



Threat Intelligence platform integration with Microsoft Azure File Storage

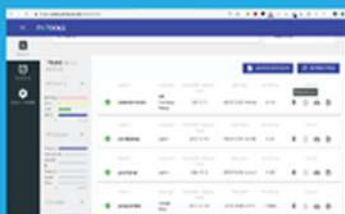


Azure Files

Connector app connects to File storage using the connection string and fetch the files

File storage returns the requested files for the scan

Threat Intelligence Platform



Connector app retrieves the files from the storage, sample it based on predefined sampling techniques, parse the response and sends it to the Customer Platform



Connector App

Connector triggers a call to the connector app to initiate a scan on the File storage



Customer

Customer is a leading Personal Data Privacy and Protection provider.

It enables organizations to discover and map all types of data from all enterprise data sources; automatically classify, correlate, and catalog identity & entity data into profiles; manage and protect enterprise data with advanced data intelligence; and automate data privacy and protection.

It identifies all PII across structured, unstructured, cloud & Big Data.

Customer requested to build a Connector app to integrate their platform with Microsoft File Storage to scan the files present in the File storage for finding the PII information.



Requirement



Technology Solution

- Azure Files offers fully managed cross-platform file shares in the cloud that are accessible via the Server Message Block (SMB) protocol.
- Sacumen developed the Connector app to integrate Azure File Storage using C# 8.0 (.NET Core 3.0). The connector app performs the following actions:
 - › Creates an Azure storage connection string using access key.
 - › Connects to file storage using the connection string
 - › Retrieves and downloads the files from the file storage container.
 - › Samples the fetched data using predefined sampling techniques
 - › Formats the received data in required format and pass it to the customer

