

PRESSEMITTEILUNG – ZUR SOFORTIGEN VERÖFFENTLICHUNG

Wer in Ihrem Unternehmen ist qualifiziert, Ihre KI zu sichern?

EXIN führt die Zertifizierung „AI Security Professional“ ein, die auf dem OWASP AI Exchange basiert – und damit Kompetenzen im Bereich KI-Sicherheit transparent und überprüfbar macht.

UTRECHT, Niederlande — 3. September 2026 — Die meisten Unternehmen führen KI schneller ein, als sie sie absichern können. Jedes Modell, jeder Assistent und jeder automatisierte Arbeitsablauf, der in den Produktivbetrieb überführt wird, vergrößert die Angriffsfläche und kann zu einem zusätzlichen Risiko für Sicherheitsverletzungen und Verstöße gegen das EU-KI-Gesetz führen. Nur wenige Unternehmen können anhand von Belegen darlegen, welche ihrer Mitarbeiter in der Lage sind, dieses Risiko zu bewältigen.

[EXIN](#), die globale unabhängige Zertifizierungsstelle, die bereits mehr als drei Millionen Zertifizierungen in 170+ Ländern ausgestellt hat, führt heute die neueste Ergänzung ihres KI-Portfolios ein: den „[AI Security Professional](#)“ (AISP). AISP schließt diese Lücke. Die Zertifizierung belegt, dass eine Person beide Aspekte der Aufgabe bewältigen kann: zu erkennen, wie KI-Systeme tatsächlich angegriffen werden, und deren Nutzung gemäß den Standards zu steuern, die Regulierungsbehörden mittlerweile erwarten.

Bestehende Sicherheitszertifizierungen stammen aus einer Zeit vor KI-spezifischen Bedrohungen. Governance-Rahmenwerke gehen nicht bis zur Umsetzung. AISP deckt sowohl technische Aspekte als auch Governance ab, und zwar ohne Voraussetzungen – bewusst, damit es die Sicherheitsbeauftragten, Datenschutzbeauftragten, Risikoanalysten und KI-Ingenieure erreicht, die diese Verantwortung bereits tragen.

„KI hat die Bedeutung von digitaler Kompetenz verändert“, sagte Valérie Hoeks, CEO von EXIN. „Jedes KI-System, das ein Unternehmen einsetzt, vergrößert dessen Angriffsfläche, und die Kosten für Fehler zeigen sich in der Behebung, in verlorenen Aufträgen und in einem Vertrauensverlust. Vorstände genehmigen KI-Investitionen, für deren Umsetzung sie noch nicht mit Zuversicht Personal bereitstellen können. AISP gibt ihnen die Möglichkeit, zu sehen – statt nur zu hoffen –, dass die richtigen Kompetenzen vorhanden sind.“

AISP basiert auf dem [OWASP AI Exchange](#), dem offenen KI-Sicherheitswissensbestand, der von mehr als 165 Praktikern entwickelt wurde und sowohl in die Norm ISO/IEC 27090 als auch in den Sicherheitsstandard des EU-KI-Gesetzes (pr-EN 18282) einfließt. Die Kursunterlagen wurden von dem Gründer [Rob van der Veer](#), Chief AI Officer bei der [Software Improvement Group](#), entwickelt.

„Das für die Absicherung von KI erforderliche Wissen existiert bereits (von OWASP) und steht jedem kostenlos zur Verfügung“, sagte van der Veer. „Was bisher fehlte, war eine Möglichkeit für den Einzelnen, nachzuweisen, dass er dieses Wissen beherrscht. Diese Lücke schließt die Zertifizierung. Das Wissen ist offen zugänglich. Die Fachkompetenz ist nun überprüfbar.“

AISP ist die einzige KI-Sicherheitszertifizierung, die auf den europäischen CEN-Standard für Berufsrollenprofile im KI-Bereich (CEN CWA 18398) abgestimmt ist. Prüfungsformat: keine Voraussetzungen. Die Prüfung ist online und über unsere akkreditierten Schulungsanbieter weltweit verfügbar. Erfolgreiche Teilnehmer erhalten das folgende Zertifikat und ein digitales Abzeichen: „**EXIN AI Security Professional based on the OWASP AI Exchange**“.

Die Prüfung zum „AI Security Professional“ ist ab sofort unter aisp.exin.com sowie über das globale Netzwerk akkreditierter Schulungsanbieter von EXIN verfügbar. Der OWASP AI Exchange ist weiterhin kostenlos unter owaspai.org verfügbar.

OWASP unterstützt keine bestimmten Zertifizierungsanbieter. EXIN AISP wurde von EXIN eigenständig entwickelt und baut auf dem Wissensbestand des OWASP AI Exchange auf, wobei OWASP darüber informiert wurde.

Medienkontakt

Bessie Schenk, EXIN
bessie.schenk@exin.com
+31 302 344 880

AISP Microsite: aisp.exin.com
Pressemappe: exin.com/aisp-media

Über EXIN

Seit 1984 ist EXIN eine unabhängige Zertifizierungsstelle, die in 170+ Ländern mehr als drei Millionen Zertifizierungen ausgestellt hat. Das KI-Portfolio des Unternehmens umfasst die Bereiche Sicherheit, Governance und Implementierung und ergänzt ein etabliertes Portfolio an digitalen Kompetenzen in den Bereichen Informationssicherheit, Datenschutz und Servicemanagement. KI-Kompetenzen sind ohne diese Grundlagen unvollständig, und EXIN zertifiziert beides. exin.com

Über die Software Improvement Group (SIG)

Die im Jahr 2000 gegründete Software Improvement Group (SIG) unterstützt Unternehmen dabei, die Software, auf der ihr Geschäft basiert, zu steuern. Durch umfassende Portfolioanalysen und maßgeschneiderte strategische Beratung unterstützt SIG Unternehmen dabei, KI kontrolliert einzuführen und die Softwarequalität sowie -sicherheit zu verbessern, indem strategische Anstrengungen auf Menschen, Prozesse und Technologie ausgerichtet werden. SIG wurde im Gartner Magic Quadrant™ 2026 für Technical-Debt-Management-Tools als „Leader“ ausgezeichnet. softwareimprovementgroup.com

###