Information Security Manager:in (m/w/x)

LATIDO entwickelt die führende digitale Praxislösung für Wahlärzt:innen und Therapeut:innen in Österreich. Über 3.100 Ärzt:innen arbeiten täglich mit unserer Software – wir sind Marktführer in diesem Bereich.

Als Health-Tech-Unternehmen verarbeiten wir täglich sensible Patientendaten. Informationssicherheit ist für uns kein Compliance-Thema, sondern ein zentrales Qualitätsmerkmal – gegenüber unseren Kund:innen, gegenüber Regulatoren und gegenüber uns selbst.

Zur Verstärkung unseres Teams suchen wir eine:n Information Security Manager:in, der/die operative Security-Verantwortung übernimmt, konkrete Maßnahmen umsetzt und unsere Entwicklungs- und IT-Prozesse nachhaltig härtet.

Deine Aufgaben

- **Security Monitoring:** Laufendes Monitoring relevanter Schwachstellen, Advisories und Angriffstrends – und Ableitung konkreter Maßnahmen für Prozesse, Applikationen und Code
- **Ownership:** Verantwortung für die laufende Verbesserung der Informations- und IT-Sicherheit im Unternehmen
- **Audits & Pentests:** Steuerung, Begleitung und Nachverfolgung von Security-Audits und technischen Pentests inkl. Behebungsmaßnahmen
- **Architektur & Design:** Durchführung von Architektur-Reviews mit Fokus auf Security, Datenschutz (DSGVO/GTelG), Zugriffskonzepte und sichere Systemintegration
- **Secure Development:** Etablierung von Security in Entwicklungsprozessen – GitLab, CI/CD-Pipelines, Dependency Scanning, Secret Detection, SAST/DAST – sowie Begleitung von Code-Reviews mit Security-Fokus
- **Tooling & Infrastruktur:** Bewertung und Absicherung interner Tooling-Landschaften (ERP, Odoo, Eigenentwicklungen, SaaS-Tools, Admin-Portale) sowie Security-Design für unsere Cloud-/Kubernetes-Infrastruktur
- **Prozesse & Standards:** Definition und Verbesserung sicherheitskritischer Prozesse wie MFA-Reset, Onboarding/Offboarding, Rechtevergabe und Incident Handling
- **NIS2 & ISO 27001:** Strategisches und operatives Mitwirken bei der Herstellung von ISO- & NIS 2-Readiness
- **Risikobewertung:** Bewertung sicherheitsrelevanter Anforderungen bei der Integration externer Dienstleister, neuer Schnittstellen und sensibler Datenflüsse
- **Beratung & Umsetzung:** Beratung von Management, IT, Entwicklung sowie GTM bei sicherheitsrelevanten Entscheidungen – und aktive Mitarbeit bei der Implementierung technischer Maßnahmen

Dein Profil

- **Erfahrung:** Mehrjährige Berufserfahrung in IT-Security, Application Security, DevSecOps, Cloud-Architektur oder Software Engineering – du hast Security-Maßnahmen bereits in produktiven Umgebungen verantwortet und umgesetzt.
- **Technisches Fundament:** Du verstehst moderne Softwarearchitekturen, APIs, Authentifizierungs- und Berechtigungskonzepte. Praxis mit Infrastructure as Code, CI/CD-Security, Threat Modelling und technischem Schwachstellenmanagement ist ein klares Plus.
- **Pragmatisch & strukturiert:** Du bewertest Risiken strukturiert, priorisierst sinnvoll und etablierst daraus pragmatische Standards und Kontrollmechanismen – ohne die Entwicklungsgeschwindigkeit unnötig zu bremsen.
- **Kommunikationsstärke:** Du trittst sicher gegenüber Management, Entwicklung und externen Dienstleistern auf und kannst Security-Themen verständlich vermitteln.
- **Security Mindset:** Du hinterfragst digitale Risiken, gehst bewusst mit Daten und Zugängen um und willst Systeme nicht nur funktional, sondern nachhaltig sicher gestalten.
- **Selbstständig & hands-on:** Du arbeitest eigenverantwortlich, treibst Themen aktiv voran und schreckst nicht davor zurück, selbst mit anzupacken.
- **Sprache:** Fließende Deutschkenntnisse in Wort und Schrift; Englisch für technische Dokumentation und Vendor-Kommunikation.

Das erwartet dich bei uns

- **Impact:** Eine zentrale Security-Rolle mit direktem Einfluss auf Architektur, Entwicklung und Betrieb – in einem Unternehmen, das sensible Gesundheitsdaten schützt.
- **Gestaltungsspielraum:** Du baust Security-Prozesse und -Standards von Grund auf mit – mit kurzen Entscheidungswegen und direktem Zugang zur Geschäftsführung.
- **Team:** Ein technisch starkes, wertschätzendes Team aus Entwicklung und Product, das Security als gemeinsame Aufgabe versteht.
- **Flexibilität:** Moderner Arbeitsplatz im Zentrum Wiens (1010) mit gelebter Teamkultur vor Ort und der Option auf Homeoffice-Tage.
- **Benefits:** Essenszuschuss, Öffi-Ticket, Teamevents u. v. m.

Gehalt

Für diese Position bieten wir dir ein attraktives Grundgehalt ab EUR 70.000 brutto/Jahr (Überzahlung je nach Qualifikation & Erfahrung möglich).

Interesse?

Du willst Informationssicherheit bei Österreichs führender Praxissoftware aktiv gestalten? Dann freuen wir uns auf deine Bewerbung an recruiting@latido.at – wir sind gespannt auf dich!