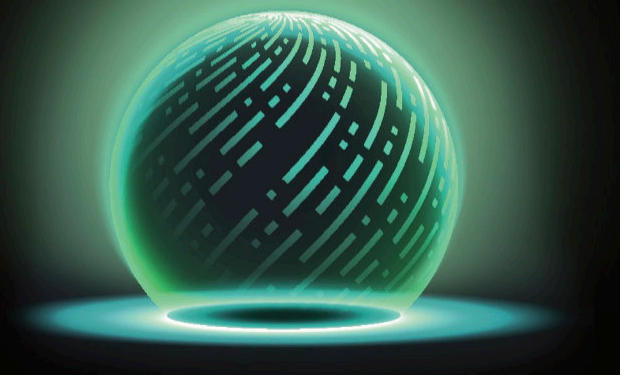
Außergewöhnliche E-Mail Sicherheit

/LIBRAESVA

Semantische KI: E-Mail Verteidigung mit Fokus auf Datenschutz

Weil die heutigen E-Mail Bedrohungen nicht mehr wie Bedrohungen aussehen.



Die heutigen E-Mail-Bedrohungen sind so raffiniert, dass sie nicht mehr wie Bedrohungen aussehen. Angreifer verwenden zunehmend gut geschriebene, gut formatierte E-Mails, die oft von künstlicher Intelligenz erstellt wurden, um herkömmliche Filter zu umgehen. Diese Nachrichten enthalten selten bekannte bösartige Signaturen oder offensichtliche Warnsignale, die eine regelbasierte Abwehr auslösen.

Semantische KI löst dieses Problem, indem sie über Schlüsselwörter, Links und den Absenderverlauf hinausgeht. Sie analysiert die tatsächliche Bedeutung und Logik innerhalb von Nachrichten, um Ungereimtheiten und absichtsbedingte Anomalien zu erkennen – selbst wenn alles andere legitim erscheint.

Semantic AI ist Libraesvas „Small Language Model" (SLM)-basierte Engine der nächsten Generation, die tiefgehende, kontextbezogene E-Mail-Bedrohungen ohne Beeinträchtigung des Datenschutzes erkennt. Sie läuft lokal auf Ihrer vorhandenen Hardware – keine Cloud, kein Daten-Offshoring, keine KI-APIs von Dritten.

- ☑ **Erkennt, was andere übersehen**: Unerwartete Anbietemamen, unpassende Töne oder unlogische Anfragen – in ansonsten einwandfreien E-Mails.
- ☑ **Day-Zero-Erkennung**: Fängt anspruchsvolle Bedrohungen ab, bevor Signaturen oder Heuristiken aktualisiert werden.
- ☑ **Erhöht die Entscheidungssicherheit**: Deterministische Ausgaben gewährleisten konsistente Ergebnisse – die gleiche Nachricht führt immer zum gleichen Ergebnis.
- ☑ **Schutz ohne Kompromisse:** Der Datenschutz steht im Vordergrund – keine Cloud, kein Offloading, keine gemeinsame Nutzung von Daten durch Dritte.
- ☑ **Funktioniert dort, wo es darauf ankommt:** Aktiviert sich nur bei Nachrichten, die von der Adaptive Trust Engine gekennzeichnet sind, und bietet so Erkennungstiefe ohne Datenabfluss.

DATENSCHUTZ DURCH DESIGN

- Keine Cloud-Verarbeitung / Auslagerung von Daten
- Kein Modelltraining mit Kundendaten
- Keine KI-APIs / Abhängigkeit von Drittanbietern
- Vollständige Ausführung / Datenkontrolle vor Ort
- 100%ige Konformität mit lokalen Datenschutzrichtlinien

HIGHLIGHTS DER KERNTECHNOLOGIE

- Diskriminierende KI: Deterministische Ergebnisse, null Entropie, Konsitenz
- Kontextbezogene Analyse: Erkennung von Anomalien in Bedeutung, Logik und Absicht
- Leichtgewichtiges SLM: Model mit 100 Mio. Parametern, trainiert auf kuratierte E-Mail Bedrohungen
- CPU-Optimiert: Läuft auf Standard-Hardware mit <1s Verzögerung
- Ergänzt bestehende Schutzmaßnahmen (ATE, Regeln, Sandboxing, AV)
- Arbeitet parallel zur Adaptiven Trust Engine (ATE), um die Ermüdung durch häufige Alarme zu verringern

Geben Sie Ihrem Sicherheits-Stack die Fähigkeit, die Absichten zu verstehen – nicht nur die Struktur. Sie erhalten sicherere Posteingänge, intelligentere Erkennung und einen Schutz, der sich an das tatsächliche Verhalten von Bedrohungen anpasst.

Bereit für den Start?

sales@libraesva.com

www.libraesva.com

Libraesva ist ein preisgekröntes Unternehmen für E-Mail-Sicherheit und wurde von GetApp, einem Gartner-Unternehmen, als Branchenführer im Bereich E-Mail-Sicherheit sowie vom Frost Radar als Innovationsführer ausgezeichnet. Libraesva wird von Virus Bulletin regelmäßig als eines der besten E-Mail-Sicherheitssysteme zertifiziert und genießt das Vertrauen führender Marken weltweit.

/LIBRAESVA

EmailSecurity