Les 6 piliers d'une pratique **DevSecOps performante**

splunk>
turn data into doing®

La croissance fulgurante du DevOps que l'on observe actuellement est loin d'être surprenante. Parmi ses nombreux avantages, le DevOps permet aux entreprises de raccourcir le cycle de vie du développement logiciel (SDLC) et d'assurer une livraison continue de logiciels de haute qualité. Les entreprises poursuivent leur transition vers le cloud, et le DevOps les aide à se développer et à évoluer rapidement, en réduisant le délai de mise sur le marché tout en accélérant la création de valeur pour les clients.

La disponibilité immédiate des ressources de cloud computing et la prolifération des référentiels de logiciels et de code open source ont aidé les entreprises à devenir des producteurs de logiciels prolifiques. Pour cette raison, le DevOps est devenu une option séduisante pour des projets de plus en plus nombreux et variés, et cette approche est sortie d'une obscurité relative pour devenir un ensemble de pratiques largement acceptées et courantes. Selon une étude menée en 2021 auprès de décideurs d'acquisition de services cloud aux États-Unis et au Royaume-Uni par ClearPath Strategies, une société indépendante de conseil stratégique et d'étude d'opinion publique, 62 % des entreprises ont des pratiques DevOps standards, soit dans l'ensemble de l'organisation, soit à l'échelle des équipes. Elles sont 28 % de plus à avoir intégré le DevOps dans des équipes spécifiques.

Le DevOps a toutefois amplifié les défis de sécurité en élargissant et en dynamisant la surface d'attaque, et en multipliant les points de compromission potentielle. Et si les entreprises doivent intégrer la sécurité plus tôt et de manière plus complète dans le processus DevOps pour résoudre ces problèmes, les pratiques de sécurité traditionnelles et le DevOps sont clairement en contradiction. Ce paradoxe a fait naître un intérêt croissant pour la sécurité en tant qu'élément essentiel de la pratique DevOps, conduisant au développement d'une nouvelle discipline : les opérations de sécurité du développement, ou DevSecOps.

Le DevSecOps garantit une livraison sécurisée des logiciels au rythme du DevOps. Mais dans la mesure où le DevSecOps est encore une discipline émergente, de nombreuses entreprises ne comprennent pas entièrement ce que cela représente et nécessite, et ne savent pas comment l'adopter efficacement. Dans ce guide, nous allons apporter un éclairage pour aider les organisations de toutes tailles à adopter une vision à la fois stratégique et tactique, dans le but de créer une pratique DevSecOps durable. En utilisant les six piliers décrits ci-dessous, les organisations peuvent jeter les bases d'une stratégie DevSecOps réussie et obtenir des résultats tangibles plus rapidement.

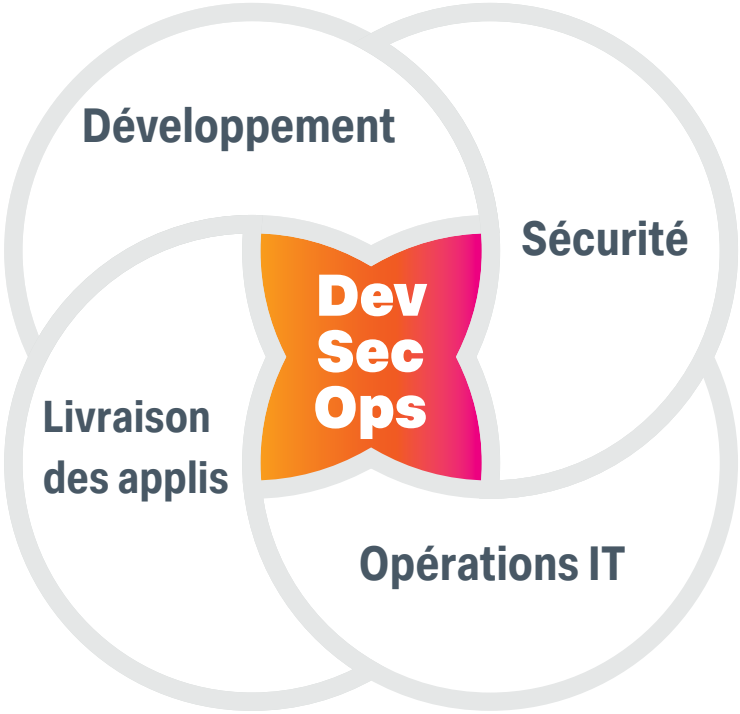
DevSecOps :
déplacer la sécurité vers l'amont

Historiquement, la sécurité relevait d'un groupe de spécialistes qui examinaient et testaient les applications au début et/ou à la fin du cycle de développement. Mais avec le rythme imposé par les pratiques DevOps, les approches traditionnelles qui renforcent la sécurité après coup ne sont pas durables.

À la base, le DevSecOps consiste à intégrer la sécurité à chaque phase du cycle de vie du développement DevOps, de la conception et du code initial, en passant par les tests, au déploiement et enfin à l'exécution. Cela permet aux praticiens d'identifier et de corriger les vulnérabilités de sécurité beaucoup plus tôt dans le cycle DevOps, pour produire un code de meilleure qualité et réduire les problèmes au cours des étapes ultérieures.

Pour être efficace, le DevSecOps exige également que toutes les équipes partagent la responsabilité de la sécurité des applications et de leur environnement, et que les équipes de sécurité, de développement et d'exploitation œuvrent vers des objectifs communs. C'est sans doute plus facile à dire qu'à faire car chaque équipe est animée par des priorités différentes : les équipes de développement se concentrent généralement sur la vitesse et la qualité du code ; les équipes d'exploitation sur la stabilité et la résilience de l'architecture ; et les équipes de sécurité sur la rigueur, la couverture et l'assurance contre les failles ou les vulnérabilités. Un programme DevSecOps réussi permet d'aligner tous ces objectifs afin que les organisations puissent créer des applications au même rythme ou à un rythme plus rapide, en intégrant beaucoup plus de sécurité.

Les entreprises doivent aussi évoluer plus rapidement pour rester compétitives, et les développeurs peuvent être hésitants à adopter ces pratiques au début, soit parce qu'ils craignent de ralentir le rythme du DevOps, soit parce qu'ils manquent d'expérience avec les pratiques de développement sécurisées. Mais lorsqu'il est bien exécuté, le DevSecOps n'est pas seulement bénéfique pour l'équipe de sécurité, il aide également les développeurs à gagner en productivité et à livrer à temps des produits de meilleure qualité. Pour l'entreprise, le DevSecOps peut réduire les risques et délivrer une posture de sécurité renforcée tout en soutenant le rythme du développement.



Les 6 piliers de la réussite du DevSecOps

Bien que les avantages du DevSecOps soient indéniables, réussir sa mise en œuvre n'a rien de simple. Fondamentalement, le DevSecOps est une pratique, pas un produit autonome ; il nécessite à la fois un changement de mentalité et de culture au sein de l'organisation, et de nouvelles approches et outils technologiques. Il impose de combler les écarts entre les équipes qui travaillent traditionnellement de manière indépendante avec leurs propres outils et flux de travail, et souvent différents KPI.

Pour être efficace, une stratégie DevSecOps doit s'appuyer sur les systèmes existants et supprimer les processus ou technologies obsolètes tout en en ajoutant de nouveaux si nécessaire. Elle doit aussi répondre aux besoins des équipes de développement, des opérations et de sécurité, et couvrir toutes les couches de la pile technologique et de l'application elle-même, à travers toutes les étapes du SDLC.

Nous résumons ci-dessous les six piliers qui permettent de créer et de maintenir une stratégie DevSecOps réussie, et nous allons voir comment Splunk peut faciliter et accélérer ces approches.

1 **Ouvrez les silos organisationnels :** pour implémenter le DevSecOps efficacement, il faut avant tout éliminer les barrières entre les équipes de développement, des opérations, de l'ingénierie de la fiabilité des sites (SRE) et de la sécurité, et faire de la sécurité une responsabilité partagée. Les équipes doivent s'aligner sur un ensemble commun d'objectifs et de KPI. Toutes les parties concernées seront inévitablement amenées à faire des compromis, mais identifier les objectifs prioritaires et s'aligner dessus sans ajouter à la dette de sécurité devrait favoriser l'adoption. Les outils qui permettent aux utilisateurs de travailler à partir d'une source commune de vérité sont essentiels pour faciliter la collaboration.

L'approche de Splunk : Splunk contribue à briser les silos organisationnels et soutient la collaboration en proposant une plateforme commune et des solutions spécialisées pour les équipes de sécurité, IT et DevOps. Splunk rassemble les données provenant de l'ensemble du paysage technologique et des outils associés, avec une fidélité totale, à grande échelle. Les données et les rapports partagés permettent aux équipes d'identifier et de hiérarchiser plus facilement les tâches critiques, de créer des KPI communs, de suivre les progrès et d'itérer selon les besoins tout au long du cycle de vie DevOps.

2 **Adoptez de nouveaux outils et processus de sécurité pour réduire les frictions entre les équipes DevOps et de sécurité :** au fil de l'adoption du DevSecOps, les entreprises peuvent être amenées à enrichir leurs outils et leurs processus, qui doivent tous s'intégrer dans les flux de travail existants. Les développeurs ne sont pas des experts en sécurité. Pour qu'ils continuent à livrer à un rythme rapide, les outils et processus de sécurité doivent s'intégrer de manière transparente dans la chaîne d'outils DevOps, pour leur permettre de travailler dans l'environnement de développement qui leur est familier. Dans le même temps, les outils et les processus doivent s'intégrer aux flux de travail de sécurité et aux opérations SOC existants pour que les équipes de sécurité deviennent de véritables partenaires de leurs homologues DevOps.

L'approche de Splunk : en rassemblant des données de toutes les sources, quelle que soit l'échelle, sur toute la pile technologique, Splunk apporte une visibilité contextuelle aux équipes de développement, de sécurité et d'exploitation au sein de leurs processus et flux de travail existants. En plus de fournir des vues de données discrètes adaptées aux différentes équipes, Splunk permet aux utilisateurs de créer des tableaux de bord composites offrant une vue commune et exhaustive des métriques pertinentes, aussi utile aux équipes qu'aux décideurs.

3 **Focalisation sur l'automatisation :** les approches traditionnelles de la sécurité des applications sont généralement lourdes et basées un système de barrières. Elles doivent souvent être confiées à des professionnels de la sécurité. Ces approches ne sont pas adaptées aux processus DevSecOps, qui sont agiles et nécessitent un feedback continu. Tout comme le DevOps, le DevSecOps a besoin d'automatisation pour être rapide et précis, et pour veiller à ce que les équipes suivent les protocoles et les bonnes pratiques convenus. En cas d'incident, l'automatisation est également essentielle pour apporter de la visibilité et simplifier la résolution. Cela dit, l'automatisation doit faire l'objet d'une réflexion approfondie : il faut viser des résultats précis et exploitables, sans surcharger inutilement les systèmes ni inonder les développeurs de fausses alertes.

Pour les tâches qui doivent être effectuées « hors bande » et qui ne peuvent pas être automatisées, les équipes doivent créer un calendrier itératif et prédéterminé, et mettre en place un système reliant les résultats au processus DevSecOps.

L'approche de Splunk : Splunk propose deux voies d'automatisation. L'une consiste à unifier les données des différents outils du SDLC. Cette démarche est facilitée par des intégrations prédéfinies pour une grande variété d'outils de pointe, et par l'architecture pilotée par API de Splunk, qui assure la connectivité aux outils de niche et spécifiques à l'entreprise. En fin de compte, cette automatisation permet de réduire les interventions manuelles et libère les équipes des tâches répétitives, qui peuvent alors se concentrer sur des scénarios d'utilisation plus innovants.

La seconde est la prise en charge par Splunk d'initiatives d'automatisation plus importantes axées sur le DevSecOps. En offrant une visibilité sur la santé et la fonctionnalité de ces automatisations, Splunk atténue les défis créés par les processus de boîte noire, notamment grâce à l'analyse prédictive qui peut signaler les problèmes avant qu'ils ne surviennent.

4 **Assurez une visibilité continue et partagée :** la visibilité et le feedback doivent être contextuels, de bout en bout (de la définition d'une fonctionnalité à sa mise en production) et transmis au même rythme que la progression du code dans le système. Les équipes de développement et des opérations doivent avoir accès à cette visibilité au sein de leur chaîne d'outils et de leurs processus existants : systèmes de tickets ou notifications Slack, par exemple. Les équipes de sécurité doivent également avoir une visibilité sur tous les indicateurs utiles au sein de leurs propres processus et d'outils afin de pouvoir se coordonner avec leurs collègues du développement et des opérations, et avoir accès à toutes les informations nécessaires pour résoudre les problèmes de sécurité qui surviennent après la production.

L'approche de Splunk : en collectant des données sur l'ensemble des outils et des piles technologiques, Splunk apporte une visibilité contextuelle sur les applications et l'infrastructure qui les supporte, ainsi que sur la façon dont les différentes étapes du processus s'articulent au sein du pipeline. De plus, Splunk extrait des informations exploitables grâce à l'IA/ML intégré, rationalisant les flux de travail des équipes de développement, des opérations et de sécurité. Des fonctionnalités comme les alertes basées sur les risques hiérarchisent les incidents, réduisent le déluge d'alertes et contribuent à simplifier la sécurité pour les développeurs.

5 **Traitez toutes les vulnérabilités de sécurité comme des défauts de qualité :** les entreprises consignent souvent les deux types d'observations (sécurité et qualité) en deux endroits différents. Non seulement cette pratique réduit la visibilité, mais elle conduit souvent les développeurs à accorder une moindre priorité aux défauts de sécurité. Pour résoudre ce problème, les organisations doivent pouvoir consulter les observations de sécurité et de qualité en un même endroit, afin d'obtenir une vue commune précise de la posture de sécurité et d'aider l'équipe de développement à accorder aux problèmes de qualité et de sécurité une importance égale.

L'approche de Splunk : comme Splunk peut extraire des données de toutes les chaînes d'outils DevOps et de sécurité, puis fournir des tableaux de bord consolidés et partagés, il permet aux équipes d'accéder à un référentiel commun et à une vue précise des défauts de sécurité et de qualité, en temps réel. Cette vue commune contribue à faire en sorte que les défauts de sécurité importants soient traités dès le début pour éviter des reprises coûteuses après le passage en production, avec la participation de toutes les équipes impliquées.

6 **Développer/renforcer la stratégie de réponse post-incident :** bien que des problèmes de sécurité surviennent inévitablement en production, le fait d'avoir une visibilité contextuelle complète dès l'instant de la définition d'une fonctionnalité aidera les équipes à identifier rapidement le problème. Et du fait de la nature éphémère de l'architecture cloud, il est également essentiel qu'elles disposent d'un traçage haute-fidélité sur chaque interaction. Même une fois qu'un incident a été affecté, les équipes de réponse et de résolution peuvent encore avoir besoin de collaborer : des outils et une visibilité partagés ne feront que contribuer à une résolution plus efficace et plus rapide.

L'approche de Splunk : au-delà du développement, Splunk offre une visibilité sur toutes les données d'incident, accompagnées d'outils intégrés pour une réponse efficace aux incidents. Grâce à cela, les SRE, qui sont généralement en première ligne, ont accès à toutes les données dont ils ont besoin pour analyser les incidents de sécurité. Splunk leur permet d'acheminer les alertes vers les bonnes personnes, d'attribuer une réponse et de superviser l'état et l'évolution du dossier. Lorsqu'un dossier est confié à un spécialiste de la sécurité, Splunk veille à ce que toutes les données d'investigation déjà compilées par le SRE soient mises à sa disposition, évitant ainsi toute duplication des efforts. Splunk offre également une visibilité de bout en bout dès la définition des fonctionnalités, ce qui permet aux spécialistes de la sécurité de comprendre l'incident sans demander des efforts supplémentaires au développeur. Même lorsque l'intervention des développeurs n'est pas nécessaire dans le processus de résolution, ils ont toujours une visibilité sur celui-ci, ce qui leur permet de comprendre l'impact de leur code sur la sécurité en production, et donc de définir et hiérarchiser les exigences de sécurité des projets à venir.

Le DevSecOps en action

Il existe potentiellement des milliers de façons d'utiliser DevSecOps dans de nombreux secteurs et verticales. Pour la plupart, on peut toutefois les classer en trois grandes catégories : sécurisation de l'atelier de développement, appui à la création d'applications plus sécurisées et sécurisation des applications en production.

1 **Sécuriser l'atelier de développement :** pour permettre aux développeurs d'exploiter la chaîne d'outils DevOps avec efficacité, leur environnement doit être sécurisé et résilient. Mais l'arsenal DevOps implique une multitude d'outils ponctuels qui prennent en charge diverses fonctions discrètes. Cette complexité est encore aggravée par une dépendance croissante vis-à-vis des logiciels open source pour la création d'applications, et par l'adoption de modèles architecturaux découplés et éphémères.

Que peut faire Splunk ? Splunk connecte la télémétrie à ces nombreux outils et analyse les modèles de données à l'aide de l'IA/ML pour créer des alertes lisibles et basées sur les risques. Les entreprises peuvent ainsi s'assurer que leurs employés respectent les stratégies de sécurité, quels que soient les outils utilisés, tout en minimisant les fausses alertes. Splunk prend également en charge la réponse automatisée aux incidents pour simplifier la résolution.

2 **Créez des applications plus sécurisées :** pour développer des applications plus sécurisées, il faut traiter la sécurité à chaque couche de l'application : composants d'application, services cloud et bibliothèques OSS. Cela s'applique également au code personnalisé de l'application, aux interactions API entre les différents services, aux images créées et déployées, et à l'infrastructure (de plus en plus souvent cloud ou en conteneurs) sur laquelle le code s'exécute.

Que peut faire Splunk ? Splunk rassemble les journaux de toutes ces couches en temps réel et permet de suivre le pipeline d'activités de la définition des fonctionnalités à leur publication, et jusqu'aux incidents de sécurité en production. Cette visibilité contextuelle approfondie est offerte par le biais de tableaux de bord partagés en temps réel, ainsi qu'au sein des outils existants. En conséquence, les développeurs peuvent non seulement créer un code plus sécurisé, mais également corriger les violations de politique et de sécurité en temps réel. Cette compréhension commune à toutes les équipes aide également à établir, suivre et mesurer des pratiques de codage optimales tout au long du SDLC.

3 **Sécuriser les applications en production :** lorsqu'un incident de sécurité se produit après le déploiement, le SRE et l'équipe de sécurité sont généralement chargés de le résoudre. Mais il est souvent difficile d'apporter une résolution efficace à un problème, non seulement en raison du rythme du développement, mais aussi parce que les développeurs doivent comprendre aussi bien les premières étapes du cycle de développement et les dernières étapes du cycle d'utilisation.

Que peut faire Splunk ? Splunk effectue un suivi de l'ensemble du pipeline d'activités : cela accélère à la fois les investigations de sécurité et la résolution des incidents, et rend ces processus plus efficaces en réduisant significativement les allers-retours entre développeurs, SRE et équipes de sécurité.

Le DevSecOps est fondamental pour réussir à l'ère des données

La sécurité est devenue une préoccupation stratégique dans les entreprises avec l'évolution rapide des menaces. Mais ces mêmes entreprises sont également poussées à accélérer la production et le développement d'applications, sans quoi elles risquent de perdre leur avantage compétitif au profit d'acteurs plus rapides et plus agiles.

Le DevSecOps apporte une réponse à ces deux défis en intégrant les tests de sécurité dans le cycle de vie du développement logiciel sans ralentir le rythme du DevOps. Comme le DevSecOps traite les risques de sécurité et les vulnérabilités dès le début, les organisations peuvent rapidement atténuer, voire éviter complètement, les surprises dommageables et coûteuses qui auraient autrement pu apparaître au cours des phases ultérieures. L'adoption du DevSecOps permet également de mettre en œuvre une sécurité continue, et donc de protéger les actifs 24 heures sur 24, tous les jours de l'année.

Splunk peut faciliter la mise en place et l'évolutivité de ces nouvelles approches DevSecOps en offrant une visibilité de bout en bout, en intégrant les bonnes données dans les flux de travail pertinents et en assurant le fonctionnement fluide des nouveaux outils et processus pour les équipes de sécurité et DevOps. En adoptant une approche holistique, Splunk garantit la compatibilité des solutions, non seulement avec les processus DevOps existants, mais également avec les équipes de sécurité et leurs pratiques au sein du SOC.

À l'avenir, il est probable que DevSecOps occupe une plus grande place dans le processus de développement, mais aussi qu'il revête une importance plus critique pour le succès global des entreprises et leur capacité à prospérer à l'ère des données. Instaurer et entretenir une culture DevSecOps ne se fait pas du jour au lendemain, mais repenser le pipeline de développement en mettant l'accent sur le DevSecOps aidera les organisations à gagner en productivité, à réduire les risques et à cultiver une posture de sécurité renforcée dès le début.

Pour découvrir comment Splunk peut appuyer une initiative DevSecOps, contactez le service commercial Splunk.

En savoir plus

splunk> turn data into doing®

21-21001-Splunk-6 Pillars