02.06.2026 – 09:57 Uhr

TrendAI startet Inception-Programm zur Unterstützung von KI-Startups bei Sicherheit und Skalierung

TrendAI startet Inception-Programm zur Unterstützung von KI-Startups bei Sicherheit und Skalierung

Gemeinsam mit AWS, GMI Cloud und Partnern aus dem KI-Startup-Ökosystem sollen Sicherheitsanforderungen frühzeitig in die Entwicklung von KI-Produkten integriert werden

Wallisellen, 02. Juni 2026 – TrendAI™, der Enterprise-Cybersecurity-Geschäftsbereich von Trend Micro, lanciert eine Initiative, die KI-Lösungsanbieter dabei unterstützt, sichere KI nach dem Secure-by-Design-Prinzip schneller zu entwickeln, zu validieren und auf den Markt zu bringen. Das Programm vereint Expertise in KI-Sicherheit, technisches Enablement und Go-to-Market-Unterstützung und hilft Partnern so, ihr Tempo sicher zu erhöhen, ohne dafür eigenständig tiefgreifendes Security-Know-how aufbauen zu müssen.

KI-Startups sind bekannt für schnelle Innovation – doch Enterprise-Kunden treffen ihre Kaufentscheidungen auf Basis von Vertrauen, Governance und Sicherheitsreife. Das Programm zielt darauf ab, neue KI-Anbieter dabei zu unterstützen, die Reife ihrer Produkte frühzeitig über den gesamten KI-Stack hinweg zu stärken – einschliesslich Modellen, Pipelines, Agenten und Daten. Konkret umfasst das Angebot technisches Enablement, KI-Sicherheitsvorteile sowie partnerorientierte Leistungen:

- **AI Red Teaming oder Purple Teaming Service** (zu Sonderkonditionen für Partner): TrendAI-Cybersecurity-Experten validieren die Resilienz der KI-Anwendung gegenüber Prompt Injection, Jailbreak, System Prompt Leakage und Tool-Abuse-Szenarien – gemessen an den Frameworks OWASP LLM Top 10 und MITRE ATLAS

und dokumentiert in Validierungsberichten. So gelangen Lösungen mit nachgewiesener Sicherheit auf den Markt.

- **Kostenlose Credits**: Sechs Monate kostenfreier Zugang zu TrendAI Vision One™ AI Security für Tests und Validierungen in der Entwicklungs- oder PoC-Umgebung.
- **Integration und Enablement**: Referenzarchitekturen, SDKs/APIs sowie Integrationsbeispiele, abgestimmt auf gängige KI-Entwicklungs-Frameworks.
- **Security-Assets für die Kundenansprache**: Whitepaper und Solution Briefs, die dabei helfen, den Mehrwert von KI-Sicherheit gegenüber Kunden klar zu kommunizieren.
- **AI-Security-Beratung und -Mentorship**: Strukturierte Schulungen und Expertenberatung zu Best Practices der KI-Sicherheit, Bedrohungsszenarien und Implementierungsempfehlungen für Entwicklungsteams.
- **Co-Marketing und Kundensichtbarkeit**: Gemeinsame Auftritte auf den TrendAI Spark Events sowie Listung im TrendAI Partner Locator, um neue Kundengruppen zu erschliessen, die gezielt nach qualifizierten KI-Partnern suchen.

„KI gelangt schneller in den produktiven Einsatz, als die meisten Unternehmen in der Lage sind, sie abzusichern. Gleichzeitig wächst mit dem Kundeninteresse auch die Aufmerksamkeit der Angreifer“, erklärt Rachel Jin, Chief Platform and Business Officer bei TrendAI. „Vielen KI-Entwicklern fehlen dedizierte Sicherheitsteams oder die Erfahrung, KI-Systeme in grossem Massstab zu schützen. Wir stellen unsere langjährige Expertise zur Verfügung, um diesen Unternehmen zu helfen, sichere und vertrauenswürdige KI-Lösungen schneller auf den Markt zu bringen. So werden aus Innovationen belastbare, Enterprise-taugliche Lösungen.“

TrendAI-Partner wie GMI Cloud entwickeln und betreiben Plattformen, die die nächste Welle KI-gestützter Innovation tragen sollen. Das Inception-Programm entstand als unmittelbare Reaktion auf die Nachfrage von KI-Startups, die eine unabhängige Sicherheitsvalidierung benötigen, um ihren Markteintritt im Enterprise-Umfeld zu beschleunigen.

Als Teil von TrendAI Vision One™ AI Security erhalten Partner des Inception-Programms Zugang zu einem AI-Security-Paket, das unter anderem Daten- und Security-Posture-Management, Echtzeit-Scanning-Tools, Secure Access sowie ein agentenbasiertes SIEM umfasst.

„Während Unternehmen KI von der Experimentierphase in den breiten Produktiveinsatz überführen, rückt Sicherheit als kritischer Bestandteil des KI-Infrastruktur-Stacks in den Mittelpunkt“, betont Alex Yeh, Gründer & CEO von GMI Cloud. „Bei GMI Cloud liegt unser Fokus auf skalierbarer KI-Infrastruktur und Inferenz-Plattformen für den realen Einsatz in Unternehmen. Zugleich ist uns bewusst, dass KI neue Angriffsflächen über Modelle, Agenten, Daten-Pipelines und Inferenz-Workflows hinweg eröffnet. Über das Inception-Programm verknüpfen wir skalierbare KI-Infrastruktur mit der jahrzehntelangen Cybersecurity-Expertise von TrendAI und helfen Kunden so, KI mit mehr Vertrauen, Governance und operativer Sicherheit einzusetzen. Das Ergebnis sind sicherere, skalierbare und Enterprise-taugliche KI-Deployments.“

„Cybersicherheit ist bei Ontonics Lab kein nachgelagertes Thema, sondern ein fundamentaler Bestandteil unserer Produktphilosophie. Als KI-native Plattform für industrielle Unternehmen müssen wir vom ersten Tag an höchste Standards in puncto Sicherheit, Zuverlässigkeit und Vertrauen erfüllen“, sagt Robin Wong, COO von Ontonics Lab, einem KI-nativen Startup für Industrial Intelligence, das von der LCY Group und Eternal Materials unterstützt wird. „Die Purple-Teaming-Experten von TrendAI helfen uns, unsere Architektur zu validieren, bislang unentdeckte Schwachstellen aufzudecken und unsere Plattform vor dem Launch zu härten. Diese unabhängige Validierung stärkt das Vertrauen unserer Kunden und verschafft uns einen klaren Wettbewerbsvorteil, während wir KI-native Lösungen für industrielle Unternehmen einführen.“

Weitere Informationen

Weitere Informationen zum TrendAI™ Inception-Programm finden Sie unter:
https://resources.trendmicro.com/TrendAI-Inception-Partner-Program.html

Pressestelle TrendAI™
c/o BRAND AFFAIRS AG

Mischa Keller / MSc Business Administration
Partner

Telefon: +41 44 254 80 00
E-Mail: trendmicro-media@brandaffairs.ch
Mühlebachstrasse 8 / 8008 Zürich / Switzerland

Medieninhalte

Diese Meldung kann unter https://www.presseportal.ch/de/pm/100103176/100940432 abgerufen werden.