Synack

Member of Microsoft Intelligent Security Association

Microsoft

Synack-integratie met Microsoft Sentinel versnelt de behandeling van beveiligingslekken

Overzicht

Microsoft Sentinel is een schaalbare, cloud-eigen, enkelvoudige oplossing voor intelligente beveiligingsanalyses, eventbeheer, detectie van bedreigingen, overzicht van bedreigingen, proactieve opsporing en reactie op bedreigingen.
Het verzorgt vroegtijdige opsporing van bedreigingen en snelle reactie op uitgekiende aanvallen, zodat deze sneller worden opgelost en het aantal beveiligingsincidenten in uw Microsoft Azure-cloudsoftware afneemt. Om nog sneller tot een herstel of oplossing te komen, biedt Synack nu een directe integratie met Microsoft Sentinel om automatisch Microsoft Sentinel-incidenten aan te maken op basis van de beveiligingstestgegevens van Synack.

- Help uw Microsoft Azure-cloud te beschermen door de resultaten van Synack-beveiligingtesten te synchroniseren met Microsoft Sentinel.
- Nieuw gevonden beveiligingsproblemen maken automatisch incidenten aan in Microsoft Sentinel voor snelle analyse en herstel.
- Eenvoudige integratie en configuratie zodat u snel aan de slag kunt.
- Bekijk en beheer incidenten op vertrouwde Microsoft Sentinel-schermen

Synack en Microsoft Sentinel werken samen om sneller tot een oplossing te komen

Microsoft Sentinel combineert twee beveiligingstechnologieën, namelijk beveiligingsinformatie- en eventbeheer (Security Information and Event Management, SEIM) en de geautomatiseerde respons via beveiligingsorkestratie (Security Orchestration automated Response, SOAR) in één enkele oplossing. Het neemt verschillende gegevensbronnen uit de hele onderneming op en voert gegevenscorrelatie tussen deze bronnen uit, waarbij gebruik wordt gemaakt van intelligente beveiligingsanalyses en informatie over bedreigingen. Met Microsoft Sentinel kunnen beveiligingsactiviteiten:

- realtime waarschuwingen ontvangen
- incidenten verhelpen met behulp van machine learning en kunstmatige intelligentie (AI) voor detectie, analyse en identificatie van bedreigingen
- proactief opsporingen uitvoeren

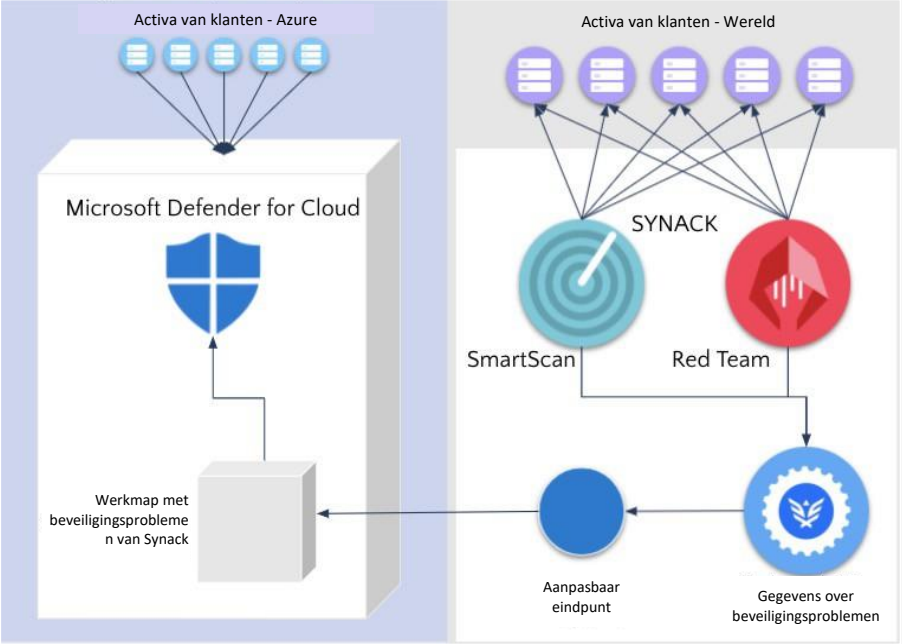
Daardoor hebben beveiligingsteams een end-to-end-zicht op beveiligingsgerelateerde events, krijgen ze onmiddellijk inzichten en kunnen ze mogelijkheden analyseren, allemaal op één locatie. Microsoft Sentinel kan zelfstandig mogelijke bedreigingen voor de cloud onderzoeken en proberen aan te pakken of u waarschuwen voor de mogelijke bedreigingen.

Snel beheer en verhelpen van beveiligingsproblemen die kunnen worden misbruikt, is van uiterst groot belang om bedreigingen voor uw cloud te beperken. Synack maakt gebruik van 's werelds beste en meest betrouwbare crowd-sourced penetratietestteam en eigen AI-technologie, om doorlopend of op een bepaald moment beveiligingsproblemen op te sporen. De Microsoft Sentinel-oplossing van Synack helpt deze problemen sneller op te lossen door de resultaten te synchroniseren met Microsoft Sentinel.

De Microsoft Sentinel-oplossing van Synack biedt een dataconnector, om gegevens over beveiligingsproblemen van uw Synack-account te synchroniseren met Microsoft Sentinel. Het maakt in Microsoft Sentinel een incident aan voor elk beveiligingsprobleem en houdt de incidentgegevens up-to-date met de laatste wijzigingen van beveiligingsproblemen. Er is geen menselijke tussenkomst nodig om de informatie over beveiligingsproblemen naar Microsoft Sentinel te versturen. Microsoft Sentinel kan de gegevens van Synack in deze incidenten gebruiken bij de analyse en verwerking van bedreigingen. Bovendien kunt u alles beheren in de Microsoft Sentinel-omgeving waarmee u al vertrouwd bent.

Eenvoudige integratie

Gegevenssynchronisatie wordt uitgevoerd door een Microsoft Azure-functie die API's van Synack en van Microsoft Sentinel gebruikt om Synack-gegevens over te brengen naar Microsoft Sentinel. De Microsoft Sentinel-oplossing van Synack is beschikbaar via de Microsoft Azure-portal in Visual Studio Marketplace. Nadat u de gegevensverzamelaar van Microsoft Sentinel hebt geïnstalleerd, wordt de synchronisatie onmiddellijk gestart. Extra configuraties in de Microsoft Azure- of Synack-portal zijn niet nodig.



Scherm met Microsoft Sentinel-incidenten die Synack-beveiligingsproblemen weergeven

Als alle parameters die zijn ingevoerd tijdens de implementatie van de gegevensconnector juist zijn, zult u nieuwe incidenten te zien krijgen die zijn aangemaakt in Microsoft Sentinel van Synack-beveiligingsproblemen. U kunt ook de logbestanden van de geïmplementeerde Microsoft Azure-functie controleren.
Elk beveiligingsprobleem in Synack maakt een nieuw incident aan in Microsoft Sentinel. De waarden van Synack-velden worden overgebracht naar de veldbeschrijving in het Microsoft Azure-incident. Als de status van een beveiligingsprobleem in Synack verandert, wordt de status van het overeenkomstige Microsoft Sentinel-incident bij de volgende synchronisatie dienovereenkomstig bijgewerkt. In Microsoft Sentinel hebben incidenten één van de drie statussen: nieuw, actief of gesloten. Deze reeks statussen in Microsoft Sentinel ligt vast en kan niet worden geconfigureerd. In Synack kunnen er een willekeurig aantal statussen worden toegewezen. Maar elk van deze behoort tot een van de drie belangrijke categorieën: nieuw, open of gesloten.