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

Gartner

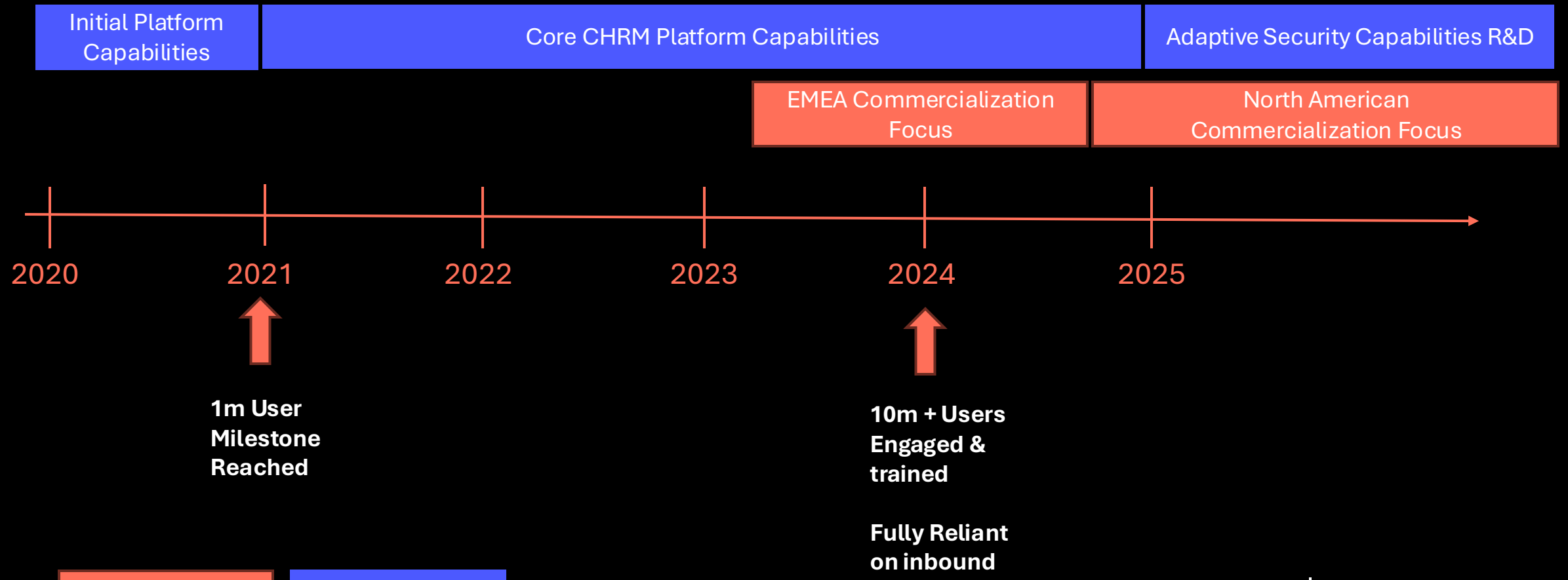
Gartner has recognized OutThink as a Leading Representative Provider in the Security Behaviour and Culture Programs (SBCP) Category.

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.

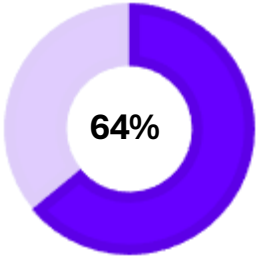


Enterprise organizations we work with

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

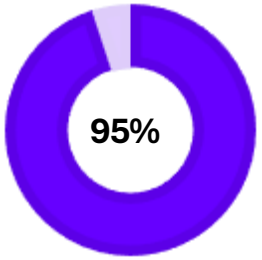
People Are Vulnerable

Human Risk Exposure



Employees **Admitted** to Bypassing Security Controls

Gartner

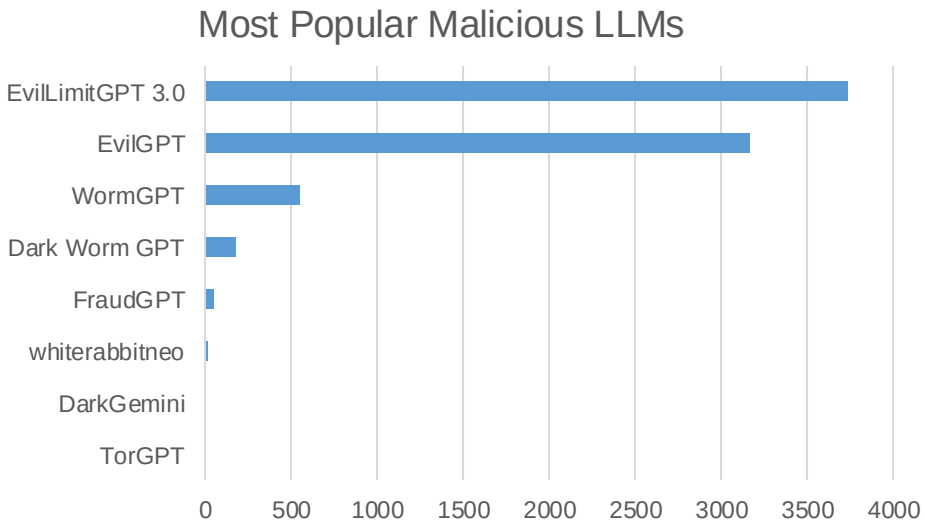


Knowing Their Behaviours Increase Risk to the Organization

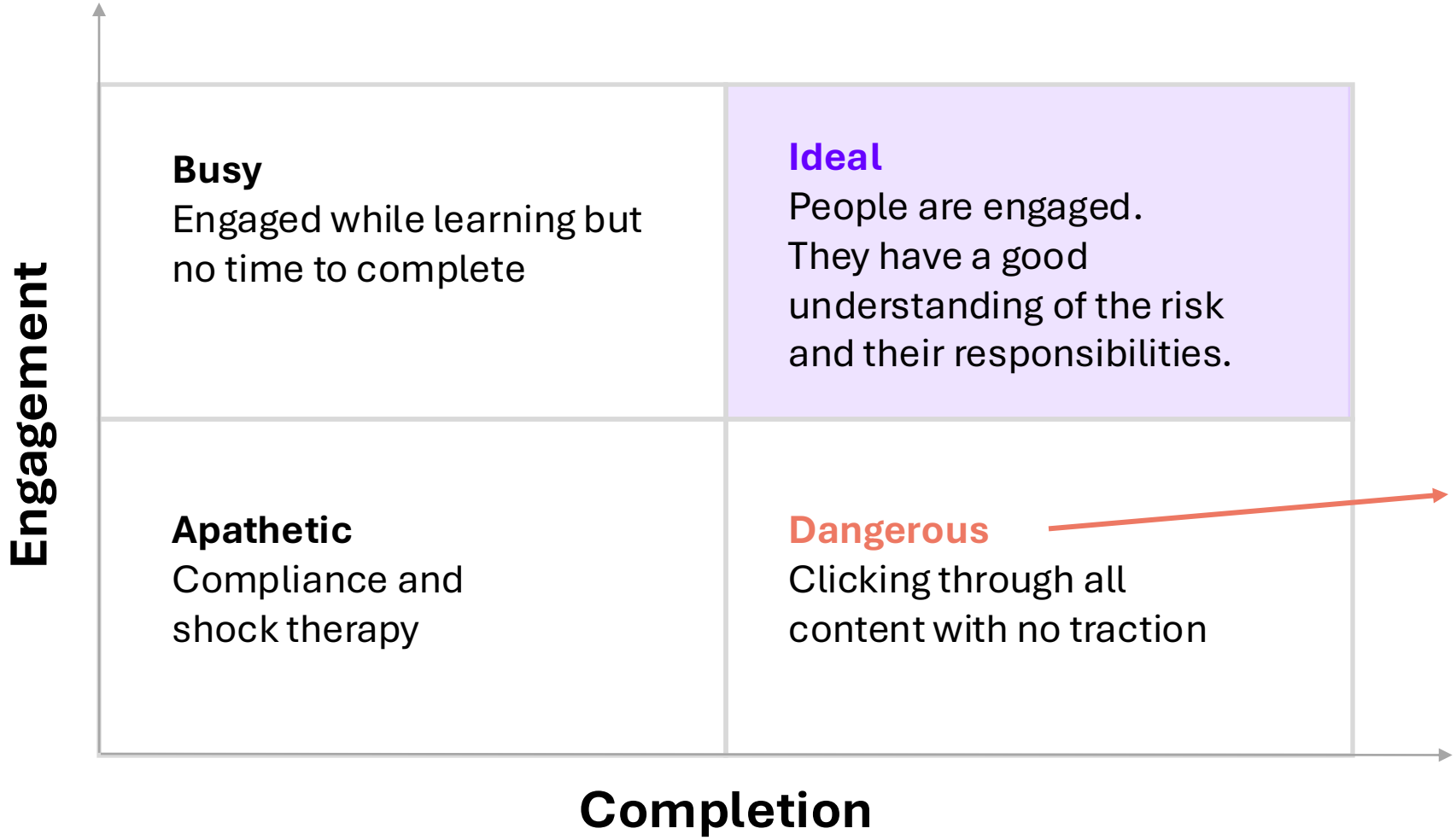
Gartner

Hackers are Engaging your Users

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



Training Completion ≠ Engagement

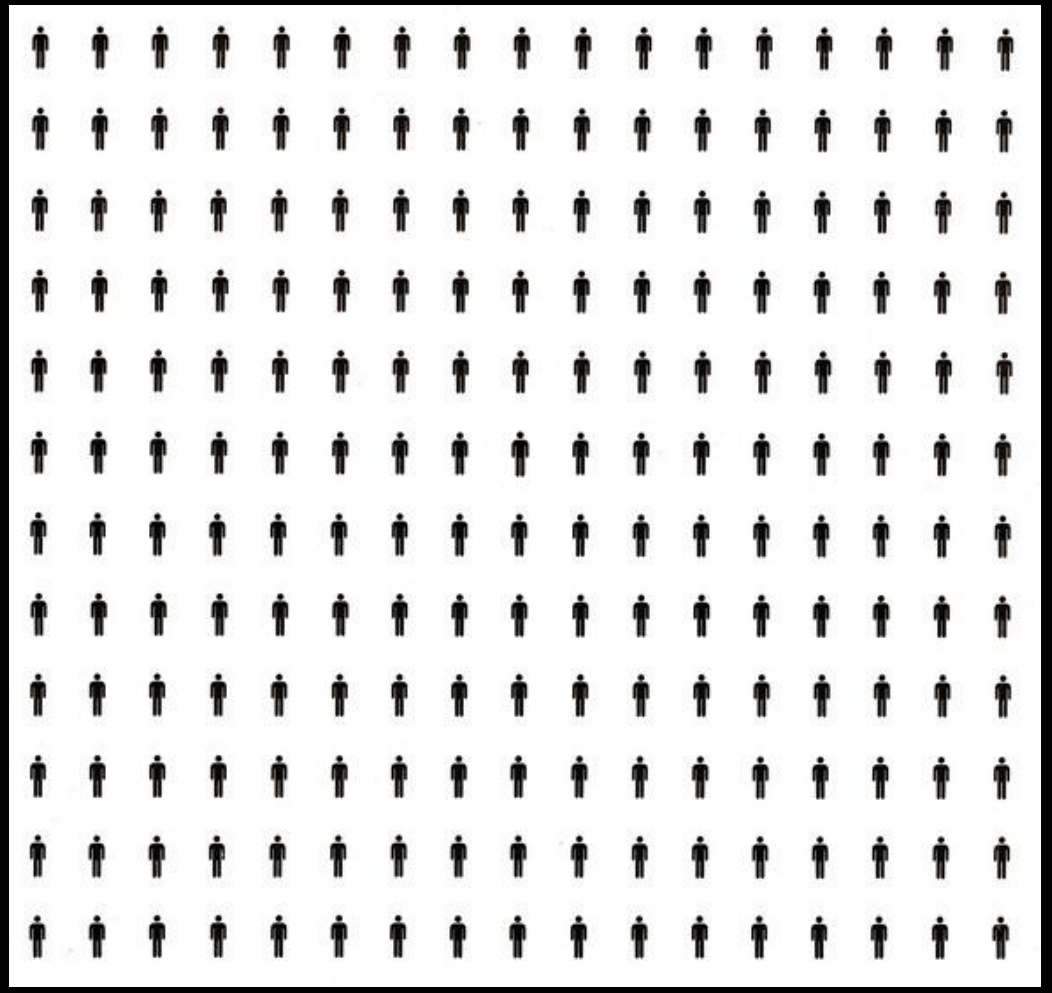


39%

of employees feel that legacy SAT CBT and videos are a waste of time.

OutThink Labs Research

Just Training Completion



Completion Score %

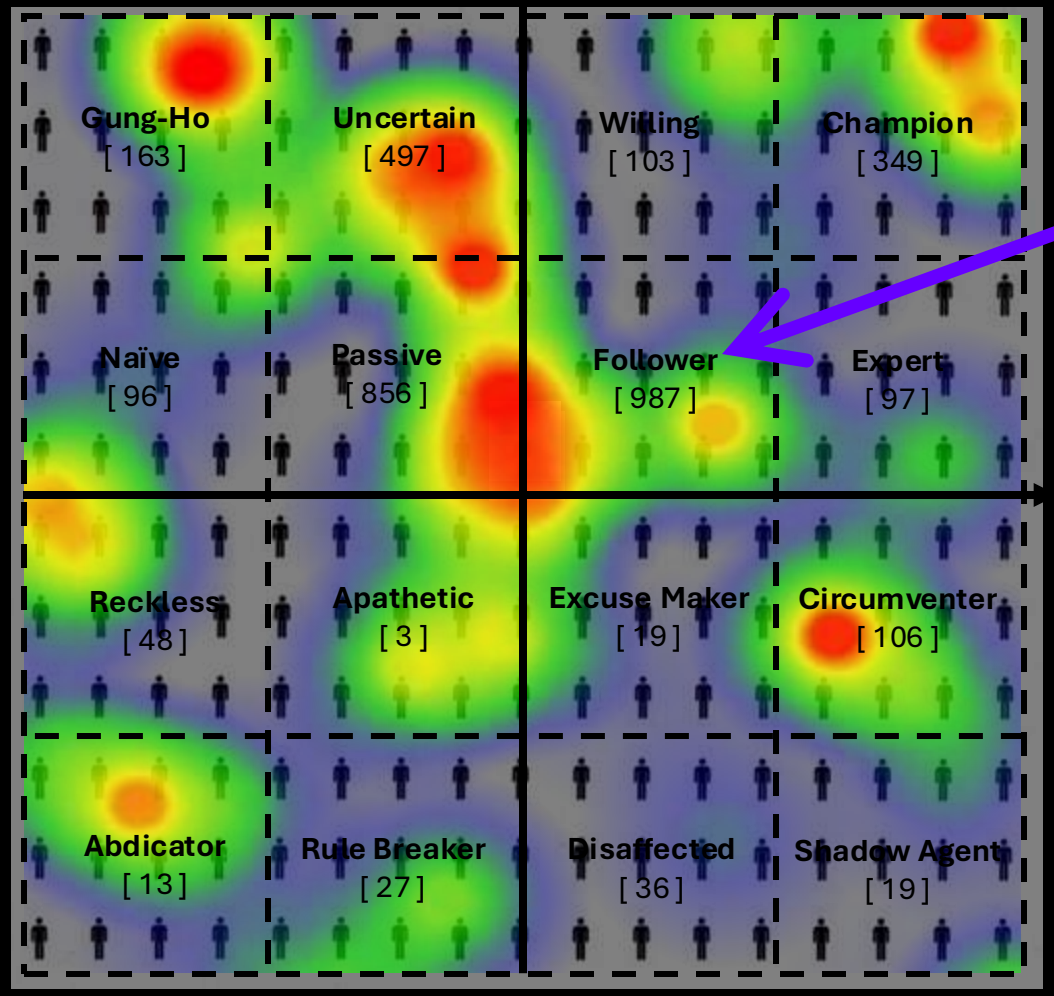
Knowledge Score %

Compliance Check-Box

No Two Users Are The Same

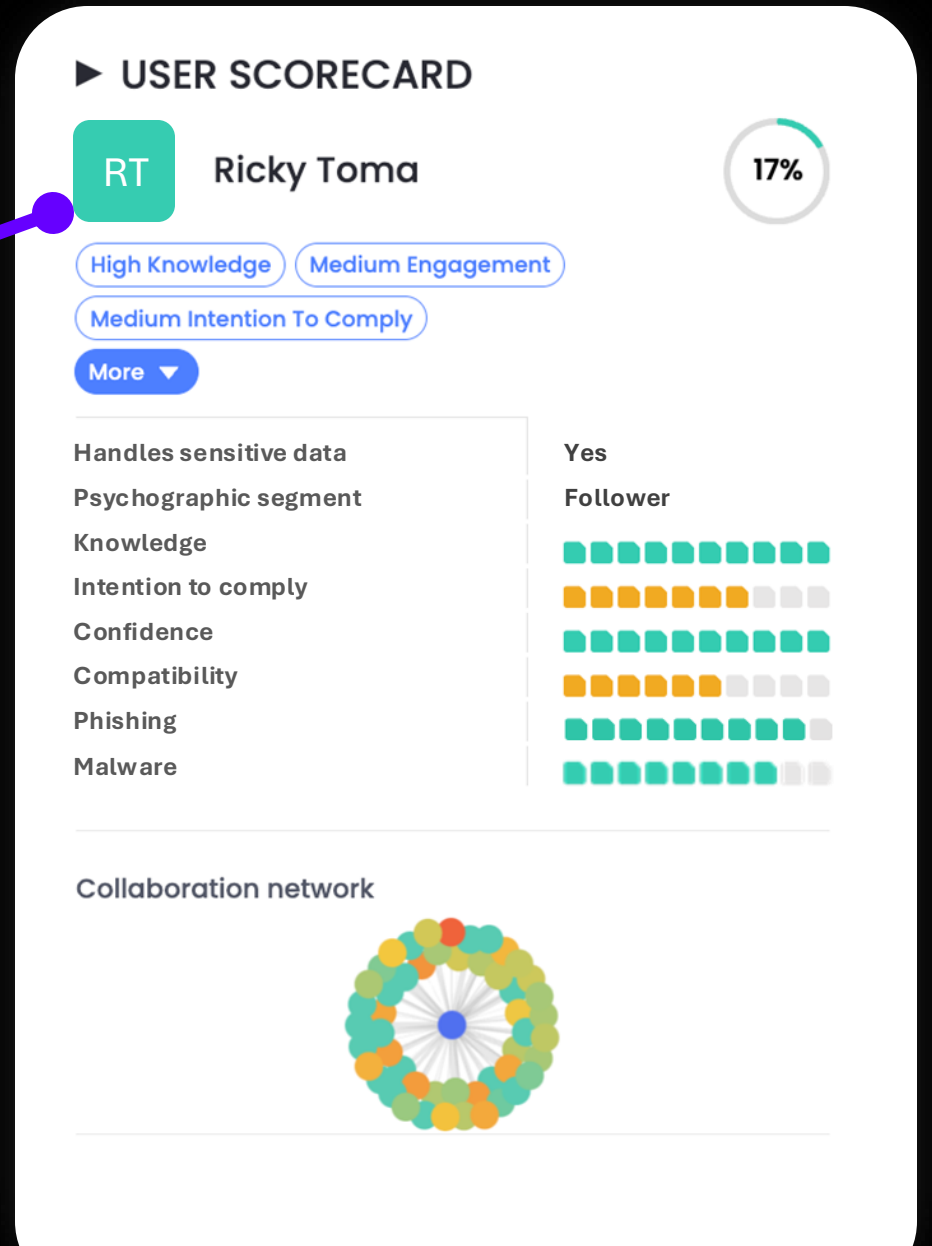
AS

***'Affective Security'* (AS)**
shows the individual's emotional response to security, as represented by the organization's security policy.



RU

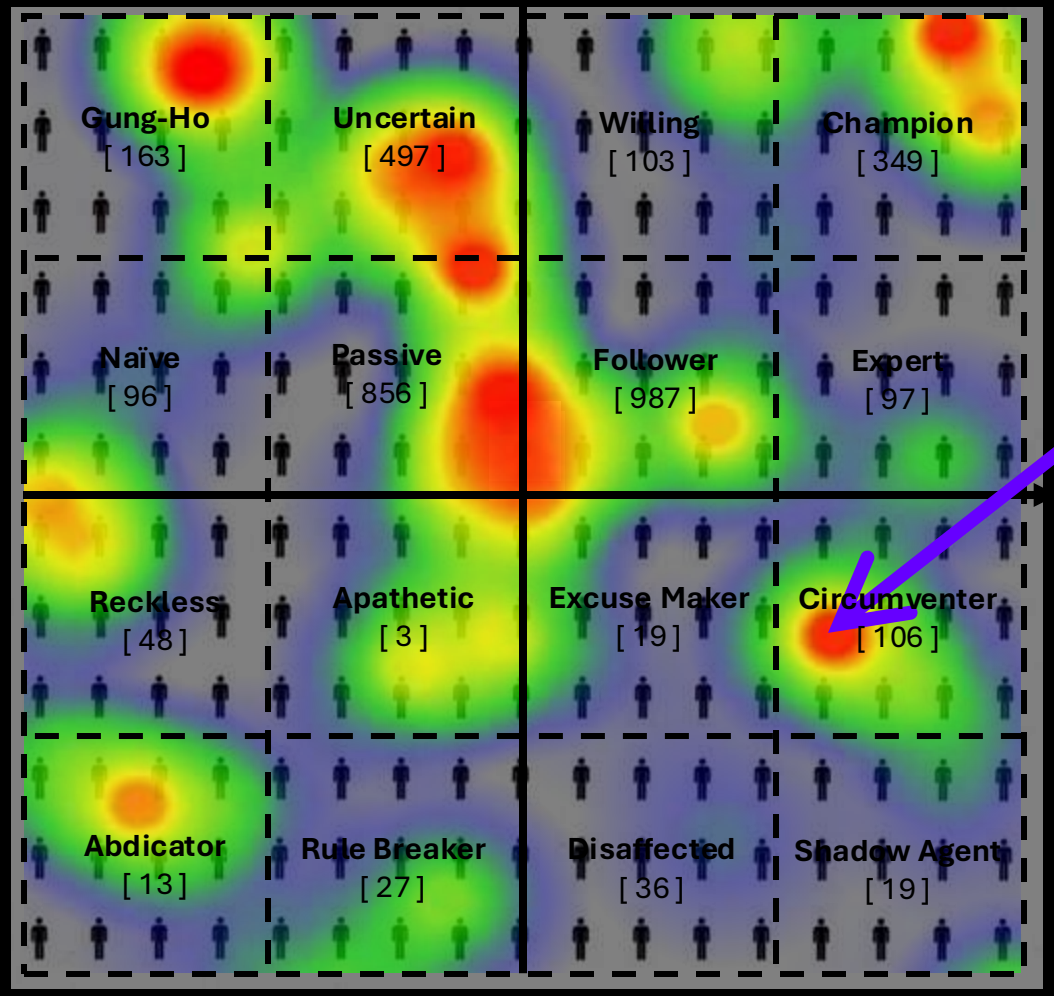
***'Risk Understanding'* (RU)**
denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.



No Two Users Are The Same

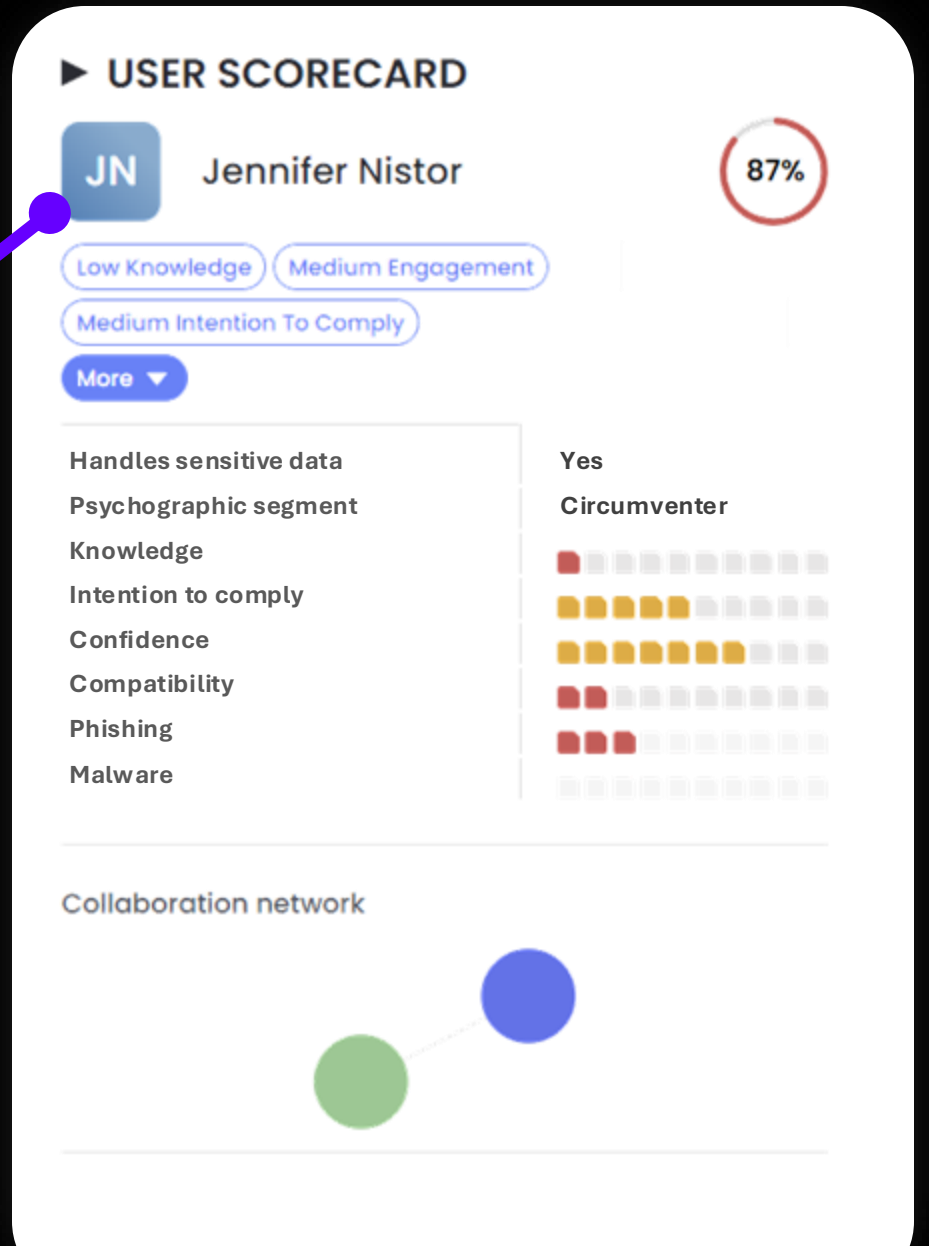
AS

***'Affective Security'* (AS)**
shows the individual's emotional response to security, as represented by the organization's security policy.



RU

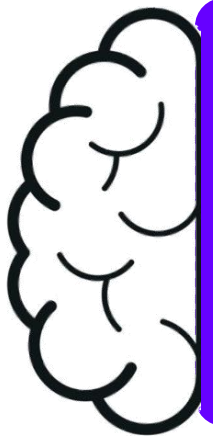
***'Risk Understanding'* (RU)**
denotes the individual's ability to accurately perceive the existence and severity of the risks associated with their actions, as well as those they observe in the surrounding environment.



Human Risk Management (HRM) Explained

Adaptive Training

Adaptive Security



1

Effectively
Train & ENGAGE
Your People

2

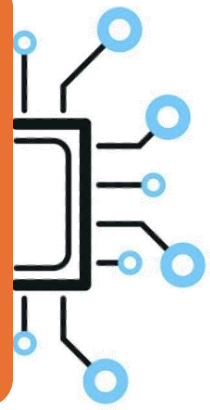
Build
Phishing Resilience

3

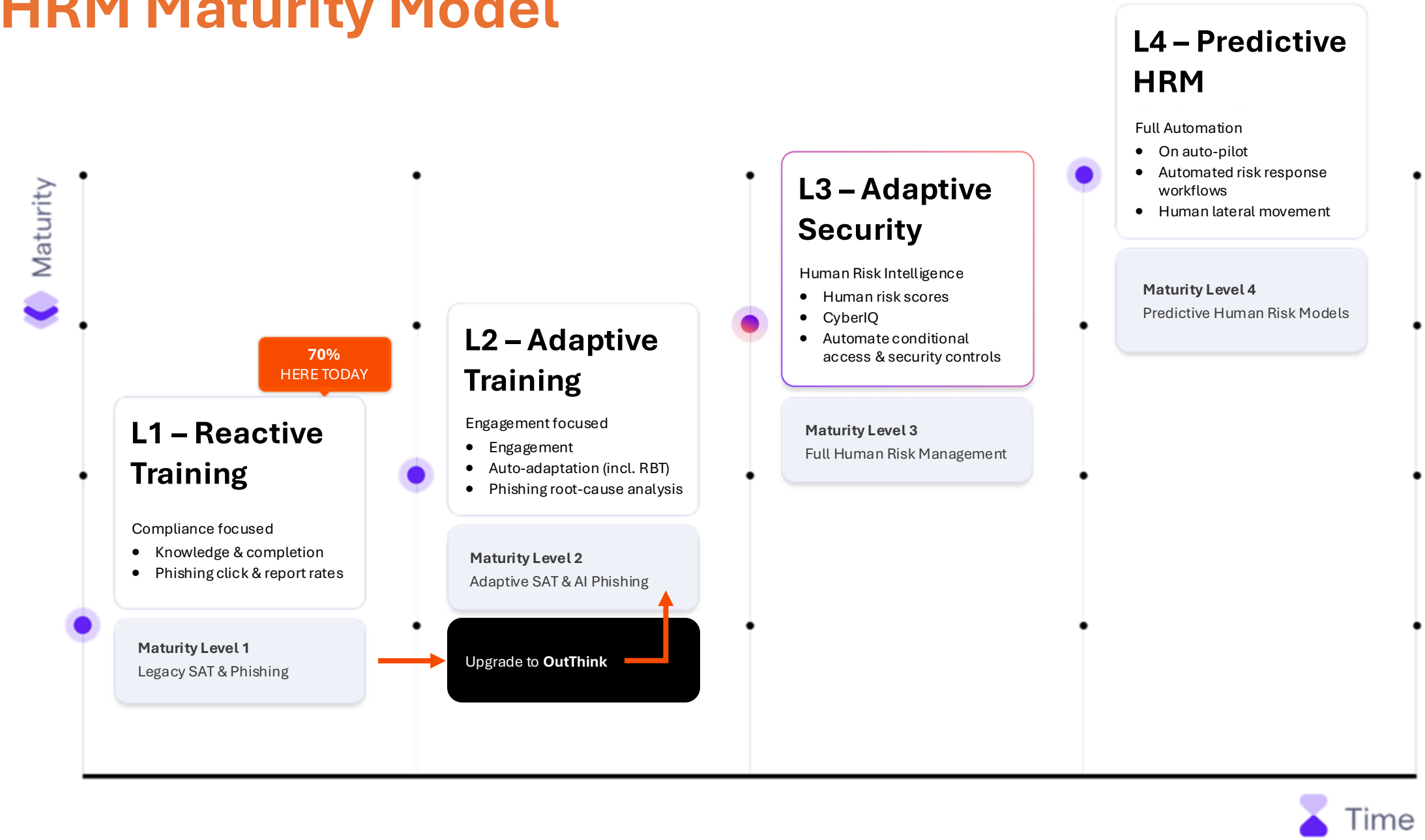
Automate
Conditional Access
& Security Controls

4

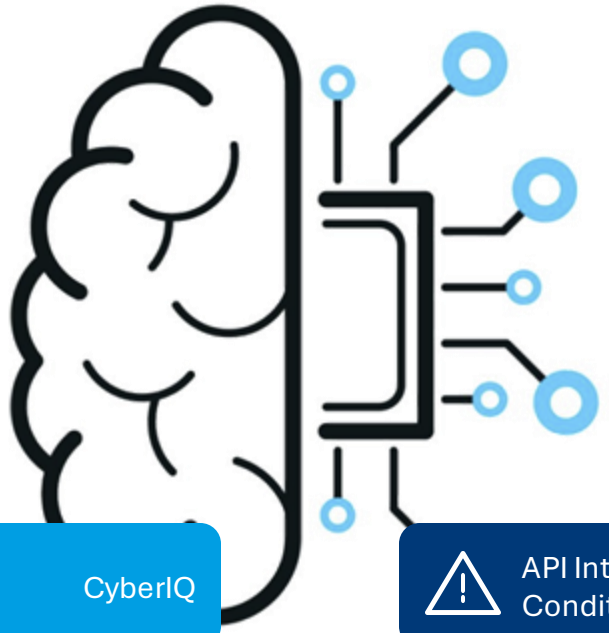
Build Effective &
Sustainable Security

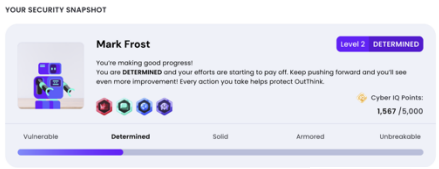


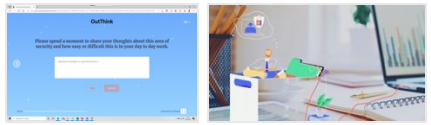
HRM Maturity Model



The How - Cybersecurity Human Risk Management







CyberIQ

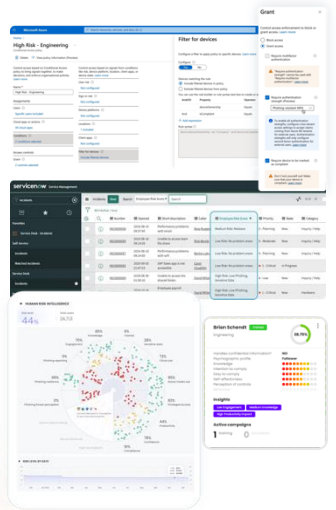
AI Phishing Simulator

Adaptive SAT

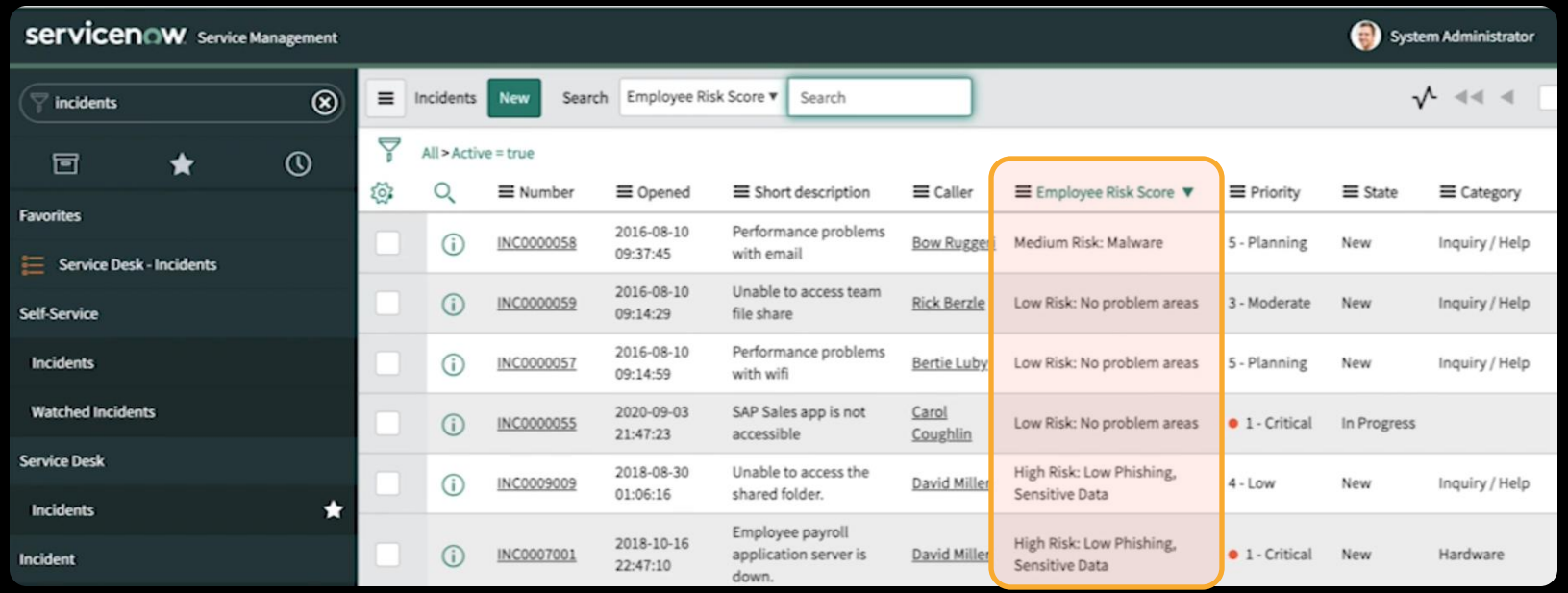
API Integrations – Automate Conditional Access

API Integrations – Give Teams Intel On Human Risk

Human Risk Intelligence



Build Effective & Sustainable Security



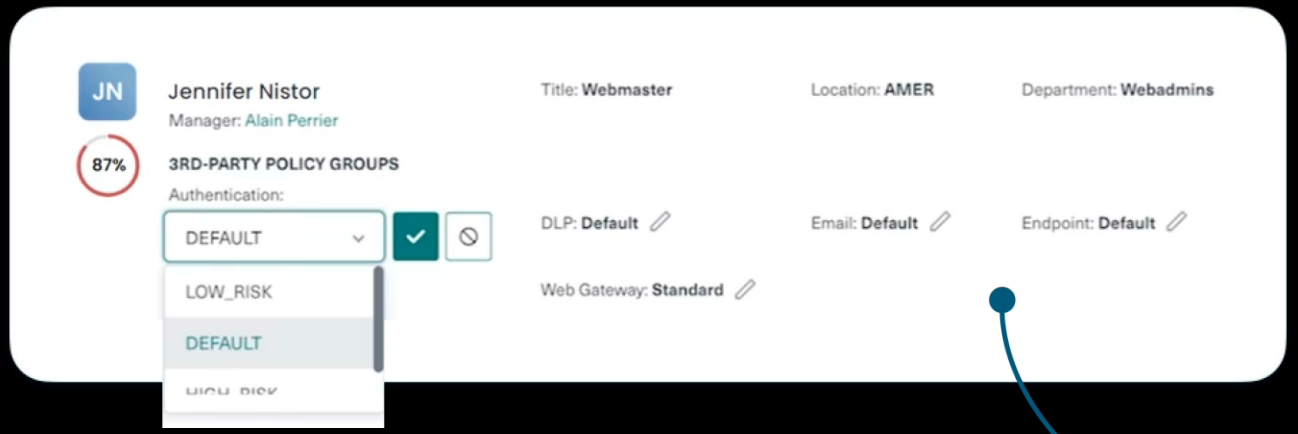
Feed Human Risk Intelligence into:

- 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

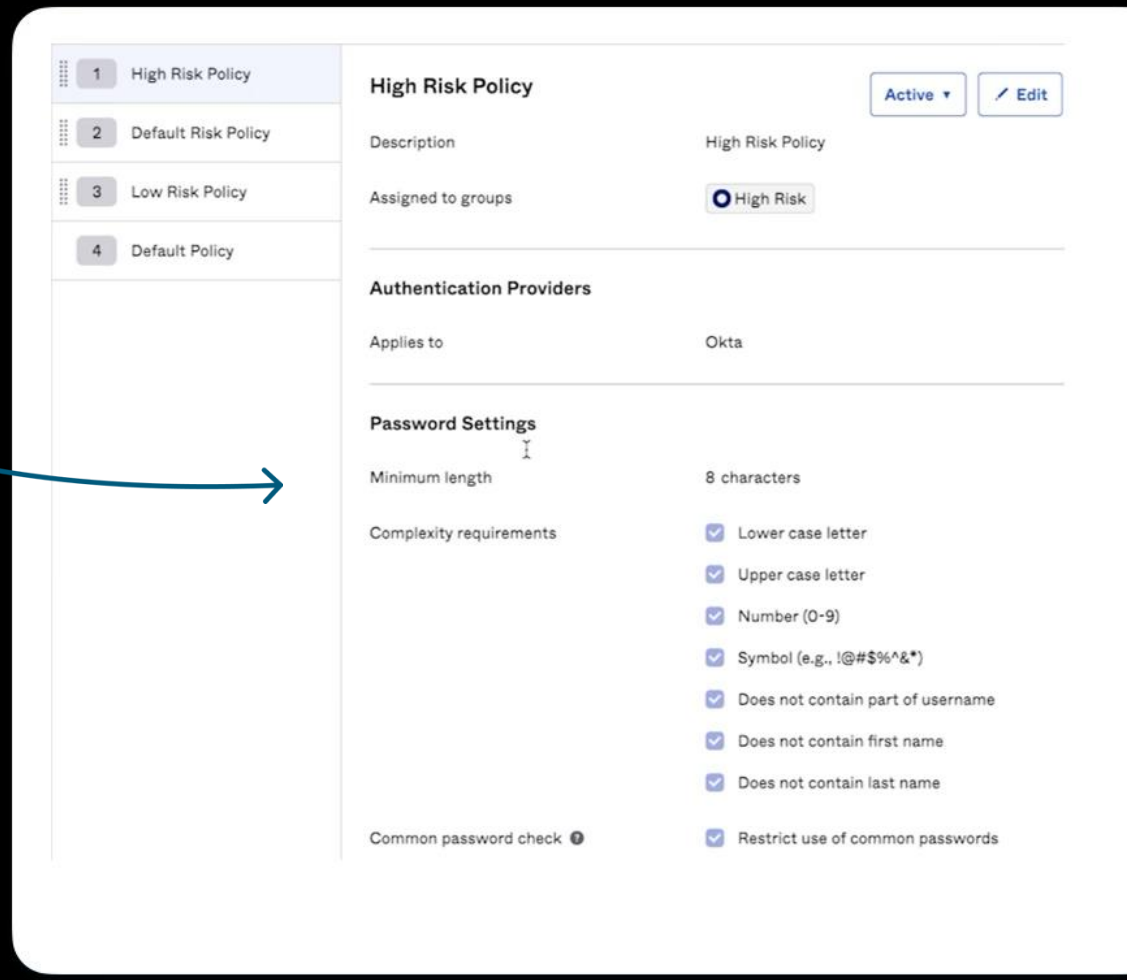
Security / risk analyst reviews Human Risk Intelligence to:

- 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



okta



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

Example:

Authentication - Okta

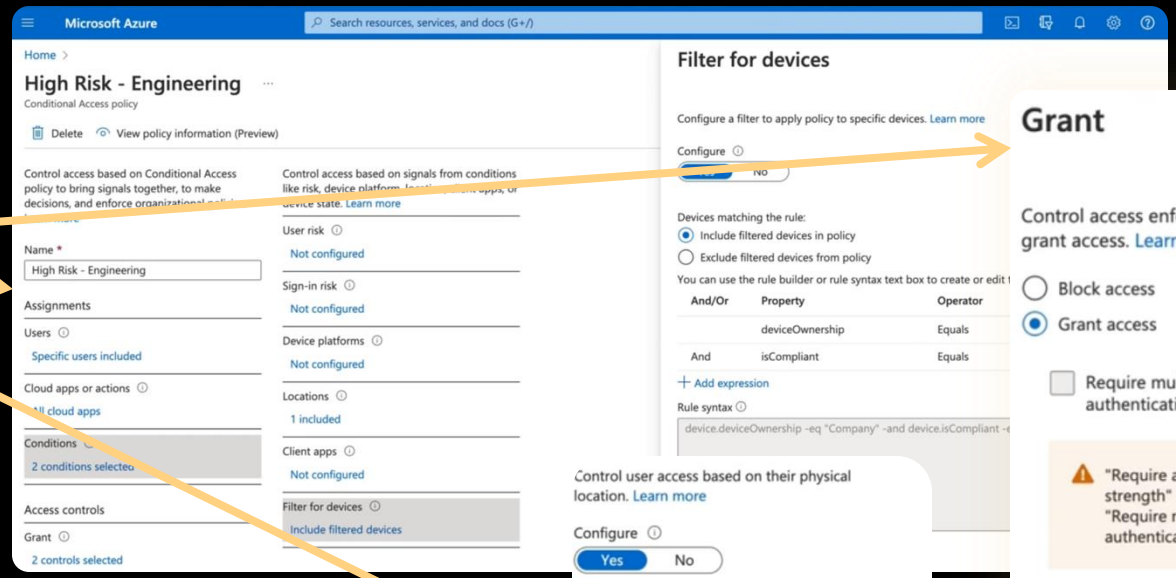
DLP – MS Purview

Email - Proofpoint

Endpoint - Jamf

Web Gateway - Zscaler

Automate Conditional Access & Security Controls



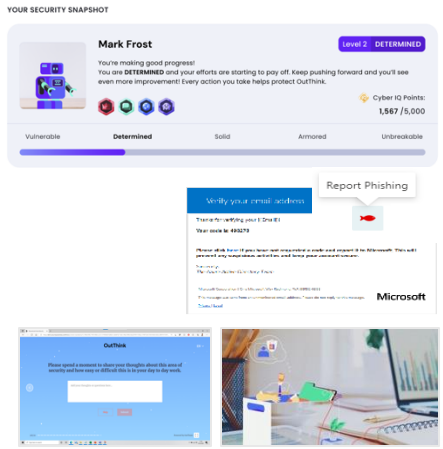
Because of the overall risk (exceeded the 75% risk threshold) and being an Engineer, the user has been added to AAD (Entra ID) high-risk group automatically.

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.)



CyberIQ

AI Phishing Simulator

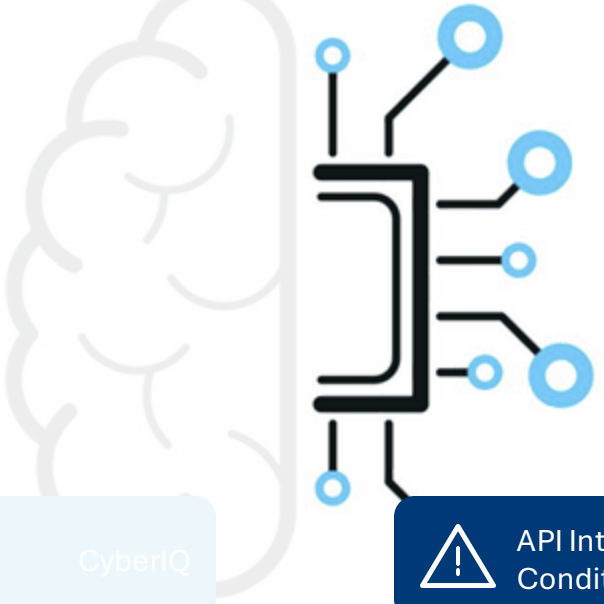
Adaptive SAT

API Integrations – Automate Conditional Access

API Integrations – Give Teams Intel On Human Risk

Human Risk Intelligence

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



CyberIQ

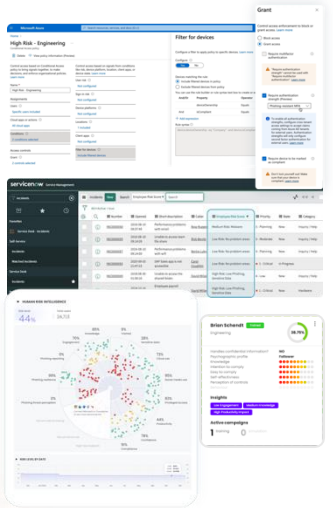
AI-Phishing Simulator

Adaptive SAT

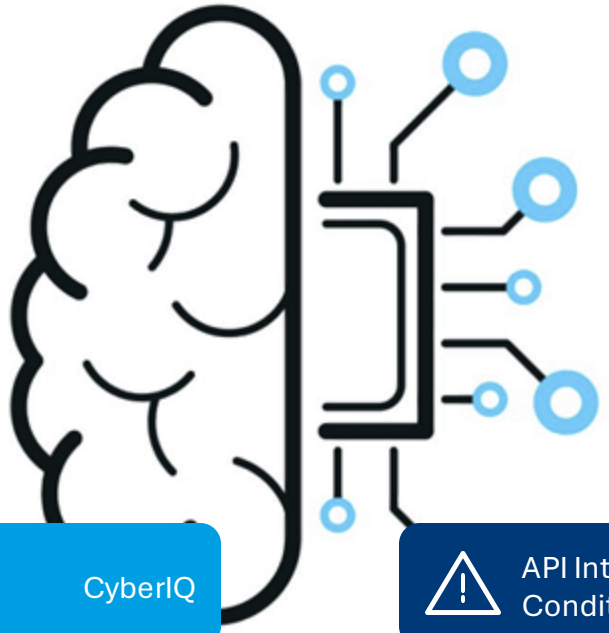
API Integrations – Automate Conditional Access

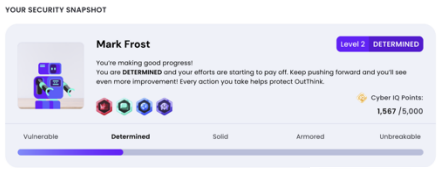
API Integrations – Give Teams Intel On Human Risk

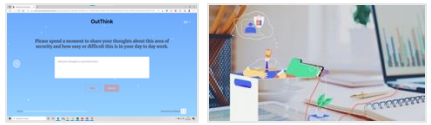
Human Risk Intelligence



The How - Cybersecurity Human Risk Management







CyberIQ

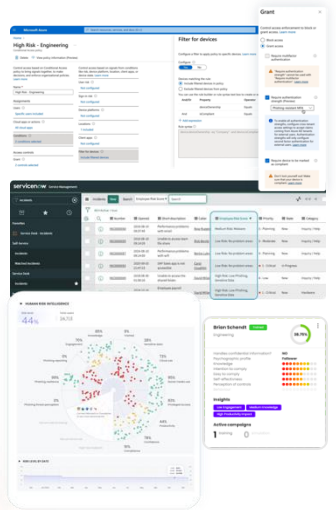
AI Phishing Simulator

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