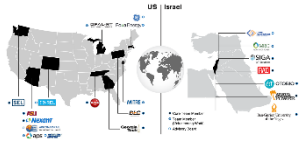
Task 3

Data Collection and Aggregation

Task status

6/9/2022

The Task Overview - Recap

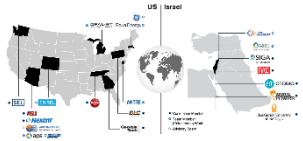


- Task Leader - ASU
- Participants - ASU, BGU, OTORIO, DK Innovation, DLC, Nexant, Delek, Arava
- Task Goal - Provide **reliable & comprehensive IT/OT datasets** that will include Cyber attacks simulated in various of ways and logged 360°
- Task objectives - Lab environments operations, Advisory emulation + Datasets generation

How -

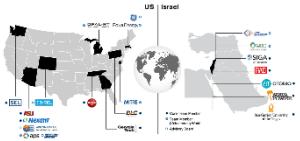
- Setting up multiple lab environments
- Setting up multiple sensors to monitor the network from different aspects
- Setting up RAM² as central logging system + build necessary plugins
- Execute live attack scenarios

Existing datasets



Dataset Name	Sensors Data	Network Data	Electrical Data
OTORIO Labs	X	V	X
Arava Power Dataset	X	X	V
Delek US Dataset	V	X	X
Energy Management	V	X	V
Gas Pipeline & Water Tank	V	X	X
HAI	V	X	X
OPC UA Dataset	X	V	X
Kaggle Faulty Sensor Dataset	V	X	X
Power System Attack Dataset	V	X	V
BATADAL Dataset	V	X	X
CISS Dataset	V	X	X
EPIC Dataset	V	V	V
WADI Dataset	V	X	X
SWaT Dataset	V	V	X

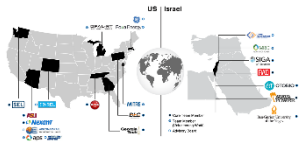
What's been Done



- ✓ Lab sheet - Standard document summarizing all labs and their contents
- ✓ Delek Lab - Architecture design + infrastructure purchase
- ✓ Meptagon Lab - In final stages of construction
- ✓ OTORIO lab - initial attacks pcaps
- ✓ ASU Lab - RAM² deployment in progress
- ✓ **Grid Lab** - Discussions with Resource Innovation & DLC started
- ✓ Open-Source datasets - Overview and mapping by BGU

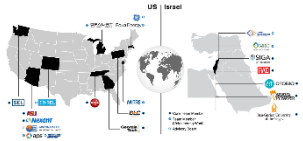
- ✓ New addition! Industrial-Wireless devices in the OTORIO lab

Current labs status



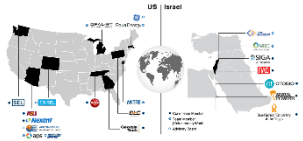
Lab	When it will be ready estimation	Attack simulation estimation
OTORIO	July 2022	August 2022
Delek US	August 2022	September 2022
ASU Lab	May 2022	October 2022
Meptagon	July 2022	August 2022
Grid Lab	October 2022 ?	February 2023
Arava	-	-

Commercialization Plan



- **Datasets commercialization**
  - Multiple IT/OT sources
  - Both raw data and processed
  - Multiple attack scenarios (tagged)
  - Multiple Verticals, processes

Major Next Steps



- Grid Lab -
  - Together with Nexant, DLC, ASU, BGU
  - Finalize architecture, location, simulations needed
- First attacks simulation + sharing results and hear feedback