

# **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 Environment	Framework in a Recruitment
Word Count:	<b>1</b> 047 <b>P</b>	age 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.

<u>ALL</u> 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.<sup>1</sup> 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.

<sup>&</sup>lt;sup>1</sup> https://docs.microsoft.com/en-us/cloud-app-security/what-is-cloud-app-security

	Cloud App Security			م		]		© ? ©	8
	Dashboard		Activity log						0
8 D	Discover	~	Queries: Select a query ~ 🔚 Save as					Advanced fil	lters
	Activity log Files		App: Salesforce V User name: Select users.	. V Raw IP address: Enter IP address			① ↔ Show details Y	Hide filters Table settings	~
	Users and accounts Security configuration		Activity [→ Log on	User	App SF MS Security	IP address	Location Device	Date ~ Aug 4, 2021, 1:33 PM	
	OAuth apps Connected apps (5)		[→ Log on		SF MS Security		Q 📾 😪	Aug 4, 2021, 1:29 PM	:
		~	[→ Log on		SF MS Security		□ # ©	Aug 4, 2021, 1:29 PM	:
_	Policies		為 Change password: user	-	SF MS Security		-	Aug 4, 2021, 1:28 PM	:
	Templates		[→ Log on		SF MS Security		₽ 4 0	Aug 4, 2021, 1:28 PM	
<b>(6</b> )	Alerts		[→ Log on		SF MS Security		- 40	Aug 4, 2021, 1:26 PM	
			ぷ。 FileAccessedExtended: file https:/		<ul> <li>Microsoft One</li> </ul>		-	Aug 4, 2021, 1:37 PM	:
			ぷ FileModifiedExtended: file https:		Microsoft One		Other	Aug 4, 2021, 1:37 PM	:

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.

	Cloud App Security			م					۵	? © A
≡ ⊘	Dashboard	Users and accounts								
_	Discover V	Filters: User name: Select users Y Affiliation:	a Internal an External	Type: User Accourt	nt App: Salesforce ~	Groups: Select user group ~	Show admins only		۲	Advanced filters
	Activity log Files Users and accounts		Investigation p	Affiliation	Туре	Email	Apps	I - 20 of 1,000+ users and accounts Groups	Hide filters 😨 Ta	ible settings 🗸
	Security configuration OAuth apps		-	afi External G <sub>a</sub> Internal	Account		•	External users	-	
	Connected apps (5) Control $\checkmark$	0	-	$\ensuremath{\mathfrak{G}}_{\lambda}$ Internal $\ensuremath{\mathfrak{G}}_{\lambda}$ Internal	Account		•	-	-	
(p	Alerts	<b>0</b>	-	$\boldsymbol{\Theta}_{\!\!\boldsymbol{\lambda}}$ internal	Account		•	Salesforce (SF MS Security) .Candid.	Aug 6, 2021, 11:50 A	IM :

Figure 2: User Configuration

	Cloud App Security	R
=		
0	Settings	
$\bigcirc$	Q, Search	Organization details
69	System	Configure your organization's details
<u>→</u>	Organization details	Organization display name 🛈
சூ	Mail settings Export settings Automatic sign out Activity privacy Cloud Discovery	Environment name ()
	Score metrics Snapshot reports Continuous reports Automatic log upload App tags Exclude entities	Select a file_ Managed domains ①

Figure 3: Authorised domain configuration

							_
							Advanced filte
<ul> <li>Category: Select cat</li> </ul>	tegory v Type: Bu	ilt-in Custom					
					1 - 20 of 77 IP address ranges	√ Hide filters	Table settings Y
address ranges	Location	Source ISP	Registered ISP	Tags	Category	Туре	
	address ranges					1 - 20 of 77 IP address ranges	1 - 20 of 77 IP address ranges 🛛 🖓 Hide filters

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. <sup>2</sup> 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.

	Cloud App Security	م				
	Policies					
0	Threat detection Information protection Conditional access Shadow IT A	Il policies				
\$	Filters:					
<b>→</b>	Name: salesforce Type: Select type V Status: ACTIVE DISABLED Severity:	Category: Select risk catego	ry ~			
<u></u>	+ Create policy 👻 🛓 Export				(	1 - 10 of 10 Policies
	Policy	Count	Severity 🗸	Category	Action	Modified
	Salesforce: Mass download by a single user     Alet when a single user performs more than 20 downloads within 1 minute.	5 open alerts	•••	O Threat detection	Ω	Aug 6, 2021
	A Salesforce: Multiple failed user log on attempts to an app Aiert when a single user attempts to log on to a single app, and fails more than 10 times within 5 minutes.	3 open alerts	•••	O Threat detection	Q	Aug 5, 2021
	A Salesforce: Logon from a risky IP address Aiert when a user logs on to your sanctioned apps from a risky IP address. By default, the Risky IP address category contains ad	0 open alerts	•••	C Threat detection	Φ	Aug 6, 2021
	A Salesforce: Potential ransomware activity Alert when a user uploads files to the cloud that might be infected with ransomware.	0 open alerts	•••	① Threat detection	Q	Jul 30, 2021
	Salesforce: File shared with unauthorized domain [Disabled]     Alert when a file is shared with an unauthorized domain (such as your competitor).	556 matches		🛱 Sharing control	Q	Aug 4, 2021
	Salesforce: Administrative activity from a non-corporate IP address [Disabled] Aiet when an administrative activity from an IP address that is not included in the corporate IP addres	0 open alerts	683	C Threat detection	Ф.	Aug 3, 2021
	A Salesforce: Unauthorized user viewing and editing objects [Disabled] This policy detects an unauthorized user that is attempting to see, create, edit, or deiete any object	0 open alerts		C Threat detection	Д	Aug 3, 2021
	과 Salesforce: Sharing setting changed [Disabled] This policy detects any unwanted changes in the Sharing settings.	0 open alerts	<b>E</b> = 1	C Threat detection	Q.	Aug 3, 2021
	Salesforce: File contains PPSN number [Disabled]     This alert triggers if any file contains the ireand Personal Public Service (PPS) Number is accessed publicly or by an external user.	1,276 matches	<b>E</b> = 1	C DLP	Ф.	Aug 4, 2021
	A Salesforce: Mass deletion This policy is triggered when there is a large deletion of content delivery and content document links.	0 open alerts		C Threat detection	Q	Aug 3, 2021

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.

 $<sup>^{2}\</sup> https://docs.microsoft.com/en-us/cloud-app-security/control-cloud-apps-with-policies$ 

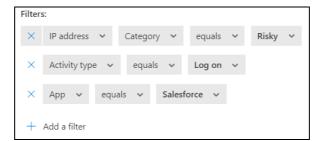


Figure 6: Filters in Logon from a risky IP address policy

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

Filters		
×	Activity type 👻 equals 👻 Upload file, Sync file upload, Rename file 😒	
×	iles and folders v Name v ends with v Jocky	
	OR .LUKITUS	_
	OR .wncry	_
	OR .ecc	_
	OR .ezz	_
	OR .exx ·	_
	OR	_
×	App 🗸 equals 🗸 Salesforce 🗸	

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.

Filter	s:				
×	Access level	✓ equals	∽ Public (I	Internet), Exte	ernal, Public 🗸 🗸
×	App 🖌 e	quals 🗸 S	alesforce v		
×	File type 💙	equals 🗸	4 selected	~	
+	Add a filter				
Apply	v to:				
all f	files		Ŧ		
Apply	v to:				
all f	file owners		Ŧ		
Inspe	ction method				
Dat	a Classification S	ervice	٣		
	atch if Any	▼ of the follo	wing occur:		
M					

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.

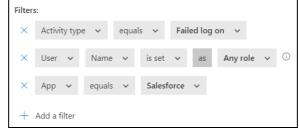


Figure 9: Filters in Multiple failed log-on attempts policy

• 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.

Filters:	
X App V equals V Salesforce V	
× Activity type × equals × Changed email ×	
X User V From group V equals V External users V as Actor only V O	
× User ~ From domain ~ does not equal ~ 35 selected ~	
+ Add a filter	

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.

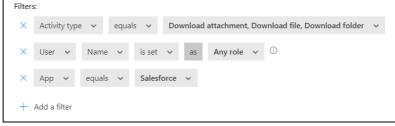


Figure 11: Filters in Mass file downloads policy

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

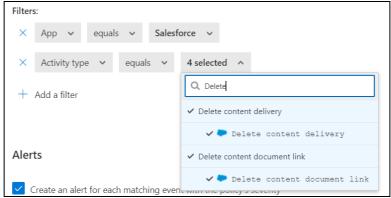


Figure 12: Filters in Mass file deletion policy

• 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.

×	Арр	~	equals	~	Salesf	orce 🗸	
<	Activi	ty type	e 🗸	equals	5 🗸	Sharing	rules, Sharing default

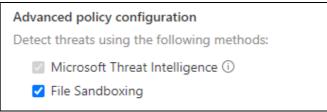
Figure 13: Filters in Sharing settings modified on Salesforce policy

• 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.

Filters	5:
×	IP address 👻 Category 💙 does not equal 👻 Corporate 👻
×	Administrative activity 🗸 is True 🗸
×	IP address 👻 Raw IP address 💙 is set 💙
×	App 🗸 equals 🖌 Salesforce 🗸
+	Add a filter

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.

oud App Security			٩						© ? (
SF MS Secu	rity Sales								
Dashboard	Info	Insights	Files	Accounts	OAuth apps	Activity log	Alerts	Special privileged accounts	
Overview									
User activities by top free	uent locations								
					5	6			
Active users ①				7		, ,			
500									
400									1
200			/						
0 Jul 10 Jul	12 Jul 14	Jul 16 Jul 18	Jul 20	Jul 22 Jul 24	Jul 26 Jul	28 Jul 30	Aug Aug 0	3 Aug 05 Au	g 07 Aug

Figure 16: User activity

Cloud App Security				Q							
🗢 SF MS Secu	rity <sub>Sales</sub>										:
Dashboard	Info	Insights	Files	Accounts	OAuth apps	Activity log	Alerts	Special privileged accounts			
File types 🛈					File sharing permission	ns 🛈					
	11661 Total		<ul> <li>Text</li> <li>Image</li> <li>Spreadsheet</li> <li>Other</li> <li>Document</li> <li>Presentation</li> </ul>	r		1166 Tot		Public Internal Public (Internet) Private External			
Top users sharing files ①	C			530.363 docs shared	External collaborators	00			530.363 do	nos share	ed
				318,245 docs shared 15,117 docs shared 8,260 docs shared 6,646 docs shared 1,644 docs shared 1,160 docs shared 1,143 docs shared 895 docs shared 832 docs shared					318,244 do 15,117 doc 8,260 docs 1,161 docs 1,161 docs 985 docs si 832 docs si 710 docs si	ocs share cs shared s shared s shared s shared s shared shared shared	ed d

Figure 17: Insights of the File sharing

# 4 Monthly Internship Activity Report

you and what you signed off by your submission.	have learned during the Company and included	hat month. The Internship A I in the configuration manual	l as part of the portfolio
Student Name:	Harshal Meher	Student number:	X19193521
Company:	CPL	Month Commencing:	June 2021
In this Month I pe	rformed research activi	ties described a below,	
to impleme 2. Analyzed a 3. Installed a and Salesf 4. Configured Unauthoriz download	ent SOC. the configuration and w nd configured the sand force for monitoring and d various security zed user viewing and ec	present in the C <sup>3</sup> L environm vorking of Microsoft Security box environment of Microsoft a lerting of the data breach. policies like Potential liting objects, Logon from a shared with unauthorized do	y tools and Salesforce. oft Cloud App Security ransomware activity, risky IP address, Mass
<ol> <li>Tested the True Positi</li> <li>Followed to cybersecur</li> <li>Presented to</li> </ol>	ive, and Benign. the Detection function ity event. he demo of work done	cies and distinguished the al from the NIST to identify on Integration of Salesforce activities on Salesforce and	y the occurrence of a with Microsoft Cloud
<ol> <li>Tested the True Positi</li> <li>Followed a cybersecur</li> <li>Presented t App Secur observed.</li> </ol>	working of these polic ive, and Benign. the Detection function ity event. he demo of work done ity for monitoring the s	on Integration of Salesforce activities on Salesforce and	y the occurrence of a e with Microsoft Cloud alerting if data breach
<ol> <li>Tested the True Positi</li> <li>Followed a cybersecur</li> <li>Presented t App Secur observed.</li> </ol>	working of these polic ive, and Benign. the Detection function ity event. he demo of work done ity for monitoring the s	on Integration of Salesforce activities on Salesforce and	y the occurrence of a e with Microsoft Cloud alerting if data breach
<ol> <li>Tested the True Positi</li> <li>Followed a cybersecur</li> <li>Presented t App Secur observed.</li> </ol>	working of these polic ive, and Benign. the Detection function ity event. he demo of work done ity for monitoring the s	on Integration of Salesforce activities on Salesforce and	y the occurrence of a e with Microsoft Cloud alerting if data breach
<ol> <li>Tested the True Positi</li> <li>Followed a cybersecur</li> <li>Presented t App Secur observed.</li> </ol>	working of these polic ive, and Benign. the Detection function ity event. he demo of work done ity for monitoring the s	from the NIST to identify on Integration of Salesforce	y the occurrence of a e with Microsoft Cloud alerting if data breach

Figure 18: Monthly Internship Activity Report