Devolutions

DÉVELOPPEMENT SÉCURITAIRE DE LOGICIELS

Le programme de sécurité de Devolutions comprend une politique de développement sécuritaire de logiciels, qui régit tous les aspects de développement logiciel de l'entreprise. Notre approche est basée sur le SSDF (de l'anglais Secure Software Development Framework) développé par l'Institut national des normes et de la technologie (NIST). Le SSDF définit un ensemble de normes et de pratiques de sécurité à intégrer dans le cycle de vie du développement logiciel (Software Development Life Cycle, SDLC, en anglais).

Ce document décrit sept aspects fondamentaux de nos pratiques de sécurité intégrées dans notre SDLC :

1. Rôles et responsabilités

2. Expertise et formation

3. Environnement de contrôle

4. Technologies

5. Activités internes et de tierces parties

6. Protection intégrée de la vie privée

7. Signalement et correction des vulnérabilités

1. Rôles et responsabilités

Pour offrir des logiciels sécurisés et fiables, il est primordial de suivre un solide programme de pratiques sécurisées de développement. Ce programme, d'une importance capitale pour notre entreprise, est géré et soutenu par notre Comité exécutif, le Directeur de la sécurité, le Directeur des affaires juridiques, risques et protection des renseignements personnels et par le Chef de pratique en développement sécuritaire. Chaque rôle contribue au succès de notre programme. Ils sont détaillés dans le tableau suivant :

Rôle	Mandat
Comité exécutif	Le Comité exécutif s'engage à fournir des logiciels sécurisés et fiables à nos clients. Ses membres fournissent tout le soutien et toutes les ressources nécessaires pour administrer efficacement le programme.
Chef de la sécurité (CSO)	Le Chef de la sécurité (CSO) est responsable de la conception, de la mise en œuvre et du contrôle des stratégies de sécurité nécessaires à l'atteinte des objectifs de l'organisation. Il supervise toutes les initiatives de sécurité et se rapporte directement au Comité exécutif. Il fournit également le soutien nécessaire au Chef de pratique en développement sécuritaire pour assurer la performance et la réussite des objectifs du programme.

Directeur des affaires juridiques, risques et protection des renseignements personnels	Le Directeur des affaires juridiques, risques et protection des renseignements personnels est responsable de la mise en œuvre des politiques, procédures et contrôles relatifs à la gestion et à la protection des informations personnelles identifiables (PII), en conformité avec toutes les lois et tous les règlements en vigueur. Le directeur se rapporte au Comité exécutif et travaille en collaboration avec le CSO pour appliquer les stratégies de protection des renseignements personnels.
Le Chef de pratique en développement sécuritaire	Le Chef de pratique en développement sécuritaire collabore avec le Chef de la sécurité afin de conceptualiser, mettre en place, et surveiller la performance et l'amélioration continues du programme tout en promouvant ses bénéfices et motivant son adoption à l'ensemble de l'organisation.

2. Expertise et formation

Un programme SDLC sécuritaire requiert une expertise et des compétences particulières. C'est pourquoi notre entreprise investit dans des programmes annuels de formation et de développement des compétences. Voici quelques faits qui en témoignent :

• Notre équipe de sécurité est composée de professionnels qui détiennent des certifications reconnues dans le monde entier, octroyées par des organisations de premier plan telles que GIAC, (ISC)2 et Offensive Security. Les membres de notre équipe de sécurité sont encouragés à assister et à contribuer à divers événements en lien avec la sécurité, comme des conférences ou des ateliers dans le monde entier. Nous sommes fiers de contribuer financièrement pour leur participation à ce type d'évènements.

• Notre équipe de développeurs assiste régulièrement à des formations obligatoires à l'interne qui couvrent un large éventail de sujets liés à la sécurité, tels que les types de vulnérabilités et les moyens de les éviter, les consignes et principes de sécurité généraux, l'utilisation de la cryptographie, etc. La formation est offerte sous différentes formes telles que des cours interactifs en ligne, des sessions en direct et des sessions lunch and learn. La présence et le suivi de la réussite de ces formations sont supervisés par l'organisation afin de s'assurer que tous les employés répondent aux critères exigences en matière de développement sécuritaire.

3. Environnement de contrôle

L'environnement de contrôle est d'une importance vitale, parce qu'il influence directement le succès de notre programme. Les facteurs environnementaux sont identifiés et contrôlés pour limiter la présence et l'impact des menaces externes au développement des produits et services. Vous trouverez ci-dessous certains des contrôles que nous avons actuellement en place chez Devolutions.

• Les environnements de développement, de tests et de production sont séparés. Cette façon de faire permet de garantir que le code non testé et non autorisé ne parvienne pas à la production. La transition du code entre les différents environnements est contrôlée par l'équipe des opérations.

• Notre processus de contrôle des changements exige que le code soit examiné par des pairs, testé et approuvé par le personnel autorisé avant son déploiement en production.

• Les données utilisées dans les environnements de développement et de tests sont artificielles ou anonymisées et ne contiennent aucune donnée de production.

• L'intégrité du code source est assurée par les technologies de contrôle de source et de versionnage. Toute modification doit passer par le processus de révision du code source avant d'être fusionnée avec la base de code.

• Tous les accès et actions effectués dans l'environnement de production sont contrôlés, monitorés et audités périodiquement afin d'identifier ou de détecter toute anomalie et non-conformité à nos procédures et politiques internes.

4. Technologies

Le choix et l'implantation de la technologie sont deux facteurs majeurs qui influencent la qualité du logiciel. Pour mieux prévenir et combattre les menaces, notre entreprise favorise des technologies reconnues pour leur sécurité, leur stabilité et leur fiabilité. De manière plus précise :

• Nous utilisons des plateformes de programmation qui permettent d'effectuer des opérations de mémoire sécurisées et qui bénéficient d'une sécurité renforcée par rapport au C/C++ traditionnel. C#, Rust et Typescript sont des langages utilisés dans notre environnement qui répondent à ces critères.

• Nous utilisons des fonctionnalités de sécurité par compilation telles que GS, SafeSEH, NX et ASLR, qui nous permettent de renforcer les applications contre l'exploitation des vulnérabilités.

• Nous affichons l'intégrité de nos produits avec la technologie de signature de code par certificats numériques pour tous les logiciels que nous rendons accessibles au public.

5. Internal and Third-Party Activities

Notre organisation évalue constamment la sécurité des logiciels produits par des activités manuelles et automatisées. Notre méthodologie et notre approche s'appuient sur des normes et des directives documentées et reconnues, publiées par l'OWASP et le NIST. De plus, les principes, standards et régulations en matière de protections des renseignements personnels sont respectés et intégrés dans nos actions afin d'assurer le respect de la vie privée. Voici un aperçu de ces actions :

Actions	Description
Modélisation de la menace	Cette action implique un brainstorming et une analyse de scénarios de menaces pour évaluer leur impact négatif. L'objectif est de s'assurer que des contrôles adéquats sont en place afin de prévenir ou d'atténuer les risques identifiés dès que possible dans le SDLC. Le principal avantage de cette action est d'aider à identifier les problèmes structurels dans la conception d'une application, ce qui réduit considérablement le coût des modifications et la probabilité d'exposition aux vulnérabilités.
Revue de code de sécurité	L'équipe de sécurité utilise des techniques manuelles et automatisées pour identifier les vulnérabilités potentielles dans le code source. Les revues de code permettent de s'assurer que les contrôles de sécurité (authentification, autorisation, filtrage, contrôles d'accès, etc.) ont été correctement implantés pour identifier et empêcher les vulnérabilités d'atteindre la production.
Analyse automatisée statique	Cette action consiste à utiliser un outil d'analyse de code automatisé qui inspecte le code source sans l'exécuter. Les problèmes de sécurité peuvent être identifiés en traçant les entrées de données et leurs chemins d'exécution où la validation et le filtrage sont manquants. Le principal avantage de cette activité est qu'elle peut être faite directement dans la chaîne d'outils d'environnement de développement intégré (IDE) et d'intégration continue (CI), afin de ne pas exposer les vulnérabilités au moment où les développeurs construisent leur code.
Fuzzing (ou test de données corrompues)	Il s'agit d'un test qui permet d'évaluer la robustesse d'un programme lorsqu'il est exposé à des données non valides ou mal formées. Combiné aux informations de couverture du programme, le fuzzing peut être très efficace pour identifier les problèmes de gestion de la mémoire dans les langages de bas niveau tels que C et C++.
Test d'intrusion	Cette action est effectuée par l'équipe de sécurité et des auditeurs tiers pour simuler des attaques ciblées sur les logiciels. L'objectif est de valider l'efficacité ou l'absence de contrôles de sécurité dans les logiciels en identifiant les vulnérabilités et en tentant de les exploiter. Les tests d'intrusion sont considérés comme la dernière ligne de défense.
Audit et tests de conformité	Des audits sont effectués périodiquement par des partenaires de confiance afin d'évaluer l'engagement de notre entreprise à l'égard de programmes de conformité, tels que SOC2 et GDPR. Divers processus, politiques, normes et contrôles techniques conçus et mis en œuvre dans nos logiciels et nos services sont validés par des auditeurs réputés. Cela assure la transparence de nos pratiques de sécurité. Combinés aux autres actions, ces audits procurent un haut niveau de confiance de nos clients et partenaires envers notre pratique de développement sécuritaire.

6. Protection intégrée de la vie privée

Le Comité exécutif s'engage fermement à la sécurité et la protection des renseignements personnels. L'intégration de la protection de la vie privée est planifiée dès la conception des produits et services et tout au long du cycle de vie logiciel. Cette responsabilité est assignée à notre Directeur des affaires juridiques, risques et protection des renseignements personnels qui veille à son intégration à tous les niveaux du processus de développement et à travers toute l'organisation. La collecte d'informations personnelles est effectuée uniquement lorsque :

• Il y a un besoin d'affaires clairement défini.

• Les données sont échangées et stockées selon les exigences de sécurité prévues par nos politiques.

• L'accès est limité sur la base du « besoin de savoir ».

Notre organisation se conforme aux exigences du Règlement général sur la protection des données (RGPD) de l'Union européenne et de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE). En appliquant les principes de confidentialité et les mesures de sécurité appropriées dès les premières étapes du SDLC, la probabilité et l'impact de fuite ou brèche de renseignements personnels sont considérablement réduits.

7. Signalement et correction des vulnérabilités

Avoir un processus défini de signalement des vulnérabilités et de correction est essentiel au succès du programme de développement sécuritaire de notre entreprise. Ce processus réduit les risques d'exploitation de vulnérabilités pouvant affecter notre organisation, nos clients et nos partenaires en nous permettant de mettre en œuvre rapidement des correctifs de sécurité.

Les utilisateurs et les chercheurs en sécurité sont encouragés à signaler les problèmes de sécurité à security@devolutions.net chaque fois qu'un problème logiciel ou d'infrastructure expose la clientèle ou l'organisation à un impact négatif sur la confidentialité, l'intégrité ou la disponibilité des données ou du service. Pour accélérer le processus de résolution, les informations suivantes doivent être incluses dans le rapport :

• Une preuve de concept et/ou des captures d'écran pertinentes qui nous permettent de confirmer et de reproduire le problème.

• Une courte explication de la manière dont le problème peut affecter la sécurité l'organisation et/ou les clients s'il est exploité.

• Un correctif proposé (si possible et si applicable).

Après avoir reçu un rapport, notre équipe de sécurité :

• Reproduira et confirmera la vulnérabilité décrite dans le rapport.

• Établira un indice de sévérité conformément à CVSS 3.1.

• Prendra en compte les recommandations du rapport et construira un plan d'action avec les équipes concernées.

• Maintiendra la communication avec l'utilisateur ou le chercheur en sécurité jusqu'à la résolution du cas.