Project Documentation SecOverview

Samuel Giger

Project Page: samuelgiger.com

Github: gigersam/SecOverview

May 20, 2025

Introduction

This document describes the installation and usage of my hobby project Sec-Overview to enable you to create a simple assessment of your infrastructure.

Do not scan assets without the permission of the owner. Use this app at your own risk.

For feedback or input on optimizations, don't hesitate to contact me via the contact form on the page: samuelgiger.com

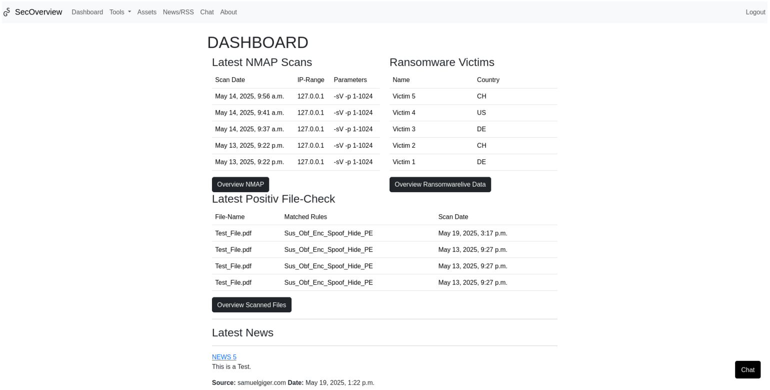
Contents

1 Overview

This document describes the installation and handling of the hobby project github.com/gigersam/SecOverview. This project is intended to help small infrastructures gain better insight and an overview of possible leaks or assets that are accessible. Therefore, the project aims to help analyze certain aspects of it.
In this version, the following actions are implemented:

- RSS Feeds
- Ransomware Victims (Source: Ransomware.live)
- NMAP Scans
- DNS Query
- IP Check (Source: bgpview.io, abuseipdb.com, MISP Threat Shareing)
- File Check (YARA Rules)
- Chat
- ML NIDS (Custom Random-Forest Model and Isolated-Forest Model)

The NMAP scans also save the discovered assets in a database for later viewing. These scans should provide an overview of the assets in the infrastructure.
Following the Dashboard View:



DASHBOARD

Latest NMAP Scans

Scan Date	IP-Range	Parameters
May 14, 2025, 9:56 a.m.	127.0.0.1	-sV -p 1-1024
May 14, 2025, 9:41 a.m.	127.0.0.1	-sV -p 1-1024
May 14, 2025, 9:37 a.m.	127.0.0.1	-sV -p 1-1024
May 13, 2025, 9:22 p.m.	127.0.0.1	-sV -p 1-1024
May 13, 2025, 9:22 p.m.	127.0.0.1	-sV -p 1-1024

Ransomware Victims

Name	Country
Victim 5	CH
Victim 4	US
Victim 3	DE
Victim 2	CH
Victim 1	DE

Latest Positiv File-Check

File-Name	Matched Rules	Scan Date
Test_File.pdf	Sus_Obf_Enc_Spoof_Hide_PE	May 19, 2025, 3:17 p.m.
Test_File.pdf	Sus_Obf_Enc_Spoof_Hide_PE	May 13, 2025, 9:27 p.m.
Test_File.pdf	Sus_Obf_Enc_Spoof_Hide_PE	May 13, 2025, 9:27 p.m.
Test_File.pdf	Sus_Obf_Enc_Spoof_Hide_PE	May 13, 2025, 9:27 p.m.

Latest News

NEWS 5
This is a Test.

Source: samuelgiger.com **Date:** May 19, 2025, 1:22 p.m.

Figure 1: Dashboard View

2 Installation

The current version has been tested on a basic Debian 12 (Bookworm). The application uses Python, Django, Gunicorn, and NGINX. This version only supports SQLite as a database. For Debian 12, an install script is available.
Script: SecOverview Install Script
Download the script via a browser or use the following command:

```
wget https://github.com/gigersam/SecOverview/blob/main/install.sh
```

After downloading the script, add execution rights to the file with the following command:

```
sudo chmod +x install.sh
```

Then execute the file as an administrator with the command:

```
sudo ./install.sh
```

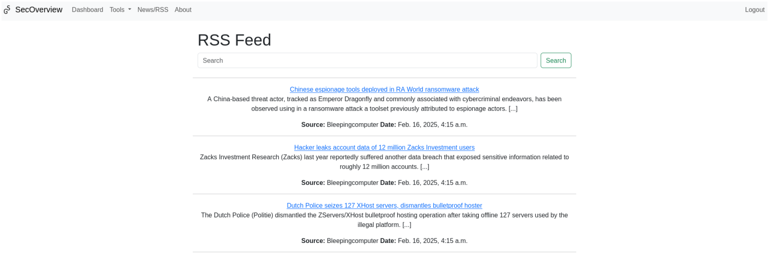
After installation, an output with the admin password will be displayed.
The script also creates a service for the Django application named ”secoverview.service”.
To access the application, use a browser and navigate to the server at:

```
http://YOUR-IP/
```

After that, a login screen will be displayed, where you will be able to log in with the admin credentials.

3 News/RSS

On the ”News/RSS” page, all the latest news from the added RSS feeds will be displayed:



RSS Feed

Chinese espionage tools deployed in RA World ransomware attack

A China-based threat actor, tracked as Emperor Dragonfly and commonly associated with cybercriminal endeavors, has been observed using in a ransomware attack a toolset previously attributed to espionage actors. [...]

Source: Bleepingcomputer **Date:** Feb. 16, 2025, 4:15 a.m.

Hacker leaks account data of 12 million Zacks Investment users

Zacks Investment Research (Zacks) last year reportedly suffered another data breach that exposed sensitive information related to roughly 12 million accounts. [...]

Source: Bleepingcomputer **Date:** Feb. 16, 2025, 4:15 a.m.

Dutch Police seizes 127 XHost servers, dismantles bulletproof hoster

The Dutch Police (Politie) dismantled the ZServers/XHost bulletproof hosting operation after taking offline 127 servers used by the illegal platform. [...]

Source: Bleepingcomputer **Date:** Feb. 16, 2025, 4:15 a.m.

Figure 2: RSS News Overview

To add a new RSS feed, you will be required to access the admin panel. Therefore, navigate to the page *http://YOUR-IP/admin*. Under RSSAPP - Feed Sources - Add Feed Source, you can add more sources. For example, add BleepingComputer’s RSS feed to the database:

URL: *https://www.bleepingcomputer.com/feed/*
NAME: *BleepingComputer*

After visiting the ”News/RSS” page tab, you will be able to see the latest news. This way, you can add more news feeds.

4 File Check (YARA Scans)

To use the YARA scanner, you will be required to add some YARA rules. In this example, the YARA rules from abuse.ch will be used. These rules need to be placed in the folder */home/secoverview/secoverview/secoverview/media/yararules/*. This example shows how to add the rules if there is direct access to the server.

All the following commands need to be run as an administrator!

First, get the YARA rules from abuse.ch:

```
wget https://yaraify.abuse.ch/yarahub/yaraify-rules.zip
```

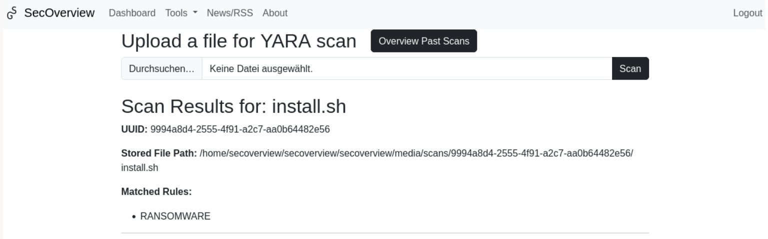
After downloading, the rules need to be unzipped using the unzip command:

```
unzip yaraify-rules.zip -d /home/secoverview/secoverview/secoverview/media/yararules/
```

If the files are successfully unzipped, the service ”secoverview.service” needs to be restarted:

```
systemctl restart secoverview.service
```

After adding the YARA rules, there is an option under Tools - YARA Scan to upload a file and scan it. After the scan, the result will be displayed under the document selection.



Upload a file for YARA scan

Scan Results for: install.sh

UUID: 9994a8d4-2555-4f91-a2c7-aa0b64482e56

Stored File Path: /home/secoverview/secoverview/secoverview/media/scans/9994a8d4-2555-4f91-a2c7-aa0b64482e56/install.sh

Matched Rules:

- RANSOMWARE

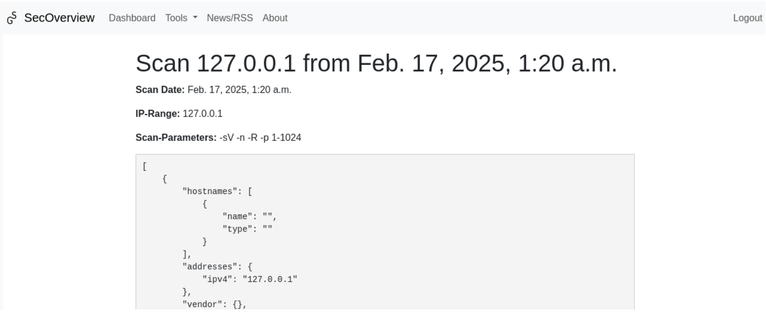
Figure 3: YARA Scan Result

5 NMAP Scan

With the help of the NMAP integration, the application is able to scan the network for assets. These assets are stored in a database along with the scan results. Under Tools - NMAP - Scans - Create Scan, a scan can be created. The following inputs are valid:

IP/Subnet: *192.168.1.1 or 192.168.1.0/24*
Scan Parameters: *All NMAP parameters, e.g., ”-sV -n -R -p 1-1024”*

After running the scan, the scan results will be available under NMAP Overview - Scans - View.



Scan 127.0.0.1 from Feb. 17, 2025, 1:20 a.m.

Scan Date: Feb. 17, 2025, 1:20 a.m.

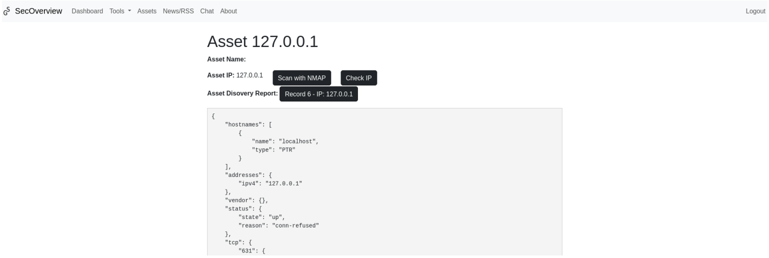
IP-Range: 127.0.0.1

Scan-Parameters: -sV -n -R -p 1-1024

```
[
    {
        "hostnames": [
            {
                "name": "",
                "type": ""
            }
        ],
        "addresses": {
            "ipv4": "127.0.0.1"
        },
        "vendor": {},
```

Figure 4: NMAP Scan

In the overview under Tools - NMAP, past scans and assets are visible. The assets will have the latest scan result attached and allow checking the IP data if it’s a public IP.



Asset 127.0.0.1

Asset Name:

Asset IP: 127.0.0.1

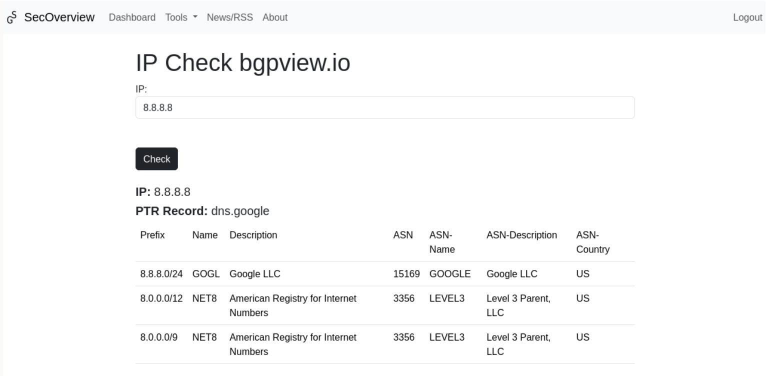
Asset Disovery Report: Record 6 - IP: 127.0.0.1

```
{
    "hostnames": [
        {
            "name": "localhost",
            "type": "PTR"
        }
    ],
    "addresses": {
        "ipv4": "127.0.0.1"
    },
    "vendor": {},
    "status": {
        "state": "up",
        "reason": "conn-refused"
    },
    "tcp": {
        "631": {
```

Figure 5: NMAP Scan

6 IP Check

With the help of the IP Check, the ASN (BGP) data can be viewed. The IP Check app can be found under Tools - IP Check. Therefore, the data is fetched from bgpview.io and displayed:



IP Check bgpview.io

IP:

8.8.8.8

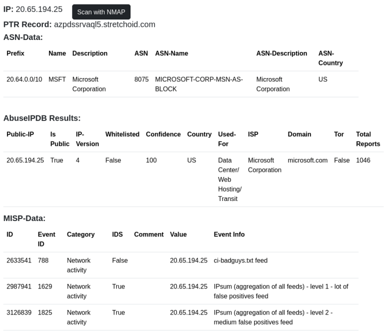
IP: 8.8.8.8

PTR Record: dns.google

Prefix	Name	Description	ASN	ASN-Name	ASN-Description	ASN-Country
8.8.8.0/24	GOGL	Google LLC	15169	GOOGLE	Google LLC	US
8.0.0.0/12	NET8	American Registry for Internet Numbers	3356	LEVEL3	Level 3 Parent, LLC	US
8.0.0.0/9	NET8	American Registry for Internet Numbers	3356	LEVEL3	Level 3 Parent, LLC	US

Figure 6: IP Check Result

Additional checks can be run against AbuseIPDB or MISP. These information sources need to be configured. The additional data helps detect suspicious IPs. The data will be displayed as follows:



IP: 20.65.194.25

PTR Record: azpdssrvaql5.stretchoid.com

ASN-Data:

Prefix	Name	Description	ASN	ASN-Name	ASN-Description	ASN-Country
20.64.0.0/10	MSFT	Microsoft Corporation	8075	MICROSOFT-CORP-MSN-AS-BLOCK	Microsoft Corporation	US

AbuseIPDB Results:

Public-IP	Is Public	IP-Version	Whitelisted	Confidence	Country	Used-For	ISP	Domain	Tor	Total Reports
20.65.194.25	True	4	False	100	US	Data Center/ Web Hosting/ Transit	Microsoft Corporation	microsoft.com	False	1046

MISP-Data:

ID	Event ID	Category	IDS	Comment	Value	Event Info
2633541	788	Network activity	False		20.65.194.25	ci-badguys.txt feed
2987941	1629	Network activity	True		20.65.194.25	IPsum (aggregation of all feeds) - level 1 - lot of false positives feed
3126839	1825	Network activity	True		20.65.194.25	IPsum (aggregation of all feeds) - level 2 - medium false positives feed

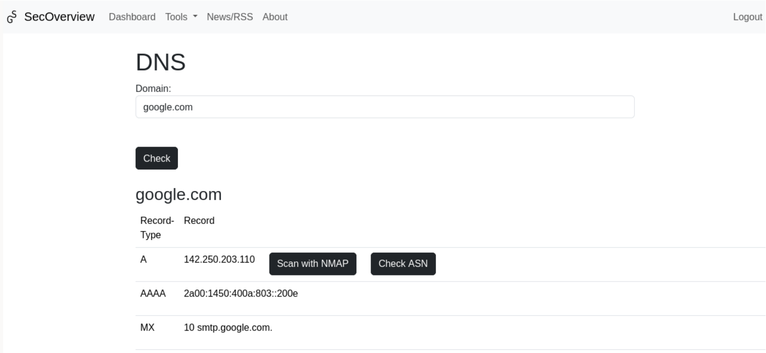
Figure 7: IP Check Result AbuseIPDB and MISP

To minimize the checks on the different sources, the data will be cached.

- bgpview.io: 1 hours
- AbuseIPDB: 1 hours
- MISP: 24 hours

7 DNS Operation

With the help of the DNS Operation, a DNS record can be queried and later analyzed or its values checked with other apps. The DNS Operation app can be found under Tools - DNS Operations. After a query, the following is returned:



DNS

Domain: google.com

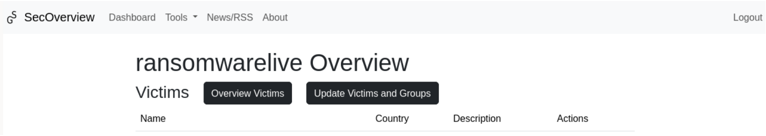
google.com

Record-Type	Record
A	142.250.203.110
AAAA	2a00:1450:400a:803::200e
MX	10 smtp.google.com.

Figure 8: DNS Operation Result

8 Ransomware Data

The app Ransomware Data fetches the victims and ransomware groups from ransomware.live. To fetch the data, go to Tools - Ransomware Data and use the button **Update Victims and Groups**. After updating the data, it is searchable in the Overview views.



ransomwarelive Overview

Victims

Name	Country	Description	Actions

Figure 9: Ransomware Data Overview

9 Chat

With the help of the Chat, there will be an option to ask questions about the current context of the page using the Chat Button at the bottom right side of the page. This will enable the viewer to ask questions about the handling of certain functions of a page. For example: *"What parameters can I use for the NMAP-Scan?"*.
Ollama is used as the provider for the models. Depending on the model and model size, the hardware requirements can vary. The following hardware was used to run the model for 1-3 users:
These specifications are not fully tested or recommended, just experiences!

Model	**Hardware Requirements**	**User Experience**
deepseek-r1:1.5b	NVIDIA GeForce GTX 960, 4GB VRAM	Speed: Slow, Answers/Context-Window: Short
deepseek-r1:8b	NVIDIA GeForce RTX 2070, 8GB VRAM	Speed: Moderate, Answers/Context-Window: Medium

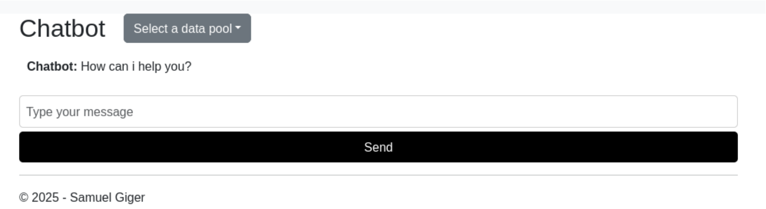
Table 1: Model Hardware Requirements

9.1 Chat Page with Data-Pools

The Data-Pools enable loading additional context from external sources. Currently, the following data formats are supported:

- Text File (.txt)
- PDF File (.pdf)
- JSON File (.json)
- API Data (Auth: Bearer Token and response format JSON)

To use the additional context, select a Data-Pool using the button *Select a data pool*. After selecting the Data-Pool, simply enter a question and submit it.

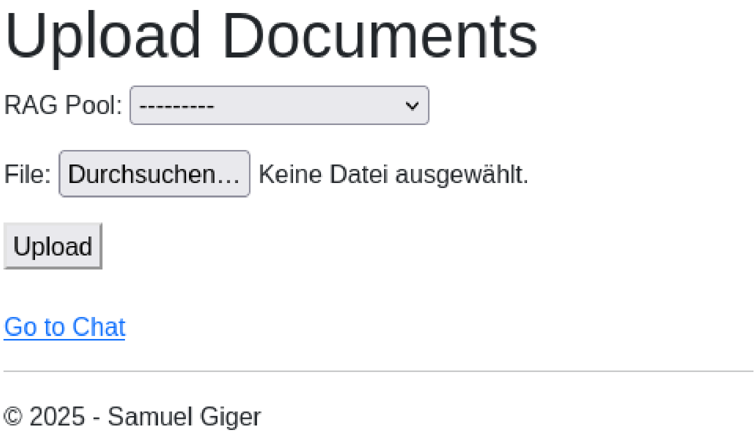


Chatbot: How can i help you?

© 2025 - Samuel Giger

Figure 10: Chat View

Files can be uploaded to a Pool. To access the Upload Page, use the URL https://YOUR-IP/chat/upload or use the button *Upload-Files* on the Chat Page.



Upload Documents

RAG Pool: ---------

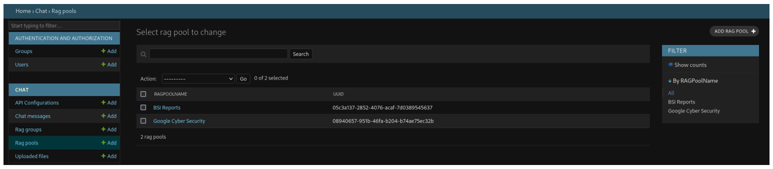
File: Durchsuchen... Keine Datei ausgewählt.

© 2025 - Samuel Giger

Figure 11: Chat Upload Documents

Files can be uploaded to a Data-Pool. If a new Data-Pool is required, it can be created in the Admin-Portal. The Admin Panel is accessible here: https://YOUR-IP/admin
After accessing the Admin-Portal, there is a database under CHAT - RAG Pools. With *Add New*, you will be able to add a Data-Pool using the button *ADD RAG POOL*.

Do not add spaces to the Pool Name.



Select rag pool to change

Action: --------- 0 of 2 selected

□	RAGPOOLNAME	UUID
□	BSI Reports	05c3a137-2852-4076-acaf-7d0389545637
□	Google Cyber Security	08940657-951b-46fa-b204-b74ae75ec32b

2 rag pools

Figure 12: Chat RAG Pools

If API data integration is required, you can add the API Endpoint and Bearer Token in the Admin Panel. The Admin Panel is accessible here: https://YOUR-IP/admin
The entry can be made under CHAT - API Configurations - *ADD API CONFIGURATION*.

The following conditions and configurations are required:

- The name must be unique (no spaces)
- Assign a RAG Pool
- The Base URL must be the API Endpoint
- The API Key needs to be a Bearer Token
- *The response must be in JSON format*

After adding the Endpoint, the service needs to be restarted. Connect to the server and restart the service *secoverview.service* with the following command:

systemctl restart secoverview.service

9.2 Chat Box

With the help of the Chat Box, the user can obtain additional information about certain actions or ask for help or an explanation.

9.2.1 Chat Box Context RSS Feeds

The Chat Box on the RSS Feeds page */rss/* has access to the latest news headlines and descriptions.

9.2.2 Chat Box Context YARA Scans

The Chat Box on the YARA Scans page */yara/* has access to the results of the current scan. If a past scan is opened with */yara/overview/ID*, the Chat Box also has access to the scan results.

9.2.3 Chat Box Context NMAP Scan

The Chat Box on the */nmap/scan* page has knowledge about the input fields of the form. On the scan results page */nmap/scans/ID*, the Chat Box has access to the scan data, including the scanned IP/IP range as well as the scan results.

9.2.4 Chat Box Context BGP Check

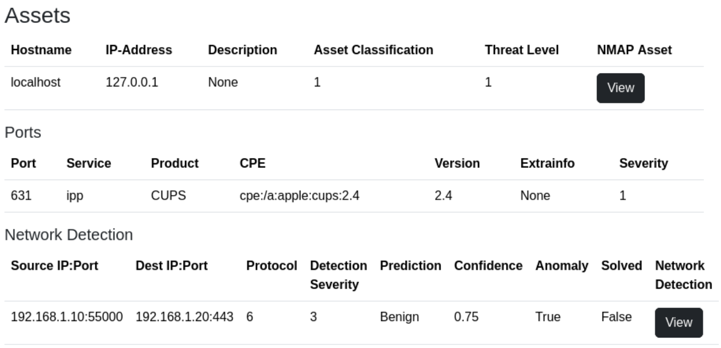
The Chat Box on the */bgpviewcheck/* page has access to the response data.

9.2.5 Chat Box Context DNS Operation

The Chat Box on the */dns/* page has access to the response data.

10 Assets

With help of the Assets App, data from the ML NIDS and NMAP Scan can be coorelated and displayed in one view to analyse the risk of a asset. Therefore the detected Ports of the NMAP Scan will be classified and if a ML NIDS Detection exist it will be linked to the Asset.



Assets

Hostname	IP-Address	Description	Asset Classification	Threat Level	NMAP Asset
localhost	127.0.0.1	None	1	1	View

Ports

Port	Service	Product	CPE	Version	Extrainfo	Severity
631	ipp	CUPS	cpe:/a:apple:cups:2.4	2.4	None	1

Network Detection

Source IP:Port	Dest IP:Port	Protocol	Detection Severity	Prediction	Confidence	Anomaly	Solved	Network Detection
192.168.1.10:55000	192.168.1.20:443	6	3	Benign	0.75	True	False	View

Figure 13: Asset View

11 MLNIDS

MLNIDS is a lightweight service designed to classify data from NIDS tools such as Suricata. The service can analyze PCAP files and detect anomalies. After detection, the results can be uploaded into the tool *SecOverview*, where they can be visualized.

The service analyzes the PCAP files using two different algorithms:

- **Random Forest** – to detect anomalies and classify them.
- **Isolation Forest** – to detect network anomalies.

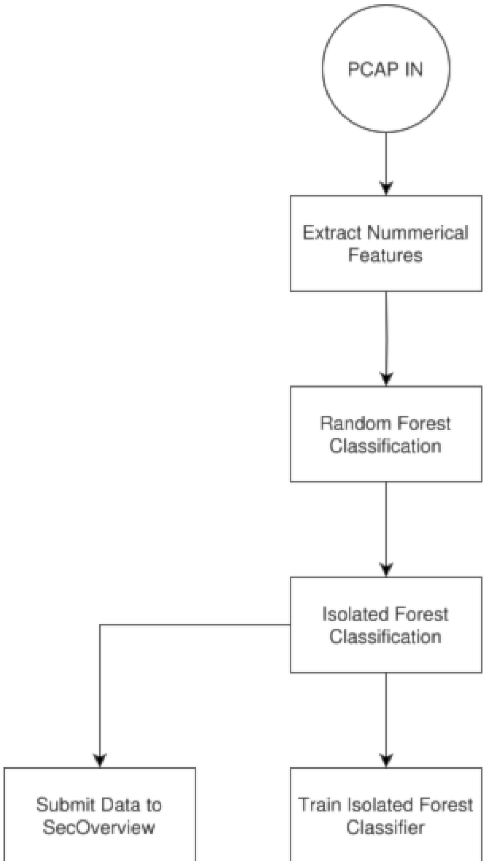

PCAP IN
Extract Nummerical Features
Random Forest Classification
Isolated Forest Classification
Submit Data to SecOverview
Train Isolated Forest Classifier

Figure 14: MLNIDS classification diagram

11.1 MLNIDS Installation

First, Suricata needs to be installed and configured. Use the official installation guide for Suricata: Suricata Installation Guide.

After enabling PCAP logging, the script copy_suricata_pcap.py can be used to copy the PCAP files into MLNIDS's processing and analysis workflow.

Change the source_folder to the directory where Suricata stores the PCAP files:

```
def main():
    # Define the source folder and file pattern
    source_folder = "/path/to/source/folder"
    file_pattern = "log.pcap.*"  # File pattern for
       matching
    remote_directory = "analyse/pcap/todo"
```

Listing 1: Python code to define source folder and pattern

To run the script as a service, create the following service file under /etc/systemd/system/copy_suricata_pcap.service with the content below:

```
[Unit]
Description=Copy Suricata Data with Python
After=network.target

[Service]
ExecStart=/home/secoverview/secoverview/venv/bin/
   python /home/secoverview/secoverview/services/
   mlnids_service/uploader_script_for_analysis.py
WorkingDirectory=/home/secoverview/secoverview/
   services/mlnids_service
Restart=always
User=secoverview
StandardOutput=append:/home/secoverview/secoverview/
   services/mlnids_service/log/default.log
StandardError=append:/home/secoverview/secoverview/
   services/mlnids_service/log/error.log

[Install]
WantedBy=multi-user.target
```

Listing 2: Systemd service file for Suricata PCAP uploader

After creating the service file, enable and start the service using the following commands:

```
sudo systemctl daemon-reload
sudo systemctl enable mlnids.service
sudo systemctl start mlnids.service
```

Listing 3: Enable and start the MLNIDS service

Once this configuration is complete, all PCAP files will be analyzed by the MLNIDS service. Files will be copied if they are older than 30 minutes.

To obtain pre-trained models for MLNIDS, please contact me.

12 Services

With the help of the services, data or tasks will be updated or executed.

12.1 Update Service

With the help of the update service, the following data will be updated:

- Assets gathering: every 30 minutes
- Ransomware data: every 24 hours
- RSS feeds: every 1 hour