Synack

Member of Microsoft Intelligent Security Association

Microsoft

L’intégration de Synack avec Microsoft Sentinel accélère la gestion des vulnérabilités de sécurité

Aperçu

Microsoft Sentinel est une solution unique, évolutive et native du cloud pour l’analyse intelligente de la sécurité, la gestion des événements, la détection des menaces, la visibilité des menaces, la chasse proactive et la réponse aux menaces.
Il aide à fournir une détection précoce des menaces et une réponse rapide aux attaques sophistiquées pour faciliter des temps de résolution plus courts et une réduction du volume d’incidents de sécurité dans vos ressources cloud Microsoft Azure. Pour aider à réduire encore plus les temps de remédiation et de résolution, Synack fournit désormais une intégration directe à Microsoft Sentinel pour créer automatiquement des incidents Microsoft Sentinel à partir des données de test de vulnérabilité de Synack.

- Protégez votre cloud Microsoft Azure en synchronisant les résultats des tests de vulnérabilité Synack avec Microsoft Sentinel
- Les vulnérabilités nouvellement découvertes créent automatiquement des incidents dans Microsoft Sentinel pour une analyse et une correction rapides
- L’intégration et la configuration faciles vous permettent de démarrer rapidement
- Affichez et gérez les incidents dans les écrans familiers de Microsoft Sentinel

Synack et Microsoft Sentinel travaillent ensemble pour accélérer le délai de résolution

Microsoft Sentinel combine deux technologies de sécurité en une seule solution, la gestion des informations et des événements de sécurité (SEIM) et la réponse automatisée d’orchestration de la sécurité (SOAR). Il prend en charge différentes sources de données de toute l’entreprise et effectue une corrélation des données entre ces sources, en tirant parti des analyses de sécurité intelligentes et des renseignements sur les menaces. Avec Microsoft Sentinel, les opérations de sécurité peuvent :

- Recevoir des alertes en temps réel
- Corriger les incidents à l’aide de l’apprentissage automatique et de l’intelligence artificielle (IA) pour la détection, l’analyse et l’identification des menaces
- Exécuter une chasse proactive

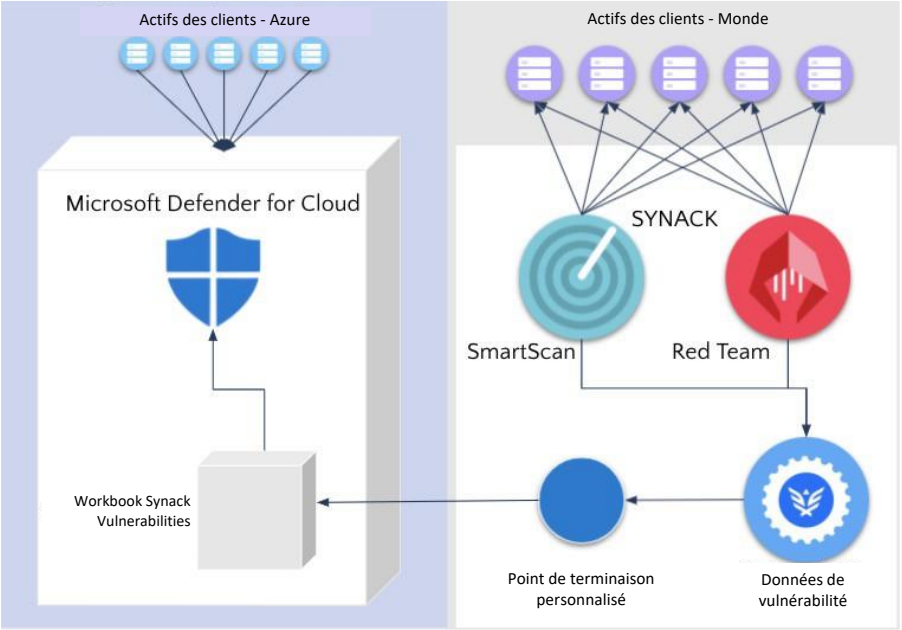
Cela donne aux équipes de sécurité une visibilité de bout en bout des événements liés à la sécurité et les aide à obtenir des informations directes ainsi qu’à analyser les capacités au même endroit. Microsoft Sentinel peut explorer et tenter de traiter les menaces potentielles sur le cloud par lui-même ou il peut vous alerter des menaces potentielles.

La gestion et la correction rapides des vulnérabilités exploitables sont essentielles pour minimiser les menaces pesant sur votre cloud. Synack emploie L'équipe de chercheurs éthiques la plus compétente et la plus fiable au monde, ainsi qu'une technologie d'intelligence artificielle propriétaire, pour effectuer une découverte continue ou ponctuelle des vulnérabilités. La solution Microsoft Sentinel de Synack aide à réduire les temps de résolution en synchronisant ces résultats avec Microsoft Sentinel.

La solution Microsoft Sentinel de Synack fournit un connecteur A effacer pour synchroniser les données de vulnérabilité de votre compte Synack vers Microsoft Sentinel. Il crée un incident dans Microsoft Sentinel pour chaque vulnérabilité et maintient les données d'incident à jour avec les dernières modifications de la vulnérabilité. Aucune intervention humaine n'est nécessaire pour transmettre les informations de vulnérabilité à Microsoft Sentinel. Microsoft Sentinel peut ensuite utiliser les informations Synack de ces incidents dans l'analyse et le traitement des menaces. De plus, vous pouvez tout gérer dans l'environnement Microsoft Sentinel que vous connaissez déjà.

Intégration facile

La synchronisation des données est effectuée par une fonction Microsoft Azure qui utilise à la fois les API Synack et Microsoft Sentinel pour transférer les données Synack vers Microsoft Sentinel. La solution Microsoft Sentinel de Synack est disponible sur le portail Microsoft Azure sur la place de marché Visual Studio. Une fois l'installation réussie du collecteur de données Microsoft Sentinel, la synchronisation démarre immédiatement. Aucune autre configuration n'est nécessaire dans le portail Microsoft Azure ou Synack.



L'écran d'incident Microsoft Sentinel montrant les vulnérabilités de Synack

Si tous les paramètres saisis lors du déploiement du connecteur de données sont corrects, vous devriez commencer à voir les nouveaux incidents créés dans Vulnérabilités Microsoft Sentinel de Synack. Vous pouvez également consulter les journaux de la fonction Microsoft Azure déployée.

Chaque vulnérabilité Synack créera un nouvel incident dans Microsoft Sentinel. Les valeurs des champs Synack sont transmises à la description du champ dans l'incident Microsoft Azure. Si l'état d'une vulnérabilité Synack change, l'état de l'incident Microsoft Sentinel correspondant est mis à jour en conséquence lors de la prochaine synchronisation. Dans Microsoft Sentinel, les incidents ont l'un des 3 états : Nouveau, Actif, Fermé. Cet ensemble d'états dans Microsoft Sentinel est fixe et n'est pas modifiable. Dans Synack, vous pouvez avoir n'importe quel nombre d'états. Cependant, chacun d'entre eux appartient à l'une des 3 catégories majeures : Nouveau, Ouvert, Fermé.