Microsoft | Synack

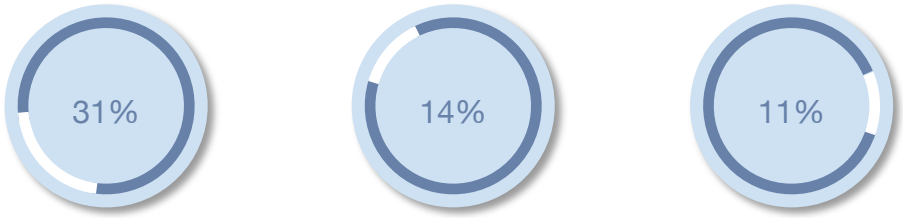
Microsoft Azure Security Modernization

Integriert mit Synack

Cloud Configuration and Security

Im Jahr 2020 beruhten 80% der Datenverstö ße in Clouds auf fehlerhaften Konfigurationen, schlecht verwalteten Anmeldedaten oder auf Datendiebstahl durch Insider (Quelle: Gartner). Die Teams der Sicherheitsabteilungen tragen nicht nur die Verantwortung für die Absicherung der Cloud-Ressourcen, sondern auch für die Organisation von Schulungen zum Thema Sicherheitshygiene und den Rollout von Richtlinien für die Entwickler. Die Zunahme der vom Synack Red Team im Jahr 2020 gemeldeten Sicherheitslücken durch Fehlkonfigurationen der Cloud macht deutlich, dass die vorhandenen Lösungen und Frameworks fragmentarisch sind und böswilligen Absichten viel Spielraum bieten.

Schwachstellen bei Authentifizierungssitzungen, wie unter anderem Standard-Anmeldedaten, Verzeichnisinhalten und Code-Injektionen, machen 40% der von Synack genannten Cloud-Exploits aus.



Standard-Anmeldedaten | Verzeichnisinhalte | Code-Injektion

Microsoft und Synack haben sich zusammengetan, um gemeinsam das erste Framework mit proaktiver End-to-End-Cloud-Sicherheit und einer Testlösung auf den Markt zu bringen.

Microsoft Azure Security Modernization Integriert mit Synack

Durch die Zusammenarbeit der Microsoft Sicherheitsexperten für Microsoft Azure mit den erstklassigen Sicherheitsforschern von Synack entsteht ein effizienter Feedback-Kreislauf, und die Microsoft-Berater können die Sicherheitsdaten von Synack in die Sicherheits- und Entwicklungsprogramme Ihres Unternehmens integrieren. Ausgehend von Ihrer tatsächlichen Angriffsresilienz werden für Microsoft Azure spezifische Verfahren, Richtlinien und Umgebungen konzipiert, entwickelt und angepasst. Die Microsoft Azure Security Modernization (ASM) kann für die Plattform, Dienste und Workloads von Azure ausgelegt und auf Ihre Bedürfnisse zugeschnitten werden, um die Sicherheit nachhaltig zu verbessern.

ERGEBNISSE

INTEGRIERT

- Von Microsoft gelenkte Entwicklung und Verwaltung von Azure-Richtlinien
- Out-of-the-Box Microsoft Azure-Integrationen für Multi-Cloud-Tests im Web, in Infrastrukturen und API-Ressourcen
- Für Microsoft Azure konzipierte, manuelle Testkampagnen
- Integration von Microsoft Azure DevOps Boards, Jira, Splunk und ServiceNow

AGIL

- Skalierbare Sicherheitskontrollen, eingesetzt in Ihrer CI/CD-Pipeline über Microsoft Azure Policy oder Azure Resource Manager
- Kontinuierliche manuelle Tests für dynamische Cloud-Bedrohungen in Produktions- oder Vorproduktionsumgebungen
- Sprint-Tests („Microtest-Kampagnen“) für manuelle Tests, die auf DevOps-Releases abgestimmt sind

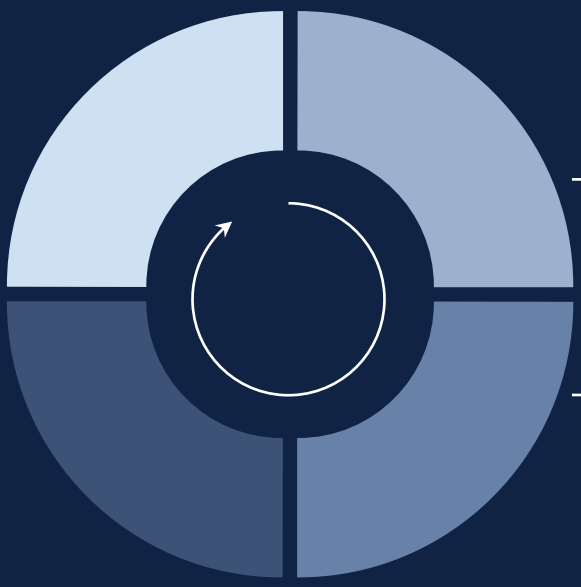
TRANSPARENT

- Best Practices von Microsoft im Einklang mit der Risikobereitschaft Ihres Unternehmens
- Integrierte Microsoft Azure Security Center-Funktionen zur kontinuierlichen
- Prüfung der Sicherheitsanforderungen
- Metriken und Analysen für manuelle Tests über die Synack-Plattform zur Echtzeit-Überprüfung der Abdeckung

REGELKONFORM

- Microsoft Azure Security Benchmark-Framework, das gemäß Ihren Geschäfts- und Compliance-Anforderungen bereitgestellt wird
- Penetrationstests und Berichterstattung gemäß Branchenstandards (NIST, CIS, OWASP, PCI und HIPAA)

Das Konzept der Microsoft Azure Security Modernization



PLANEN

Beschreiben Sie maßgeschneiderte Kontrollziele und Risikoanforderungen (die „Security Baseline“) für Ihre Microsoft Azure Plattform, Services und Workloads.

ENTWICKELN

Definieren und Programmieren Sie automatisierte, auf Ihre Security Baseline abgestimmte Kontrollen, die dem Wachstum des Unternehmens und seinen zukünftigen Anforderungen angepasst werden können.

LIEFERN

Wenden Sie einen kontinuierlichen Workflows für die Prüfung und Bereitstellung von Codes an, um Zusammenarbeit und Code-Konsistenz zu gewährleisten.

MESSEN

Synack misst die Effektivität der angewendeten Sicherheitskontrollen und lässt im Rahmen von gezielten Missionen und Kampagnen des Microsoft ASM und über die Schwachstellenermittlung Daten in die *Planungsphase* einfließen.

Die Synack Plattform

Synack ist die einzige Lösung mit einer betriebsbereiten Microsoft Azure-Integration für offensive Anwendungstests. Die Integration ermöglicht kontinuierliche Penetrations- und offensive Sicherheitstests, die auf Web- und mobile Anwendungen, interne und externe Netzwerke sowie auf von Microsoft Azure verwaltete Ressourcen mit dynamisch zugewiesenen IPs ausgedehnt werden können.

Die Synack-Plattform stützt sich auf eine Riege von Spitzenforschern aus aller Welt sowie auf proprietäre Technologien für On-Demand-Tests, Kontrollen und Transparenz. Wir stellen unseren Kunden rauschfreie, sofort verwertbare Daten in Echtzeit zur Verfügung:

- Einzelheiten zu anfälligen Schwachstellen und Risikobewertungen
- Testen von Sicherheitskontrollen
- Daten und Erkenntnisse von Forschern
- Angriffsresistenz-Scores
- Bedarfsgerechte Testwiederholungen über das Verifizieren von Patches
- Benutzerdefinierte und umfassende Berichterstattung nach Bedarf

Microsoft Consulting Services

Seit mehr als 35 Jahren haben wir uns der Sicherheit unserer Produkte und Dienstleistungen verschrieben: von der Unterstützung unserer Kunden und Partner beim Schutz ihrer Vermögenswerte bis hin zur Gewährleistung der Sicherheit und Vertraulichkeit ihrer Daten. Wir befassen uns vorrangig mit Ökosystemen in den Bereichen Sicherheit, Identität und Informationsschutz und nutzen Partnerschaften mit Anbietern und Beratungsunternehmen weltweit, um Änderungen unserer Produkte und Dienstleistungen voranzutreiben und Ihnen den Schutz Ihres geistigen Kapitals zu ermöglichen.

Weitere Informationen

Kontaktieren Sie Ihren Vertreter für die Synack Consulting Services unter microsoft@synack.com.

Microsoft | Synack