Behavioral Defense Engineering in Unternehmen: CYBERDISE gibt erste Implementierungspartner und Version 3.3 bekannt

Voith und Teleperformance sind erste BDE-Einführungspartner. CYBERDISE V3.3 verbindet Mitarbeiterverhalten und Security-Signale mit der Cyberabwehr

ZUG, SWITZERLAND, September 28, 2026 /EINPresswire.com/ -- Drei Monate nach der Einführung von Behavioral Defense Engineering (BDE) bringt Cyberdise AG das Konzept nun in den Einsatz in Unternehmen und in die operative Sicherheit. Voith und Teleperformance sind die ersten Partner für den Einsatz von CYBERDISE Behavioral Defense Engineering, während CYBERDISE V3.3 die technologische Grundlage für die Verknüpfung von Mitarbeiterverhalten und von Menschen generierten Sicherheitssignalen mit bestehendem Security Operations erweitert.

> “Sicherheitsteams sammeln bereits enorme Mengen an maschinengenerierten Telemetriedaten. Das menschliche Urteilsvermögen ist eine unterschätzte Informationsquelle.”
>
> *Palo Stacho*

KI macht Angriffe schneller, persönlicher und schwerer zu erkennen. Einige werden unweigerlich die Mitarbeitenden erreichen. An diesem Punkt ist die entscheidende Frage nicht nur, was die Menschen wissen, sondern ob sie den Angriff erkennen, richtig reagieren und ihn rasch melden. CYBERDISE nutzt realistische, personalisierte Übungen, um dieses Verhalten zu verbessern und die Meldungen und Reaktionen der Mitarbeitenden für das SOC nutzbar zu machen.

Voith und Teleperformance werden erste BDE-Einführungspartner

Mit Voith und Teleperformance werden zwei grosse internationale Unternehmen zu den ersten Einführungspartnern für CYBERDISE Behavioral Defense Engineering.

Die Partnerschaften bringen reale Unternehmensanforderungen in die weitere Einführung von BDE ein, insbesondere in Bezug auf komplexe Infrastrukturen, internationale Belegschaften und bestehende SOC-Prozesse.

«Als wir im Juni Behavioral Defense Engineering eingeführt haben, war es nicht unser Ziel, einen weiteren Begriff für Sicherheitsbewusstsein zu schaffen», sagt Palo Stacho, Gründer von CYBERDISE. «Wir wollen menschliches Verhalten mit Security-Operations / Cyberabwehr

verbinden. Voith und Teleperformance geben uns die Möglichkeit, diesen Ansatz in grossen, komplexen Unternehmensumgebungen zu validieren.»

Der Ansatz stützt sich auf Forschungsergebnisse, die CYBERDISE gemeinsam mit der Hochschule Luzern (HSLU) erarbeitet hat. Dort konnten gezielte Verhaltensinterventionen das messbare Risikoverhalten um bis zu 60 % verbessern.
CYBERDISE V3.3 integriert menschliche Signale direkt in die Security Operations
Die neue Version CYBERDISE V3.3 stärkt die operative Grundlage von BDE. Eine wichtige Neuerung ist die überarbeitete Funktion «Direct Message Injection» für Microsoft 365, mit der Nachrichten zur Angriffssimulation über Microsoft Graph direkt in die Posteingänge von Microsoft 365 zugestellt werden können. Dies vereinfacht insbesondere die zuverlässige Zustellung von Simulationen in Unternehmensumgebungen.

CYBERDISE hat zudem seine Funktionen zur Phishing-Meldung/Reporting für Outlook und Gmail erweitert. Simulationsberichte und echte verdächtige Nachrichten können unterschiedlich weitergeleitet werden, sodass von Mitarbeitenden erstellte Meldungen in die entsprechenden Sicherheitsworkflows einfliessen können.
Dies ist zentral für den BDE-Ansatz: Ein Mitarbeiter, der etwas Verdächtiges meldet, absolviert nicht einfach nur eine Sensibilisierungsübung. Der Mitarbeiter erzeugt ein Securitysignal. «Sicherheitsteams sammeln bereits enorme Mengen an maschinengenerierten Telemetriedaten», fügt Stacho hinzu. «Das menschliche Urteilsvermögen ist eine unterschätzte Informationsquelle. Bei Behavioral Defense Engineering geht es darum, dieses Urteilsvermögen durch realistische Übungen zu verbessern und die daraus resultierenden Signale für die Cyberabwehr nutzbar zu machen.»

Human Defense Month und it-sa 2026
Die Veröffentlichung der Version V3.3 fällt mit dem Cybersecurity Awareness Month 2026 zusammen, den CYBERDISE im Rahmen seiner Initiative «Human Defense Month» unterstützt. Im Oktober stellt das Unternehmen ein kostenloses «Human Defense Community Kit» in Deutsch und Englisch zur Verfügung, welches editierbare Sensibilisierungsmaterialien, Cybersicherheitsübungen und Phishing-Simulationen enthält.
CYBERDISE wird ausserdem V3.3 und Behavioral Defense Engineering an der it-sa 2026 in Nürnberg vom 27. bis 29. Oktober in Halle 7, Stand 301a, vorstellen.

Weitere Informationen: 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/945767494

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.