Microsoft Azure

Author: mdecrevoisier
Date: 2021.12.01

Event Hub

Log collection supported with Logstash

- Activity logs
- Active Directory audit logs
- Active Directory sign-ins logs
- Azure Active Directory Domain Services (AADDS)
- Microsoft Defender for Cloud (ex Azure Security Center / ASC)
  - Cloud security posture management (CSPM)
  - Cloud workload protection (CWP)
  - *Source: https://docs.microsoft.com/en-us/azure/security-center/defender-for-cloud-introduction*
- Microsoft 365 Defender
  - Defender for Endpoint (ex Defender ATP / MDATP)
  - Defender for Office 365
    - Exchange Online Protection EOP)
  - Defender for Identity (ex Azure Advanced Threat Protection / Azure ATP)
  - Defender for Cloud Apps (ex Microsoft Cloud App Security / MCAS)
  - *Source: https://docs.microsoft.com/en-us/microsoft-365/security/defender/microsoft-365-defender*

Log analytics

Used for storage by Microsoft Sentinel (SIEM)

API

- Office 365 Service Communications API
- Azure Sentinel Management API
- Microsoft Defender for Endpoint API
- Microsoft Defender 365 Streaming API (forward to Event Hub or Azure Storage)
- Microsoft Graph API

Log collection supported with Filebeat

- Office 365 Management Activity API
  - Azure Active Directory
  - Exchange
    - Admin
    - Mailbox
    - Quarantaine
  - SharePoint (includes OneDrive)
  - General
    - Security and Compliance
      - Security & Compliance Center Alerts
      - Office 365 alerts from Cloud App Security
    - Defender for Office 365
      - Defender for Office 365 alerts
      - Threat Investigation and Response events
    - Office 365 automated investigation and response (AIR)
    - [others]
  - Data Loss Protection (DLP)