Microsoft | Synack

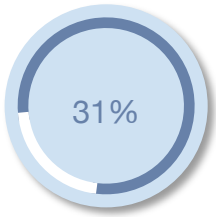
Microsoft Azure Security Modernization

Intégré avec Synack

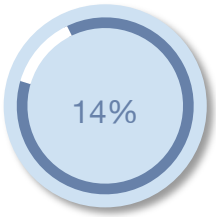
Configuration et sécurité du cloud

80% des violations du cloud en 2020 étaient dues à une mauvaise configuration, à des informations d'identification mal gérées ou à des vols de l'intérieur (Source : Gartner). Les équipes de sécurité sont responsables non seulement de la sécurisation des actifs cloud, mais également du déploiement de la formation et des politiques en matière d'hygiène de sécurité pour les développeurs. Sur la base d'une augmentation des vulnérabilités pour cause de mauvaise configuration du cloud signalées par l'équipe Synack Red en 2020, il apparaît clairement que les solutions et les structures existantes sont fragmentées, laissant amplement de place aux exploits malveillants.

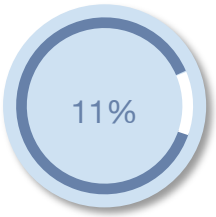
Les vulnérabilités des sessions d'authentification, y compris les informations d'identification par défaut, le contenu des annuaires et l'injection de code, représentent 40 % des exploits cloud signalés par Synack.



Informations d'identification par défaut



Contenu des annuaires



Injection de code

Microsoft et Synack se sont associés pour lancer la toute première solution de test et cadre de sécurité de sécurité cloud proactif de bout en bout.

Microsoft Azure Security Modernization Intégré avec Synack

L'association des experts en sécurité Azure de Microsoft avec les chercheurs en sécurité de classe mondiale de Synack crée une boucle de rétroaction efficace dans laquelle les consultants Microsoft intègrent les données de sécurité Synack dans les programmes de sécurité et de développement de votre entreprise. Les procédures, les stratégies et les environnements spécifiques à Microsoft Azure sont conçus, développés et affinés en fonction de votre résilience réelle aux attaques. L'évaluation Microsoft Azure Security Modernization (ASM) peut être étendue à la plateforme, aux services et aux charges de travail Microsoft Azure et adaptée à vos besoins d'amélioration continue de la sécurité.

EFFICACE

INTÉGRÉ

- Microsoft a dirigé le développement et la gestion des stratégies d'Azure
- Intégrations Microsoft Azure clé en main pour les tests multi-cloud sur les actifs Web, les infrastructures et les API
- Campagnes de tests manuels spécifiques à Microsoft Azure
- Intégrations Microsoft Azure DevOps Boards, Jira, Splunk et ServiceNow

AGILE

- Contrôles de sécurité évolutifs déployés dans votre pipeline CI/CD via Microsoft Azure Policy ou Azure Resource Manager
- Tests manuels continus pour les menaces cloud dynamiques dans les environnements de production ou de pré-production
- Tests de sprint—«Campagnes de microtest»—pour les tests manuels alignés sur les versions DevOps

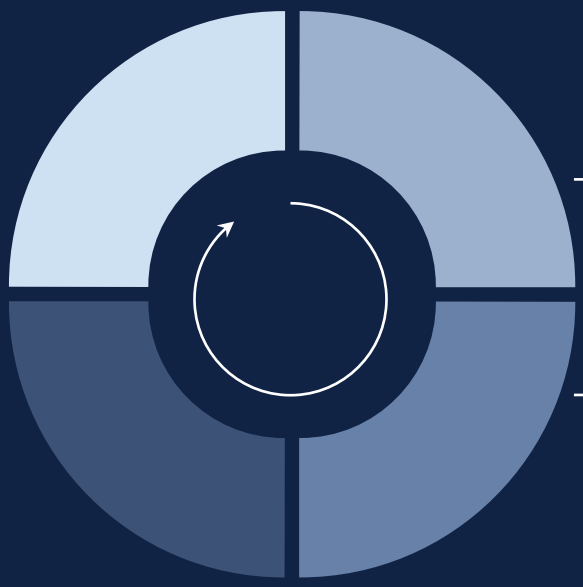
TRANSPARENT

- Bonnes pratiques Microsoft alignées sur votre appétence au risque d'entreprise
- Fonctionnalités Microsoft Azure Security Center intégrées pour auditer en continu les exigences de sécurité
- Mesures et analyses des tests manuels via la plateforme Synack pour un examen en temps réel de la couverture

COMFORME

- Structure Microsoft Azure Security Benchmark déployée en fonction de vos exigences commerciales et de conformité
- Tests d'intrusion et rapports alignés sur les normes du secteur (NIST, CIS, OWASP, PCI et HIPAA)

Approche à l'évaluation Microsoft Azure Security Modernization



PLANNIFIER

Décrivez les objectifs de contrôle et les exigences en matière de risque personnalisés (la « base de référence de sécurité ») pour votre plateforme, vos services et vos charges de travail Microsoft Azure.

DÉVELOPPER

Définissez et codez des contrôles automatisés alignés sur votre base de sécurité pour évoluer avec la croissance de votre entreprise et vos exigences futures.

DÉLIVRER

Appliquez un flux de travail continu pour la révision et le déploiement du code afin d'assurer la collaboration et la cohérence du code.

MESURER

Synack pour mesurer l'efficacité des contrôles de sécurité déployés et alimenter les données dans les phases de planification via les campagnes de missions ciblées Microsoft ASM et la découverte des vulnérabilités.

La plateforme Synack

Synack est la seule solution avec une intégration Microsoft Azure clé en main pour des tests offensifs. L'intégration permet une pénétration continue et des tests de sécurité offensifs qui s'étendent aux applications Web et mobiles, aux réseaux internes et externes ainsi qu'aux actifs gérés par Azure avec des adresses IP attribuées dynamiquement.

La plateforme Synack s'appuie sur une grande élite de chercheurs mondiaux et sur une technologie exclusive pour les tests, le contrôle et la transparence à la demande. Nous apportons à nos clients des données sans frictions et exploitables en temps réel :

- Détails des vulnérabilités exploitables et évaluations du risque
- Tests des contrôles de sécurité
- Données et points de vue des chercheurs
- Scores de résistance aux attaques
- Répétition à la demande des tests via la vérification des correctifs
- Rapports personnalisés et complets à la demande

Microsoft Consulting Services

Depuis plus de 35 ans, nous nous engageons à promouvoir la sécurité de nos produits et services, en aidant nos clients et partenaires à protéger leurs actifs jusqu'à garantir que leurs données restent sécurisées et privées. Nous nous concentrons sur la sécurité, l'identité et les écosystèmes de protection des informations, en tirant parti de partenariats avec des fournisseurs et des sociétés de conseil du monde entier pour apporter des changements à nos produits et services afin de vous offrir une protection pour vos actifs intellectuels.

En savoir plus

Contactez votre représentant Synack Consulting Services en écrivant à microsoft@synack.com.