OFFICE 365 MONITORING WITH VIGILANTE

Frequently Asked Questions

Technical

1. What data is accessed?

Vigilante accesses the Azure Active Directory Audit Log data. A typical record contains:

- User Details (e.g. email address, names, job title, department)
- Activity (e.g. uploaded file, downloaded file)
- IP Address (of person performing activity)
- User Agent (e.g. Chrome on Windows 10)
- Operation (e.g. email forwarding rules, FileUploaded)
- Detail (e.g. uploaded to Documents library)

Metadata is collected under controlled and restricted access methods preventing view of content of emails or documents.

2. Access to the data

Vigilante is designed for all employees to be trained and engaged in monitoring and triaging threats using its IOC Dashboard. Your management decides on how this is implemented to your employees. However, ingested metadata will only be accessible to Aquta Sciences Data Analysts and your approved personnel.

3. 90-day logs & live feed

Upon authorization during on-boarding Vigilante requires you to enable the following 4 logs:

- Sharepoint
- Exchange
- Audit logs
- Sign-in logs

(https://docs.microsoft.com/en-us/microsoft-365/compliance/turn-audit-log-search-on-or-off)

Vigilante ingests two types of logs:

- 15min live-feed of logs
- 90-day audit log

4. How is data stored?

Vigilante uses the MS Azure infrastructure. All data at rest or in transit is secured to meet required international standards

5. Revoking access later

Removing Vigiante access is simple. Just disable all the apps in your Azure tenant that has been enabled for the data access by Vigilante.