FPT Education
FPT UNIVERSITY

THESIS DEFENSE

# SMART MONITORING AND AUTOMATED RESPONSE FOR ENDPOINT USING SPLUNK MACHINE LEARNING

**Supervisor: Tran Van Ninh**

**Capstone Project code: SU25IA05_GSU05**

FPT Education
FPT UNIVERSITY

# TEAM MEMBERS

Nguyen Thanh Hai - SE172059 - Leader

Huynh Minh Thang - SE172703

Nguyen Quoc Dai - SE173556

Pham Minh Nghia - SE150935

FPT Education
FPT UNIVERSITY

# Table of contents

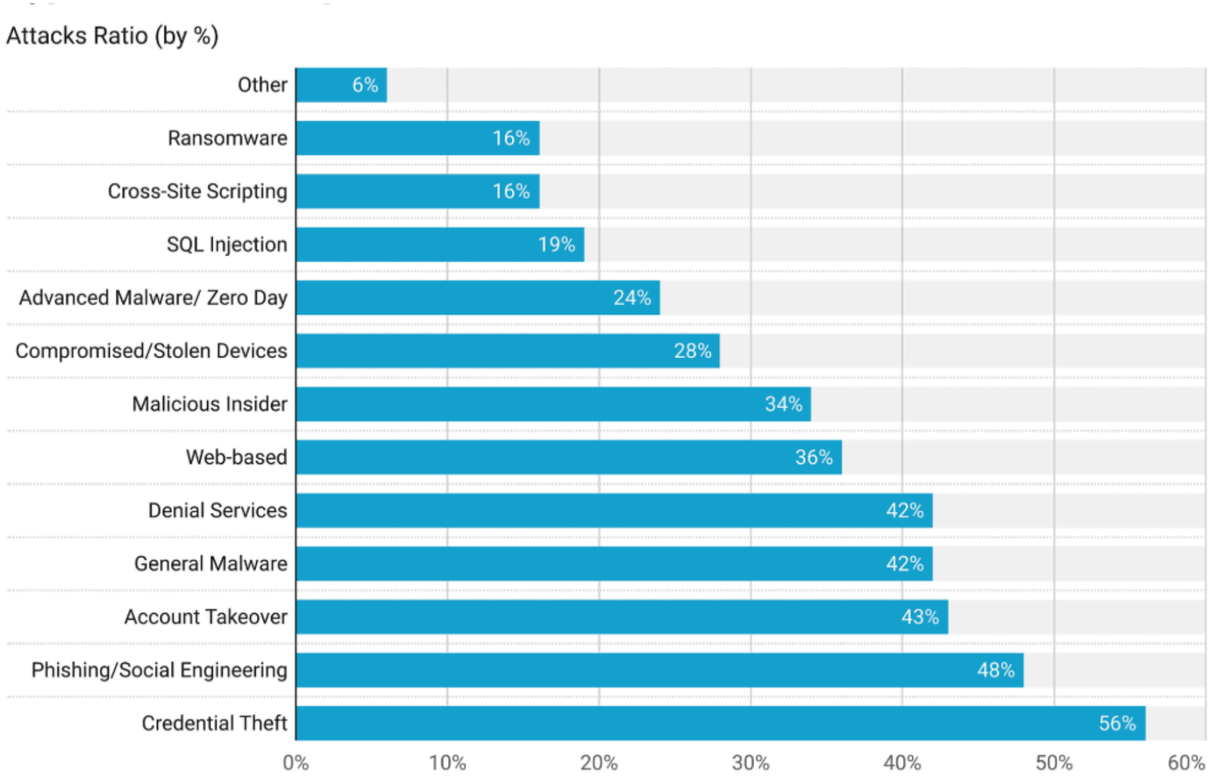
# 1. Background:

659.000 cyber attacks targeting Vietnamese businesses

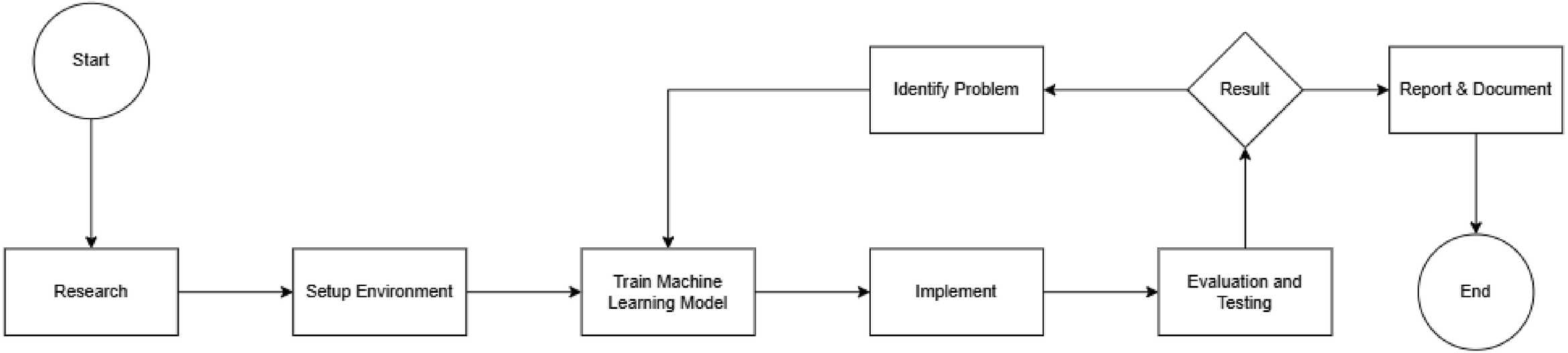
46% of agencies and enterprises experienced a cyber intrusion

6,77% reported experiencing regular cyberattacks

**9,5%** ↑



# 2. Objectives



# Problems

## Cyber attacks on the rise

Attack methods are becoming increasingly sophisticated

## Limitations of traditional systems

Traditional monitoring measures mainly based on rules and signatures

## Lack of automated response

Manual processing
→ time consuming

# Solutions

## Build smart monitoring system for endpoint

Scalability & centralized management

Visual display via dashboard

## Splunk Applications Combine ML

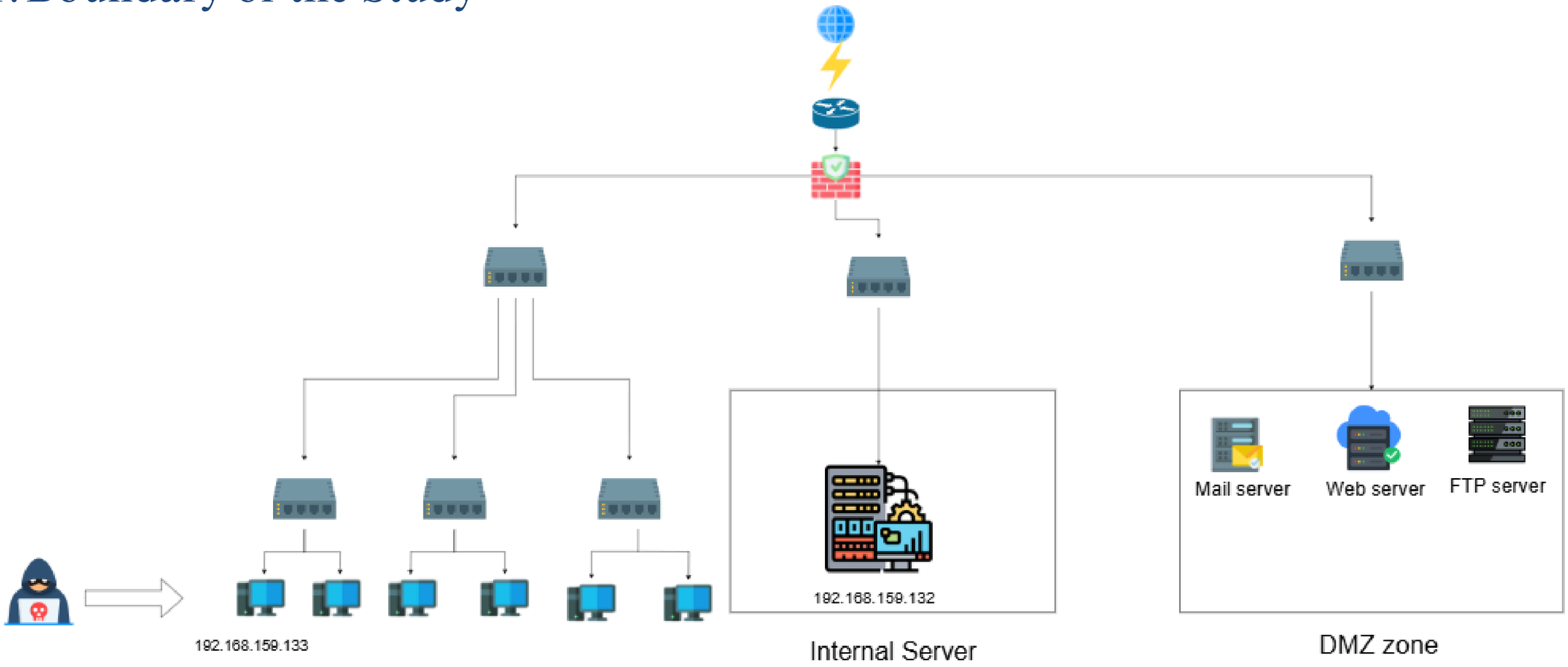
Early detection of attack signs

## Automated response

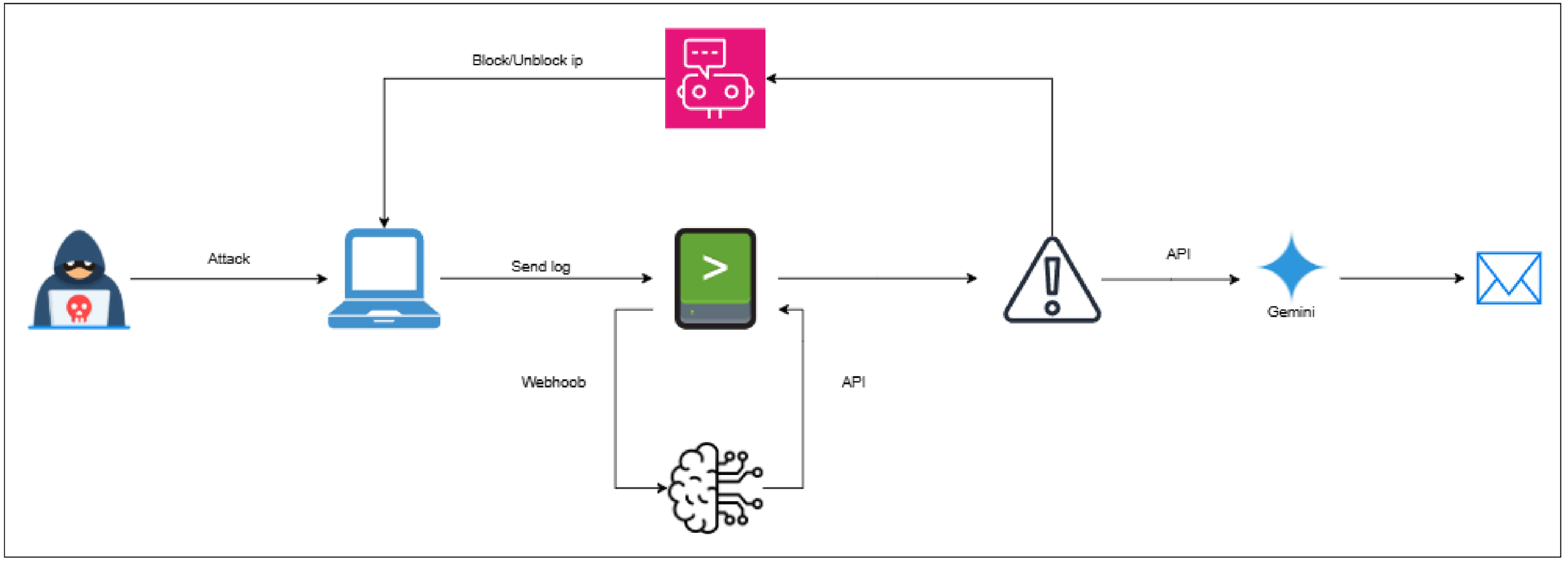
Splunk alert via HEC
→ Python script

Automatic IP blocking,alert

# 1. Boundary of the Study

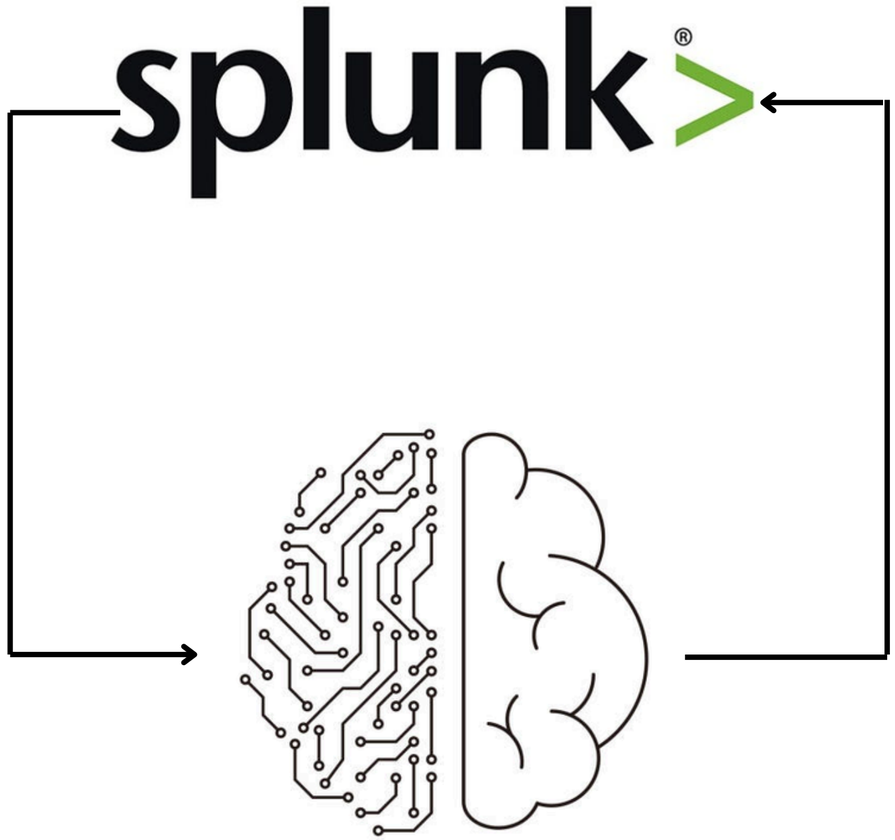


# 2. System Architecture



# 3. What is Splunk?

Splunk is a software primarily used for searching, monitoring, and inspecting machine-generated data through a web interface, enabling analysis to generate reports and provide real-time alerts.

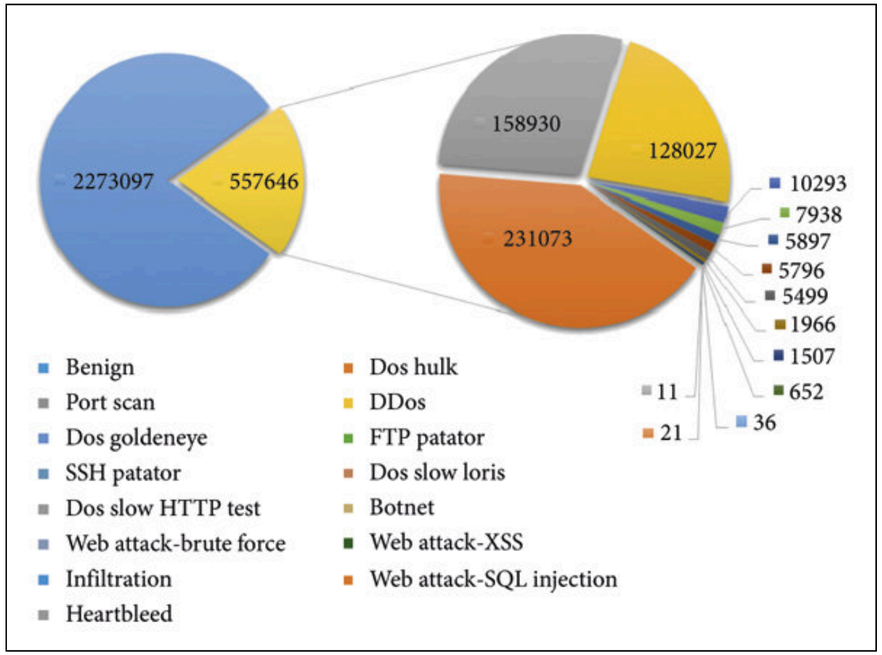



## Splunk Applications Combine ML

- Expand into an intelligent monitoring system
- Proactive response
- Predict, detect early, and automatically prevent threats

# 4. Dataset

The CICIDS2017 dataset is a benchmark dataset developed specifically for research in the field of network intrusion detection systems




| Name of Files | Day Activity | Attacks Found |
|---|---|---|
| Monday-WorkingHours.pcap_ISCX.csv | Monday | Benign (Normal human activities) |
| Tuesday-WorkingHours.pcap_ISCX.csv | Tuesday | Benign, FTP-Patator, SSH-Patator |
| Wednesday-workingHours.pcap_ISCX.csv | Wednesday | Benign, DoS GoldenEye, DoS Hulk, DoS Slowhttptest, DoS slowloris, Heartbleed |
| Thursday-WorkingHours-Morning-WebAttacks.pcap_ISCX.csv | Thursday | Benign, Web Attack – Brute Force, Web Attack – Sql Injection, Web Attack – XSS |
| Thursday-WorkingHours-Afternoon-Infilteration.pcap_ISCX.csv | Thursday | Benign, Infiltration |
| Friday-WorkingHours-Morning.pcap_ISCX.csv | Friday | Benign, Bot |
| Friday-WorkingHours-Afternoon-PortScan.pcap_ISCX.csv | Friday | Benign, PortScan |
| Friday-WorkingHours-Afternoon-DDos.pcap_ISCX.csv | Friday | Benign, DDoS |

# 4. Dataset

The CICIDS2017 dataset comprises 15 distinct traffic classes, encompassing both benign (normal) activities and various types of malicious attacks.

84 features describing network traffic characteristics.

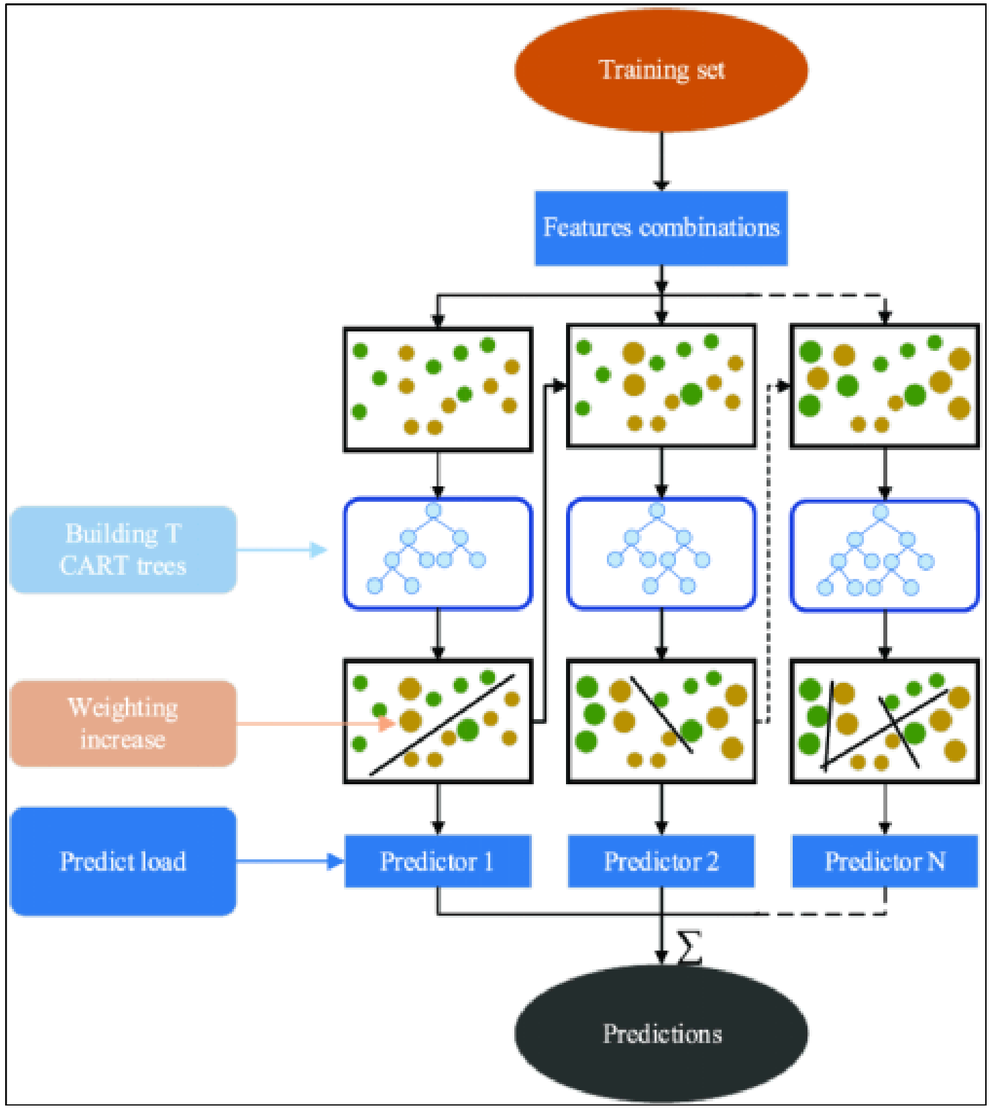
| No. | Feature | No. | Feature | No. | Feature |
|---|---|---|---|---|---|
| 1 | Flow ID | 29 | Fwd IAT Std | 57 | ECE Flag Count |
| 2 | Source IP | 30 | Fwd IAT Max | 58 | Down/Up Ratio |
| 3 | Source Port | 31 | Fwd IAT Min | 59 | Average Packet Size |
| 4 | Destination IP | 32 | Bwd IAT Total | 60 | Avg Fwd Segment Size |
| 5 | Destination Port | 33 | Bwd IAT Mean | 61 | Avg Bwd Segment Size |
| 6 | Protocol | 34 | Bwd IAT Std | 62 | Fwd Avg Bytes/Bulk |
| 7 | Time stamp | 35 | Bwd IAT Max | 63 | Fwd Avg Packets/Bulk |
| 8 | Flow Duration | 36 | Bwd IAT Min | 64 | Fwd Avg Bulk Rate |
| 9 | Total Fwd Packets | 37 | Fwd PSH Flags | 65 | Bwd Avg Bytes/Bulk |
| 10 | Total Backward Packets | 38 | Bwd PSH Flags | 66 | Bwd Avg Packets/Bulk |
| 11 | Total Length of Fwd Pck | 39 | Fwd URG Flags | 67 | Bwd Avg Bulk Rate |
| 12 | Total Length of Bwd Pck | 40 | Bwd URG Flags | 68 | Subflow Fwd Packets |
| 13 | Fwd Packet Length Max | 41 | Fwd Header Length | 69 | Subflow Fwd Bytes |
| 14 | Fwd Packet Length Min | 42 | Bwd Header Length | 70 | Subflow Bwd Packets |
| 15 | Fwd Pck Length Mean | 43 | Fwd Packets/s | 71 | Subflow Bwd Bytes |
| 16 | Fwd Packet Length Std | 44 | Bwd Packets/s | 72 | Init_Win_bytes_fwd |
| 17 | Bwd Packet Length Max | 45 | Min Packet Length | 73 | Act_data_pkt_fwd |
| 18 | Bwd Packet Length Min | 46 | Max Packet Length | 74 | Min_seg_size_fwd |
| 19 | Bwd Packet Length Mean | 47 | Packet Length Mean | 75 | Active Mean |
| 20 | Bwd Packet Length Std | 48 | Packet Length Std | 76 | Active Std |
| 21 | Flow Bytes/s | 49 | Packet Len. Variance | 77 | Active Max |
| 22 | Flow Packets/s | 50 | FIN Flag Count | 78 | Active Min |
| 23 | Flow IAT Mean | 51 | SYN Flag Count | 79 | Idle Mean |
| 24 | Flow IAT Std | 52 | RST Flag Count | 80 | Idle Packet |
| 25 | Flow IAT Max | 53 | PSH Flag Count | 81 | Idle Std |
| 26 | Flow IAT Min | 54 | ACK Flag Count | 82 | Idle Max |
| 27 | Fwd IAT Total | 55 | URG Flag Count | 83 | Idle Min |
| 28 | Fwd IAT Mean | 56 | CWE Flag Count | 84 | Label |

# 5. Algorithm

XGBoost is a boosting algorithm optimized for speed and performance. It is widely used in supervised learning tasks.

The XGBoost algorithm works by combining boosting techniques with multiple decision trees to produce the final prediction

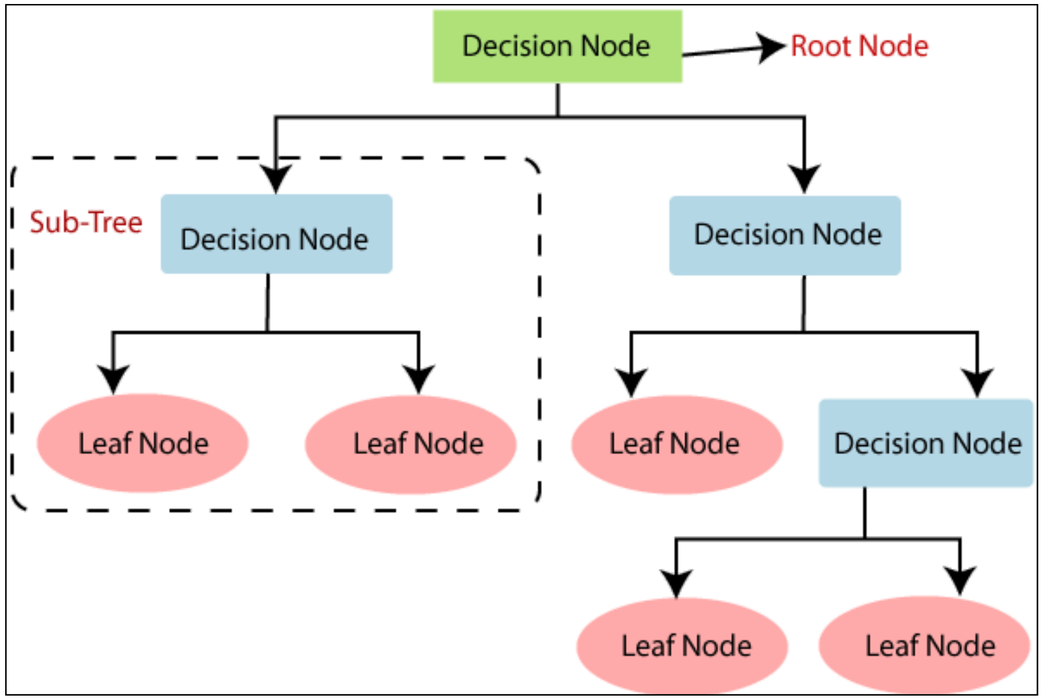
=> Enhances accuracy and improves overall model performance



# 5. Algorithm

Boosting is a machine learning technique that incrementally improves weak models by adding more models that focus on correcting the errors made by previous ones


Decision Trees are algorithms that use a tree-like structure to make predictions.



# 1. Training ML

## 1. Load & merge data

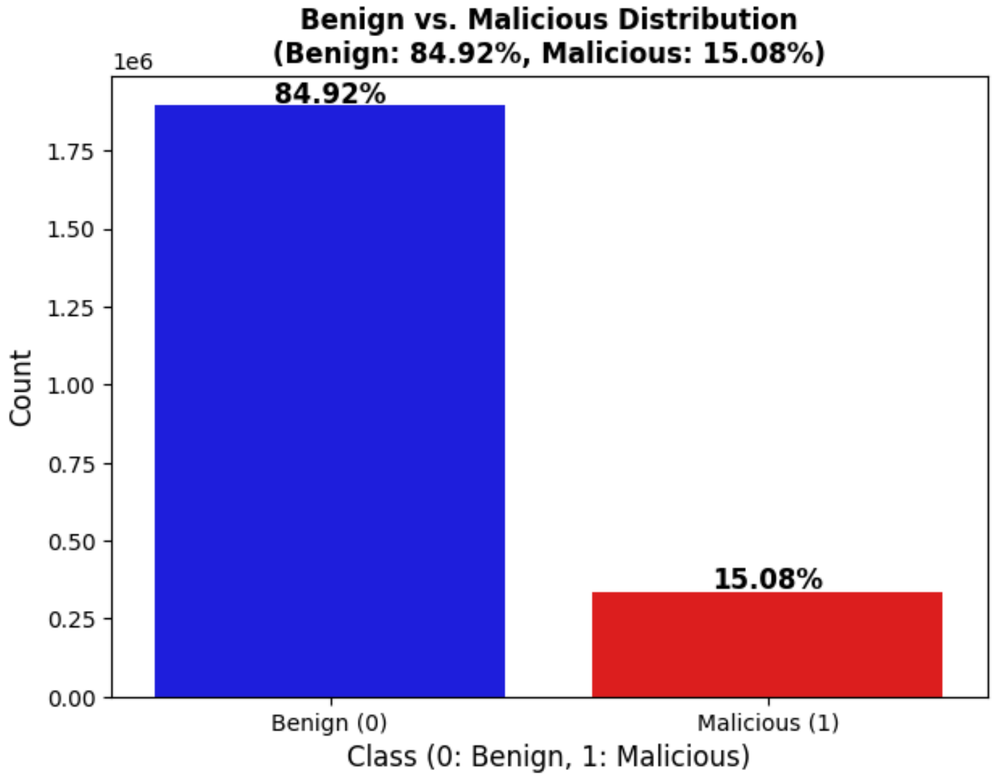
Import library
Read all CIC-IDS-2017 files into DataFrame.

## 2. Preprocessing & labeling

Remove null values and duplicate records,
reset index.

Convert Label column to binary
(0=Benign, 1=Malicious) and check class balance.

```
Class Distribution:
Benign (0): 1,895,314 samples (84.92%)
Malicious (1): 336,492 samples (15.08%)
```



# 1. Training ML

### 3. Split & scale

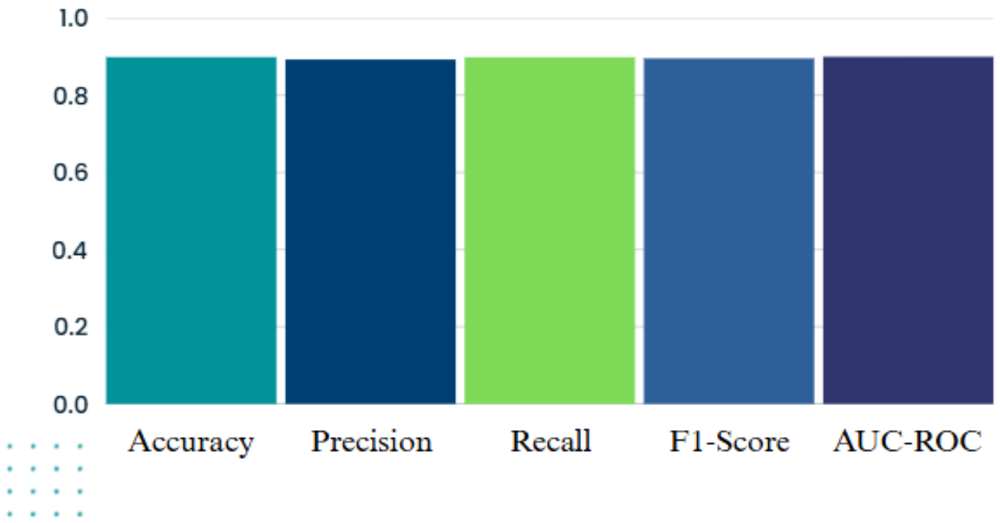
Split stratified train/validation/test (80%/10%/10%).
Fit RobustScaler on train and transform for all three sets

```
Training Set: 1785444 samples
Validation Set: 223181 samples
Test Set: 223181 samples
```

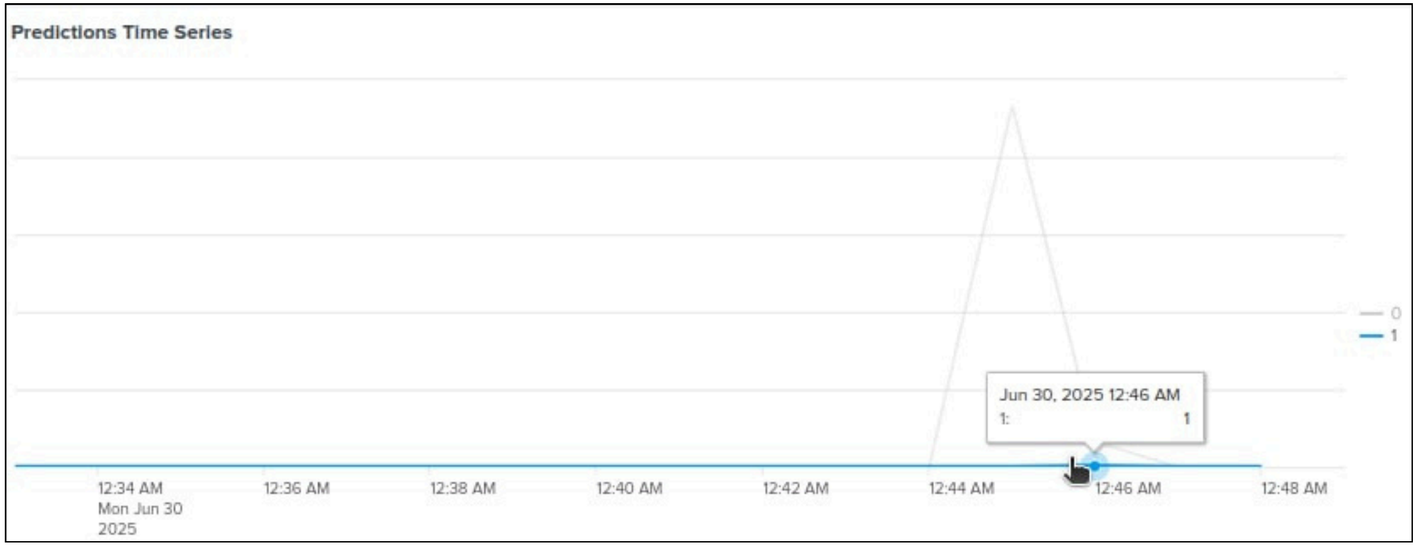
### 4. Configure & train with XGBoost

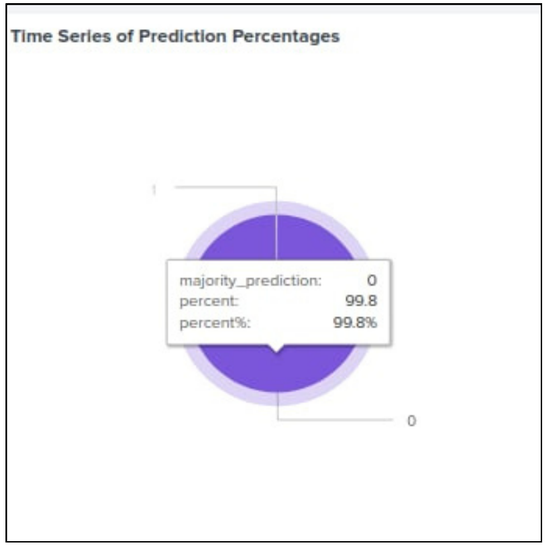
Initialize XGBClassifier with key parameters, train with early stopping on validation set.

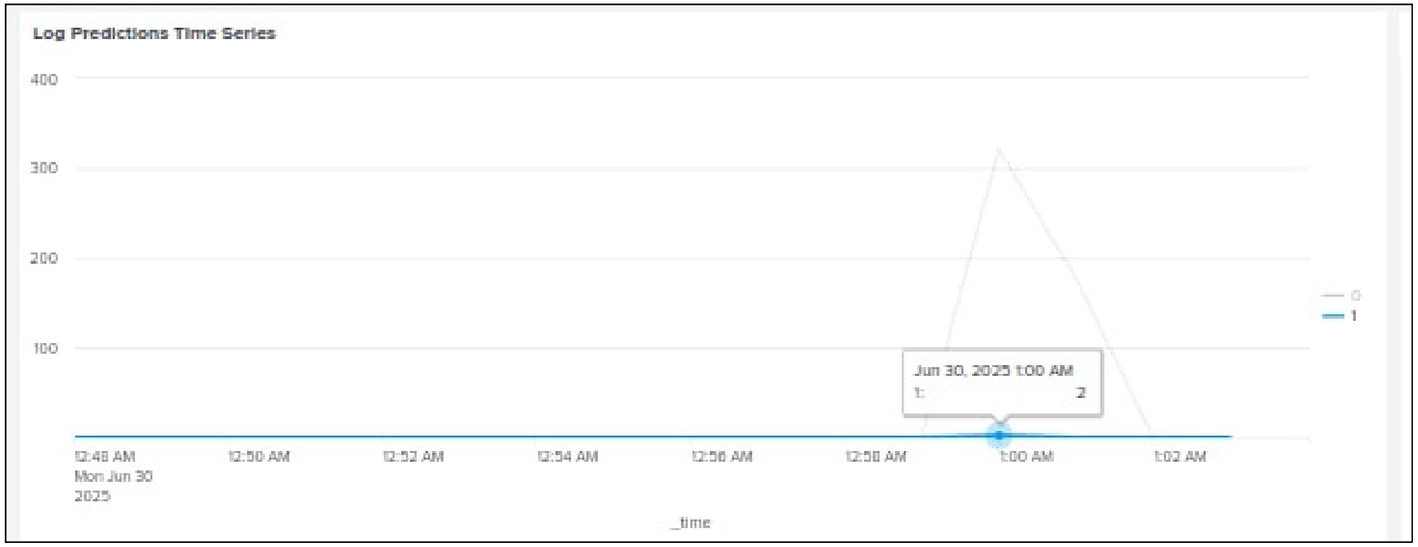
```
Validation Metrics:
Accuracy:  0.8986
Precision: 0.8925
Recall:    0.8983
F1-Score:  0.8954
AUC-ROC:   0.8996
✅ Model and feature names saved.
```

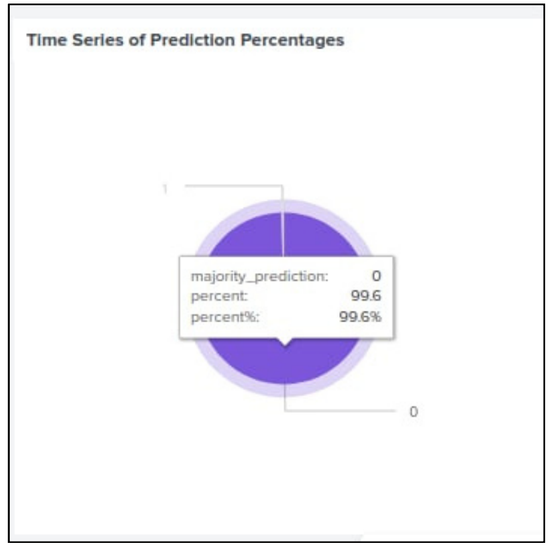


# 2. Testing

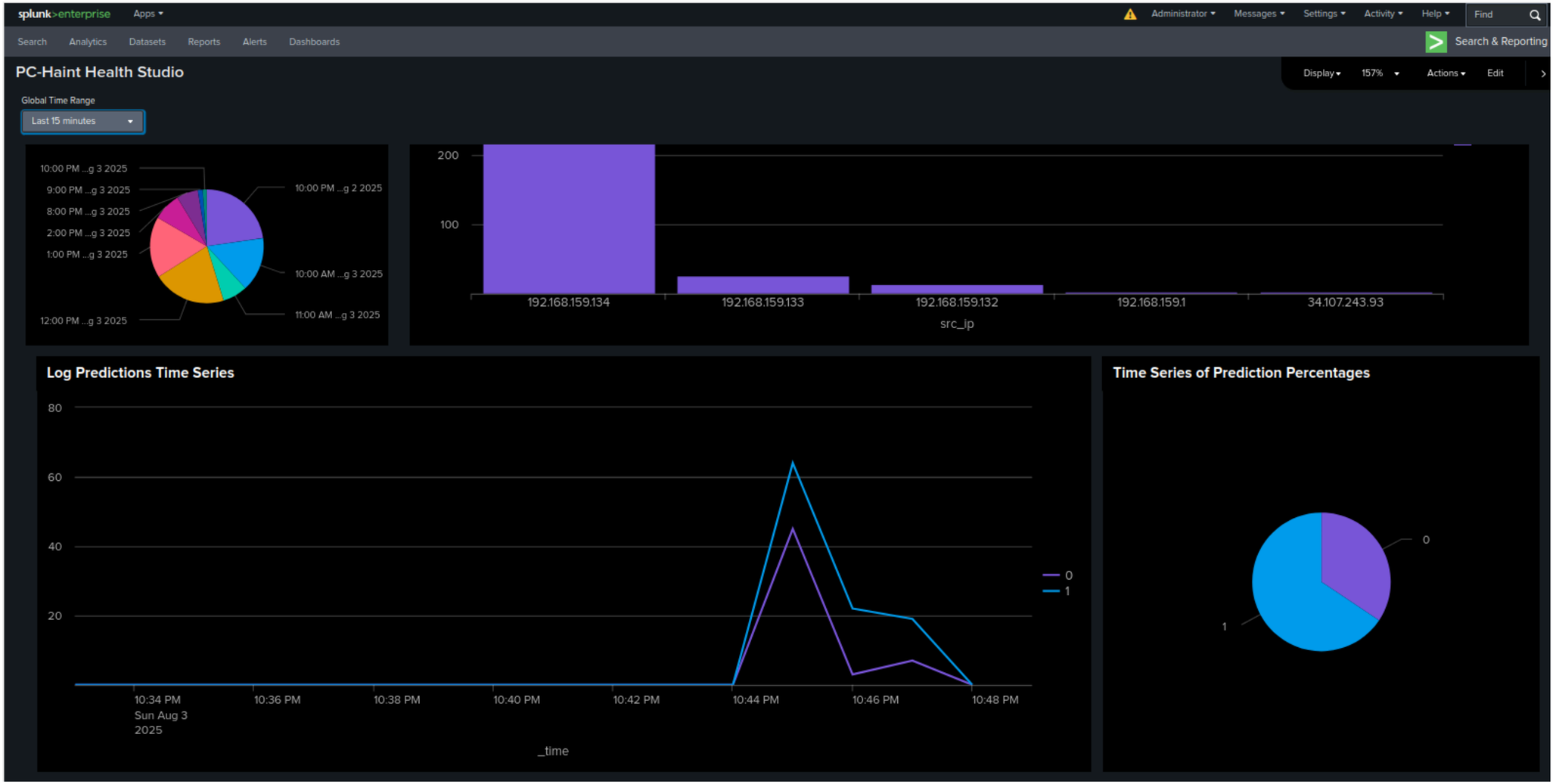

Predictions Time Series
Jun 30, 2025 12:46 AM
1: 1
12:34 AM
Mon Jun 30
2025
12:36 AM
12:38 AM
12:40 AM
12:42 AM
12:44 AM
12:46 AM
12:48 AM
0
1


Time Series of Prediction Percentages
majority_prediction: 0
percent: 99.8
percent%: 99.8%
1
0


Log Predictions Time Series
400
300
200
100
Jun 30, 2025 1:00 AM
1: 2
12:48 AM
Mon Jun 30
2025
12:50 AM
12:52 AM
12:54 AM
12:56 AM
12:58 AM
1:00 AM
1:02 AM
_time
0
1


Time Series of Prediction Percentages
majority_prediction: 0
percent: 99.6
percent%: 99.6%
1
0

# 2. Testing


splunk>enterprise
Apps
Administrator
Messages
Settings
Activity
Help
Find
Search
Analytics
Datasets
Reports
Alerts
Dashboards
Search & Reporting
PC-Haint Health Studio
Display
157%
Actions
Edit
Global Time Range
Last 15 minutes
10:00 PM ...g 3 2025
9:00 PM ...g 3 2025
8:00 PM ...g 3 2025
2:00 PM ...g 3 2025
1:00 PM ...g 3 2025
12:00 PM ...g 3 2025
10:00 PM ...g 2 2025
10:00 AM ...g 3 2025
11:00 AM ...g 3 2025
200
100
192.168.159.134
192.168.159.133
192.168.159.132
192.168.159.1
34.107.243.93
src_ip
Log Predictions Time Series
80
60
40
20
10:34 PM
Sun Aug 3
2025
10:36 PM
10:38 PM
10:40 PM
10:42 PM
10:44 PM
10:46 PM
10:48 PM
_time
0
1
Time Series of Prediction Percentages
0
1

# 2. Testing

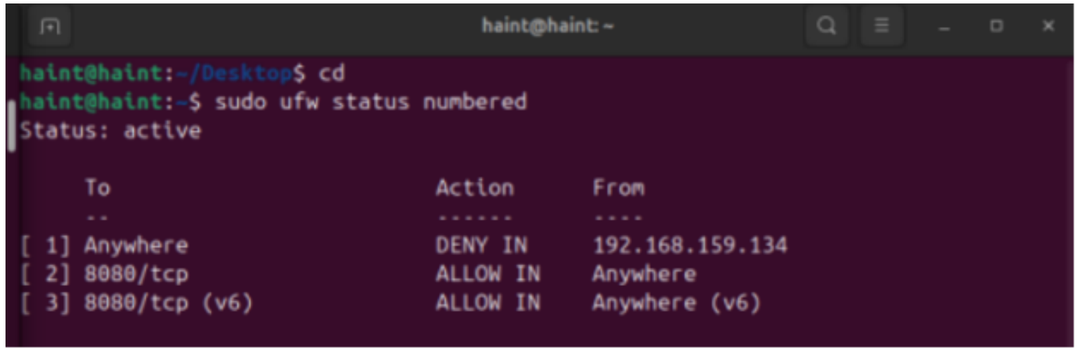

PC-Haint Health Studio
Display
157%
Actions
Edit
Global Time Range
Last 15 minutes
other (16)
11:00 AM ...g 3 2025
10:00 AM ...g 3 2025
10:00 PM ...g 2 2025
2:00 PM ...g 2 2025
3:00 PM ...g 2 2025
4:00 PM ...g 2 2025
5:00 PM ...g 2 2025
7:00 PM ...g 2 2025
8:00 PM ...g 2 2025
20
10
192.168.159.134
192.168.159.133
192.168.159.132
192.168.159.1
34.107.243.93
src_ip
Log Predictions Time Series
20
15
10
5
11:50 AM
Sun Aug 3
2025
11:52 AM
11:54 AM
11:56 AM
11:58 AM
12:00 PM
12:02 PM
12:04 PM
0
1
Time Series of Prediction Percentages
0
1

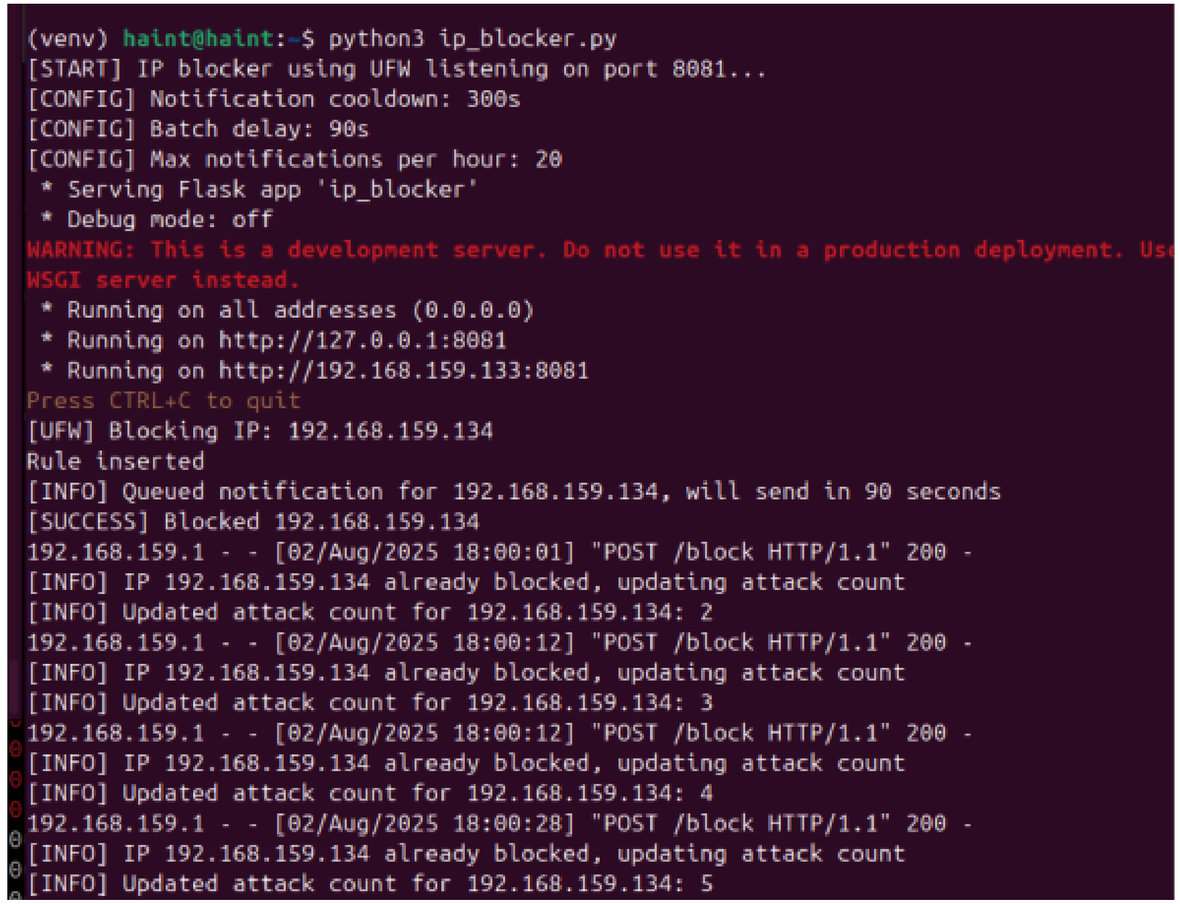
# 2. Testing


PC-Haint Health Studio
Display
157%
Actions
Edit
Global Time Range
Last 15 minutes
other (16)
11:00 AM ...g 3 2025
10:00 AM ...g 3 2025
10:00 PM ...g 2 2025
2:00 PM ...g 2 2025
3:00 PM ...g 2 2025
4:00 PM ...g 2 2025
5:00 PM ...g 2 2025
7:00 PM ...g 2 2025
8:00 PM ...g 2 2025
20
10
192.168.159.134
192.168.159.133
192.168.159.132
192.168.159.1
34.107.243.93
src_ip
Log Predictions Time Series
20
15
10
5
11:50 AM
Sun Aug 3
2025
11:52 AM
11:54 AM
11:56 AM
11:58 AM
12:00 PM
12:02 PM
12:04 PM
0
1
Time Series of Prediction Percentages
0
1

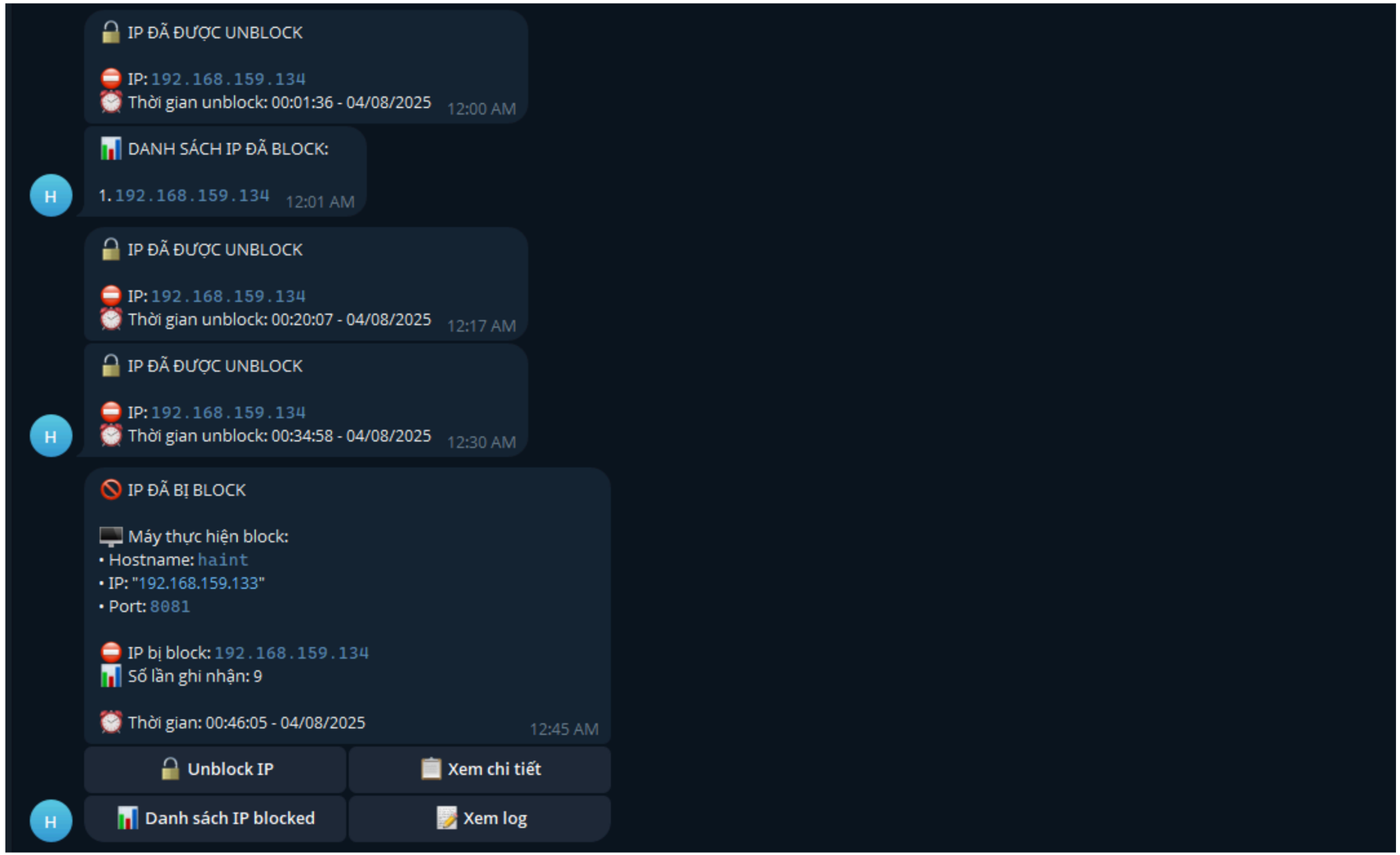
# 3. Block Suspicious IPs

If the IP is not yet in the block list, the system executes a firewall rule using iptables to deny any incoming traffic from that address.



# 4. Telegram Chatbot



# 5. Email Notification to Administrators

🚨 CRITICAL: Network Intrusion Detected Inbox ×

haintse172059@fpt.edu.vn Mon 4 Aug, 00:45 (13 days ago)
to me

🚨 NETWORK INTRUSION ALERT 🚨

📍 Attack Details:
Source IP: 192.168.159.134
Target IP: 192.168.159.133
Detection Time: 2025-08-04 00:45:05
Threat Probability: 0.0014959999825805426
Confidence Level: High

🤖 AI Attack Analysis:
ATTACK_TYPE: SCANPORT
CONFIDENCE: High
REASONING: The alert indicates "suspicious network traffic patterns" identified by an ML model that analyzed "77 parameters." This suggests a series of network interactions over time. While both `scanport` and `bruteforce` involve multiple attempts, there is no explicit mention of login failures or authentication attempts which would specifically point to `bruteforce`. A `scanport` operation, as a reconnaissance activity, typically involves probing various ports, creating diverse patterns across many parameters that an ML model would analyze to detect reconnaissance behavior. Therefore, given the generic nature of the "suspicious patterns" and the absence of authentication-specific keywords, `scanport` is the most likely attack type.

⚡ Automated Actions Taken:
- IP blocking command sent
- Event logged to Splunk
- Admin notification triggered

Built an intelligent monitoring and response system for endpoints on Splunk combined with Machine Learning.

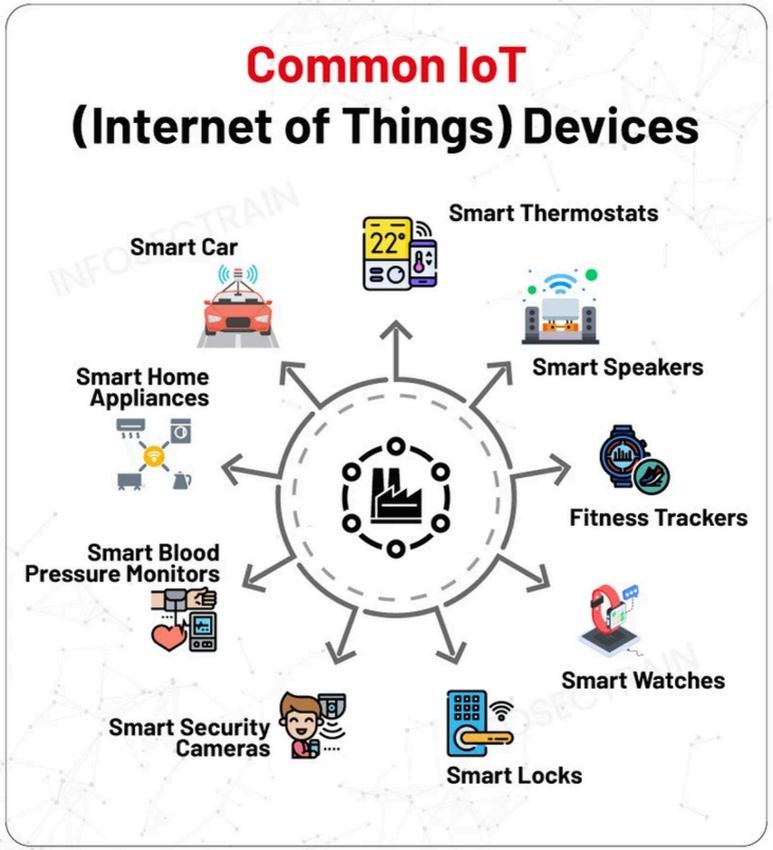
The system helps detect early - respond quickly - reduce manual dependence.

The model results achieved high accuracy (Accuracy, Precision, Recall, F1, AUC) → proving its effectiveness compared to traditional monitoring.

The automatic response mechanism (auto-block) supports preventing attacks in real time.

Limitations: Depends on training data, can generate false positives, needs to be optimized for large environments.

Future development: Dataset expansion, Deep Learning, IoT devices, smartphones and integration of other security systems.



FPT Education

FPT UNIVERSITY

# Thank you