

# MicroSec Traffic: Manual do Usuário

Utilizando Estratégias de Engenharia de Tráfego para Aprimoramento da  
Eficiência de Sistemas de Detecção de Intrusão

Curitiba - 2025

## Sumário

<b>1</b>	<b>Introdução</b>	<b>2</b>
<b>2</b>	<b>Recomendações de Sistema</b>	<b>2</b>
2.1	Hardware . . . . .	2
2.2	Software . . . . .	2
<b>3</b>	<b>Estrutura do Repositório</b>	<b>2</b>
<b>4</b>	<b>Instalação e Configuração</b>	<b>3</b>
4.1	Instalação do Docker . . . . .	3
4.2	Instalação do Python e Ambiente Virtual . . . . .	3
4.3	Instalação do Wireshark (Editcap) . . . . .	3
<b>5</b>	<b>Dataset</b>	<b>3</b>
<b>6</b>	<b>Dataset Processado</b>	<b>5</b>
<b>7</b>	<b>Execução</b>	<b>6</b>
7.1	Processar o Dataset . . . . .	6
7.2	Gerar os Chunks . . . . .	6
7.3	Rodar o Container . . . . .	6
7.4	Copiar Dados para o Container . . . . .	6
<b>8</b>	<b>Execução de Experimentos</b>	<b>7</b>
8.1	Acessar o Container e Rodar o Snort . . . . .	7
8.2	Cenários . . . . .	7
8.3	Copiar Logs para a Máquina Host . . . . .	7
8.4	Rodar Scripts de Avaliação . . . . .	7
<b>9</b>	<b>Resultados Esperados</b>	<b>7</b>
<b>10</b>	<b>Preocupações com Segurança</b>	<b>7</b>
<b>11</b>	<b>Licença</b>	<b>8</b>

# 1 Introdução

Este trabalho apresenta o **MicroSec Traffic**, uma abordagem para melhorar a eficiência de sistemas de detecção de intrusão (IDS) tradicionais, como Snort e Suricata. A técnica utiliza engenharia de tráfego para reduzir o volume de dados analisados, sem comprometer a geração de alertas.

O método não requer alterações nas ferramentas IDS, apenas ajustes nas regras utilizadas. A abordagem foi avaliada em ambiente controlado com Snort, demonstrando efetividade em manter a detecção de ameaças com menor tempo de processamento.

## 2 Recomendações de Sistema

### 2.1 Hardware

- CPU: AMD EPYC 7401 24-Core 2.0GHz
- RAM: 16 GB
- Kernel: 6.6.6-Atwood
- Sistema Operacional: Debian GNU/Linux 12 (bookworm)

### 2.2 Software

- Docker - versão 28.0.2
- Wireshark - versão 4.0.17
- Python - versão 3.12

## 3 Estrutura do Repositório

SBSeg-2025-Herbele

```
datasets/  
  microsec/  
    chunks/  
    original/  
      chunks/  
docker/  
  Dockerfile  
logs/  
  microsec/  
    chunks/  
    original/  
      chunks/  
README.md  
rules/  
  microsec-pcap.rules  
  original-pcap.rules
```

```
scripts/  
    cenario-1.sh  
    cenario-2.sh  
    cenario-3.sh  
    cenario-4.sh  
    microsec.py  
    requirements.txt
```

## 4 Instalação e Configuração

### 4.1 Instalação do Docker

```
sudo apt install ca-certificates curl gnupg  
sudo install -m 0755 -d /etc/apt/keyrings  
curl -fsSL https://download.docker.com/linux/debian/gpg | sudo gpg --dearmor -o  
    /etc/apt/keyrings/docker.gpg  
sudo chmod a+r /etc/apt/keyrings/docker.gpg  
echo \  
    "deb [arch=$(dpkg --print-architecture) signed-by=/etc/apt/keyrings/docker.  
    gpg] \  
    https://download.docker.com/linux/debian \  
    $(. /etc/os-release && echo "$VERSION_CODENAME") stable" | \  
    sudo tee /etc/apt/sources.list.d/docker.list > /dev/null  
sudo apt update  
sudo apt install docker-ce docker-ce-cli containerd.io docker-buildx-plugin  
    docker-compose-plugin  
cd SBSeg-2025-Herbele/docker  
docker build -t snort3-docker .
```

### 4.2 Instalação do Python e Ambiente Virtual

```
sudo apt install python3.12  
python3.12 -m venv venv  
source venv/bin/activate  
cd SBSeg-2025-Herbele/scripts  
pip install -r requirements.txt
```

### 4.3 Instalação do Wireshark (Editcap)

```
sudo apt install wireshark
```

## 5 Dataset

O dataset original usado neste projeto é o **CIC-IDS-2017**, disponível em:  
<https://www.unb.ca/cic/datasets/ids-2017.html>

Vá até a parte inferior do site e procure pela opção *Download the dataset* (indicada com a seta vermelha na figura 1) e clique nela.

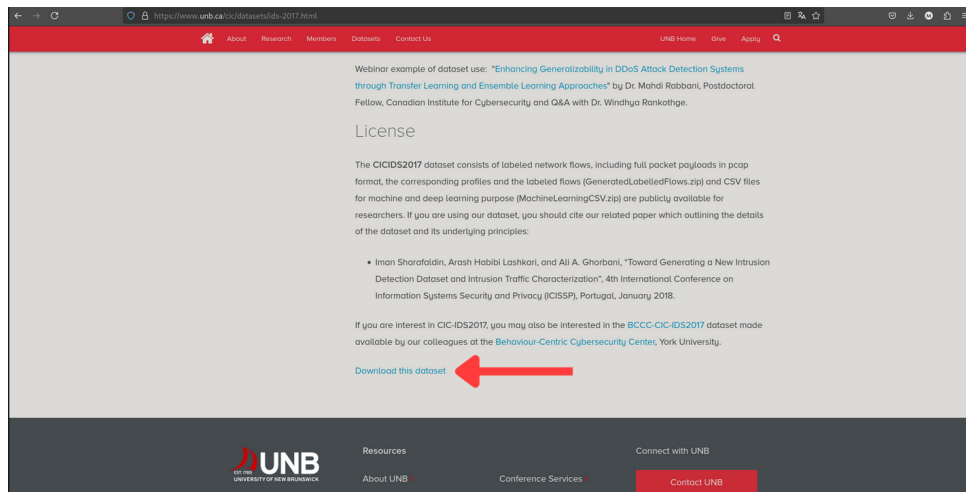


Figura 1: Homepage do site que disponibiliza o dataset original.




Você será direcionado para um formulário que requisita informações sobre quem está requisitando o uso do dataset. Preencha-o para a liberação da página que possibilita o download do dataset.

A screenshot of a web form titled 'CIC DATASET DOWNLOAD FORM for "CIC-IDS-2017"'. The form is set against a dark background with a yellow shield logo at the top. It asks users to fill in the following fields: First Name, Last Name, Email, Organization/Company, Job Title, and Country (a dropdown menu currently showing 'Brazil'). There are 'Submit' and 'Clear' buttons at the bottom of the form fields. Below the form, a disclaimer states: 'DISCLAIMER: Your information provided will only be for internal CIC Statistical Purpose and will not be disclosed.' At the very bottom, there are logos for UNB, Canadian Institute for Cybersecurity, LinkedIn, Twitter, and YouTube.

Figura 2: Formulário para a liberação do dataset.

Clique em *PCAPs*.

### Index of /CICDataset/CIC-IDS-2017/Dataset/CIC-IDS-2017












Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">CSVs/</a>	2024-02-01 16:28	-	
 <a href="#">PCAPs/</a>	2024-02-01 17:08	-	

Apache/2.4.41 (Ubuntu) Server at cicresearch.ca Port 80

Figura 3: Lista com opção entre os arquivos PCAPs e CSVs do dataset.

Baixe o arquivo `Wednesday-workingHours.pcap`.

### Index of /CICDataset/CIC-IDS-2017/Dataset/CIC-IDS-2017/PCAPs

Name	Last modified	Size	Description
 <a href="#">Parent Directory</a>		-	
 <a href="#">Friday-WorkingHours.md5</a>	2024-02-01 16:28	59	
 <a href="#">Friday-WorkingHours.pcap</a>	2024-02-01 16:36	8.2G	
 <a href="#">Monday-WorkingHours.md5</a>	2024-02-01 16:36	59	
 <a href="#">Monday-WorkingHours.pcap</a>	2024-02-01 16:48	10G	
 <a href="#">Thursday-WorkingHours.md5</a>	2024-02-01 16:48	61	
 <a href="#">Thursday-WorkingHours.pcap</a>	2024-02-01 16:57	7.7G	
 <a href="#">Tuesday-WorkingHours.md5</a>	2024-02-01 16:57	60	
 <a href="#">Tuesday-WorkingHours.pcap</a>	2024-02-01 17:08	10G	
 <a href="#">Wednesday-workingHours.md5</a>	2024-02-01 17:08	62	
 <a href="#">Wednesday-workingHours.pcap</a>	2024-02-01 17:20	12G	

Apache/2.4.41 (Ubuntu) Server at cicresearch.ca Port 80

Figura 4: Lista com todos os arquivos disponíveis do dataset.

## 6 Dataset Processado

O dataset já processado com a técnica MicroSec Traffic pode ser baixado em:  
<https://www.inf.ufpr.br/msh22/microsec.html>

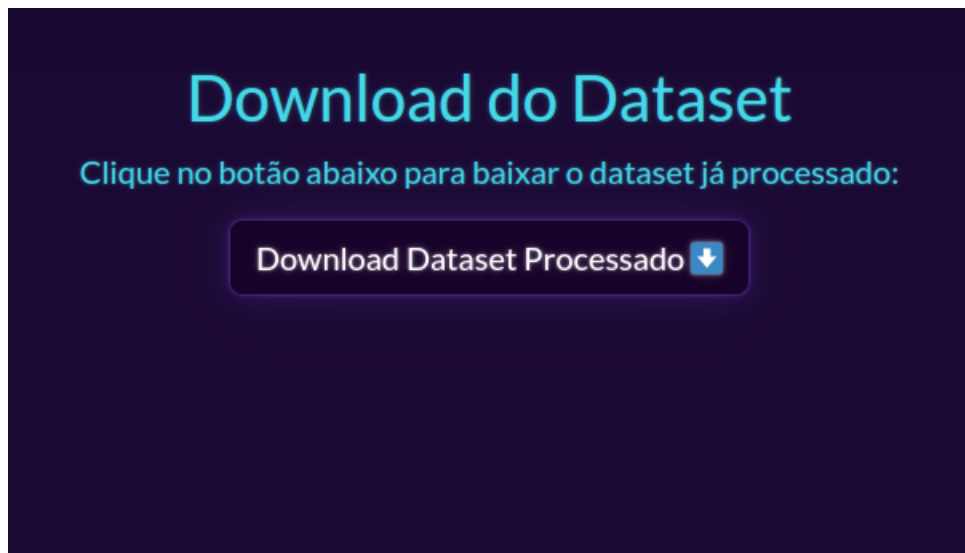


Figura 5: Site com a opção de *download* do dataset processado com a técnica MicroSec.

**Importante:** Ambos os arquivos devem estar nas rotas:

- Dataset original: SBSeg-2025-Herbele/datasets/original
- Dataset processado: SBSeg-2025-Herbele/datasets/microsec

## 7 Execução

### 7.1 Processar o Dataset

```
cd SBSeg-2025-Herbele/scripts
python microsec.py
```

### 7.2 Gerar os Chunks

```
editcap -c 1000000 datasets/microsec/microsec.pcap datasets/microsec/chunks/
microsec-%d.pcap
editcap -c 1000000 datasets/original/Wednesday-workingHours.pcap datasets/
original/chunks/original-%d.pcap
```

### 7.3 Rodar o Container

```
docker run -d --name snort-container snort3-docker
```

### 7.4 Copiar Dados para o Container

```
docker cp datasets/microsec/* snort-container:/usr/src/datasets/microsec/
docker cp datasets/original/* snort-container:/usr/src/datasets/original/
docker cp rules/* snort-container:/usr/src/rules/
```

## 8 Execução de Experimentos

### 8.1 Acessar o Container e Rodar o Snort

```
docker exec -it snort-container /bin/bash
cd /usr/src/snort3/lua
snort --daq pcap -R [regras] -r [arquivo] -A cmg > [log]
```

### 8.2 Cenários

- Cenário 1:

```
snort --daq pcap -R /usr/src/rules/original.rules -r /usr/src/datasets/
original/Wednesday-workingHours.pcap -A cmg > /usr/src/logs/original-[
n].txt
```

- Cenário 2:

```
snort --daq pcap -R /usr/src/rules/microsec.rules -r /usr/src/datasets/
microsec/microsec.pcap -A cmg > /usr/src/logs/microsec-[n].txt
```

- Cenário 3 e 4: repetir para chunks.

### 8.3 Copiar Logs para a Máquina Host

```
docker cp snort-container:/usr/src/logs/microsec/* logs/microsec/
docker cp snort-container:/usr/src/logs/original/* logs/original/
```

### 8.4 Rodar Scripts de Avaliação

```
cd scripts/
./cenario-1.sh
./cenario-2.sh
./cenario-3.sh
./cenario-4.sh
```

## 9 Resultados Esperados

Os scripts imprimem no terminal métricas como tempo de execução e número de alertas para cada execução e para a média entre execuções.

## 10 Preocupações com Segurança

Não foram identificadas preocupações de segurança relevantes.

## 11 Licença

Este projeto está licenciado sob a licença **GNU GPL v3**.