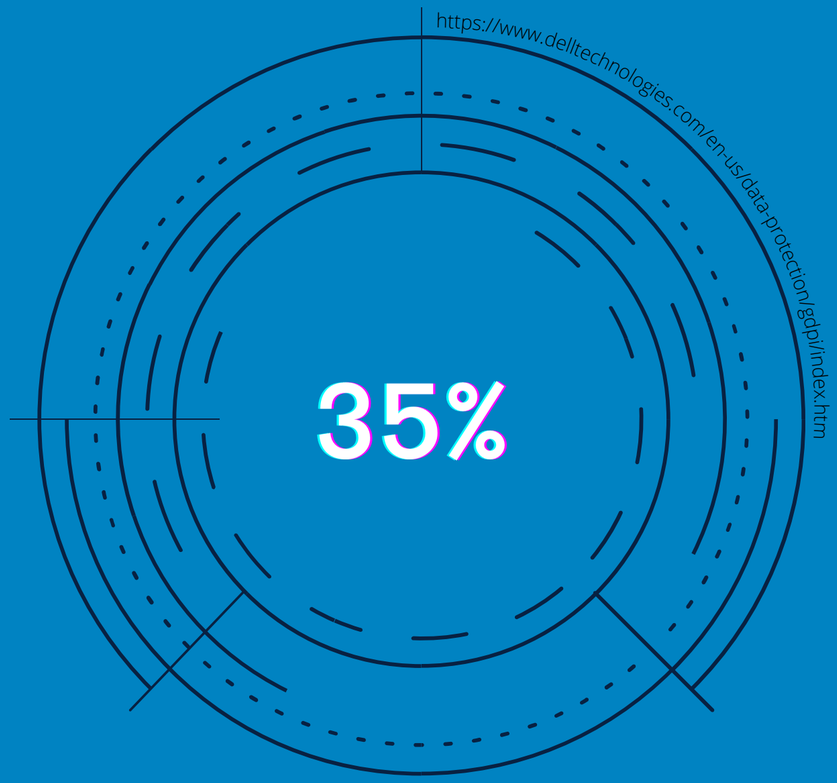
MACHINE LEARNING & DEEP LEARNING INTRUSION DETECTION WORKBENCH SYSTEM

April 1st, 2021

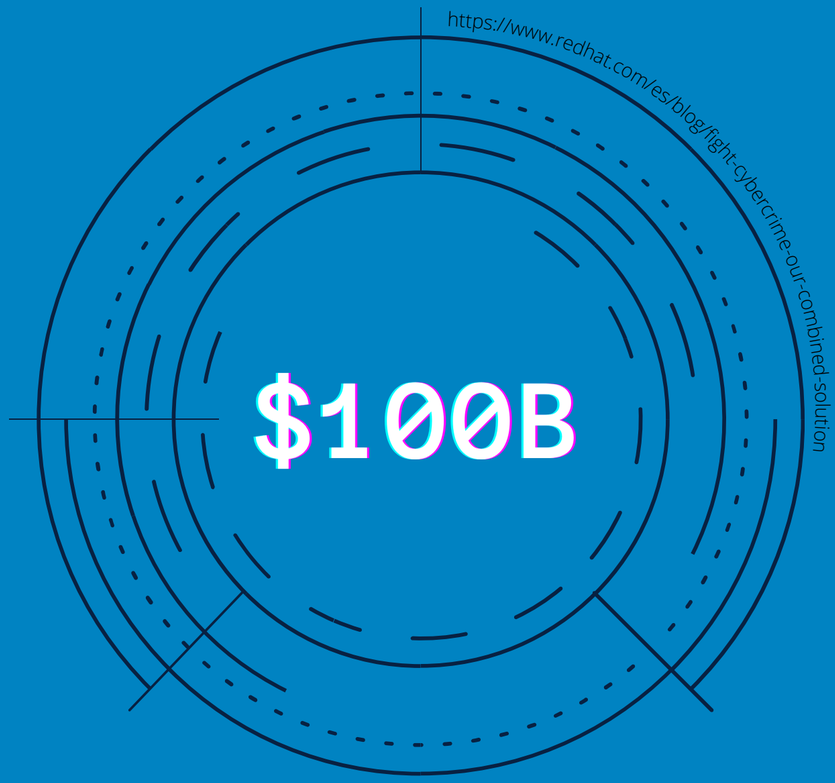
DELL EMC

PROBLEM STATEMENT

- Attacks are constantly changing.
- Security systems must detect known/zero-day attacks.
- Timely detection of attacks.
- Complexity of such systems.



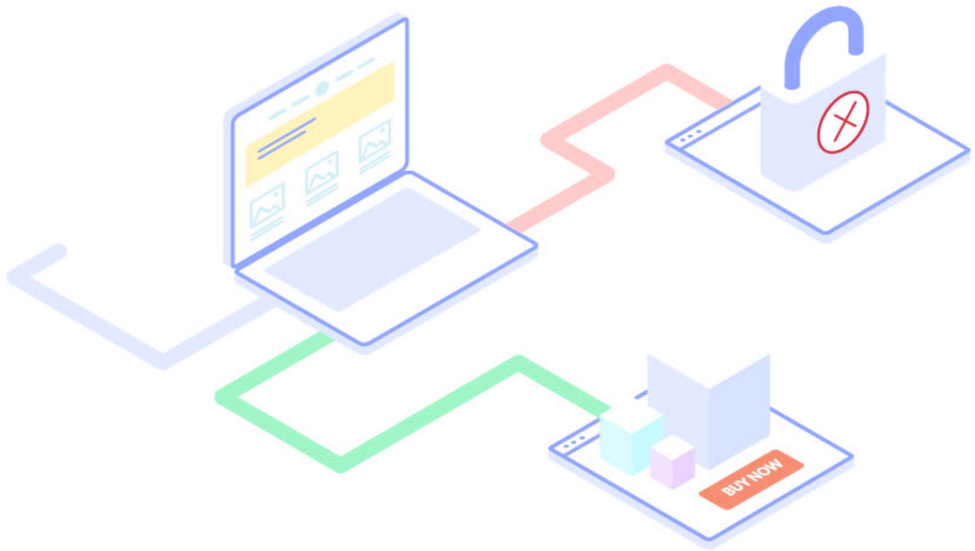
OF ORGANIZATIONS SUFFERED FROM CYBER-ATTACKS IN 2019 (ACCORDING TO DELL GDPI SURVEY)



ESTIMATED COST OF CYBERCRIME BUSINESS WORLDWIDE (REDHAT)

HOW TO PREVENT SUCH ATTACKS?

INTRUSION DETECTION SYSTEMS (IDS)



TYPES OF IDS

Signature-Based

Anomaly-Based

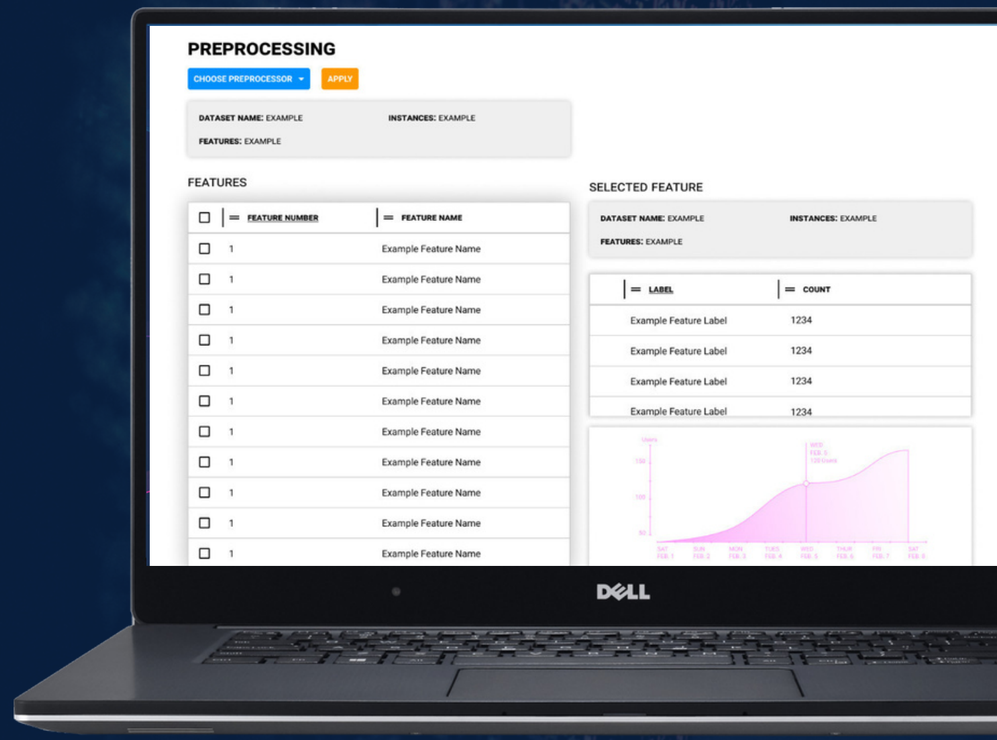
ANOMALY-BASED IDSs

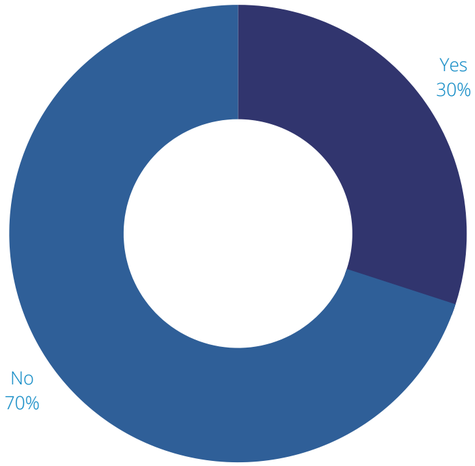
EFFECTIVE AGAINST ZERO-DAY ATTACKS

BUT.. ITS A NEW TECHNOLOGY UNDER DEVELOPMENT

TO FACILITATE THEIR DEVELOPMENT

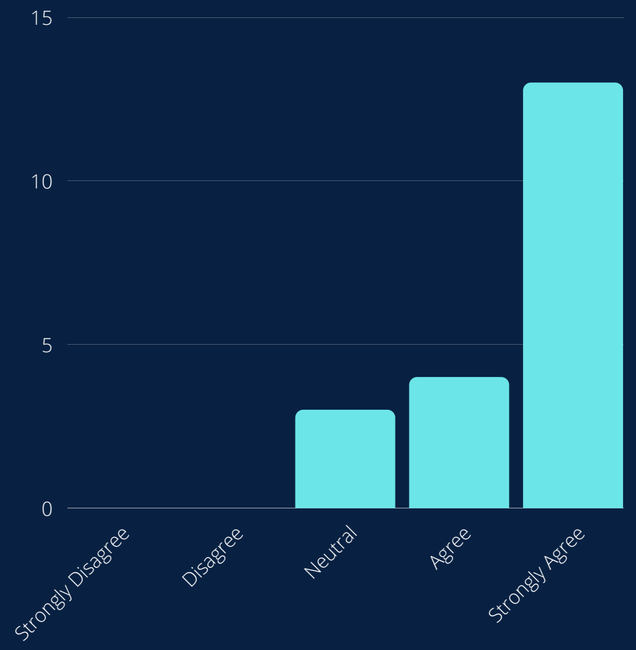
WE PRESENT A WORKBENCH SYSTEM FOR THE DEVELOPMENT OF ANOMALY-BASED IDS

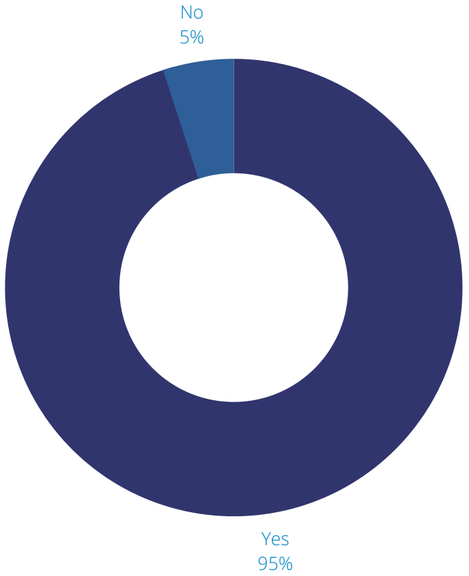




Ability of existing Firewall/IDS to detect and stop attacks

Importance of developing a workbench for machine and deep learning based IDSs





With-or-against the development of behavior-based IDS alongside traditional signature-based

LIVE PACKET ATTACK DETECTION

UTILIZING 3RD PARTY DATASETS

PERFORMING PREPROCESSING & CLASSIFICATION TASKS

ANALYZE DETECTION TIME AND ACCURACY PERFORMANCE

GENERATE METRICS AND ANALYTICAL REPORTS

INTEGRATES VARIOUS TASKS NEEDED BY SECURITY PROFESSIONALS

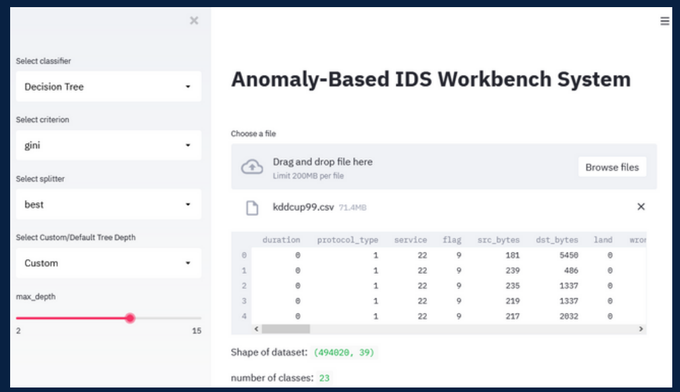
NO SIMILAR SYSTEM FULFILLS THIS MARKET NEED

UTILIZES OF STATE-OF-THE-ART DEVELOPMENT PLATFORMS

CUTS DOWN REPETITIVENESS AND DEVELOPMENT TIME FOR ANOMALY-BASED IDS PIPELINES.

01

02



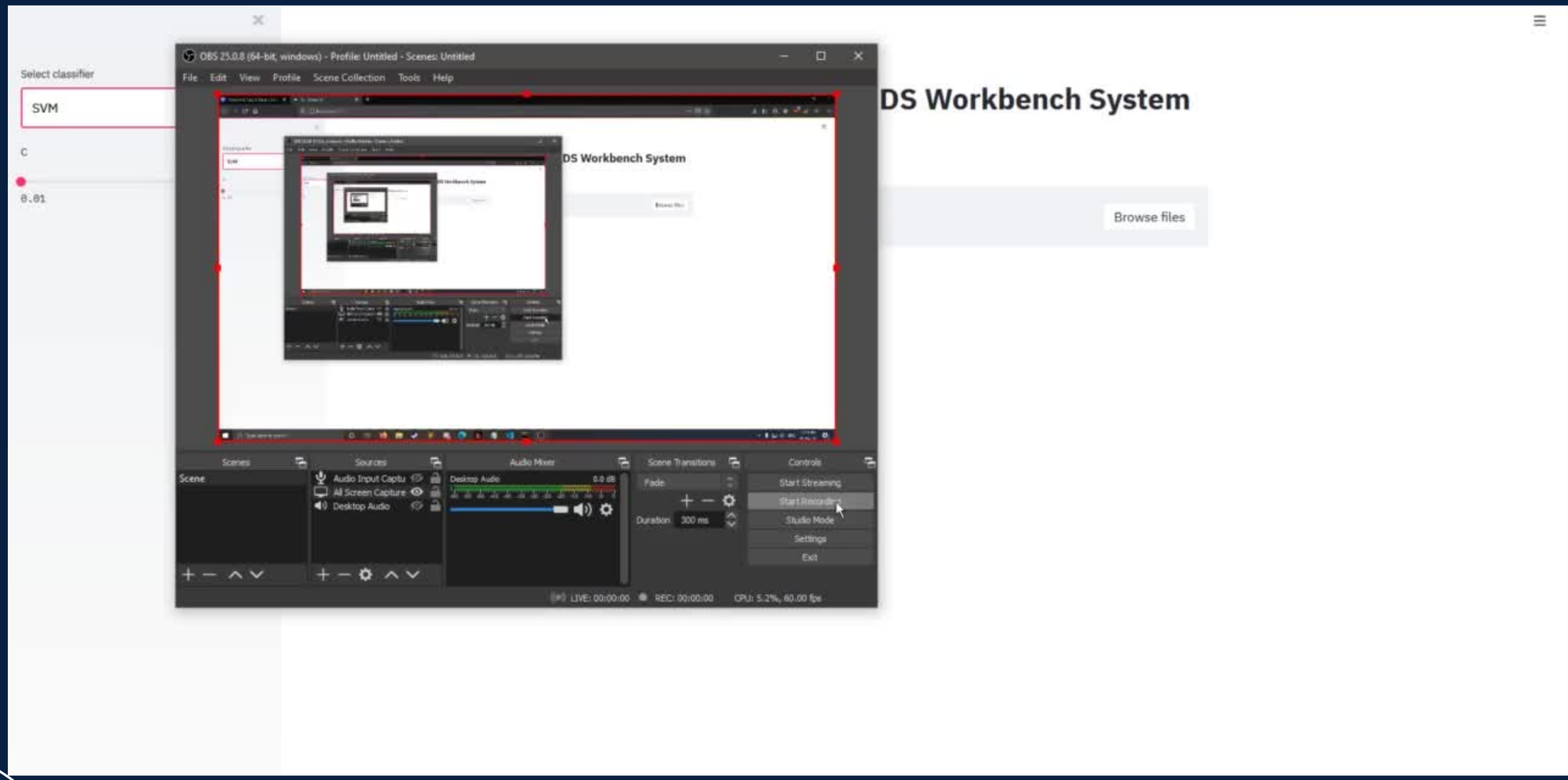
01 PUBLISHED PAPER

Comparative study regarding machine/Deep learning methods in anomaly-based IDSs (IEEE).

02 PRELIMINARY DEMO

A preliminary proof-of-concept system has been developed

02


Select classifier
SVM
C
0.01
DS Workbench System
Browse files
OBS 25.0.8 (64-bit, windows) - Profile: Untitled - Scenes: Untitled
File Edit View Profile Scene Collection Tools Help
DS Workbench System
Scenes
Scene
Sources
Audio Input Captu
All Screen Capture
Desktop Audio
Audio Mixer
Desktop Audio
0.0 dB
Scene Transitions
Fade
Duration 300 ms
Controls
Start Streaming
Start Recording
Studio Mode
Settings
Exit
LIVE: 00:00:00
REC: 00:00:00
CPU: 5.2%, 60.00 fps

FUTURE WORK

EXTEND

The workbench's capabilities

INTEGRATE

The workbench with CVE listings

EXPAND

The system to support IOT-based networks

ENHANCE

The available IDS network datasets

DEVELOP

Mobile-specific Anomaly-Based IDSs

MACHINE LEARNING &
DEEP LEARNING
INTRUSION DETECTION
WORKBENCH SYSTEM

THANK YOU FOR WATCHING

DELL EMC