**Frequently Asked questions – Microsoft Graph Security connector**

**What Email address can I send questions to?**

MDREarlyAccessProgram@sophos.comEarlier communications may have used an incorrect email address. All questions can be sent to MDREarlyAccessProgram@sophos.com or posted on the community forum

**When trying to configure the MS Graph Connector I am prompted for my Microsoft account credential, but I get an error that I am not authorized?**

To authorize the connector with Microsoft you need to authenticate with a credential that has privileges in the Microsoft security center. This is not always the same user as the admin or super admin for Sophos Central. You will need someone else in your company with privileges to complete the configuration.



**When I try and configure the Connector nothing happens, what is wrong?**

To configure the MS Graph Connector, you need to be a super admin account in central. As an Admin you can join the EAP but configuration of the connector itself requires super admin rights.

**When does the EAP start?**

The EAP will be open on May 30th. To participate you need an activation key and must be an MTR Advanced account. You can request an activation key by emailing your account License and deployment region to Sophos contacts Contact the product team at mtreap2@sophos.com

**Will an additional license be required?**

The MS Graph Security connector will be available at the end of June for all MTR Advanced customers at no additional charge?

**What does the MS Graph Security connector do and why should I enable it?**

The MS Graph Security Connector allows the Sophos managed security operations team to view data from the MS Graph Security API. Depending on the Microsoft license you have the MS Graph Security API will aggregate detection and alert information from multiple Microsoft and 3rd party systems. With the connector deployed and configured these alerts will be available to the operators for review and triage. The alerts will be used to generate cases for investigation and remediation depending on the severity of the alert and the information will be available during ongoing case investigations for correlation with other alerts already in the data lake.

**Is the severity score available in the MS Graph Security API altered by Sophos?**

MS 'Severity' score are - High, Med, Low, and informational. Sophos do not write back to the MS Security center, so the data is not altered by Sophos.

We have found that the MS Security score is not sufficient to determine if a case is warranted or not. They number of High severity alerts from MS is in the thousands per day for a typical deployment of 5,000 devices so we apply additional correlation and evaluation logic to determine if a case is warranted or not.

During the EAP we will be evaluating the types of alerts generated to determine when a MS Graph Security alert warrants an active case creation and investigation.

**Will the data lake entry have data about which connector the data came in from?**

We will save all data provided in the alert. Most of the alerts are associated to a User or Public/Private IP address that we can use to correlate to a user in our systems or a protected device.

**What happens if you double link to the same account?**

If you create two connectors to the same MS Security Graph account, you will get duplicate alerts in central