Whitepaper zur Sicherheit

www.insights.com

Insights hat in eine umfassende Neugestaltung seiner Technologieplattformen investiert, wobei der Schwerpunkt auf Sicherheit und Compliance liegt. Die neue Kundenplattform, die nächste Generation von Insights Online, konzentriert sich auf eine verbesserte Benutzerfreundlichkeit und - was noch wichtiger ist - auf robuste, in das System integrierte Sicherheitsmaßnahmen. Unsere Kundenanwendungen wurden unter Verwendung sicherer Kodierungspraktiken, eines sicheren Entwicklungslebenszyklus und sicherheitstechnischer Grundsätze, einschließlich Maßnahmen wie Verschlüsselung und Multi-Faktor-Authentifizierung, neu entwickelt. Dieser datenschutz- und sicherheitsorientierte Ansatz erstreckt sich auch auf unsere unterstützende Infrastruktur.
Wir legen großen Wert auf das Feedback der Nutzer und haben die Erkenntnisse unserer Kunden in den Entwicklungsprozess einfließen lassen. Mit Blick auf die Zukunft verpflichten wir uns zu kontinuierlichen Verbesserungen und Aktualisierungen, um sicherzustellen, dass unsere Plattform sicher und beschwerdefrei bleibt und den Branchenstandards entspricht.

ISO 27001:2022 Zertifizierung
Seit dieser Umstrukturierung hat Insights die Zertifizierung nach ISO 27001:2022 erfolgreich abgeschlossen. Diese prestigeträchtige Zertifizierung ist ein Beweis für unser Engagement, die höchsten Standards der Informationssicherheit aufrechtzuerhalten.

Warum ist die Zertifizierung nach ISO 27001:2022 so wichtig?
ISO 27001:2022 ist eine international anerkannte Norm für Informationssicherheitsmanagementsysteme (ISMS). Das Erreichen dieser Zertifizierung zeigt, dass unsere Organisation einen robusten Rahmen für die Verwaltung und den Schutz sensibler Informationen eingeführt hat. Sie beinhaltet eine strenge Bewertung und kontinuierliche Verbesserung unserer Sicherheitspraktiken und stellt sicher, dass wir Risiken effektiv identifizieren, verwalten und abmildern.

Was bedeutet das für unsere Kunden?
Ein nach ISO 27001:2022 zertifiziertes Unternehmen bietet mehrere wichtige Vorteile:

- **Verbessertes Vertrauen und Zuversicht:** Die Kunden können sich darauf verlassen, dass ihre Daten mit äußerster Sorgfalt und Sicherheit behandelt werden, wodurch das Risiko von Datenschutzverletzungen und Cyber-Bedrohungen verringert wird.
- **Einhaltung von Vorschriften:** Viele Branchen verlangen die Einhaltung bestimmter Sicherheitsstandards. Unsere ISO 27001:2022-Zertifizierung hilft unseren Kunden, diese gesetzlichen Anforderungen zu erfüllen.
- **Risikomanagement:** Die Zertifizierung bedeutet, dass wir einen proaktiven Ansatz zur Identifizierung und Bewältigung potenzieller Sicherheitsrisiken verfolgen, der die Kontinuität und Widerstandsfähigkeit des Unternehmens gewährleistet.
- **Wettbewerbsvorteil:** Die Zusammenarbeit mit einem zertifizierten Unternehmen kann Ihren Ruf verbessern und Ihnen einen Wettbewerbsvorteil auf dem Markt verschaffen, da es Ihr Engagement für bewährte Verfahren im Bereich der Informationssicherheit widerspiegelt.
- **Kontinuierliche Verbesserung:** Der Rahmen von ISO 27001:2022 fördert die kontinuierliche Bewertung und Verbesserung von Sicherheitsmaßnahmen, um sicherzustellen, dass wir neuen Bedrohungen und Schwachstellen immer einen Schritt voraus sind.

Mit der Zertifizierung nach ISO 27001:2022 demonstriert Insights sein Engagement für den Schutz von Kundendaten und die Bereitstellung einer sicheren Umgebung für alle Geschäftsabläufe.

Wie gehen wir bei Penetrationstests vor?
Insights ist bestrebt, seinen Kunden sichere Lösungen zu bieten. Wir führen regelmäßig Penetrationstests für unsere Anwendungen mit einem von CREST zugelassenen Drittanbieter durch. Außerdem wenden wir bei diesen Tests die richtigen Sicherheitsgrundsätze an.

Die neueste Neukundenplattform wurde einem externen Penetrationstest für Webanwendungen unterzogen und wies NULL Schwachstellen auf.

Highlights der Sicherheit

Nachstehend finden Sie die wichtigsten Sicherheitsmerkmale, die wir implementiert haben, um unseren Kunden ein Höchstmaß an Schutz zu bieten:

Zugangskontrolle und Authentifizierung

Null Vertrauen
Zero Trust ist ein Sicherheitsrahmen, der vorschreibt, dass alle Nutzer, ob innerhalb oder außerhalb des Insights-Netzwerks, authentifiziert, autorisiert und fortlaufend auf Sicherheitskonfiguration und -zustand überprüft werden müssen, bevor sie Zugang zur Neukundenplattform erhalten oder behalten. Dieser Ansatz entspricht den Kontrollzielen der Norm ISO 27001:2022, einschließlich der Zugriffskontrolle und der privilegierten Zugriffsrechte, um den "am wenigsten privilegierten" Zugriff sicherzustellen.

Einmalige Wertmarke
Der One Time Token verhindert Identitätsdiebstahl, indem er sicherstellt, dass eine erfasste E-Mail-Adresse nicht wiederverwendet werden kann, so dass keine Benutzernamen und Passwörter gespeichert werden müssen.

Einzelanmeldung
Single Sign-On (SSO) ermöglicht es den Kunden, ihre eigenen Identitätsanbieter zu verwenden, um ihre Benutzer innerhalb der Anwendung zu sichern, wobei alle Sicherheitsmaßnahmen an die eigenen Systeme der Organisationen weitergegeben werden.

Netz- und Infrastruktursicherheit

Grundsatz des geringsten Rechtsanspruchs
Dieser Grundsatz stellt sicher, dass Mitarbeiter, Systeme und Anwendungen **nur** den Zugang erhalten, den sie zur Erfüllung ihrer Aufgaben und Verantwortlichkeiten benötigen. Die Zugriffsrechte werden sorgfältig festgelegt, um sie mit den betrieblichen Erfordernissen und den Sicherheitsrichtlinien in Einklang zu bringen.

Keine öffentliche IP
Die Insights-Server haben keine direkte Verbindung zum Internet und bieten eine Sicherheitslösung, die vor externen Bedrohungen schützt. Der Datenverkehr wird über einen ausgehenden Proxy geleitet, der eine Whitelist der zulässigen Domänen enthält.

Anwendungslastausgleicher
Unsere Anwendung Load Balancers verwaltet den Internetverkehr und fungiert als Barriere zwischen dem Internet und den Servern. Er stellt sicher, dass nur zulässiger Verkehr mit dem Insights-Portal kommunizieren kann und verwendet immer die neuesten Sicherheits-SSL/TLS-Chiffren und -Protokolle.

Überwachung und Zurückweisung von verdächtigem Verkehr
Der gesamte eingehende HTTP-Datenverkehr durchläuft eine Web Application Firewall (WAF). Verdächtiger Datenverkehr wird automatisch zurückgewiesen, und unser Technologie-Team wird benachrichtigt, um ihn zu untersuchen, was ein proaktives Bedrohungsmanagement gewährleistet.

Schnelle Software-Patch-Verwaltung
Alle unsere Infrastruktur- und Anwendungs-Hosting-Umgebungen werden alle 24 Stunden mit den neuesten Versionen von Betriebssystemen und Anwendungen aktualisiert, um sicherzustellen, dass die neuesten Sicherheits-Patches angewendet werden, um die Einhaltung der neuesten Sicherheitsstandards zu gewährleisten und vor neuen Bedrohungen zu schützen.

Datenverschlüsselung
Alle in unseren Datenbanken gespeicherten Daten werden mit dem branchenüblichen Verschlüsselungsalgorithmus AES-256 verschlüsselt. Dadurch wird sichergestellt, dass die Daten auch bei unbefugtem Zugriff nicht gelesen oder manipuliert werden können.

Daten im Transit
Die zwischen Datenbanken und Anwendungen ausgetauschten Daten werden durch Transport Layer Security (TLS)-Protokolle geschützt. Dadurch werden die Daten während der Übertragung verschlüsselt und gegen Abfangen und Abhören geschützt.

Entwicklung und betriebliche Sicherheit

Sicher durch Design
Unser Secure by Design-Ansatz stellt sicher, dass die Insights-Entwicklungsteams das Cybersicherheitsrisiko vom Konzept bis zur Produktion selbst in der Hand haben und es während des gesamten Lebenszyklus effektiv verwalten. Dies führt zur Bereitstellung eines sicheren Produkts durch klarere Verantwortlichkeiten, vereinfachte Prozesse und die Einhaltung von Sicherheitsstandards.

System-Block-Modus
Unsere Systeme sperren standardmäßig alle Anwendungen und Benutzer und erlauben den Zugriff nur denjenigen, die in den Sicherheitsrichtlinien angegeben sind. Diese Richtlinien legen die Berechtigungen für jeden Benutzer, jeden Prozess und jede Ressource fest.

Trennung der Server-Rollen
Die Server haben getrennte Rollen, so dass sich die Auswirkungen einer Systemverletzung auf einen einzigen Teil des Produkts beschränken.

Trennung der Daten von Evaluatoren und Lernenden
Die Forschungsdaten der Evaluatoren werden anonymisiert und getrennt von den Daten der Lernenden gespeichert, so dass der Datenschutz und die Sicherheit für beide Arten von Informationen gewährleistet sind.

Gehärtete Client- und Server-Verschlüsselung
Alle Webanwendungen werden unter Verwendung von TLS 1.2/1.3 und HTTP/2/3 bereitgestellt, was zu einer A+-Bewertung von SSL Labs führt. Dies gewährleistet eine zuverlässige Verschlüsselung und sichere Kommunikation.

Umfassende Prüfpfade
Alle technologischen Änderungen werden mit einem umfassenden Prüfpfad versehen und erfordern ein Genehmigungsverfahren, das die Verantwortlichkeit und Nachvollziehbarkeit gewährleistet.

Prüfung der Kundeninteraktion
Alle Kundeninteraktionen werden auditiert, so dass wir auf Anfrage jeden Datenmissbrauch gezielt nachweisen können.

Ratenbegrenzung
Die Ratenbegrenzung begrenzt, wie oft Aktionen innerhalb eines bestimmten Zeitraums wiederholt werden können, und hilft so, bösartige Bot-Aktivitäten zu verhindern und die Serverbelastung zu verringern.

Schutz vor Cross-Site Scripting (XSS)
Die Neukundenplattform blockiert XSS-Angriffe durch den Einsatz von gehärteten Content Security Policies und verhindert so potenzielle Lecks in den Kundendaten.

Schutz vor SQL-Injektion
Die neue Kundenplattform schützt vor SQL-Injektionsangriffen, indem sie die dynamische Konstruktion und Ausführung von Abfragen über parametrisierte Anweisungen ermöglicht und so die Kundendaten vor Kompromissen schützt.

Kundenanfragen
Datenschutz und Sicherheit sind uns wichtig, und wir bemühen uns, unsere Sicherheitspraktiken auf dem Niveau der Branchenführer zu halten.
Lesen Sie die am häufigsten gestellten Fragen zum Datenschutz und zur Datensicherheit.

Wo werden die Daten gespeichert?
Bei der Residenz in einem EU-Rechenzentrum werden die Recheninfrastruktur und alle Kundeninhalte (Produktionsdaten, Sicherungsdaten und Metadaten) in der EU gehostet.

Bieten Sie allen Ihren Nutzern das gleiche Maß an Datenschutz
Ja, Sie können sicher sein, dass Ihre Daten sicher verwaltet und gespeichert werden. Mit TLS 1.2 oder höher für die Übertragung und AES 256 im Ruhezustand, in Übereinstimmung mit GDPR- und CCPA-Standards, sind Ihre Daten auf höchstem Niveau ohne zusätzliche Kosten gesichert.

Verkaufen Sie Daten an Drittanbieter
Nein, wir verkaufen unsere Nutzerdaten nicht, wie in unserer Datenschutzrichtlinie angegeben.

Insights hat erhebliche Fortschritte bei der Verbesserung seiner Technologieplattform gemacht und sich dabei auf die Benutzerfreundlichkeit und Sicherheitsmaßnahmen konzentriert. Die erfolgreiche Erlangung der Zertifizierung nach ISO 27001:2022 unterstreicht unser Engagement für die Aufrechterhaltung hoher Standards im Informationssicherheitsmanagement. Diese Zertifizierung stärkt nicht nur das Vertrauen der Kunden, sondern gewährleistet auch die Einhaltung von Branchenvorschriften und fördert ein effektives Risikomanagement.

Unser proaktives Sicherheitskonzept wird auch durch regelmäßige Penetrationstests unter Beweis gestellt, die keine Schwachstellen in unserer neuesten Neukundenplattform ergeben haben. Wichtige Sicherheitsmerkmale wie Zero Trust-Zugang, One Time Tokens und strenge Netzwerkschutzmaßnahmen verdeutlichen unser Engagement für den Schutz von Kundendaten.

Da wir der Sicherheit weiterhin höchste Priorität einräumen, möchten wir unsere Kunden ermutigen, sich mit uns in Verbindung zu setzen, wenn sie Fragen oder Bedenken bezüglich des Datenschutzes und der Sicherheitspraktiken haben. Wir verpflichten uns zur kontinuierlichen Verbesserung und Anpassung an neue Bedrohungen, um eine sichere Umgebung für alle unsere Nutzer zu gewährleisten.
Bei weiteren Fragen oder für den Zugang zu rechtlichen Informationen können sich die Kunden je nach Bedarf an unser Sicherheitsteam (security@insights.com) oder unser Rechtsteam (legal@insights.com) wenden.

British Assessment Bureau

Part of the **Amtivo** group

CERTIFICATE OF REGISTRATION

The management system of certificate number **247224**

Insights Learning and Development Ltd

Terra Nova, 3 Explorer Road, Dundee, DD2 1EG, United Kingdom

has been assessed and certified as meeting the requirements of:

ISO/IEC 27001:2022

Provision of the delivery of the customer platform for training and development worldwide

This is in accordance with the Statement of Applicability **version 3.3, seen 10 September 2024.**.

Further clarifications regarding the scope of this certificate and the applicability of requirements may be obtained by consulting the certifier.

UKAS MANAGEMENT SYSTEMS

8289

Valid from:
Initial certification: 21 November 2023
Latest issue: 18 December 2024
Expiry date: 20 November 2026
Subject to annual assessments.

Authorised by

Mike Tims
Chief Executive Officer

british-assessment.co.uk

Certificate issued by Amtivo Group Limited T/A British Assessment Bureau Ltd.

Certification is conditional on maintaining the required performance standards throughout the certified period of registration.
Amtivo Group Limited. 30 Tower View, Kings Hill, Kent, ME19 4UY.