Infosys Springboard

SentinelNet: AI-Powered Network Intrusion Detection System

Building a Smarter Shield for Cyberspace

Presented by:
Amit Yadav
Intern, Infosys Springboard 6.0

SentinelNet Project: Main Goals

- AI-powered Threat Detection
- Real-time Monitoring & Response
- Detect Both Known and Novel Attacks
- Reduce Risk of Data Breaches

SENTINELNET

Key Objectives for SentinelNet

01 Data-Driven Intrusion Detection:

Leverages advanced analytics machine learning to identify and predict threats

02 Real-Time Monitoring:

Provides continuous, live overschem of network activity mimediate threat response

03 Robust Performance

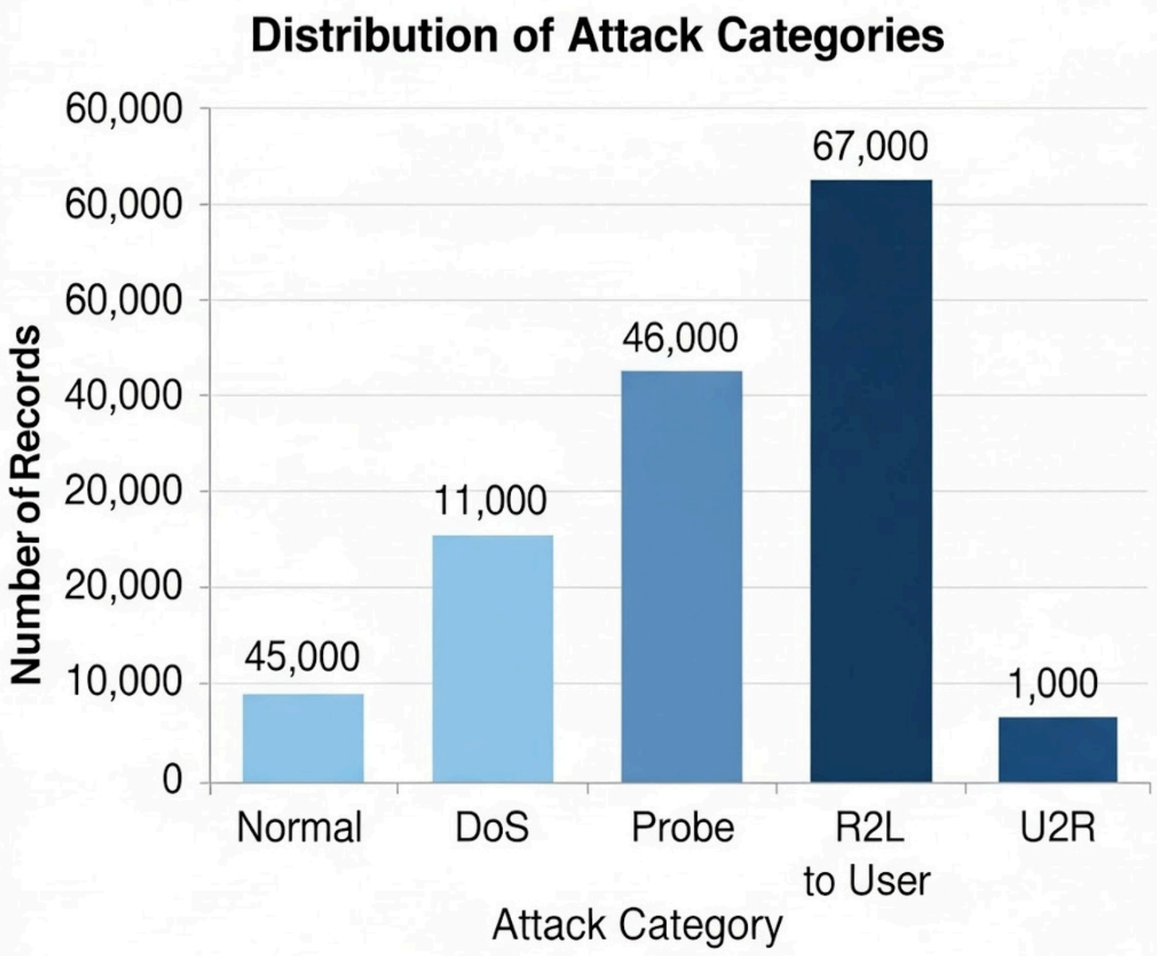
Ensures high accruacy of reliability under varjng network conditions

44 Scalabiity & Deployment:

Designed for easy integration and expansion across diverse environments

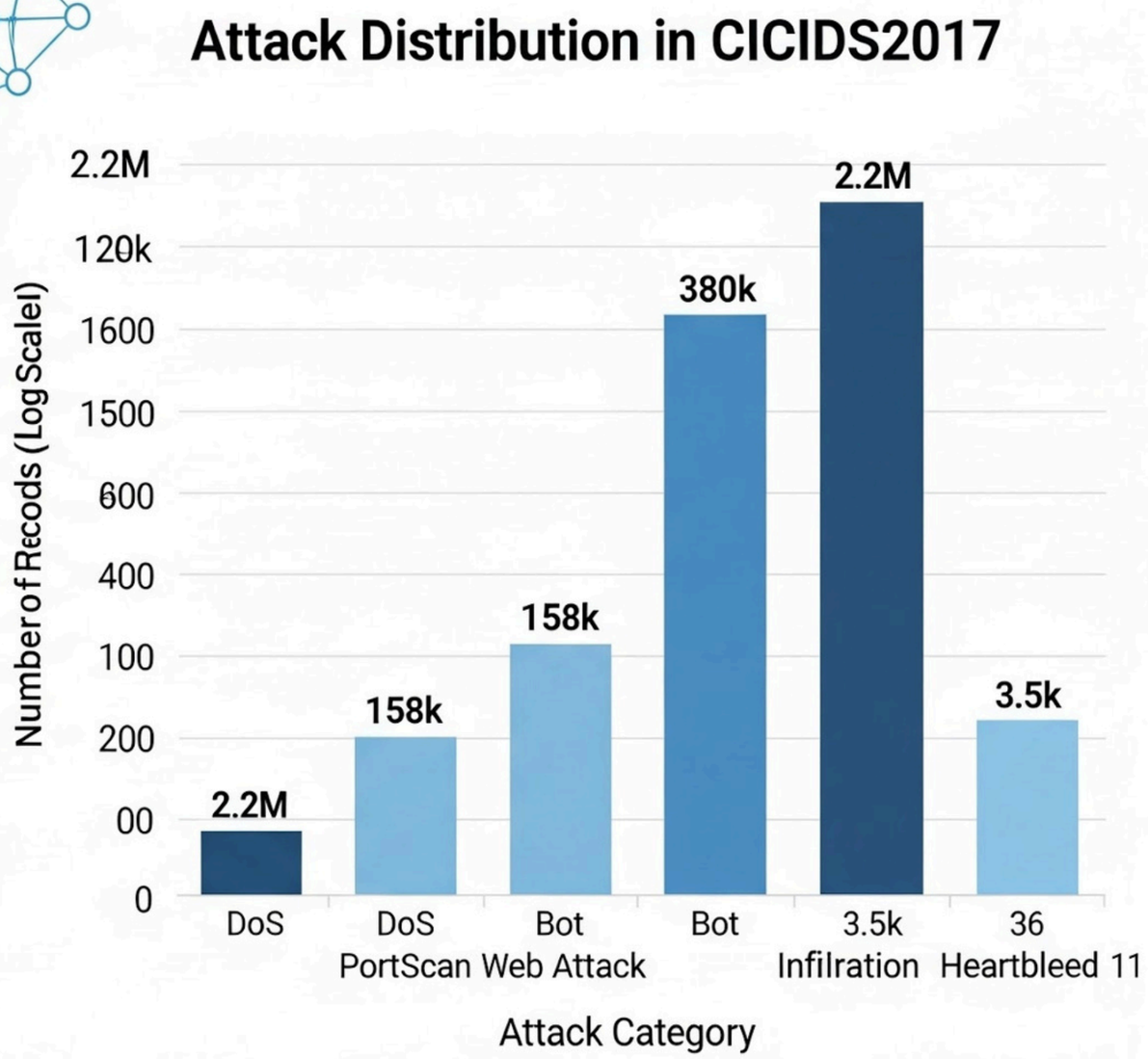
Introducing the NSL-KDD Dataset

- Historical benchamrk for network intrusion detection
- Contains 125,973 network connection records
- Each record has 43 features



Introducing CICIDS2017 Dataset: A Modern Benchnark for Network Intrusion Detection

- Modern & Realistic Benchmark
- Over 80 Flow-based Features
- Contemporary Attack Types: DoS, Botnet, Web Attacks



Dataset Comparison: NSL-KDD vs. CICIDS2017

Aspect	NSL-KDD	CICIDS2017
Era & Relevance	**Historical Benchmark** (1999)	**Modern Benchmark** (2017)
Data Nature	Synthetic, connection-based records	**Realistic**, based on raw PCAPS
Feature Type	41 hand-crafted features	80+ flow-based features
Feature Type		**Contemponrary attacks**
Attack Types	Older styles (e.g,., sendmail, per)	(e.g., Heartbleed, Botnet, Web Attacks)
Primary Use in SentinelNet	Ideal for initial model training and algorithm comparision due to simplicity and manageable size.	Essential for final validation and testing agains modest modern threats to prove real-world applicability.

SentinelNet®

Real-World Impact on Proactive Cyber Defense

Reduced Financial Loss

- Proactive threat intelligence and rapid respons capabiilties prevent cossly data breackts and fraud

Minimized Downtime

- Continuous monitoring and automated incident responss ensurre business continuity and operational resilience

Empowering Organizations with Adaptive Security Against Evolving Cyber Threats

Conclusion: - Your Future-Proof Solution

SentinelNet: Future-Proofing Network Security

Next Steps

- Model Training
- Performance Evaluation
- Deployment Strategy

Thank you!

Presented by:

Amit Yadav

Intern, Infosys Springboard 6.0