



<German Version below>

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

CYBERDISE Launches Behavioral Defense Engineering and CYBERDISE V3.2

Behavioral Defense Engineering integrates human behavior into cybersecurity processes and workflows. CYBERDISE V3.2 is the first release fully built around this concept.

Zug, Switzerland – June 17, 2026 – CYBERDISE today announced Behavioral Defense Engineering (BDE) and the release of CYBERDISE V3.2, representing the next evolution of cybersecurity attack simulation, threat reporting and incident response.

For more than two decades, cybersecurity awareness has primarily focused on improving knowledge. For CYBERDISE it is proven that the next stage of human cyber defense must focus on improving measurable risk behavior when employees are confronted with real attacks.

or is this better? The launch follows research conducted together with the Lucerne University of Applied Sciences and Arts (HSLU), which confirmed a distinction long observed in practice: improving what employees know is not the same as improving how they behave when confronted with realistic attacks.

CYBERDISE has therefore redesigned its strategic direction and solution around measurable risk behavior. Behavioral Defense Engineering operationalizes human behavior as part of the cybersecurity stack. Instead of treating employees as the weakest link, CYBERDISE transforms human signals into a measurable and adaptive cyber defense intelligence system that strengthens detection, accelerates response and continuously improves organizational resilience.

*“Traditional awareness changes what employees know. Behavioral Defense Engineering changes how employees act. In the age of AI-powered social engineering, knowledge alone is no longer sufficient,” - said **Palo Stacho, Founder of CYBERDISE.** “Modern attacks unfold across multiple channels, and some of the most dangerous ones reach employees before they reach the Security Operations Centre. Organizations need a way to transform human signals into security intelligence and continuously improve risk behavior.”*

CYBERDISE V3.2 introduces multi-channel attack simulations across phishing, smishing, conversational vishing, QR-code attacks, Microsoft Teams scenarios and instant exercise execution based on real threats. The objective is not to run more simulations, but to continuously improve measurable risk behavior and reduce human



attack risk against the social engineering techniques used by modern attackers in the age of AI.

The release also expands AI-powered reconnaissance and personalized Educational Vulnerability Profiles, helping organizations identify behavioral vulnerabilities before attackers exploit them. Cross-platform threat reporting, automated threat analysis and SOC-integrated incident workflows transform human signals into actionable security intelligence and shorten the path from employee report to security response. The option of an on-premises installation remains available.

For enterprises and MSSPs, V3.2 adds expanded automation, multi-directory synchronization, white-labeling and multi-tenant management capabilities designed to reduce operational effort while improving security outcomes.

CYBERDISE will continue to offer a fully functional Freemium edition, reflecting its belief that improving risk behavior should be accessible to organizations of all sizes.

About CYBERDISE

CYBERDISE is a Behavioral Defense Engineering company that helps organizations reduce human cyber risk. Its AI-first solution combines reporting, analysis, attack simulations, training and fast incident response capabilities to improve how people act when facing cyber threats and accelerate the handling of human-originated security incidents. Built on behavioral science and evidence-based cybersecurity research, the platform is designed to measurably improve employee cyber risk behavior. Founded in 2023 and headquartered in Zug, Switzerland, CYBERDISE supports more than 500,000 licensed users worldwide. Further information is available at www.cyberdise.io.

Contact

Palo Stacho
Cyberdise AG
Poststrasse 26, 6300 Zug, Switzerland
+41 41 511 7810
palo.stacho@cyberdise.io

Awareness verhindert keine Angriffe - Verhalten schützt - Geschwindigkeit entscheidet

CYBERDISE stellt Behavioral Defense Engineering und CYBERDISE V3.2 vor

Behavioral Defense Engineering integriert menschliches Verhalten in Cybersecurity Prozesse und Abläufe. CYBERDISE V3.2 ist die erste Version, die vollständig auf diesem Konzept basiert.

Zug, Schweiz – 17. Juni 2026 – CYBERDISE gab heute die Einführung von Behavioral Defense Engineering (BDE) und die Veröffentlichung von CYBERDISE V3.2 bekannt. Es ist die nächste Evolutionsstufe in den Bereichen Cybersecurity, Angriffssimulation, Bedrohungsreporting und Incident Response darstellen. Seit mehr als zwei Jahrzehnten konzentriert sich Security Awareness in erster Linie auf die Verbesserung des Wissens. Für CYBERDISE gilt es als erwiesen, dass sich die nächste Stufe der menschlichen Cyberabwehr und Angriffsprävention darauf konzentrieren muss, das messbare Risikoverhalten zu verbessern, wenn Mitarbeiter mit echten Angriffen konfrontiert werden.

Oder ist das besser? Die Einführung folgt auf eine gemeinsam mit der Hochschule Luzern (HSLU) durchgeführte Studie, die eine in der Praxis seit langem beobachtete Unterscheidung bestätigte: Die Verbesserung des Wissensstands der Mitarbeiter ist nicht gleichbedeutend mit einer Verbesserung ihres Verhaltens, wenn sie mit realistischen Angriffen konfrontiert werden.

CYBERDISE hat daher seine strategische Ausrichtung und seine Lösung auf der Grundlage messbarer Risikoverhaltensweisen neu konzipiert. Behavioral Defense Engineering macht menschliches Verhalten zu einem operativen Bestandteil des Cybersicherheits-Stacks. Anstatt Mitarbeiter als das schwächste Glied zu betrachten, wandelt CYBERDISE menschliche Signale in ein messbares und adaptives Cyber Defense Intelligence System um, das die humane Erkennung verbessert, die Reaktion beschleunigt und die Widerstandsfähigkeit des Unternehmens kontinuierlich stärkt. *„Traditionelle Sensibilisierungsmaßnahmen verändern das Wissen der Mitarbeiter. Behavioral Defense Engineering verändert das Handeln der Mitarbeiter. Im Zeitalter von KI-gestütztem Social Engineering reicht Wissen allein nicht mehr aus“, - so Palo Stacho, Gründer von CYBERDISE. „Moderne Angriffe laufen über mehrere Kanäle, und einige der gefährlichsten erreichen die Mitarbeiter, bevor sie das Security Operations Center erreichen. Unternehmen benötigen eine Möglichkeit, Human Signals in Security Intelligence umzuwandeln und das Risikoverhalten kontinuierlich zu verbessern.“*

CYBERDISE V3.2 führt Mehrkanal-Angriffssimulationen ein, die Phishing, Smishing, Conversational Vishing, QR-Code-Angriffe und Microsoft-Teams-Szenarien abdecken, sowie die sofortige Durchführung von Übungen auf der Grundlage realer Bedrohungen. Das Ziel besteht nicht darin, mehr Simulationen durchzuführen, sondern das messbare Risikoverhalten kontinuierlich zu verbessern und das Risiko menschlicher Angriffe durch Social-Engineering-Techniken zu verringern, die moderne Angreifer im Zeitalter der KI einsetzen.

Die neue Version erweitert zudem die KI-gestützte Aufklärung und personalisierte Schulungs-Schwachstellenprofile, wodurch Unternehmen Schwachstellen beim Verhalten identifizieren können, bevor Angreifer diese ausnutzen.

Plattformüber-greifende Bedrohungsberichte, automatisierte Bedrohungsanalysen und in SOCs integrierte Incident-Workflows wandeln menschliche Signale in verwertbare Cyber Aufklärung um und verkürzen den Weg von der Mitarbeitermeldung bis zum Incident Response. Die Option einer lokalen Installation bleibt weiterhin verfügbar. Für Unternehmen und MSSPs bietet V3.2 erweiterte Automatisierungsfunktionen, Multi-Verzeichnisdienst Synchronisierung, White-Labeling sowie Mehrmandatenmanagement, die darauf ausgelegt sind, den Betriebsaufwand zu reduzieren und gleichzeitig die Sicherheit im System und beim Menschen zu verbessern.

CYBERDISE bietet weiterhin eine voll funktionsfähige Freemium-Edition an. Die Verbesserung des Risikoverhaltens muss für Organisationen jeder Grösse zugänglich sein.

Über CYBERDISE

CYBERDISE ist ein Unternehmen für Behavioral Defense Engineering, das Organisationen dabei unterstützt, durch menschliches Verhalten verursachte Cyberrisiken zu reduzieren. Die AI-first-Lösung kombiniert Incident Reporting, Analyse, Angriffssimulationen, Schulungen und schnelle Reaktionsmöglichkeiten bei Vorfällen, um das Verhalten von Mitarbeitern im Umgang mit Cyberbedrohungen zu verbessern und die Bearbeitung von durch menschliches Verhalten verursachten Sicherheitsvor-fällen zu beschleunigen. Die Lösung basiert auf wissenschaftlicher Evidenz zu menschlichem Verhalten, um das Cyber-Risikoverhalten der Mitarbeitenden messbar zu verbessern. CYBERDISE wurde 2023 gegründet, hat seinen Hauptsitz in Zug, Schweiz, und unterstützt bedient mehr als 500.000 lizenzierte Nutzer. Weitere Informationen finden Sie unter www.cyberdise.io.

Kontakt

Palo Stacho
Cyberdise AG
Poststrasse 26, 6300 Zug, Switzerland
+41 41 511 7810
palo.stacho@cyberdise.io