# Behavioral Defense Engineering Moves into Enterprise Adoption: CYBERDISE Announces First Adoption Partners and V3.3

*Voith and Teleperformance become first enterprise adoption partners as CYBERDISE V3.3 connects human behavior, security signals and cyber defense*

ZUG, SWITZERLAND, September 28, 2026 /EINPresswire.com/ -- Three months after introducing Behavioral Defense Engineering (BDE), Cyberdise AG is moving the concept into enterprise adoption and operational security. Voith and Teleperformance have become the first adoption partners for CYBERDISE Behavioral Defense Engineering, while CYBERDISE V3.3 expands the technological foundation for connecting employee behavior and human-generated security signals with existing security operations.

> “Security teams already collect enormous amounts of machine-generated telemetry. Human judgement is another source of information.”
>
> *Palo Stacho*

AI is making attacks faster, more personal and harder to detect. Some will inevitably reach employees. At that point, the decisive question is not only what people know, but whether they recognize the attack, react correctly and report it quickly. CYBERDISE uses realistic, personalized exercises to improve this behavior and make employee reports and reactions useful to the SOC.

Voith and Teleperformance Become First BDE Adoption Partners

With Voith and Teleperformance, two large international organizations are becoming the first adoption partners for CYBERDISE Behavioral Defense Engineering.

The partnerships bring real enterprise requirements into the further adoption of BDE, particularly across complex infrastructures, international workforces and existing SOC processes.

“When we introduced Behavioral Defense Engineering in June, our objective was not to create another name for security awareness,” says Palo Stacho, founder of CYBERDISE. “We want to connect human behavior with cyber defense. Voith and Teleperformance give us the opportunity to validate that approach in large, complex enterprise environments.”

The approach is supported by research conducted by CYBERDISE together with the Lucerne University of Applied Sciences and Arts (HSLU), where targeted behavioral interventions improved measurable risk behavior by up to 60%.

CYBERDISE V3.3 Brings Human Signals Closer to Security Operations

The new CYBERDISE V3.3 release strengthens the operational foundation behind BDE. A major addition is the redesigned Direct Message Injection for Microsoft 365, enabling attack-simulation messages to be delivered directly into Microsoft 365 inboxes through Microsoft Graph. This simplifies reliable simulation delivery in enterprise environments.

CYBERDISE has also expanded its phishing-reporting capabilities for Outlook and Gmail. Simulation reports and genuine suspicious messages can be routed differently, allowing employee-generated reports to feed into the appropriate security workflows.

This is central to the BDE approach: an employee reporting something suspicious is not simply completing an awareness exercise. The employee is producing a security signal. “Security teams already collect enormous amounts of machine-generated telemetry,” Stacho adds. “Human judgement is another source of information. Behavioral Defense Engineering is about improving that judgement through realistic exercises and making the resulting signals usable in cyber defense.”

Human Defense Month and it-sa 2026

The V3.3 release coincides with Cybersecurity Awareness Month 2026, which CYBERDISE is supporting through its Human Defense Month initiative. During October, it will provide a free English/German Human Defense Community Kit with editable awareness material, cybersecurity exercises and phishing simulations.

CYBERDISE will also present V3.3 and Behavioral Defense Engineering at it-sa 2026 in Nuremberg, 27–29 October, Hall 7, Booth 301a.

Further information: www.cyberdise.io
CYBERDISE V3.3 Release Notes: https://cyberdise-awareness.com/release-note/
Human Defense Month 2026: https://cyberdise-awareness.com/cybersecurity-awareness-month-kit/

Palo Stacho
Cyberdise AG
+41 41 511 78 10
email us here
Visit us on social media:

LinkedIn
YouTube

---

This press release can be viewed online at: https://www.einpresswire.com/article/945769991

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2026 Newsmatics Inc. All Right Reserved.