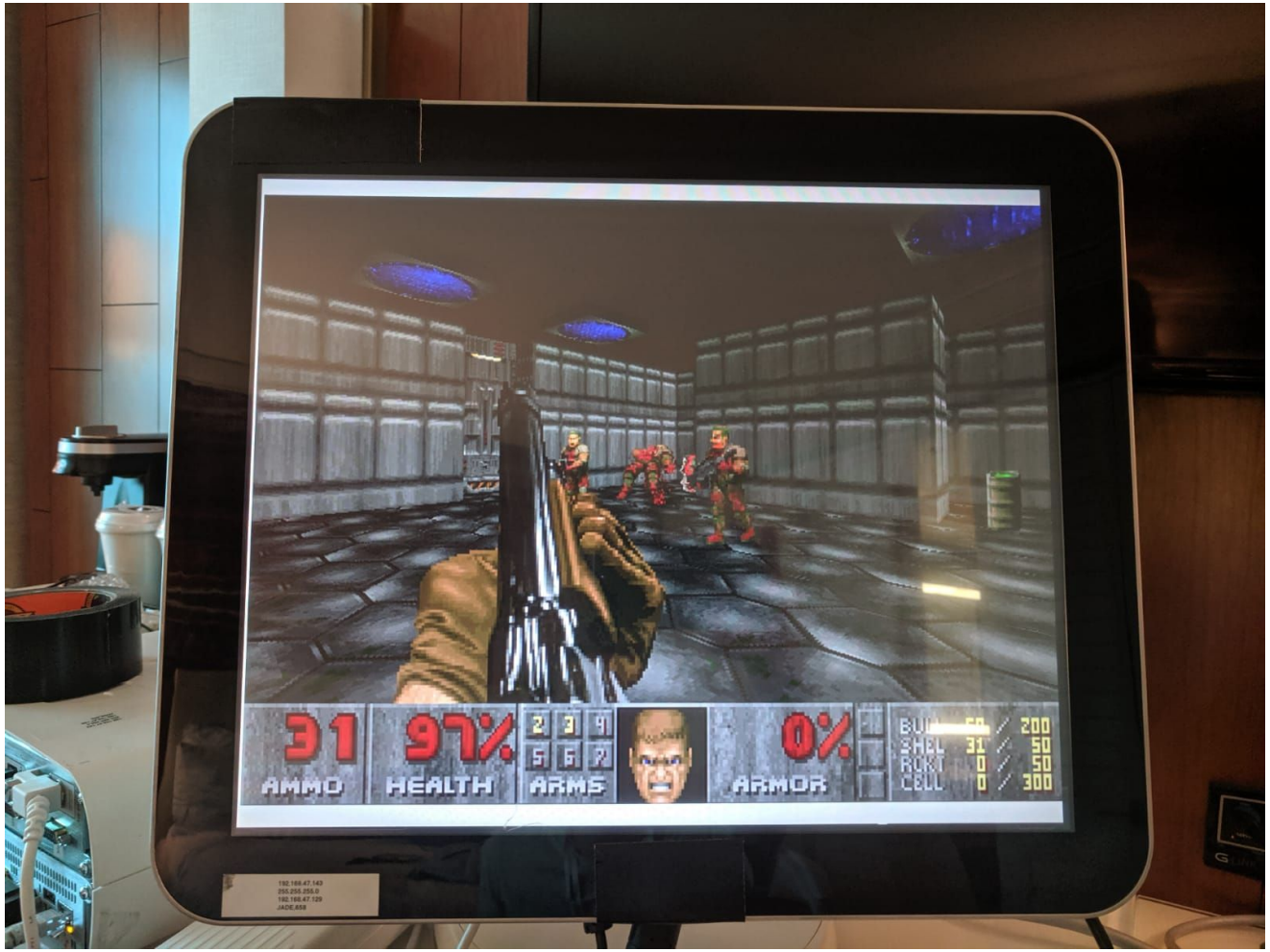
devices-gone-rogue

A challenge by 

Noa Weiss

Armis at a Glance

- IoT (Internet of Things) security
- Eliminating the security blindspot
  - Discover
  - Monitor
  - Protect
- Agentless & passive protection



URGENT/11

Data Science at Armis

- Identification
  - You can’t protect what you cannot see
- Anomaly Detection

Anomaly Detection

- Behavioral data
- Types of anomalies
  - Cyberattacks
  - Suspicious usage
  - Softer issues
- **Unlabeled data**

DataHack Challenge:

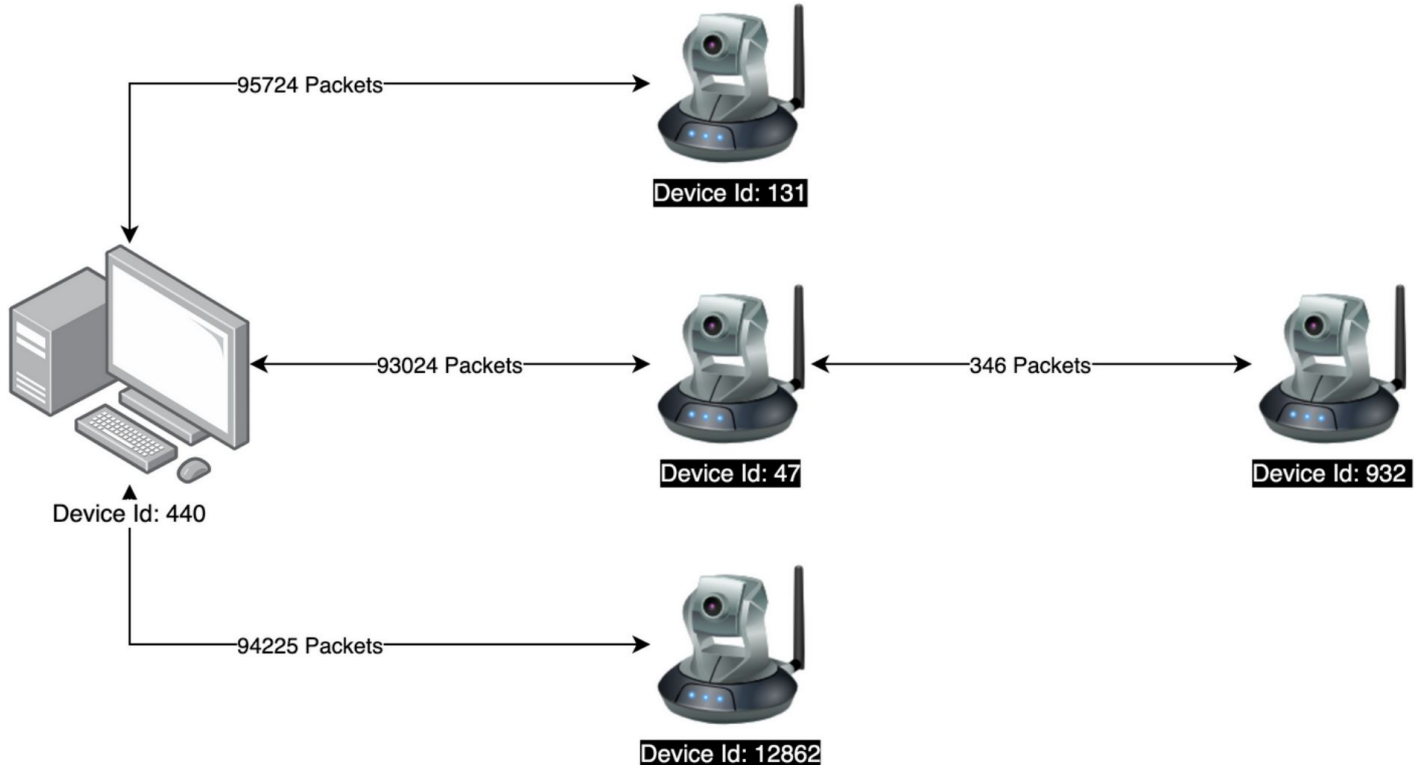
devices-gone-rogue

Your Mission, Should You Accept It

- Protect your clients: **find the devices that misbehave.**
- (No prior knowledge required).

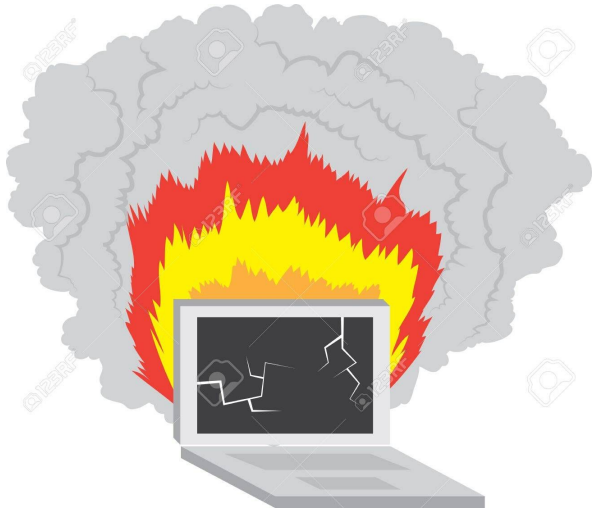
Your Data

- Behavioral
- Two CSVs:
  - Devices.csv
  - Sessions.csv
- Several networks



(Fully detailed at our repo).

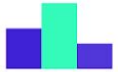
Each Anomaly is a Unique Snowflake



Evaluation

- Leaderboard (70%)
  - AUC (auto-matched against a pre-labeled set)
- Explainability (20%)
  - In what measures is this an anomaly?
  - How important is it?
- Innovation (10%)
  - Non-trivial algorithm
  - Ingenious useful features
  - Surprise us!

Prizes



1st

6000 nis

2nd

3000 nis

3rd

1500 nis

GO GET THOSE ANOMALIES!

This and more at https://github.com/armis-security/DataHack2019

Questions? Shoot us an email at **datahack@armis.com**.

ARMIS™