CYBERDISE Establishes 'Behavioral Defense Engineering' to Combat AI-Driven Threats

A Paradigm Shift in Cybersecurity

ZUG, ZUG, SWITZERLAND, June 23, 2026 /EINPresswire.com/ -- 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.

> Traditional awareness changes knowledge. Behavioral Defense Engineering changes how people act”
>
> *Palo Stacho*

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

Palo Stacho
Cyberdise AG
+41 41 511 78 10
palo.stacho@cyberdise.io
Visit us on social media:
LinkedIn
