Livre blanc

Sécurisation de votre plateforme DevOps :

Pipelines de logiciel, d'intergiciel et d'infrastructure pour **l'entreprise moderne**

CloudOps

Devenez maître de votre destin infonuagique

Agnostique, mais opiniâtre en matière de nuage et de code

CLOUDOPS.COM/FR

1 (888) 796-8364 | info@cloudops.com | @cloudops_

Les défis de sécurité auxquels les entreprises sont confrontées

Les grandes entreprises accumulent généralement de grandes quantités de données, ce qui peut les rendre particulièrement attirantes pour les pirates. Qu'elles offrent des services financiers, des assurances ou tout autre type de service, les entreprises accumulent inévitablement des informations sensibles qui peuvent être exploitées. Chargées de protéger les données personnelles, les entreprises ont la responsabilité de résoudre les problèmes de sécurité et de protéger les informations afin de minimiser le risque de brèches.

De plus en plus, les réglementations du secteur exigent des informations concrètes sur les procédures et contrôles mis en place par une entreprise. Au fur et à mesure que les clients prennent davantage conscience des risques liés à la sécurité des informations, ils se posent des questions telles que :

- Quelles sont les stratégies d'authentification et de contrôle d'accès?
- Quelles politiques de cryptage protégeront nos données lors de leur transfert ou de leur stockage?
- Comment la sécurité de notre code et de notre code en source libre peut-elle être résolue efficacement tout en gardant la vélocité de l'entreprise?
- Mes API et l'infrastructure sous-jacente sont-elles sécurisées?

Il est assez courant de voir des appels d'offres pour des entreprises qui recherchent une assurance d'une tierce partie indépendante, telle que le rapport SOC (Service Organization Control) 2 et la Cloud Security Alliance (CSA) STAR, pour des certifications de sécurité ou des contrôles pour leur entreprise. Cela peut garantir des niveaux de disponibilité élevés, garantir l'intégrité du traitement et fournir une protection suffisante de la confidentialité et de la vie privée.

Les entreprises sont censées faire preuve de transparence lorsqu'elles découvrent une violation de la sécurité. Au Canada, dans le cadre de La Loi sur la protection des renseignements personnels numériques, les amendes peuvent atteindre 100 000 $ par violation lorsqu'une entreprise enfreint les exigences de notification d'infraction.[1] Aux États-Unis, plusieurs nouveaux projets de loi ont été présentés au Congrès. S'ils deviennent des lois, les dirigeants d'entreprises risquent l'emprisonnement s'ils ne signalent pas les violations de données en temps voulu.[2] L'Europe a suivi un chemin similaire en mai 2018 avec l'introduction du règlement général sur la protection des données (RGPD), qui a remplacé la loi sur la protection des données de 1998.[3] Grâce à cette législation et à la couverture accrue par la presse des atteintes à la confidentialité des données, les entreprises ne peuvent prétendre à l'ignorance dans le domaine de la cybersécurité. Si elles ne réduisent pas correctement les risques liés aux cybermenaces et ne répondent pas aux obligations de conformité, elles peuvent être confrontées à de graves conséquences commerciales et personnelles.

Alors que les entreprises tentent de prévenir les violations de données, leur écosystème est en constante évolution. De nombreux facteurs rendent cette tâche encore plus difficile :

- 43% des entreprises livrent des modifications chaque semaine, chaque jour ou de manière continue. La rapidité accrue des changements rend plus difficiles la compréhension et l'analyse des conséquences sur la sécurité. Il n'y a pas assez de temps pour mener des tests ou des examens exhaustifs et le profil de risque change constamment.[4]
- Différents langages de programmation et trousses d'outils affectent directement la manière dont les équipes d'ingénierie et de sécurité livrent et testent. Il est important de comprendre les risques de sécurité au niveau du langage et de la bibliothèque. Par exemple, JavaScript et d'autres langages de script dynamiques, tels que PHP et Python, sont plus difficiles à vérifier au moment de la compilation que les langages statiques, ce qui signifie qu'un plus grand nombre de problèmes peuvent échapper à la surveillance et sont découverts uniquement au moment de l'exécution.[5]
- Lorsque les plateformes et les conteneurs infonuagiques deviennent les entreprises d'infrastructure par défaut, ils introduisent des risques liés au contrôle d'identité et d'accès, aux images non fiables, à l'orchestration de la sécurité, à la fragmentation des conteneurs et à d'autres problèmes liés à la capacité des développeurs à configurer leur propre infrastructure à la volée.

[1] Le 18 juin 2015, la loi sur la protection des données numériques (également appelée projet de loi S-4) a modifié la loi sur la protection de la vie privée dans le secteur privé au Canada, soit la Loi sur la protection des renseignements personnels et des documents électroniques (LPRPDE), en ce qui concerne l'établissement d'exigences de déclaration obligatoire des violations de données.

[2] Par exemple, le projet de loi H.R. 3806 ("Personal Data Notification and Protection Act of 2017") et le projet de loi S. 1815 ("Data Broker Accountability and Transparency Act of 2017").

[3] Règlement général sur la protection des données (GDPR), Europe.

[4] The 2017 State of Application Security: Balancing Speed and Risk

[5] The 2017 State of Application Security: Balancing Speed and Risk

Les équipes de sécurité doivent faire du rattrapage afin de comprendre ces architectures en évolution et savoir comment les protéger. Les mécanismes de sécurité traditionnels, tels que les pare-feux, peuvent être défaillants dans le paysage infonuagique actuel, où on peut retrouver des niveaux sans précédent de propriété intellectuelle, de données et d'étalement d'identité.

- Les grandes entreprises ont souvent des ratios d'un travailleur en sécurité informatique pour dix travailleurs en infrastructure et cent développeurs.[6] Ceci est particulièrement insuffisant lorsque les développeurs ne sont pas conscients des risques de sécurité courants. Lorsque la sécurité se trouve à la toute fin du cycle de vie du logiciel, les problèmes peuvent être difficiles et fastidieux à résoudre.
- Beaucoup d'entreprises ont un manque d'automatisation de la sécurité. Elles dépendent encore fortement des tests et examens manuels, notamment des tests d'intrusion et des audits de conformité externes.
- Les parties externes (auditeurs, testeurs d'intrusion, services de balayage de vulnérabilités) et les équipes de sécurité internes sont principalement responsables des tests et des évaluations de sécurité, tandis que les équipes de développement et les architectes de système sont principalement responsables des actions correctives.[7]

Chaque jour, de nouvelles attaques exploitant une autre faiblesse cachée dans les applications en nuage sont lancées. Cela signifie que de nouvelles vulnérabilités sont exposées et exploitées plus rapidement, à un rythme que beaucoup d'entreprises ne peuvent tout simplement pas soutenir. Cela met en évidence l'importance de la conformité dans la prise en charge des programmes et des contrôles de sécurité.

La conformité aux normes de sécurité offre-t-elle une solution viable ?

L'accès, le stockage et le traitement des données sensibles doivent être soigneusement contrôlés et peuvent être régis par divers règlements, lois ou normes de l'industrie tels que ISO-27001, le rapport SOC 2, CSA STAR, la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), la Loi Sarbanes-Oxley (SOX), la Loi Gramm-Leach-Bliley (GLBA), la Norme de sécurité de l'industrie des cartes de paiement (PCI-DSS) ainsi que le "Health Insurance Portability and Accountability Act" (HIPAA).

Le rapport SOC 2 se concentre spécifiquement sur les contrôles de comptes rendus non financiers d'une entreprise en ce qui concerne la sécurité, la disponibilité, l'intégrité des traitements et la confidentialité d'un système. C'est le rapport le plus ciblé pour comprendre le SOC et la façon dont les standards sont vérifiés. Les rapports SOC peuvent être de type 1 ou de type 2. Un rapport de type 1 décrit les contrôles et l'opinion de l'auditeur à un moment précis. C'est généralement le point de départ qui établit la conception des contrôles, la fréquence à laquelle vous effectuez certaines activités et la manière dont certains processus sont exécutés. Un rapport de type 2 contient l'opinion de l'auditeur sur la manière dont l'entreprise exécute ces activités sur une période donnée (c'est-à-dire généralement six mois ou plus).

La sécurité des entreprises n'est pas toujours une tâche simple en raison du partage des responsabilités. La responsabilité de la sécurité peut être répartie sur quatre niveaux différents (voir la figure 1) :

1. Le centre informatique/installations de colocation, qui couvrent des domaines tels que la sécurité physique, la puissance et le système CVC (chauffage, ventilation et climatisation).
2. Le fournisseur d'infrastructure en tant que service, qui couvre les responsabilités telles que les hyperviseurs, le réseau, le stockage, les serveurs, la virtualisation et les pare-feux.
3. La plateforme applicative, qui comprend le moteur d'exécution, l'intergiciel et le système d'exploitation. Ce niveau se compose généralement d'éléments normalisés même si la configuration est personnalisée pour une application particulière.
4. L'application, qui comprend des domaines tels que la logique et le code de l'application, les langages de programmation, les bases de données, les transactions, les interfaces externes ainsi que les processus et politiques de sécurité pertinents.

[6] James Wickett, "Attacking Pipelines - Security Meets Continuous Delivery", Slideshare.net, June 11, 2014

[7] The 2017 State of Application Security: Balancing Speed and Risk

Figure 1 : Domaines de responsabilité
(Source: CloudOps)

Être affilié à un centre de données ou un fournisseur infonuagique d'infrastructure en tant que service ayant déjà reçu la certification SOC 2 n'offre pas à l'entreprise un niveau de conformité transitif. Bien qu'un centre de données ou un fournisseur d'hébergement peut avoir obtenu un rapport SOC 2, cela ne signifie pas que l'entreprise ait un rapport SOC 2 correspondant qui est pertinent à la portée particulière de ses services.

En fait, le rapport sur l'état de la sécurité des applications de 2017 du SANS Institute affirme que les applications Web s'exécutant sur le nuage public sont la principale source de violations de données (voir la figure 2 ci-dessous), comme indiqué précédemment par le SANS Institute.[8]

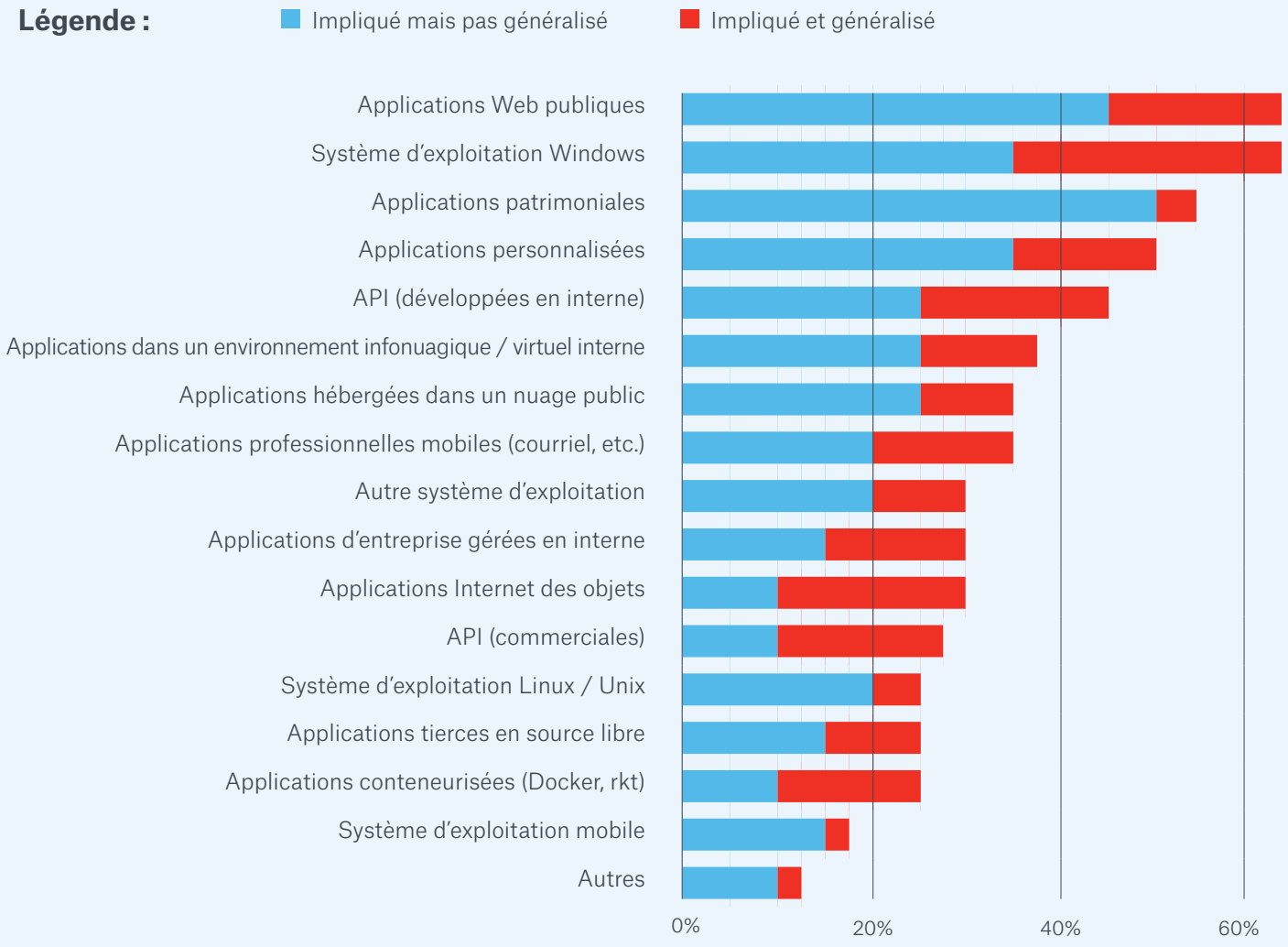

Figure 2 : Applications et composants impliqués dans des brèches de sécurité
(Source: SANS Institute)

[8] The 2017 State of Application Security: Balancing Speed and Risk, page 5.

Lorsque vous décomposez les différents types d'attaques sur les applications Web, vous pouvez remarquer que 65% proviennent de failles XSS (Cross-Site Scripting) et d'injection SQL (voir figure 3)[9]. L'injection SQL est utilisée pour accéder à des informations sensibles ou exécuter des commandes du système d'exploitation pour un accès ultérieur au système. En outre, les fuites d'informations et l'injection XML peuvent entraîner la divulgation d'informations.[10]

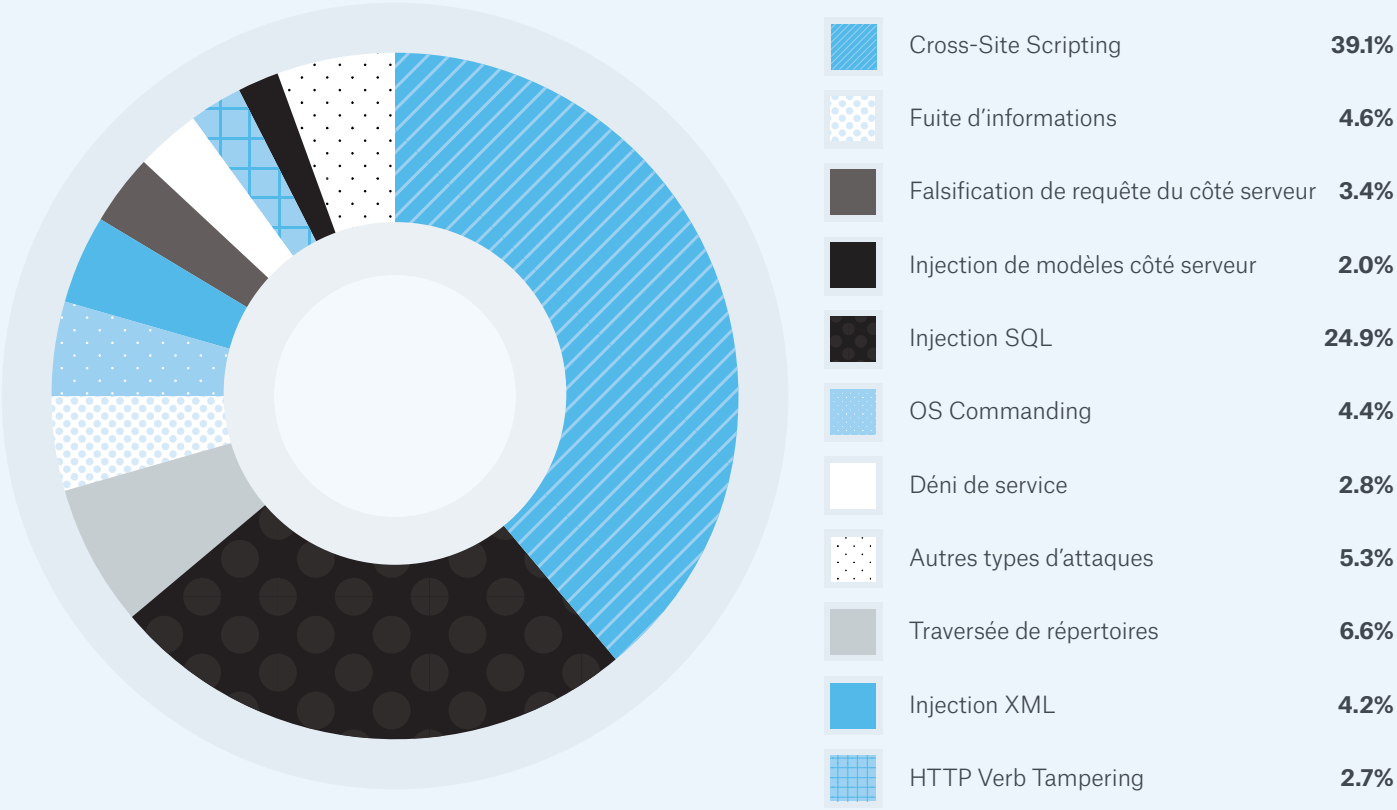

Figure 3 : Répartition des types d'attaques utilisées contre les applications de logiciel en tant que service
(Source: Positive Technologies)

Il est clair que le niveau du code de l'application est l'une des couches les plus vulnérables. Il est de la responsabilité exclusive de chaque entreprise d'être responsable et de se conformer à la certification de sécurité, au rapport d'audit ou aux exigences réglementaires applicables aux risques spécifiques inhérents à son modèle de déploiement et au risque potentiel de sécurité propre à son cas.

[9] XSS est une attaque par injection de code côté client destinée à exploiter une vulnérabilité d'un site Web ou d'une application Web visité par une victime infectée.

[10] The Web Application Attack Statistics Q2 2017, page 5.

La valeur de la certification et de l'audit sectoriels

En cas de brèches de données, les entreprises sont confrontées à une publicité négative, à une baisse de loyauté de leurs clients et à une perte de revenus. L'Institut Ponemon a indiqué que les cyberattaques sont de plus en plus coûteuses chaque année. Le coût moyen mondial dû aux dommages ou au vol d'actifs et d'infrastructures informatiques est passé de 879 582 $ à 1 027 053 $ en 2017 seulement. De même, le coût moyen dû à la perturbation des activités normales est passé de 955 429 $ à 1 207 965 $.[11] Au palmarès des pays ayant le plus haut coût de violations de données par habitant,[12] les États-Unis occupent la première place, suivis du Canada, puis de l'Allemagne.[13]

L'utilisation d'un programme de certification sectorielle ou d'un rapport d'audit externe permet à une entreprise de logiciel en tant que service de garantir les procédures et contrôles de sécurité les plus rigoureux et de minimiser les risques pour la sécurité. Les certifications du secteur telles que CSA STAR ou les rapports d'audit tels que SOC 2 s'appuient sur des contrôles de sécurité éprouvés qui, à leur tour, permettent de minimiser et d'éviter le coût des violations de données. Les certifications et les rapports d'audit externe apportent également une valeur ajoutée indirecte à l'entreprise :

- La certification et les rapports d'audit externe peuvent générer de nouvelles ventes ou, à tout le moins, garantir que la sécurité ne constitue pas un obstacle pour de nouvelles activités. Avoir un rapport d'audit détaillé peut être un facteur déterminant pour savoir si un client est à l'aise à utiliser votre plateforme.
- Le fait de savoir que votre entreprise respecte les normes de sécurité les plus strictes du secteur accroît la confiance de vos clients et encourage leur fierté à faire partie de votre communauté. Cela peut conduire à des niveaux de fidélisation et d'acquisition plus élevés.
- Certains secteurs / prospects ont des exigences en matière d'audit et de conformité qui ne peuvent être satisfaites qu'avec une certification et un audit de sécurité effectués par un tiers (par exemple, HIPAA pour les soins de santé et PCI-DSS pour le commerce électronique). Les différents cadres de sécurité offrent un inventaire exhaustif des exigences de sécurité qui pourraient être appliquées aux entreprises de logiciel en tant que service.

Des certifications de sécurité et des rapports d'audit externe réputés du secteur permettent de réduire le nombre de réponses aux vérifications de sécurité et de demandes d'audit émanant de clients ou de prospects, réduisant considérablement les frais généraux, les risques et les coûts liés à la livraison de services pour une compagnie de logiciel en tant que service.

Options pour sécuriser votre plateforme DevOps

Supposons maintenant que nous avons décidé de créer et d'opérer une plateforme DevOps qui respecte les bonnes pratiques afin de recevoir un rapport SOC 2. Il y a deux façons de s'y prendre:

L'approche bricolée à la main

Cette option requiert, au préalable, que vous disposiez de ressources internes assez informées sur la sécurité afin de pouvoir acheter le matériel et les logiciels requis, et possédant l'expertise nécessaire pour définir les contrôles de sécurité. Les experts internes doivent définir les contrôles et les procédures en fonction de SOC 2, installer et configurer les serveurs, sélectionner les outils logiciels et établir la surveillance et la personnalisation pour garantir que tous les aspects des contrôles de sécurité soient pris en compte.

Cette approche est généralement mise en œuvre dans les cas d'utilisation suivants :

- Utilisation d'une technologie exclusive qui ne correspond pas aux outils et processus de sécurité standards utilisés par des tiers fournisseurs de services.
- Procédures de sécurité nécessitant un haut niveau de personnalisation et un contrôle total sur la plateforme.
- Un centre d'opérations déjà établi, ayant mis en place des opérations sécurisées.

De nombreuses entreprises n'ont pas le talent, les outils et l'expertise nécessaires pour réussir une approche bricolée. Celles qui le font peuvent être handicapées par des outils et des systèmes patrimoniaux difficiles à convertir en équivalents sur le nuage natif. De la même manière, leurs équipes de sécurité informatique pourraient ne pas vouloir acquérir de nouvelles compétences et adopter de nouvelles pratiques pour faire face aux risques de sécurité présentés par le nuage. Ces entreprises devront construire des pipelines DevSecOps modernes.

[11] The 2017 State of Cybersecurity in Small & Medium-Sized Businesses (SMB), Ponemon Institute Research Report, page 2.

[12] The 2017 Cost of Data Breach Study: Global Overview, page 8.

[13] Per capita cost is defined as the total cost of data breaches divided by the size of the data breach (i.e., the number of lost or stolen records).

L'approche des services gérés

Ce modèle d'impartition, également appelé sécurité en tant que service ("SECaaS"), permet la gestion de la plateforme applicative, des politiques de sécurité et de l'administration générale sur le nuage. Les outils de sécurité et leurs équipes d'experts travaillent en permanence pour assurer le respect des contrôles de sécurité prédéfinis et répondre aux exigences du rapport SOC 2. SECaaS devient une partie de DevOps en tant que service lorsque les outils et pratiques de DevOps sont appliqués à la sécurité. Il est tout de même important de souligner que les développeurs d'applications doivent s'approprier la sécurité du code de l'application, qui ne relève pas de la responsabilité de la plateforme applicative.

Les cas d'utilisation courants de cette approche sont les cas où l'entreprise espère :

- Se concentrer principalement sur le développement de code et de produits sans se laisser distraire par la gestion des opérations et des procédures de sécurité.
- Minimiser les investissements importants dans la création et la maintenance de la plateforme applicative, des outils de sécurité et d'une formation poussée de l'équipe.
- Réduire le temps passé à concevoir et à construire une plateforme applicative.
- Accéder facilement à la maturité opérationnelle requise pour maintenir une plateforme applicative.

Analyse des coûts

Le coût d'une approche bricolée peut être nettement supérieur à celui d'une approche de services gérés, en particulier si on prend en compte les coûts des efforts internes en ressources humaines, des frais de conseil, des outils et des honoraires des auditeurs.

Efforts internes en matière de ressources humaines

Il peut être long et difficile de se tenir au courant des exigences en matière de conformité aux normes de sécurité ou de contrôles SOC 2, qui sont toujours en constante évolution. Une fois que vous commencez à mettre en place de nouvelles procédures de sécurité, l'entreprise s'engage à effectuer régulièrement la surveillance ou les tests requis. Cela entraîne souvent un besoin de nouveaux employés, parfois même assez pour créer une équipe 24h / 24 et 7j / 7. L'embauche et la formation du personnel figurent parmi les coûts internes liés au maintien de la conformité pour les programmes de sécurité avec une approche bricolée.

Pour de nombreuses entreprises, il est judicieux de faire appel à un tiers fournisseur de SECaaS afin de se concentrer sur le développement de logiciels et la création de code et d'éviter de se laisser distraire par la gestion de certains contrôles et procédures de sécurité. Ces ressources externes possèdent l'expertise nécessaire et se tiennent au courant des dernières exigences de réglementation et de conformité. Des ressources en sous-traitance peuvent s'adapter immédiatement pour répondre à de nouveaux besoins. La possibilité de disposer de personnes polyvalentes au service de plusieurs équipes ou de plusieurs objectifs devient une nécessité dans les environnements de l'infonuagique d'aujourd'hui.

Frais de conseil

Traditionnellement, nous constatons que même les entreprises qui optent pour la méthode du bricolage ont besoin d'un soutien initial de consultants externes pour compléter les compétences disponibles en interne ou pour valider certaines décisions internes. Les ressources internes ne disposant généralement pas assez de temps pour se mettre à jour sur les modifications apportées au programme de sécurité, un expert est souvent engagé pour conseiller l'équipe interne qui serait chargée de la majorité du travail. Cela signifie que des frais de consultation externe seraient nécessaires pour une approche personnalisée.

Lorsque des services gérés de sécurité sont mis en œuvre, la plupart de ces frais de consultation sont évités, car les professionnels qui fournissent le service sont à jour avec les dernières exigences de contrôle de sécurité et savent comment les mettre en œuvre. Les seuls éléments qu'ils doivent prendre en compte sont les considérations spéciales propres au déploiement de l'entreprise. Cela signifie que les honoraires de consultation pour les services de sécurité gérés représenteront une fraction de ceux facturés lors d'une approche bricolée.

Outils

Dans une approche bricolée, l'entreprise doit évaluer, apprendre, concevoir, déployer et gérer les outils commerciaux de sécurité liés à la surveillance, la détection de vulnérabilités, etc. Dans les années à venir, l'entreprise devra acheter et mettre en œuvre les outils de sécurité et payer la maintenance.

Grâce aux services de sécurité gérés, le personnel externe qui prend en charge l'entreprise possède une connaissance approfondie des outils de sécurité requis. En fonction des besoins en contrôle de sécurité de l'entreprise, certains outils ne seront plus nécessaires car ils chevaucheraient avec les outils de la plateforme de sécurité gérée. Cela peut entraîner une réduction du coût des outils dans l'approche des services de sécurité gérés.

Honoraires de l'auditeur

Alors que l'approche bricolée impose à l'entreprise de concevoir et de mettre en œuvre tous les contrôles de sécurité, dans le cas de services de sécurité gérés, les entreprises peuvent réduire le coût de l'audit externe. Les services de sécurité gérés minimisent les écarts de conformité en exploitant une plateforme tierce déjà auditée et dotée d'une solution éprouvée. Cela réduit le niveau d'audit des contrôles de sécurité déjà traités par le SECaaS. En réduisant l'étendue de l'audit que les auditeurs doivent traiter, les honoraires de l'auditeur sont réduits pour les efforts et les frais de l'entreprise.

Conclusion

En tirant profit de l'expertise d'entreprises de services de sécurité gérés par des tiers, les entreprises peuvent :

- Adopter rapidement les bonnes pratiques en matière de sécurité dans le nuage et réduire les cyberrisques dans leur ensemble;
- Rapidement réaliser des rapports d'audit de sécurité de l'industrie réputés, tels que SOC 2, afin de générer de nouvelles ventes;
- Réduire les besoins en personnel supplémentaire, en formation et en investissement dans les outils de sécurité;
- Se concentrer sur le développement de nouveaux code et produits, plutôt que de gérer des programmes de conformité de sécurité;
- Réduire au minimum le risque de livraison de services tout en abaissant leurs coûts d'exploitation.

En fait, le marché des services de sécurité gérés se développe rapidement. Selon Allied Market Research, le marché mondial devrait générer 40,97 milliards de dollars d'ici 2022, enregistrant un TCAC de 16,6% pour la période 2016-2022.[14] Les entreprises ont réussi à tirer parti des services gérés par des tiers.

[14] Managed Security Services Market Is Expected to Reach $40.97 Billion, globally by 2022.

À propos de la plateforme de services DevOps gérés de CloudOps
(aussi appelée DevOps en tant que service)

La plateforme de services DevOps gérés permet aux petites et moyennes entreprises de tirer pleinement parti du nuage et de la conformité SOC 2. Notre service géré permet à votre application d'exécuter la configuration infonuagique qui répondra le mieux à vos exigences commerciales et techniques au fur et à mesure que votre entreprise croît, tout en réduisant vos risques de sécurité.

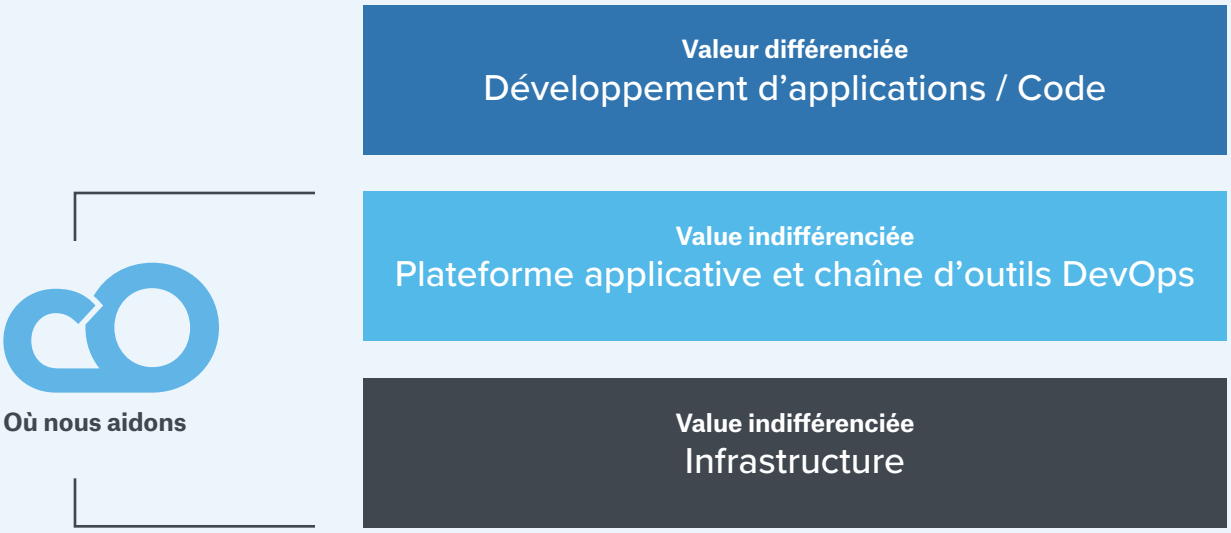

Figure 6 : Valeur différenciée vs. indifférenciée
(Source: CloudOps)

Les piles technologiques se composent de trois niveaux: le développement d'applications, la plateforme applicative et l'infrastructure. Pour prospérer, les entreprises doivent concentrer leur attention sur le développement de leurs applications, où elles doivent se différencier afin de fournir une valeur différenciée à leurs clients. En revanche, la plateforme applicative et l'infrastructure offrent une valeur indifférenciée. Leur rôle est de fournir au développement d'applications les services rendus possibles par le nuage: le libre-service, des économies d'utilité et une livraison continue des TI automatisée par API.

Le DevOps en tant que service de CloudOps vous aide au niveau de la plateforme applicative, la chaîne d'outils et l'infrastructure. Nos équipes DevOps prennent en charge, gèrent, surveillent et automatisent la plateforme applicative que vous exécutez 24h / 24 et 7j / 7. Nos services consistent à évaluer vos besoins, à définir votre stratégie, puis à construire votre plateforme applicative, complètement ou en partie. Nous construisons et gérons des plateformes applicatives très rapides composées de solutions évolutives et fonctionnant sur plusieurs clients et domaines.

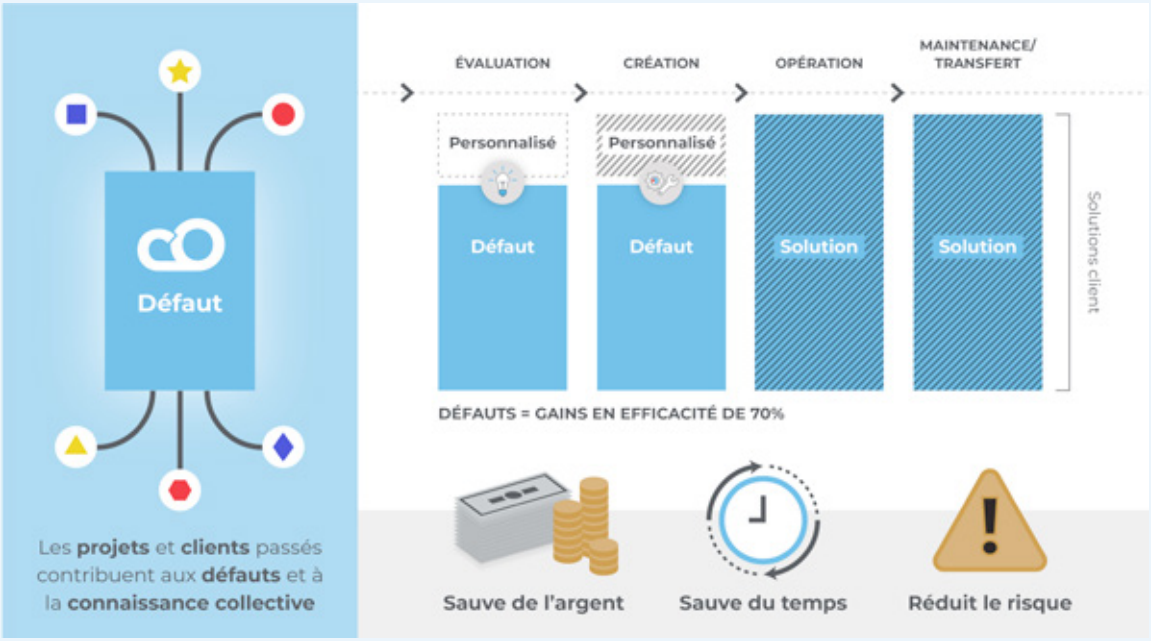

Figure 7 : Défauts
(Source: CloudOps)

Notre plateforme DevOps bénéficie de la connaissance collective d'une équipe d'experts et de la valeur résiduelle de tous les projets sur lesquels nous avons travaillé. Avec chaque projet, nous améliorons les bibliothèques partagées de recettes d'automatisation, qui deviennent des composants par défaut qui apportent une valeur à toutes les plateformes. Celles-ci sont complétées par des composants personnalisés en fonction des exigences commerciales et techniques spécifiques des clients. Nous garantissons un retour sur investissement plus rapide et la bonne expertise au bon moment, ce qui permet aux clients de se concentrer sur le développement de leurs applications sans se soucier de la façon de concevoir et de construire leur plateforme et leur infrastructure d'applications.

Les services CloudOps sont tous certifiés SOC 2, ce qui signifie que tous les systèmes sont dotés de mécanismes de sécurité. Cependant, la plateforme DevOps de CloudOps comporte une option de sécurité SOC 2 qui prend des précautions supplémentaires et comprend ce qui suit :

- Administration des systèmes
- Gestion des incidents
- Installation, réglage et optimisation (gestion des périphériques, incluant une surveillance approfondie de l'instrumentation, des procédures de notification et d'escalade et la création du runbook et du guide d'opérations personnalisées)
- Évaluation de la sécurité
- Balayage des vulnérabilités
- Surveillance des événements de sécurité
- Sécurité en tant que service (avec rapport SOC 2)
- Sécurité du réseau - sécurité du périmètre et du réseau
- Identité, journal et gestion des accès, gestion des intrusions
- Continuité d'activité et reprise sur sinistre
- Respect des contrats de niveau de service
- Soutien 24h / 24, 7j / 7

Le tableau ci-dessous fournit un aperçu des domaines de responsabilité des services de la plateforme DevOps sur AWS, Google Cloud Platform, Microsoft Azure et cloud.ca. Ce tableau est une matrice de haut niveau des activités et des rôles dans la livraison de la plateforme applicative.

Ce tableau RACI montre qui est **(R)esponsable**, **input(A)ble**, **(C)onsulté** et **(I)nformé** selon les différents domaines de responsabilité.

Légende

Inclus dans l'offre MAP standard	Module optionnel de Sécurité SOC 2

Opérations de l'application / code

CloudOps	Opérations de l'application / code	Client ou tierce partie
I	Déploiement et opérations de l'application	RA
I	Surveillance de la performance de l'application	RA
I	Surveillance de la disponibilité de l'application	RA
I	Révision et conception de l'architecture	RA
I	Restauration d'une application après reprise sur sinistre	RA
CI	Test de restauration de la sauvegarde	RA
I	Dépense et gestion de la capacité ou de l'infrastructure en tant que service	RA
I	Service de journalisation de l'application	RAC
CI	Balayage de vulnérabilités de l'application Web	RA

Opérations de la plateforme applicative

CloudOps	Opérations de la plateforme applicative	Client ou tierce partie
RA	VM / AMI limitée + déploiement et opérations du SE	CI
RA	Installation et mises à jour de la plateforme applicative **	CI
RA	Documentation de la plateforme applicative	CI
RA	Exécution et restauration de la sauvegarde	CI
	Réponse de reprise sur sinistre *	CI
RA	Centre de services pour l'infrastructure et la plateforme applicative	CI
RA	Gestion des identités et des accès des utilisateurs (y compris sécurité multi-facteurs)	CI
RA	Surveillance de la plateforme applicative	CI
RA	Disponibilité de la plateforme applicative	CI
RA	Surveillance des performances du serveur, du réseau local et du stockage	CI
RA	Gestion rigoureuse des incidents pour la plateforme applicative	CI
RA	Gestion rigoureuse des changements pour la plateforme applicative	CI
RA	Balayage des vulnérabilités pour le réseau externe	CI
RA	Balayage des vulnérabilités pour le réseau interne	CI
RA	Gestion et correction des vulnérabilités	CI
RA	Renforcement de la sécurité des systèmes d'exploitation (par SE pris en charge)	CI
RA	Renforcement de périphérique réseau (par périphérique réseau pris en charge)	CI
RA	Surveillance de la sécurité de l'ordinateur hôte	CI
RA	Gestion des programmes malveillants (par SE pris en charge)	CI

** La restauration nécessite un plan de reprise sur sinistre déterminé par une entente mutuelle*
*** La plateforme applicative inclut une orchestration de conteneur*

Opérations d'infrastructure

CloudOps	Opérations d'infrastructure	Client ou tierce partie
I	Opérations de l'infrastructure physique et de l'hôte	RAC
	Surveillance du matériel et de l'hyperviseur	RACI
I	Disponibilité de l'infrastructure et du réseau	RAC
	Sécurité, alimentation et environnement du centre de données	RAC
I	Surveillance et opérations du réseau	RACI

Comme on peut le constater, la plateforme DevOps de CloudOps nous confie la responsabilité et l'imputabilité de la plateforme applicative. Le module complémentaire SOC 2 inclut des mécanismes de sécurité rigoureux qui ont été audités par un tiers et couvrent toutes les vulnérabilités connues.

Conclusion

Les entreprises doivent protéger leurs données, mais cette tâche devient plus ardue d'année en année dans un paysage qui devient de plus en plus chaotique. Parallèlement à la couverture médiatique généralisée des violations de données, les exigences de conformité deviennent de plus en plus strictes et urgentes avec de lourdes amendes. Les entreprises doivent mettre en place de solides mécanismes de sécurité.

La certification SOC 2 est un standard de référence en matière de sécurité de l'information. Elle se concentre spécifiquement sur les contrôles de comptes rendus non financiers relatifs à la sécurité, la disponibilité, l'intégrité du traitement et la confidentialité du système. Elle audite de manière exhaustive tous les systèmes et évalue les vulnérabilités potentielles, aidant ainsi à prévenir les violations de données.

La plateforme DevOps de CloudOps peut inclure des processus certifiés SOC 2 pour la gestion sécurisée des composants de la plateforme applicative. Cela permet aux entreprises de se concentrer sur le développement de leurs applications tout en faisant confiance à la santé et à la sécurité sous-jacentes de leur plateforme applicative. Contactez-nous pour plus d'informations sur la manière dont nous pouvons vous aider à créer et à utiliser des plateformes applicatives sécurisées.

CloudOps est une entreprise de conseil et de services dans le nuage qui aide les clients à devenir maîtres de leur destin infonuagique. CloudOps utilise des plateformes et des réseaux infonuagiques de source libre et offre des solutions multi-nuage aux compagnies de logiciels, aux entreprises et aux fournisseurs de télécommunications.