National College of Ireland

Automated Threat Hunting for JavaScript-based Obfuscated Phishing Email Attachments

MSc Industrial Internship
MSc Cyber Security

Saraunsh Shewale
Student ID: X21215057

School of Computing
National College of Ireland

Supervisor:	Vikas Sahni
Industry Mentor:	Colm Gallagher

National College of Ireland
Project Submission Sheet
School of Computing

Student Name:	Saraunsh Shewale
Student ID:	X21215057
Programme:	MSc Cyber Security
Year:	2023-2024
Module:	MSc Industrial Internship
Supervisor:	Vikas Sahni
Submission Due Date:	05/01/2024
Project Title:	Automated Threat Hunting for JavaScript-based Obfuscated Phishing Email Attachments
Word Count:	729
Page Count:	15

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:	Saraunsh Shewale
Date:	29th January 2024

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):	

Automated Threat Hunting for JavaScript-based Obfuscated Phishing Email Attachments

Saraunsh Shewale
X21215057

1 Introduction

This configuration manual details a step-by-step guide to successfully install and set up all required project dependencies to host an automated phishing analysis workflow. The project is configured on a **cloud-based SaaS service** known as **Tines**[1]. It allows the execution of customized automated workflows and generates the output in the form of events. These events appear in JSON notation and can be further parsed according to one's requirements. Parsed output can be delivered through email to a single or list of email recipients.

2 Prerequisites

This project requires the following dependencies to satisfy the pre-requisites criterion for successful installation and execution.

1. A free or paid account subscription to Tines (Smart, secure workflows).
2. API Key for VirusTotal[2]
3. API Key for URLScan.io[3]
4. API Key for EmailRep.io[4]
5. API Key for OpenAI[5]
6. Install Firefox (Version used - 121.0)

   OR

   Chrome Web Browser (Version used - 120.0.6099.130)

[1]https://www.tines.com
[2]https://www.virustotal.com/gui/join-us
[3]https://urlscan.io/user/signup
[4]https://emailrep.io/free
[5]https://platform.openai.com/signup

3 Sign Up for Tines

1. Create a free account on Tines (Smart, secure workflows).
2. Enter the required information and proceed.
3. Once signed up successfully, a unique sign-in link will be shared to the registered email address. Click on the link to verify the account.

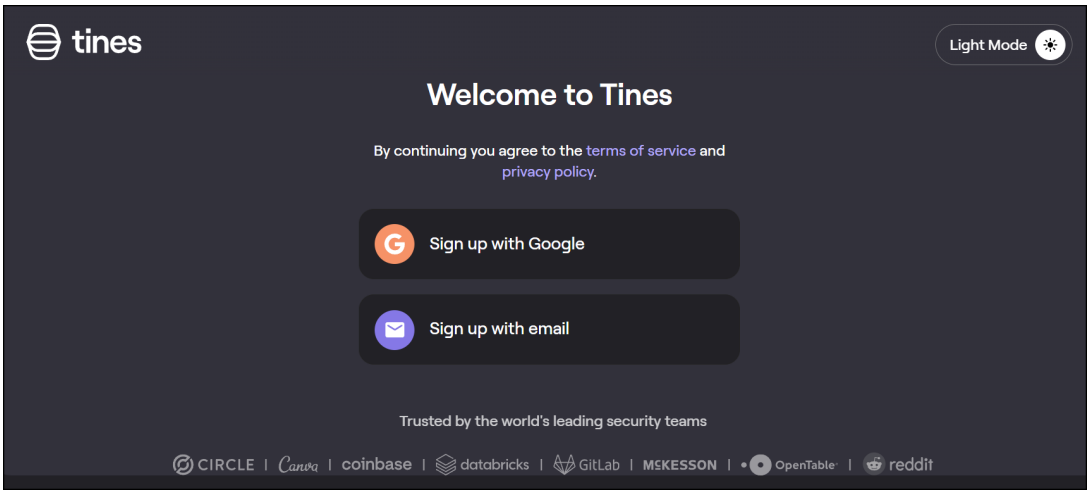

Figure 1: Tines - Account Sign Up

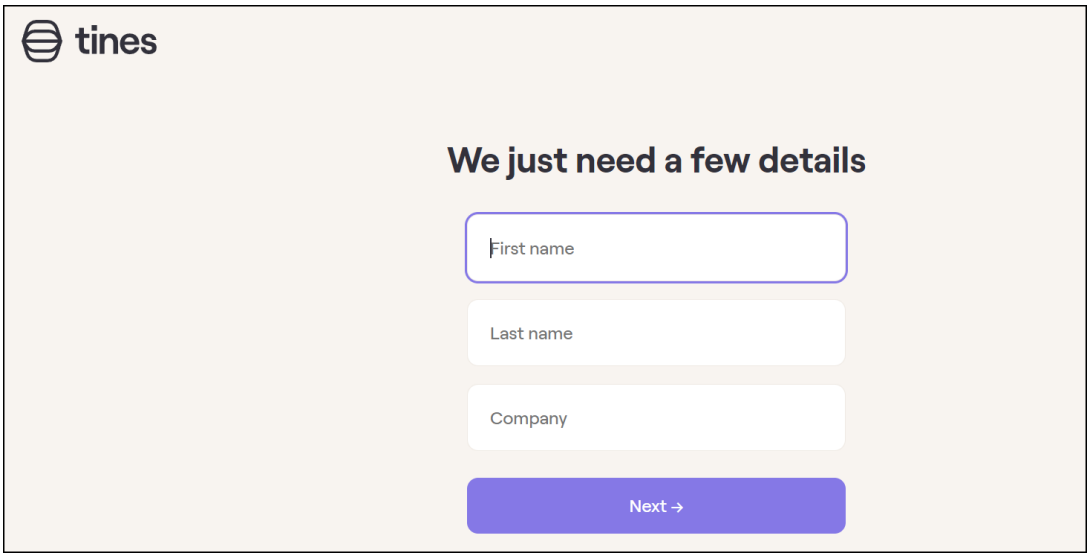

Figure 2: Tines - Provide Required Information

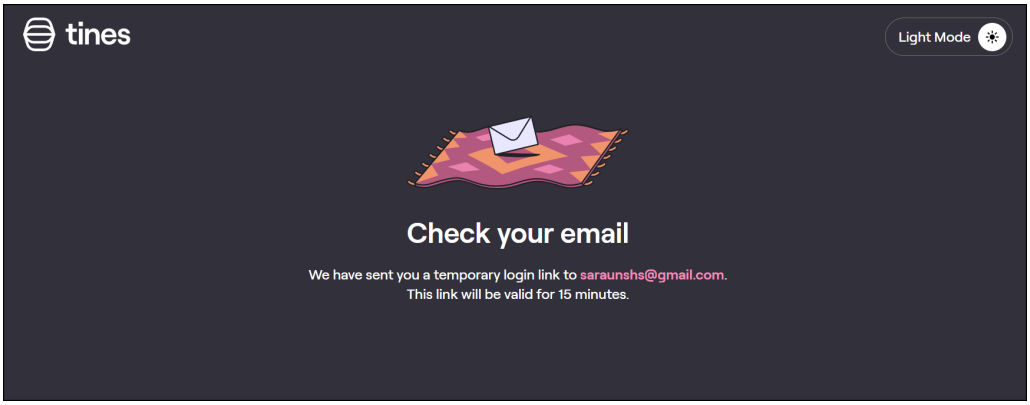

Figure 3: Tines - Verify Email Address

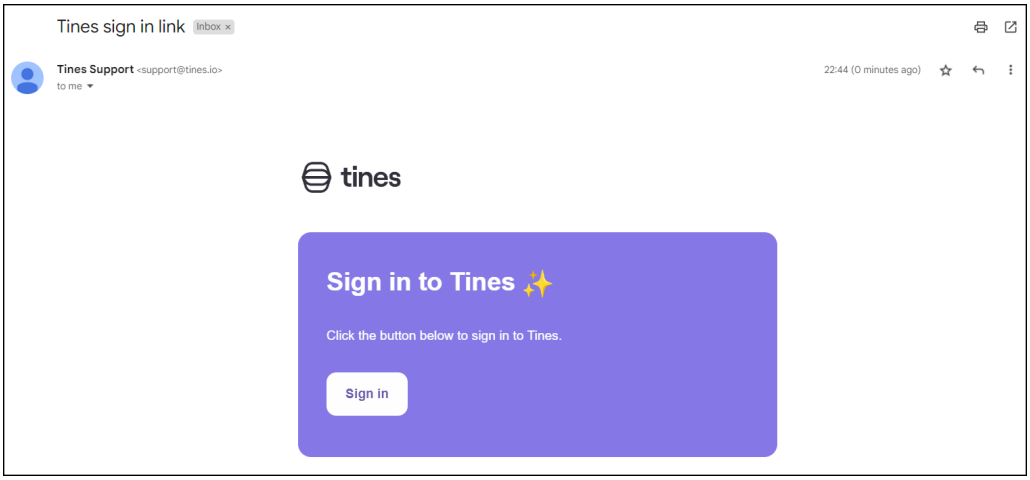

Figure 4: Tines - Account Confirmation

4. After signing in, Tines will redirect the user to the story dashboard.

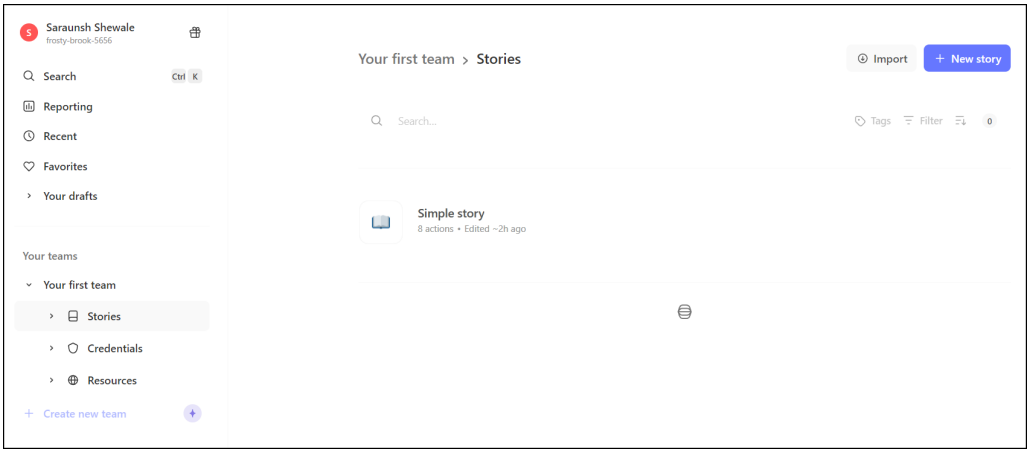

Figure 5: Tines - Story Dashboard

4 Setting up API Keys

4.1 VirusTotal

1. Sign up for a free account on VirusTotal and verify the email address.
2. Go to the Profile section and click on the API key. Save the Key in a safe place as it will be imported at a later stage.

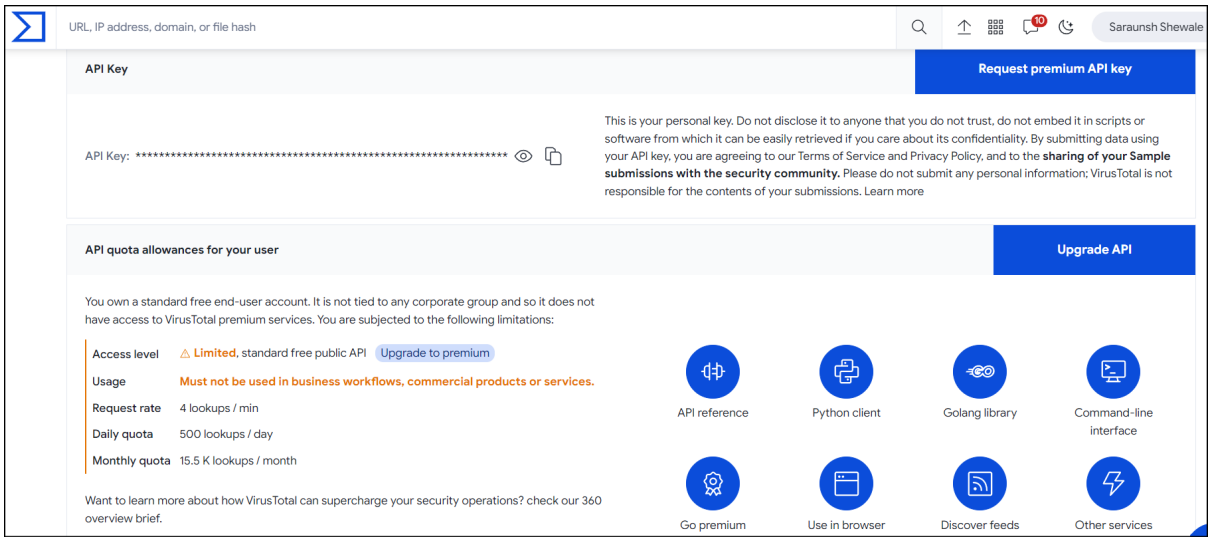

Figure 6: VirusTotal - API Key

4.2 URLScan.io

1. Sign up for a free account on URLScan.io
2. Navigate to Settings & API, and create a new API key with a relevant description.

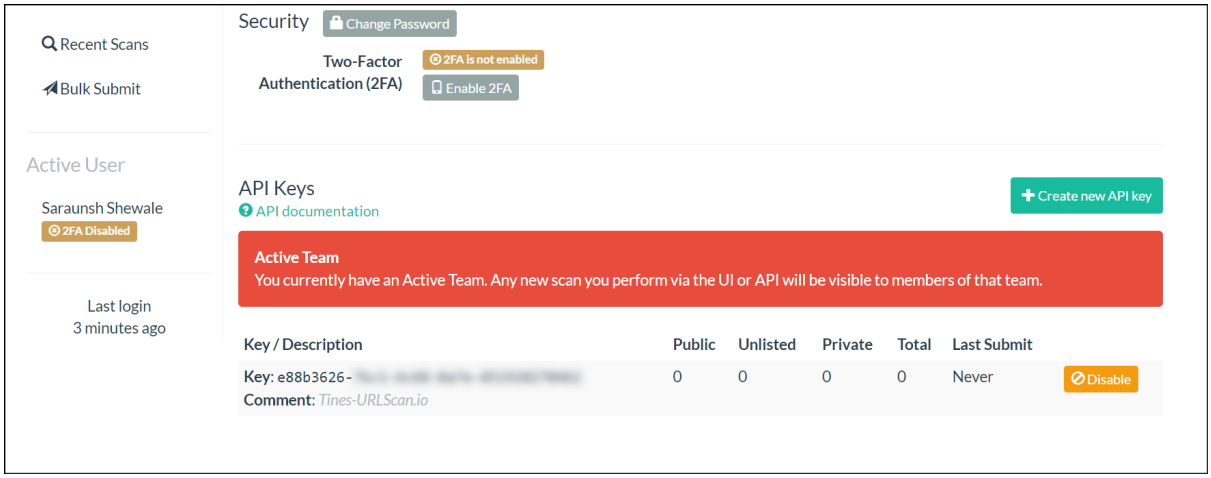

Figure 7: URLScan.io - API Key

4.3 EmailRep.io

1. Request a free or commercial API key from the EmailRep.io support team. (Free plan provides 10 requests/day and the commercial plan has no daily limits.)
2. An API key will be sent to the requested email address in 48 hours.

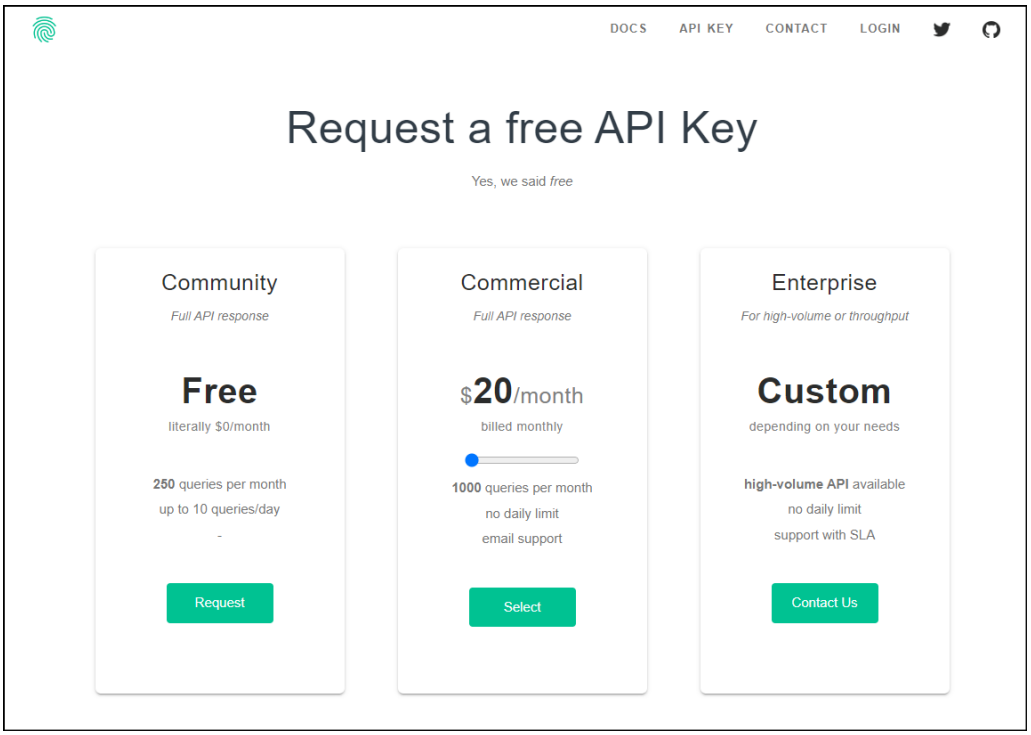

Figure 8: EmailRep.io - API Rate Limits

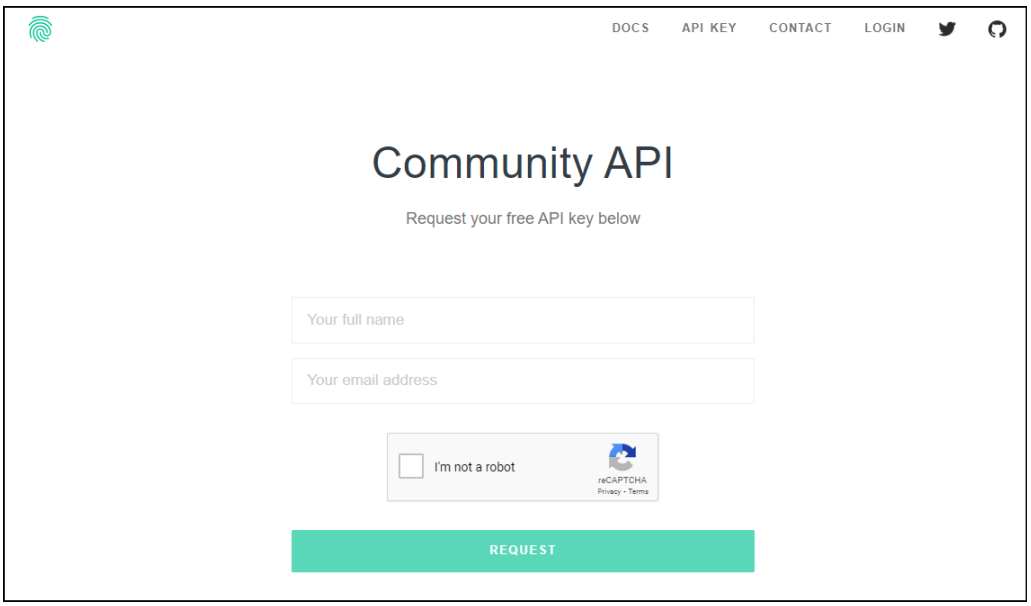

Figure 9: EmailRep.io - Request API Key

4.4 OpenAI API

1. Sign up for an account on OpenAI[6] and verify the email address.

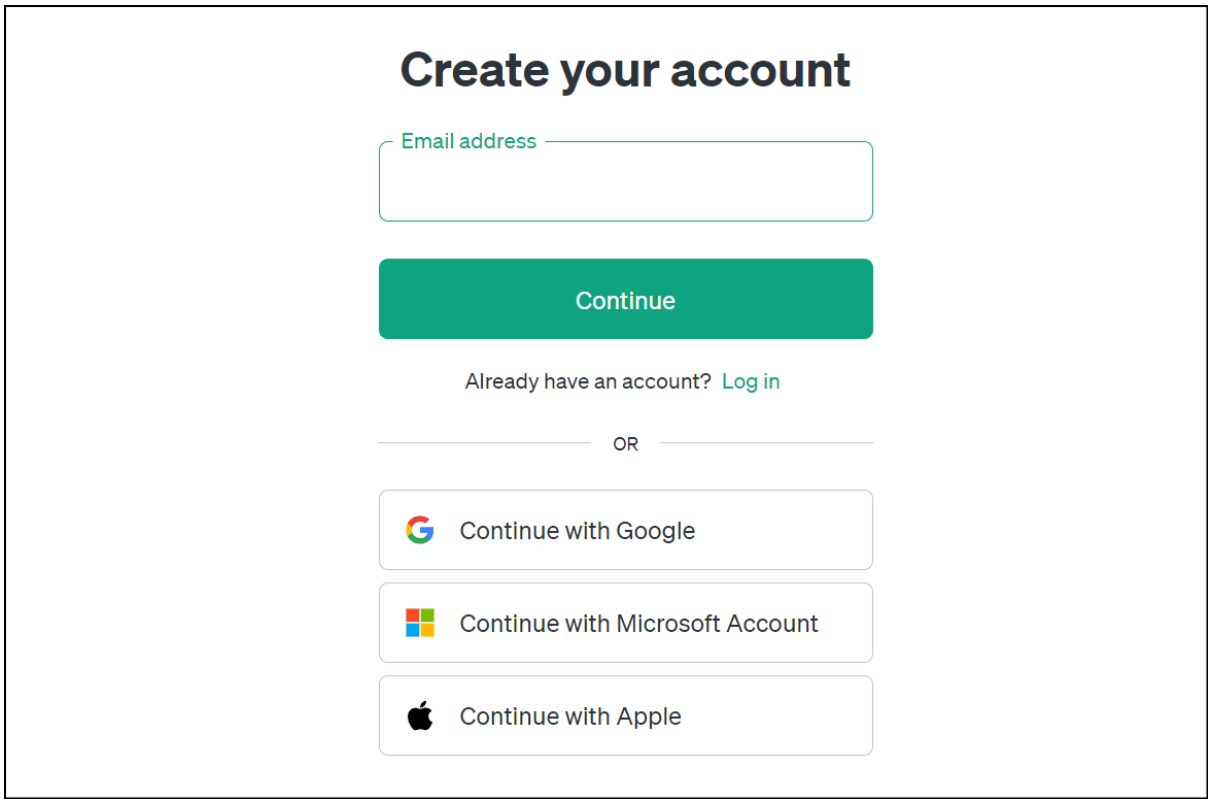

Figure 10: OpenAI - Sign Up

2. Once logged in to the account, navigate to API Keys and add the phone number to be able to create an API key.

3. Once verified, create a new secret key and provide a relevant name.

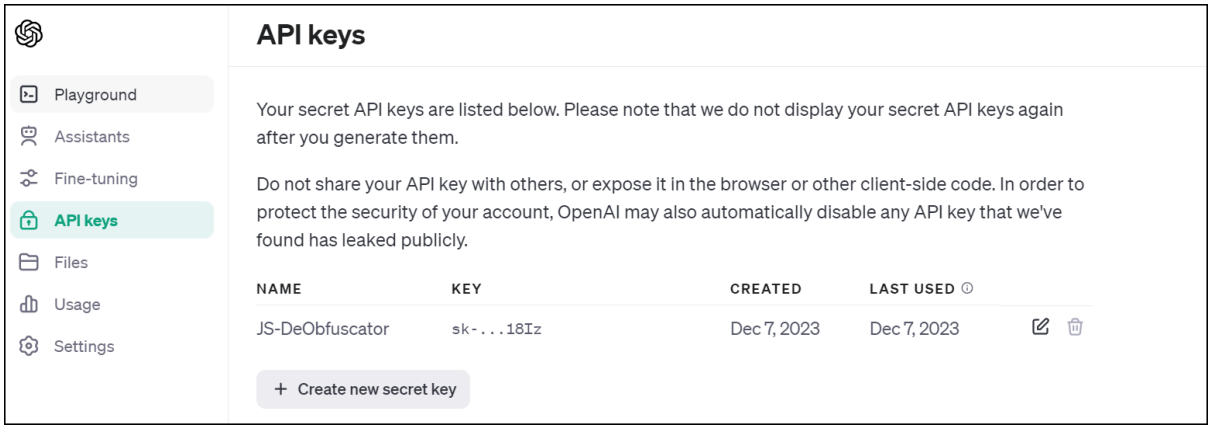

Figure 11: OpenAI - API Key

[6]https://platform.openai.com/signup

5 Import Phishing Analysis Workflow

1. Log in to the Tines account with valid user credentials.
2. Navigate to Stories under Your First Team.

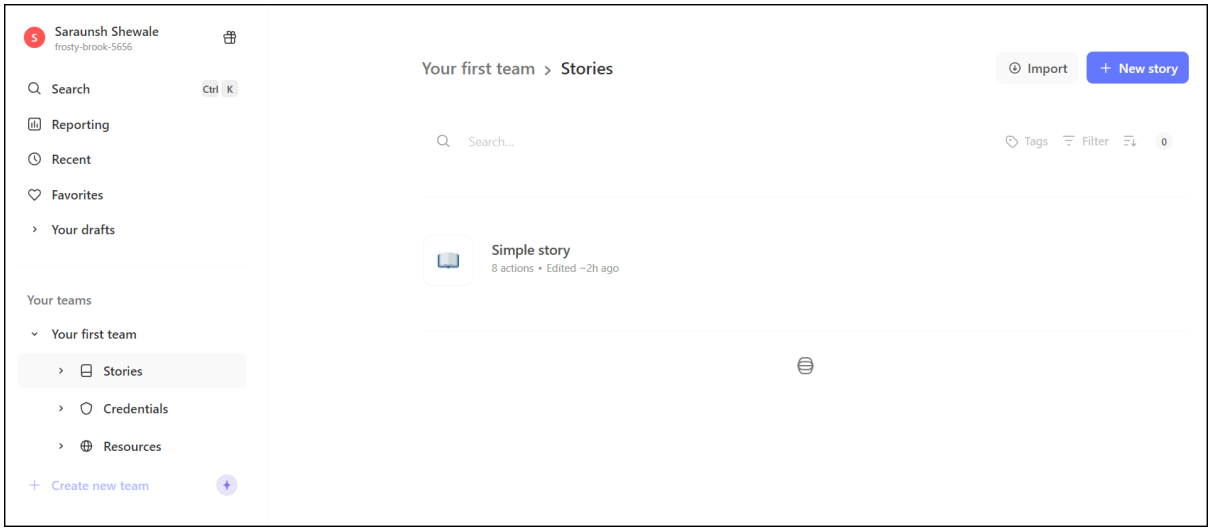

Figure 12: Tines - Story Dashboard

3. Click on the Import button and select the project JSON file (i.e., phishing-analysis-automated-work-flow.json)

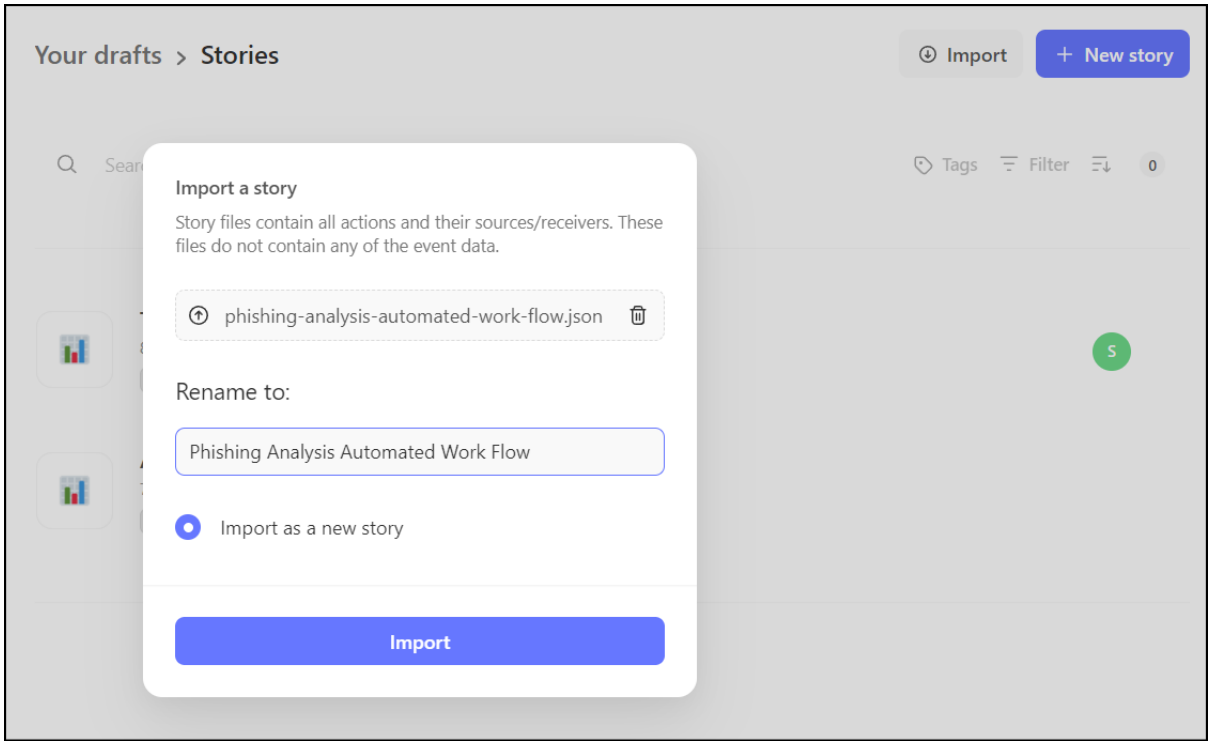

Figure 13: Tines - Import Story

4. After successful import, the user will be redirected to the story workflow where phishing email analysis takes place.

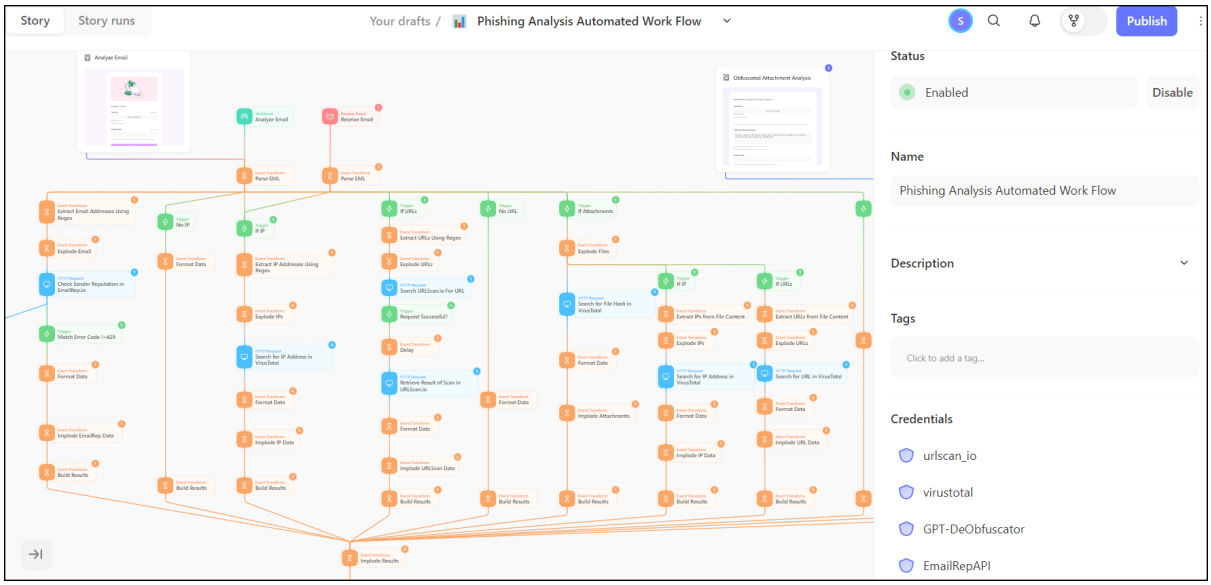

Figure 14: Tines - Story Workflow

6 Importing API Keys

The provisioned API keys must be imported into the Tines platform to allow HTTP request components to access them. To do that, follow the below steps for each of the API keys.

1. Navigate to the Credentials tab from the left sidebar.
2. Click on New Credential and select Text.
3. Provide a relevant name for the API key and description if needed as shown in figure 15
4. Copy the generated API key from section 4 and paste it into the Value field.

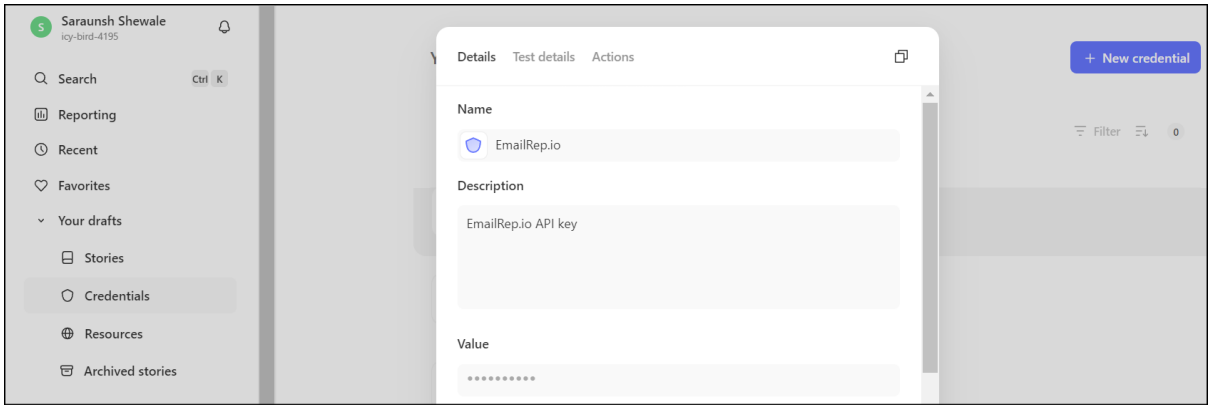

Figure 15: Tines - Import API Key

5. Click on save and the API key will be imported successfully.
6. Follow the same steps for each of the API services.

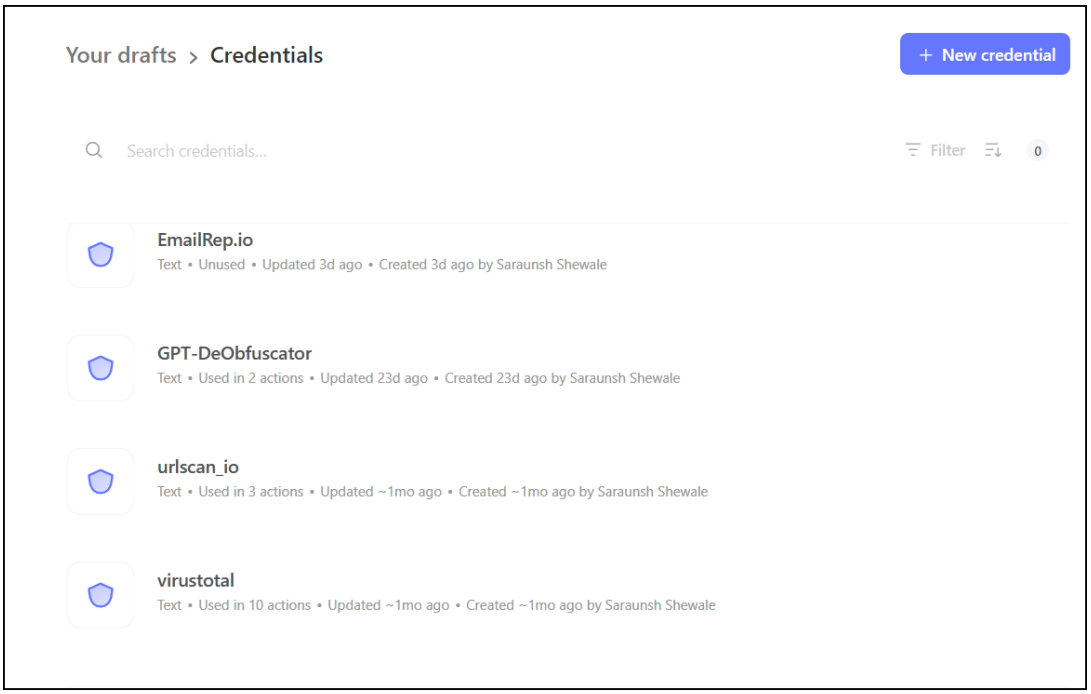

Figure 16: Tines - All API Keys Imported

7 Email Analysis

To initiate the analysis process for suspicious emails, follow the below steps -

1. Navigate to the imported analysis workflow by clicking on the story name under Stories.

Figure 17: Tines - Imported Story

2. Click on Receive Email Action from the storyboard and copy the email address from the right sidebar as highlighted in figure 18.

3. Now forward any suspicious email to the Tines email address for analysis.
4. A detailed analysis report will be sent to the email forwarder in 100 seconds.

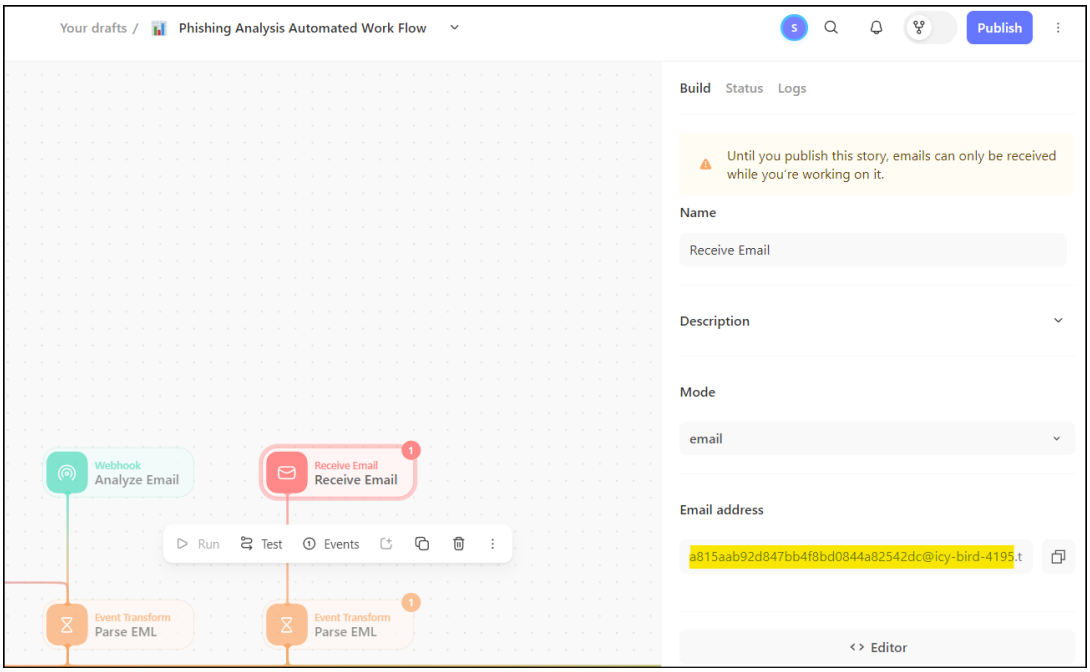

Figure 18: Tines - Receive Email Action

Appendix H – 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: Saraunsh Shewale Student number: x21215057

Company: CommSec Month Commencing: October 2023

This month was spent mostly researching existing literature on threat intelligence, specifically regarding phishing email analysis. Multiple research papers were analysed along with an exploration of various existing open-source projects.

The research methodology was determined for the project development along with the selection of an incremental model of SDLC.

Monitored and escalated alarms as a part of regular security operations (SOC) within the company's defined responsibilities to secure the client's infrastructure.

Employer comments

Student Signature: _____ Date: 02/01/2024

Industry Supervisor Signature: David McNamara Date: 02/01/2024

Appendix H – 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: Saraunsh Shewale Student number: x21215057

Company: CommSec Month Commencing: November 2023

A cloud-based SaaS service - Tines was selected to build automated workflows for phishing email analysis. Also, various online threat intel services were determined and API keys for the same have been provisioned.

Automated workflow for email analysis is designed to cater the email analysis requirements. Integrated IP/URL analysis, and email address analysis checks in the workflow along with static analysis checks using regex.

Performed web application and network pentest for the company's clients as a part of role responsibilities.

Employer comments

Student Signature:  Date: 02/01/2024

Industry Supervisor Signature: David McNamara Date: 02/01/2024

Appendix H – 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: Saraunsh Shewale Student number: x21215057

Company: CommSec Month Commencing: December 2023

The automated analysis workflow was evaluated by testing some sample phishing emails. The outcomes resulted in successful extraction of all associated IOCs from suspicious email.

Along with that regular role responsibilites including SOC operations and web application pentests were performed.

Following security certifications were obtained during internship tenure:

1. Junior Penetration Tester (eJPTv2)
2. CompTIA Security+
3. Tines Certified

Employer comments

Saranush proved himself to be a keen learner with his time with us and was very diligent, with a pleasant demeanour.

Student Signature:  Date: 02/01/2024

Industry Supervisor Signature: David McNamara Date: 02/01/2024