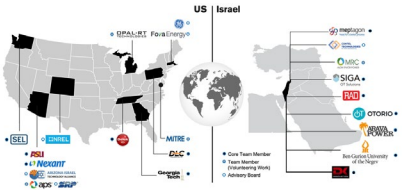
Task 4

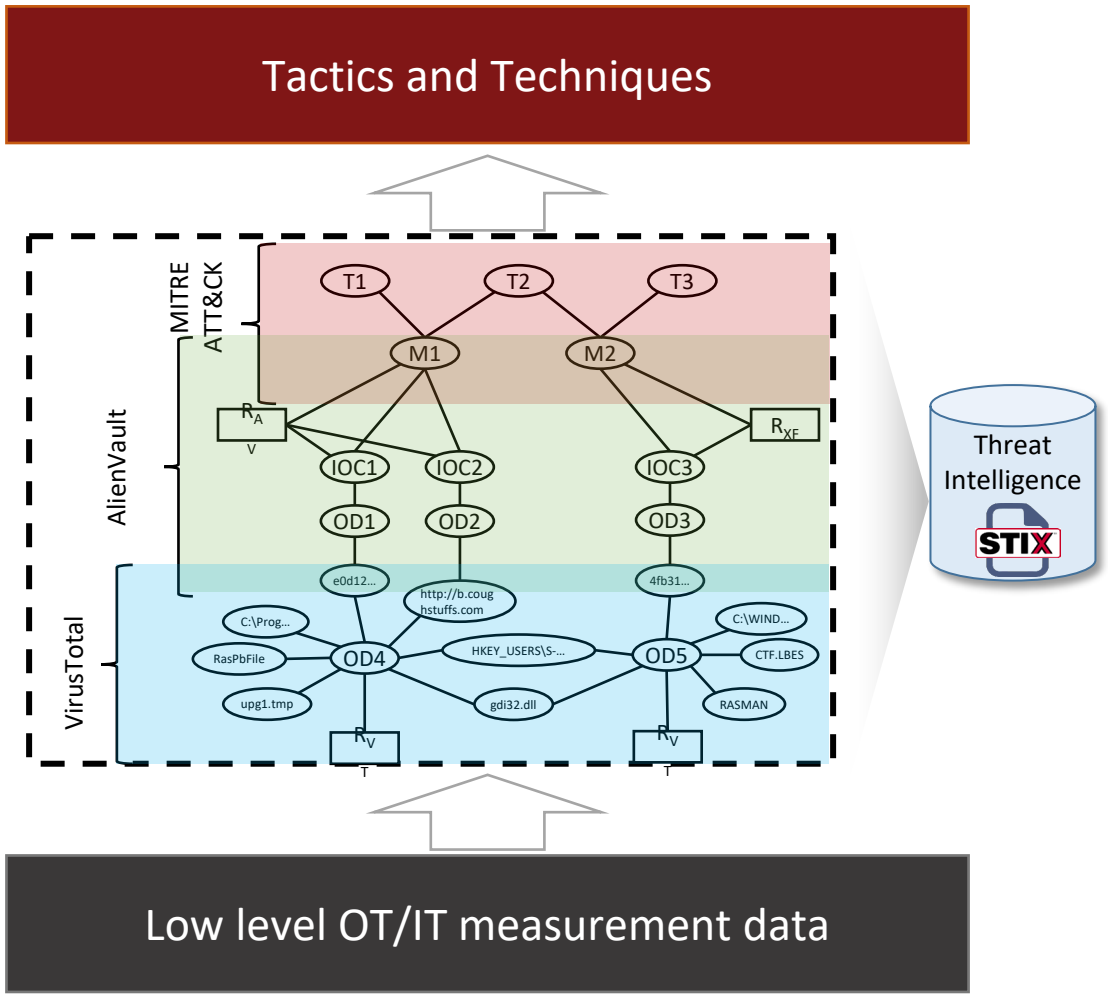
Multi-Level Threat Intelligence Knowledge Base

May. 9, 2022

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

Multi-Level Threat Intelligence Knowledge Base



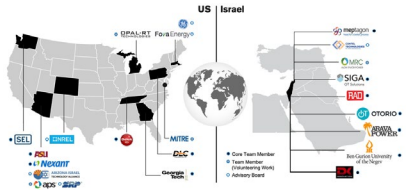


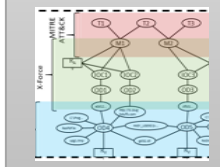
Build machine readable multi-level ICS threat ontology by fusing data from multiple cyber **threat intelligence** sources.

Challenges:

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

Strategy to building the knowledge base (orig.)

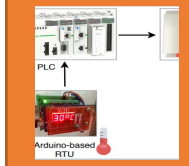




ICS Attack Ontology

Threat Intelligence

- CTI feeds and databases
- Extracting and fusing publicly reported observations



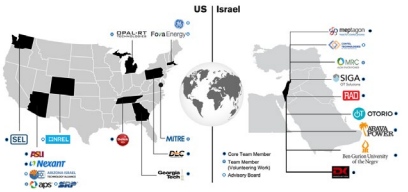
ICS Cyber Labs

- Task 3 CALDERA
- Generating missing observations

Experts

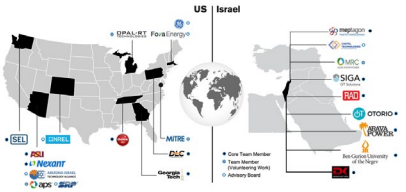
- Task 2 COPE
- How may an attack technique be reflected in OT/IT measurements?

CTI collection status



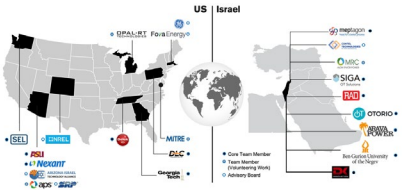
- Implemented collection of CTI data for Enterprise and ICS worlds:
  - MITRE ATT&CK
  - Alienvault
  - VirusTotal
- Implementing graph generation over Neo4j
- We made some adjustments to new APIs and Neo4j version

Enterprise status



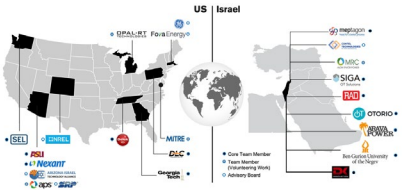
- Current status
  - Start the attack graph with malware and analytics
  - Upload pulses to graph and connect them to malware
  - Fetch IOCs for pulses and connect them to the pulses
- Additional work to be done
  - Get VT reports and load them to the graph
  - Add techniques to graph
  - Graph cleaning

Enterprise knowledge base statistics



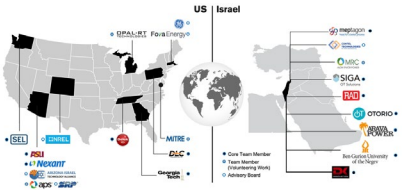
- Statistics
  - 981 malware
  - 3379 reports
  - 285677 IOCs

ICS status and statistics

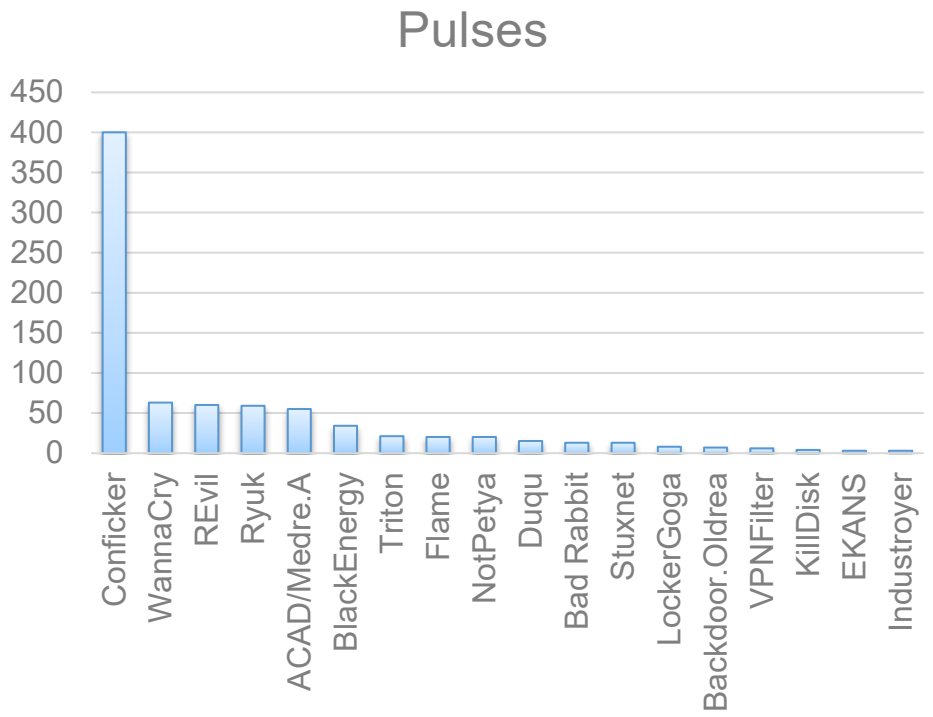


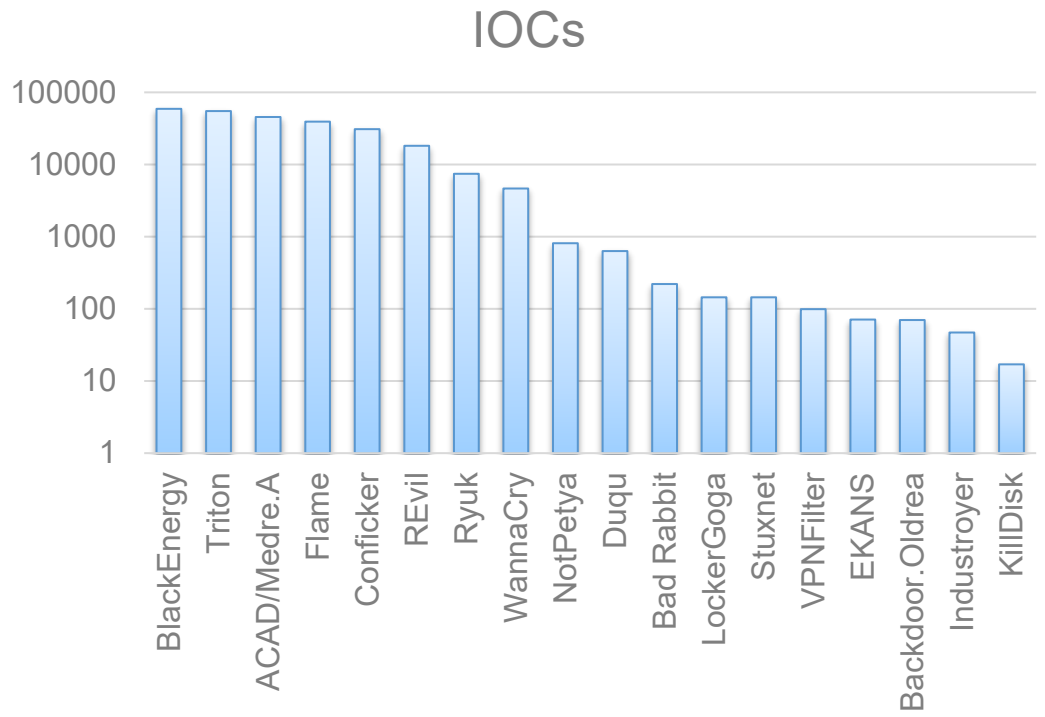
- CTI information for the ICS world is limited to the IT domain
  - Windows/Linux malware signatures
  - IT network-level signatures
  - No OT network-level signatures or OT machine level signatures
  - Need to bridge the gap using other sources (will be elaborated later)
- IT level information gathered:
  - Malwares, groups
  - Hashes and other IOCs
  - Behavioral reports

ICS statistics

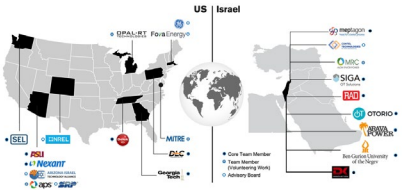


- 19 malware families collected from ATT&CK ICS
- For each malware family, we collected pulses from Alienvault and downloaded IOCs

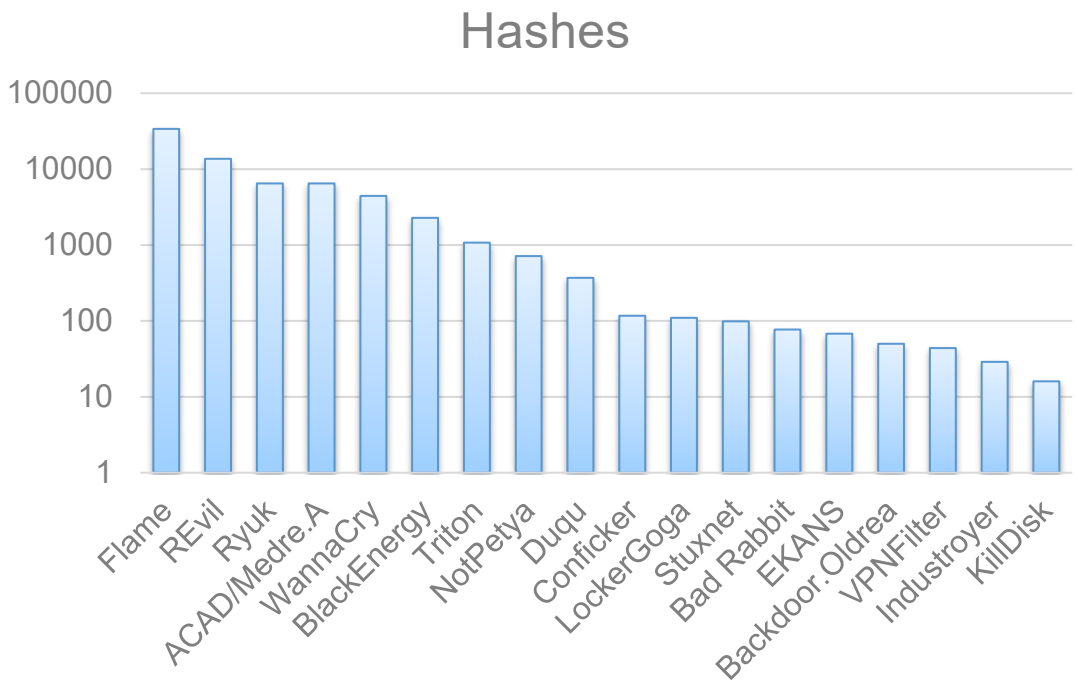




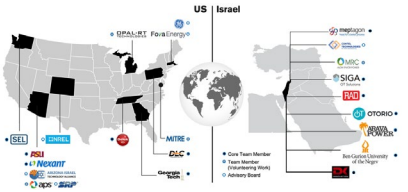
Hashes and behavior reports



- For each hash signature we extract VT report
- Out of ~67K hashes, we extracted ~47K VT reports
- We are still working on loading these reports to the graph DB
  - We are extending prior work with more extracted information from VT

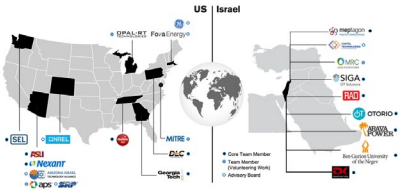


New malwares



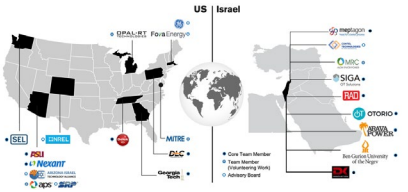
- There are new ICS malware from the past few months which do not yet exist in ATT&CK ICS
  - Industroyer2 (Industroyer exists)
  - Pipedream/incontroller
- We will collect information on these as well

ICS CTI



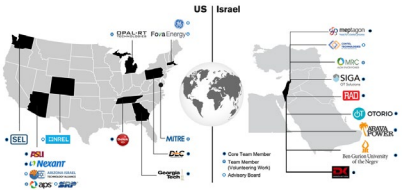
- From our extensive search, we could not find OT level CTI for ICS
- There are technical reports that analyze the ICS malware behavior
- The reports provide some information about the malware behavior concerning the ICS world
- We plan to use the textual description and structure them in the form of machine-readable OT level CTI.
- We have a meeting this week with the Israeli CERT Energy regarding CTI for OT

STIX2 cyber observable objects



- We wish to extend the STIX2 framework to support ICS observables
- This work would enable consuming CTI information for ICS, in the same manner, we do for Enterprise
- We will use this new extension to structure the information we extract from malware reports and simulations
- This work should be tightly coupled with the work done on COPEs (Task 2)

Current status and plans



- Current assets
  - Multi-level CTI ontology for enterprise
  - Multi-level Naive Bayes method for techniques inference
  - SHAP based method for explaining anomalies
- Ongoing
  - Discussion with OTORIO regarding technique-observable data generation
  - Populating the ontology using CTI data (enterprise + ICS)
- Plans
  - Applying anomaly detection to existing datasets with labeled techniques
  - Populating the ontology using simulated data
  - Extending the STIX2 framework for ICS
  - Populating the ontology using expert-based data
  - Closing the loop with unexplainable anomaly detection