Synack

Member of Microsoft Intelligent Security Association

Microsoft

Synack-Integration mit Microsoft Sentinel beschleunigt den Umgang mit Sicherheitsschwachstellen

Übersicht

Microsoft Sentinel ist eine skalierbare, Cloud-native Einzellösung für intelligente Sicherheitsanalysen, Ereignisverwaltung, Bedrohungserkennung, Sichtbarkeit von Bedrohungen, proaktive Suche und Reaktion auf Bedrohungen.
Es ermöglicht eine frühzeitige Erkennung von Bedrohungen und eine schnelle Reaktion auf raffinierte Angriffe, um die Lösungszeiten zu verkürzen und die Anzahl der Sicherheitsvorfälle in Ihren Microsoft Azure-Cloud-Ressourcen zu reduzieren. Um die Behebungs- und Lösungszeiten noch weiter zu verkürzen, bietet Synack jetzt eine direkte Integration in Microsoft Sentinel, um automatisch Microsoft Sentinel-Events aus Testdaten zu Synack-Schwachstellen zu erstellen.

- Schützen Sie Ihre Microsoft Azure-Cloud, indem Sie die Ergebnisse von Synack-Schwachstellentests mit Microsoft Sentinel synchronisieren
- Neu gefundene Schwachstellen erzeugen automatisch Vorfälle in Microsoft Sentinel, die schnell analysiert und behoben werden können
- Einfache Integration und Konfiguration ermöglichen Ihnen einen schnellen Start
- Anzeigen und Verwalten von Vorfällen in vertrauten Microsoft Sentinel-Bildschirmen

Synack und Microsoft Sentinel arbeiten zusammen, um die Zeit bis zur Lösung zu verkürzen

Microsoft Sentinel vereint zwei Sicherheitstechnologien in einer Lösung: Security Information and Event Management (SEIM) und Security Orchestration Automated Response (SOAR). Es nimmt verschiedene Datenquellen aus dem gesamten Unternehmen auf und führt eine Datenkorrelation zwischen diesen Quellen durch, wobei es intelligente Sicherheitsanalysen und Bedrohungsinformationen nutzt. Mit Microsoft Sentinel kann der Sicherheitsdienst:

- Echtzeit-Warnungen erhalten
- Events mithilfe von maschinellem Lernen und künstlicher Intelligenz (KI) zur Erkennung, Analyse und Identifizierung von Bedrohungen beheben
- Proaktive Suche durchführen

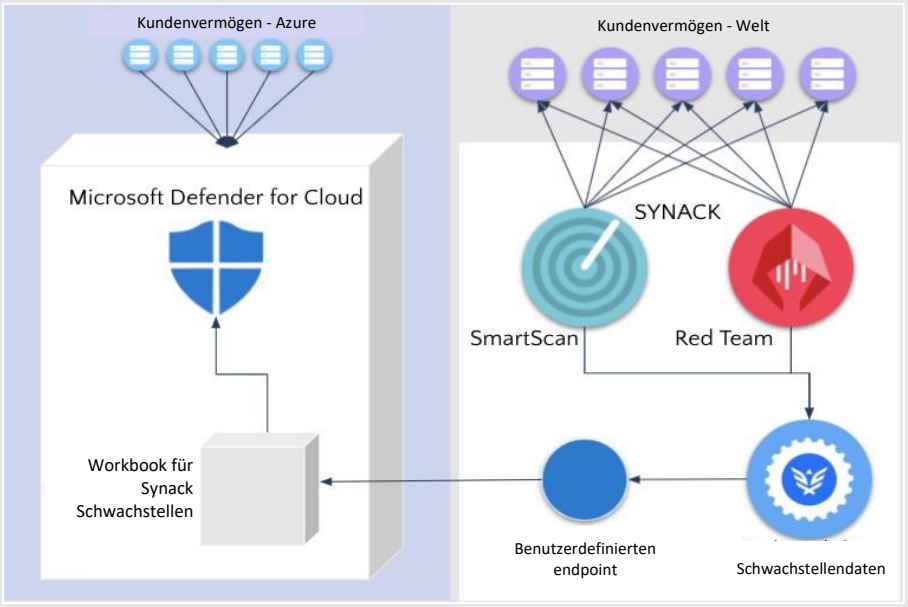
Dadurch erhalten Sicherheitsteams eine ganzheitliche Sichtbarkeit sicherheitsrelevanter Ereignisse und können an einem Ort direkte Einblicke und Analysefunktionen erhalten. Microsoft Sentinel kann mögliche Bedrohungen für die Cloud selbst untersuchen und versuchen, diese zu beseitigen, oder es kann Sie auf potenzielle Bedrohungen aufmerksam machen.

Die schnelle Verwaltung und Behebung von anfälligen Schwachstellen ist der Schlüssel zur Minimierung von Bedrohungen für Ihre Cloud. Synack setzt das weltweit erfahrenste und vertrauenswürdigste Crowd-Sourced Team für Penetrationstest zusammen mit eigener KI-Technologie ein, um eine kontinuierliche oder punktuelle Schwachstellenerkennung durchzuführen. Die Microsoft Sentinel-Lösung von Synack hilft bei der Verkürzung der Lösungszeiten durch die Synchronisierung dieser Ergebnisse mit Microsoft Sentinel.

Die Microsoft Sentinel-Lösung von Synack bietet einen Datenkonnektor, um die Schwachstellendaten von Ihrem Synack-Konto mit Microsoft Sentinel zu synchronisieren. Es erstellt für jede Schwachstelle einen Event in Microsoft Sentinel und hält die Daten zu den Vorfällen mit den neuesten Änderungen der Schwachstelle auf dem neuesten Stand. Es ist kein menschliches Eingreifen erforderlich, um die Informationen zu Schwachstellen an Microsoft Sentinel weiterzuleiten. Microsoft Sentinel kann dann die Synack-Informationen in diesen Vorfällen bei der Bedrohungsanalyse und -verarbeitung verwenden. Außerdem können Sie alles in der Microsoft Sentinel-Umgebung verwalten, mit der Sie bereits vertraut sind.

Leichte Integration

Die Datensynchronisation wird von einer Microsoft Azure-Funktion durchgeführt, die sowohl Synack- als auch Microsoft Sentinel-APIs verwendet, um Synack-Daten zu Microsoft Sentinel zu übertragen. Die Microsoft Sentinel-Lösung von Synack ist über das Microsoft Azure Portal im Visual Studio Marketplace erhältlich. Nach erfolgreicher Installation des Microsoft Sentinel-Datenkollektors beginnt die Synchronisierung sofort. Es ist keine weitere Konfiguration im Microsoft Azure oder Synack Portal notwendig. Wenn alle während der Bereitstellung des Datenkonnektors eingegebenen Parameter korrekt sind, werden neue, von Synack identifizierte Schwachstellen in Microsoft Sentinel als Event angezeigt.



Im Microsoft Sentinel-Vorfallsbildschirm sehen, die Synack-Schwachstellen anzeigen

Sie können auch die Protokolle der bereitgestellten Microsoft Azure-Funktion überprüfen. Jede Synack-Schwachstelle erzeugt einen neuen Event in Microsoft Sentinel. Die Werte der Synack-Felder werden in die Feldbeschreibung im Microsoft Azure Event übernommen. Wenn sich der Status einer Synack-Schwachstelle ändert, wird der Status des entsprechenden Microsoft Sentinel-Events bei der nächsten Synchronisierung entsprechend aktualisiert. In Microsoft Sentinel haben die Events einen der 3 Status: Neu, Aktiv, Geschlossen. Dieser Satz von Status in Microsoft Sentinel ist festgelegt und kann nicht konfiguriert werden. In Synack können Sie eine bestimmte Anzahl von Status haben. Jede von ihnen gehört jedoch zu einer der 3 Hauptkategorien: Neu, Offen, Geschlossen.