Synack

Member of Microsoft Intelligent Security Association

Microsoft

Verwalten Sie die Ergebnisse für Synack Penatrationstests mit Microsoft Defender for Cloud

Synack und Microsoft Defender for Cloud - Eine leistungsstarke Sicherheitspartnerschaft

Die Sicherheit Ihrer Hybrid-Cloud vor Cyber-Kriminellen zu gewährleisten, ist eine gewaltige Aufgabe. Hacker sind ständig auf der Suche nach Schwachstellen in Anwendungen, die in der Cloud gehostet sind, um diese gezielt zum Durchgriff auf weitere Kernsysteme eines Unternehmen auszunutzen. Microsoft Defender for Cloud hilft beim Schutz vor Bedrohungen und bietet Tools zur Verwaltung der Sicherheitsrichtlinien und der Compliance Ihres Unternehmens. Es ermöglicht die Überwachung von Fehlkonfigurationen und bekannten Schwachstellen und bietet Sicherheitsingenieuren und Managern einen Echtzeitüberblick über den Sicherheitsstatus ihrer Microsoft Azure-Cloud in übersichtlichen Dashboards.

In dieser Sicherheitsbetrachtung fehlt allerdings ein entscheidender Teil. Sie müssen in der Lage sein, diese Fehlkonfigurationen zu validieren und Angriffsvektoren zu erstellen, um nach Schwachstellen auf der Netzwerkebene sowie intern in Ihrer Cloud-Umgebung zu suchen und diese zu melden. Synack, mit dem weltweit kompetentesten und vertrauenswürdigsten Crowd-Sourced Team für Penetrationstests und einer eigenen KI-Technologie, kann einen Penetrationstest durchführen und die Ergebnisse an Microsoft Defender for Cloud melden, wo die Schwachstellen untersucht und behoben werden können.

Hacker sind ständig auf der Suche nach Schwachstellen in Anwendungen, die in der Cloud gehostet sind, um diese gezielt zum Durchgriff auf weitere Kernsysteme eines Unternehmen auszunutzen.

- Integrieren Sie die von Synack entdeckten Schwachstellen in Ihre Microsoft Defender for Cloud-Instanz, um Ihre Prozesse für das Schwachstellenmanagement zu optimieren.
- Schützen Sie Ihre dynamische Cloud-Umgebung durch Penetration- und kontinuierliche Security Tests von Synack und der Integration mit Microsoft Azure.
- Übertragen Sie mit unserer einfachen Integration Ihre Synack-Testergebnisse automatisch an Microsoft Defender for Cloud.
- Überwachen und verwalten Sie den Status von Schwachstellen in der zentralen Anzeige von Microsoft Defender for Cloud asl "Single Source".

Optimierung der Schwachstellenverwaltung in Microsoft Azure

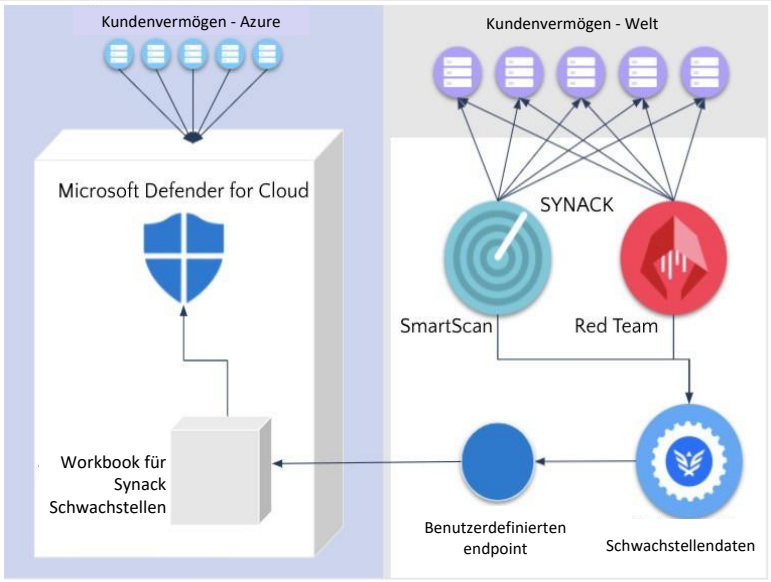
Durch die Integration von Synack mit Microsoft Defender for Cloud können Sie die Ergebnisse Ihres Synack Penetrationstests automatisch an ein benutzerdefiniertes Workbook von Microsoft Defender for Cloud senden und dort anzeigen lassen. Das bedeutet, dass Sicherheitsingenieure und -manager, die bereits mit den Dashboards und Anzeigen von Microsoft Defender for Cloud vertraut sind, nicht das Anzeigeformat eines anderen Tools erlernen müssen, um Informationen zu Schwachstellen anzuzeigen und darauf zu reagieren.

Integration

Synack stellt ein benutzerdefiniertes Microsoft Azure Workbook mit Daten zu Synack Schwachstellen innerhalb Ihres Microsoft Defender for Cloud zur Verfügung. Eine von Synack gehostete Backend-Anwendung bietet einen benutzerdefinierten Endpunkt für das Workbook. Synack stellt eine Standardvorlage für das Workbook für Synack Schwachstellen zur Verfügung, das es dem Endbenutzer ermöglicht, das Aussehen des Workbooks weiter zu verändern oder den Endpunkt zur Erstellung neuer Workbooks zu verwenden.

Synack macht die Integration einfach.

Um die Synack Workbook ARM (Microsoft Azure Resource Manager)-Vorlage mit Microsoft Defender for Cloud bereitstellen zu können, muss zunächst ein Synack API-Token erstellt werden.



Die Arbeitsmappe wird dann in Microsoft Defender for Cloud zugänglich gemacht. Jedes Mal, wenn Synack einen Penetrationstest durchführt, werden die Ergebnisse in der Arbeitsmappe Microsoft Defender for Cloud angezeigt.

Mehr als 90 % der Sicherheitsprobleme in der Cloud werden direkt durch Fehlkonfigurationen verursacht.

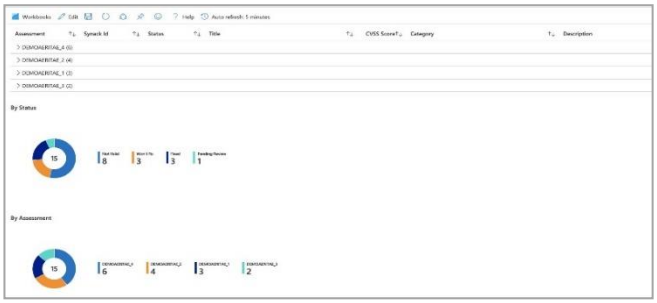
Anzeige der Synack-Bewertungsergebnisse in Microsoft Defender for Cloud

Mehr als 90 % der Sicherheitsprobleme in der Cloud werden direkt durch Fehlkonfigurationen verursacht.[1] Synack hilft Ihnen, anfällige Schwachstellen zu entdecken, die aus diesen Fehlkonfigurationen resultieren können.
Schwachstellen bei Authentifizierungssitzungen, wie unter anderem Standard-Anmeldedaten, Verzeichnisinhalten und Code-Injektionen, machen 40% der von Synack genannten Cloud-Exploits aus. Jetzt können Sie diese Schwachstellen direkt in Microsoft Defender for Cloud anzeigen und verwalten.

Mit dieser Integration können Kunden ihre Daten aus dem Synack Client Portal automatisch mit Microsoft Defender for Cloud synchronisieren. Alle ausgegebenen Schwachstelleninformationen werden zentralisiert und nutzen Formate, die von Microsoft Azure-Benutzern häufig verwendet werden, sodass Sicherheitsingenieure und -manager die gesamte Netzwerksicherheit effizient überwachen können.

Synack berechnet und vergibt für jede entdeckte Schwachstelle manuell einen CVSS-Score als Teil der robusten Qualitätssicherungsprüfung, die in jeder Bewertung enthalten ist. Alle erkannten Schwachstellen werden im Workbook Microsoft Defender for Cloud angezeigt. Sicherheitsteams können den Schwachstellenstatus im Workbook einsehen und entsprechende Maßnahmen ergreifen.
Autorisierte Benutzer können zusätzliche Informationen zu jeder erkannten Schwachstelle anfordern, die im Synack Client Portal zur Verfügung gestellt werden.

Liste der Sicherheitsrisiken in Microsoft Defender for Cloud Workbook



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