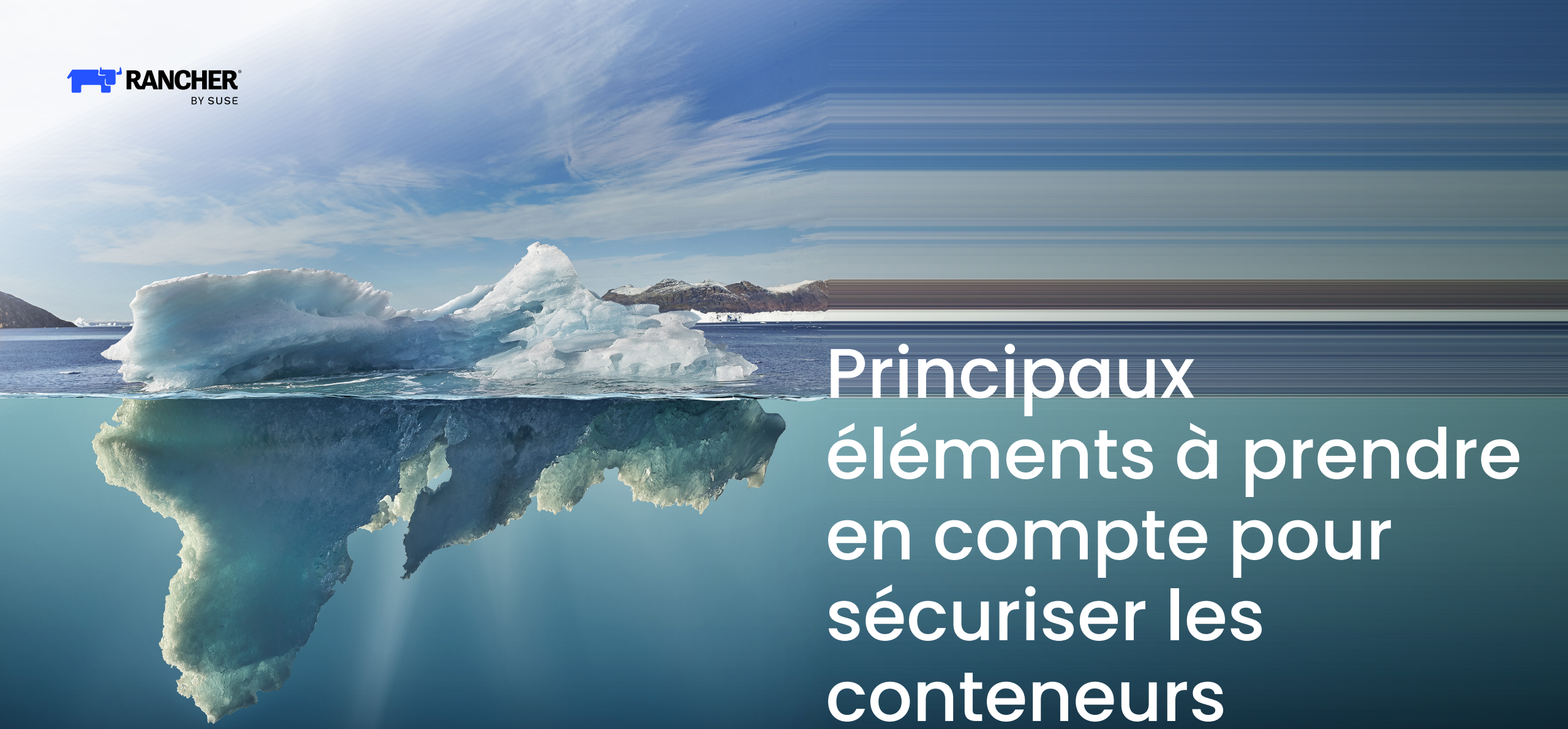
RANCHER
BY SUSE

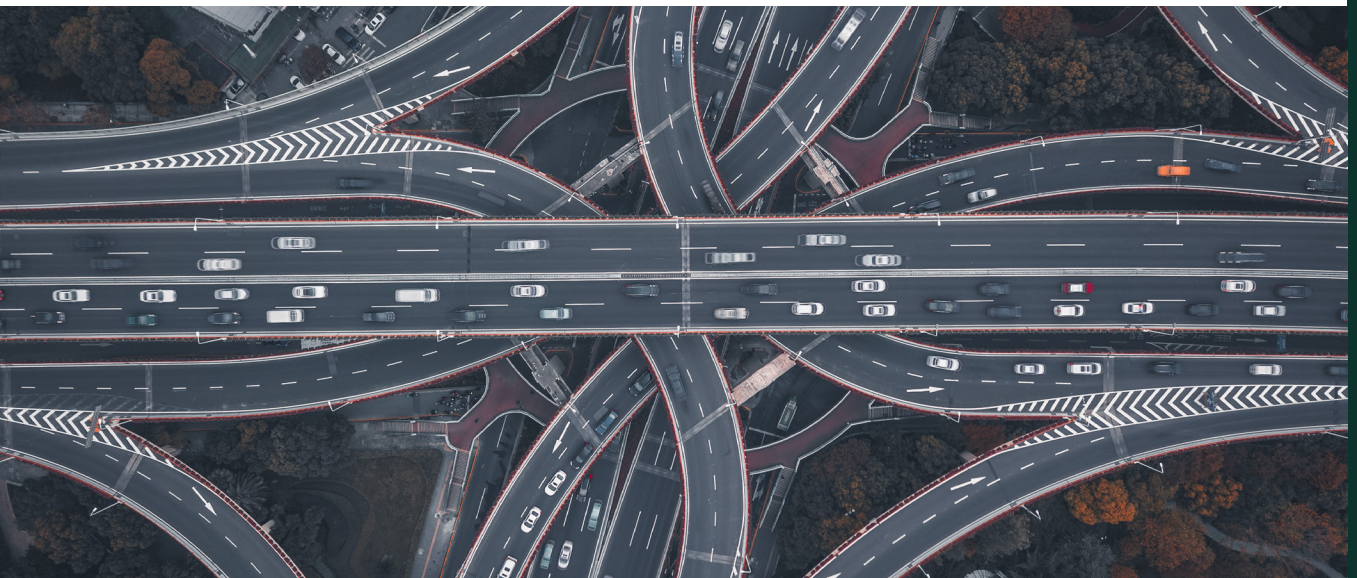


Principaux éléments à prendre en compte pour sécuriser les conteneurs

RANCHER
BY SUSE

Introduction

La sécurisation des conteneurs et des environnements Kubernetes, ainsi que de la chaîne d'approvisionnement logicielle dans son ensemble, n'a rien de glamour, mais elle est rapidement devenue l'un des sujets les plus importants et les plus commentés de l'informatique d'entreprise.



Une série de violations de données et d'autres incidents de sécurité, tels que le piratage SolarWinds et la vulnérabilité Log4j, a révélé l'urgence avec laquelle les entreprises doivent agir pour s'assurer que leurs pipelines de développement et de logiciels ne les exposent pas à des risques inutiles. Il s'agit ici de chaque élément de rédaction, création, déploiement et gestion de leurs applications et services logiciels. Le gouvernement fédéral des États-Unis a même publié un décret sur la cybersécurité et des conseils connexes sur l'amélioration de la sécurité des logiciels et de la chaîne d'approvisionnement de développement.

Les risques potentiels des approches réactives et héritées en matière de sécurité de la chaîne d'approvisionnement sont trop importants pour être ignorés.

Les pirates utilisent un large éventail de points d'entrée différents dans les pipelines de développement et de logiciels pour déployer des logiciels malveillants, des ransomwares et d'autres menaces, dans le but de perturber les opérations métier, de voler des ressources financières, d'accéder à des données personnelles ou sensibles et à d'autres fins malveillantes. Cela expose les entreprises à des risques importants pour la réputation de leur marque, l'expérience client et, en fin de compte, leurs résultats.

C'est pourquoi la sécurité, le renforcement des pipelines de développement et les chaînes d'approvisionnement sont devenus des sujets importants, et pourquoi les entreprises de tous les secteurs doivent prendre des mesures pour les hiérarchiser. Dans cet ebook, nous approfondirons la sécurité de la chaîne d'approvisionnement en matière de conteneur natif dans le cloud, les défis qu'elle représente et les solutions disponibles.

RANCHER BY SUSE

Qu'est-ce que la sécurité de la chaîne d'approvisionnement des conteneurs ?

Alors que de nombreuses personnes associent la « chaîne d'approvisionnement » à la production de marchandises physiques (tout ce qu'il faut pour fabriquer une voiture ou approvisionner les magasins, par exemple), le concept est tout aussi pertinent pour les pipelines et processus de développement modernes, en particulier dans les environnements conteneurisés gérés avec Kubernetes.

La chaîne d'approvisionnement des environnements basés sur conteneur renvoie à tout ce qui est nécessaire pour écrire, créer, déployer et faire fonctionner des applications et services natifs dans le cloud, des bibliothèques Open Source aux composants logiciels commerciaux en passant par les pipelines CI/CD et les chaînes d'outils DevOps, et bien plus encore.

La sécurisation de la chaîne d'approvisionnement de Kubernetes est devenue une priorité cruciale : c'est essentiel pour les entreprises qui veulent rapidement faire évoluer et développer leurs activités de manière résiliente.

Pourtant, cela pose des défis considérables : les équipes d'ingénierie utilisent plus de composants, de bibliothèques, de processus et d'outils que jamais dans leurs applications et services, en particulier lorsqu'elles adoptent des technologies et des modèles natifs dans le cloud tels que les conteneurs, l'orchestration de conteneurs et les microservices. Ces solutions offrent de nouvelles fonctionnalités et opportunités puissantes aux entreprises, mais elles modifient et élargissent considérablement leur surface de menace en introduisant une myriade de nouvelles vulnérabilités potentielles tout au long de leur chaîne d'approvisionnement.

En outre, la complexité croissante du développement d'applications natives cloud va de pair avec l'infrastructure sur laquelle ce développement est exécuté. Le « réseau » est donc un terme de plus en plus flou, et les défenses axées sur le périmètre ne suffisent plus. Les équipes de développement modernes déploient leurs applications dans un datacenter principal et, de plus en plus, dans plusieurs clouds. De plus, les architectures de type « edge computing » permettent à ces entreprises d'étendre leurs environnements centralisés aux environnements et aux noeuds d'extrémité les plus éloignés de leur entreprise, ce qui augmente encore leur surface de menace.

L'écosystème animé autour de la conteneurisation et du développement natif dans le cloud n'est pas seulement attractif pour les entreprises légitimes. Il l'est également pour les cybercriminels et autres acteurs malveillants, qui opèrent eux-mêmes comme des entreprises et recherchent constamment de nouvelles opportunités pour attaquer les systèmes professionnels.

Les personnes mal intentionnées aiment attaquer les plates-formes et outils émergents, notamment parce que les plates-formes matures comme Enterprise Linux sont déjà très sécurisées lorsqu'elles sont correctement renforcées. La diversité et la vitesse de la chaîne d'approvisionnement moderne, basée sur les conteneurs, leur offrent un grand nombre de nouveaux vecteurs de menaces si les entreprises ne prennent pas les mesures nécessaires pour renforcer et sécuriser leurs pipelines. Ces dernières années, les attaques sur la chaîne d'approvisionnement ont été à l'origine d'un grand nombre de violations de grande envergure, telles que celles ayant touché SolarWinds et Mimecast.

RANCHER BY SUSE

Composants de l'environnement de création Open Source

Une chaîne d'approvisionnement Kubernetes sécurisée nécessite une combinaison appropriée d'outils, de processus, de stratégies et de culture, et doit être basée sur un modèle Zero Trust, pour permettre aux organisations de créer, d'itérer et de faire évoluer leurs logiciels rapidement sans s'exposer à des risques inutiles.

Elle doit notamment tenir compte de tous les composants de développement qui relient les projets Open Source ou le code communautaire aux systèmes d'entreprise ou orientés client. En voici quelques exemples :

Sélection du code

Révision du package

Tests automatisés

Tests manuels

Build Service

Service de distribution

300-400 %
Pourcentage de croissance des attaques de la chaîne d'approvisionnement logicielle en 2021, selon des études distinctes.

Security Today, ENISA

265 G $
Le montant que les attaques par ransomware coûteront aux entreprises du monde entier d'ici 2031.

ZDNet

60 %
Le pourcentage d'entreprises touchées qui ont peut-être payé la rançon d'une attaque par ransomware en Europe.

ENISA

9 M $
Le coût moyen d'une violation de données dans une entreprise basée aux États-Unis.

Statista

10,5 T $
Le coût global de toute la cybercriminalité d'ici 2025.

Cybersecurity Ventures

RANCHER BY SUSE

Les défis : technologie, personnes et processus

Le paysage natif du cloud est immense. L'écosystème Open Source est plus dynamique que jamais, mais tous les logiciels ne sont pas fiables immédiatement. Chaque nouvel élément de code, chaque nouveau composant, chaque nouveau partenaire technologique, chaque nouvel outil augmente la surface de menace d'une entreprise et introduit des vulnérabilités potentielles.

Ajoutez à cela la nature de plus en plus hybride et/ou distribuée de l'infrastructure informatique de nombreuses entreprises, et le besoin d'une chaîne d'approvisionnement de conteneurs sécurisée devient presque évident, en particulier à la suite de violations très médiatisées comme le piratage de SolarWinds. Mais la diversité des applications et de l'infrastructure actuelles crée des défis considérables qui doivent être résolus.

En voici quelques exemples :

- **Mauvaises configurations :** les outils et technologies mal configurés constituent un point d'entrée courant pour les pirates à différents endroits de la chaîne d'approvisionnement logicielle traditionnelle. Par exemple, les erreurs de configuration des comptes cloud ou les utilisateurs avec des privilèges trop élevés sont des vulnérabilités courantes. Il en va de même pour les outils natifs dans le cloud tels que Kubernetes. Les fonctionnalités robustes qui en font un outil si puissant peuvent également devenir des vecteurs d'attaque lorsqu'elles ne sont pas correctement configurées et gérées.
- **Vulnérabilités connues ou inconnues du code :** on le sait, la plupart des applications sont construites avec d'autres logiciels. Qu'il s'agisse de code provenant d'un dépôt Open Source, d'une image de conteneur issue d'un registre partagé ou de tout autre composant, ces éléments peuvent introduire des vulnérabilités connues (et inconnues) dans vos propres applications s'ils ne sont pas correctement approuvés et intégrés.
- **Mauvaise visibilité :** une infrastructure distribuée peut entraîner des silos cloisonnés lorsqu'elle n'est pas conçue dans un souci de visibilité et de monitoring, ce qui crée des angles morts qui permettent aux attaquants d'agir dans vos environnements sans être détectés.
- **Processus et stratégies faibles :** stratégies faibles ou inexistantes concernant l'accès et les privilèges des utilisateurs, systèmes d'exploitation non sécurisés ou obsolètes, cycle de vie des applications, etc.
- **Automatisation « Set and Forget » :** l'automatisation est une arme majeure dans la lutte contre le cybercrime, mais uniquement lorsqu'elle est supervisée et optimisée à mesure que les conditions changent.
- **Erreur humaine :** l'humain reste l'un des éléments les plus importants (et souvent les plus vulnérables) de la chaîne d'approvisionnement des conteneurs, en raison du manque de formation, de hiérarchisation et de culture en matière de sécurité. Le phishing est l'un des principaux vecteurs d'attaques par ransomware. Les attaquants utilisant ce type d'attaques comptent essentiellement sur les erreurs humaines pour accéder aux données et systèmes sensibles.
- **Menaces externes :** bien que les incidents puissent se produire simplement en raison de mauvaises pratiques de sécurité, les organisations elles-mêmes proactives sur ce front sont confrontées à un nombre croissant de menaces externes provenant de pirates informatiques et autres acteurs malveillants.

RANCHER
BY SUSE

Clés pour sécuriser la chaîne d'approvisionnement des conteneurs

La sécurisation de la chaîne d'approvisionnement des conteneurs nécessite de se pencher sur trois domaines clés :

- **Source :** code vulnérable ou exploité introduit au cours du développement.
- **Création :** tous les composants et processus de la phase de création, tels qu'une version qui contourne le système CI/CD ou un package compromis.
- **Dépendances :** toutes les dépendances externes dont une application a besoin pour s'exécuter correctement, mais qui peuvent introduire des vulnérabilités.

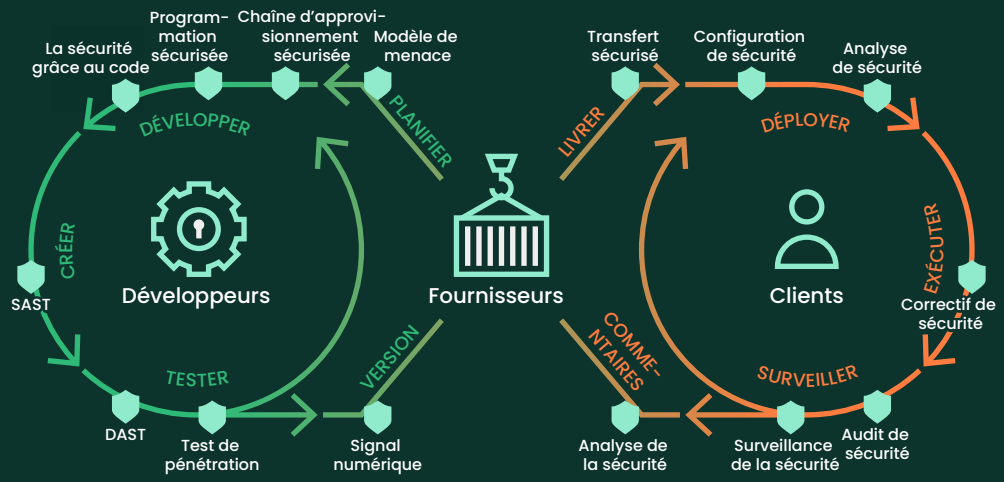
La résolution des défis complexes inhérents aux pipelines de développement modernes nécessite une approche globale qui englobe la technologie, les processus et les personnes. Vous devez également choisir les bons fournisseurs et partenaires, ceux qui offrent non seulement des produits sécurisés, mais également des certifications robustes et des offres de support d'entreprise qui vous garantissent qu'ils seront à votre disposition quand vous en aurez le plus besoin. Les incidents peuvent se produire, même en ayant mis en place les mesures de sécurité les plus strictes. Lorsqu'ils surviennent, vous devez avoir la certitude que vos fournisseurs et partenaires seront là pour vous aider, afin de vous permettre d'atténuer le problème rapidement et de minimiser les perturbations pour l'entreprise.

La sécurité de votre chaîne d'approvisionnement de conteneurs équivaut à celle de votre élément le plus faible. Elle doit donc correspondre à une stratégie complète, avec l'engagement de toute l'organisation et de tous les prestataires qui doivent choisir, dans la mesure du possible, des fournisseurs certifiés.

Il existe des moyens supplémentaires pour sécuriser la chaîne d'approvisionnement des conteneurs :

- Utilisation de produits disposant de certificats de sécurité pertinents et conformes aux normes du secteur.
- Exploitation des outils de gestion du cycle de vie du système et d'automatisation compatibles avec les produits certifiés.
- Application de la signature d'artefact à toutes les couches et validation permanente des signatures et des sommes de contrôle.
- Adoption de l'automatisation : la sécurisation de votre chaîne d'approvisionnement peut s'avérer difficile si elle est mise en oeuvre manuellement. Tirez donc parti d'outils d'automatisation tels que Salt ou Ansible.

Secure Software Development Process



cisa.gov

RANCHER BY SUSE

Modernisation de la technologie et des outils

La sécurité d'une chaîne d'approvisionnement de conteneurs dépend du choix des technologies et partenaires technologiques appropriés, non seulement pour les outils de sécurité eux-mêmes, mais aussi pour l'ensemble de la pile d'infrastructure.

Pour protéger l'ensemble de la chaîne d'approvisionnement, les équipes doivent s'efforcer de renforcer leur pile avec une approche ascendante.

Cela implique de s'appuyer sur des plates-formes et des outils dotés de certifications, de conformité et de sécurité solides, complétés par une prise de décision humaine efficace, un code hautement qualitatif et des processus optimisés qui minimisent les surfaces d'attaque.

L'une des mesures qui s'imposent est l'examen des certifications et des attributs associés d'un fournisseur. Voici quelques éléments à rechercher dans votre évaluation des outils et partenaires technologiques potentiels :

Exemples de certifications et d'autres attributs à rechercher dans vos outils et chez vos partenaires technologiques :

- La certification CC (Common criteria) EAL4+ : la certification EAL4+ est exhaustive et difficile à obtenir. EAL4+ couvre le processus de création Open Source lui-même, mais également tout ce qui l'entoure : RH (comment les employés sont embauchés), systèmes informatiques internes (services d'authentification et d'autorisation, antivirus, sécurisation renforcée des PC, etc.) et sécurité physique (accès aux datacenters, surveillance, etc.). Il faut beaucoup de temps et d'argent pour obtenir la certification EAL4+. Seules les entreprises réellement soucieuses de leur sécurité l'ont.
- Conformité de la transition FIPS 140-2 et 3 : indique les exigences de sécurité qui seront satisfaites par un module cryptographique, avec quatre niveaux qualitatifs progressifs destinés à couvrir une large gamme d'applications et d'environnements potentiels. Les domaines couverts, liés à la conception et à la mise en oeuvre sécurisées d'un module cryptographique, comprennent la spécification, les ports et les interfaces, les rôles, les services, et l'authentification, les modèles à nombre d'états fini, la sécurité physique, l'environnement opérationnel, la gestion des clés cryptographiques, les interférences électromagnétiques et la compatibilité électromagnétique, les auto-tests, l'assurance de la conception et l'atténuation d'autres attaques.
- Conformité STIG : norme de configuration consistant en des exigences de cybersécurité pour un produit spécifique. STIG permet de mettre en place une méthodologie de sécurisation des protocoles au sein des réseaux, des serveurs, des ordinateurs et des conceptions logiques afin d'améliorer la sécurité globale. Lorsqu'ils sont mis en oeuvre, ces guides améliorent la sécurité des logiciels, du matériel et des architectures physiques et logiques afin de réduire davantage les vulnérabilités.
- Conformité SCAP : le SCAP (Security Content Automation Protocol) est une synthèse des spécifications interopérables issues des idées de la communauté. La participation de la communauté est un atout considérable pour SCAP, car la communauté de l'automatisation de la sécurité garantit que le plus grand nombre possible de cas d'utilisation est reflété dans la fonctionnalité SCAP.
- Prise en charge du registre privé : pour les applications conteneurisées, les plates-formes qui offrent une prise en charge du registre privé, incluant notamment des capacités d'analyse, peuvent offrir des avantages significatifs en termes de sécurité et de gouvernance, car les images fournies ont passé avec succès des filtres et des tests cohérents, et ont été choisies par des professionnels.
- SLSA : parrainé par la Fondation Linux, SLSA est un ensemble émergent de normes et de contrôles techniques en faveur de la sécurité de la chaîne d'approvisionnement logicielle. Il s'agit d'un sous-ensemble plus petit par rapport à EAL4+, mais qui aborde des sujets intéressants tels que la création d'un format décrivant le processus de construction afin qu'il puisse être reproduit par des tiers si nécessaire (il peut s'agir de clients d'autorités de certification). SLSA a été soumis au NIST pour normalisation.
- SBOM (Software Bill of Materials) : bien qu'il ne s'agisse pas d'une certification, SBOM couvre le travail difficile qui consiste à s'assurer que tous les composants d'une solution logicielle sont correctement identifiés et contrôlés. Il existe différentes options SBOM, mais SPDX semble devenir la norme pour la communication SBOM pour plusieurs fournisseurs et plates-formes.

RANCHER BY SUSE

Hiérarchisation des processus et des stratégies sécurisés

La technologie seule ne sécurisera pas le pipeline logiciel de bout en bout. Les organisations doivent également mettre en œuvre des politiques et des processus intelligents qui donnent aux équipes la liberté de travailler rapidement, mais avec des garde-fous pour s'assurer qu'elles n'introduisent pas de risques ou de menaces inutiles.

En voici quelques exemples :

- **Maintenance proactive :** application de correctifs, mises à jour, mises à niveau et gestion du cycle de vie de manière proactive et opportune afin de minimiser les bugs et les failles connus.
- **Normalisation et cohérence :** mise en oeuvre des politiques et des processus cohérents et standardisés dans l'ensemble de l'organisation et de son écosystème logiciel plus large.
- **Automatisation de la sécurité :** exploitation des analyses de vulnérabilité automatisées et d'autres technologies telles que les outils de gestion de la configuration pour renforcer l'intelligence humaine et la surveillance, en intégrant ces mécanismes de sécurité à vos processus automatisés.
- **Approche déclarative :** utilisation des principes Zero Trust pour définir et vérifier en permanence l'état de votre choix et interdire toute autre activité et tout autre comportement, que ce soit de la part d'un utilisateur humain ou d'une application/d'un service.
- **Contrôle d'admission :** également appelé contrôle d'accès, il s'agit de pratiques et de processus permettant de limiter l'accès des personnes et des systèmes aux données, aux applications, aux réseaux et à d'autres ressources.

RANCHER PRIME

Rancher Prime

Rancher Prime vous aide à faire évoluer vos conteneurs en toute confiance. Rancher Prime est une solution complète conçue pour aider les utilisateurs de Rancher à tirer le meilleur parti de leur souscription d'entreprise et à développer la continuité et l'assurance métier dont ils ont besoin dans les environnements Kubernetes à croissance rapide.

Rancher Prime offre à ses utilisateurs :

- L'accès à une plate-forme Rancher fortifiée
- Le support technique d'une équipe d'experts Kubernetes de premier plan
- Des services professionnels en option pour aider les organisations à être opérationnelles en deux jours et à mettre en oeuvre les meilleures pratiques de sécurité

RANCHER
BY SUSE

Création d'un état d'esprit axé sur la sécurité

Ces dernières années, l'accent a été mis sur le glissement de la sécurité dans le cycle de développement logiciel : les tactiques de sécurité telles que les analyses de vulnérabilité automatisées doivent être déplacées vers les premières phases du développement logiciel pour garantir la sécurité de la chaîne d'approvisionnement. C'est un gros changement par rapport aux approches héritées, où la sécurité était traitée comme une étape ou une vérification unique, souvent juste avant le déploiement.

Ce concept de glissement doit s'appliquer non seulement à la technologie, mais aussi aux personnes : les organisations doivent promouvoir et récompenser une culture qui privilégie la sécurité partout, pas seulement au sein d'une seule équipe.

Cela inclut la sensibilisation et la formation à la sécurité (y compris pour le personnel non technique), l'adoption des principes DevOps et/ou DevSecOps, l'instauration d'une culture sans reproches qui récompense les personnes pour l'accent mis sur la sécurité (au lieu de punir les faux pas) et la possibilité pour les équipes de développement d'agir rapidement, avec la certitude que des garde-fous sont en place pour garantir que la vitesse ne sacrifie pas la sécurité et la fiabilité.

Gardez également à l'esprit que la priorisation de la sécurité doit également inclure vos fournisseurs et partenaires technologiques. Il est essentiel de choisir et de travailler avec des fournisseurs et des partenaires qui ont également un état d'esprit axé sur la sécurité.

Cela réduit la probabilité d'incorporer des composants risqués ou compromis dans votre chaîne d'approvisionnement basée sur Kubernetes. Mais, et c'est également important, il faut admettre la réalité : les erreurs et les incidents peuvent se produire. En matière de cybersécurité, le risque zéro n'existe pas. Vous devez avoir la certitude que vos fournisseurs et partenaires seront là pour vous lorsque des incidents se produiront, et qu'ils agiront rapidement afin de limiter l'impact du problème et de vous permettre de reprendre vos activités le plus rapidement possible.

NeuVector

SUSE NeuVector

SUSE NeuVector est une solution de sécurité de conteneur tout au long de son cycle de vie. Il s'agit d'une plate-forme de sécurité de conteneur Zero Trust 100 % Open Source qui couvre l'ensemble du cycle de vie du conteneur, de l'analyse des vulnérabilités et de la conformité à la sécurité d'exécution.

- Arrêtez les attaques sur la couche 7 avant qu'elles n'atteignent l'application et qu'elles puissent être intégrées à n'importe quel pipeline CI/CD pour les plates-formes Kubernetes grâce à des fonctionnalités d'inspection approfondie des paquets de la couche 7
- Analysez le conteneur en continu tout au long de son cycle de vie
- Éliminez les obstacles à la sécurité
- Dès le début, appliquez des stratégies de sécurité pour optimiser l'agilité des développeurs

RANCHER BY SUSE

Mise en oeuvre du modèle Zero Trust

Le modèle Zero Trust est à la base d'une chaîne d'approvisionnement de conteneurs sécurisée. Le modèle Zero Trust repose sur le principe du moindre privilège : tout utilisateur ou système au sein de l'environnement ne doit disposer que des droits d'accès et des privilèges dont il a explicitement besoin pour exécuter sa fonction, et rien d'autre.

Autrement dit, l'approche Zero Trust passe des mesures de sécurité réactives traditionnelles (qui atténuent les menaces uniquement une fois qu'elles sont détectées) à une approche plus proactive et déclarative, dans laquelle l'organisation définit une utilisation ou un comportement acceptable et interdit tout le reste. Par exemple, vous ne donnez jamais à un utilisateur (qu'il s'agisse d'un employé, d'un partenaire ou d'autres acteurs) ou à une application l'accès à des données dont il n'a pas réellement besoin.

Du point de vue de la sécurité de la chaîne d'approvisionnement, c'est essentiel, car cela limite la possibilité pour un pirate d'exploiter un point de vulnérabilité unique pour se déplacer librement dans un environnement et compromettre d'autres ressources.

Harvester

Conçu pour aider les opérateurs à consolider et unifier les charges de travail de leurs machines virtuelles avec les clusters Kubernetes, Harvester est la nouvelle génération de solutions d'infrastructure Open Source hyperconvergées conçues pour les environnements natifs modernes dans le cloud. Harvester peut être intégré à Rancher pour offrir une expérience unifiée permettant de déployer des conteneurs et des charges de travail de machines virtuelles n'importe où. Cliquez ici pour en savoir plus sur Harvester.

Longhorn

Longhorn est un projet CNCF officiel qui propose une puissante plate-forme de stockage distribué, qui peut fonctionner n'importe où et native dans le cloud, pour Kubernetes. Associé à Rancher, Longhorn facilite, accélère et garantit la fiabilité du déploiement d'un stockage permanent de blocs à haute disponibilité dans votre environnement Kubernetes. Cliquez ici pour en savoir plus sur Longhorn.

Kubewarden

Kubewarden est un moteur de stratégies pour Kubernetes qui permet d'appliquer la stratégie en tant que code. Il aide les opérateurs à maintenir la sécurité et la conformité de leurs clusters Kubernetes en écrivant des stratégies dans le langage de programmation de leur choix via WebAssembly. Avec Kubewarden, les opérateurs peuvent écrire, distribuer, publier et créer des stratégies partout. Cliquez ici pour en savoir plus sur Kubewarden.

RKE2

RKE2 est la distribution Kubernetes nouvelle génération de SUSE. Conçu à l'origine pour répondre aux exigences en matière de sécurité et de conformité des environnements gouvernementaux fédéraux, RKE2 passe le Benchmark CIS de Kubernetes avec une intervention minimale de la part des administrateurs, tout en permettant la conformité à la norme FIPS 140-2. Cliquez ici pour en savoir plus sur RKE2.

L’atout SUSE

SUSE fait partie d’un petit groupe d’entreprises qui connaissent les vulnérabilités critiques avant qu’elles ne soient largement publiées, ce qui nous permet d’apporter rapidement des correctifs et des mises à jour, et de minimiser les risques. Preuve de notre engagement en matière de sécurité de la chaîne d’approvisionnement logicielle, nous sommes certifiés CC (Common Criteria) EAL4+ et conformes à la norme FIPS 140-2/3. Nous continuons de proposer une large gamme d’autres protocoles, processus et documentations de sécurité robustes.

Le portefeuille de solutions natives dans le cloud Rancher by SUSE a été spécialement conçu pour permettre aux organisations de tirer parti de la puissance des technologies natives dans le cloud et Open Source tout en garantissant la sécurité, l’intégrité et la résilience de l’ensemble de leur chaîne d’approvisionnement de conteneurs. Rancher Prime hébergé est conforme à la norme SOC 2 Type 1, et notre nouvelle distribution Kubernetes renforcée certifiée RKE2 est certifiée FIPS 140-2 et approuvée par la DISA. Dans le cadre de notre engagement en matière de sécurité de la chaîne d’approvisionnement de conteneurs, nous cherchons également à obtenir la certification FIPS 140-3 et SLSA niveau 2 et 3 pour Rancher Prime, prévue pour 2023.

Notre approche complète visant à aider les organisations à renforcer la sécurité de leur chaîne d’approvisionnement de conteneurs est évidente au vu de notre vaste portefeuille.

Rancher Prime

L’offre complète de solutions d’entreprise SUSE pour Rancher, la plate-forme de gestion Kubernetes préférée de la communauté. Cette offre permet aux utilisateurs d’accéder à une plate-forme Rancher renforcée, à une équipe d’assistance composée d’experts Kubernetes de premier plan et à des services professionnels, le tout dans un seul et même abonnement.

Conçu pour les utilisateurs de Rancher qui recherchent une valeur supplémentaire à leur investissement dans Kubernetes et qui veulent renforcer leur pipeline d’applications de conteneurs avec des garanties de sécurité, Rancher Prime aide à renforcer la résilience sur l’ensemble des chaînes d’approvisionnement de conteneurs en permettant d’être opérationnel en deux jours et en offrant une unification des charges de travail hybrides et multiclusters et une option de déploiement à partir d’un registre de conteneurs privés fiable.

Rancher Prime s’intègre également à d’autres solutions natives dans le cloud telles que SUSE NeuVector, Harvester et Longhorn pour fournir aux utilisateurs une base permettant de construire un écosystème d’outils à la fois sécurisé et ouvert afin de garantir la mise en oeuvre des meilleures pratiques opérationnelles et de sécurité dans des environnements de conteneurs qui font partie d’une chaîne d’approvisionnement logicielle globale. De plus, Rancher Prime travaille à l’obtention des certifications SLSA Level 2 et 3 et FIPS 140-3 en 2023 afin d’étendre la garantie de conformité et d’assurance de SUSE en tant que fournisseur technologique de confiance. Cliquez ici pour en savoir plus sur Rancher Prime.

RANCHER BY SUSE

L'atout SUSE (suite)

RKE 2

Rancher Kubernetes Engine 2 (RKE2)

La distribution Kubernetes nouvelle génération de Rancher by SUSE. Entièrement conforme et axé sur la sécurité et le respect des règles, RKE2 fournit des options par défaut et de configuration qui permettent aux clusters de réussir le benchmark CIS de Kubernetes avec une intervention minimale de l'opérateur. RKE2 permet également la conformité à la norme FIPS 140-2 et analyse régulièrement les composants pour détecter les CVE.

RKE2 combine les meilleurs composants des principales distributions développées et gérées par SUSE, RKE et K3s. Il hérite la facilité d'utilisation et le modèle de déploiement de K3s, et il hérite l'alignement sur Kubernetes en amont de RKE. Cliquez ici pour en savoir plus sur RKE2.

NeuVector

SUSE NeuVector

Une plate-forme de sécurité de conteneur entièrement Open Source qui utilise un modèle de sécurité en tant que code pour appliquer le contrôle d'accès Zero Trust à tous les réseaux, applications et environnements dès la première phase du processus de développement logiciel.

NeuVector offre une gestion des vulnérabilités de bout en bout, une sécurité automatisée des pipelines CI/CD, une sécurité complète des temps d'exécution et une protection contre les menaces internes et les failles zero-day. Étant donné qu'il s'agit d'un système Open Source et natif de Kubernetes, il fonctionne avec n'importe quelle plate-forme de gestion de conteneurs de premier plan.

Mieux encore, il s'intègre à Rancher Prime, ce qui signifie que vous pouvez déployer une stratégie de sécurité Zero Trust agressive sur l'ensemble de votre environnement Kubernetes en quelques clics. Cliquez ici pour en savoir plus sur SUSE NeuVector.

Enfin, une grande variété de projets sous-jacents, tels que **Kubewarden**, un moteur de stratégies pour Kubernetes, **Harvester**, pour l'infrastructure hyperconvergée et **Longhorn**, pour le stockage de blocs natif dans le cloud, vous permettent d'obtenir le même engagement en matière de sécurité sur l'ensemble de votre pile et de suivre le rythme de l'écosystème natif dans le cloud en constante évolution.

RANCHER BY SUSE

Solutions SUSE conçues pour vous aider à construire une chaîne d'approvisionnement de conteneurs sécurisée

Pile de solutions de conteneurs d'entreprise

Services de développeurs	EPINIO	Epinio fournit des environnements sécurisés préconfigurés pour que les développeurs puissent mettre leur code en production.
	SLE BCI	SLE BCI (Base Container Images, images de conteneur de base) est basé sur SLE et fournit donc la même sécurité, notamment la chaîne d'approvisionnement logicielle sécurisée, afin que vous puissiez lancer vos applications en toute sécurité.
RANCHER PRIME	KUBEWARDEN	Kubewarden améliore OPA pour vous éviter d'apprendre un nouveau langage spécifique à un domaine ou un langage de requête, et vous permet de répartir des stratégies à l'aide de registres de conteneurs.
	Open Policy Agent	Open Policy Agent facilite le contrôle basé sur des stratégies pour les environnements natifs du cloud en fournissant la stratégie en tant que code et des API simples pour décharger la prise de décision de vos logiciels.
	NeuVector	NeuVector, une plate-forme de sécurité de conteneur complète proposée par SUSE, fournit les outils permettant une approche Zero Trust pour les conteneurs ainsi que la conformité, la défense en profondeur et l'analyse et la gestion des vulnérabilités.
Kubernetes	RKE 2	Entièrement conforme et axé sur la sécurité et le respect des règles, RKE2 fournit des options par défaut et de configuration qui permettent aux clusters de réussir le benchmark CIS de Kubernetes avec une intervention minimale de l'opérateur. RKE2 permet également la conformité à la norme FIPS 140-2 et analyse régulièrement les composants pour détecter les CVE.
	K3S	K3S apporte une sécurité supplémentaire en plus de Kubernetes upstream en activant la conformité FIPS 140-2, en analysant régulièrement les composants pour détecter les CVE et en utilisant des conteneurs au moment de l'exécution.
Infrastructure de base	HARVESTER	Harvester fournit une couche de sécurité supplémentaire, car vous pouvez apporter différents niveaux d'isolation aux machines virtuelles que vous exécutez, ainsi que de nombreux avantages de sécurité hérités de Kubernetes.
	Gamme SLE	Les distributions SLE sont certifiées aux plus hauts niveaux pour les certifications CC (Common Criteria) EAL 4+ et FIPS 140-2 sur x86-64, Arm et IBM Z. AppArmor et SELinux sont tous deux pris en charge, tout comme les Confidential VM sur Google Cloud Platform.

Création de valeur pour nos clients

SUSE est l'un des premiers utilisateurs de SLSA, et nous avons déjà atteint le niveau 4 dans l'ensemble de nos activités sur Linux. Nous avons l'intention d'atteindre le niveau 2 pour Rancher Prime en 2023. SUSE a constamment démontré, et confirmé par des validateurs et autorités de certification externes, que la sécurité est au coeur de nos activités et que nous investissons massivement pour être le fournisseur de logiciels d'infrastructure le plus sécurisé du marché.

Notre engagement en matière de certification et de validation externe crée de la valeur ajoutée pour nos clients, non seulement en leur donnant confiance en nos solutions, mais également parce qu'ils peuvent réutiliser la documentation et les procédures de nos certifications pour simplifier leur propre processus d'acquisition et de certification de logiciels, et renforcer l'ensemble de la chaîne d'approvisionnement de leur infrastructure au passage.

La sécurité ayant toujours été au coeur de la mission de SUSE, nos services professionnels et de support de premier plan sont extrêmement compétents pour minimiser les risques sur l'ensemble des pipelines et processus de développement natifs dans le cloud.

Nos agents professionnels expérimentés sont équipés pour former le personnel interne et mettre en oeuvre les meilleures pratiques en matière de conteneurs et de leur sécurité.

Enfin, les ISV et autres partenaires qui s'appuient sur la pile de SUSE n'ont généralement besoin de certifier que leur propre couche supérieure et non la pile complète grâce à nos investissements en matière de sécurité, de conformité et de gouvernance. Cela permet à ces partenaires d'offrir une valeur ajoutée considérable à leurs propres clients en adaptant leurs solutions à des secteurs tels que la santé et les services financiers, où la sécurité et les certifications sont des éléments incontournables.

Découvrez dans quelle mesure l'équipe de Rancher by SUSE peut vous aider à sécuriser votre chaîne d'approvisionnement de conteneurs pour que votre organisation puisse développer et faire évoluer ses activités avec résilience.

RANCHER
BY SUSE

SUSE est un leader mondial en matière de solutions Open Source innovantes, fiables, sécurisées et adaptées aux besoins des entreprises. Plus de 60 % des entreprises du classement Fortune 500 font confiance à SUSE pour exécuter leurs workloads stratégiques. Notre entreprise est spécialisée dans les solutions Linux stratégiques, de gestion des conteneurs d'entreprise et de périphérie. Nous collaborons avec des partenaires et des communautés pour permettre à nos clients d'innover partout, depuis le datacenter jusqu'au cloud, en passant par la périphérie et au-delà.

SUSE renforce l'Open Source en offrant aux clients la flexibilité nécessaire pour relever les défis actuels en matière d'innovation, et la liberté de faire évoluer leur stratégie et leurs solutions à l'avenir. L'entreprise emploie plus de 2 000 personnes dans le monde. SUSE est cotée à la Bourse de Francfort.

Pour en savoir plus, contactez SUSE aux numéros suivants :

+1 800 796 3700 (États-Unis/Canada)

Maxfeldstrasse 5

90409 Nuremberg

www.suse.com