Synack

Member of
Microsoft Intelligent
Security Association
Microsoft

Synack Integration with Microsoft Sentinel Speeds Handling of Security Vulnerabilities

Microsoft Sentinel is a scalable, cloud-native single solution for intelligent security analytics, event management, threat detection, threat visibility, proactive hunting and threat response. It helps provide early threat detection and rapid response to sophisticated attacks to facilitate shorter resolution times and a reduction in the volume of security incidents in your Microsoft Azure cloud assets. To help shorten resolution times even further, Synack now provides a direct integration to Microsoft Sentinel for automatically creating Microsoft Sentinel incidents from Synack vulnerability testing data.

- Help protect your Microsoft Azure cloud by syncing results of Synack vulnerability testing to Microsoft Sentinel
- Newly found vulnerabilities automatically create incidents in Microsoft Sentinel for quick analysis and remediation
- Easy integration and configuration allow you to get started fast
- View and manage incidents in familiar Microsoft Sentinel screens

Synack and Microsoft Sentinel work together to speed time to resolution

Microsoft Sentinel combines two security technologies in one solution, security information and event management (SIEM) and security orchestration automated response (SOAR). It takes in different data sources from across the enterprise and performs data correlation across these sources, leveraging intelligent security analytics and threat intelligence. With Microsoft Sentinel, security operations can:

- Receive real-time alerts
- Remediate incidents using machine learning and artificial intelligence (AI) for detection, analysis and identification of threats
- Perform proactive hunting

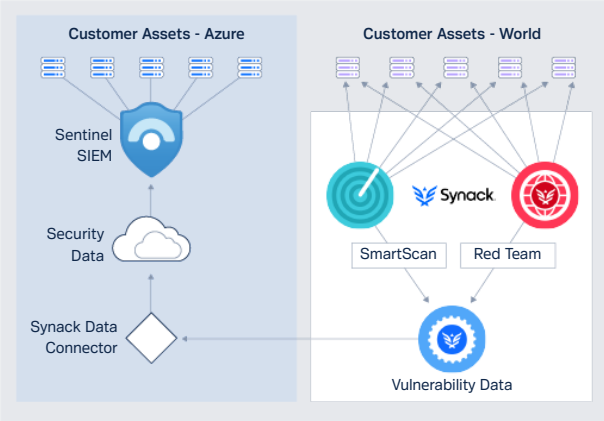
This gives security teams an end-to-end visibility of security related events and helps them get direct insights and analyze capabilities all in one location. Microsoft Sentinel can explore and attempt to deal with possible threats to the cloud on its own or it can alert you to the potential threats.

Quick management and remediation of exploitable vulnerabilities is key to minimizing threats to your cloud. Synack, the premier security testing platform powered by a skilled and trusted community of global security researchers, provides continuous penetration testing and vulnerability discovery with actionable results. Synack's Microsoft Sentinel solution helps in reducing resolution times by syncing these results with Microsoft Sentinel.

Synack's Microsoft Sentinel solution provides a Data Connector to synchronize the vulnerability data from your Synack account to Microsoft Sentinel. It creates an incident in Microsoft Sentinel for each vulnerability and keeps the incident data up-to-date with the latest changes in the vulnerability. There's no need for human intervention to feed the vulnerability information to Microsoft Sentinel. Microsoft Sentinel can then use the Synack information in these incidents in threat analysis and processing. Plus, you can manage it all in the Microsoft Sentinel environment you're already familiar with.

Easy integration

Data synchronization is performed by a Microsoft Azure Function that uses both Synack and Microsoft Sentinel APIs to pull Synack data over to Microsoft Sentinel. Synack's Microsoft Sentinel solution is available from the Microsoft Azure Marketplace. Once you successfully install the Microsoft Sentinel data collector, synchronization starts immediately. No further configuration is necessary in the Microsoft Azure or Synack Platform. Provided all parameters entered during the data connector deployment are correct, you should start seeing new Incidents created in Microsoft Sentinel from Synack vulnerabilities. You can also check the logs of the deployed Microsoft Azure Function.



Microsoft Sentinel incident screen showing Synack vulnerabilities

Each Synack vulnerability will create a new incident in Microsoft Sentinel. The values of Synack fields are pushed to the field description in the Microsoft Azure incident. If the status of a Synack vulnerability changes, the status of the corresponding Microsoft Sentinel incident is updated accordingly on the next synchronization. In Microsoft Sentinel, incidents have one of the three statuses: New, Active or Closed. This set of statuses in Microsoft Sentinel is fixed and cannot be configured. In the Synack Platform, you can have any number of statuses; however, each of them will correlate to one of the three Microsoft Sentinel categories.

Learn More

Contact your Synack/Microsoft Security representative at microsoft@synack.com