revel8

formerly:

AI will generate
$4 Trillion in value

Cyber Fraud will cost
$11 Trillion in damages

Employees Risk
At the root of 90% of attacks

✕

AI Advancements
Wave of GenAI social engineering

Incumbent Tools
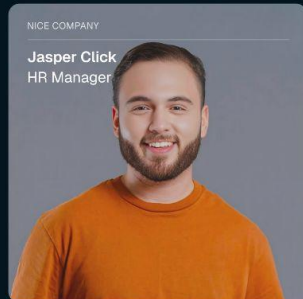# Do Not Address the Problem

---

KnowBe4

Microsoft Defender

sosafe

Lucy
Powered by ThriveDX

The Future of Awareness
Train each employee with a tailored playlist of the latest attacks

NICE COMPANY

Jasper Click
HR Manager

★ 55 Score

✔ 600 Rank

Nice Company	Munich, GER
Human Resources	Manager
Talent Acquisition	Recruiting
German	Workers Council
Personio	

Jasper Click, HR-Manager

#	Channel	Attack Name	Response		Training
1	💬 🌐	**Login attempt from new device** Microsoft	Fakewebsite Opened + 0 pts	Credentials Typed + 0 pts	⊖ +0
2	✉ ▦	**Invitation to Bayern Munich game** External Service Provider	Reported + 10 pts		✔ +5
3	✉ 📎	**New application: CV attached** External Applicant	Ignored + 2 pts		✔ +5
4	📞 ✉	**Urgent change of bank details** Employee	Call Interacted + 0 pts	File Downloaded + 0 pts	✔ +5
5	💬	**Lost password** Manager			
6	📹 ✉	**Video call about payroll issue** Chief People Officer	Upcoming		
7	📹 ▦	**Helpdesk: Spamfilter Restoration** Internal IT	Upcoming		
8	📞 💬	**Confidential wire transfer approval** Chief Financial Officer	Upcoming		

What Makes our Solution so Effective?

8

01

Live Human Threat Intelligence

02

OSINT Risk Profiling

03

AI-Powered Attack Simulation

04

Next-Gen Learning & Gamification

05

Compliance & Reporting

Simulate the most Dangerous Real-World Threats

Live Human Threat Intelligence	→	OSINT Risk Profiling	→	AI-Powered Attack Simulation	→	Next-Gen Learning & Gamification	→	Compliance & Reporting
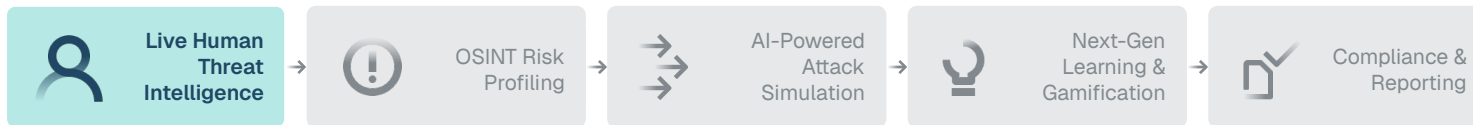
1. Public Information

- Threat intelligence databases
- Web scraping of news, cyber blogs & other publications

2. Industry Community

- Customers willing to share real social-engineering attacks
- Industry-specific training simulations shared among customers

3. Ethical Hackers - Platform

- Open up threat composer technology to the public
- Ethical hackers to contribute to open-source database

Recent example: Spambombing attack

Spambombing Call
1:17 (675 kB)

Step 1: Multiple newsletter signups   Step 2: Call from IT Helpdesk

Translate Latest Attacks into Training Scenarios

8

Live Human Threat Intelligence → **OSINT Risk Profiling** → AI-Powered Attack Simulation → Next-Gen Learning & Gamification → Compliance & Reporting

Parameters (Example)

- Individual
  - University | Previous employer | ...
- Team
  - Voice sample | Open positions | ...
- Company
  - Latest acquisition | Date of annual meeting | ...
- Market & Industry
  - New industry trend | Trade fair | ...
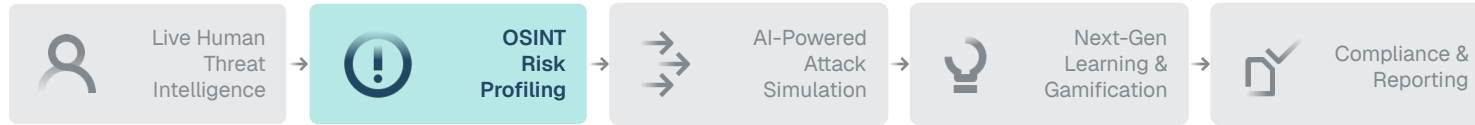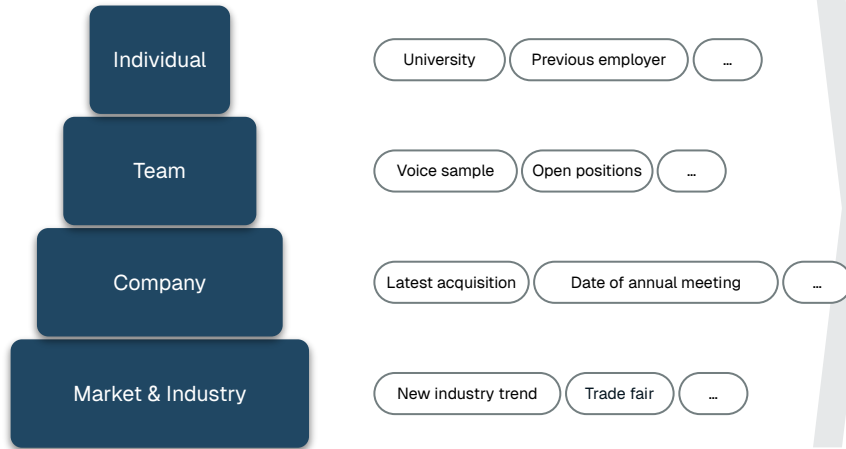
OSINT Graph – Admin interface

revel8 — Harald Mustermann

Phishing Awareness Monitor
- Overview
- Simulation Details
- Security Incidents
- Threat Intelligence
- OSINT Risk Profiling

Settings
- Employees
- Simulation
- Context Collector

OSINT Risk Profiling

| 650 Weekly Vulnerabilities | 3278 New Data Points Found | 65/100 Risk Score | 3 Critical Findings | 75 Digital Shadow Score |

Responsible: Harald Mustermann (Group 4)

Exposed: Software Version/Tools — Risk: Vulnerabilities Exploitation

Exposed: Strategic Initiatives/Project Leaders — Risk: Spearphishing

Exposed: Employee Interactions/R&D Efforts — Risk: Social Engineering/IP Theft

Top OSINT Risk Probability (Today)
- Social Engineering — 85%
- Spearphishing — 50%
- IP Theft — 60%

AI simulations across the human attack surface

Live Human Threat Intelligence → OSINT Risk Profiling → **AI-Powered Attack Simulation** → Next-Gen Learning & Gamification → Compliance & Reporting

Simulation playlist for example user from HR
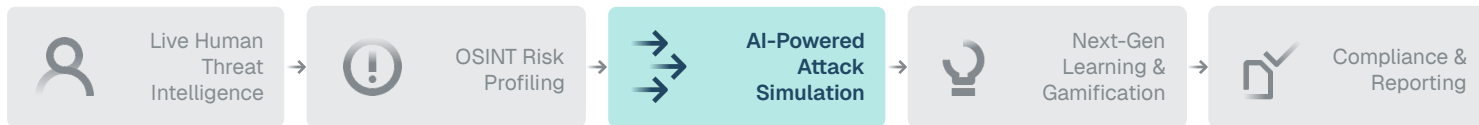
USER TYPES	ATTACK VECTOR(S)	SIMULATIONS
Executive	**C-Level channels:** Phone calls, whatsapp	Custom scenarios enriched with personal OSINT risk profiles
High-Risk Profile	**All relevant channels:** Email, SMS, calls, etc.	User-specific, OSINT based on job title
White Collar	**3 standard channels:** Email, SMS, messenger	Role-specific, OSINT based on department
Blue Collar	**1 channel:** Email	Current phishing schemas enriched with company OSINT data

100% of human attack surface

Playlist

First name	Last name	Simulation Name	Simulation Type	Events	Scheduling St
Tom	Müller	InvoiceInteractive_EU	Call and email		Finished
Tom	Müller	Hermes	Email		Finished
Tom	Müller	InvoiceInteractive_EU	Call and email		Finished
Tom	Müller	InteractivePayroll	Call and email		Finished
Tom	Müller	Sheets	Email	Training completed / Training started / Mail clicked	Finished
Tom	Müller	ADAC	Email	Mail clicked / Credentials typed	Finished
Tom	Müller	SharepointFW	Email and fake website	Training completed / Training started	Finished
Tom	Müller	Slack	Email	Training started / Mail clicked	Finished
Tom	Müller	Hermes	Email		Finished
Tom	Müller	InvoiceInteractive_EU	Call and email		Finished
Tom	Müller	SharepointFW	Email and fake website	Credentials typed / Training started	Finished
Tom	Müller	3CX	Email		
			Email		

Holistic attacks across multiple channels

Difficulty & frequency based on user behavior

Bite-sized Learning & Gamification

Live Human Threat Intelligence	→	OSINT Risk Profiling	→	AI-Powered Attack Simulation	→	**Next-Gen Learning & Gamification**	→	Compliance & Reporting
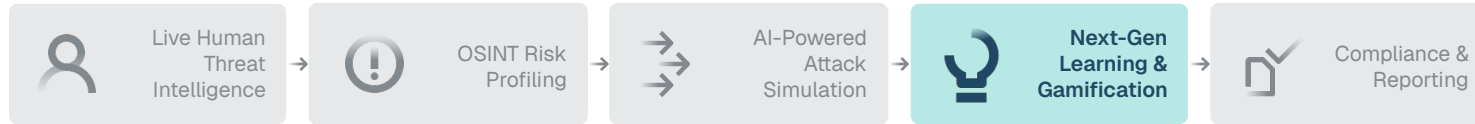
1. In-the-moment Training Nuggets

- Train employees in an optimal psychological moment with bite-sized lesson
- Learning effect that drives long-term behavioral change

2. Gamification

- Internal company ranking encourages healthy competition
- Individual user performance determines difficulty and frequency of simulation playlist

3. AI Course Builder

- Interactive, personalized training approach to cover awareness beyond simulations
- Training depth adjusts on current awareness level and interactions of the employee

Gamification dashboard for employees

b03937c7-249e-42e6-836e-b2295a8594eb
Mette Schwital
☆ 108 Points earned   🛡 30 Simulations received

Leaderboard
of top performers | Department | Company |

Name	Points
Compliance	137
Compliance	124
Communications	115
Compliance	113
Administration	112
Compliance	111
Communications	110
Mette Schwital	108
Business Development	106
Accounting	106
Accounting	105
Business Development	104
Compliance	103
Accounting	103

Simulation Playlist

Channel	Name	Response	Training	Earned	Missed
EMAIL	Klarna				
SMS AND FAKE WEBSITE	SMS -				
EMAIL	Dayfor				
EMAIL	Faceboo				
SMS	CECI S				
EMAIL	Conflu				
EMAIL	Custor				
EMAIL	Fake in				
EMAIL	Linked				
EMAIL	Perso				
EMAIL	DHL- F				
EMAIL	Heme				
EMAIL	SageD				
EMAIL AND ATTACHMENT	Date				
EMAIL	Klama				
EMAIL	Navisi				
EMAIL	Lufthar				
EMAIL	Sharep				
EMAIL AND ATTACHMENT	O88-				
EMAIL	DocuS				

Call from an unknown number 💡

Did you just receive a call from your manager? Listen to the call again very carefully:

▶ 0:00 / 0:28 🔊 ⋮

revel8 tip: Pay attention to the choice of words and tone of voice. If in doubt, hang up and call back.

Back	Next

In-the-moment training

Reporting and Live Human Risk Assessment

| Live Human Threat Intelligence | → | OSINT Risk Profiling | → | AI-Powered Attack Simulation | → | Next-Gen Learning & Gamification | → | **Compliance & Reporting** |
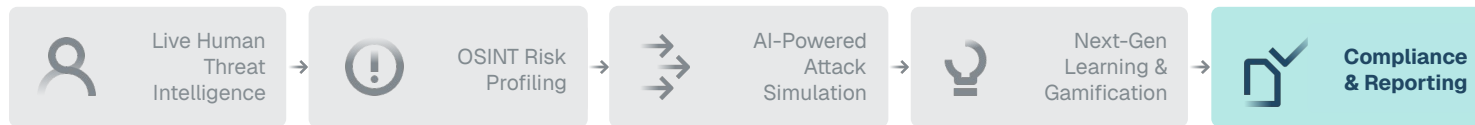
1. Live Awareness Monitor

- Live reporting of awareness levels on group level
- Data-driven vulnerability analysis including details on severe interactions and repeated offenders
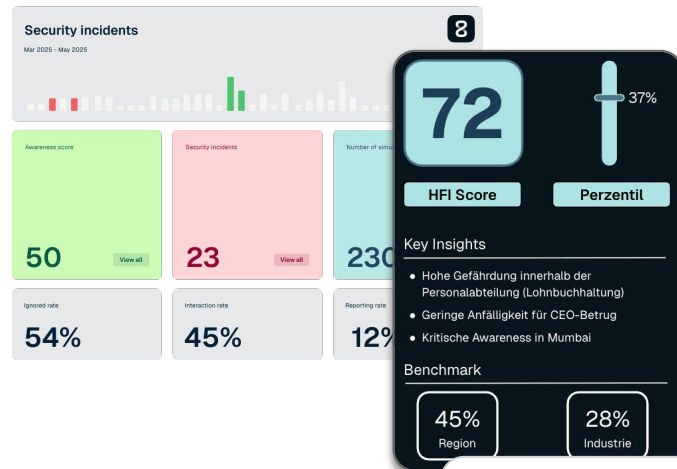
2. Human Firewall Index

- One-week standardized assessment of awareness to compare with industry benchmark
- Development in cooperation with Prof. Dr. Krcmar

3. Compliance Fulfillment

- Certificate of successful user awareness training fulfills specific requirements of compliance standards such as ISO27001, NIS-2, TSAX, etc.

Live human awareness monitor example

Security incidents
Mar 2025 - May 2025

Awareness score
50 View all

Security incidents
23 View all

Number of simu...
230

Ignored rate
54%

Interaction rate
45%

Reporting rate
12%

72
HFI Score

37%
Perzentil

Key Insights
- Hohe Gefährdung innerhalb der Personalabteilung (Lohnbuchhaltung)
- Geringe Anfälligkeit für CEO-Betrug
- Kritische Awareness in Mumbai

Benchmark
45% Region
28% Industrie

Example HFI scorecard

Becoming the Global Standard for Human Cyber Risk

Horizon 3:
Proactive layer for
human cyber security

Horizon 2:
Global benchmark for
human cyber risk

Horizon 1:
AI-native, threat-based
E2E awareness platform

We are revel8

Our Founder Team

Tom Müller
Co-CEO

Julius Muth
Co-CEO

Robert Seilbeck
CTO

+7 Revels

Supported by Leading Cyber Experts

Sergej Epp
CISO Sysdig

Michael Schrank
CISO Adidas

Peter Dornheim
CISO Daimler Trucks

Mahdi Abdulrazak
CISO SHV Energy

Max Ruhwinkel
CIO Knauf

Ibrahim Memis
CISO Beumer

Hartmut Müller
CTO ServiceNow

Naby Diaw
CISO Lufthansa

Rogier Fischer
CEO Hadrian.io