SDL

SDL Language Cloud

Sicherheitsaspekte

Inhaltsverzeichnis

SDL Language Cloud – Sicherheit

Einleitung

Die Sicherheit von Kundeninformationen ist für unser Unternehmen von entscheidender Bedeutung. SDL legt höchsten Wert darauf, den Schutz Ihrer Daten zu gewährleisten. SDL verpflichtet sich, Ihr Unternehmen und Ihre Daten zu schützen, unterstützt von unseren Mitarbeitern, Richtlinien und Prozessen.

In diesem Whitepaper erfahren Sie, wie wir **SDL Language Cloud** entwickeln und hosten, um eine Umgebung zu schaffen, in der Kunden ihre Inhalte sicher verarbeiten und verwalten können. Diese Maßnahmen gelten auch für Produkte, die auf SDL Language Cloud basieren, wie z. B. SDL Trados Live.

ISO 27001 und integrierte Sicherheit

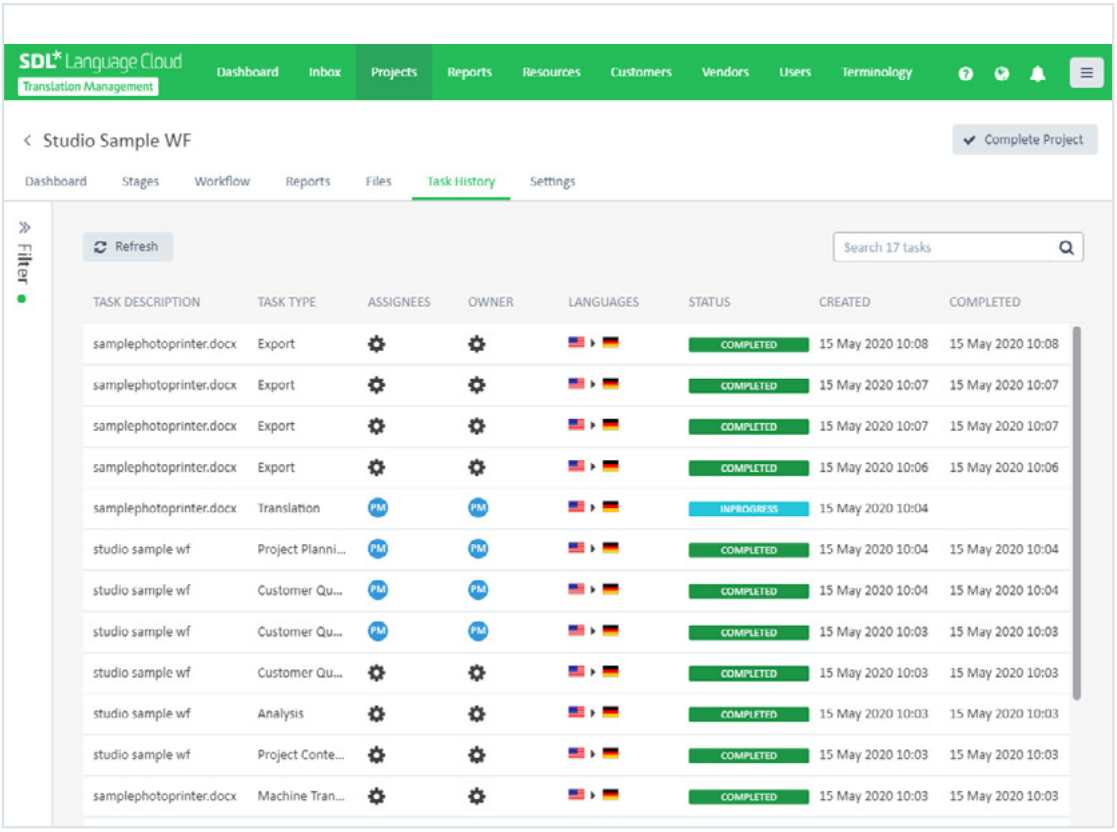
Die Organisation, in der SDL Language Cloud entwickelt wird, ist nach ISO 27001 zertifiziert, d. h. die Einrichtungen, Teams, Richtlinien und Verfahren werden regelmäßig von unabhängigen, externen Gutachtern geprüft. Bei der Erstellung neuer Produktmerkmale und -funktionen verfolgen wir einen Ansatz, bei dem Sicherheit an erster Stelle steht. Während des Entwicklungsprozesses werden umfassende Tests durchgeführt, um sicherzustellen, dass SDL Language Cloud eine sichere Umgebung für die verarbeiteten Daten bleibt, egal ob es sich dabei um die zur Übersetzung weitergeleiteten Inhalte handelt oder um Benutzerdaten.

Sicherheitstests für Anwendungen

Jede Version von SDL Language Cloud wird strengen Scans zur Ermittlung interner Schwachstellen sowie Penetrationstests unterzogen. Dazu gehören immer auch Tests zur Absicherung gegenüber den zehn kritischsten Sicherheitsrisiken bei Webanwendungen (OWASP Top 10). Probleme werden behoben, bevor Aktualisierungen in einer Produktionsumgebung bereitgestellt werden.

Prüfprotokolle

SDL Language Cloud erstellt für jede Datei, die in der Anwendung verarbeitet wird, ein lückenloses Prüfprotokoll. Im unwahrscheinlichen Fall eines Sicherheitsvorfalls kann ein Administrator den Verlauf einer Datei während des Workflows abfragen, um zu bestimmen, welche Workflow-Aufgaben für die Datei ausgeführt wurden und welche Benutzer auf die Datei zugegriffen haben.



Sichere Projekte

Bei der Erstellung eines neuen Projekts können Benutzer das Projekt mit SDL Language Cloud als „Sicheres Projekt" klassifizieren. Wenn diese Option aktiviert ist, werden alle Dateien, die zur Übersetzung in SDL Trados Studio heruntergeladen wurden, sowohl während der Übertragung als auch im Ruhezustand verschlüsselt. Mit einer neuen Funktion von SDL Trados Studio können Übersetzer und Reviewer diese Projekte öffnen und bearbeiten, wobei jedoch Einschränkungen dazu gelten, wie die zu übersetzenden Inhalte verarbeitet werden können. Weitere Informationen zu diesen Einschränkungen folgen, wenn die Funktion in der zweiten Jahreshälfte 2020 veröffentlicht wird.

Sicherheit für Benutzerkonten

SDL Language Cloud enthält verschiedene Sicherheitsfunktionen.

SDL ID

SDL ID ist die Single Sign-on (SSO)-Lösung von SDL. Sie basiert auf einer Drittanbieter-Identitätsplattform, die von Auth0 bereitgestellt wird und folgende Compliance-Stufen aufweist:

- ISO 27001
- ISO 27018
- EU-US Privacy Shield
- PCI DSS-Zertifizierung
- SOC 2 Typ II
- HIPAA BAA
- CSA STAR Gold
- DSGVO

Weitere Informationen zur Auth0-Sicherheit finden Sie unter **auth0.com/security**

Benutzerdaten

Benutzerdaten, die als personenbezogene Daten angesehen werden können, werden in SDL Language Cloud gespeichert, aber nicht für andere Systeme zur Verfügung gestellt. Sobald ein Benutzer in SDL Language Cloud definiert wurde, wird er nur noch anhand seiner eindeutigen Benutzeridentifizierungsnummer identifiziert. In Übereinstimmung mit den Bestimmungen der DSGVO können die personenbezogenen Daten, die einem Benutzer zugeordnet sind, auf Anfrage bearbeitet, exportiert und gelöscht werden.

Multi-Faktor-Authentifizierung

Für alle Benutzerkonten kann optional die Multi-Faktor-Authentifizierung (MFA) aktiviert werden. Dabei handelt es sich um ein Authentifizierungsverfahren, das einem Benutzer erst dann Zugriff gewährt, wenn einem Authentifizierungsmechanismus erfolgreich zwei oder mehr Berechtigungsnachweise (Faktoren) präsentiert wurden, wie zum Beispiel:

- Geheimes Wissen (etwas, das der Benutzer kennt, z. B. ein Passwort oder eine PIN)
- Gegenstand (etwas, das der Benutzer hat, z. B. ein Mobilgerät oder eine Karte)
- Biometrische Merkmale (z. B. ein Fingerabdruck)

Security Information Event Management System

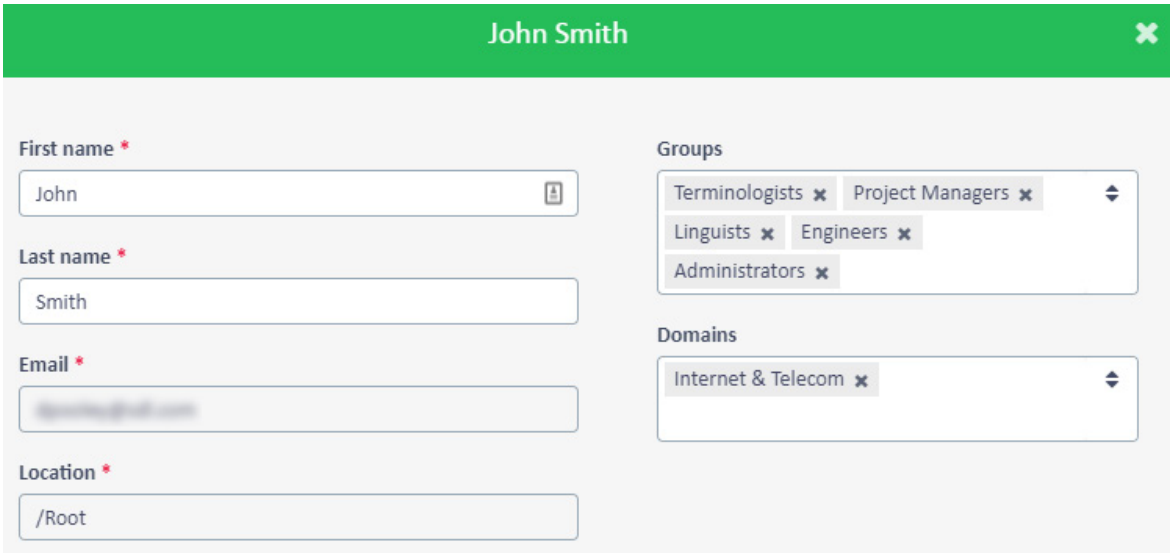
Alle Aktionen im Zusammenhang mit Benutzerkonten werden protokolliert und können zur weiteren Analyse an ein Security Information Event Management System (SIEMS) übertragen werden. Mithilfe solcher Systeme können Administratoren potenzielle Sicherheitsverletzungen wie Brute-Force-Angriffe und automatisierte Passwortgeneratoren erkennen. SDL setzt für diese Analyse Alert Logic ein, bei Bedarf können aber auch andere SIEMS unterstützt werden. Beispiele für Aktionen im Zusammenhang mit Benutzerkonten sind:

- Erfolgreiche Anmeldung
- Fehlgeschlagene Anmeldung
- Abmeldung
- Anfrage zum Zurücksetzen des Kennworts
- Anfrage zum Ändern des Kennworts

ALERT LOGIC

Benutzerberechtigungen

In SDL Language Cloud gehört jeder Benutzer zu einer oder mehreren Benutzergruppen. Jede Gruppe verfügt über eine begrenzte Anzahl von Berechtigungen (eine „Rolle"), die festlegt, welche Aktionen die Mitglieder der Gruppe auf welcher Ebene der Organisationsstruktur ausführen können. Die Berechtigungen für Benutzer, die Mitglieder mehrerer Gruppen sind, werden durch Erstellen eines übergeordneten Sets aller Berechtigungen dieser Gruppen bestimmt.



Alle Benutzer und Gruppen werden von Kontoadministratoren verwaltet. Wenn Kunden einen verwalteten Service nutzen, sind diese Administratoren Mitarbeiter von SDL, die die Benutzer und Gruppen einrichten, anschließend aber keinen Zugriff auf die Kundendaten haben. Kunden, die ihre Konten selbst verwalten möchten, können dies ohne jede Beteiligung von unserer Seite tun.

Benutzerdefinierte Rollen

Zusätzlich zu den bereitgestellten Standardrollen können Sie mit SDL Language Cloud benutzerdefinierte Rollen erstellen, die Gruppen zugewiesen werden können. Einer benutzerdefinierten Rolle können bestimmte Berechtigungen erteilt werden, die Flexibilität bei der Festlegung der Aktionen ermöglichen, die von den Mitgliedern dieser Gruppen ausgeführt werden können. Weitere Informationen zu benutzerdefinierten Rollen folgen, wenn die Funktion freigegeben wird.

Sicherheitsfunktionen der Hosting-Umgebung

SDL Language Cloud wird von SDL Cloud Operations als SaaS-Anwendung gehostet. Die Zertifizierung all unserer gehosteten Produkte nach ISO 27001 gewährleistet, dass SDL Cloud Operations die Kontrollen und Ziele der SOC 2 Typ 2-Zertifizierung hundertprozentig erfüllt. Mit der Implementierung von ISO 27017 im Jahr 2020 verstärkt SDL die Spezialisierung und Anpassung der Sicherheit seiner Cloud-Services noch.

SDL hat mit den führenden Drittanbietern Amazon Web Services, NTT Communications und Alibaba Cloud das Hosting von SDL Produkten vertraglich vereinbart. Alle verfügen über verschiedene Zertifizierungen für die Sicherheit, darunter unter anderem ISO 27001, SSAE 16, SOC 1, SOC 2 und SOC 3. Zusätzlich zu den von unseren Hosting-Partnern implementierten Sicherheitsmaßnahmen verfügt SDL auch über Richtlinien und Verfahren in Bezug auf:

- Administrative Zugriffskontrolle
- Physische Zugriffskontrolle
- Technische Zugriffskontrolle
- Datensicherung
- Datensicherheit
- Verfügbarkeit und proaktive Überwachung
- Risikobewertung

SDL Cloud Operations verfügt außerdem über eine Reihe von Sicherheitstools und -funktionen, um die Sicherheit von Kundendaten zu gewährleisten. Dazu gehören:

- Ereignismanagement-Überwachungstools zur Erkennung von Anomalien
- Perimeter-Firewalls und Network Threat Protection (NTP) mit Virenschutz (integriert)
- Rund-um-die-Uhr-Betrieb zur Unterstützung der Ereignisverwaltung in Echtzeit
- Von der Branche empfohlene Tools für die Bedrohungserkennung
- Ein wegweisender Sicherheitsscanner für Schwachstellen- und Penetrationstests
- Ein ITIL-konformes Ticketing-Tool (ITIL: IT Infrastructure Library) für das Störfallmanagement

Verschlüsselung im Ruhezustand

Im weiteren Verlauf des Jahres 2020 werden alle Dateien und Daten, die in SDL Language Cloud gespeichert sind, im Ablagesystem verschlüsselt. Diese Verschlüsselung verringert das Risiko, dass ein Angreifer die physische Hardware stehlen und auf die Daten zugreifen kann.

Bewertungen von Sicherheitsstandards

SDL bewertet die Sicherheit von SDL Language Cloud kontinuierlich. Neben den aktuellen Sicherheitszertifizierungen beachtet SDL auch die Anforderungen seiner Kunden und die regulatorischen Umgebungen, in denen sie tätig sind. Wir bewerten die Vorteile von Compliance und Zertifizierung fortwährend anhand zahlreicher Sicherheitsstandards, darunter:

- NIST
- HIPAA
- HITRUST CSF

Serverstandort

Der Serverstandort befindet sich in Frankfurt am Main.

Serverstandort Deutschland

Weiterführende Informationen

Weitere Informationen zum Sicherheitsansatz von SDL finden Sie auf unserer speziellen Sicherheitsseite unter **sdl.com/de/about/security**

Informationen zu den Datenschutzrichtlinien von SDL finden Sie auf unserer speziellen Datenschutzseite unter **sdl.com/de/about/privacy**

Wenn Sie mehr über die DSGVO in Bezug auf Ihre Nutzung von SDL Übersetzungssoftware erfahren möchten, können Sie **hier** unser eBook herunterladen.

SDL*

SDL (LSE: SDL) ist der Marktführer in den Bereichen Übersetzungstechnologie und -services sowie Content Management. Seit mehr als 25 Jahren unterstützen wir Unternehmen dabei, ihre Kunden gezielt anzusprechen und weltweit erfolgreich zu sein. 90 weltweite Topmarken vertrauen auf unsere Dienstleistungen, worauf wir sehr stolz sind!

Zusammen meistern wir die Content-Herausforderungen der heutigen Zeit, egal ob Formate, Volumen, Zeitdruck, Qualität, Sprachen, Kanäle oder Sonstiges.

Erfahren Sie auf **sdl.com/de** oder **sdltrados.com/de**, warum weltweit führende Unternehmen auf SDL vertrauen, und folgen Sie uns auf **XING** oder **Twitter**.

language-cloud-security-whitepaper-sdl-de-a4-100620