Secure Software Supply Chain

Les applications de fabricants de logiciels externes peuvent renfermer des composants inconnus, manipulés ou peu sûrs pouvant nuireà votre entreprise. Votre chaîne d'approvisionnement logicielle est-elle suffisamment protégée?

Les attaques de la chaîne d'approvisionnement logicielle (comme l'attaque «Sunburst» de SolarWinds en décembre 2020) ont montré la sensibilité et la criticité des chaînes d'approvisionnement logicielles. Ce n'est qu'en connaissant le niveau de menace et le risque que l'on peut définir et mettre en œuvre des mesures de protection adéquates. Swisscom vous aide à comprendre le paysage actuel des risques et à mesurer vos risques TIC, à définir votre stratégie en matière de chaîne d'approvisionnement logicielle et à mettre en œuvre les mesures nécessaires. Nous vous aidons aussi à définir et gérer des critères TIC pertinents – en interaction avec vos fournisseurs – et à concevoir des recommandations et des mesures concrètes pour une chaîne d'approvisionnement logicielle sécurisée.

Vos avantages avec Secure Software Supply Chain

Transparence et acceptation des risques dans le domaine du développement logiciel externe

Les accords avec vos fournisseurs de logiciels sont analysés pour déterminer quels processus ont une incidence sur la sécurité. Une liste des artefacts logiciels non dignes de confiance et dangereux est dressée et ces derniers peuvent être retirés de votre environnement de développement et de production.

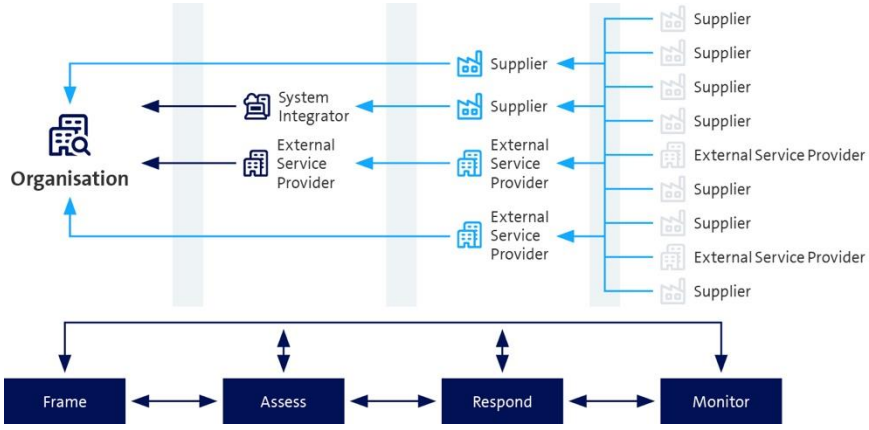
Software Bill of Material as a Service (SBOMaaS)

Représentation et explication des dispositions réglementaires pour une chaîne d'approvisionnement logicielle sécurisée. Génération d'une Software Bill of Material (SBOM) grâce à laquelle le contenu (Source code), les dépendances (Dependencies) ainsi que la création (Creation data) du pack logiciel à proprement parler peuvent être créés et enregistrés de manière vérifiable.

Monitoring de votre chaîne d'approvisionnement logicielle

Vérification constante des SBOM générées ou remises par des partenaires et tiers ainsi qu'évaluation continue des Dependencies par des experts de l'équipe Consulting. Votre entreprise peut ainsi atteindre le niveau de sécurité qu'elle souhaite et réagir de manière adéquate en cas de nouvelles vulnérabilités dans ces dépendances.

Voici comment fonctionne le monitoring de la chaîne d'approvisionnement logicielle



swisscom

Facts & Figures

Services de base

Que propose le pack de base?
Atelier: Secure Software Supply Chain

Situation de départ et analyse des besoins
Swisscom va se familiariser avec votre situation de départ: vos besoins de protection, les dangers de votre chaîne d'approvisionnement logicielle, les mesures de protection existantes, votre stratégie Open Source, les Code Repositories et Artifacts déjà utilisés, les accords avec vos fournisseurs de logiciels.

Risk Assessment et mesures
Swisscom détermine les risques sur base de la situation de départ et de l'analyse des besoins et définit les mesures adéquates pour y remédier (également notamment dans la gestion des approvisionnements et des fournisseurs). Un plan de mise en œuvre possible est ensuite élaboré conjointement.

Détermination d'outils efficaces
Sur base de la matrice des risques élaborée, Swisscom analyse l'utilisation de solutions avec lesquelles vous pouvez augmenter durablement la sécurité de la chaîne d'approvisionnement logicielle. Il peut s'agir de processus spécifiques mais aussi de solutions basées sur des logiciels.

Services en option

L'équipe Consulting vous propose les services suivants en option:
Software Bill of Material as a Service (SBOMaaS)

Cas d'utilisation SBOM Management
- Génération d'une Software Bill of Material (SBOM) pour votre application spécifique.
- Identification de tous les composants et de leurs vulnérabilités dans votre Open et Closed Source.
- Traçabilité de tous les composants Open et Closed Source, internes et externes (prestataires tiers).
- Accompagnement du processus et intégration des preuves SBOM dans tous vos projets logiciels.

Cas d'utilisation Gestion des risques
- Des fonctions de recherche performantes trouvent en quelques secondes chaque dépendance sur base des risques, vulnérabilités ou autres informations.
- Aucun logiciel ou composant logiciel inconnu n'entrera dans un processus de fabrication du logiciel (software built) ou d'implémentation du logiciel (software deployment process).

Services supplémentaires

L'équipe Consulting vous propose les prestations supplémentaires suivantes:
Monitoring de votre chaîne d'approvisionnement logicielle

- Monitoring continu de tous les composants Open et Closed Source, internes et externes (prestataires tiers) sur une plateforme (SBOM).
- Gestion des vulnérabilités des conteneurs utilisés sur une plateforme de conteneurs.
- Hausse de la visibilité, meilleure compréhension et meilleur contrôle des chaînes d'approvisionnement TIC spécifiques à votre entreprise.

Vous trouverez de plus amples informations et les données de contact de nos experts sous
swisscom.ch/security-consulting

Swisscom (Suisse) SA Enterprise Customers, Case postale, CH-3050 Berne, tél. 0800 800 900, www.swisscom.ch/enterprise