Task 4

Multi-Level Threat Intelligence Knowledge Base

Arizona — ASU, Nexant, Arizona Israel Technology Alliance

Colorado — NREL

Georgia — Georgia Tech

Tennessee — Delek

Massachusetts — Fova Energy

Michigan — OPAL-RT Technologies

Pennsylvania — DLC

Washington — SEL

Washington, DC — MITRE

meptagon — head for a better process

Contel Technologies

MRC — Alon Tavor Power

SIGA — OT Solutions

Ben-Gurion University of the Negev

OTORIO

Arava Power

cybereason

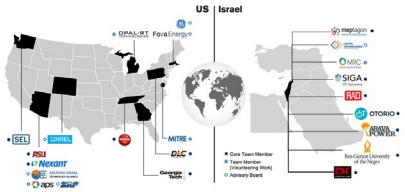
RAD

DK Innovation

Q1 - Jan. 24, 2022

BIRD Israel-U.S. Binational Industrial Research and Development Foundation

Reasoning and acting based the highest levels of the pyramid of pain



Tactics and Techniques

Machine Learning
Anomaly Detection
Intrusion Detection

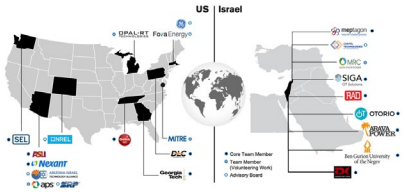
Low level OT/IT measurement data

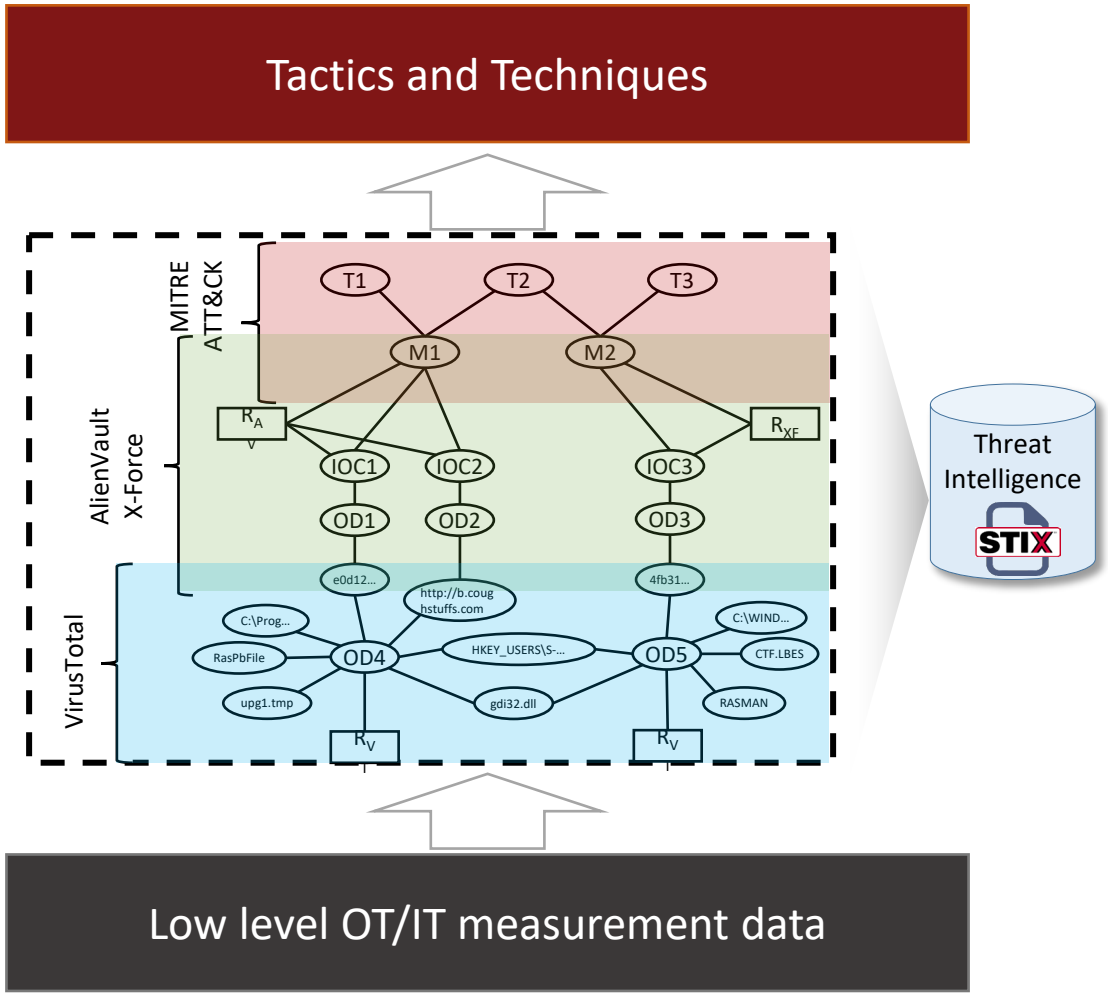
MITRE ATT&CK for ICS | **Mitigations**

- Requires extensive data
- Measurements of (emulated) attacks
- ICS Cyber Labs with many operational use cases
- Real data requires strict privacy controls

The **variety of attacks** that we can generate
The **variety of vendors and** operational **environments** we can monitor
are very limited

Multi-Level Threat Intelligence Knowledge Base



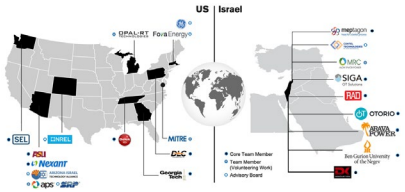


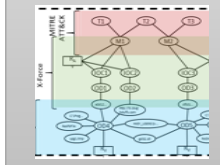
Build machine readable multi-level ICS threat ontology by fusing data from multiple cyber **threat intelligence** sources.

Challenges:

- Few Threat Intelligence sources compared to Enterprise
- Diverse types of observables (vendors/protocols/environments)

Strategy to building the knowledge base



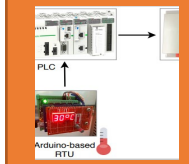


ICS Attack Ontology

Threat Intelligence

CTI feeds and databases

Extracting and fusing publicly reported observations



ICS Cyber Labs

CALDERA

Task 3

CALDERA

Generating missing observations

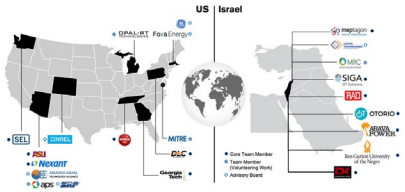
Experts

Task 2

COPE

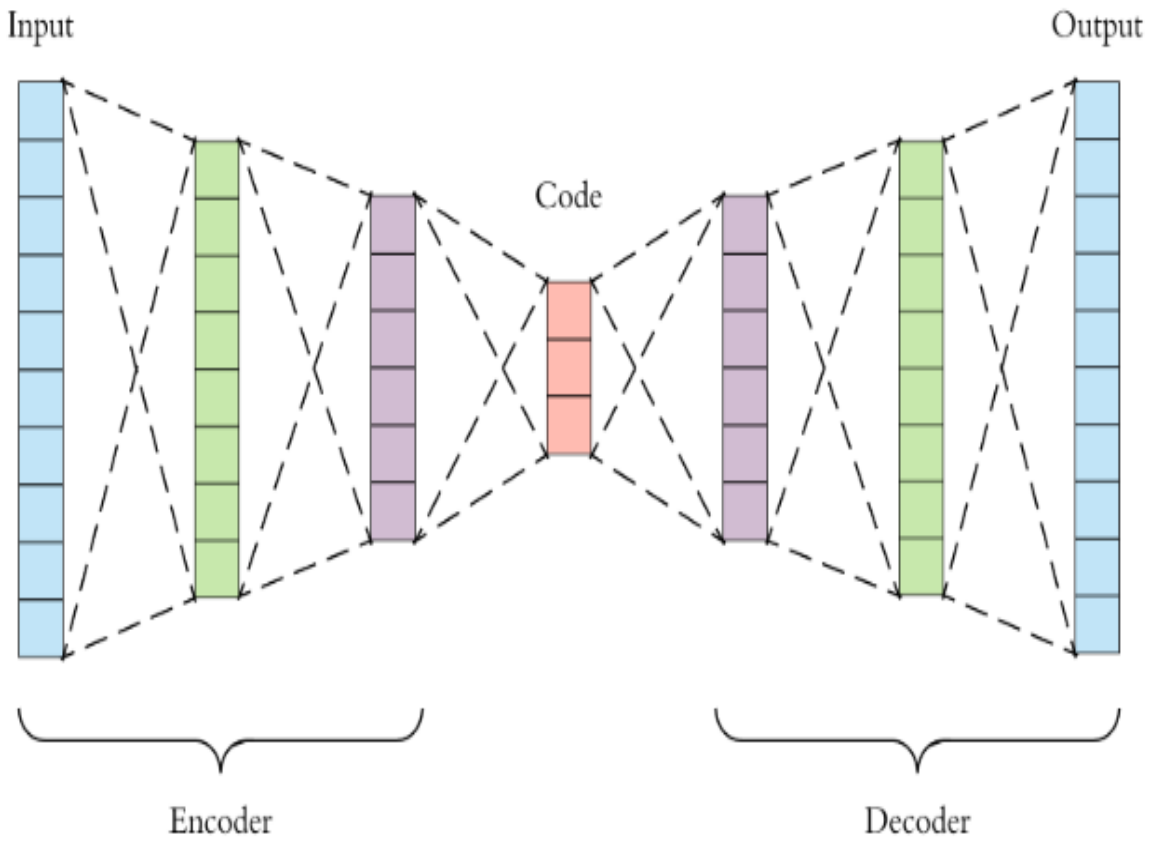
How may an attack technique be reflected in OT/IT measurements?

ICS Attack Ontology – what is it good for?



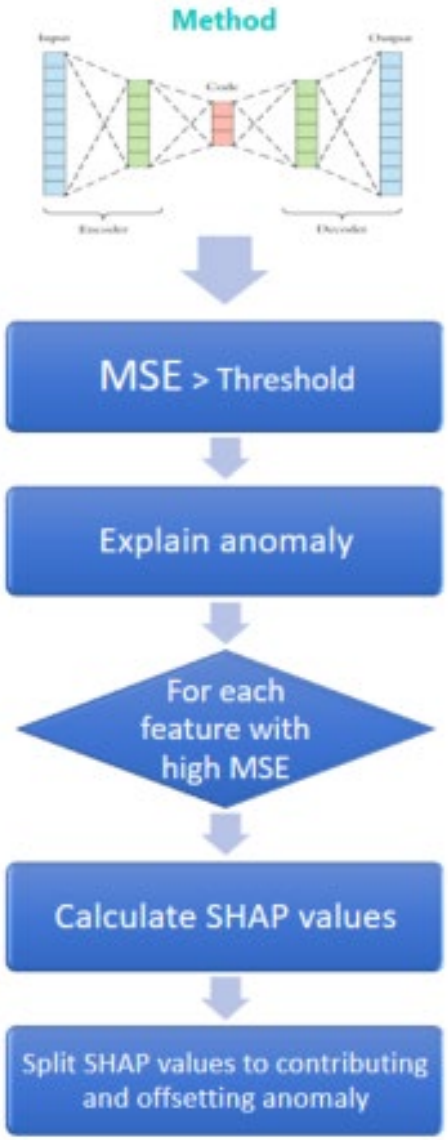
- Inferring the ATT&CK techniques from measurements.
  - Already showed good results in the enterprise domain
- Threat hunting (Task 6)
  - Know what kind of measurements to inspect and what to look for
- Explaining anomalies (Task 12)
  - Do the reasons for the detected anomalies correspond to the same Technique?
- Improving the anomaly detection and explanation (Tasks 10, 12)
  - Using the ontology to put more or less attention to certain measurements.

Anomaly detection using autoencoder

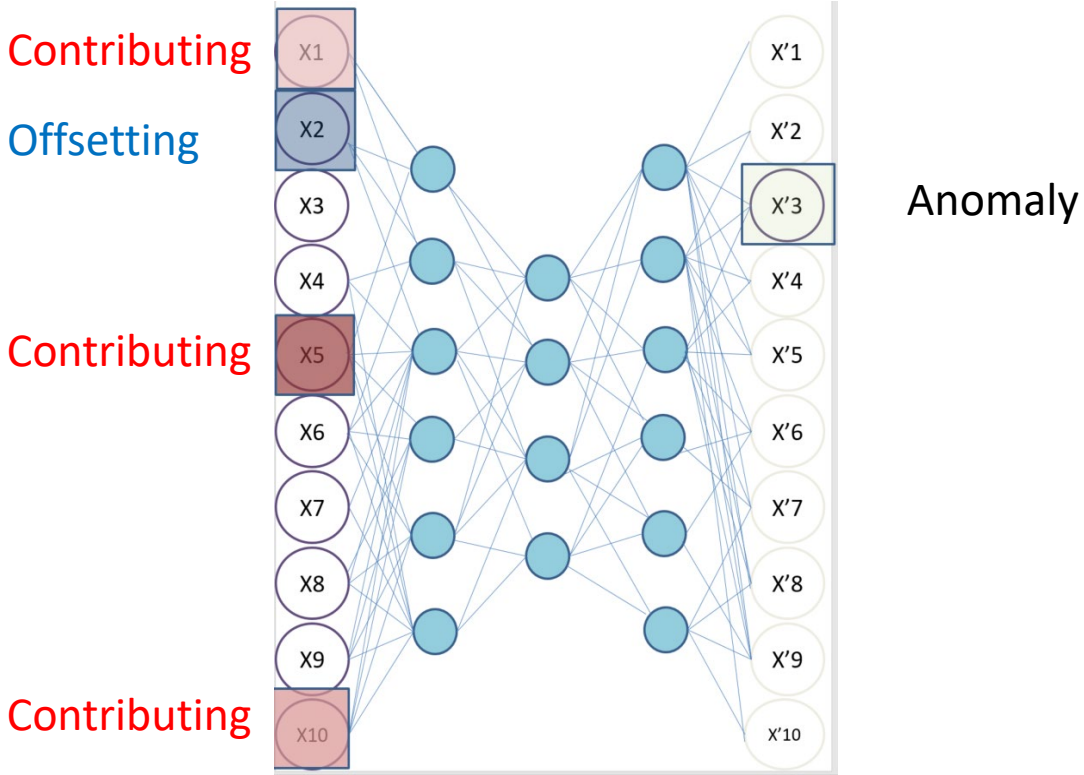


- Unsupervised learning
- Neural network trained to represent the normal data in lower dimensionality (encoding)
- and reconstruct the data into the original dimensionality (decoding)
- Normal instances are properly reconstructed
- Outliers are marked as anomalies

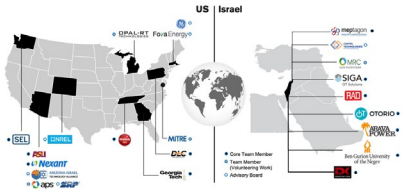
Explaining anomalies using SHAP values



Identify features contributing/offsetting the anomaly



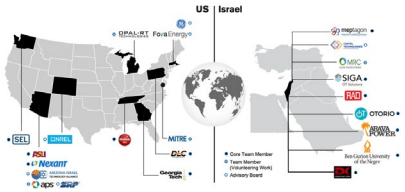
Explaining an anomaly



Feature name	Error	Real value
X'3	0.99	1
X'6	0.8	0
X'8	0.38	0.84
X'7	0.25	0.85
X'2	0.1	1
..	..	..

Explaining X3 reconstruction error

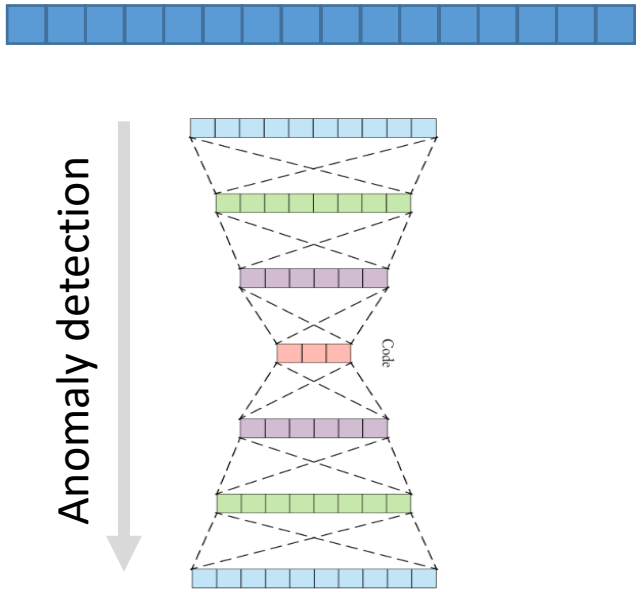
Explaining and improving anomaly detection



Input data

- ✓ Event
- ✓ Time window
- ✓ Environment state

Observable artifacts

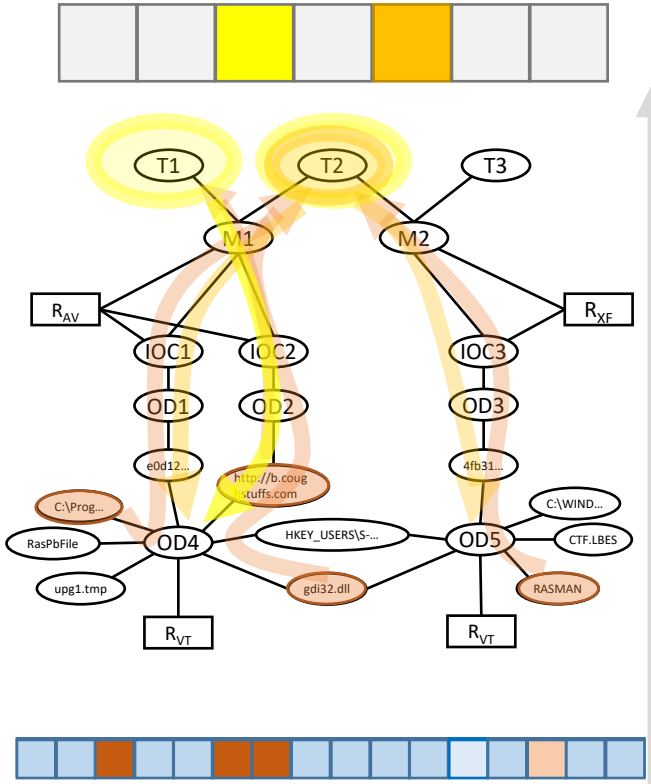


Improved anomalies

3. Improved explanations will be used as the **attention** weights to improve the anomaly detection.

Anomaly explanation

1. Inferred techniques
(a.k.a. Attack Hypotheses, IoA)

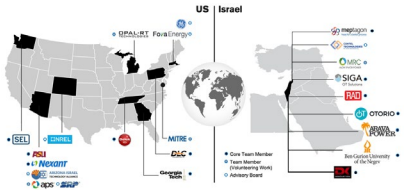


2. Improved explanations

Multi-layer naïve Bayesian classification

Explained anomalies

Commercialization plans



- OTORIO
  - RAM^2 analytical plugins
  - Ongoing discussion

- MITRE
  - Discussion started