Awareness Doesn't Stop Attacks. Behavior Does. Speed Contains.

A Paradigm Shift in Cybersecurity: CYBERDISE Establishes "Behavioral Defense Engineering" to Combat AI-Driven Threats

<German version below>

Zug, Switzerland – June 23, 2026 – For years, the global cybersecurity industry has been fighting the right problem with the wrong methods. While traditional security awareness programs have focused on theoretical knowledge transfer for two decades, measurable organizational risk remains consistently high. A joint study by CYBERDISE and the Lucerne University of Applied Sciences and Arts (HSLU) scientifically confirms what practice has long shown: more knowledge does not automatically translate into secure behavior when employees are targeted by real, psychologically optimized attacks.

In response to this industry-wide realization, CYBERDISE is driving a fundamental paradigm shift by introducing **Behavioral Defense Engineering (BDE)**. The objective is to stop treating human behavior as a mere theoretical compliance checkbox and instead integrate it as a measurable, operational component of active IT security processes. With the launch of its new platform version, CYBERDISE V3.2, the company provides the technological infrastructure required to improve habits and translate human behavioral signals directly into actionable cyber defense intelligence.

The Problem is Not Knowledge, It is Action

Most employees today are aware that phishing emails contain dangerous links. Yet, under the pressure of daily business operations, individuals still click on malicious attachments, leak data, or fail to report incidents to IT in a timely manner. The issue in modern cybersecurity is not a lack of knowledge, but a behavioral gap.

"Traditional awareness changes knowledge. Behavioral Defense Engineering changes how people act," **explains Palo Stacho**, founder of CYBERDISE. *"In the era of AI-driven social engineering, theoretical knowledge is no longer enough. Attacks are highly personalized and carried out across multiple channels, and there will always be messages that reach the recipient, bypassing the Security Operations Center (SOC). Organizations must be capable of transforming human signals into real-time security data to maximize collective response speed."*

"Our research shows employees can become an effective first line of defense, but only if the right tools are deployed at the exact right time. As attackers evolve, our responses must stay one step ahead. A system that actively activates human behavior is a necessary addition to the modern security arsenal," **adds Dr. Carlo Pugnetti** from HSLU.

Behavioral Defense Engineering as an Operational Security Factor

The core of Behavioral Defense Engineering is the continuous measurement and optimization of live behavior in real-world scenarios – moving away from simply checking boxes on training

videos or multiple-choice quizzes. Human reactions are thus transformed into an active early warning framework (Cyber Defense Intelligence System).

From Real-Time Attack to Instant Immunization

Automated instant campaigns demonstrate how this approach works in practice: if a real phishing email bypasses technical defenses, CYBERDISE immediately converts the attack vector into a safe simulation as soon as the SOC identifies and purges the threat from user mailboxes. The workforce is confronted with a copy of the actual live attack in real time, effectively immunizing them against that specific threat vector.

Version 3.2 of the CYBERDISE Suite validates this strategic approach through a series of additional, coordinated tools: :

- **Multi-Channel Attack Simulations:** Evaluation of real-world responses to phishing, smishing, vishing, quishing, and Microsoft Teams threats.
- **Educational Vulnerability Profiles:** AI-powered OSINT analyzes publicly available employee data to execute automated, highly personalized attack simulations in real time.
- **SOC Infrastructure Integration:** Automated workflows drastically reduce the time elapsed from a reported signal to active IT security incident response.

To make this essential security approach broadly accessible to organizations of all sizes, CYBERDISE continues to offer a fully functional Freemium Edition for download.

About CYBERDISE

Cyberdise AG is a pioneer in Behavioral Defense Engineering. Founded in 2023 and headquartered in Zug, Switzerland, the company combines behavioral science insights with an AI-powered suite for incident reporting, attack simulation, rapid incident response, and traditional training. CYBERDISE actively prevents complex social engineering threats for more than 500,000 licensed users today.
Further information can be found at: www.cyberdise.io

Media Contact:
Palo Stacho, Cyberdise AG | Poststrasse 26, 6300 Zug, Switzerland
Phone: +41 41 511 7810 | Email: palo.stacho@cyberdise.io

Perspektivwechsel in der Cybersecurity: CYBERDISE etabliert „Behavioral Defense Engineering“ als Antwort auf KI-gestützte Bedrohungen

Zug, Schweiz – 23. Juni 2026 – Die globale Cybersicherheitsbranche hat jahrelang das richtige Problem mit den falschen Methoden bekämpft. Während klassische Security-Awareness-Programme seit über zwei Jahrzehnten stark auf theoretischen Wissenstransfer setzen, bleibt das messbare Risiko unverändert hoch. Eine gemeinsame Studie von CYBERDISE und der Hochschule Luzern (HSLU) belegt wissenschaftlich, was die Praxis längst zeigt: Mehr Wissen führt bei Mitarbeitenden nicht automatisch zu sicherem Handeln, wenn sie mit realen, psychologisch optimierten Angriffen konfrontiert werden.

Als Konsequenz aus dieser Branchenerkenntnis leitet CYBERDISE einen grundlegenden Paradigmenwechsel ein und stellt das Konzept des **Behavioral Defense Engineering (BDE)** vor. Ziel ist es, menschliches Verhalten nicht länger als rein theoretisches Compliance-Kriterium zu betrachten, sondern als messbaren, operativen Bestandteil der aktiven IT-Sicherheitsprozesse. Mit der Veröffentlichung der neuen Systemversion CYBERDISE V3.2 liefert das Unternehmen die technologische Infrastruktur, um Verhalten zu verbessern und menschliche Reaktionen direkt in verwertbare Cyber-Abwehrdaten zu übersetzen.

Das Problem liegt nicht im Wissen, sondern im Handeln

Die meisten Angestellten wissen heute, dass Phishing-Mails gefährliche Links enthalten können. Dennoch klicken Menschen im stressigen Arbeitsalltag auf bösartige Anhänge, geben Daten preis oder versäumen die rechtzeitige Meldung an die IT-Abteilung. Das Problem moderner Cybersecurity ist demnach kein Wissensdefizit, sondern eine Verhaltenslücke.

„Klassische Sensibilisierung zielt auf das Wissen. Dagegen verbessert Behavioral Defense Engineering das konkrete Verhalten der Leute“, erklärt Palo Stacho, Gründer von CYBERDISE. *„Im Zeitalter des KI-gestützten Angriffe reicht theoretisches Wissen nicht mehr aus. Social Engineering erfolgt hochgradig personalisiert über mehrere Kanäle und es wird immer Angriffe geben, welche bis zum Empfänger durchschlagen, am Security Operations Center (SOC) vorbei. Unternehmen müssen in der Lage sein, auch menschliche Signale in Echtzeit-Sicherheitsdaten umzuwandeln, um die kollektive Reaktionsgeschwindigkeit zu optimieren*.“

"Unsere Forschung zeigt, dass Mitarbeitende eine effektive erste Verteidigungslinie bilden können – aber nur, wenn die richtigen Werkzeuge zum exakt richtigen Zeitpunkt eingesetzt werden. Da Angreifer immer raffinierter vorgehen, müssen unsere Reaktionen einen Schritt voraus sein. Ein System, das menschliches Verhalten aktiv mobilisiert, ist eine notwendige Ergänzung im modernen Sicherheitsarsenal“, ergänzt Dr. Carlo Pugnetti von der (HSLU)."

Behavioral Defense Engineering als operativer Sicherheitsfaktor

Der Kern von Behavioral Defense Engineering liegt in der kontinuierlichen Messung und Optimierung des realen Verhaltens in Akut-Situationen – statt des blossen Abhakens von

Schulungsvideos oder Multiple-Choice-Tests. Menschliche Reaktionen werden dadurch zu einem aktiven Frühwarnsystem, dem Cyber Defense Intelligence System geformt.

Vom Echtzeit-Angriff zur sofortigen Immunisierung

Wie dieser Ansatz in der Praxis funktioniert, zeigen automatisierte Sofortkampagnen: Durchbricht eine echte Phishing-Mail die technischen Filter, wandelt CYBERDISE den Angriffsvektor sofort in eine sichere Simulation um, sobald das SOC die Bedrohung identifiziert und aus den Mailboxen entfernt hat. Die Belegschaft wird so in Echtzeit mit einer Kopie des realen Angriffs konfrontiert und für diese spezifische Bedrohung immunisiert.

Die Version 3.2 der CYBERDISE Suite validiert diesen strategischen Ansatz durch eine Reihe weiterer, koordinierter Werkzeuge:

- **Mehrkanal-Angriffssimulationen:** Überprüfung des Realverhaltens bei Phishing, Smishing, KI-gestütztem Conversational Vishing, QR-Code-Betrug (Quishing) und Microsoft-Teams-Szenarien.
- **Edukative Schwachstellenprofile**: KI-gestütztes OSINT analysiert öffentlich verfügbare Daten der Mitarbeitenden für automatisierte, hochgradig personalisierte Angriffssimulationen in Echtzeit**.**
- **SOC-Infrastruktur-Integration:** Automatisierbare Workflows verkürzen die Zeitspanne vom gemeldeten Signal bis zur aktiven Incident Response drastisch.

Um diesen notwendigen Sicherheitsansatz für Organisationen jeglicher Grösse flächendeckend zugänglich zu machen, stellt CYBERDISE weiterhin eine voll funktionsfähige Freemium-Edition zum Download bereit.

Über CYBERDISE
Die Cyberdise AG ist ein Pionier im Bereich Behavioral Defense Engineering. Das 2023 gegründete Schweizer Unternehmen mit Hauptsitz in Zug kombiniert wissenschaftliche Erkenntnisse der Verhaltensforschung mit einer KI-gestützten Suite für Incident Reporting, Angriffssimulation, schneller Vorfallreaktion und klassischer Schulung. CYBERDISE beugt heute komplexen Social-Engineering-Bedrohungen bei mehr als 500.000 lizenzierten Nutzern effektiv vor. Weitere Infos unter: www.cyberdise.io

Pressekontakt:
Palo Stacho, Cyberdise AG | Poststrasse 26, 6300 Zug, Schweiz
Telefon: +41 41 511 7810 | palo.stacho@cyberdise.io