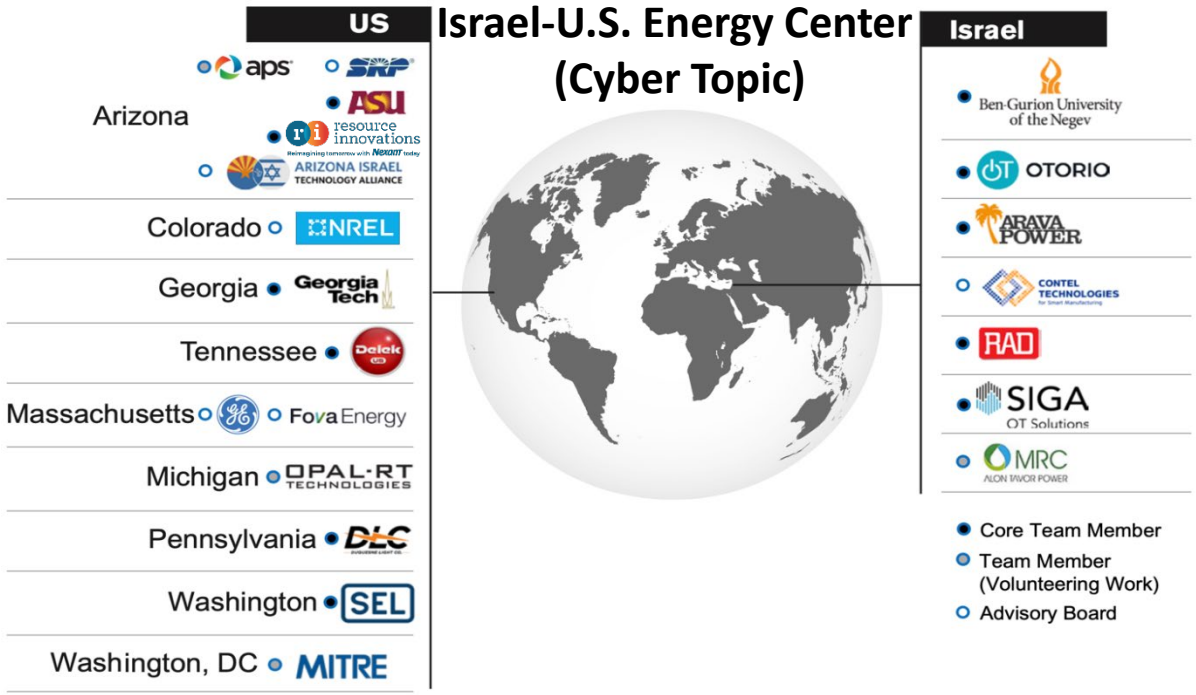
Task 6
Threat Hunting



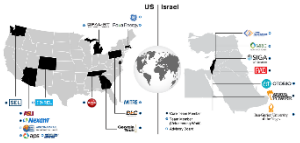
Project Review Workshop

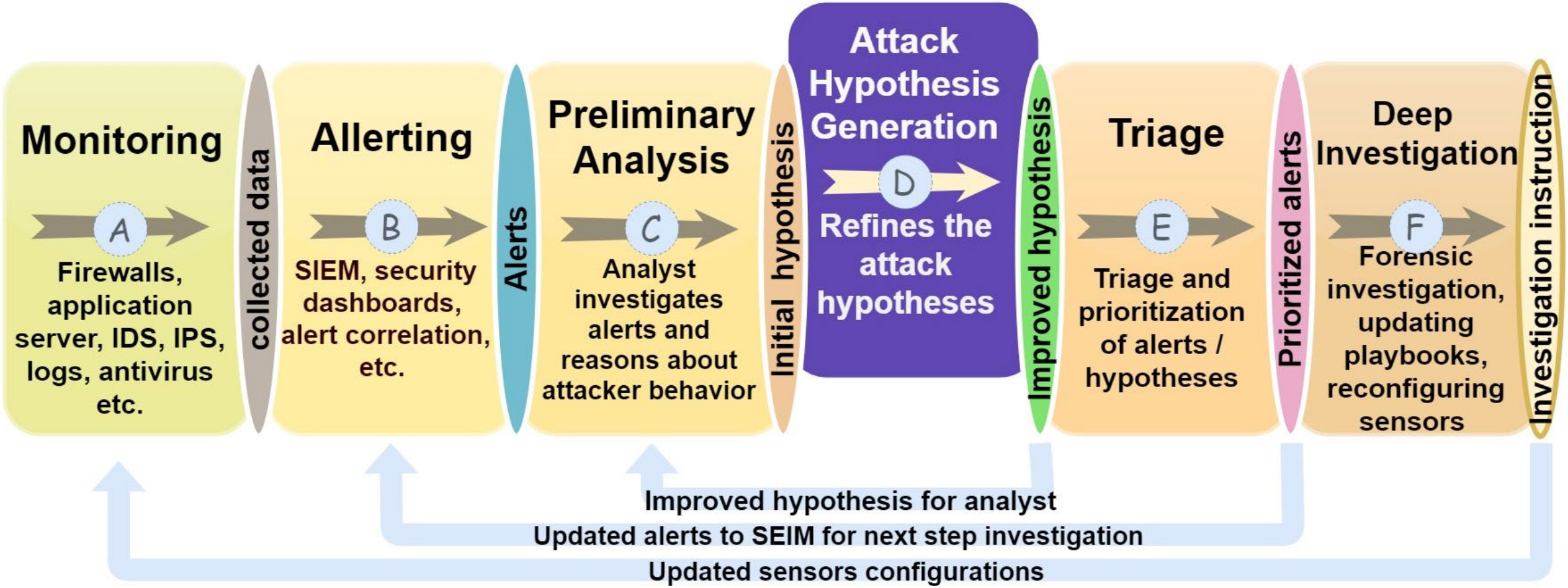
Rami Puzis

BGU

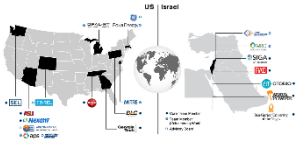
Mar 20, 2023

Attack Hypothesis Generation

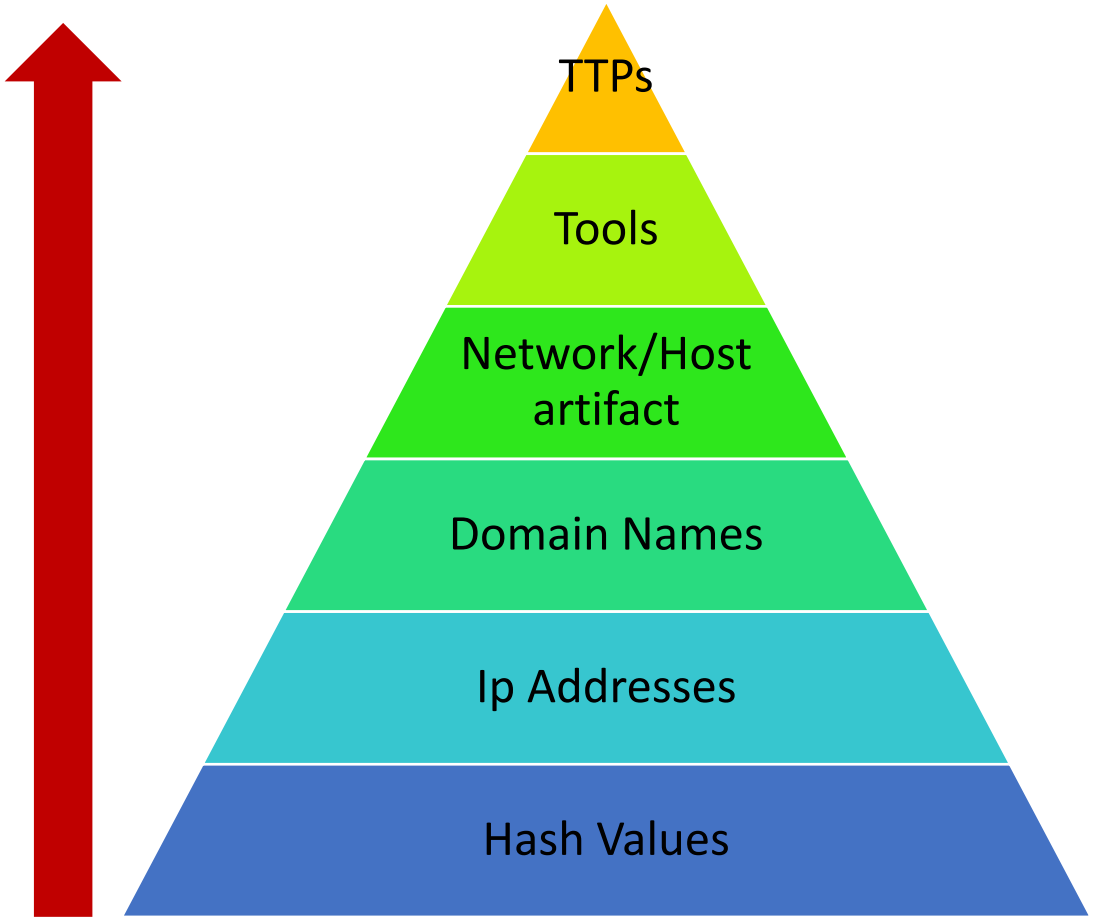




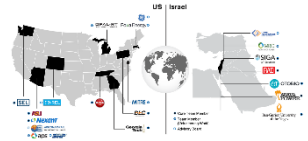
Attack Techniques Classification



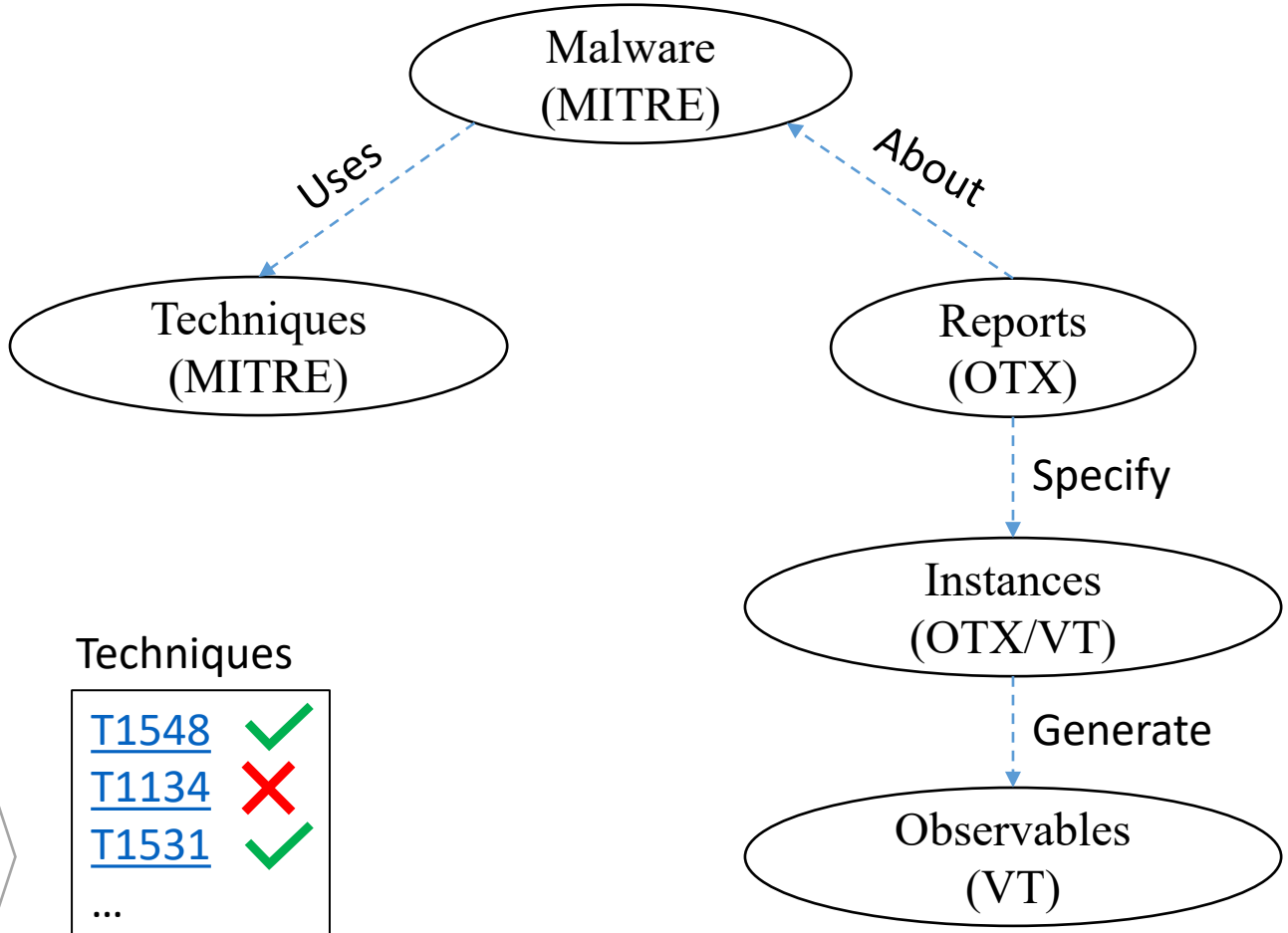
- An essential step in Threat Hunting is to identify the techniques being used by the attacker
- We want to use observed artifacts to find the techniques that generated them
- That means we want to get from bottom to top in the Pyramid of Pain



Attack Techniques Classification – approach for enterprise



- We have a graph KB composed of data collected from (Task 4):
  - MITRE ATT&CK
  - VirusTotal
  - AlienVault OTX
- The artifacts are used as input to a classification algorithm and the output is the techniques used



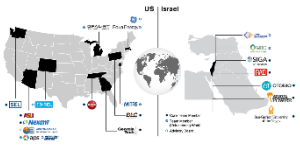
ML multi-label classification

Techniques

T1548 ✓
T1134 ✗
T1531 ✓
...
T1220 ✗

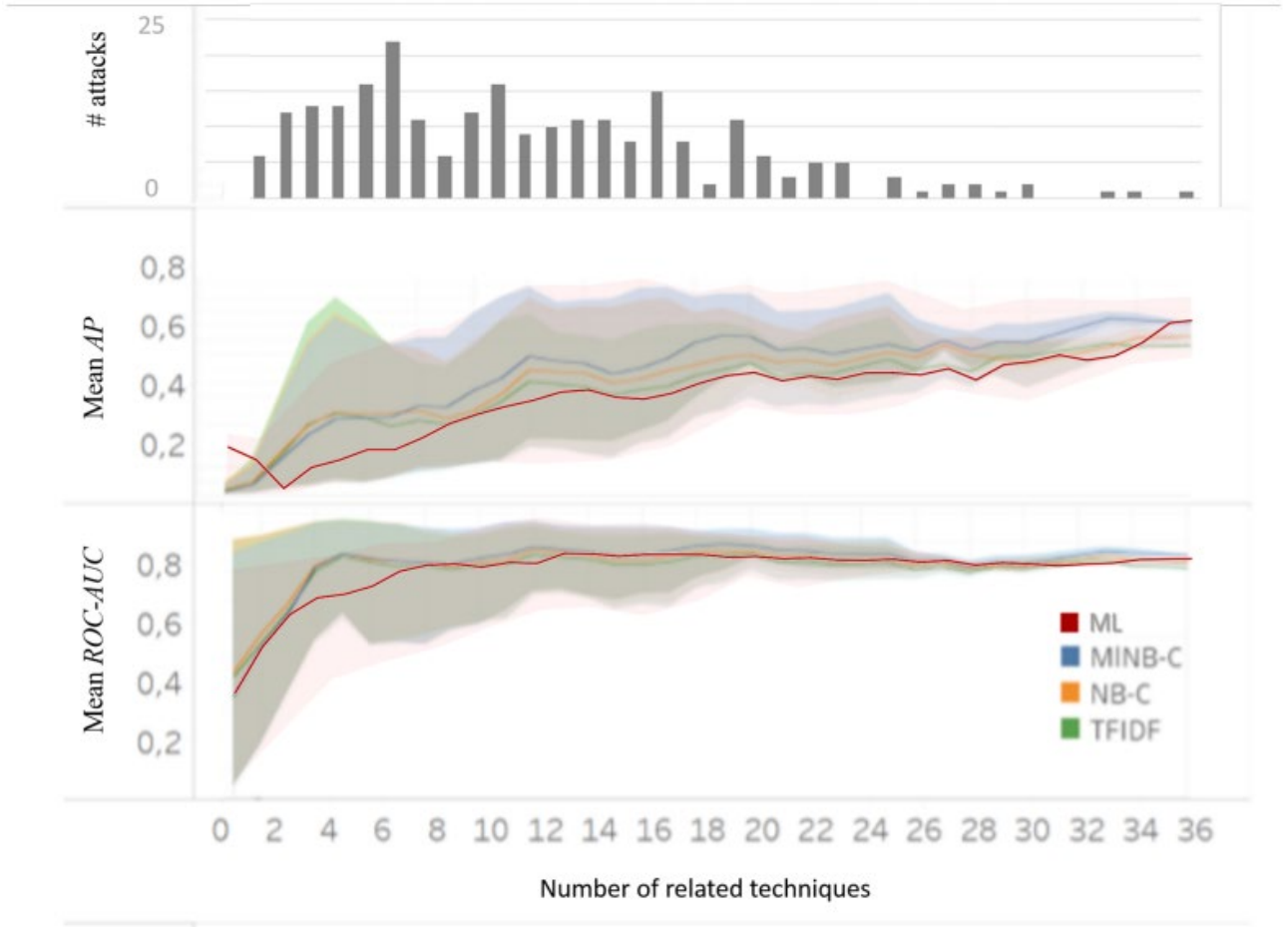
Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph

Florian Klaus Kaiser, Uriel Dardik, Aviad Elitzur, Polina Zilberman, Nir Daniel, Marcus Wiens, Frank Schultmann, Yuval Elovici, and Rami Puzis



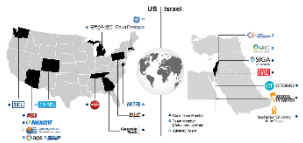
- Published 04 January 2023
- IEEE transactions on dependable and secure computing

Focus on the privilege escalation, lateral movement, discovery, and C&C tactics

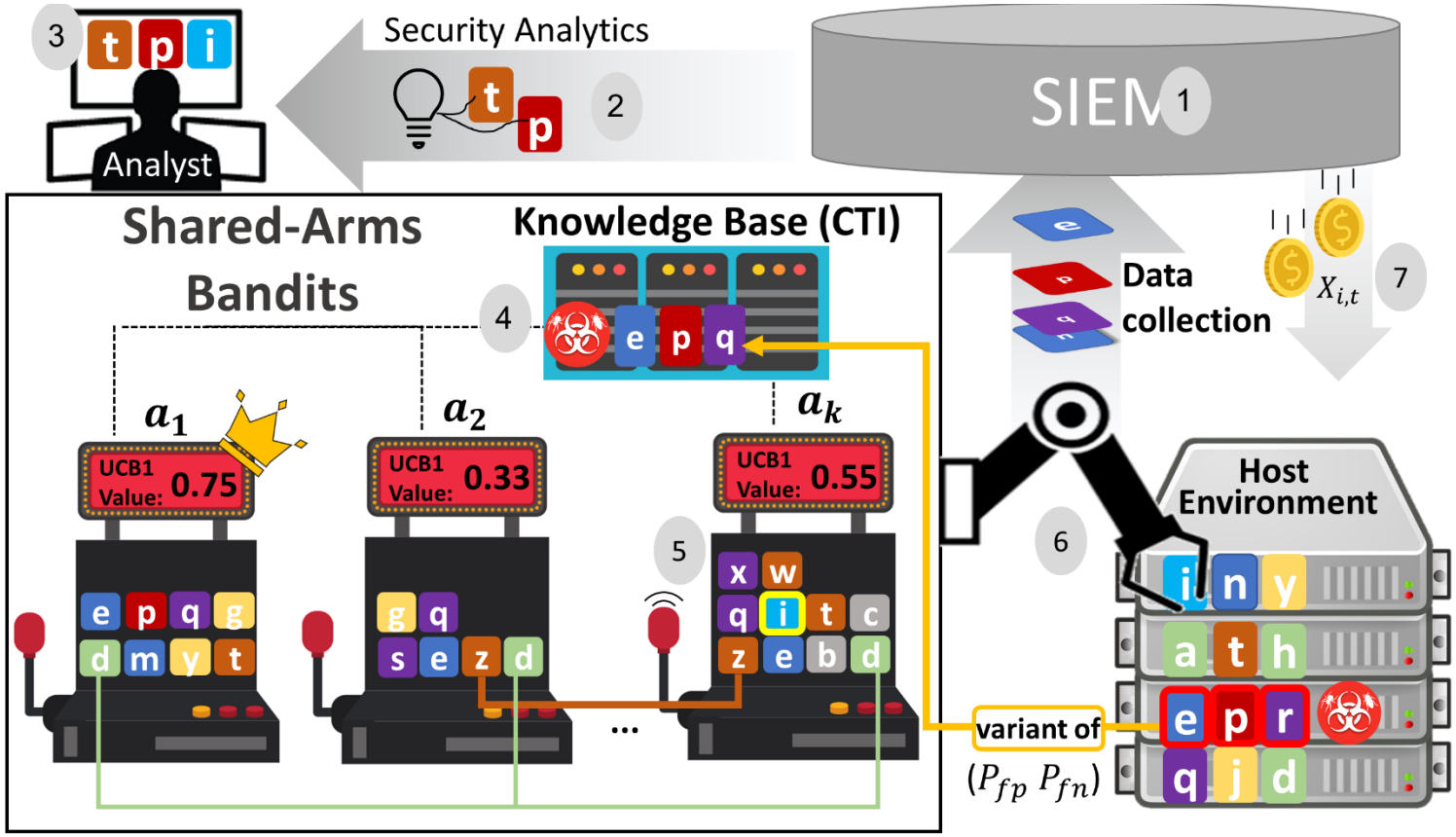


MABAT: A Multi-Armed Bandit Approach for Threat-Hunting

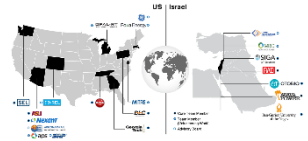
Liad Dekel, Ilia Leybovich, Polina Zilberman, and Rami Puzis

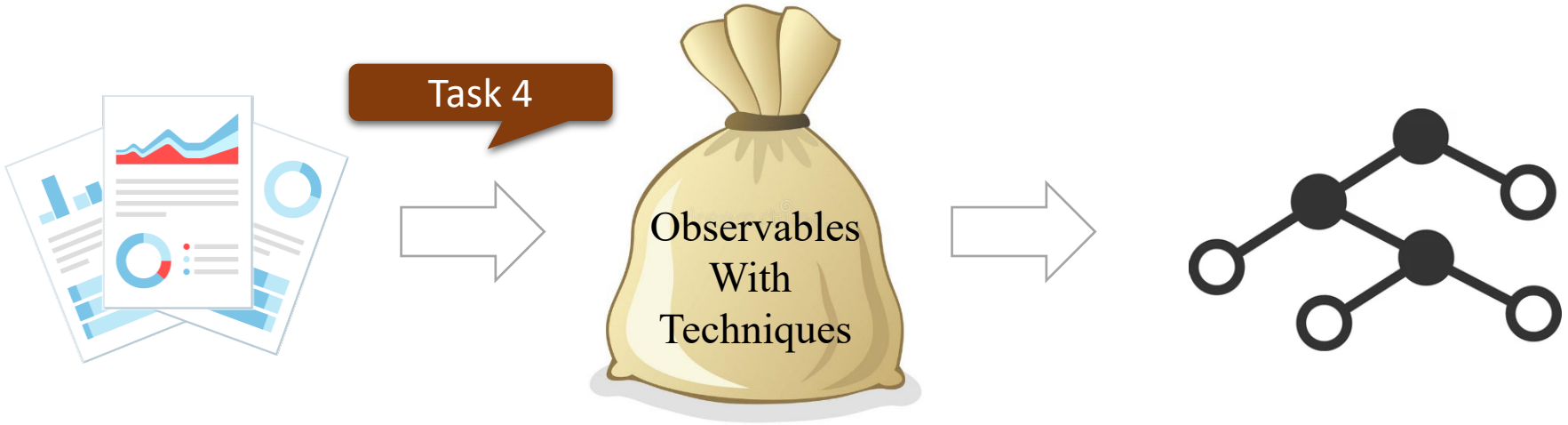


- Published 17 October 2022
- IEEE Transactions on Information Forensics and Security



Building an attack techniques provenance graph





The techniques will be ordered in the graph by their related MITRE ATT&CK tactics, such that each depth of the graph contains tactics corresponds to a level of The Cyber Kill Chain:

Current approach for Targeted Data Collection in Threat Hunting for ICS

Receive an alert from blocked rule

Task 4

Identify the techniques used by the attacker using the KB

Threat Intelligence

STIX

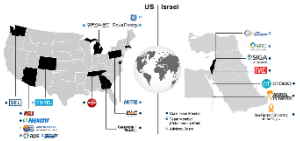
Extract the observables matching the attackers next moves (techniques)

Turn the observables back into firewall rules according to the scheme and alert

Build an attack techniques provenance graph

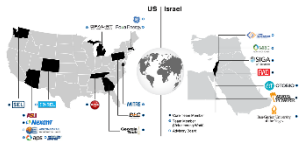
Security analyst together with operators may decide to block traffic

Towards next milestone – October 2023



- We will develop a plugin for the RAM^2 system which implements the method presented previously and is based on the knowledge base from Task 4.
- The plugin will dynamically configure the Palo-Alto Next-Gen Firewall:

Collaboration



OTORIO

- Nir Daniel visited OTORIO and worked with RAM^2
- OTORIO connected the Palo-Alto Next-Gen Firewall to their lab
- RAM^2 analytical plugins development
- Ongoing discussion

MITRE

- ICS observables extraction and scheme
- Ongoing discussion