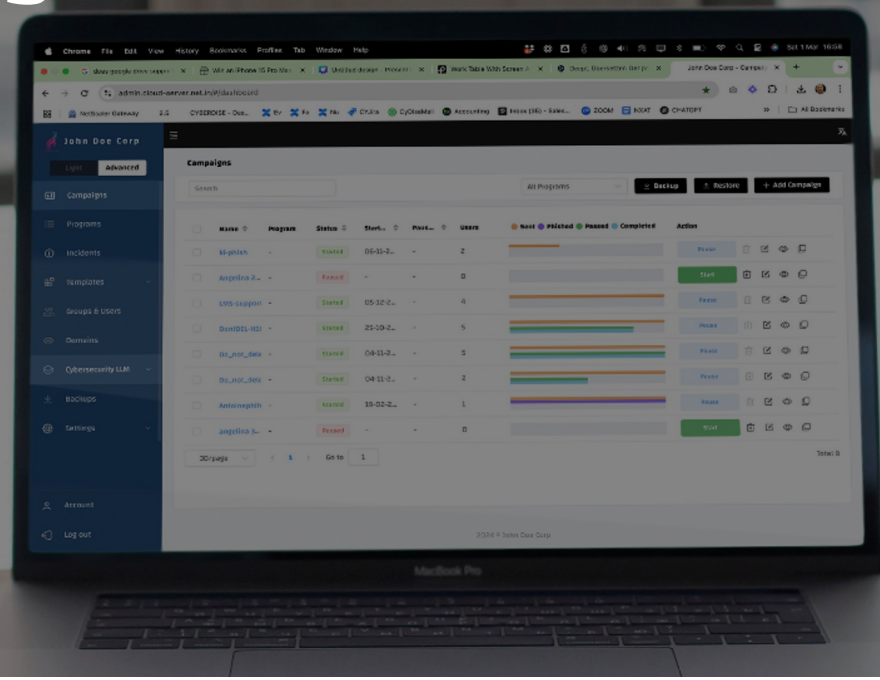
Was hat Awareness mit Schweizer Eishockey gemein?

CYBERDISE

Palo Stacho, Managing Director
palo.stacho@cyberdise.io
+41793017810

Pioneering Cybersecurity Awareness in the Age of AI



Supported by:
Start-up innovation project supported by
Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra
Swiss Confederation
Innosuisse – Swiss Innovation Agency


Die Schweiz hatte schon immer ausgezeichnete Eishockey Trainer
Ralph Krueger
Trainer Schweizer Nationalmannschaft 1991—1997, 2000-2004
CYBERDISE

Doch kamen die Eidgenossen vor 2004 im welt-weiten Vergleich nicht über das Mittelfeld hinaus...

1985-2004:
2 x in Top 5

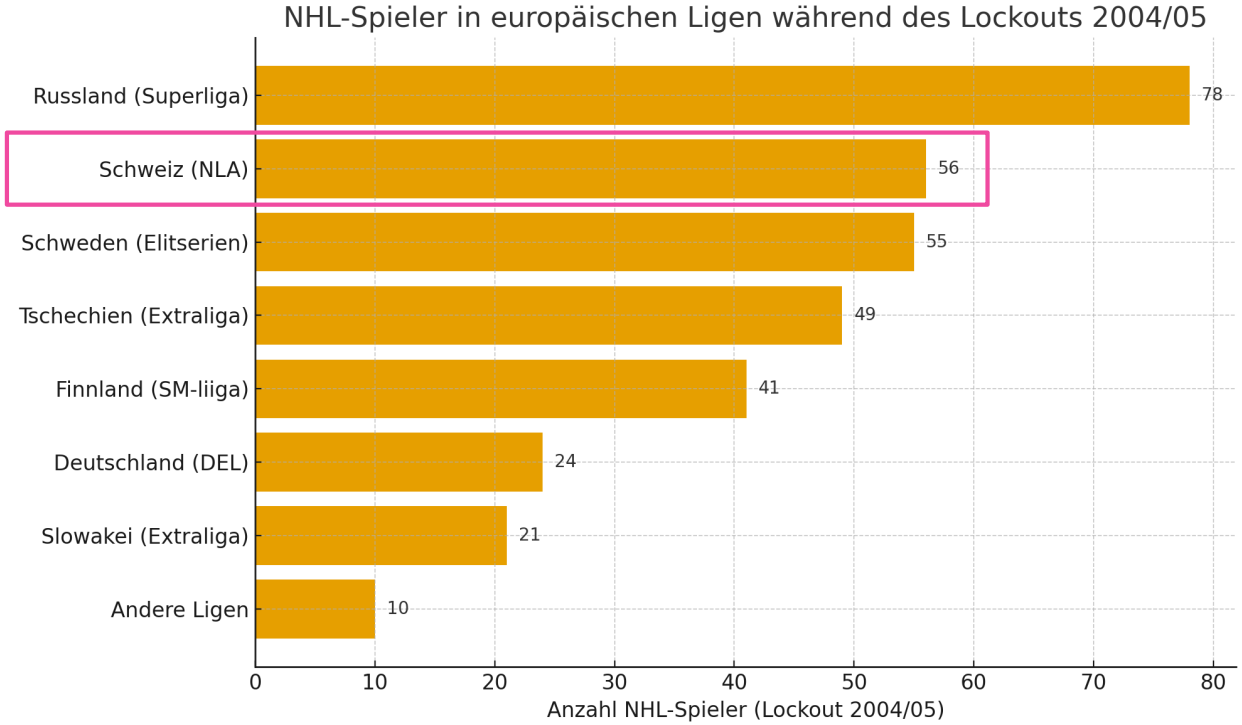
1985: 10. Platz	1995: 12. Platz
1986: 9. Platz	1996: 14. Platz
1987: 8. Platz	1997: 15. Platz
1988: keine WM	1998: 4. Platz
1989: 12. Platz	1999: 8. Platz
1990: 9. Platz	2000: 6. Platz
1991: 7. Platz	2001: 9. Platz
1992: 4. Platz	2002: 10. Platz
1993: 10. Platz	2003: 8. Platz
1994: 13. Platz	2004: 8. Platz

WM-Rankings

CYBERDISE

credits: horge@wikipedia

Erst der NHL Lockout 2004/05 brachte den entscheidenden Schritt!



Die Kombi von Spitze-Trainern und world-class Gastspielern änderte alles!

CYBERDISE

Die Parallelen zu Cybersecurity Awareness

Die Studie: Leveraging AI-enabled spearphishing to enhance Cybersecurity

Innocheck (73275.1 INNO-ICT), AISP (AI enabled Spear Phishes)

Studienpartner

- Lucerne University of Applied Sciences and Arts
- CYBERDISE Awareness
- GLB (A Swiss medium-sized construction company)

Studienperiode November 2024 bis Juni 2025

Start-up innovation project supported by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Innosuisse – Swiss Innovation Agency

HSLU Hochschule Luzern

CYBERDISE

AISP - Research Questions

Wird KI effektivere Cyberangriffe ermöglichen und wie sollen wir darauf reagieren? Konkret:

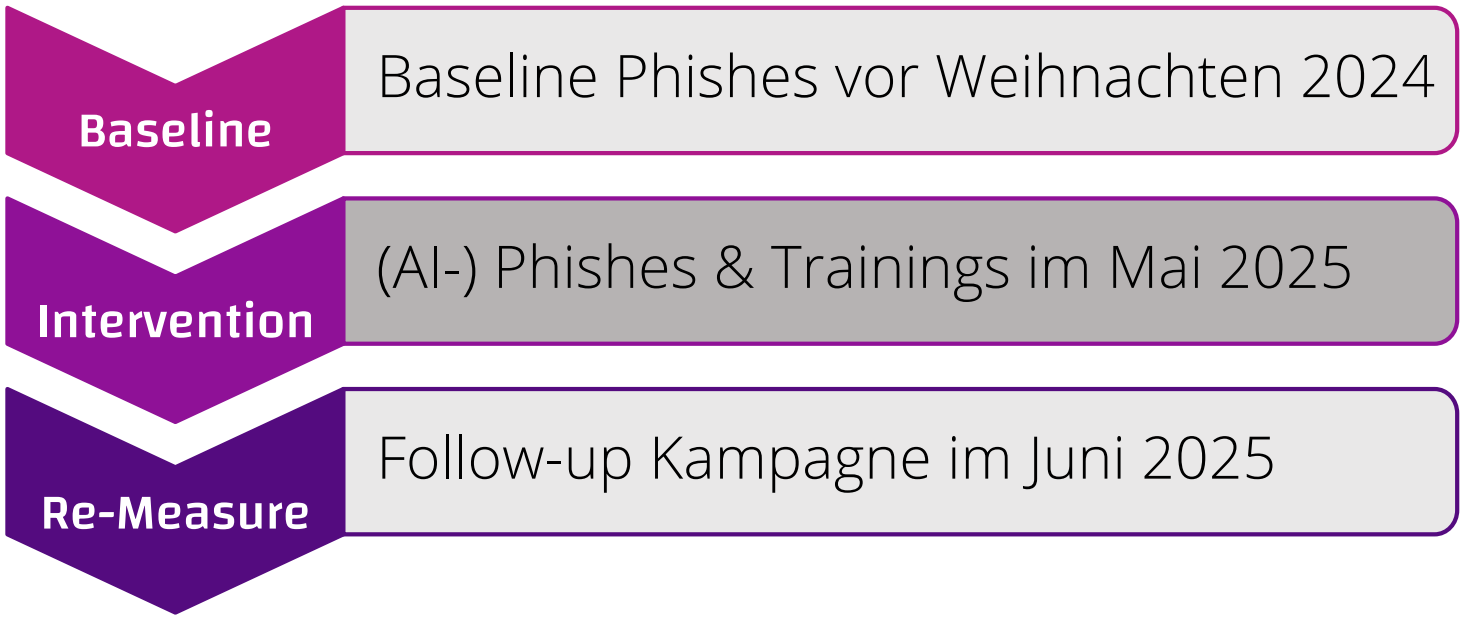
- Sind KI-gestützte Spearphishing-Angriffe im europäischen OSINT-Kontext gefährlicher als herkömmliches Phishing?
- Wie effektiv ist Risiko-Exposition im Vergleich zu normativem Training? (Sprich: angegriffen zu werden und zu wissen, dass man angegriffen wird vs. Standardausbildung zum richtigen Verhalten)?

Will AI enable more effective cyber attacks and how do we respond? Specifically:

Are AI-enabled spearphishing attacks more dangerous than conventional phishing in a European OSINT context?

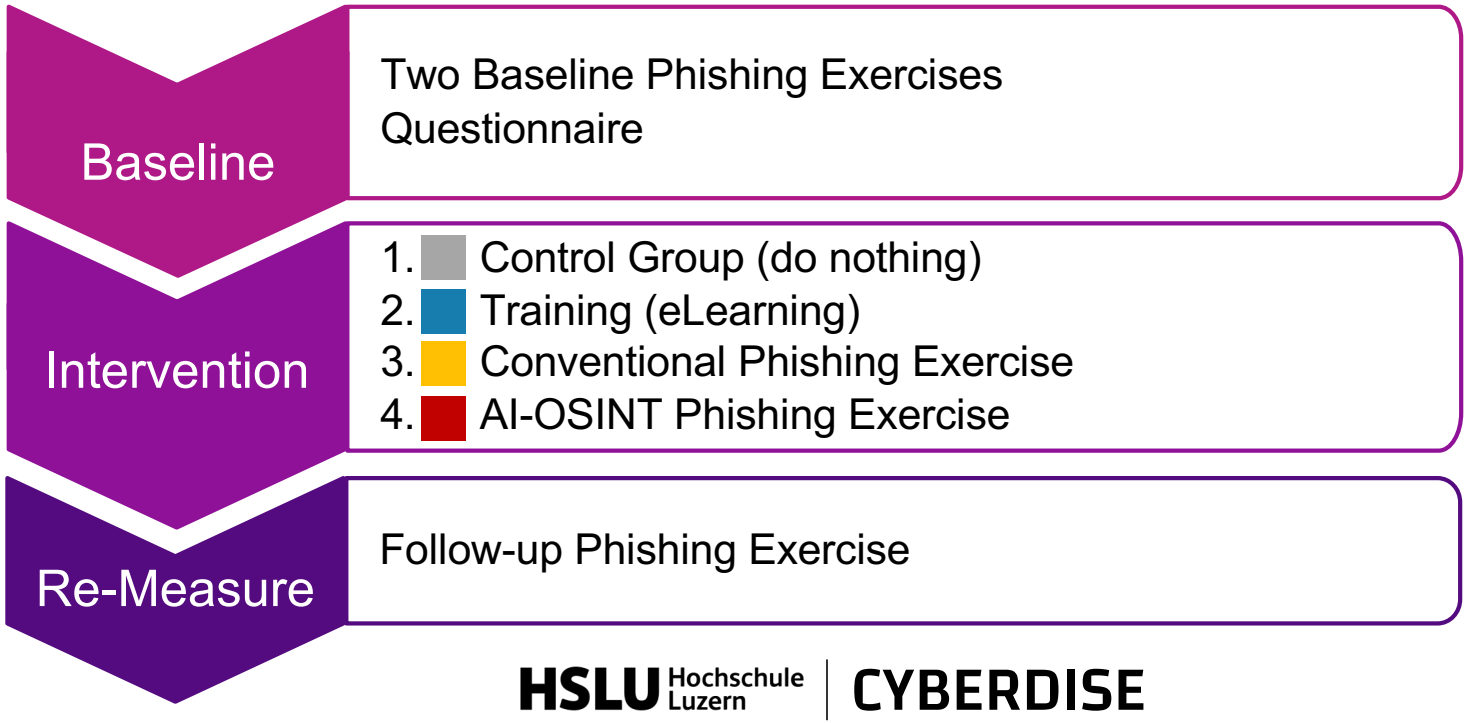
How effective is risk exposure (being attacked and knowing you are being attacked) vs. normative training (standard education on how to behave)?

AISP – Studienstruktur und Ablauf



HSLU Hochschule Luzern | CYBERDISE

AISP – Vier Kohorten in der Interventionsphase



HSLU Hochschule Luzern | CYBERDISE

Resultate und Erkenntnisse aus der Studie

AISP - Leveraging AI-enabled spearphishing to enhance cybersecurity

AISP – Studienresultate: Attitüde vs Verhalten

"This project allowed us to investigate the effect of different interventions to impact risk behavior and risk attitude in cybersecurity." - Dr. Carlo Pugnetti, Scientific Study Director, HSLU

= actions

Beobachtbare Handlungen der Mitarbeiter im Bereich Cybersicherheit (z. B. Meldung von Phishing-E-Mails, Befolgung von Richtlinien).

= mindset

Grundlegende Einstellungen gegenüber Sicherheitsrisiken (z. B. Risikobereitschaft, Bedrohungswahrnehmung, Vertrauen vs. Skepsis).

AISP – Studienresultate

Wirksamkeit von Interventionen	Wirksamkeit von ‚Attacken'[1]

• Normative Schulungen reduzierten die Anfälligkeit für Phishing um ~40 %.
• Die Risikoexposition (Phishing-Simulation) war besser:
  • Herkömmliche Phish-Sims reduzierten riskantes Verhalten um ~45 %.
  • KI-/OSINT-Phish-Sims reduzierten es sogar noch stärker (≈60 %).
In allen Gruppen gab es Verbesserungen.
	• Weniger OSINT-Daten in Europa verringern den Realismus von KI-Phishing.
	• Herkömmliches Phishing kann ebenso gefährlich sein, ist jedoch kostspieliger.
	• KI-Spearphishing ist günstiger sobald die Tools vorhanden sind, ist jedoch weniger effektiv, als US-Studien vermuten lassen.

[1] Simulated Phishing Attacks is one subtype of an intervention.

AISP – Studienresultate

Risk Behavior

Ergebnisse zu Risikoverhalten

Gemessen durch Phishingergebnisse:

- Baseline Daten-Eingaberate 8–10%.
- Nach der Interventionsphase, Eingaberaten:
  1. Control Gruppe 11%, keine Änderung[1].
  2. Training Gruppe 6%.
  3. Konventionelle Phishing Exposition 7%.
     AI/OSINT Phishing Exposition 4%.
- Direkte Konfrontation mit Angriffen veränderte das Verhalten am stärksten, insbesondere bei KI/OSINT-Phish-Übungen

[1] Das bedeutet, dass der Sensibilisierungseffekt nach 5 Monaten verschwunden ist.

Risk Attitude

Ergebnisse zur Attitüde

Gemessen mit Fragebögen[2].

- Schulungsmaßnahme: führte zu einer signifikanten positiven Veränderung der Einstellung gegenüber dem Risikobewusstsein.
- Phishing-Maßnahmen: führten trotz einer Verringerung des Verhaltens zu keiner wirklichen Verbesserung der Risiko-Einstellung (Attitüde).
- Kontrollgruppe: leichte Besserung, statistisch nicht signifikant

[2] Fragen wie z. B. „Wir sind ein Ziel für Hacker“, „Cybersicherheit ist jedermanns Verantwortung“ usw.

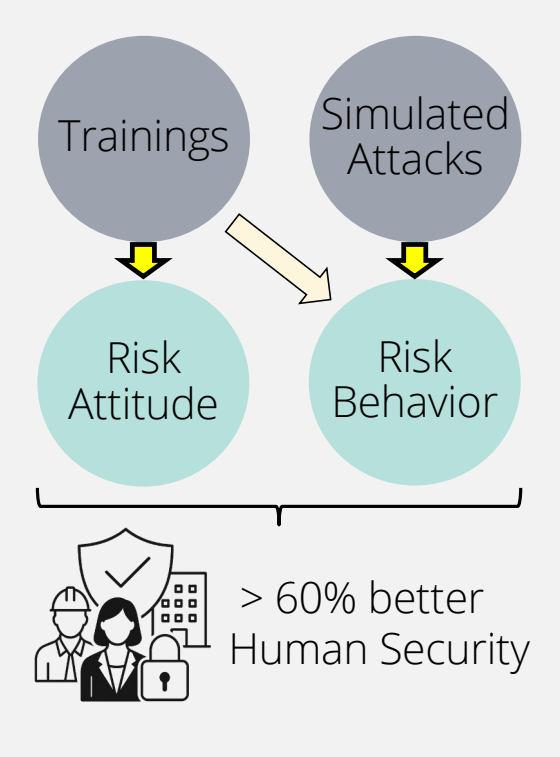
Konklusionen

aus der Studie «*AISP - Leveraging AI-enabled spearphishing to enhance cybersecurity*»

AISP-Studienresultate: AI-enabled Spear Phishing Exercises

Haupterkenntnisse

- E-Learning/CBTs eignen sich hervorragend, um die Einstellung der Menschen zum Thema Cybersicherheit zu beeinflussen.
- Exposure (Phishing-Übungen, insbesondere auf Basis von KI/OSINT) eignet sich toll, um das tatsächliche Verhalten der Menschen zu beeinflussen.
- KI-Phishing-Übungen sind am Besten, sie verbessern das Risikoverhalten um bis zu 60 %
- Aktion & Attitüde - Du brauchst beides: Phish-Sims und Infosec Schulungen.



Aktion & Attitüde während Lockout 2004

Trainer stärkten das Mindset, NHL-Profis das Verhalten

1985-2004:
2 x in Top 5

2005-2025:
8 x in Top 5
4 x Silber

2005 – 8. Platz
2006 – 9. Platz
2007 – 8. Platz
2008 – 7. Platz
2009 – 9. Platz
2010 – 5. Platz
2011 – 9. Platz
2012 – 11. Platz
2013 – Silber
2014 – 10. Platz
2015 – 8. Platz
2016 – 11. Platz
2017 – 6. Platz
2018 – Silber
2019 – 8. Platz
2020 – kein Turnier
2021 – 6. Platz
2022 – 5. Platz
2023 – 5. Platz
2024 – Silber
2025 – Silber

WM-Rankings
2005-2025

CYBERDISE

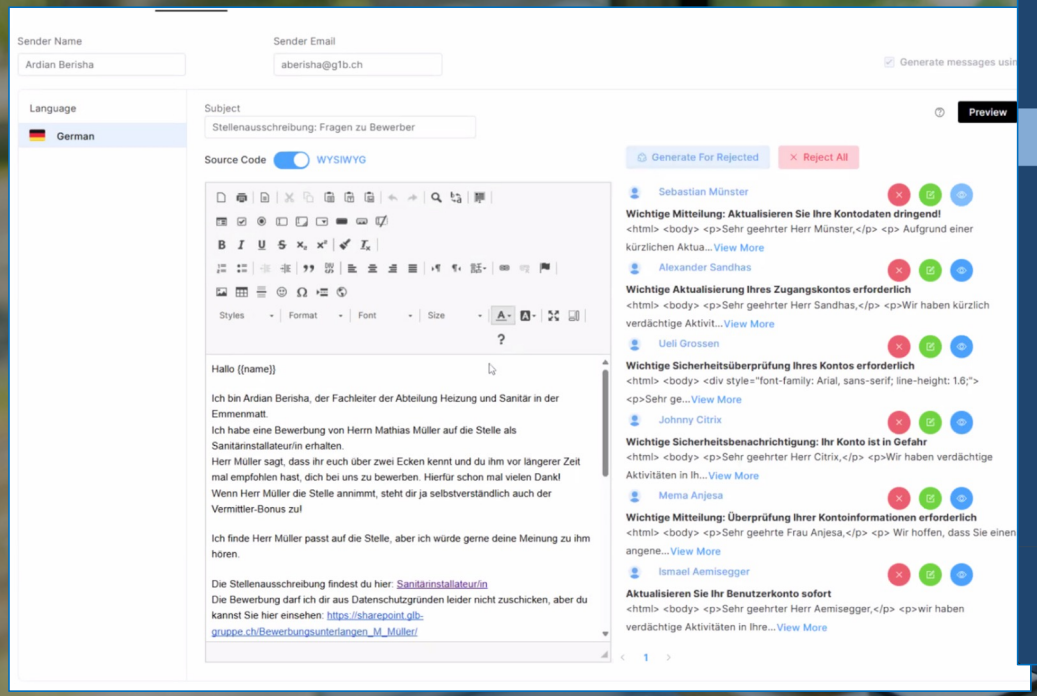
Was haben wir daraus gemacht?

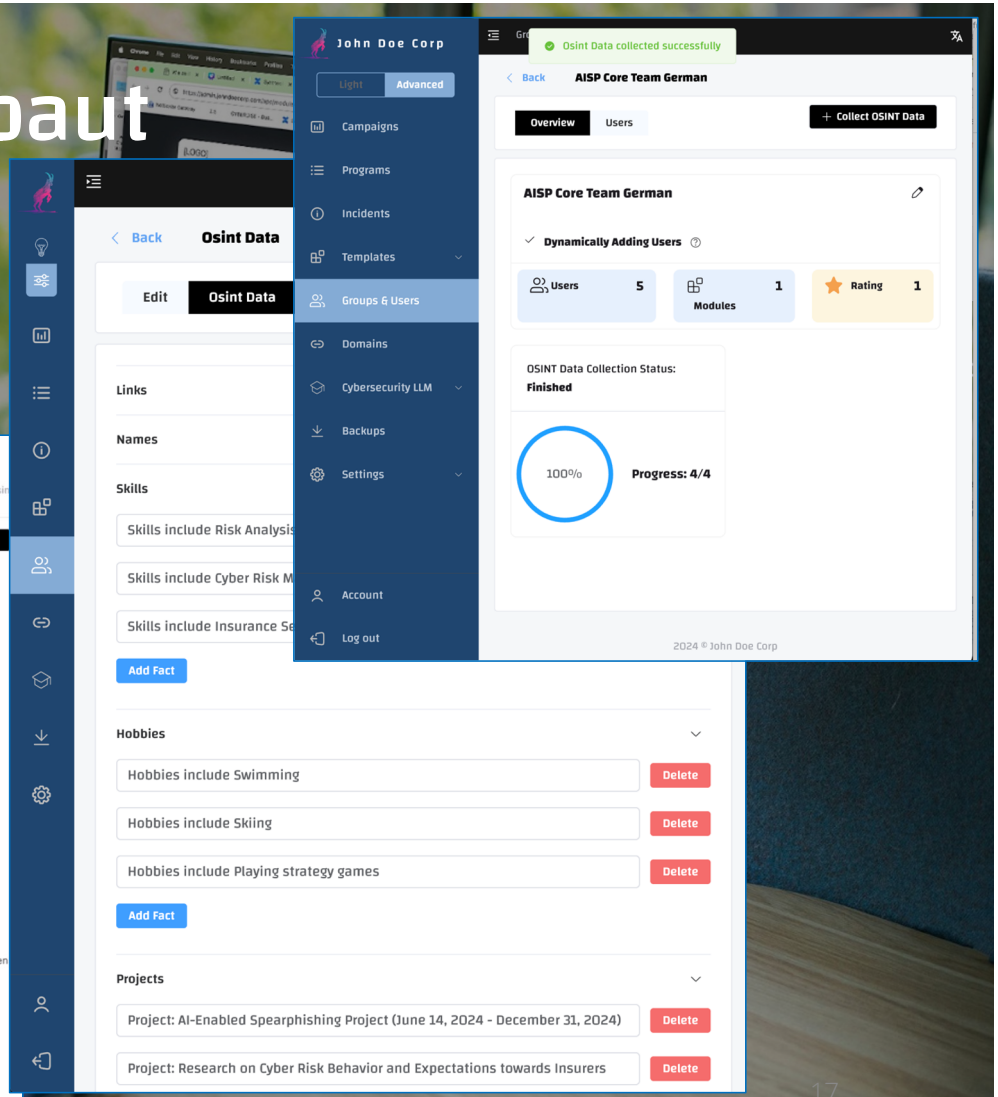
Produkt-Implikationen der Studie «*AISP - Leveraging AI-enabled spearphishing to enhance cybersecurity*»

CYBERDISE

Wir haben KI-Features gebaut

-OSINT Reconnaissance
-Educational Vulnerability Profiles
-AI Phish Generator
-Custom InfoSec-Chatbot





CYBERDISE AWARENESS

Wo KI-Forschung auf menschliches Verhalten trifft

450'000+ licensed Users

6 Countries served

220+ Templates

First AI-native Solution

CYBERDISE

Supported by:

Start-up innovation project supported by

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Swiss Confederation

Innosuisse – Swiss Innovation Agency