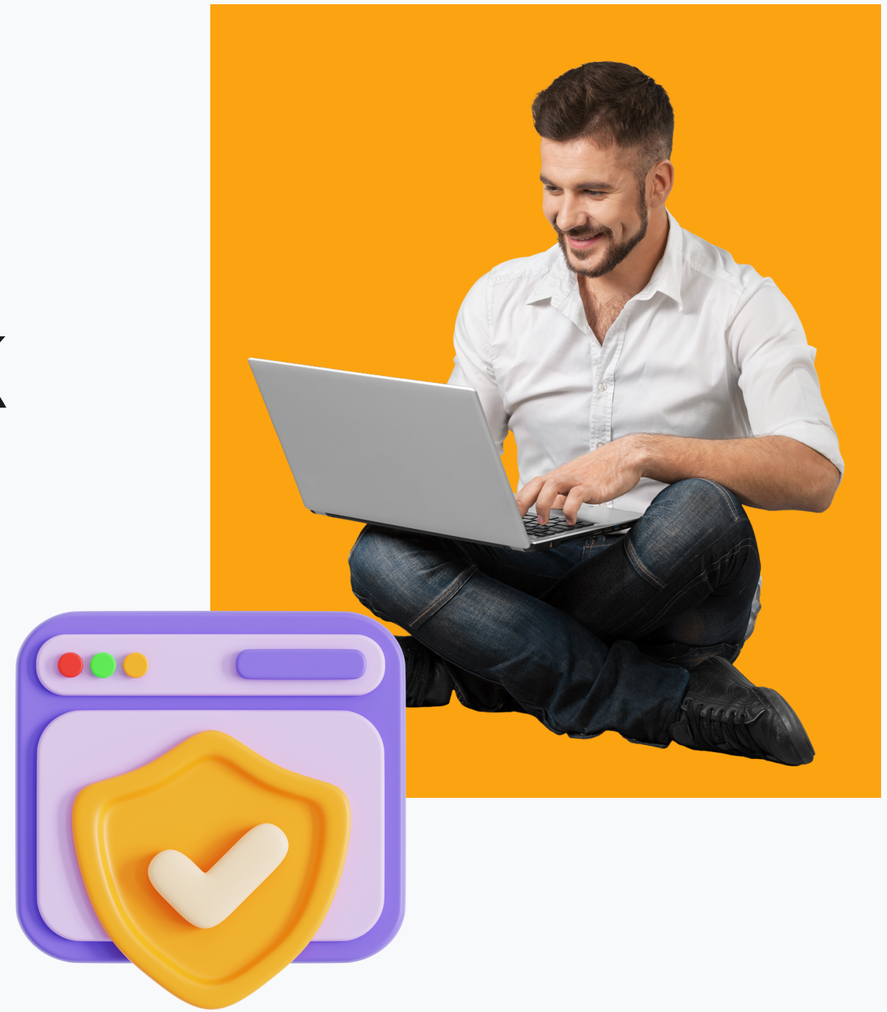
Nova Threatix

An Advanced Threat Detection Framework

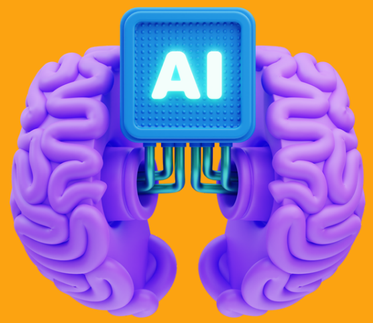
Forged by Nawfal, Ahmed, Zeehan, & Hassan when it comes to network security, our jokes are encrypted, but our projects are crystal clear.

Read More



Introduction

Designed for continuous monitoring and advanced threat detection.

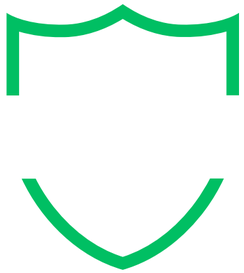


Integrates machine learning, boosting algorithms, & personalized Threat Intelligence.

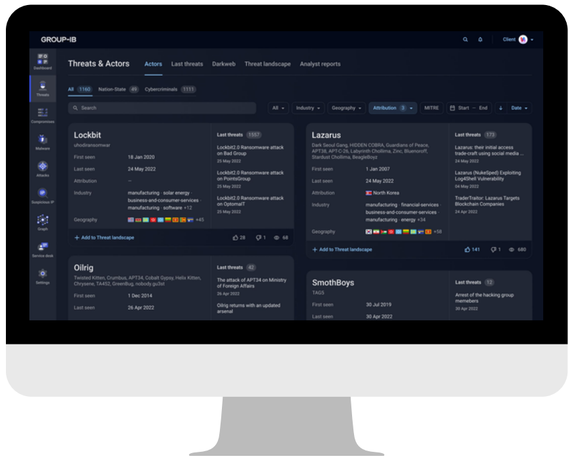
Utilizes the external threat intelligence for proactive threat identification.

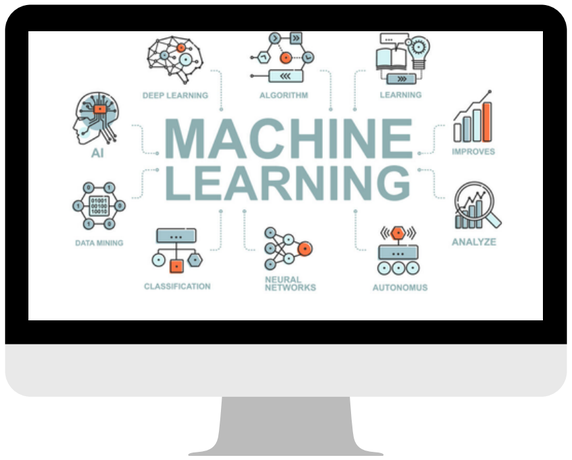
FRAMEWORK OVERVIEW FLOW

IDS/IPS LOGS

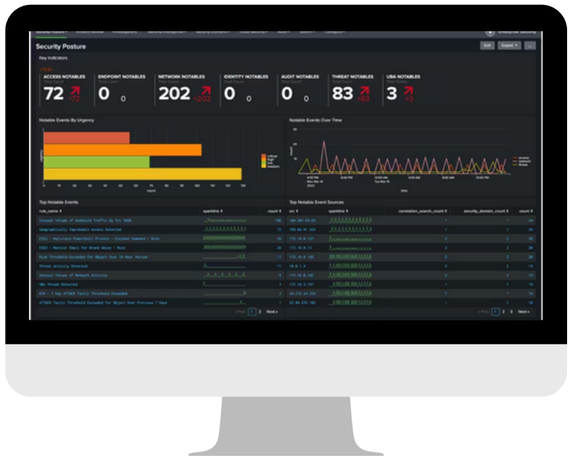


External Threat Intelligence



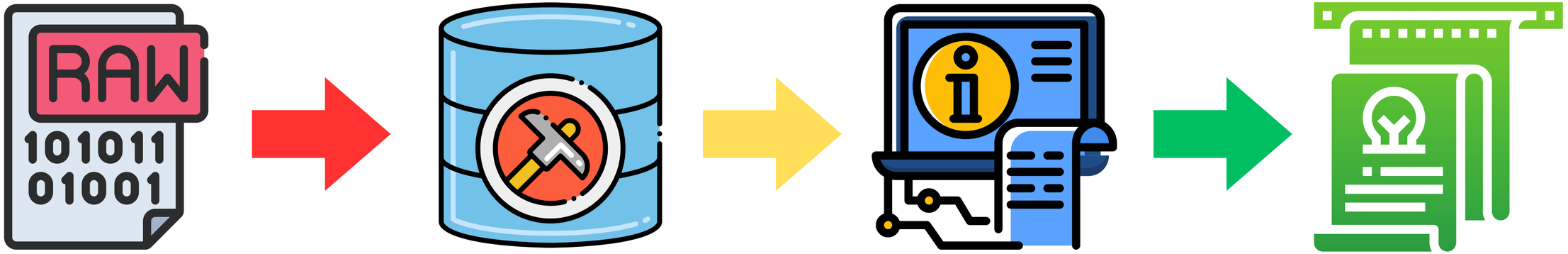


OUTPUT: SIEM



PROCESSING & MODELS

Methodology - Data Flow

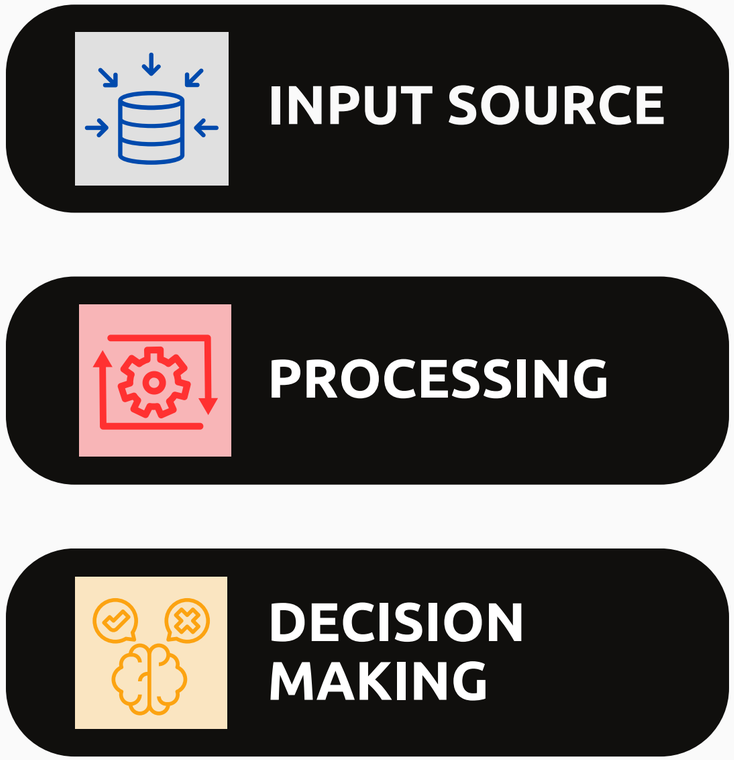


Acquisition of raw data from IDS/IPS

Preprocessing & feature engineering

Feeding processed data into ML-models

Output results of the model



Core Components of the Framework

- **Data Input Sources: IDS and IPS logs.**
- **Processing Modules: Data preprocessing, machine learning models.**
- **Decision-Making Components: Boosting models, ensemble methods, and stacking techniques.**

Diving Deep into the Framework: Data & Detection

INPUT SOURCE

- Data logged in our IDS/IPS systems is essential for our models to train & test based on them. Primarily we focus that our logs are properly brought in to the model, where first feature engineering & selection is performed. These logs are monitored & provided to the model in real time for continous detection with upgraded Threat intelligence.

TOP FEATURES	DESCRIPTION
- `IP_Risk_Score`	- Risk associated with a particular IP address.
- `Response_Effectiveness`	- Measures the effectiveness of the response to detected threats.
- `Source_Port_Risk`	- Risk associated with the source or destination port of network traffic.
- `Event_Risk_Score`	- A score assigned to specific network events based on their perceived risk.
- `Network_Layer_Score`	- Assessment of risk at different layers of the network.
- `Signature_Frequency`	- Frequency and diversity of detected attack signatures.
- `Protocol_Risk`	- Risk associated with different network protocols.
- `Anomaly_Index`	- Overall severity of threats or deviation from normal activity.

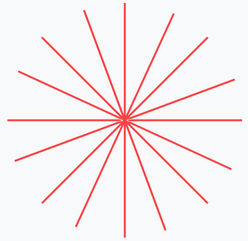
- **Boosting Models: Enhance accuracy by focusing on complex instances.**
- **Ensemble Methods: Aggregate predictions for robustness and reliability.**
- **Stacking Techniques: Layer models for a comprehensive defense strategy.**

- **Enhanced Detection: Improve threat detection with sophisticated algorithms.**
- **Predictive Power: Anticipate and prevent future threats for proactive security.**
- **Security-Centric: Every technique is chosen to bolster network safety and responsiveness.**

DECISION MAKING

Decision Making in Security

Algorithmic Approaches



#1
GRADIENT BOOSTING
Accuracy: 0.9994

#2
XG BOOST
Accuracy: 0.9994

#3
LIGHTGBM MODEL
Accuracy: 0.9993

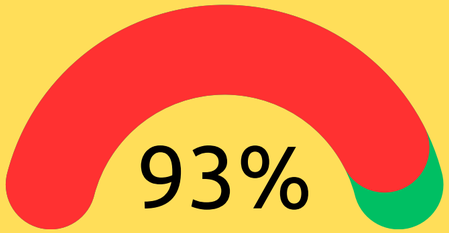
#4
ADA BOOSTING
Accuracy: 0.9992

#5
Neural Networks
Accuracy: 0.9652

#6
Random Forest
Accuracy: 0.9073

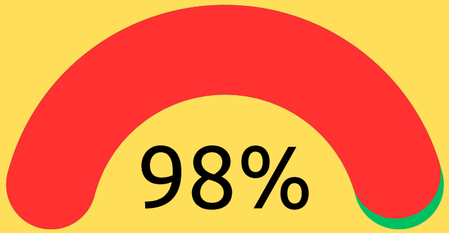
MODEL OUTCOMES

RANDOM DATASET



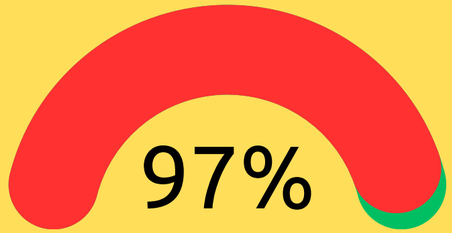
16K Rows of data, showed us that 93% servers were hacked (ACC: 99%)

ALL HACKED



16K Rows of data, showed us that when all server's were hacked, accuracy was 98%

NON-HACKED



16K Rows of data, showed us that when all server's weren't hacked, accuracy was 98%

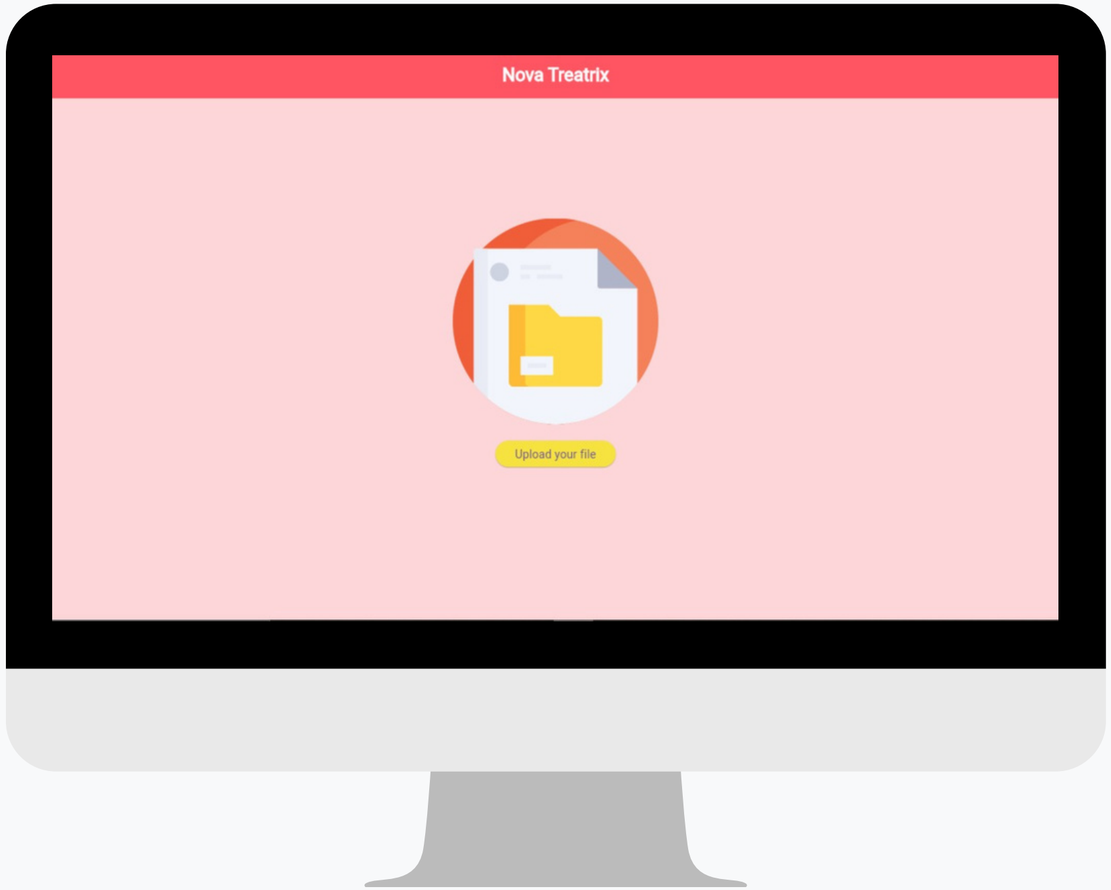
Practical Applications of Nova Threatix Model

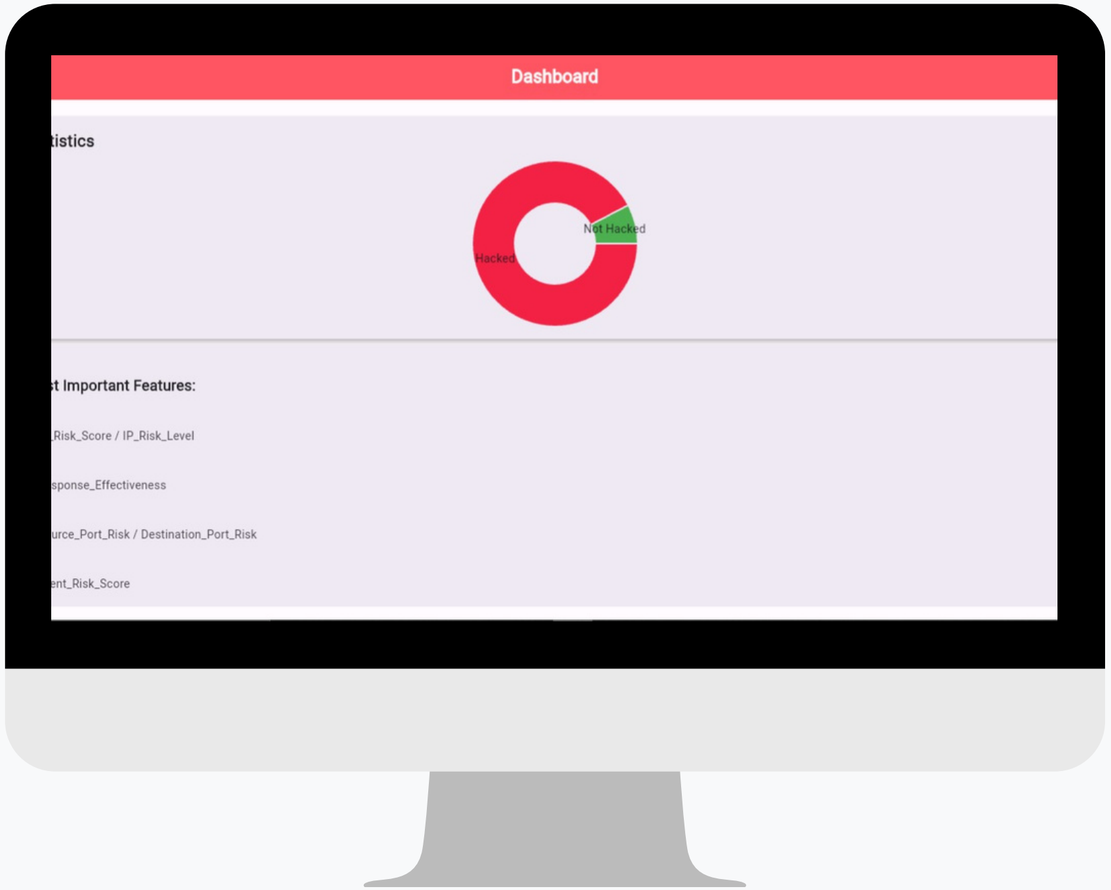
Large-scale enterprise security

Cloud-based infrastructure monitoring

Defense against advanced persistent threats (APTs)

NOVA THREATIX APP





Towards Real-Time Threat Detection

- *The necessity of continuous monitoring in network security.*
- *Adapting to evolving network conditions.*
- *Future development goals for the framework.*

Nawfal Ahmed Khan
Project - Lead