التقرير الأمني

V1.1

08.11.2022

1. شركتنا

سيفي هي شركة رائدة في تقديم خدمات تتبع المركبات عبر نظام تحديد المواقع العالمي جي بي إس وحلول إدارة الأسطول وتتبع ومراقبة الأصول. منذ تأسيس الشركة، فإن المهمة الرئيسية لها كانت ولا تزال متمثلة في تمكين المجتمعات عبر التزويد بأفضل تطبيقات الوب لإدارة الأسطول وأكثرها سهولة في الاستخدام. اليوم، الآلاف من الشركات والأعمال التجارية وحتى المنظمات غير الربحية في أكثر من 25 دولة تستفيد من خدماتنا السحابية في تتبع المركبات وإدارة الأساطيل.

يتم تقديم سيفي للعملاء كحل SaaS أي البرمجية كخدمة. يمكن للعملاء الوصول بسهولة إلى تطبيق الوب الخاص بسيفي عبر متصفح الإنترنت. يمكن لمستخدمي سيفي الاستفادة من الميزات المتعددة للمنصة مثل:

- اللوحات المتقدمة للمراقبة والتحكم الشامل في الزمن الحقيقي.
- عمليات الترشيح والتصفية الفعالة للبيانات وعمليات الإدراج القابلة للتخصيص.
- نظام التنبيه اللحظي والإنذارات الفورية لعمليات إدارة أسطول أكثر فعالية.
- التقارير الديناميكية القابلة للتخصيص والتي تساعد في تقليل زمن إعداد التقارير إلى الحد الأدنى.
- أدوات إدارة استهلاك الوقود وتتبع الوزن الأكثر موثوقية.

تقدم سيفي أيضاً واجهة برمجة التطبيقات API الخاصة بها والمتقدمة للغاية لأغراض التطوير وتكامل الأعمال.

2. الأمن وإدارة المخاطر في سيفي

أولويتنا القصوى هي حماية بيانات عملائنا وخصوصية مستخدمي المنصة. لدينا استثمارات ضخمة في الموارد الأساسية والبنى التحتية الخاصة بمسألة حماية البيانات ونقوم بتنفيذ تدابير وضوابط الأمان الأكثر تقدماً لضمان قدرتنا على خدمة عملائنا باستمرار وحماية بياناتهم دون أي انقطاع.

في سيفي، أنشأنا فرقاً عالية المهارات في أمن التطبيقات وأمن العمليات التشغيلية، وهي فرق بمسؤولية رئيسية تتمثل في تطوير وإدارة برنامج الأمن وتقييم المخاطر بالكامل عبر التسلسل الهرمي للشركة وجميع منتجاتها والبنية التحتية لخدماتها.

3. الأهداف

لتطوير إطار العمل الأمني الخاص بنا، قمنا بتطبيق أفضل ممارسات أمان تطبيقات الوب في صناعة الخدمات السحابية.

الأهداف الرئيسية لعملية التطوير هي:

- **ضمان سلامة الخدمة والبيانات**. حماية بيانات العميل من أي فساد أو تغيير.
- **استمرارية الأعمال وتوافر الخدمة**. الدفاع عن أنظمتنا وحمايتها ضد جميع التهديدات الأمنية التي قد تتسبب بفقدان البيانات أو انقطاع الخدمة.
- **ثقة الأعمال وحماية الخصوصية**. تقديم خدمات عالية الجودة تضمن حماية خصوصية البيانات وسرية العملاء.

- **التوافق مع المعايير وقوانين البيانات**. تصميم وتطوير إجراءات وضوابط الأمان وإدارة المخاطر لدينا لتتوافق تماماً مع اللوائح التنظيمية والتدابير الأمنية الخاصة بحماية البيانات في صناعة الخدمات السحابية. يمتثل برنامجنا الأمني للقانون العام لحماية البيانات GDPR الخاص بالاتحاد الأوروبي، ويطبق البرنامج معايير ISO 27001 وNIST SP 800-53، كما أنه يتوافق مع معايير مثل COBIT وCCM.

4. ضوابط أمان سيفي

فيما يلي مجموعة من ضوابط الأمان التي نفذتها سيفي لتأمين بيانات العملاء والعمليات التشغيلية ولتقليل المخاطر إلى الحد الأدنى عبر الشركة بأكملها.

1.4. البنية التحتية للخدمة

1.1.4. أمن مركز البيانات

بشكل أساسي، لا تستضيف سيفي خدماتها السحابية على مخدمات موجودة في مقر الشركة أو في أي من مكاتبها. يتم توظيف مصادر خارجية لاستضافة تطبيق الوب الخاص بإدارة الأساطيل، وتستفيد سيفي من توظيف مزودي البنية التحتية السحابية الرائدين مثل Microsoft Azure و Google Cloud Platform و Oracle Cloud Infrastructure لاستضافة المنتج.

يوفر كل من Microsoft و Google و Oracle مستويات عالية من الأمان التشغيلي وأمن الشبكة والبنية التحتية. تقع مراكز بيانات مزودي البنية التحتية السحابية لدينا والتي نستخدمها لاستضافة خدماتنا السحابية وتخزين بيانات عملائنا في كل من الولايات المتحدة والاتحاد الأوروبي ومنطقة الخليج العربي. تمتلك كل من مراكز بيانات Microsoft و Google و Oracle برامج أمان قوية ومُحكمة خاصة بها تتوافق مع المعايير SOC 2 II و ISO 27001.

يتمتع مزودو البنية التحتية السحابية بإمكانيات هيكلية هي الأكثر تطوراً وتشمل أمن شبكات الإمداد بالطاقة وشبكات البيانات والأمن التشغيلي والفيزيائي:

- جهوزية الخدمة واستمرارية التشغيل بنسبة أعلى من 99.95%.
- الحد الأدنى للزيادة والوفرة في البنية التحتية هو N+1 بالنسبة لشبكة الطاقة وشبكة البيانات وخدمات HVAC.
- الوصول الفيزيائي والإلكتروني المقيد والمحدود للغاية إلى المواقع والأبنية والمنشآت.
- خطط استمرارية الأعمال والتعافي من الكوارث تتوافق مع المعايير المعتمدة SOC 2 II و ISO 27001.

الشهادات متاحة على صفحات الوب الخاصة بالأمان والامتثال على الموقع الإلكتروني لكل من Microsoft Azure وGoogle Cloud Platform وOracle Cloud Infrastructure.

2.1.4. أمن الشبكة

تطبق سيفي مجموعة من وسائل حماية أمان الشبكة الأكثر تقدماً والمصممة خصيصاً لمنع الوصول غير المصرح به إلى شبكة الإنترنت الخاصة بالمنتج وداخل شبكة الإنترانت أي الشبكة الداخلية الخاصة بالبنية التحتية للخدمة. توظف ضوابط حماية سيفي التقنيات المتقدمة في مسائل التوجيه الشبكي على مستوى الشركة وضبط جدار الحماية الرقمية وتسجيل حركة المرور ضمن الشبكة ومراقبتها وتحليلها وإصدار التقارير الدورية.

3.1.4. إدارة التشكيل والإعداد

إن إجرائياتنا المتعلقة بتوسيع نطاق البنية التحتية للمنتج والعمليات التشغيلية للخدمة لتلبية الاحتياجات المتغيرة للعملاء مؤتمتة بالكامل. يتم تضمين تشكيل وإعداد المخدمات في صور وملفات puppet. تتم إدارة التشكيل والإعداد من خلال هذه الصور والخطاطات scripts عندما يتم بناء الخادم. تتم إدارة التغييرات في ملفات الإعداد والصور من خلال إجراءات مركزية لإدارة التغيير خاضعة للرقابة الصارمة. تتم معالجة عمليات إدارة التصحيح عن طريق استبدال مثيلات الخادم التي لم تعد متوافقة مع المثيلات الجديدة المجهّزة والمتوافقة تماماً.

4.1.4. التنبيه والمراقبة

قامت شركة سيفي باستثمارات كبيرة في إنشاء نظام مؤتمت بالكامل للتنبيه والمراقبة، وطوّرت إجراءات استجابة عالية التقنية من أجل تقييم ومعالجة جميع المخاطر المحتملة في وقت مبكر وحل المشكلات في أسرع وقت ممكن.

تم ضبط وإعداد البنية التحتية القوية للمنتج في نظام إدارة بيانات سيفي لإطلاق إنذارات لفريق الأمان المتخصص عند حدوث أي مشكلة، مثل:

- زيادة معدلات الفشل.
- أنشطة غير متوقعة أو خبيثة.
- سيناريوهات إساءة استخدام المنتج.
- هجمات الأمن السيبراني.

الفريق الأمني مسؤول عن التحقيق في الموقف الحاصل وتطوير الحل المناسب وتصحيح المشكلة على الفور وفي الزمن الحقيقي.

نظام سيفي قادر على حماية نفسه من جميع المواقف غير المرغوب فيها من خلال الاستفادة من عدد من تقنيات الحماية المؤتمتة القوية:

- تسجيل الأنشطة والمراقبة في الزمن الحقيقي.
- ضبط العتبات الأمنية الصارمة والمعرّفة مسبقاً.
- الحظر الفوري لحركة المرور المشبوه ضمن الشبكة.
- الحجر اللحظي والمباشر.
- الإنهاء الفوري للإجرائيات.

إحدى أقوى نقاط نظامنا هي القدرة على تسجيل ومراقبة كل نشاط فردي على مستوى التطبيق وفي طبقة البنية التحتية للخدمة. يرتبط نظام مراقبة الأحداث بنظام الاستجابة الفورية الذي ينبه متخصصي الأمن في الزمن الحقيقي لتطوير واتخاذ الإجراءات الصحيحة.

5.1.4. الوصول إلى البنية التحتية

تحمي سيفي البنية التحتية لمنتجها من التهديدات الأمنية المحتملة من خلال تطبيق نموذج وصول متقن التصميم وخاضع للتحكم الصارم. يتم منح الموظفين الوصول إلى الخدمات بناءً على وظائفهم وطبيعة عملهم باستخدام نموذج التحكم في الوصول المستند إلى الدور Role-Based Access Controls يوجد المزيد من التفاصيل حول تطبيق نموذج RBAC عبر شركة سيفي في فقرة لاحقة.

بعض تقنيات التحكم في الوصول إلى البنية التحتية لسيفي:

- يتم تقليل سماحيات الوصول إلى الحد الأدنى وفقاً لاحتياجات عمل الموظف.
- نموذج JITA Just-In-Time Access لطلبات الوصول الطارئة والإدارية.
- يتم تسجيل جميع طلبات JITA ومراقبتها لتتبع الطلبات غير الطبيعية.

- منع الوصول المباشر للشبكة إلى بيئة الإنتاج عبر SSH.
- المصادقة والتحقق مطلوبين من الموظفين للوصول إلى بيئة ضمان الجودة وبيئة الإنتاج.
- المصادقة الثنائية واستخدام الرموز غير القابلة للاستبدال NFTs للحصول على أذونات الوصول التي تتعلق بالمخدمات.

2.4. حماية التطبيق

1.2.4. دفاعات تطبيقات الوب

لحماية الخدمات الإلكترونية المقدمة إلى عملائنا وجميع بيانات عمليات الإرسال الخاصة بتلك الخدمات، فإن جدار حماية تطبيقات الوب Web Application Firewall WAF المصمم بشكل دقيق مع أفضل ممارسات الأمان الموثقة من قبل OWASP Open Web Application Security Project تم تنفيذه في سيفي.

ولضمان استمرارية الأعمال، قمنا أيضاً بدمج وإشراك عدد ضخم من قواعد الحماية الموصى بها في صناعة تطبيقات الوب ضمن منصة سيفي للتصدي لهجمات المنع الموزع للخدمة Distributed Denial of Service DDoS. تعمل حمايات WAF وDDoS معاً لحماية جميع الخدمات الإلكترونية التي يتم إنشاؤها واستضافتها والوصول إليها عبر متصفح الإنترنت من خلال https://tracking.safee.com وجميع تكاملات الأعمال عبر سيفي API على https://tracking.safee.com/api وبالطبع، تتم أيضاً حماية جميع بيانات العملاء المخزنة في مراكز البيانات الخاصة بنا تلقائياً عن طريق قواعد الكشف والحظر المجهزة جيداً ضد جميع أنواع ومعدلات تكرار حركة المرور الخبيث أو الضار على الشبكة.

2.2.4. إدارة التطوير والتحديث

في سيفي، يعتبر التقدم والتطور من العناصر الأساسية لبيئة العمل لدينا. هناك دائماً ميزات جديدة تضاف إلى المنصة لخدمة الاحتياجات المتغيرة لعملائنا وحل مشاكلهم المستقبلية. بالإضافة إلى ذلك، تخضع المنصة الرئيسية للتحديثات الدورية والمستمرة على أساس منتظم.

يتضمن نهج التسليم المستمر للتطوير البرمجي لدينا الخطوات التالية:

1. يتم اقتراح الرمازات البرمجية الخاصة بالميزات الجديدة.
2. فرق عالية التخصص من المطورين لإجراء المراجعات البرمجية ومهام ضمان جودة البرامج المكتوبة.
3. تجميع وتغليف واختبار الوحدات البرمجية بعد تقديم الرمازات البرمجية المعتمدة إلى بيئة التكامل.
4. يتم عمل أرشيفات للرمازات البرمجية الموجودة على مستوى الإنتاج حالياً.
5. يتم نشر الرمازات البرمجية الجديدة على مستوى التطبيق.
6. تتضمن خطوة ما بعد النشر المراقبة المستمرة لحالة التطبيق وأدائه.
7. في حالة حدوث أي فشل، يتم تفعيل الصورة المحفوظة بشكل تلقائي وعلى الفور للرمازات البرمجية على مستوى الإنتاج الموجودة سابقاً.
8. يتم توثيق جميع المعلومات حول الميزات المضافة حديثاً وتزويدها عبر منشورات تحديث الأخبار على موقع الوب الخاص بالمنتج وصفحات wiki.

إن بيئة ضمان الجودة وبيئة الإنتاج كيانان منفصلان ولا يوجد تداخل بينهما على أي مستوى. يمنع جدار الحماية القوي للشبكة أي وصول غير مصرح به وغير مرغوب فيه بين البيئتين. في سيفي، لا يتم استخدام بيانات عملائنا مطلقاً في بيئة ضمان الجودة.

3.2.4. مسح وتقييم نقاط الضعف

ينفذ فريق أمن البيانات الخاص بسيفي فحصاً دقيقاً ودورياً للثغرات الأمنية يشمل جميع طبقات البنية التحتية للمنتج، معتمدين الأدوات وأساليب التقييم الأكثر تقدماً والموصى بها في صناعة تطبيقات الوب والخدمات السحابية.

يشمل نهجنا الرئيسي في المسح والتقييم ما يلي:

- فحص نقاط الضعف على أساس منتظم.
- عبر الشبكات الداخلية والبنية التحتية للتطبيق والبنية التحتية المؤسساتية للشركة.
- الكشف المبكر عن أي ثغرات أمنية محتملة من خلال تحليل شامل لأنشطة الترميز في مراحل التطوير.
- التحديث المستمر لقوائم التواقيع الرقمية الخاصة بالثغرات الأمنية.

4.2.4. اختبار الاختراق

توظف سيفي الخدمات الأكثر شهرة في صناعة أمان تطبيقات الوب لإجراء 4 اختبارات اختراق في السنة، من أجل تحديد العيوب الأمنية المحتملة والتي قد تعرّض عملياتنا التشغيلية للمخاطر. إن اختبارات الاختراق هذه تبقي فريق سيفي مستعداً دائماً لمعالجة أي مشكلة وفي وقت استباقي.

لتوسيع قائمة أنواع المخاطر الأمنية المحتملة التي يجب تقييمها، فإن كل من طبقة الخدمة السحابية عبر الوب وطبقة الشبكة وطبقة البنية التحتية للشركة هي أهداف لاختبارات الاختراق السنوية الخاصة بنا.

5.2.4. برنامج Bug Bounty

إلى جانب جهودنا الخاصة بفحص الثغرات الأمنية واختبارات الاختراق المستقلة الدورية، نقوم بتنظيم برامج bug bounty بشكل منتظم ودوري لإعطاء فرصة للباحثين المستقلين والخبراء في مجال أمن البيانات وتطبيقات الوب، لتزويدنا بتقارير حول نقاط الضعف التي قد يرونها في خدماتنا. سيساعدنا ذلك حتماً في معالجة أي مشكلة ناشئة في وقت مبكر، ويضمن أن نبقى دائماً قادرين على تزويد عملائنا بأفضل تجربة وأكثرها أماناً على الإطلاق.

3.4. حماية بيانات العملاء

1.3.4. تشفير أثناء النقل وأثناء التخزين

إن جميع بيانات عملائنا محمية أثناء النقل وفي حالة السكون. أثناء النقل، يتم تقديم جميع الاستمارات ويمكن للعملاء الوصول إليها عبر قنوات اتصال TLS/256Bit SSL، وهو مستوى الحماية نفسه المعتمد للخدمات المصرفية والتجارة الإلكترونية والخدمات المالية. في حالة التخزين والبيانات الساكنة، نستخدم RSA2048 لتأمين الخدمات الرقمية وتشفير البيانات التي تُجمع عن طريق تلك الخدمات. جميع كلمات مرور الحسابات يتم تهشيرها وكل صفحات تسجيل الدخول مؤمنة من خلال حمايات ضد هجمات بروتفورس.

2.3.4. حماية تسجيل الدخول

يمكن لمستخدمي سيفي تسجيل الدخول إلى حساباتهم على المنصة عبر صفحة تسجيل دخول مدمجة بالنظام الأساسي. تضمن السياسة الموحدة لكلمات المرور والتي يتم فرضها على جميع مستخدمي سيفي التشغيل الآمن وفقاً للقواعد التالية:

- فرض كلمة مرور لا تقل عن 8 محارف.
- يجب أن تتضمن مزيج من الأحرف الصغيرة والكبيرة.
- تضمين محارف خاصة وأرقام.

- لا يمكن للمستخدمين تغيير السياسة الافتراضية الأساسية لكلمة المرور.
- يتم تشجيع المستخدمين على تنشيط خيار المصادقة الثنائية لحساباتهم على المنصة.

3.3.4. أذونات وسماحيات الوصول للموظفين

تتحكم سيفي بشكل صارم في مسألة وصول أفراد موظفيها إلى البيانات في بيئة الإنتاج وعلى مستوى البنية التحتية للشركة.

تُمنح أذونات الوصول إلى بيانات الإنتاج لمجموعة من موظفي سيفي بناءً على دورهم في الشركة على أساس ضوابط الوصول المستندة إلى الدور RBAC Role-Based Access Controls أو على أساس JITA Just In Time Access.

بعض احتياجات الوصول الشائعة:

- الاستجابة إلى تنبيه.
- استكشاف الأخطاء وإصلاحها.
- تحليل البيانات الخاص بصنع قرارات الاستثمار في المنتج.
- طلبات العملاء بالمساعدة والدعم حول المنتج.

تحكم مجموعة من القواعد الصارمة والمتطورة والمعقدة عمليات المصادقة والتفويض ذات الصلة بأذونات الوصول عبر الشبكة إلى البنية التحتية للمنتج. يجب أن يطلب موظفو دعم العملاء فقط وصولاً محدود الوقت إلى بوابات العملاء على أساس JITA، ويجب أن تقتصر طلباتهم على مسؤوليات عملهم المرتبطة بدعم وخدمة عملائنا. يتم تسجيل جميع طلبات الوصول والأنشطة ذات الصلة ومراقبتها في الزمن الحقيقي وتخضع لمراجعة آلية على أساس يومي.

4.4. الخصوصية

في سيفي، نولي أهمية قصوى لخصوصية بيانات عملائنا. وفقاً لسياسة الخصوصية الخاصة بنا على موقع الوب، فإننا لا نبيع بياناتك الشخصية مطلقاً إلى أي طرف ثالث. لقد نفذّت سيفي جميع إجراءات الحماية الموثقة ضمن هذا التقرير والمزيد من وسائل الحماية الإضافية، فقط للحفاظ على خصوصية بياناتك وإبقاءها آمنة وسليمة من أي تلاعب أو تغيير. تلبي جميع ممارسات الأمان التي أدرجها برنامج الخصوصية لدى سيفي المتطلبات التنظيمية ذات الصلة بحماية البيانات وتتوافق مع اللوائح التنظيمية في كل من الولايات المتحدة والاتحاد الأوروبي ومنطقة الخليج العربي.

سياسة الاستبقاء على البيانات لدينا:

- يتم تخزين بيانات العميل طالما ظل العميل نشطاً.
- توفر المنصة أدوات الحذف الضرورية لعملائنا النشطين عندما يريدون إزالة بياناتهم بشكل دائم.
- تتم إزالة بيانات العميل نهائياً من قواعد البيانات بعد طلب كتابي رسمي من العميل أو بعد فترة محددة بعد انتهاء الاتفاقية بين العميل وسيفي.

يمكن العثور على مزيد من المعلومات التفصيلية حول سياسة الخصوصية الخاصة بنا واتفاقية معالجة بيانات العملاء على موقعنا الإلكتروني.

5.4. استمرارية الأعمال وسياسة التعافي من الكوارث

تم وضع خطط سيفي لاستمرارية الأعمال والتعافي من الكوارث وفقاً للقواعد الأساسية التالية:

- الزيادة والوفرة على مستوى طبقة الشبكة وطبقة الإنتاج والبنية التحتية للشركة لمنع أي انقطاعات محتملة.
- التعافي السريع في حال انقطعت الخدمة أو حصل أي تدهور في الأداء.
- السرعة في عزل ومعالجة القضايا والمشكلات التي قد تحدث.

- نشر تحديثات حول المشكلات الحاصلة وتوضيح الحالة الراهنة لإجرائيات الحل والتعافي.

في سيفي، نتحقق من استراتيجيات استمرارية الأعمال وإجراءات التعافي على أساس يومي وهذا يجعلنا على أتم الاستعداد لأي مشكلة طارئة قد تحدث.

تعتمد استراتيجيتنا بشكل أساسي على:

- تحقيق الوفرة في البنية التحتية.
- تكرار البيانات في الزمن الحقيقي.
- النسخ الاحتياطي المنتظم.

بالإضافة إلى ذلك، يطبق مزودو البنية التحتية للمخدمات لدينا حداً أدنى من التكرار n + 1 داخل منشآتهم الموزعة بشكل استراتيجي عبر مناطق متعددة.

6.4. الأمن المؤسساتي لشركة سيفي

1.6.4. تصديق وتفويض الموظفين

تحقق سياسة كلمات المرور على المستوى المؤسساتي والخاصة بشركتنا أفضل المعايير المعتمدة في صناعة أمن المعلومات.

بعض من القواعد المطبقة عبر الشركة بأكملها:

- تغيير كلمات المرور كل 3 أشهر.
- الحد الأدنى لطول كلمة المرور الخاصة بالموظف 12 محرفاً.
- يجب أن تتضمن كلمات المرور أحرفاً كبيرة وصغيرة ومحارف خاصة وأرقاماً.
- يحظر مشاركة كلمة المرور.
- مصادقة الموظفين باستخدام مفاتيح SSH.
- المصادقة متعددة العوامل للوصول إلى البنية التحتية للمنتج.
- جميع إجراءات المصادقة والتفويض مؤتمتة.
- يتم تسجيل جميع طلبات الوصول ومراقبتها.
- فحص منتظم للنظام بأكمله للتأكد من أن الأذونات الممنوحة لا تزال سارية المفعول.

2.6.4. فحص الخلفية

يخضع جميع موظفينا لعمليات تحقق فحص للخلفية واسعة ومفصلة قبل التوظيف وذلك بما يتناسب مع اللوائح التنظيمية الوطنية ومعايير الصناعة.

يتضمن فحص الخلفية بشكل أساسي ما يلي:

- الوظائف السابقة.
- التعليم.
- السجل الجنائي.

يتعين على موظفينا الامتثال لاتفاقيات عدم الإفصاح قبل أن يتمكنوا من بدء عملهم والمشاركة في بيئة الإنتاج ومختلف بيئات الشركة.

3.6.4. أمن المكاتب

بعض تقنيات الحماية الخاصة بمكاتبنا والتي يتم تنفيذها في جميع أنحاء الشركة:

- المراقبة عبر الفيديو.
- أفراد الأمن الخاص.
- رموز RFID التعريفية للتحكم في سماحيات الوصول إلى المواقع.

4.6.4. إدارة البائعين والمورّدين

لدى سيفي نظام إدارة للبائعين والمورّدين مصمم بدقة بهدف رئيسي هو ضمان أخذ البائعين والمورّدين على محمل الجد جميع ضوابط الأمان الضرورية وتنفيذها بشكل مناسب في البنى التحتية لخدماتهم.

يتم تتبع وإجراء مراجعة شاملة لبرامج الأمان لموردينا على أساس منتظم. وكجزء من إدارة العقود، يتم تنسيق الاعتبارات الأمنية المختلفة بين فريق تكامل الأعمال الخاص بسيفي والموردين لإدارة الامتثال للوائح التنظيمية وقوانين حماية البيانات.

5.6.4. التوعية الأمنية والتدريب

لدى سيفي برنامج تدريبي خاص بأمن المعلومات مصمم ليغطي المواضيع التالية:

- متطلبات معالجة البيانات.
- اعتبارات الخصوصية.
- سياسة الاستجابة للانتهاكات.

ننظم برامج التدريب الأمني للتأكد من أن جميع الموظفين مجهّزون جيداً لوظائفهم في شركتنا. بالإضافة، يتم إنشاء معسكرات تدريب للوعي الأمني خاصة بالمطورين ومكرّسة لفرقنا من مهندسي الأنظمة ومطوري البرمجيات.

5. الامتثال للقوانين والأنظمة

تتوافق سيفي تماماً مع اللوائح التنظيمية وتمتثل للقانون العام لحماية البيانات General Data Protection Regulation GDPR الخاص بالاتحاد الأوروبي، وتحتوي المنصة أيضاً على جميع الأدوات والميزات الضرورية التي تمكن عملائنا من الحفاظ على متطلبات الامتثال الخاصة بـ EU-US Privacy Shield.

يتم استضافة جميع خدمات سيفي من قبل Microsoft Azure Cloud وGoogle Cloud Services و Oracle Cloud Infrastructure وهم مزودون عالميون لخدمات البنية التحتية السحابية يطبقون المعايير المعتمدة SOC 2 II وISO 27K ويمتثلون تماماً لقانون GDPR.