Microsoft

Microsoft Graph Security API

Tap into the power of the Microsoft Intelligent Security Graph

Build more intelligent security solutions that integrate and correlate security alerts from multiple sources, unlock contextual data to inform investigations, and automate security operations for greater efficiency.

Overview

The challenge: SecOps developers rely on dozens of different security solutions, each of which have their own alert schema. This means security organizations waste valuable time manually collecting and correlating data across multiple sources. And because these systems operate in silos, SecOps often don't have the ability to remediate problems themselves and must work with system admins and/or other departments to complete remediation tasks.

→ **Deployment challenges** | **Fragmented data** | **Operational complexity**

The solution: The Security API for the Microsoft Graph provides a standard interface and common schema to integrate with security solutions from Microsoft and partners, as well as business context from other Microsoft Graph entities (Office 365, Azure Active Directory, and more).

The Security API provides a single integration point to consolidate and standardize alerts for easier consumption, bring together contextual data to inform investigations, and enable automation for greater security operations efficiency.

- **Unify and standardize alert management.** Consolidate and correlate alerts across security solutions, write code once to integrate alerts from multiple solutions, and keep alert status and assignments in sync.
- **Unlock security context to drive investigation.** Dive deep into related entities (like users, hosts, apps, etc.) and add organizational context from other parts of the Microsoft Graph.
- **Automate security operations for greater efficiency.** Build and execute investigation and remediation runbooks, automate security policy checks and rule enforcement, and orchestrate actions across security solutions.

How can I use the Security API?

Customers, managed service providers, and technology partners can leverage the Security API to build and integrate a variety of applications. Some examples include:

- **Custom security dashboards.** Surface rich alerts in a custom SOC dashboards along with contextual information about related entities.
- **Security operations tools.** Manage alerts in your ticketing, security or IT management system—keep alert status and assignments in sync, automate common tasks.
- **Threat protection solutions.** Correlate alerts and contextual information for improved detections, take action on threats—block an IP on firewall, run AV scan…
- **Other applications.** Add security functionality to non-security applications—HR, financial, healthcare apps…

How does it work?

Part of the Microsoft Graph (graph.microsoft.com), the API provides a standard interface and schema to integrate with security solutions from Microsoft and partners, as well as connect to business context from other Microsoft Graph entities. Build solutions that authenticate once and make a single API call to access or act on security insights from multiple sources. A variety of SDKs and code samples are supported through the Microsoft Graph making it easy to get started.

Partners

The Security API opens up new possibilities for security technology partners to join the Intelligent Security Graph. Using the unified rest API, partners can consume security alerts from the Microsoft Graph as well as contribute their own alerts, context, and expose actions through the Graph. By forming a connected, extended ecosystem of security technologies, Microsoft and partners can deliver better security for customers.

Partners currently using the security API

Anomali integrates with the Security API to correlate alerts from Microsoft Graph with threat intelligence, providing earlier detection and response to cyber threats.

Palo Alto Networks can enrich alerts from Microsoft Graph Security with threat intelligence speeding up detection and prevention of cyberattacks for our shared customers.

PWC uses alerts and context from Microsoft Graph in its Secure Terrain solution to deliver improved visibility and protection.

How do I get started?

- To learn more visit: aka.ms/graphsecurityapi
- Learn about getting started with the API: https://aka.ms/graphsecuritydocs
- Join the discussion group in Microsoft Tech Community: https://aka.ms/graphsecuritycommunity
- StackOverflow: aka.ms/graphsecuritystackoverflow
- Get started with C# samples: https://aka.ms/graphsecurityaspnet
- Get started with Python samples: https://aka.ms/graphsecuritypython

Microsoft