Microsoft: Office 365 Reporting

Microsoft Office 365 (O365) reporting data is email data that provides summary information about the processing of email messages that have passed through the Office 365 system for the organization in the last 30 days. Message trace in the Security & Compliance Center follows email messages as they travel through your Exchange Online organization.

Microsoft O365 reporting data allows you to determine if a message was received, rejected, deferred, or delivered by the service. It also shows what actions were taken on the message before it reached its final status. These logs also provide the following information:

- Message size
- Message ID
- To IP
- From IP
- Date

Configuration

Guidance for onboarding data can be found in the Spunk Documentation, Getting Data In (Splunk Enterprise) or Getting Data In (Splunk Cloud). Refer to the documentation, and note the following:

- Recommended index: mail
- Source type: ms:o365:reporting:messagetrace
- Input type: ms_o365_message_trace
- Add-on or app: Microsoft Office 365 Reporting Add-on for Splunk
- Sizing estimate: There is a large amount of variability in the volume of O365 logs. There are several areas that impact volumes:
  - Subscription type and Workloads (Apps) used
  - Size of organization
  - O365 adoption inside of the organization
  - Kinds of federation / ADsync / ExpressRoute

Message trace events tend to be about 650 bytes each, with multiple events per email. Management logs tend to be about 1200 bytes each, and Azure Audit logs tend to be north of 3000 bytes each. The best way to size this information is to start ingesting it and then make necessary adjustments.
Validation

Validate the input and confirm the data is being ingested by running the following search:

```
index@mail sourcetype=ms:o365:reporting:messagetrace
```

Application

When your Splunk deployment is ingesting Microsoft O365 Reporting data, you can use the data to achieve the following:

- Managing O365 workloads
- Managing known phishing email addresses
- Detecting lateral movement with Active Directory data