



Applikationen von externen Softwareherstellern können unbekannte, manipulierte oder unsichere Komponenten enthalten, die Ihrem Unternehmen schaden könnten. Ist Ihre Software Supply Chain ausreichend geschützt?

Software-Supply-Chain-Angriffe (wie z. B. der Solar-Winds-Sunburst-Angriff im Dezember 2020) haben gezeigt, wie empfindlich und kritisch Software Supply Chains sind. Doch nur wer die Bedrohungslage und das Risiko kennt, kann geeignete Schutzmassnahmen definieren und umsetzen. Swisscom hilft Ihnen, Ihre aktuelle Risikolandschaft zu verstehen und Ihre ICT-Risiken

zu messen, Ihre Software-Supply-Chain-Management-Strategie zu definieren und die erforderlichen Massnahmen umzusetzen. Sie werden auch bei der Definition und Verwaltung relevanter ICT-Kriterien – im Zusammenspiel mit Ihren Lieferanten – und bei konkreten Empfehlungen und Massnahmen zu einer sicheren Software Supply Chain unterstützt.

Ihre Nutzen mit Secure Software Supply Chain

Transparenz und Risiko-Akzeptanz im Bereich der externen Software-Entwicklung

Vereinbarungen mit Ihren Software-Lieferanten werden auf sicherheitsrelevante Prozesse analysiert. Nicht vertrauenswürdige und gefährliche Software-Artefakte werden aufgelistet und können aus Ihrer Entwicklungs- und Produktionsumgebung entfernt werden.



Software Bill of Material as a Service (SBOMaaS)

Darstellung und Erläuterung der regulatorischen Vorgaben an eine Secure Software Supply Chain. Erzeugung einer Software Bill of Material (SBOM), mit welcher der Inhalt (Sourcecode), die Abhängigkeiten (Dependencies) sowie die Erstellung (Creation data) des eigentlichen SW-Pakets auditierbar erstellt und gespeichert werden können.

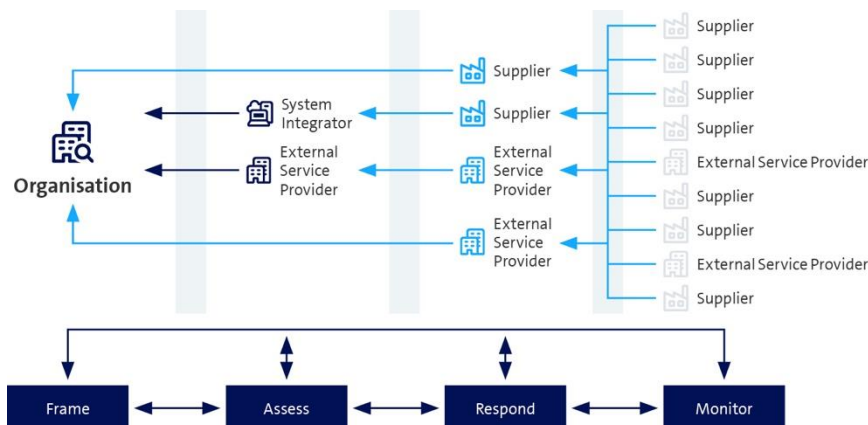


Monitoring Ihrer Software Supply Chain

Laufende Überprüfung der generierten bzw. durch Partner und Dritte eingelieferten SBOMs sowie kontinuierliche Bewertung der Dependencies durch Experten aus dem Consulting Team. Ihr Unternehmen kann somit den gewünschten Sicherheitslevel erreichen und bei neuen Schwachstellen in diesen Abhängigkeiten adäquat reagieren.



So funktioniert das Monitoring der Software Supply Chain





Facts & Figures

Basisleistungen

Was ist im Basispaket drin?

Workshop: Secure Software Supply Chain

Ausgangslage und Bedarfsanalyse

Swisscom wird Ihre Ausgangslage kennenlernen: Ihren Schutzbedarf, die Gefahren Ihrer Software Supply Chain, bestehende Schutzmassnahmen, Ihre Open-Source-Strategie, bereits verwendete Code Repositories und Artifacts, Vereinbarungen mit Ihren Software-Lieferanten.

Risk Assessment und Massnahmen

Aufgrund der Ausgangslage und der Bedarfsanalyse ermittelt Swisscom die Risiken und definiert dazu die passenden Massnahmen (unter anderem auch im Beschaffungs- und Lieferantenmanagement). Gemeinsam wird dann ein möglicher Umsetzungsplan erstellt.

Ermittlung von effizienten Werkzeugen

Aufgrund der erstellten Risikomatrix analysiert Swisscom den Einsatz von Lösungen, mit denen Sie die Software Supply Chain Security nachhaltig erhöhen können. Dies können spezifische Prozesse sein, aber auch Software-basierte Lösungen.

Optionale Leistungen

Folgende optionale Leistungen bietet das Consulting Team Ihnen:

Software Bill of Material as a Service (SBOMaaS)

Anwendungsfall SBOM Management

- Erzeugung einer Software Bill of Material (SBOM) für Ihre spezifische Applikation.
- Identifikation sämtlicher Komponenten und deren Schwachstellen in Ihrer Open und Closed Source.
- Nachvollziehbarkeit aller Open- und Closed-Source-Komponenten, intern und extern (Drittanbieter).
- Prozessbegleitung und Einbettung der SBOM-Nachweise in all Ihren SW-Projekten.

Anwendungsfall Risikomanagement

- Leistungsstarke Suchfunktionen finden in Sekundenschnelle jede Abhängigkeit basierend auf Risiken, Schwachstellen oder anderen Informationen.
- Keine unbekannt Software oder Softwarekomponente wird in einen Software-erstellungs- (software built) oder Softwarebereitstellungsprozess (software deployment process) eintreten.

Zusatzservices

Folgende Zusatzleistungen bietet das Consulting Team Ihnen:

Monitoring Ihrer Software Supply Chain

- Kontinuierliches Monitoring aller Open- und Closed-Source-Komponenten, intern und extern (Drittanbieter) auf einer Plattform (SBOM).
- Verwaltung der Schwachstellen der eingesetzten Container auf einer Container-Plattform.
- Erhöhung der Sichtbarkeit, besseres Verständnis und Kontrolle Ihrer unternehmensspezifischen ICT-Lieferketten.

Mehr Informationen und den Kontakt zu unseren Experten finden Sie auf swisscom.ch/security-consulting