

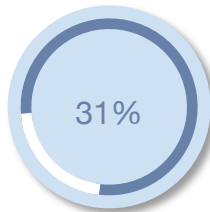
Microsoft Azure Security Modernization

Geïntegreerd met Synack

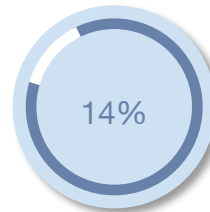
Cloudconfiguratie en beveiliging

80% cloudinbreuken in 2020 waren te wijten aan verkeerde configuratie, verkeerd beheerde toegangsgegevens of diefstalpogingen van binnenuit (bron: Gartner). Beveiligingsteams zijn niet alleen verantwoordelijk voor het beveiligen van cloud-activa, maar ook voor het uitrollen van veiligheidshygiënetraining en -beleid naar ontwikkelaars. Op basis van een toename van het aantal kwetsbaarheden in cloudconfiguraties die in 2020 door het Synack Red Team zijn gemeld, is het duidelijk dat de bestaande oplossingen en raamwerken gefragmenteerd zijn, waardoor er veel ruimte is voor kwaadwillig misbruik.

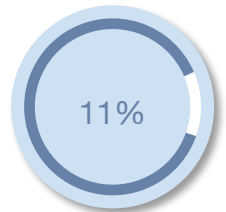
Kwetsbaarheden met betrekking tot authenticatiesessies, waaronder standaardreferenties, mapinhoud en code-injectie, maken 40% uit van de door Synack gemelde cloud-exploits.



Standaard toegangsgegevens



Mapinhoud



Code-injectie

Microsoft en Synack zijn een partnerschap aangegaan om het eerste end-to-end, proactieve cloudbeveiligings-framework en testoplossing te lanceren.

Microsoft Azure Security Modernization Geïntegreerd met Synack

Door Microsofts eigen Azure-beveiligingsexperts te koppelen aan de beveiligingsonderzoekers van wereldklasse van Synack ontstaat een efficiënte feedbackloop waarin Microsoft-consultants beveiligingsgegevens van Synack integreren in uw bedrijfsbeveiligings- en ontwikkelingsprogramma's. Specifieke Microsoft Azure-procedures, beleidsregels en omgevingen worden ontworpen, ontwikkeld en aangepast op basis van uw werkelijke aanvalsbestedigheid. Microsoft Security Modernization (ASM) kan voor het Microsoft Azure-platform worden aangepast; diensten en workloads kunnen worden geschaald naar uw behoeften voor continue verbetering van de beveiliging.

RESULTATEN

GEÏNTEGREERD

- Beleidsontwikkeling en -management van Azure, geleid door Microsoft
- Kant-en-klare Microsoft Azure integraties voor multi cloud testen op web, infrastructuur en API assets
- Handmatige testcampagnes specifiek voor Microsoft Azure
- Microsoft Azure DevOps Boards, Jira, Splunk, en ServiceNow integraties

FLEXIBEL

- Schaalbare beveiligingscontroles die worden ingezet in uw CI/CD-pijplijn via Microsoft Azure Policy of Azure Resource Manager
- Continue handmatige testen op dynamische clouddreigingen in productie- of preproductieomgevingen
- Sprint testing — „Microtest-campagnes” — voor handmatig testen afgestemd op DevOps releases

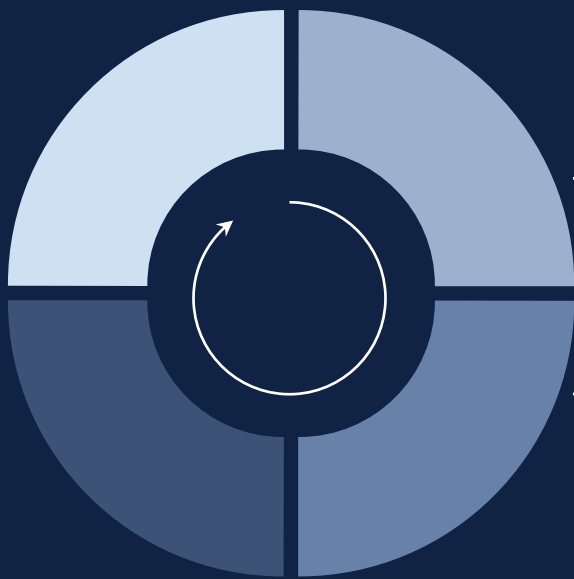
TRANSPARANT

- Microsoft best practices in lijn met uw bedrijfsrisicobereidheid
- Ingebouwde mogelijkheden van het Microsoft Azure Security Center om continu beveiligingseisen te controleren
- Handmatige metriekgebaseerde testgegevens en analyses via Synack Platform voor realtime controle van de dekking

CONFORM

- Microsoft Azure Security Benchmark framework ingezet volgens uw bedrijfs- en conformiteitseisen
- Penetratietests en rapportage afgestemd op industriestandaarden (NIST, CIS, OWASP, PCI en HIPAA)

Microsoft Azure Security Modernization Approach



PLAN

Schets op maat gemaakte controledoelstellingen en risico-eisen - de „Security Baseline” - voor uw Microsoft Azure Platform, Services en Workloads.

ONTWIKKEL

Definieer en codeer geautomatiseerde controles die zijn afgestemd op uw Security Baseline om mee te groeien met uw bedrijf en toekomstige vereisten.

LEVER

Pas een continue werkwijze toe voor controleren en implementeren van code om samenwerking en consistentie van de code te verzekeren.

MEET

Synack om de effectiviteit van de geïmplementeerde beveiligingscontroles te meten en data te leveren aan *Planning* fases via op Microsoft ASM gerichte missiecampagnes en kwetsbaarheidsonderzoek.

Microsoft Consulting Services

Al meer dan 35 jaar zetten wij ons in om de veiligheid van onze producten en diensten te bevorderen, van het helpen van onze klanten en partners om hun activa te beschermen tot het helpen ervoor te zorgen dat hun gegevens veilig en privé blijven. Wij richten ons op beveiliging, identiteit en ecosystemen voor informatiebescherming en maken gebruik van partnerschappen met leveranciers en adviesbureaus over de hele wereld om veranderingen in onze producten en diensten door te voeren, zodat u uw intellectuele eigendommen kunt beschermen.

Meer informatie

Contacteer uw Synack Consulting Services vertegenwoordiger via microsoft@synack.com.

Het Synack Platform

Synack is de enige oplossing met een kant-en-klare Microsoft Azure-integratie voor offensief testen. De integratie maakt continue penetratie en uitgebreide beveiligingstests mogelijk die schaalbaar zijn voor web- en mobiele applicaties, interne en externe netwerken, en door Microsoft Azure beheerde bedrijfsmiddelen met dynamisch toegewezen IP's.

Het Synack Platform maakt gebruik van een elitegroep van wereldwijde onderzoekers in combinatie met eigen technologie voor on-demand testen, controle en transparantie. Wij brengen onze klanten in realtime ruisvrije, bruikbare gegevens:

- Bruikbare kwetsbaarheidsdetails en risicobeoordelingen
- Beveiligingscontrole en tests
- Gegevens en inzichten van onderzoekers
- Scores voor aanvalsbestendigheid
- Opnieuw op aanvraag testen via Patchverificatie
- Aangepaste en uitgebreide rapportage op aanvraag