



USER'S MANUAL

Threat Intelligence Platform (TIP) System

Prepared by: Group 18-49

June, 2018

USER'S MANUAL

TABLE OF CONTENTS

| | <u>Page Number</u> |
|---------------------------------------|--------------------|
| 1. GENERAL INFORMATION..... | 1 |
| 1.1 System Overview..... | 1 |
| 1.2 Acronyms and Abbreviations..... | 1 |
| 2. SYSTEM SUMMARY..... | 2 |
| 2.1 System Configuration..... | 2 |
| 2.2 User Access Levels..... | 2 |
| 3. GETTING STARTED..... | 3 |
| 3.1 Setting up TIP..... | 3 |
| 4. USING the TIP system..... | 3 |
| 4.1 Accessing TIP..... | 3 |
| 4.2 Logging in to my TIP account..... | 3 |
| 4.3 Interface overview..... | 5 |
| 4.4 Analysis..... | 6 |
| 4.5 System-Users..... | 7 |
| 4.6 Logs..... | 7 |
| 4.7 Reports..... | 8 |
| 4.8 Notifications..... | 10 |
| 4.9 Settings..... | 11 |

1. GENERAL INFORMATION

1.1 System Overview

Many organizations fail to identify threats ending up spending most of their time on the wrong areas or spend too long on processes, such as risk and vulnerability analysis, instead of mitigating and fixing issues. Making effective use of Cyber threat intelligence is an important component of an organization's security program. Effective use of Cyber threat intelligence (CTI) is an important tool for defending against malicious actors on the Internet.

The threat intelligence platform is a security system that collects malicious feeds from different sources using the help of a tool known as intelmq, and uses these feeds to make sense out of this data through analysis, and visualization to help organizations understand and manage business risk turning unknown threats into known and mitigate threats, and to improve the effectiveness of defense. TIP provides a solution for IT security teams through collecting and processing security feeds and stores the results in mongo database. These feeds are retrieved from the DB for analysis using python and put back for further use. The clients access the analyzed feeds through a defined server component.

1. Acronyms and Abbreviations

TIP - Threat Intelligence Platform. Provides services to the network security.

IP - Internet Protocol. A number address that is unique for every computer on a network.

LAN - Local Area Network. This is a network of computers that are located in close vicinity.

MongoDB - is a free and open-source cross-platform document-oriented database program which stores the malicious feeds.

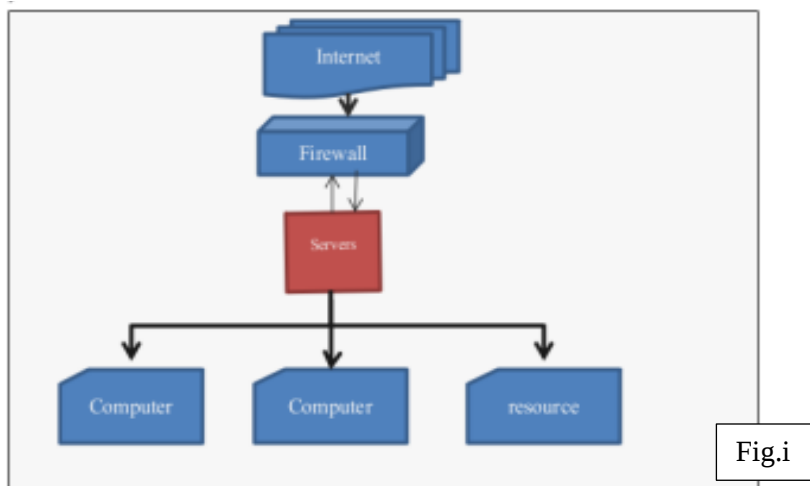
IoCs - Indicator of compromise

TTPs - Tactics, techniques and procedures

2. SYSTEM SUMMARY

2.1 System Configuration

Each employee uses their own computer running any OS. On those computers is the client application that will connect to a central server running the TIP software. All computers must be connected on a LAN with or without outside connection to the internet. This is because sensitive information such as social security numbers among others are being sent across the network.



2.2 User Access Levels

There are two different types of users as depicted in the image above. Admin Users are network security employees who have authority to view and change security information within the database/TIP. User Employees refer to employees who have permission to use the organization's resources, but don't change any of them.

3. GETTING STARTED

3.1 Setting up TIP:

Refer to the installation guide

4. USING THE TIP SYSTEM

4.1 Accessing TIP

Other users don't have any access to TIP since it just protects their computers, only the network security personnel/system admin have access to the it.

This is achieved by accessing it using the specified(custom) domain name for the organization's server or you may either type the IP address of the server.

4.2 Logging in to my TIP account

The network security personnel will get the page shown in Fig 1, which requests him/her to provide the user-name and password which provides access to log into the TIP system.

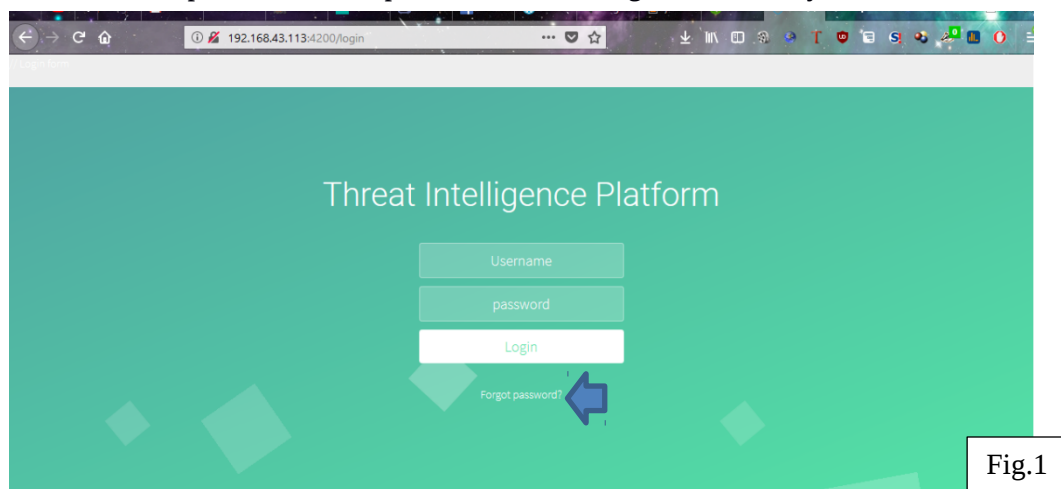


Fig.1

In case you forget the password, click “Forgot Password?” indicated by the blue arrow in Fig.1. Provide your email address which will be used to reset your password as shown in Fig 2.

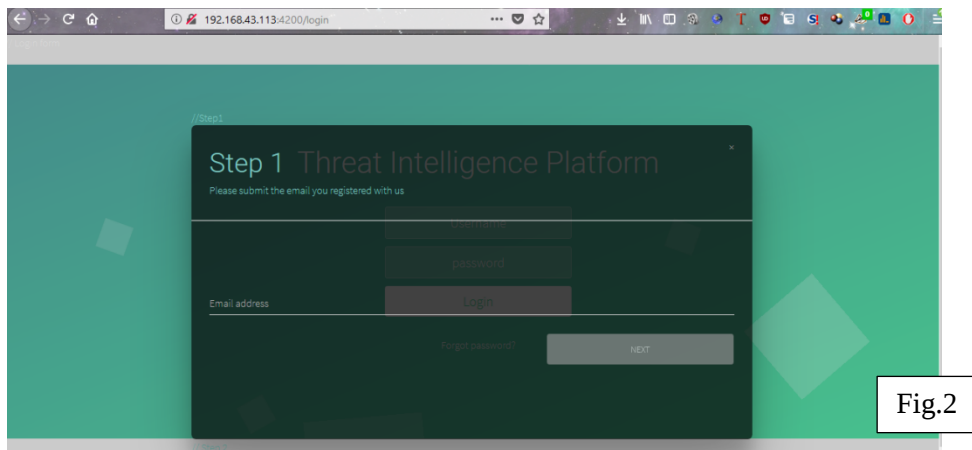




Fig.2

4.3 Interface overview

After logging into TIP, you will see many sections which will be used to perform different actions/operations.

Upper ribbon in Fig 3- On the right hand side, the notification icon  shows the number of notifications in the system and the next icon  show the current user logged in which is also used to log out of the system and viewing the user profile as shown in fig 3.1.

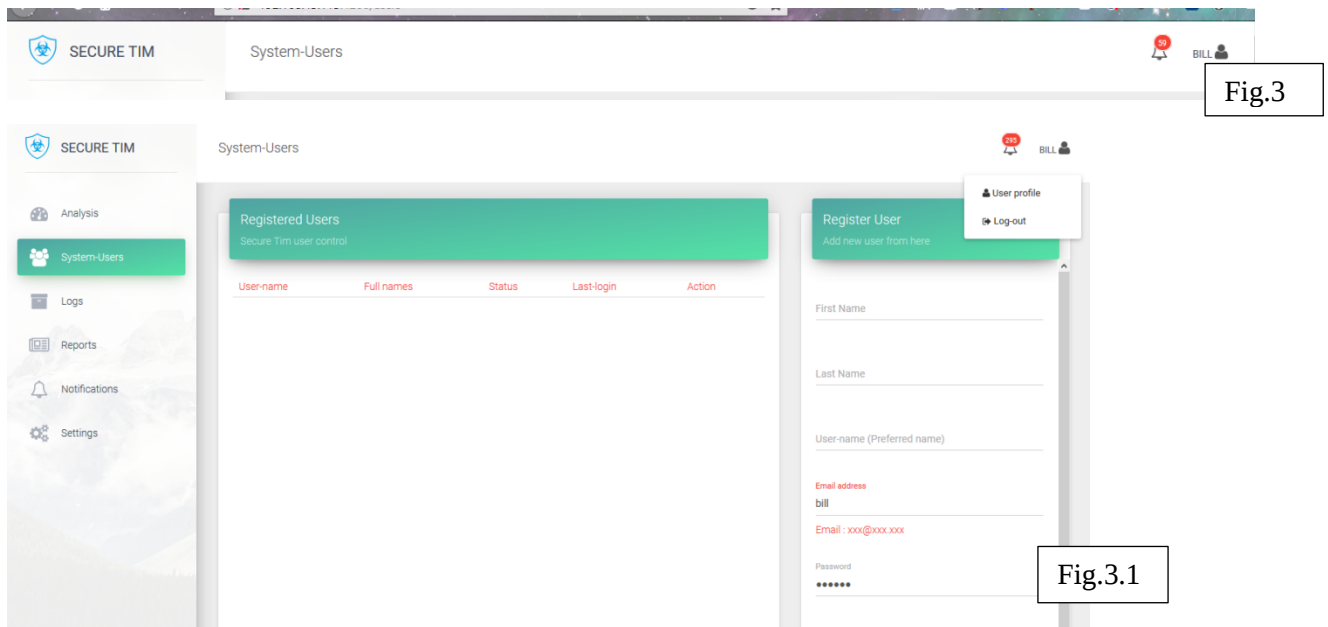
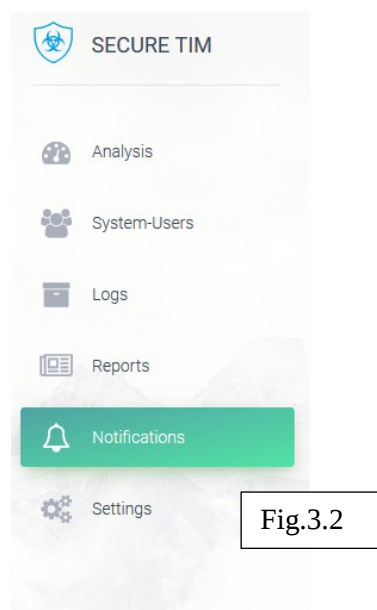


Fig.3

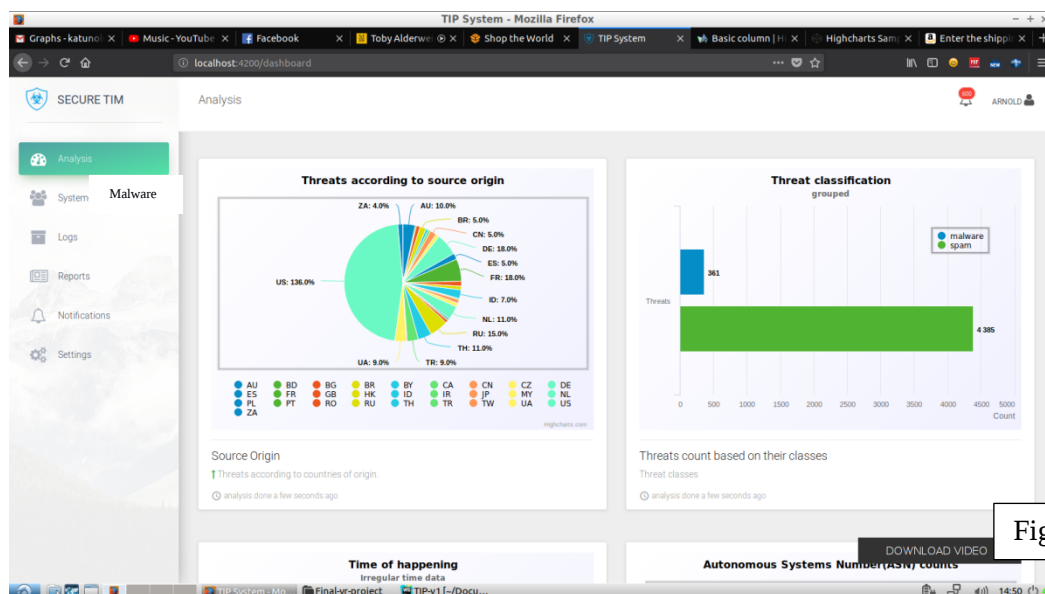
Fig.3.1

The left navigation bar. Its used to access all parts/functions of the system as shown in Fig 3.2.



4.4 Analysis

This region of the system shows you the analysis in graphical form performed on the feeds received from intelmq as shown in Fig 4.



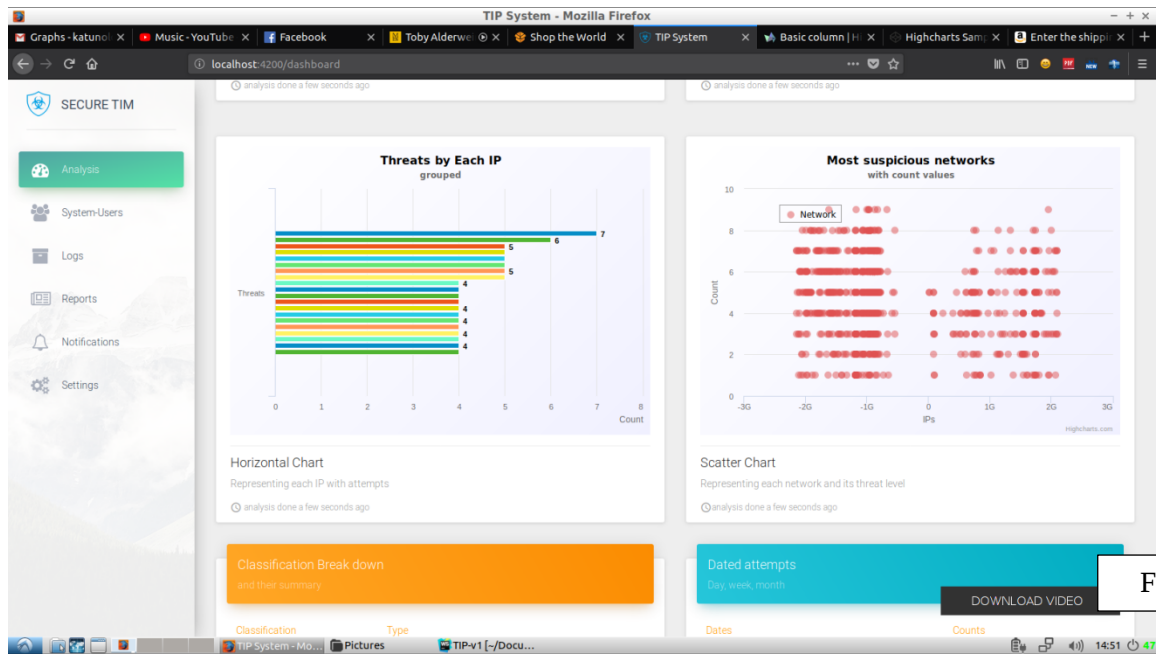


Fig.4.1

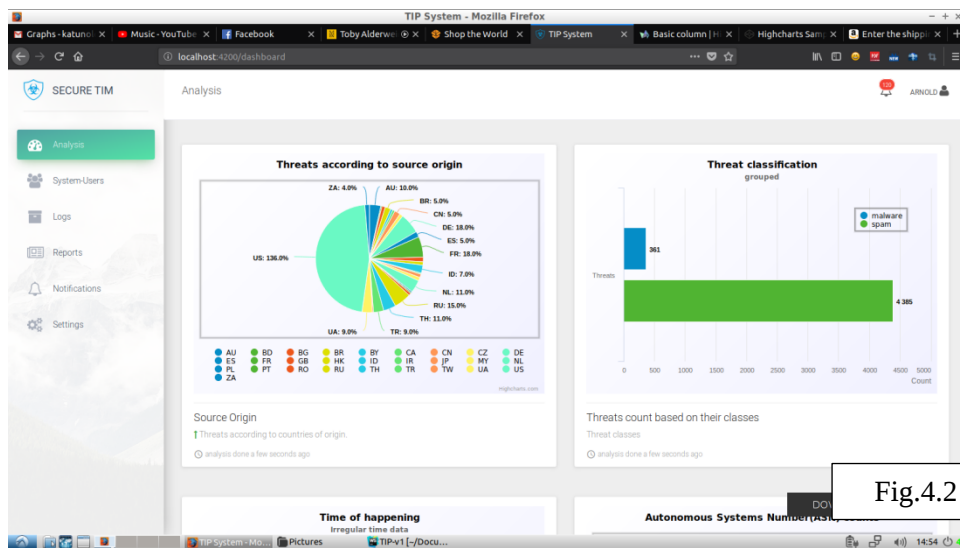



Fig.4.2

4.5 System-Users

 This offers the ability to access and edit system users information as shown in Fig 5.

The icons indicated by these icons   edit, activate and deactivate an account respectively.

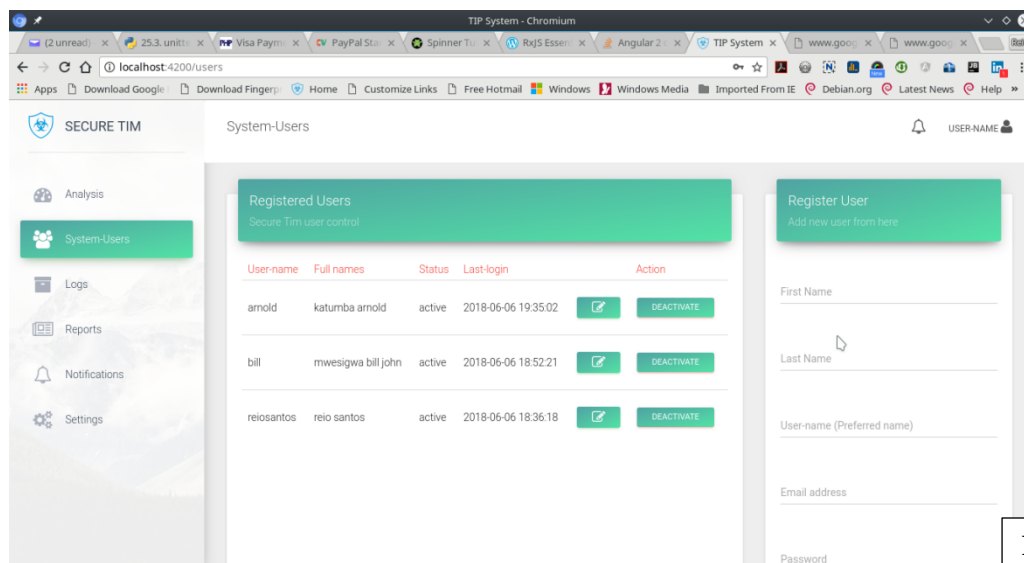


Fig.5

4.6 Logs

This helps you view all the system(the left section) and user access (the right section) Logs as show in Fig 6 , which can be filtered as shown in Fig6.1.

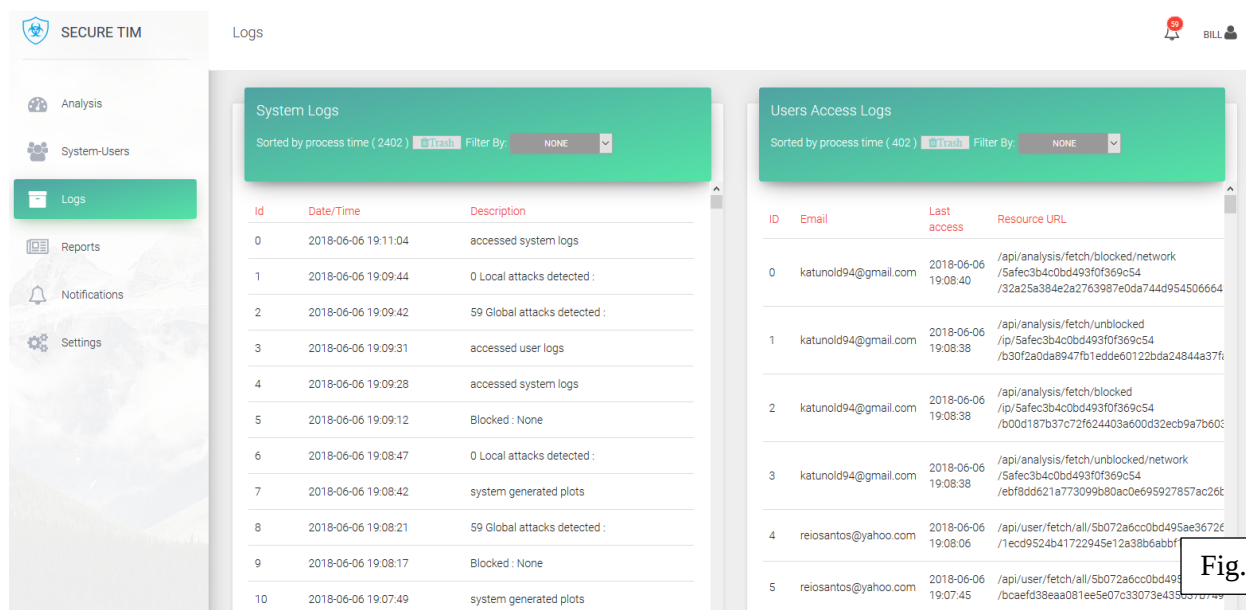


Fig.6

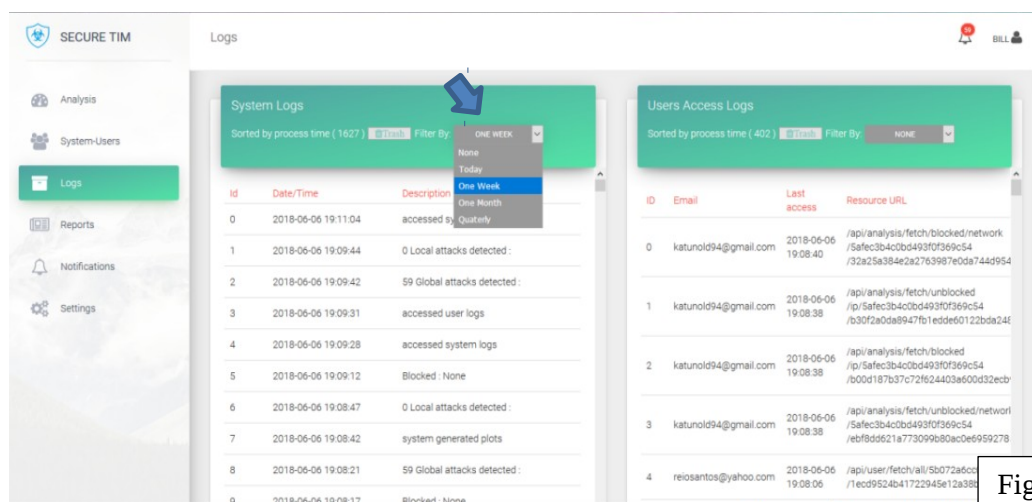






Fig.6.1

4.7 Reports

This provides a view of the blocked and warning Networks and IP addresses as shown by Fig 7, it includes the ability to manually unblock blocked resources by clicking on the Unblock link  and manually block warning (IP addresses with red flags) resources by clicking the Block link . Fig7.1 shows how to reveal a summary of the specific Ip Addresses under a given network that are reported malicious by simply clicking the network Source Name or Address with the unordered lists icon  and you can view detailed information about a selected resource as shown in Fig7.2 by clicking the link with this icon  185.61.138.74 DOTSI, PT

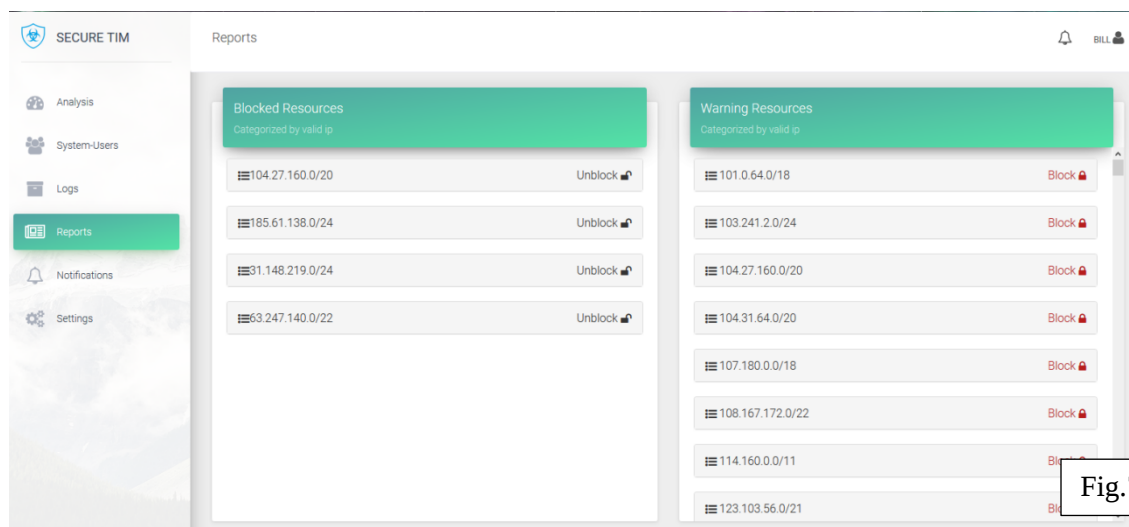
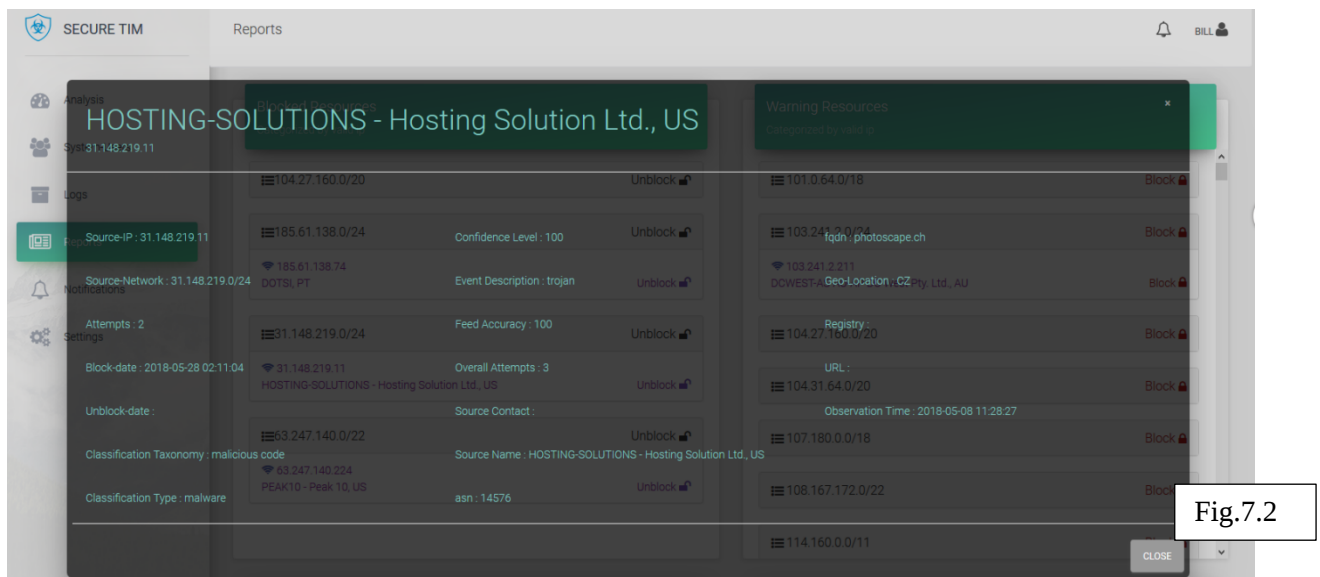
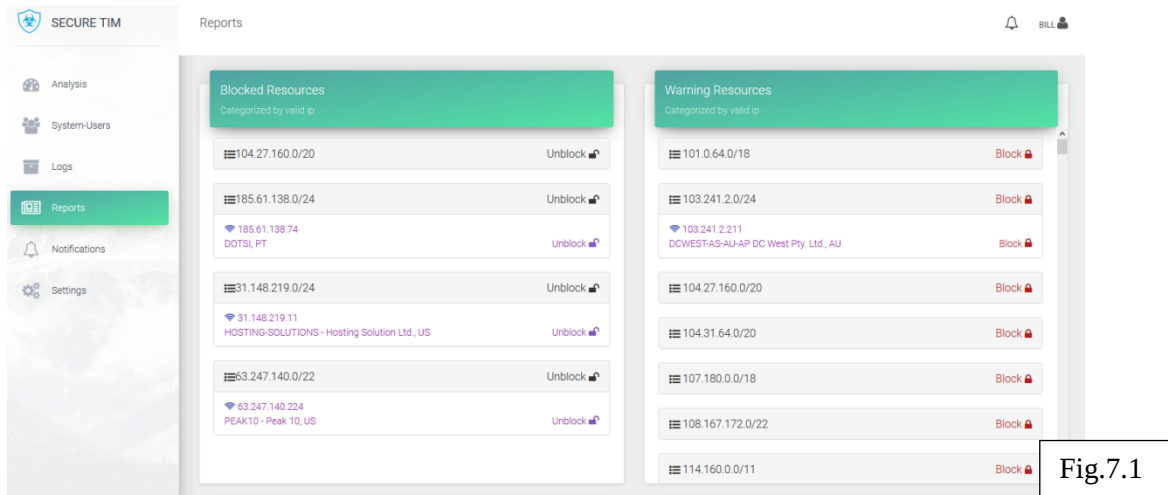


Fig.7



4.8 Notifications

If this section is chosen, you will be able to see both the global and local network security notifications in detail if you click on the source name eg

```
AS-26496-GO-DADDY-COM-LLC - GoDaddy.com, LLC, US
198.71.233.161
198.71.232.0/21
```

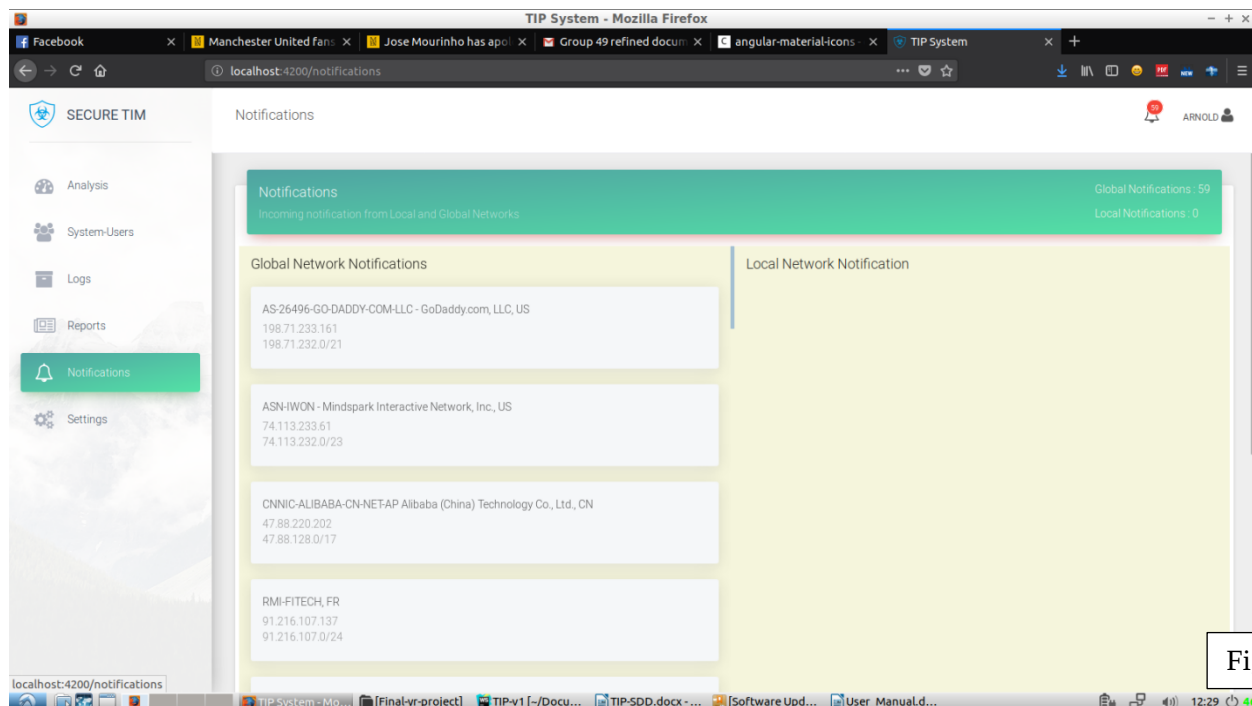


Fig.8

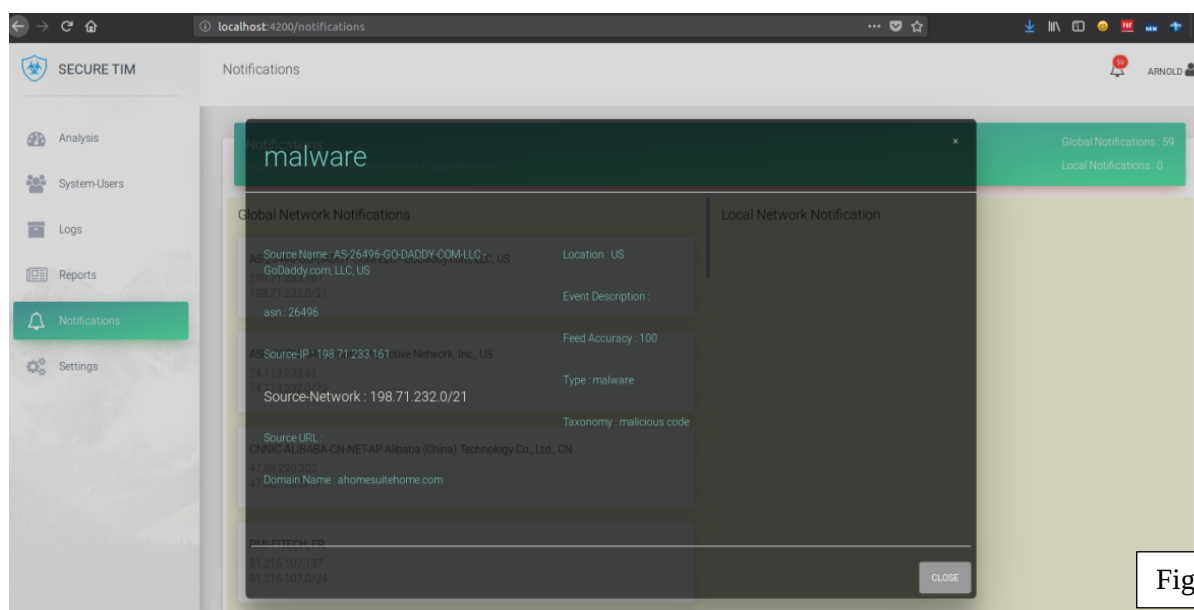


Fig.8.1

4.9 Settings

If this section is chosen, you will be able to customize the TIP system according to the organization preference. This can be achieved by pressing the **EDIT** icon and save **SAVE SETTINGS**.

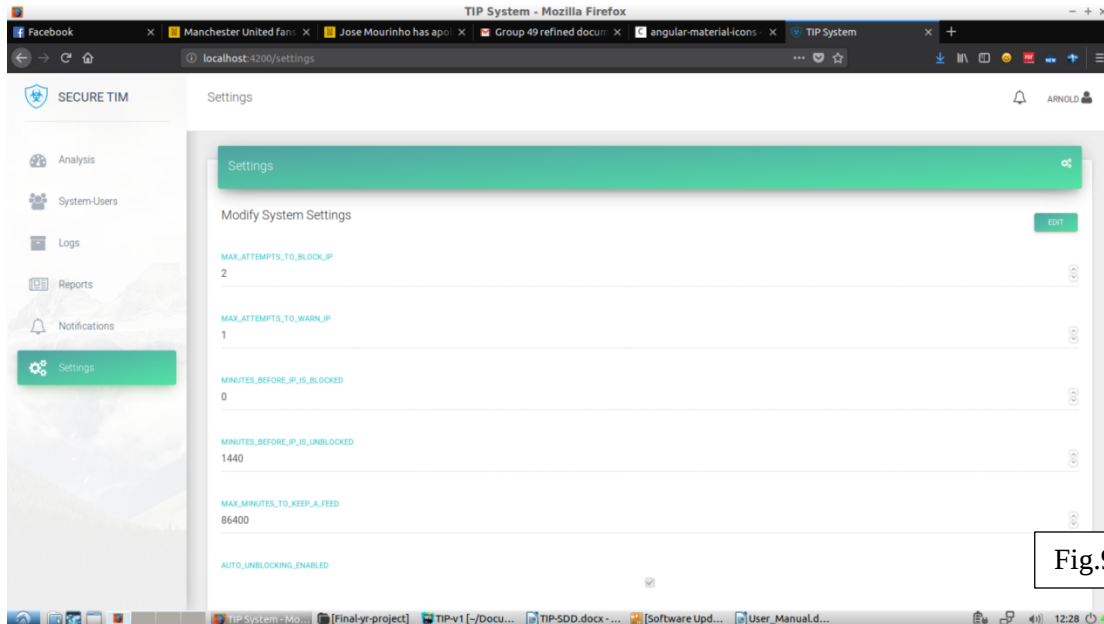


Fig.9