National College of Ireland

Configuration Manual

MSc Research Project
Cyber Security

Harshal Meher
Student ID: X19193521

School of Computing
National College of Ireland

Supervisor: Prof. Vikas Sahni

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Harshal Rajendra Meher
Student ID:	X19193521
Programme:	MSc in Cybersecurity **Year:** 2020-2021
Module:	Industry Internship
Lecturer:	Prof. Vikas Sahni
Submission Due Date:	06/09/2021
Project Title:	Threat Handling using the NIST Framework in a Recruitment Environment
Word Count:	……1047…… **Page Count:** ……10…….……

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Harshal Rajendra Meher

Date: 05/09/2021……

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Harshal Meher
X19193521

1 Introduction

Microsoft Cloud App Security (MCAS) is a security broker which supports various integration methods such as Application connector, reverse proxy, and log collection.[1] The MCAS provides an overview of the network traffic, data travel, and helps in investigating the cybersecurity threats. It acts as a perfect in-house Security Operation Centre (SOC) service for an in-house SOC.

2 Procedure

Steps to connect and set up Microsoft Cloud App Security.

2.1 Connect Apps:

The App Connector in MCAS is connected to Salesforce using REST API. This API helps in retrieving data from the Salesforce platform to MCAS. All the activity and event logs from Salesforce are retrieved with the help of his API and are collected in App Connector or MCAS.

The following steps are followed to connect data management service Salesforce to MCAS.

1. A detected Salesforce account was configured with necessary privileges.
2. Enabled the following features on Salesforce
    - API Enabled
    - View All Data
    - Manage Salesforce CRM Content
    - Manage Users
    - Query All Files
    - Salesforce CRM Content User
3. Added Salesforce application to the App Connector in MCAS

    The activity logs from Salesforce are pulled in the Activity log section of the MCAS and are used to monitor the activities on Salesforce. These logs are then used to generate an alert if any policy match's the activity logs. The screenshot below shows the activity for the Salesforce application.

[1] https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

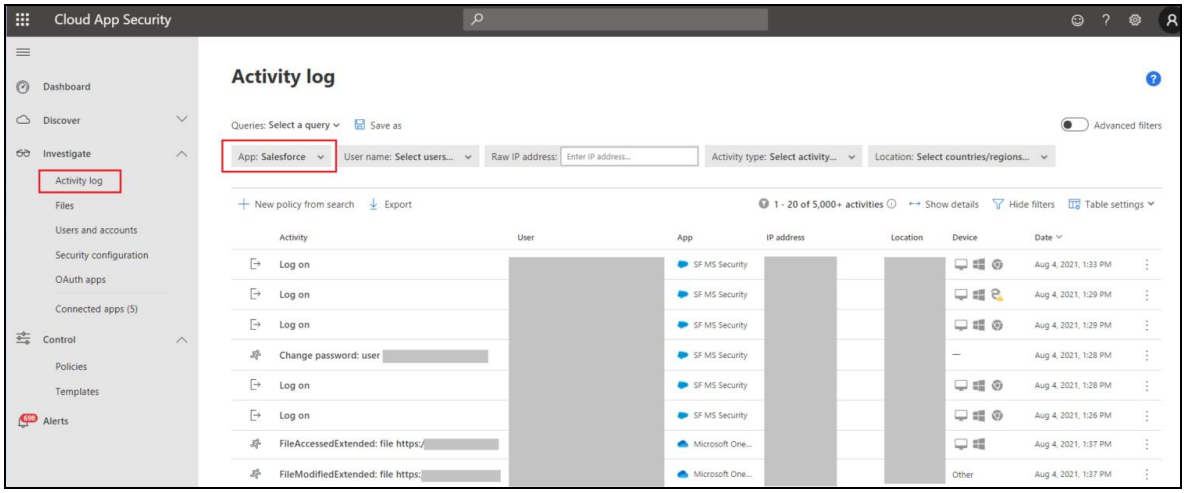


Figure 1: Activity logs

After the successful connection of the app, the group of internal and external domains are segregated. Here the internal domains are the authorized users of the recruitment company and external users are unauthorized users who have limited access like customers. The accounts of the users are configured in the User and accounts section of the MCAS. Also, the authorized domains that should have access to the data of the recruitment company are configured in the organization settings. The range of corporate IP addresses are also added in MCAS to prevent uses from accessing data from unauthorized locations.

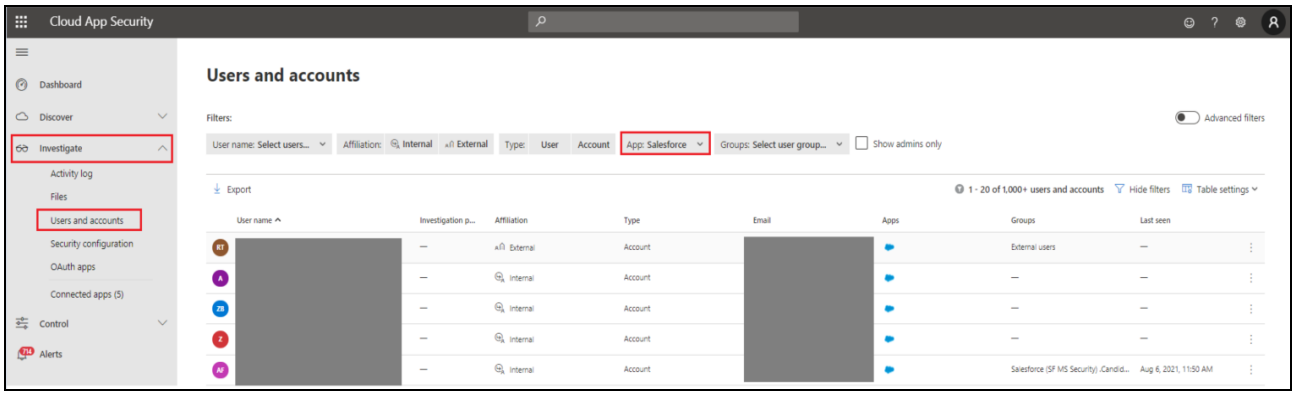


Figure 2: User Configuration

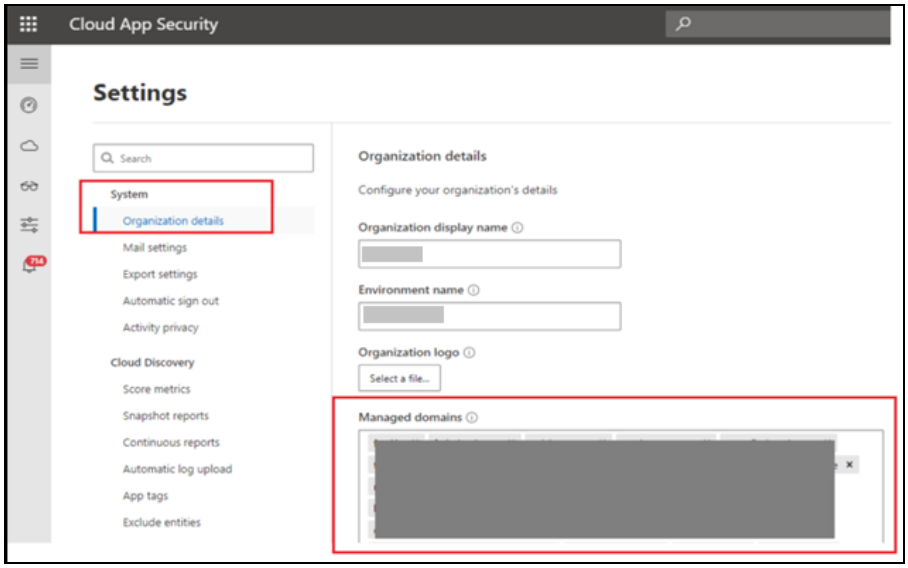


Figure 3: Authorised domain configuration

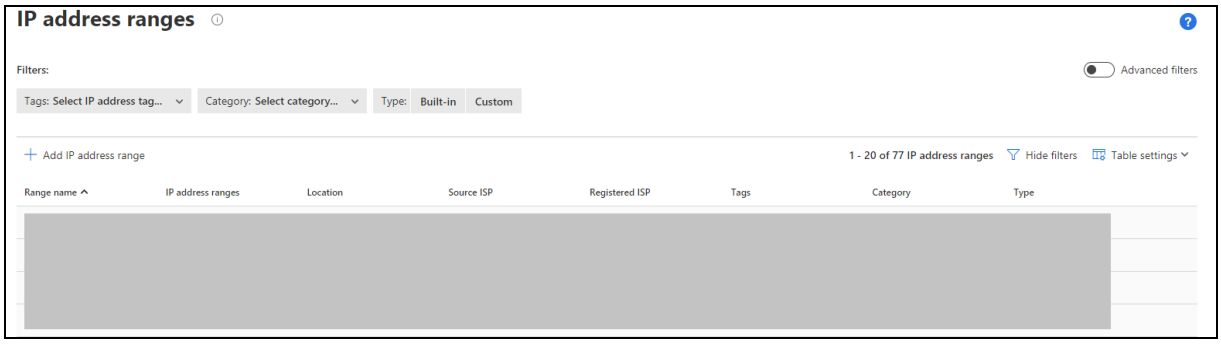


Figure 4: Corporate IP address configuration

2.2 Configure Security Policies

The policies on the MCAS help in identifying suspicious activity, risky events, and violation of rules on the data storage systems like Salesforce. [2] Multiple types of policies like Threat detection policy, Information protection, Conditional access, and Shadow IT policies are configured to analyse activities on the Salesforce. There are about 72 Threat detection policies. Policies configured for the Salesforce application are named by the following prefix as "Salesforce" to identify these policies. These policies contain multiple filters that help to match the activities as required. The filter section in each of these policies has an app selected as Salesforce to limit this policy for the Salesforce application.

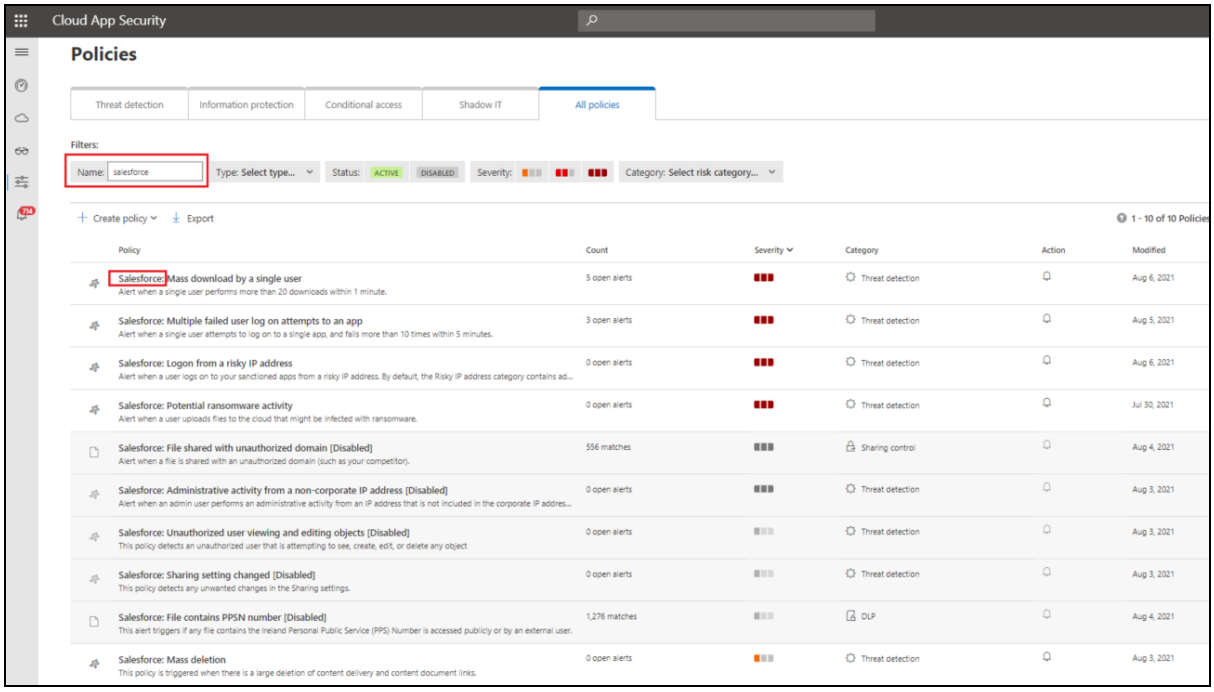


Figure 5: Custom policies configured

The custom policies configured for monitoring events on the Salesforce platform are,

- Logon from a risky IP address: Alert when a user logs on to the Salesforce application for a risky IP address. The database of the risky IP address is managed and maintained by Microsoft.

[2] https://docs.microsoft.com/en-us/cloud-app-security/control-cloud-apps-with-policies

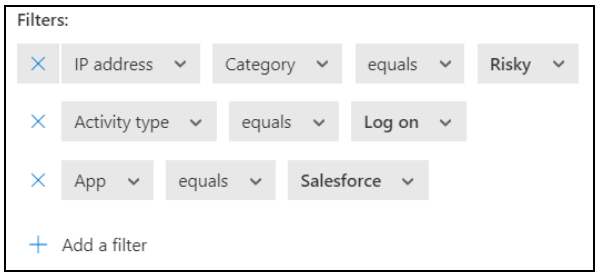


Figure 6: Filters in Logon from a risky IP address policy

- Potential ransomware activity: This policy monitors the environment and sends alerts whenever an event pattern resembling a ransomware attempt is identified.
  Filters:

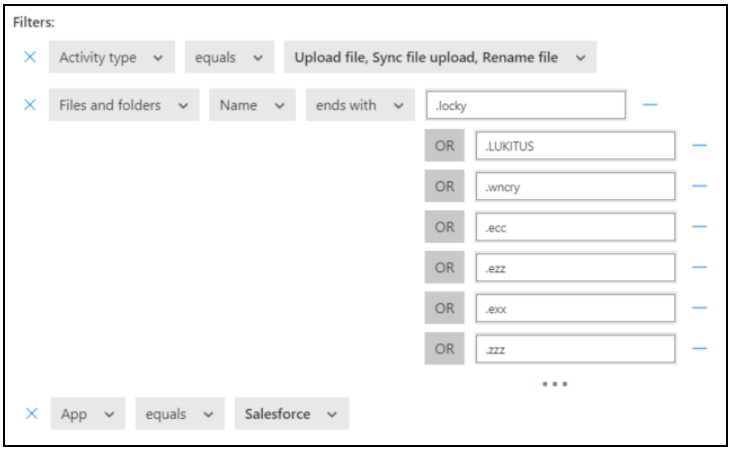


Figure 7: Filters in Potential ransomware activity address policy

- File shared with unauthorized domain contains PPSN number: An alert is triggered if a file containing PPSN number is shared with the unauthorized domain. A list of internal and authorized users is configured in the MCAS.

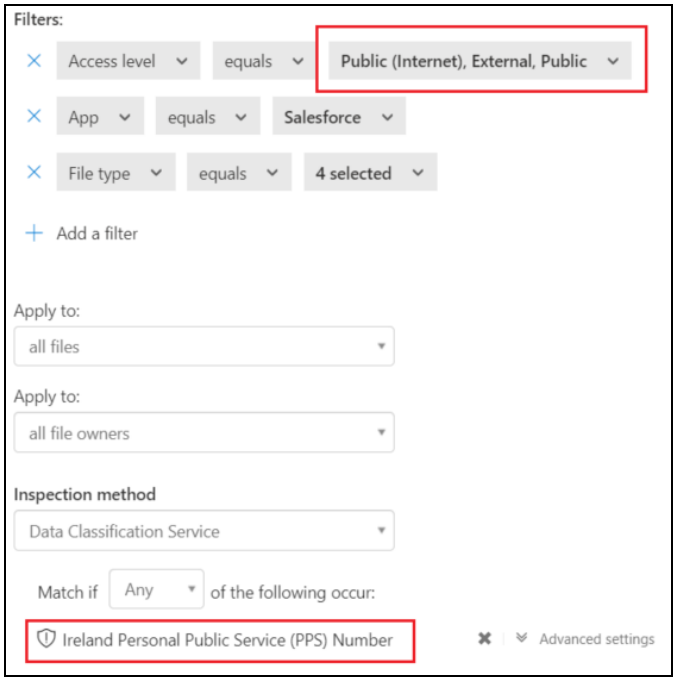


Figure 8: Filters in File shared with unauthorized domain policy

- Multiple failed log-on attempts: This policy generates an alert if an attacker tries to brute-force the Salesforce login.

Figure 9: Filters in Multiple failed log-on attempts policy

- Unauthorized user altering objects: The object configured on the Salesforce platform plays a crucial role in managing data fields. These objects are used to store and manage information on Salesforce. This policy triggers an alert when an unauthorized user tries to edit objects.

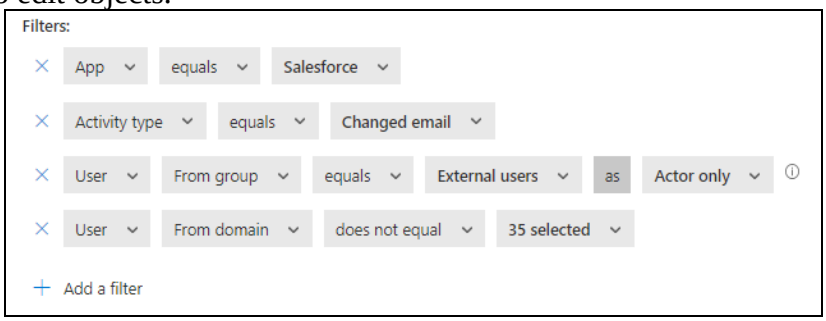


Figure 10: Filters in Unauthorized user altering objects policy

- Mass file downloads: When a single user downloads more than 20 files in one minute, an alert is generated.

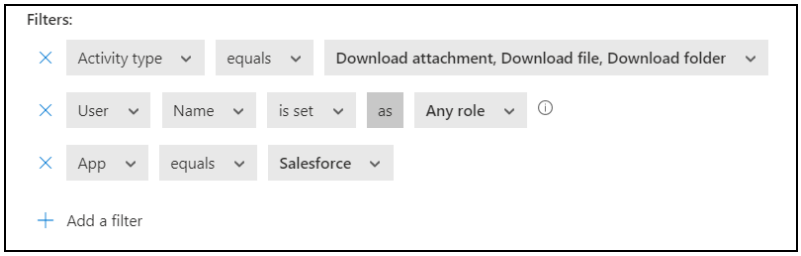


Figure 11: Filters in Mass file downloads policy

- Mass file deletion: When there is a massive deletion of content delivery and content document links, this policy is activated.

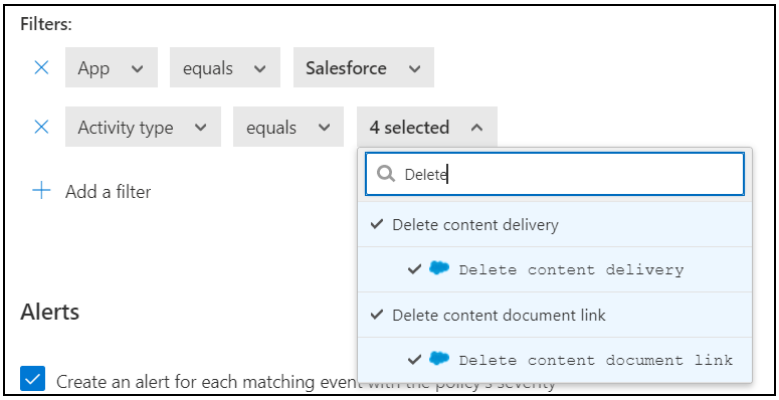


Figure 12: Filters in Mass file deletion policy

- Sharing settings modified on Salesforce: To monitor the administrative activity on the Salesforce platform this policy is configured. This policy monitors the activities performed on sharing settings in Salesforce and an alert is generated if the settings are modified. To avoid the alerts of authorized users like system admin. The system admin account is filtered to avoid unnecessary alerts.

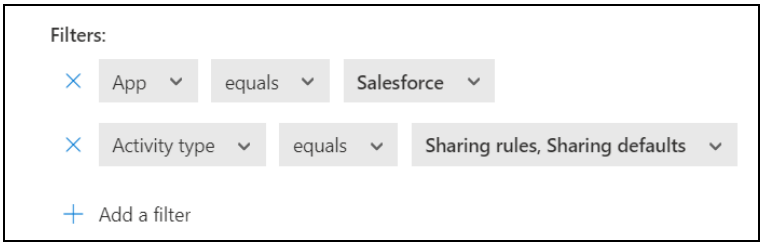


Figure 13: Filters in Sharing settings modified on Salesforce policy

- Organizational activities from a non-corporate IP: The configuration changes are monitored and the locations or IP addresses authorized to do the changes are whitelisted on MCAS. If an administrative activity is observed from non-corporate IP an alert is generated.

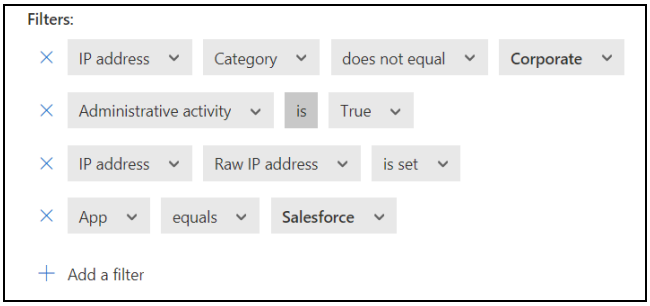


Figure 14: Filters in Organizational activities from a non-corporate IP policy

- Malware detection: Salesforce files are analyzed using Microsoft's threat intelligence engine, and if a file is detected as being associated with malware, an alert is generated.

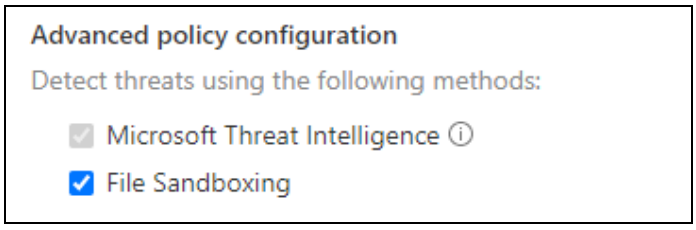


Figure 15: Malware detection policy

- Impossible travel: This policy analyzes the application and sends alerts when the same user actions are identified in various places within a time period less than the estimated travel time between the two locations. This might imply that a distinct user is attempting to use the same credentials. Detecting this abnormal conduct needs a week's learning time during which it understands a new user's activities.

3 Summary

This dashboard offers an overview of the information of the salesforce application. This dashboard provides information on app details, security, and compliance. It also presents the geographical locations from where activities are performed on the Salesforce platform. The Insights tab highlights different file types, file sharing permissions, top users sharing files, and some External collaborators. The alerts and activity logs of the Salesforce application can also be viewed from the same dashboard.

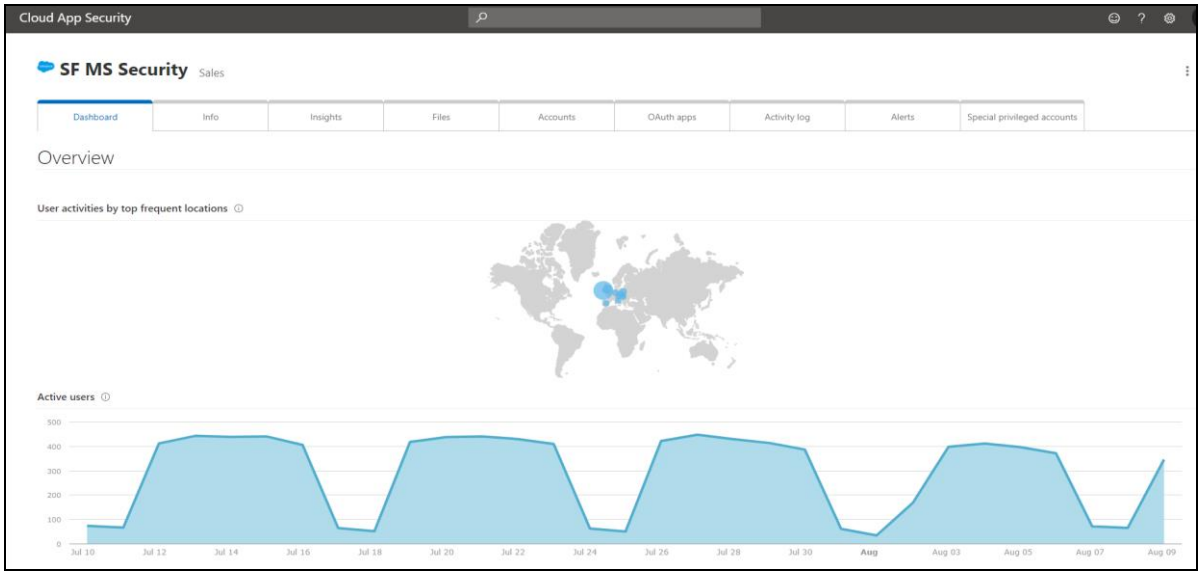


Figure 16: User activity

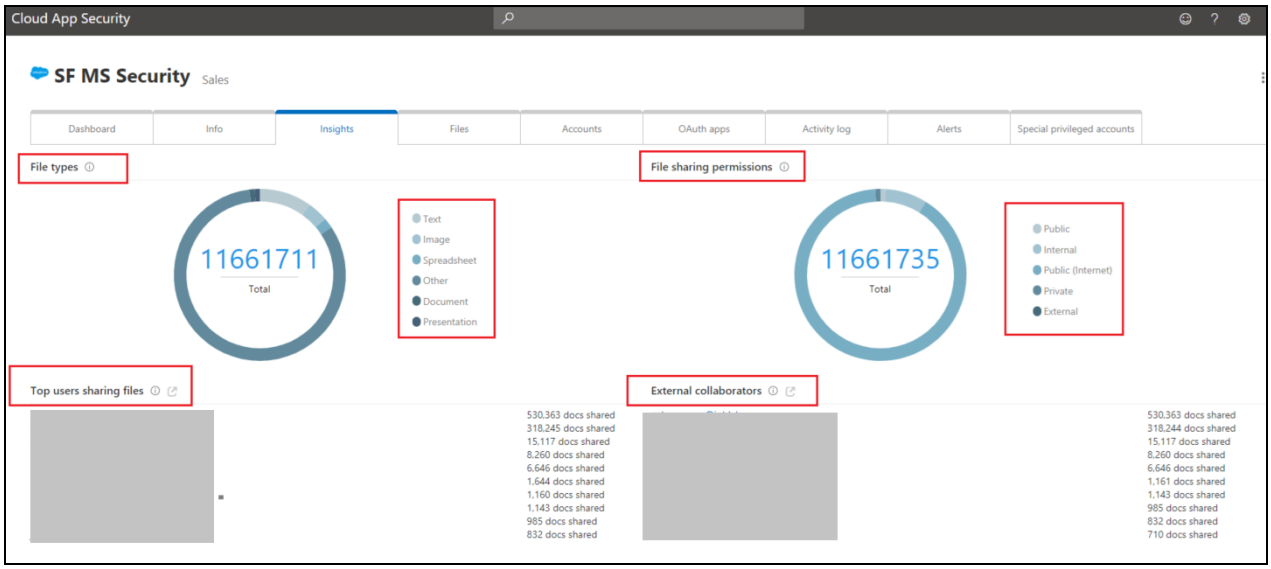
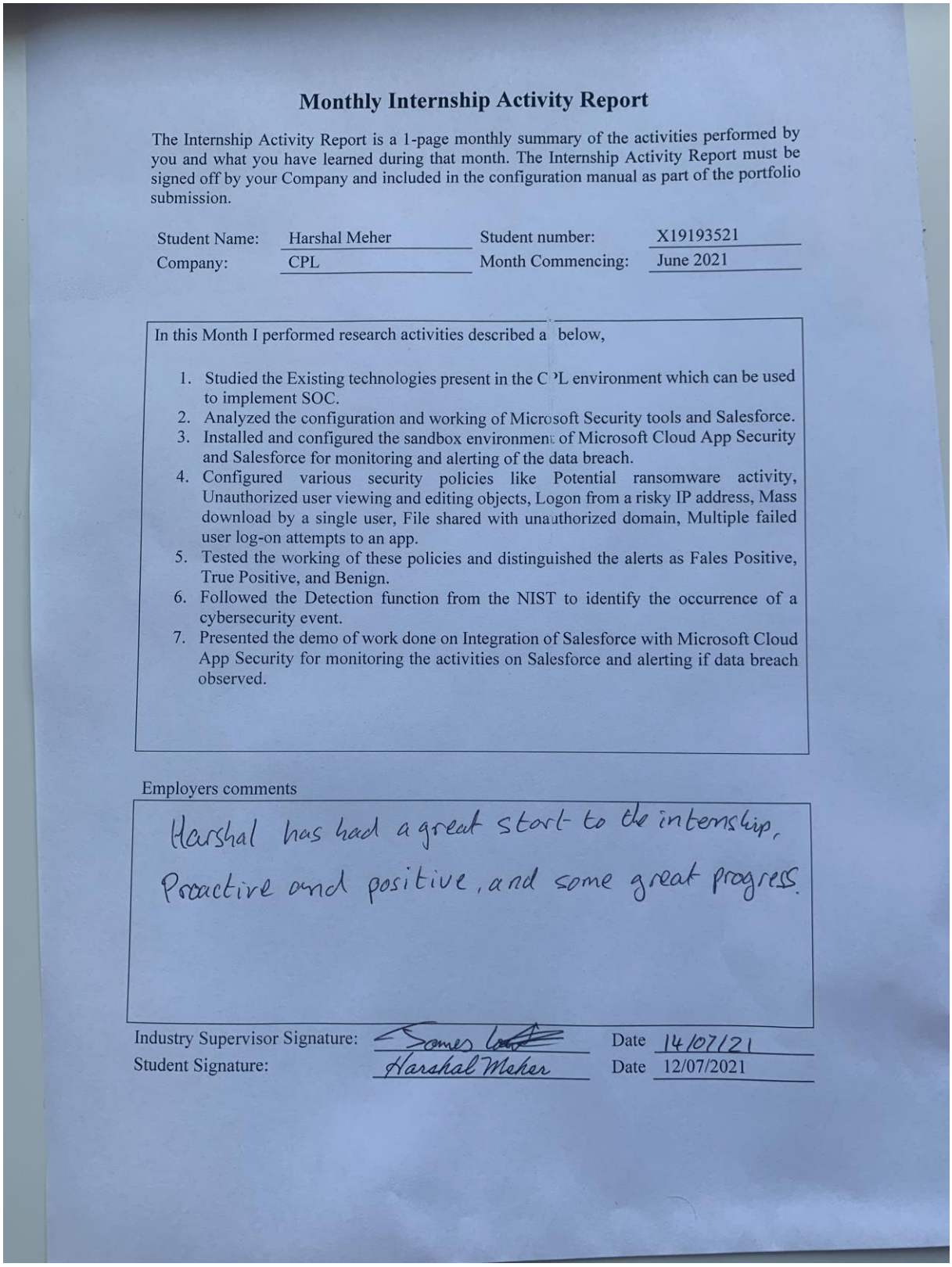


Figure 17: Insights of the File sharing

4 Monthly Internship Activity Report



Monthly Internship Activity Report

The Internship Activity Report is a 1-page monthly summary of the activities performed by you and what you have learned during that month. The Internship Activity Report must be signed off by your Company and included in the configuration manual as part of the portfolio submission.

Student Name:	Harshal Meher	Student number:	X19193521
Company:	CPL	Month Commencing:	June 2021

In this Month I performed research activities described a below,

1. Studied the Existing technologies present in the C PL environment which can be used to implement SOC.
2. Analyzed the configuration and working of Microsoft Security tools and Salesforce.
3. Installed and configured the sandbox environment of Microsoft Cloud App Security and Salesforce for monitoring and alerting of the data breach.
4. Configured various security policies like Potential ransomware activity, Unauthorized user viewing and editing objects, Logon from a risky IP address, Mass download by a single user, File shared with unauthorized domain, Multiple failed user log-on attempts to an app.
5. Tested the working of these policies and distinguished the alerts as Fales Positive, True Positive, and Benign.
6. Followed the Detection function from the NIST to identify the occurrence of a cybersecurity event.
7. Presented the demo of work done on Integration of Salesforce with Microsoft Cloud App Security for monitoring the activities on Salesforce and alerting if data breach observed.

Employers comments

Harshal has had a great start to the internship. Proactive and positive, and some great progress.

Industry Supervisor Signature: [signature] Date 14/07/21

Student Signature: Harshal Meher Date 12/07/2021

Figure 18: Monthly Internship Activity Report