Comment le DevOps peut-il s'appuyer sur la Smart Data ?

Le Cloud hybride est devenu un élément majeur de la réussite de la transformation numérique (DX) des entreprises. Elles sont de plus en plus nombreuses à y en transférer leur charge de travail, applications et services, car cette approche leur permet de bénéficier de nombreux avantages : réductions de CAPEX/OPEX, mise sur le marché plus rapide, avec notamment la promesse de nouveaux services.

Dans ce contexte, la place du DevOps est grandissante. Les développeurs et les équipes opérationnelles informatiques collaborent désormais plus étroitement afin de planifier, développer, fournir, intégrer, tester et déployer des applications et nouveaux services spécifiquement pour les environnements Cloud hybride.

Face à la rapidité d'exécution exigée par la transformation numérique, quel filet de sécurité existe-t-il pour les équipes de DevOps ?

En effet, plus le rythme de déploiements s'accélère, plus le risque de laisser passer une faille et/ou une vulnérabilité potentielle augmente. Non-identifiées dans les temps, ces dernières peuvent avoir à termes des conséquences désastreuses.

Aujourd'hui, certaines organisations réalisent des évaluations de sécurité plutôt sur la fin de leur processus de développement. Dans ce cas, l'usage d'une méthodologie de « dév' en cascade, avec des déploiements de logiciels peu fréquents, leur permet de gérer tout retard dû à la découverte de vulnérabilités de sécurité des applications.

Cependant, pour celles s'appuyant sur des pratiques de développement plus agiles où les équipes de DevOps déploient de nouvelles versions quasi quotidiennement, tout retard de détection de faille est inacceptable.

Face aux impacts négatifs qu'une application défaillante pourrait causer, la question de leur sécurité doit être prise en compte dès leur conception. Cette approche de « security by development » permet de garantir l'identification de vulnérabilités à la source et d'éviter ainsi tout retard lié à l'intégration de mesures correctives.

Pour assurer une meilleure protection des services et applications dans les environnements de Cloud hybrid, les équipes de DevOps doivent évoluer culturellement pour s'affirmer davantage comme acteurs de DevSecOps.

En intégrant le concept de sécurisation dès le développement applicatif, elles bénéficieront véritablement d'une visibilité de bout en bout sur l'ensemble de l'infrastructure de leur réseau, et surtout d'une surveillance en continu.

Des perspectives significatives et exploitables

Une visibilité claire du cycle de développement permet aux concepteurs de mieux appréhender la situation, et le cas échéant de prendre les mesures appropriées face à un problème identifié. Ainsi, les équipes opérationnelles n'ont pas besoin d'intervenir. Mais cela crée surtout de nombreux avantages dans les domaines de la performance et de la sécurité des applications, ainsi l'efficacité des processus de détection des anomalies et d'analyse des causes principales seront optimisées.

Le niveau de visibilité accessible aux équipes est aujourd'hui rendu possible grâce aux données intelligentes (Smart Data) transitant sur les réseaux. C'est-à-dire les métadonnées basées sur le traitement et l'organisation des flux de trafic IP, récupérées directement au point de collecte et optimisées pour des analyses de qualité et rapidité maximales.

Contrairement aux données log, nécessitant d'être rassemblées et analysées avant utilisation, la Smart Data se base sur l'analyse, en temps réel, de chaque paquet IP transitant sur le réseau durant un cycle de développement.

Avec elle, chaque équipe intervenant sur l'IT (développeurs, experts sécurité, etc.) bénéficie d'informations significatives et exploitables afin de travailler plus étroitement ensemble, et ce à mesure que les paramètres évoluent dans le process de développement.

Créer des applications plus sécurisées

Dans une organisation DevSecOps, cette visibilité acquière une importance accrue au niveau de la sécurité.

En effet, un ingénieur en sécurité peut y travailler avec des développeurs, des équipes de contrôle de la performance des opérations pour assurer la sécurité des applications et des services.

L'analyse des données après une violation aidera à résoudre le problème, mais le fait de connaître les failles d'une application en temps réel permettra aux développeurs, aux opérations et aux équipes de sécurité de traiter les problèmes avec plus de souplesse. Associé à l'automatisation, ce processus contribuera à la création d'applications plus sécurisée, et permettra également des économies de temps et d'argent, tout en réduisant les risques d'atteinte à la réputation de l'entreprise.

La transformation numérique est intrinsèquement liée à l'innovation et à la réussite des entreprises. Toutefois, elle n'est pas sans risque !

L'enjeu aujourd'hui est d'associer les équipes afin de disposer rapidement de codes applicatifs à la fois performants et protégés. Pour éviter des retards coûteux durant le déploiement, la sécurité doit être intégrée en amont et tout au long du cycle de développement des applications.

Dans ce contexte, une approche DevSecOps offrira une agilité nouvelle à l'entreprise, qui

bénéficiera notamment d’un nouvel atout en matière de sécurité.

crédit photo © shutterstock