

**OutThink is a recognized vendor in the Security Awareness and Human Risk Management categories.**

### **Gartner**

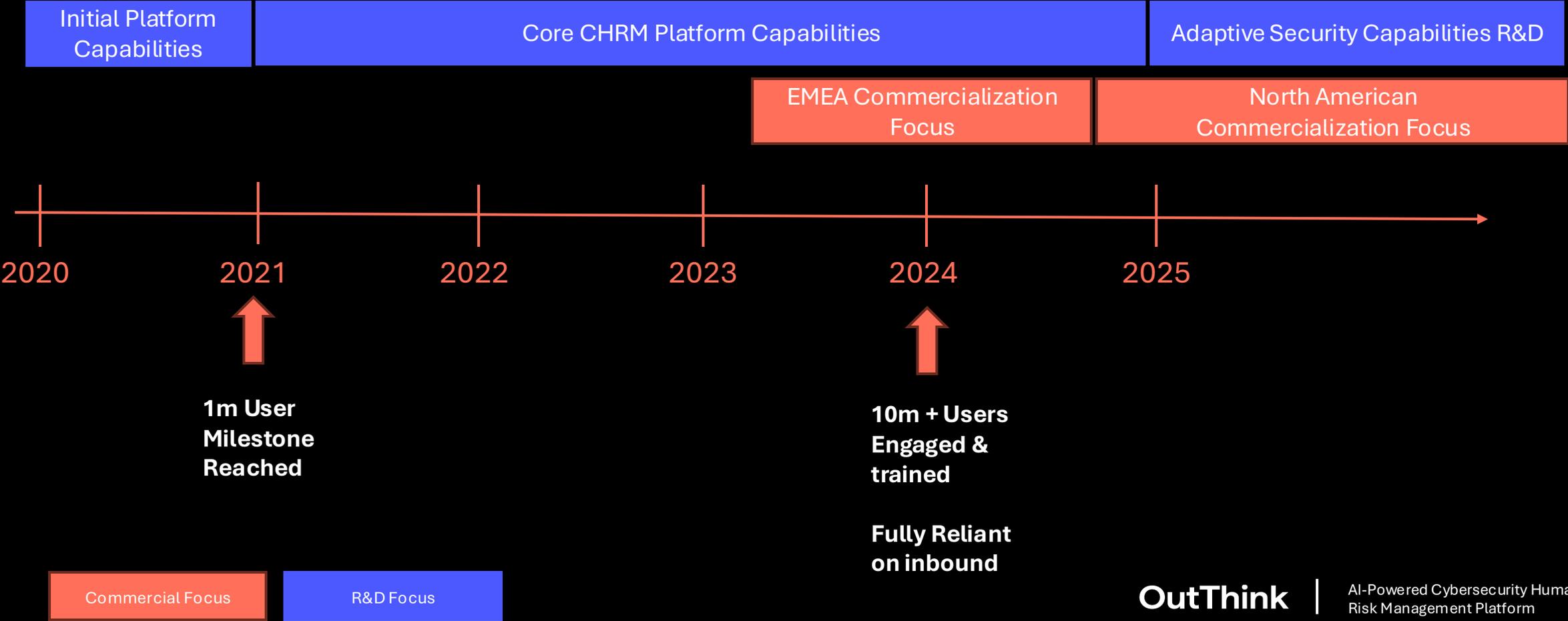
Gartner has recognized OutThink as a Leading Representative Provider in the Security Behaviour and Culture Programs (SBCP) Category.

### **FORRESTER**

Forrester has recognized OutThink as a Leading Vendor in the Human Risk Management Solutions Category.

# The OutThink journey

Founded December 2019, OutThink has been heavily focused on R&D since 2020, with increased commercialization focus in the past 18 months.



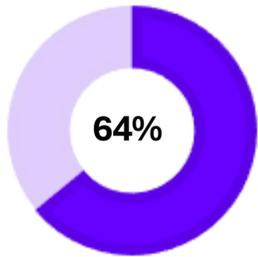
# Enterprise organizations we work with

These global organizations are already tackling their cyber human risk management challenges with OutThink.

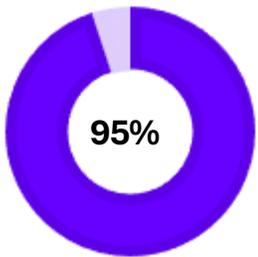


# People Are Vulnerable

## Human Risk Exposure



Employees **Admitted** to Bypassing Security Controls  
**Gartner**



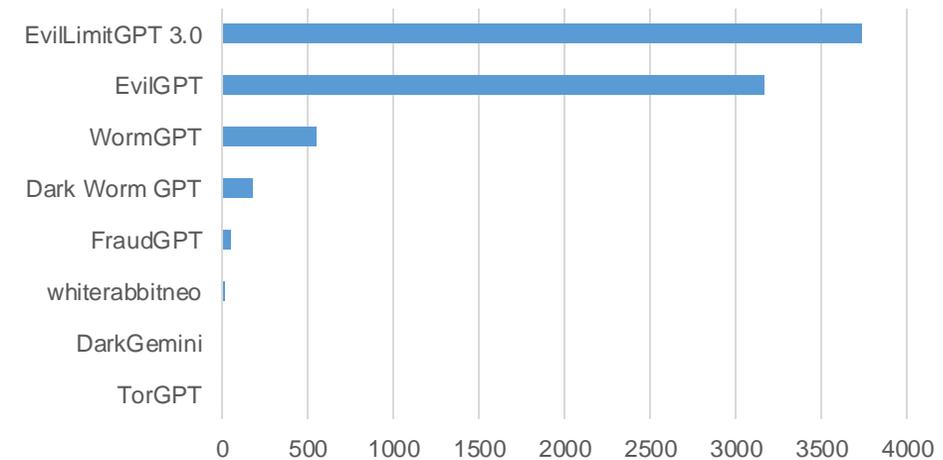
**Knowing** Their Behaviours Increase Risk to the Organization  
**Gartner**

## Hackers are Engaging your Users

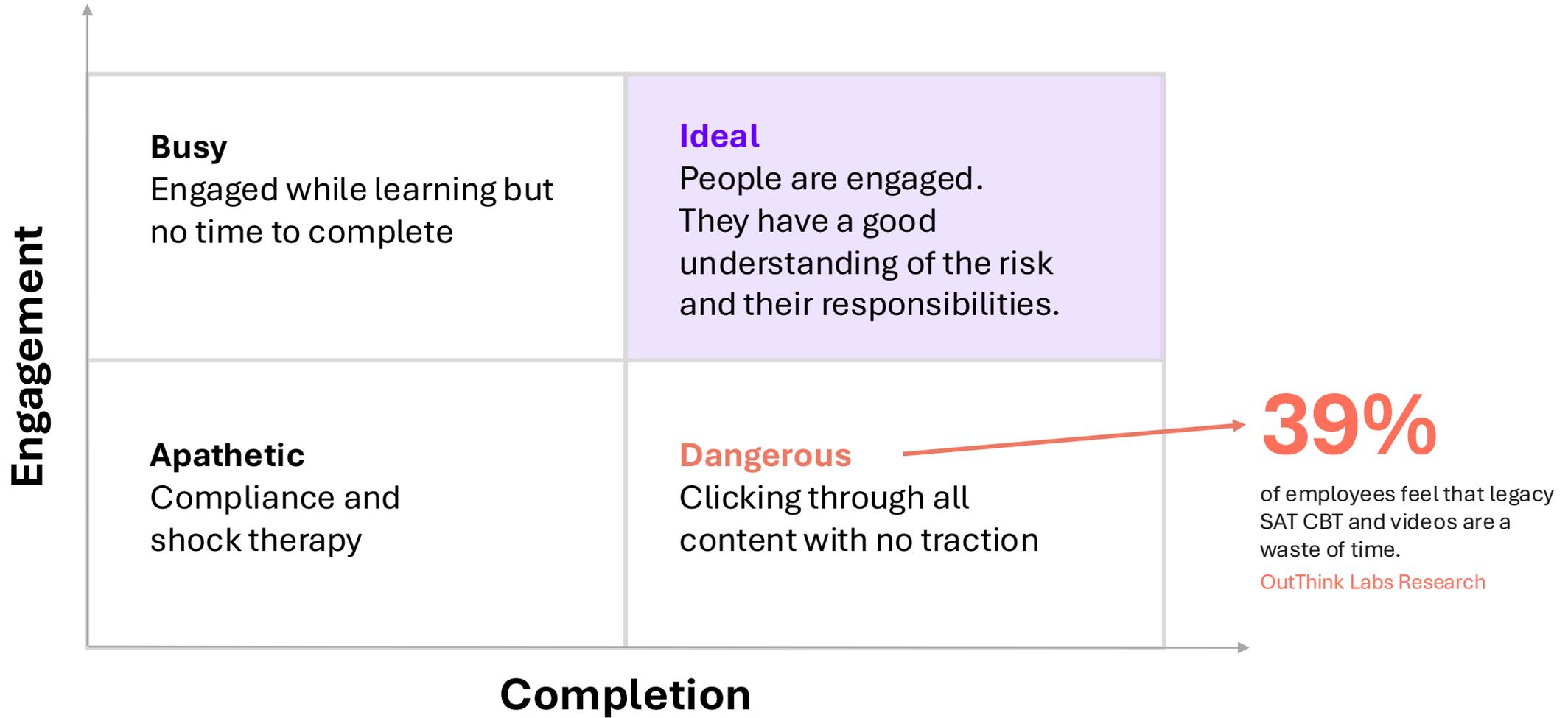
AI is driving a rapid increase in personalised and **engaging** phishing attacks, with **3.4 billion** attacks daily.



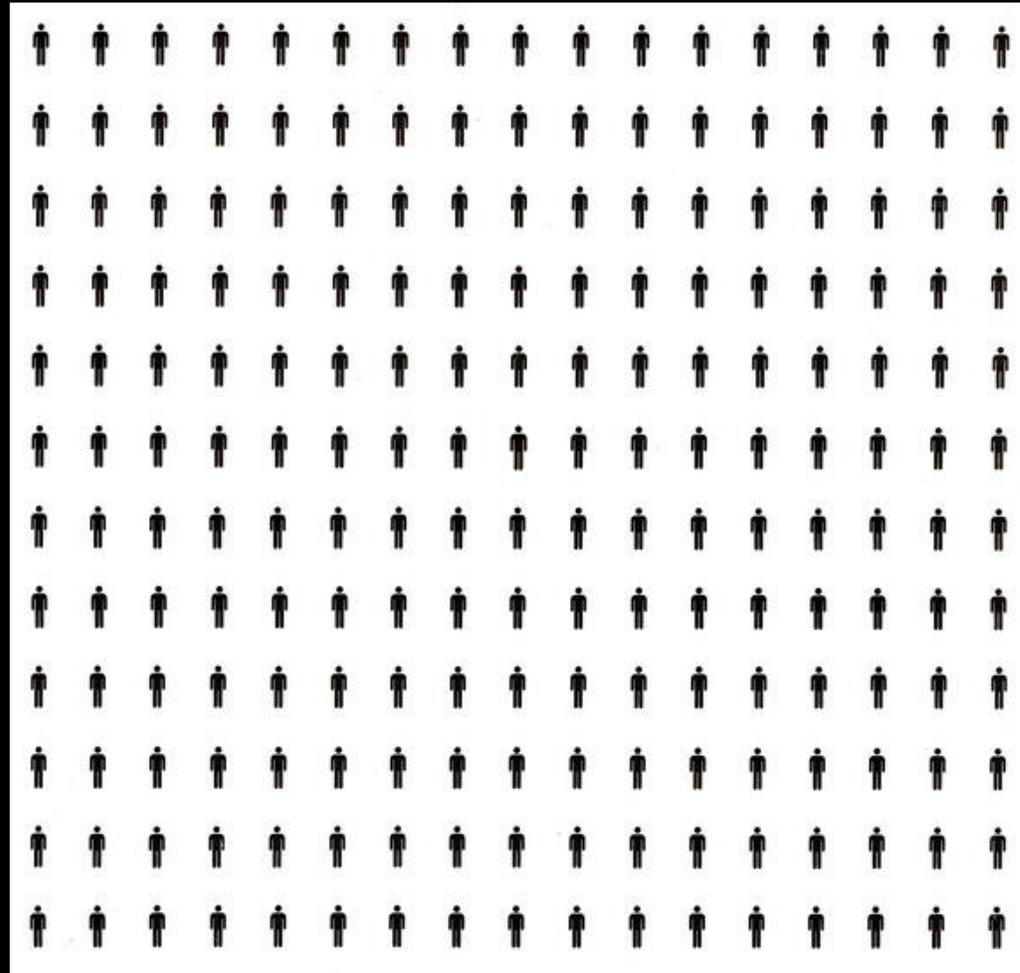
Most Popular Malicious LLMs



# Training Completion ≠ Engagement



# Just Training Completion



Completion Score %

Knowledge Score %

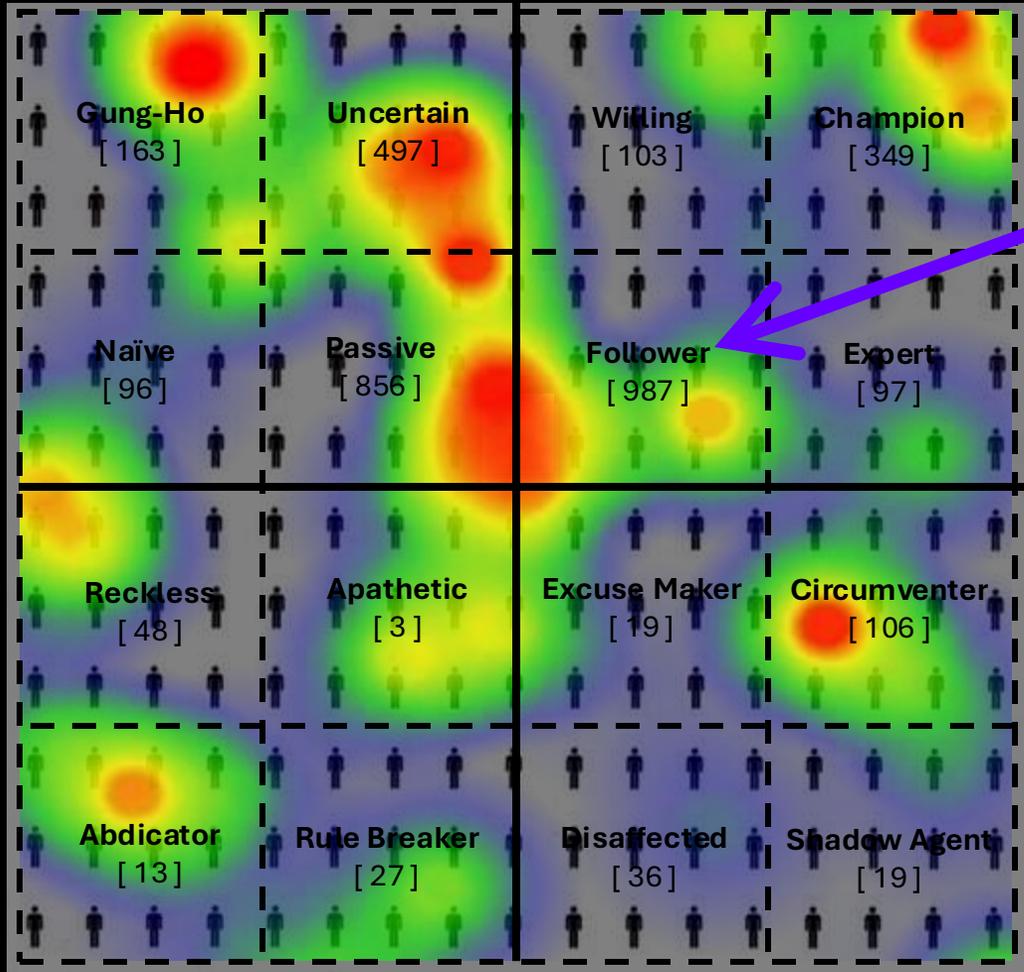
Compliance Check-Box

# No Two Users Are The Same

AS

## 'Affective Security' (AS)

shows the individual's emotional response to security, as represented by the organization's security policy.



RU

## 'Risk Understanding' (RU)

denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.

## ▶ USER SCORECARD

RT

Ricky Toma

17%

High Knowledge

Medium Engagement

Medium Intention To Comply

More ▾

Handles sensitive data

Yes

Psychographic segment

Follower

Knowledge



Intention to comply



Confidence



Compatibility



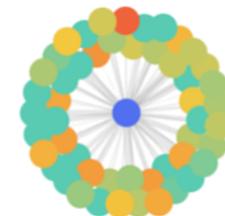
Phishing



Malware



Collaboration network

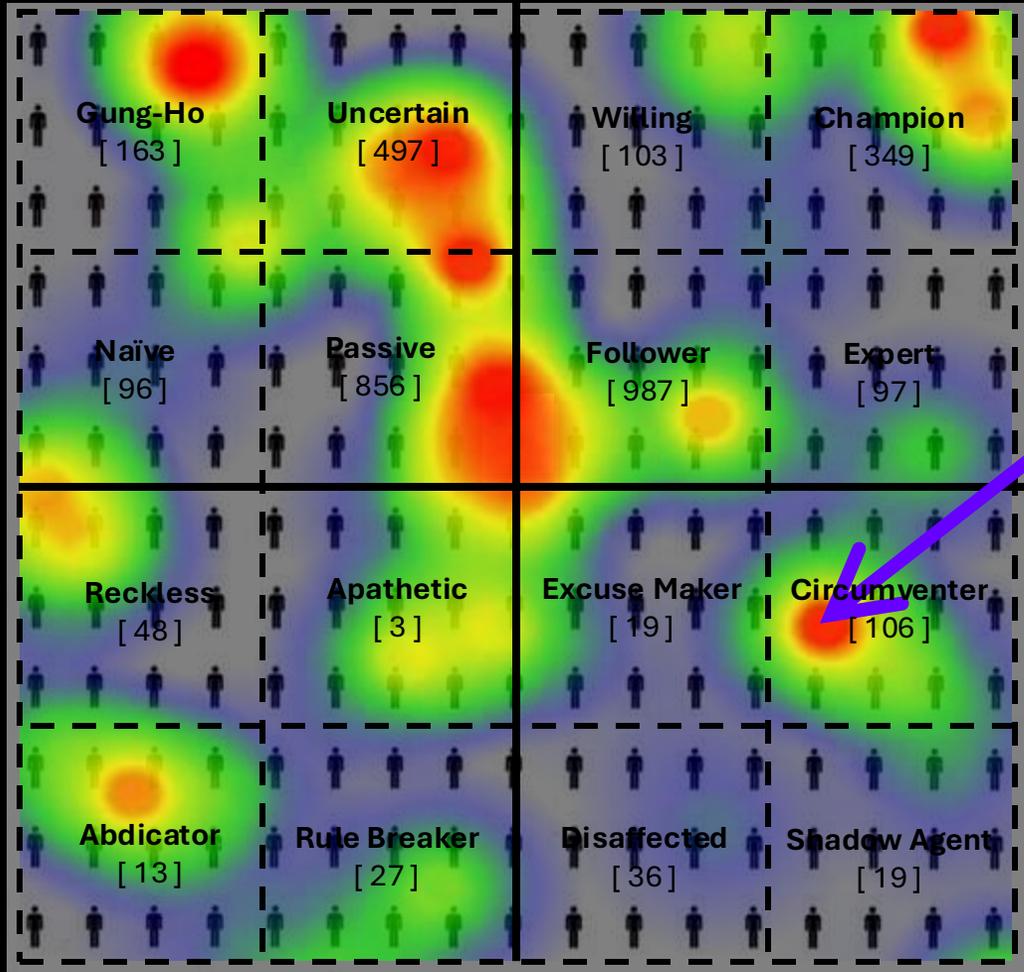


# No Two Users Are The Same

AS

## 'Affective Security' (AS)

shows the individual's emotional response to security, as represented by the organization's security policy.



RU

## 'Risk Understanding' (RU)

denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.

## USER SCORECARD

JN

Jennifer Nistor

87%

Low Knowledge

Medium Engagement

Medium Intention To Comply

More

Handles sensitive data

Yes

Psychographic segment

Circumventer

Knowledge

Intention to comply

Confidence

Compatibility

Phishing

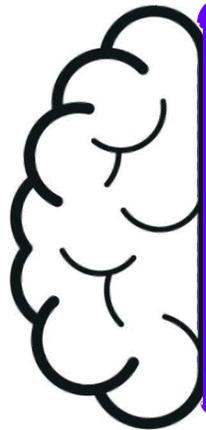
Malware

Collaboration network



# Human Risk Management (HRM) Explained

## Adaptive Training



1

Effectively  
Train & ENGAGE  
Your People

2

Build  
Phishing Resilience

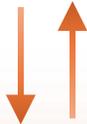
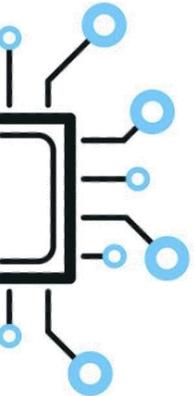
## Adaptive Security

3

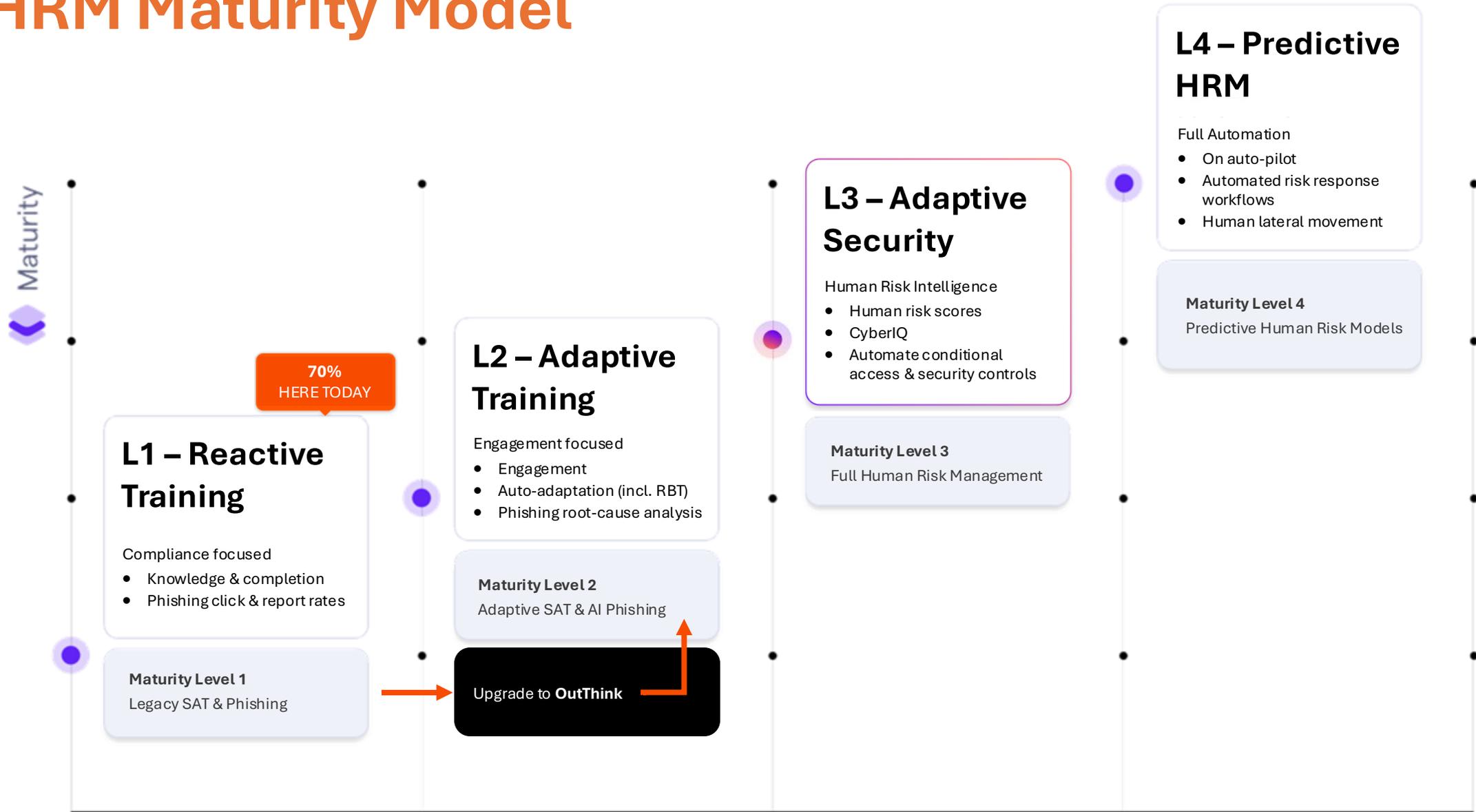
Automate  
Conditional Access  
& Security Controls

4

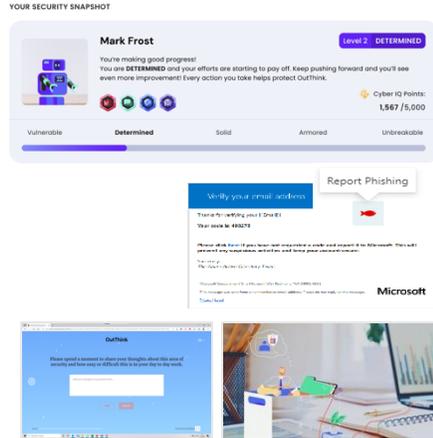
Build Effective &  
Sustainable Security



# HRM Maturity Model



# The How - Cybersecurity Human Risk Management



 CyberIQ

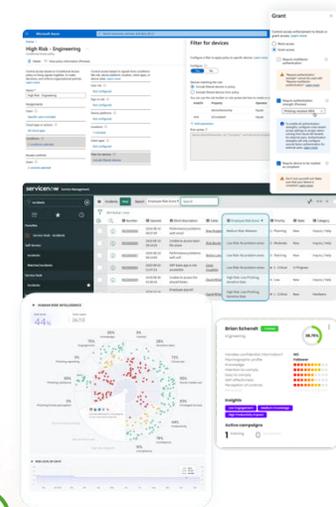
 AI Phishing Simulator

 Adaptive SAT

 API Integrations – Automate Conditional Access

 API Integrations – Give Teams Intel On Human Risk

 Human Risk Intelligence



# Build Effective & Sustainable Security

servicenow Service Management System Administrator

Incidents New Search  Search

All > Active = true

Number	Opened	Short description	Caller	Employee Risk Score	Priority	State	Category
INC0000058	2016-08-10 09:37:45	Performance problems with email	Bow Ruggel	Medium Risk: Malware	5 - Planning	New	Inquiry / Help
INC0000059	2016-08-10 09:14:29	Unable to access team file share	Rick Berzle	Low Risk: No problem areas	3 - Moderate	New	Inquiry / Help
INC0000057	2016-08-10 09:14:59	Performance problems with wifi	Bertie Luby	Low Risk: No problem areas	5 - Planning	New	Inquiry / Help
INC0000055	2020-09-03 21:47:23	SAP Sales app is not accessible	Carol Coughlin	Low Risk: No problem areas	1 - Critical	In Progress	
INC0009009	2018-08-30 01:06:16	Unable to access the shared folder.	David Miller	High Risk: Low Phishing, Sensitive Data	4 - Low	New	Inquiry / Help
INC0007001	2018-10-16 22:47:10	Employee payroll application server is down.	David Miller	High Risk: Low Phishing, Sensitive Data	1 - Critical	New	Hardware

## Feed Human Risk Intelligence into:

- Ticketing / SOC system to give teams intel to make better decisions – access grants, application download approvals, policy exceptions or triaging incidents.
- GRC platform so that security risk assessments cover all (people, process, technology) vulnerabilities

## Security / risk analyst reviews Human Risk Intelligence to:

- Drive down human risk level, not just phishing / training KPIs.
- Conduct root cause analysis and take/raise risk mitigation actions (tech & process adjustments / improvements, policy exceptions).
- Identify high human risk exposure in areas where people are more likely to bypass security controls (low intention to comply + high friction).



# Automate Conditional Access & Security Controls



**JN** Jennifer Nistor  
Manager: Alain Perrier  
Title: Webmaster Location: AMER Department: Webadmins

**87%** 3RD-PARTY POLICY GROUPS

Authentication: **DEFAULT** [check] [no]

DLP: Default [edit] Email: Default [edit] Endpoint: Default [edit]

Web Gateway: Standard [edit]

**High Risk Policy** [Active] [Edit]

Description: High Risk Policy

Assigned to groups:  High Risk

**Authentication Providers**

Applies to: Okta

**Password Settings**

Minimum length: 8 characters

Complexity requirements:

- Lower case letter
- Upper case letter
- Number (0-9)
- Symbol (e.g., !@#\$%^&\*)
- Does not contain part of username
- Does not contain first name
- Does not contain last name

Common password check  Restrict use of common passwords

**Automatically assign higher control requirements (add users to strict / high risk groups).**

Example:

Authentication - Okta

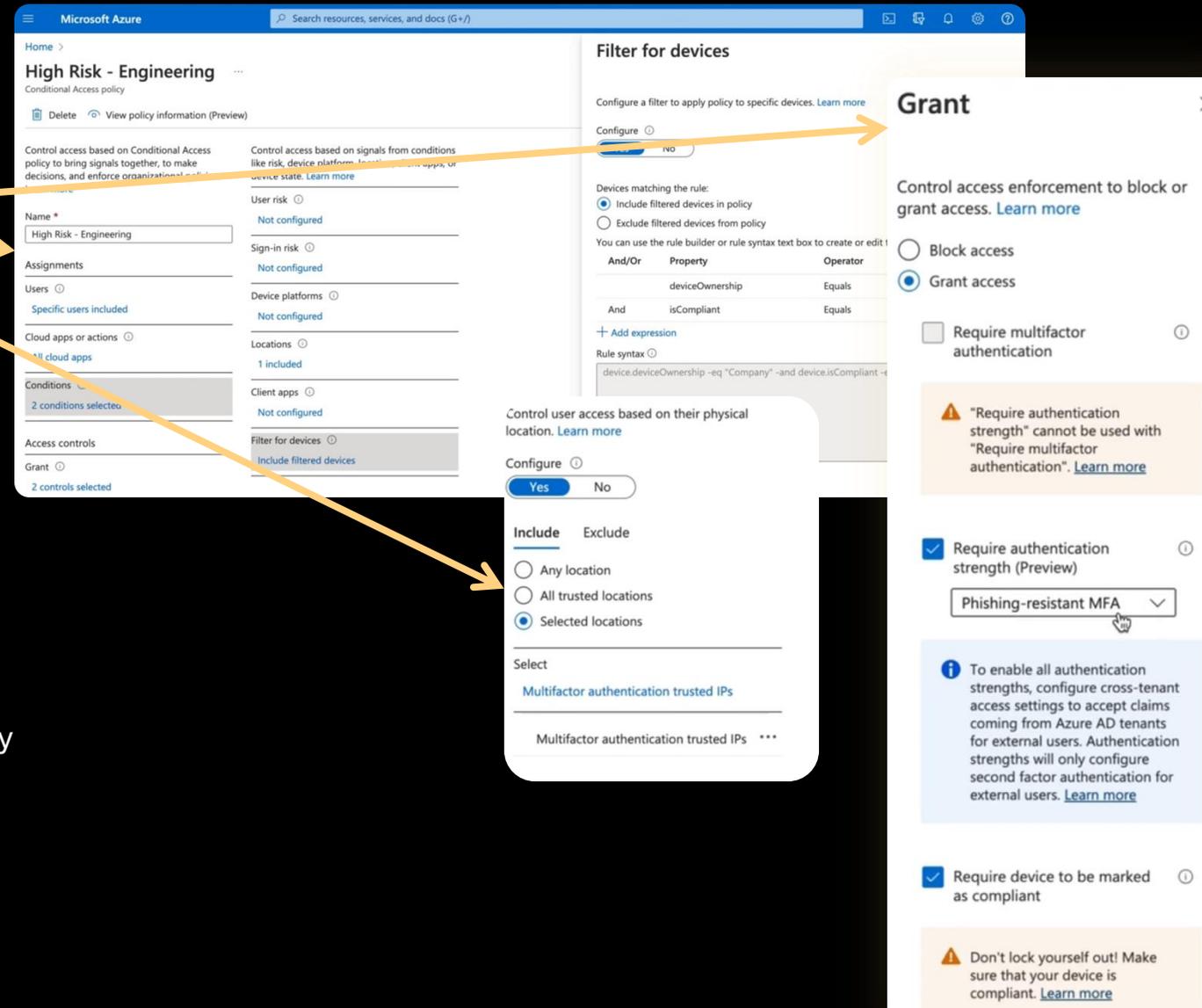
DLP – MS Purview

Email - Proofpoint

Endpoint - Jamf

Web Gateway - Zscaler

# Automate Conditional Access & Security Controls



Because of the overall risk (exceeded the 75% risk threshold) and being an Engineer, the user has been added to AAD (Entra ID) high-risk group automatically.

This assigns the user stricter conditional access policy:

- Will need MFA everywhere
- Will need to come in from a trusted location
- Will need to use a compliant device (meets company's security policies)

Strong additional authentication requirements blocking attacker from reusing stolen credentials or legacy MFA bypasses

# The How - Adaptive Training (1. & 2.)



**YOUR SECURITY SNAPSHOT**

**Mark Frost** Level 2 DETERMINED

You're making good progress! You are **DETERMINED** and your efforts are starting to pay off. Keep pushing forward and you'll see even more improvement! Every action you take helps protect Outlook.

Cyber IQ Points: 1,567 / 5,000

Vulnerable **Determined** Solid Armored Unbreakable

Verify your email address Report Phishing

Outlook

 CyberIQ

 AI Phishing Simulator

 Adaptive SAT

 API Integrations – Automate Conditional Access

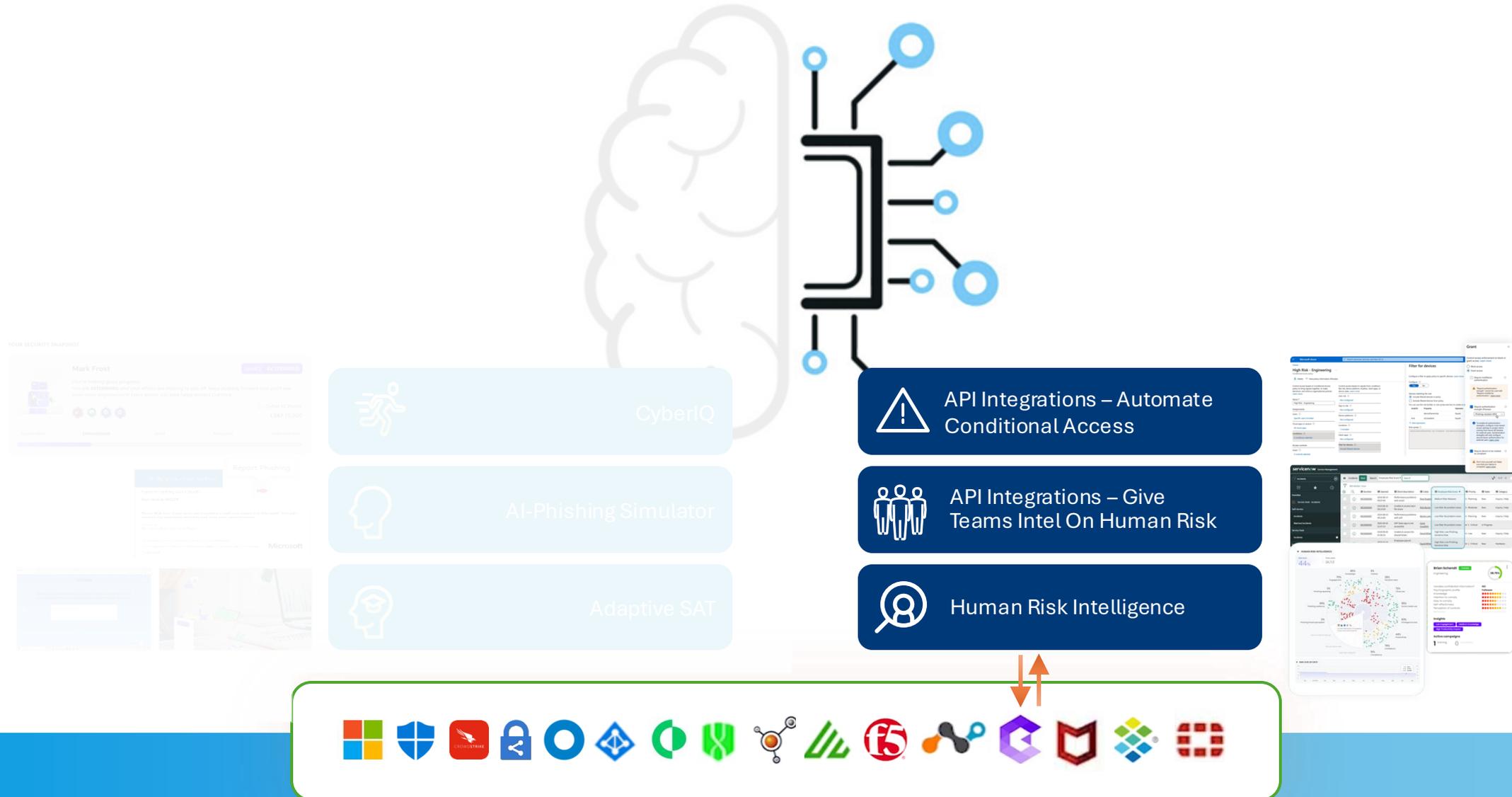
 API Integrations – Give Teams Intel On Human Risk

 Human Risk Intelligence

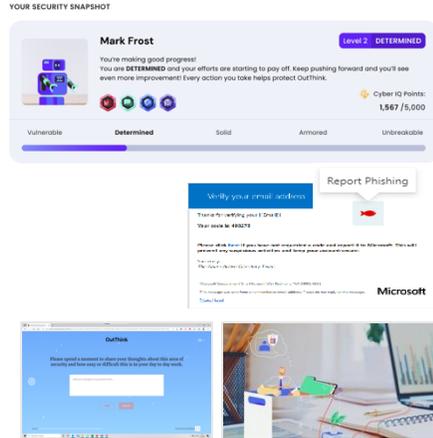




# The How - Adaptive Security (3. & 4.)



# The How - Cybersecurity Human Risk Management



 CyberIQ

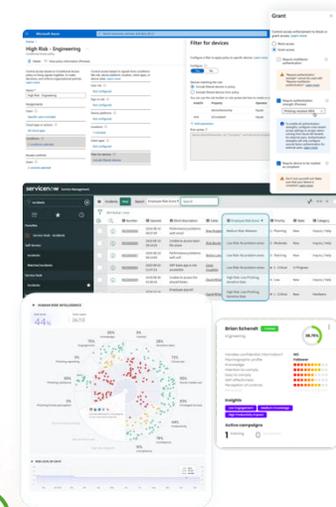
 AI Phishing Simulator

 Adaptive SAT

 API Integrations – Automate Conditional Access

 API Integrations – Give Teams Intel On Human Risk

 Human Risk Intelligence



# Traditional Phishing Simulations

## Who?...

- Phishing simulations
- Click / Report

Users who clicked



Generic Phishing Training



Why?...  
is this happening

# AI-Powered Phishing Simulations

## Who?...

- Phishing simulations
- Click / Report

Users who clicked

## Why?... is this happening

- Automated (ML/NLP) root cause analysis. Why did user X click?
- OutThink understands the reason behind the click, for each user - their psychology, vulnerability, etc.



The reason behind the click

- User simply doesn't care
- Failed to assess bad URL
- Failed to assess infected attachment
- Failed to assess spoofed webpage
- Psychographic segment Apathetic
- Psychographic segment Naïve
- Failed to Urgency / Curiosity / Authority / Reward / Loss



Targeted Training

