Synack

Member of Microsoft Intelligent Security Association

Microsoft

Beheer de testresultaten van Synack-penetraties vanuit Microsoft Defender for Cloud

Synack en Microsoft Defender for Cloud: een krachtig partnerschap voor beveiliging

Uw hybride cloud beveiligen en beschermen tegen cybercriminelen is vaak een hele klus. Hackers zijn voortdurend op zoek naar beveiligingsproblemen in uw bedrijfsmiddelen die in de cloud worden gehost. Ze willen deze misbruiken om toegang te krijgen tot uw belangrijkste systemen. Microsoft Defender for Cloud helpt u te beschermen tegen bedreigingen en biedt tools voor het beheer van het beveiligingsbeleid en de compliance van uw organisatie. U kunt er onjuiste configuraties en bekende beveiligingsproblemen mee opsporen en security engineers en managers krijgen een realtime overzicht van de beveiligingsstatus van hun Microsoft Azure-cloud via gebruiksvriendelijke dashboards.

Maar er ontbreekt iets belangrijks in dit beveiligingsoverzicht. U moet deze onjuiste configuraties kunnen valideren en aanvalsvectoren kunnen maken om beveiligingsproblemen op te sporen en te rapporteren, zowel op het netwerk als binnen uw cloudomgeving. Synack beschikt over 's werelds meest bekwame en vertrouwde crowd-sourced teams voor penetratietests en eigen AI-technologie en kan een penetratietest uitvoeren en de resultaten rapporteren aan Microsoft Defender for Cloud, waar de beveiligingsproblemen kunnen worden onderzocht en verholpen.

Als onderdeel van de wereldwijde samenwerking tussen Microsoft en Synack worden de resultaten van de Synack-beoordeling automatisch ingevuld in Microsoft Defender for Cloud, via een van onze eenvoudige Microsoft Platform-integraties.

- Integreer door Synack ontdekte gegevens over beveiligingsproblemen in uw Microsoft Defender for Cloud-instance en stroomlijn uw processen voor het beheer van beveiligingsproblemen.
- Help uw dynamische cloudomgeving te beschermen met Synack-penetratietests en doorlopende tests via een integratie met Microsoft Azure.
- Stuur uw Synack-beoordelingsresultaten automatisch naar Microsoft Defender for Cloud met onze eenvoudige integratie.
- Bekijk en beheer de status van problemen met de netwerkbeveiliging op vertrouwde Microsoft Defender for Cloud-schermen.

Optimalisatie van het beheer van beveiligingsproblemen in Microsoft Azure

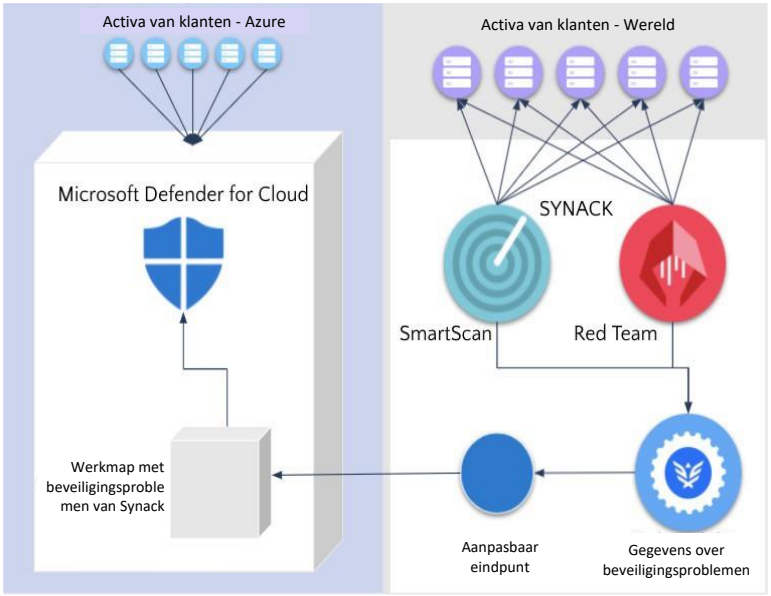
Via de integratie van Synack met Microsoft Defender for Cloud kunt u de resultaten van uw Synack-penetratietest automatisch laten versturen naar en weergeven in een gepersonaliseerde werkmap van Microsoft Defender for Cloud. Dit betekent dat security engineers en managers die al vertrouwd zijn met de dashboards en schermen van Microsoft Defender for Cloud geen andere weergave-indeling van een tool hoeven aan te leren om informatie over beveiligingsproblemen te bekijken en erop te reageren.

Integratie

Synack biedt een aanpasbare Microsoft Azure-werkmap met gegevens over beveiligingsproblemen in Synack binnen Microsoft Defender for Cloud. Een door Synack gehoste backend-applicatie biedt een aanpasbaar eindpunt voor de werkmap. Synack levert het standaardsjabloon voor de werkmap met beveiligingsproblemen van Synack. De eindgebruiker kan het uiterlijk van de werkmap verder kan aanpassen, of het eindpunt gebruiken om nieuwe werkmappen te maken.

Synack maakt de integratie ervan eenvoudig.

Er moet eerst een Synack API-token worden aangemaakt om het Synack Workbook ARM (Microsoft Azure Resource Manager)-sjabloon te kunnen implementeren met Microsoft Defender for Cloud.



De werkmap wordt vervolgens toegankelijk gemaakt in Microsoft Defender for Cloud. Telkens wanneer Synack een penetratietest uitvoert, worden de resultaten weergegeven in de Microsoft Defender for Cloud-werkmap.

Onjuiste configuraties zijn de rechtstreekse oorzaak van meer dan 90% van de beveiligingsproblemen in de cloud.

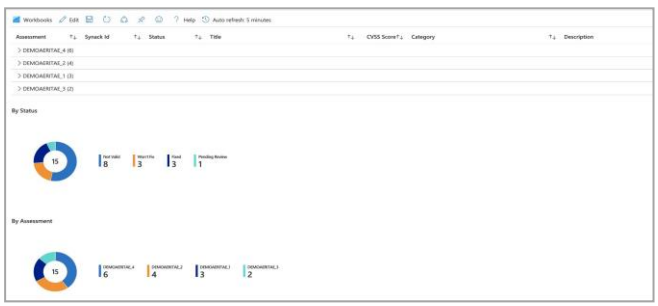
Bekijk Synack-beoordelingsresultaten in Microsoft Defender for Cloud

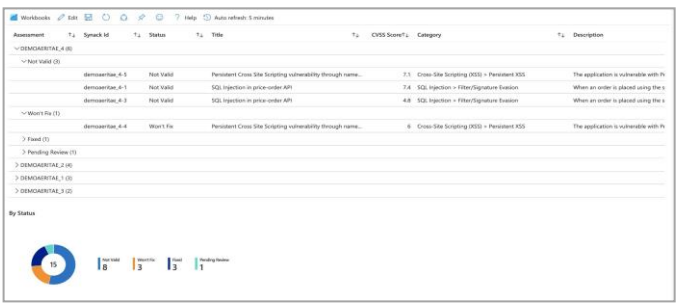
Meer dan 90% van de beveiligingsproblemen in de cloud worden rechtstreeks veroorzaakt door onjuiste configuraties.[1] Synack helpt u beveiligingsproblemen te ontdekken die door deze onjuiste configuraties worden veroorzaakt.
Beveiligingsproblemen met betrekking tot verificatiesessies, waaronder standaard inloggegevens, mapinhoud en code-injectie, maken 40% uit van de door Synack gemelde cloud-exploits. Nu kunt u deze beveiligingsproblemen rechtstreeks in Microsoft Defender for Cloud bekijken en beheren.

Dankzij deze integratie kunnen klanten hun gegevens automatisch synchroniseren van de Synack-klantenportal naar Microsoft Defender for Cloud. Alle verstrekte gegevens over beveiligingsproblemen worden gecentraliseerd en gebruiken indelingen die op grote schaal worden gebruikt door Microsoft Azure-gebruikers, waardoor security engineers en managers de algehele netwerkbeveiligingsstatus efficiënt kunnen bewaken.

Synack berekent handmatig alle ontdekte beveiligingsproblemen en kent er een CVSS-score aan toe als onderdeel van een betrouwbaar kwaliteitsoverzicht dat bij elke beoordeling wordt gegeven. Alle gevonden beveiligingsproblemen worden weergegeven in de Microsoft Defender for Cloud-werkmap. Beveiligingsteams kunnen de status van de beveiligingsproblemen in de werkmap bekijken en passende maatregelen nemen.
Gemachtigde gebruikers kunnen aanvullende informatie opvragen over alle gevonden beveiligingsproblemen en deze onmiddellijk beschikbaar maken in de Synack-klantenportal.

Lijst met beveiligingsproblemen in Microsoft Defender for Cloud-werkmap





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