Synack

Member of
Microsoft Intelligent
Security Association
Microsoft

Gérer les résultats des tests d'intrusion Synack à partir de Microsoft Defender for Cloud

Synack et Microsoft Defender for Cloud : un puissant partenariat de sécurité

Garder votre cloud hybride à l'abri des cybercriminels est une tâche ardue. Les pirates recherchent constamment des vulnérabilités dans vos actifs hébergés dans le cloud qu'ils peuvent exploiter pour accéder à vos systèmes principaux. Microsoft Defender for Cloud aide à protéger contre les menaces, en fournissant des outils pour gérer la politique de sécurité et la conformité de votre entreprise. Il vous permet de surveiller les erreurs de configuration et les vulnérabilités connues, en offrant aux ingénieurs et aux responsables de la sécurité une vue en temps réel de l'état de sécurité de leur cloud Microsoft Azure à travers des tableaux de bord faciles à consulter.

Mais il manque un élément essentiel dans cette vue de la sécurité. Vous devez être en mesure de valider ces erreurs de configuration et de créer des vecteurs d'attaque pour rechercher et signaler les vulnérabilités au niveau de la couche réseau ainsi qu'en interne dans votre environnement cloud. Synack, avec l'équipe de tests d'intrusion participative la plus qualifiée et la plus fiable au monde et une technologie d'intelligence artificielle propriétaire, peut effectuer un test d'intrusion et communiquer les résultats à Microsoft Defender for Cloud, où les vulnérabilités peuvent être étudiées et résolues.

Dans le cadre du partenariat mondial entre Microsoft et Synack, les résultats de votre évaluation Synack sont automatiquement renseignés dans Microsoft Defender for Cloud via l'une de nos intégrations À supprimer à la plate-forme Microsoft.

- Intégrez les données de vulnérabilité découvertes par Synack dans votre instance Microsoft Defender for Cloud pour rationaliser vos processus de gestion des vulnérabilités.
- Protégez votre environnement cloud dynamique avec les tests de pénétration Synack et les tests continus grâce à une intégration avec Microsoft Azure.
- Envoyez automatiquement vos résultats d'évaluation Synack à Microsoft Defender for Cloud grâce à notre intégration facile.
- Affichez et gérez l'état de la vulnérabilité de votre réseau dans les affichages familiers de Microsoft Defender for Cloud.

Optimisation de la gestion des vulnérabilités dans Microsoft Azure

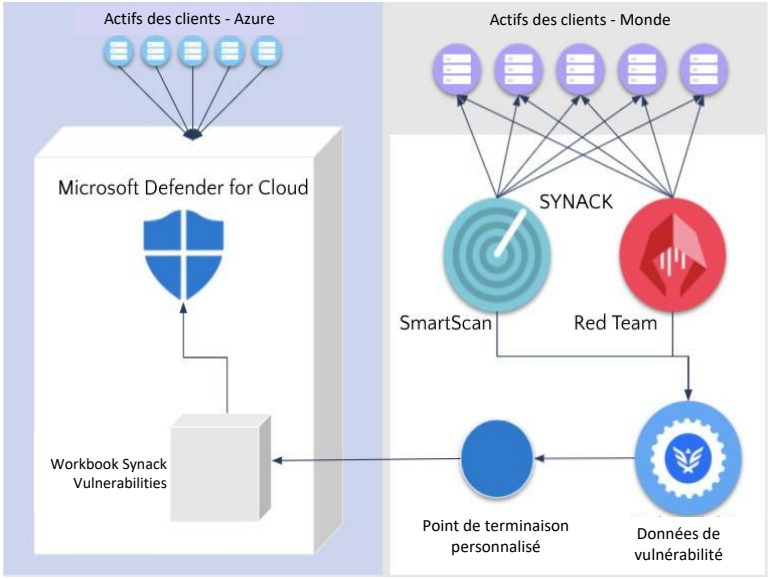
Grâce à l'intégration de Synack avec Microsoft Defender for Cloud, vous pouvez envoyer et afficher automatiquement les résultats de votre test d'intrusion Synack dans un classeur personnalisé Microsoft Defender for Cloud. Cela signifie que les ingénieurs et les responsables de la sécurité déjà familiarisés avec les tableaux de bord et les affichages de Microsoft Defender for Cloud n'ont pas besoin d'apprendre le format d'affichage d'un autre outil pour afficher et agir sur les informations de vulnérabilité.

Intégration

Synack fournit un workbook Microsoft Azure personnalisé avec des données de vulnérabilité Synack dans votre Microsoft Defender for Cloud. Une application back-end hébergée par Synack fournit un point de terminaison personnalisé pour le workbook. Synack fournit le modèle par défaut pour le workbook Synack Vulnerabilities, permettant à l'utilisateur final de modifier davantage l'apparence du workbook ou d'utiliser le point de terminaison pour créer de nouveaux classeurs.

Synack simplifie l'intégration.

Un jeton d'API Synack doit d'abord être créé afin de déployer le modèle Synack Workbook ARM (Microsoft Azure Resource Manager) avec Microsoft Defender for Cloud.



Le workbook est ensuite rendu accessible dans Microsoft Defender for Cloud. Chaque fois que Synack effectue un test d'intrusion, les résultats seront affichés dans le workbook Microsoft Defender for Cloud.

Plus de 90 % des problèmes de sécurité dans le cloud sont directement causés par des erreurs de configuration.

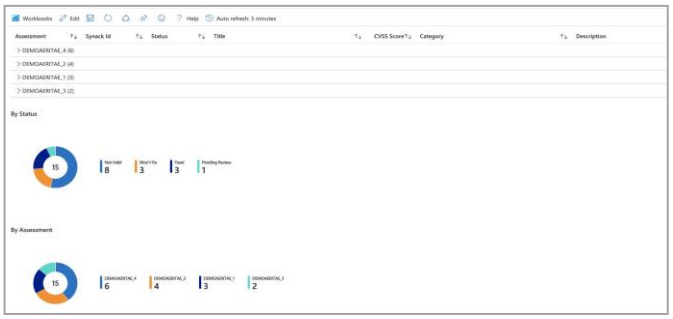
Afficher les résultats de l'évaluation Synack dans Microsoft Defender for Cloud

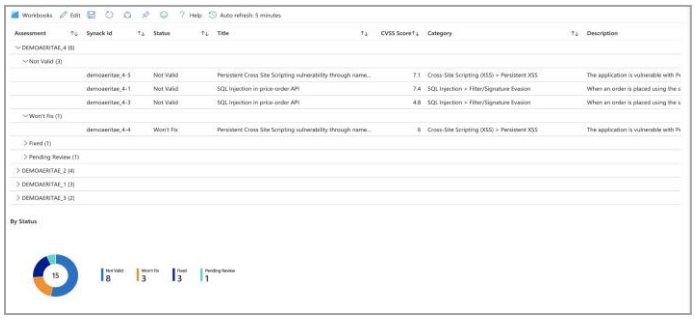
Plus de 90 % des problèmes de sécurité du cloud sont directement causés par des erreurs de configuration.[1] Synack vous aide à découvrir les vulnérabilités exploitables qui peuvent résulter de ces erreurs de configuration.
Les vulnérabilités des sessions d'authentification, y compris les informations d'identification par défaut, le contenu des annuaires et l'injection de code, représentent 40 % des exploits cloud signalés par Synack. Vous pouvez désormais afficher et gérer ces vulnérabilités directement dans Microsoft Defender for Cloud.

Grâce à cette intégration, les clients peuvent synchroniser automatiquement leurs données du portail client Synack vers Microsoft Defender for Cloud. Toutes les sorties d'informations sur les vulnérabilités sont centralisées et s'appuient sur des formats largement utilisés par les utilisateurs de Microsoft Azure, permettant aux ingénieurs et aux responsables de la sécurité de surveiller efficacement l'état général de la sécurité du réseau.

Synack calcule et attribue manuellement à chaque vulnérabilité découverte un score CVSS dans le cadre de l'examen d'assurance qualité rigoureux inclus dans chaque évaluation. Toutes les vulnérabilités identifiées sont affichées dans le workbook Microsoft Defender for Cloud. Les équipes de sécurité peuvent afficher l'état de la vulnérabilité dans le classeur et prendre les mesures appropriées.
Les utilisateurs autorisés peuvent demander des informations supplémentaires sur toute vulnérabilité identifiée et mise à disposition sur le portail client Synack.

Liste des vulnérabilités dans le workbook Microsoft Defender for Cloud





1. XM Cyber, « What is Cloud Security Posture Management », 2021, https://www.xmcyber.com/what-is-cloud-security-posture-management/