used as such. Your access and use of this publication are governed by [Gartner's Usage Policy](#). Gartner prides itself on its reputation for independence and objectivity. Its research is produced independently by its research organization without input or influence from any third party. For further information, see "[Guiding Principles on Independence and Objectivity](#)."

Gartner®

AND BY DRASTICALLY INCREASING THE AMOUNT OF LEAD IN THE WATER SUPPLIES OF THE WORLD, WITHIN THREE GENERATIONS, WE SHALL HAVE CREATED A HUMAN LEVEL ARTIFICIAL INTELLIGENCE!

I... WHAT?
HOW?



**Any AI can be made
“human level” by
lowering all human
intelligence.**

Key Areas Where New Algorithms Can Improve Enterprise's Security Posture

1

**Infrastructure
Protection**

2

**Identity and
Access Management**

3

**Risk
Management**

4

**Application
and Data Security**

5

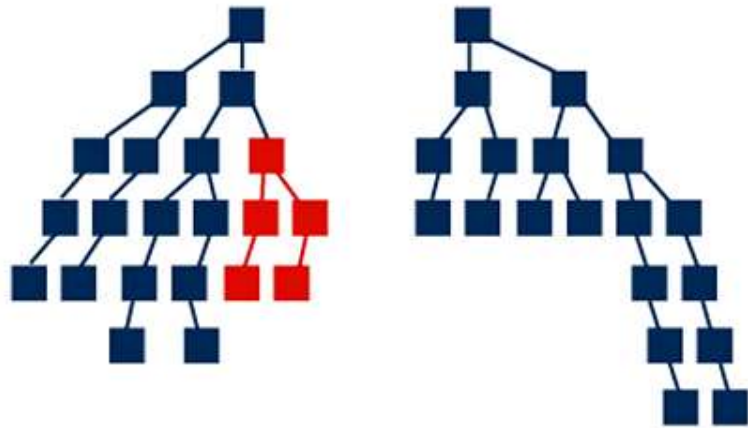
**Security
Operations**

1a

**Infrastructure
Protection —
*Prevent:
Threat Detection***

Machine Learning for Threat Detection

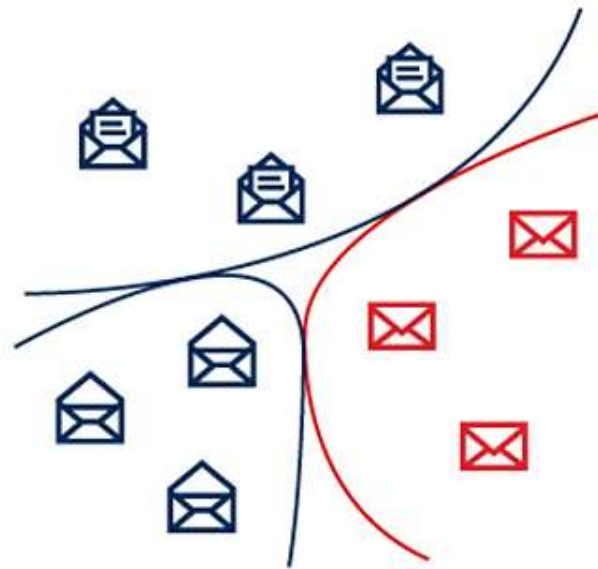
Malware



Classification

Static and dynamic analysis

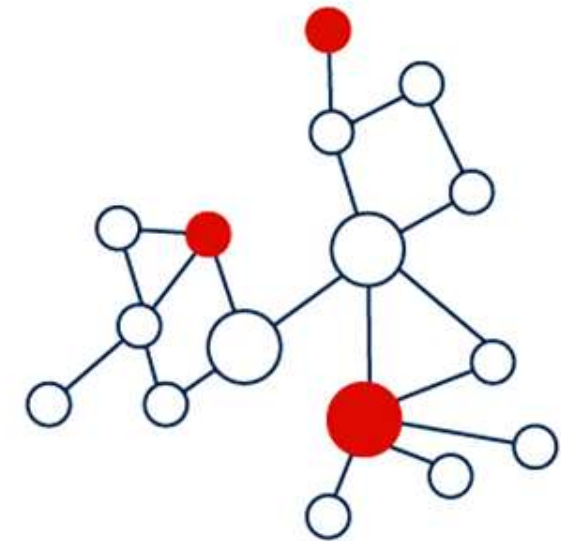
Spam



Classification

Content and header

Phishing



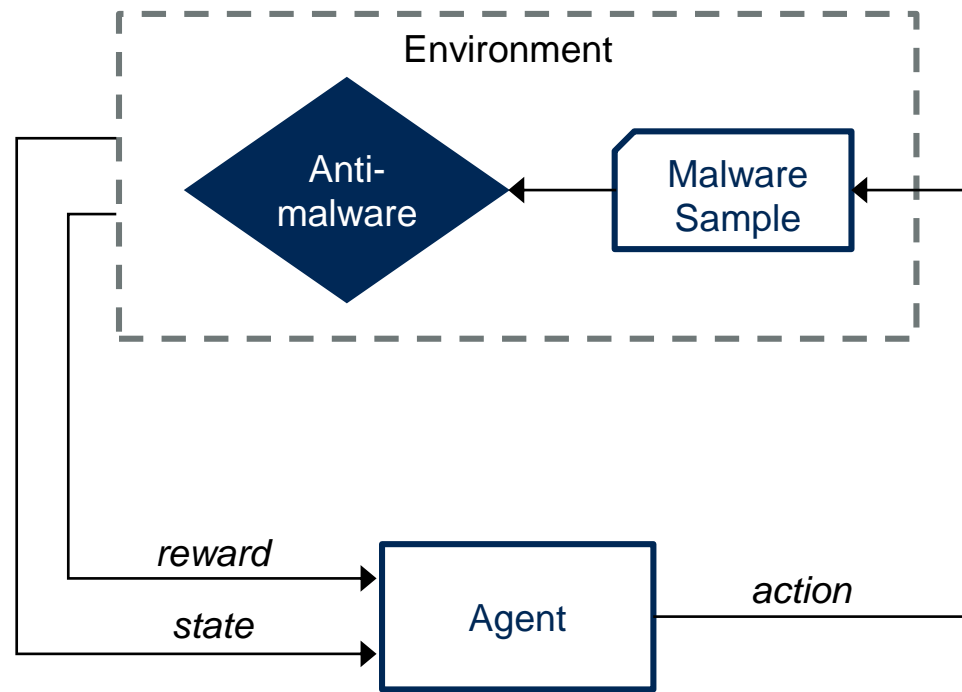
Social Graph

Links — server and sender IPs

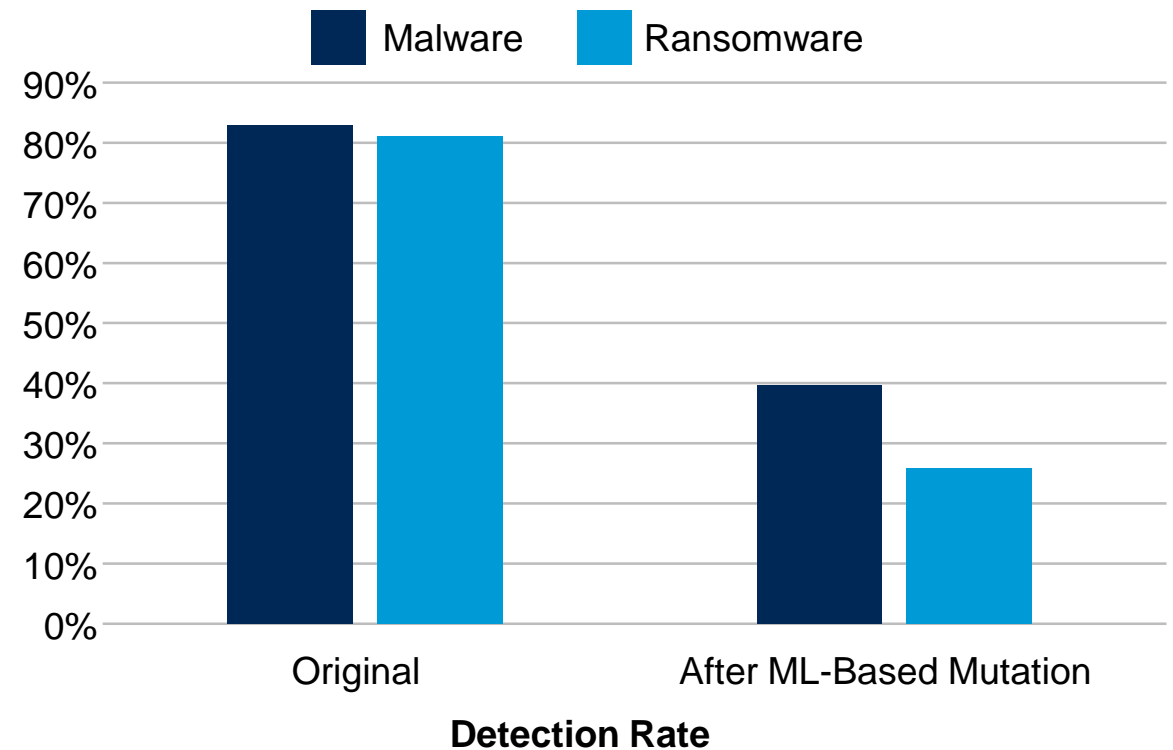
Sometimes You're the Cat and Sometimes You're the Mouse: Attackers Like "AI" Too

Using reinforcement learning to evade machine learning based malware detection:

Markov Decision Process Formulation of the Malware Evasion Reinforcement Learning Problem



Malware Detection Rate (VirusTotal)



Source: ["Learning to Evade Static PE Machine Learning Malware Models via Reinforcement Learning."](#) arXiv

1b


Infrastructure Protection — *Detect: Behavioral Analysis*

Sample Detection Leveraging Machine Learning

Mon Mar 23, 20:00:03  Ian Desktop breached model **Unusual Activity / Unusual Internal Data Volume as Client or Server**

Mon Mar 23, 19:30:00  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:29:01   **Unusual Activity 66% due to Internal Data Transfer and External Data Transfer from Ian Desktop**

Mon Mar 23, 19:28:59  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection and a recent small increase in incoming data volume from Sarah Desktop port 3389

Mon Mar 23, 19:27:59  → Ian Desktop was still connected to Sarah Desktop [3389]


An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:26:59  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:26:00  → Ian Desktop was still connected to Sarah Desktop [3389]


An unusual time for a connection and a recent small increase in incoming data volume from Sarah Desktop port 3389

Mon Mar 23, 19:25:07  → Ian Desktop was still connected to Sarah Desktop [3389]


An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:24:07  → Ian Desktop was still connected to Sarah Desktop [3389]


An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:23:06  → Ian Desktop was still connected to Sarah Desktop [3389]


An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:22:10  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:21:10  → Ian Desktop was still connected to Sarah Desktop [3389]



An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:20:10  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:19:02  → Ian Desktop was still connected to Sarah Desktop [3389]

An unusual time for a connection to Sarah Desktop on port 3389

Mon Mar 23, 19:18:31   **RDP Cookie – ben [3389]**

New activity



Unusual Interactive Traffic from an External Endpoint

COMMAND & CONTROL, ACTIONS ON OBJECTIVE

Mar 31 11:00

lasting an hour

10.10.12.9 appears to be remotely controlled through an interactive shell by the external endpoint 52.225.114.174. This behavior indicates that 10.10.12.9 has been compromised by a user outside of your local network.

Protocol and ports linked to interactive traffic:

- TCP 443 <-> 61040

OFFENDER



52.225.114.174
er31.sjc.sl.example.net

VICTIM



workstation-admin-x05
10.10.12.9

Hide

Acknowledge

Investigate This Detection →

! Geographically Unusual Remote Access ▾

! i-Ode8d37876cfcd3e4 ▾

Status Open

ID 1453

Description

Device has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source would trigger this alert. This alert uses the Remote Access observation and may indicate misuse or a compromised device.



Assign Share

Investigate in Cognito Recall ?

▼ Unusual keyboards for this network used with server 192.168.12.11

- Mar 29th 2020 18:47
- RDP Client Token: andyb
- RDP Clientname: hacktool
- Product ID: xyz

Unusual keyboard layout: Serbian (Cyrillic) - 3098

Normal keyboard layouts for this network between: Mar 29th 2020 - Mar 29th 2020 18:47

Hebrew - 1037

Finnish - 1035

US - 1033

French - 1036

Spanish - 1034

“99% of the value we see today comes from supervised learning.”

Andrew NG, April 2020



Rule-based

Supervised
Learning

Unsupervised
Learning

Deep
Learning

“99% of the value we see today comes from supervised learning.”

Andrew NG, April 2020



Rule-based + Supervised Learning + Unsupervised Learning + Deep Learning

With Machine Learning for Threat Detection, the Details Matter

- **Expect incremental, not transformative results**
- Match the threat detection technology with the threat environment
- Prioritize questions on the scope of ML techniques, rather than the efficacy
- Measure, measure, measure
- Anticipate “ML maintenance” costs
- Combine new techniques with proven ones, don’t replace

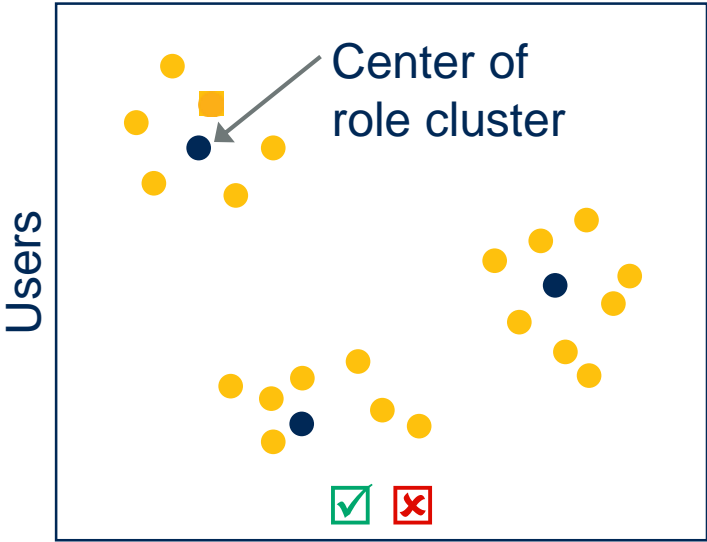
2

Identity and Access Management

IAM Machine Learning Use Cases

Identity Analytics

Governance



Entitlements

Smart Cluster Analysis

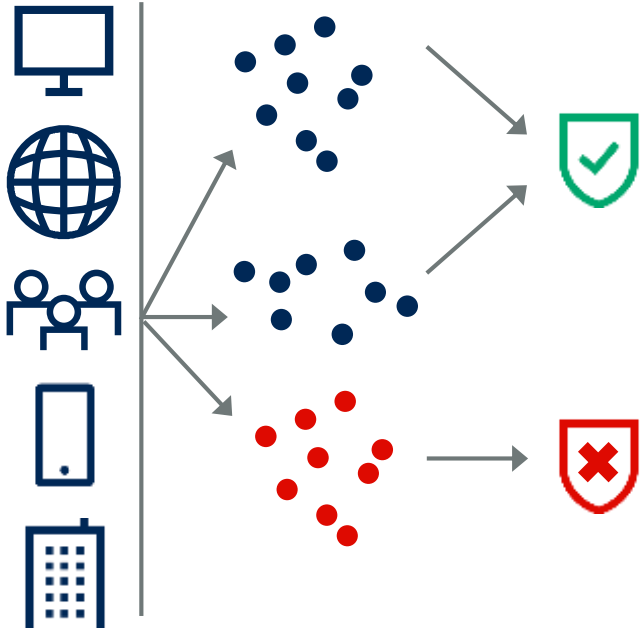
Identity Proofing



Image Recognition

Online Fraud Detection

Behavioral Profiling



Rule-based + (un)supervised machine learning + deep learning

Improve Your Organization's ML Skills Before It Is Necessary

Involvement

Required Understanding



CISO

- Set expectations
- Approve select AI experiments

- AI hype vs. reality
- AI maturity for security use



Technical Advisors

- Recommend select use of AI
- Define evaluation metrics

- Architecture impacts
- Algorithms (high level)



Privacy Leaders

- Ensure compliance
- Avoid fines

- Data usage
- Data flows
- Data control



Security Operations

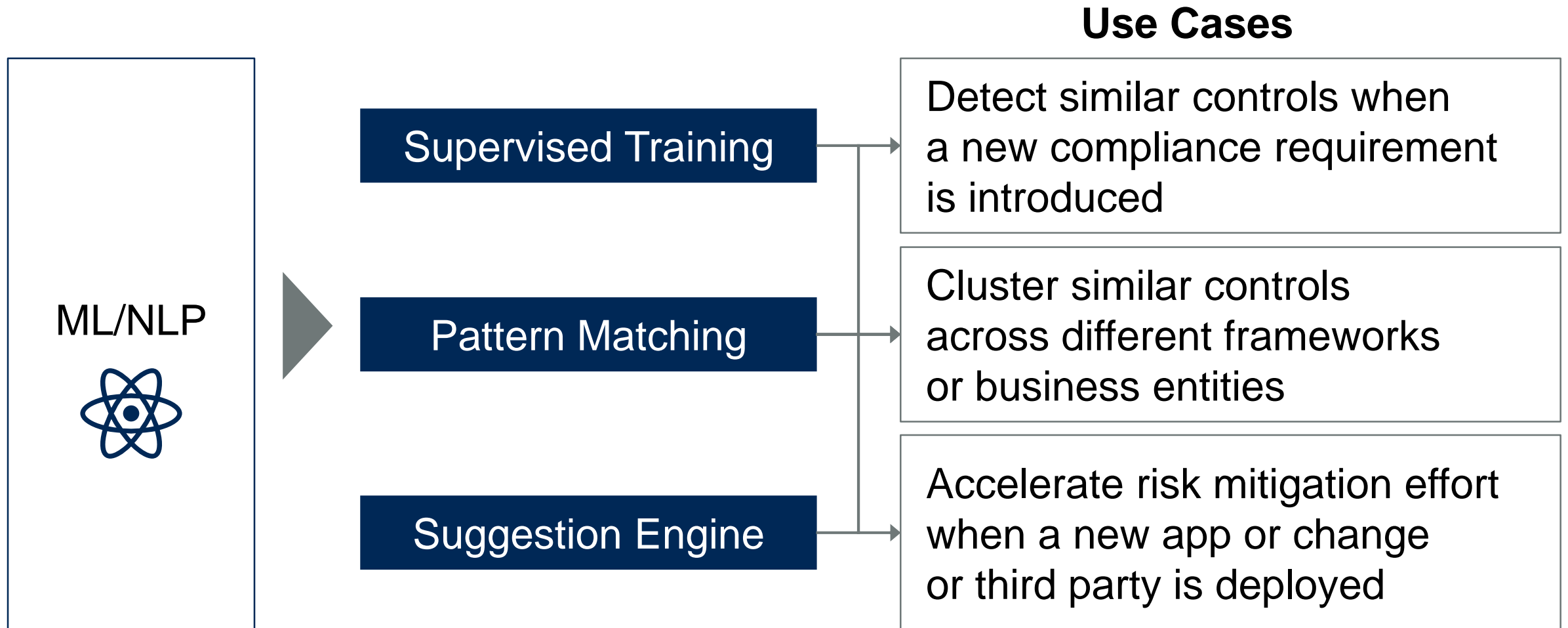
- Adapt workflows
- Measure and report efficacy
- Explain “AI results”

- Engine tuning options
- Automated decision “logic”
- Is ML the best tool or not?

3

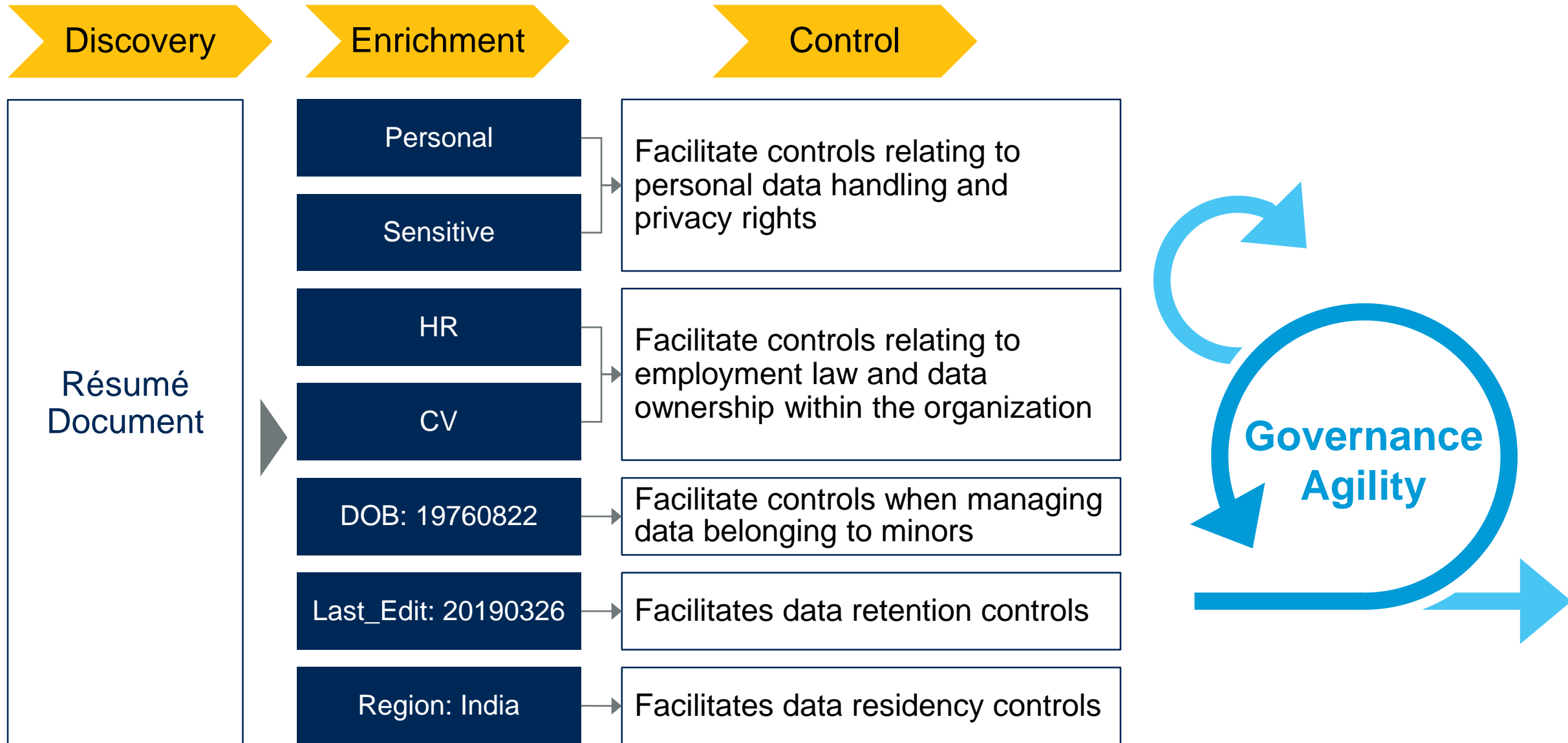
Risk Management

Emerging Risk Management Use Cases by Applying ML/NLP



Better Identifying Privacy Risks

Using techniques such as ML, computer vision and NLP to automate both static and dynamic tagging, ultimately to delivery governance agility.

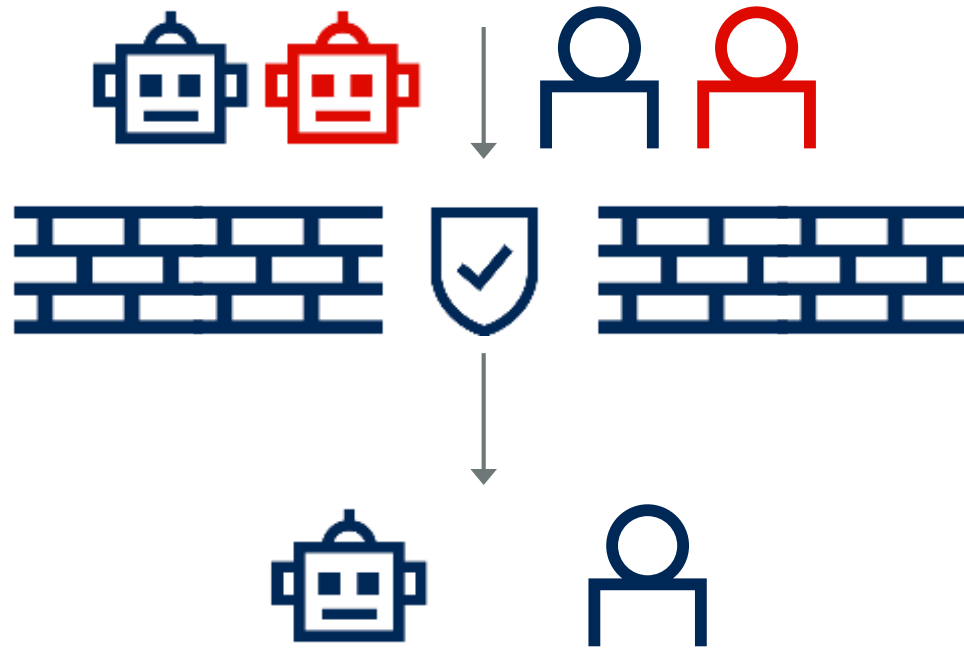


4

Application and Data Security

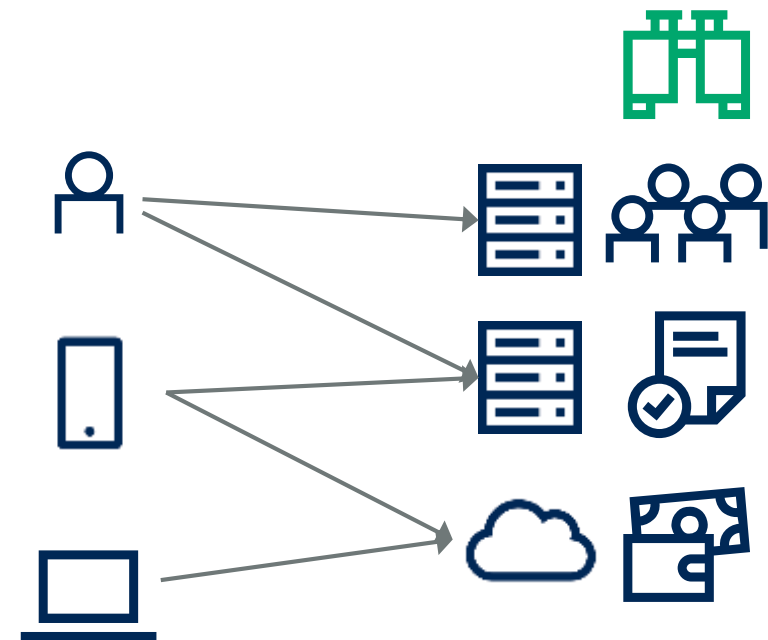
Machine Learning's Maturity Varies With Use Cases

Bot Detection



Behavioral analysis complements reputation, rule and fingerprinting.

Data Security



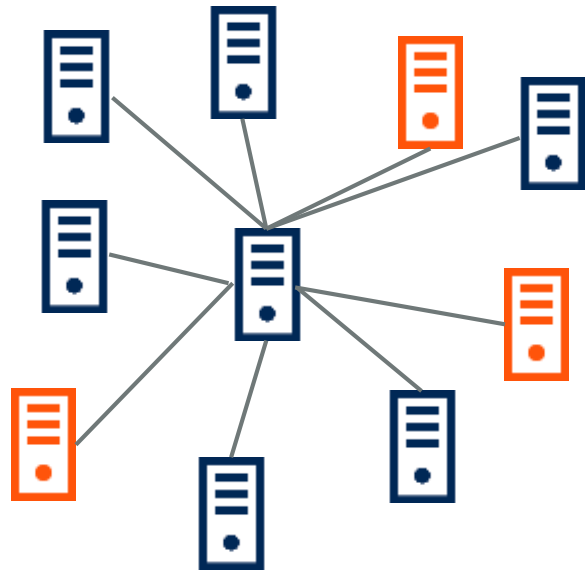
Started with data discovery and categorization. Growing use for DLP.

5

Security Operations — *Respond*

Security Operation Automation

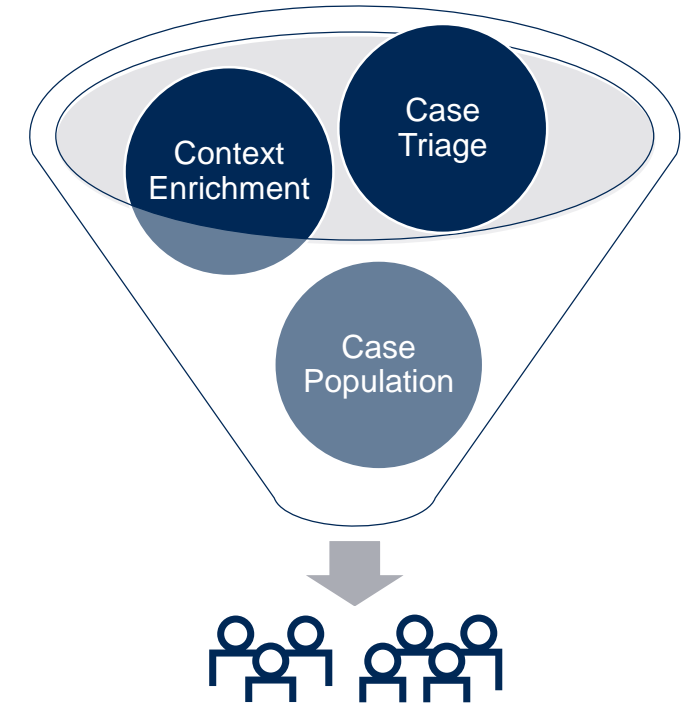
Asset Discovery



Policy Automation



Orchestration



- The value of automation stops where accountability begins.
- Good solutions enable continuous learning and incremental changes.

Optimizing Costs With AI



Don't buy AI. Purchase complementary techniques with measurable results against your higher risk threat vectors.



Do competitive Proof of Concept once you have the outcome-driven metrics ready.



Favor short-term (one year) subscriptions.



Focus on people and process before the tool. AI won't replace staff.

THAT WAS SURPRISINGLY EASY. HOW COME THE ROBOTIC UPRISING USED SPEARS AND ROCKS INSTEAD OF MISSILES AND LASERS?

IF YOU LOOK TO HISTORICAL DATA, THE VAST MAJORITY OF BATTLE-WINNERS USED PRE-MODERN WEAPONRY.



Wrapping Up

State of AI Across Security Leaders

Key Initiatives

Infrastructure Protection	<ul style="list-style-type: none">• Threat detection (malware, spam, phishing, ...)• Anomaly detection (network, endpoint, ...)
Identity and Access Management	<ul style="list-style-type: none">• Identity analytics (governance, identity proofing)• Online fraud detection
Risk Management	<ul style="list-style-type: none">• Compliance• Privacy risks
Application and Data Security	<ul style="list-style-type: none">• Bot mitigation• Data discovery and categorization
Security Operations	<ul style="list-style-type: none">• Asset discovery• Policy automation• Security orchestration

Recommendations

- ✓ Embrace AI in security for uses where there is no shortage of high-quality training data.
- ✓ Use machine learning as a complementary technique.
- ✓ Set technology as staff augmentation, not replacement.
- ✓ Choose metrics before you start evaluating.
- ✓ Test (on your data), test (to solve your problems), test (against others).

Action Plan for CISOs

Monday Morning:

- *Review* existing use of machine learning in security and risk management
- *Survey* your team about promising uses of machine learning

Next 90 Days:

- *Measure* more reliably with consistent metrics for each use case
- *Prioritize* areas for machine learning experiments

Next 12 Months:

- *Experiment* machine learning as a feature, where you can evaluate efficacy
- *Standardize* framework for evaluating new algorithms

Recommended Gartner Research

- 🔍 [5 Areas Where AI Will Turbocharge Privacy Readiness](#)
Bart Willemsen (G00380045)
- 🔍 [Practical Privacy — Discovery Automation of Privacy Risk](#)
Nader Henein and Marc-Antoine Meunier (G00376386)
- 🔍 [Market Guide for User and Entity Behavior Analytics](#)
Gorka Sadowski, Jonathan Care and Others (G00361156)

Recommended Gartner Research — IAM

- 🔍 [Modernizing IAM Architecture With Machine Learning](#)
Mary Ruddy (G00386813)
- 🔍 [Transform User Authentication With a CARTA Approach to Identity Corroboration](#)
Ant Allan and Jonathan Care (G00345217)
- 🔍 [How to Select a Machine Learning Vendor for Fraud Detection in Online Retail](#)
Akif Khan and Jonathan Care (G00382774)