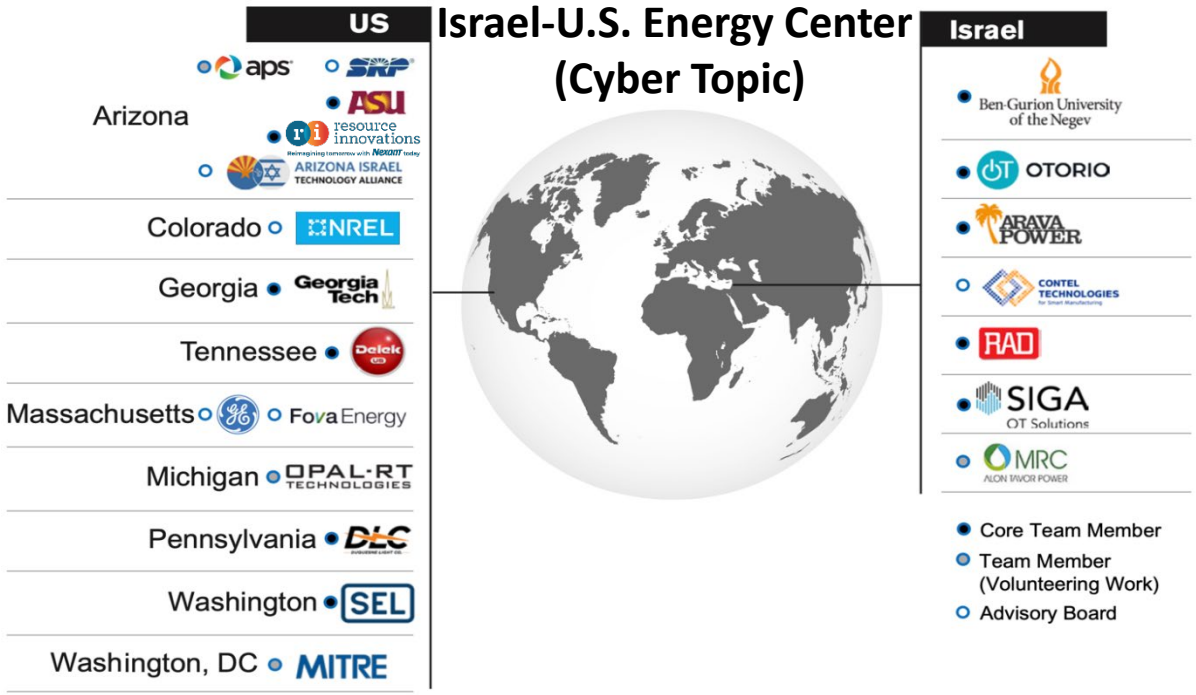
Task 6
Threat Hunting



Third Project Review Workshop

Moti Cohen

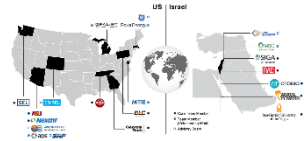
BGU

Aug 24, 2022

Cyber threat intelligence (CTI)

- Structured and actionable information for identifying adversaries and their motives, goals, capabilities, resources, and tactics
- Evidence-based knowledge in the form of measurable events and the context for the events' interpretation.

The OODA loop in Threat Hunting – **Reactive**



- Playbook execution
- Targeted data collection

OBSERVE 1

SIEM

Task 4

Threat Intelligence

STIX

ACT 4

ORIENT 2

- Human in the loop
- Triaging
- Choosing playbooks

DECIDE 3

Anomaly Detection

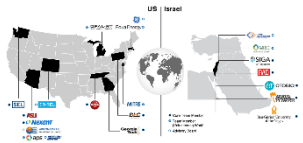
Task 10

Alert correlation and explanation

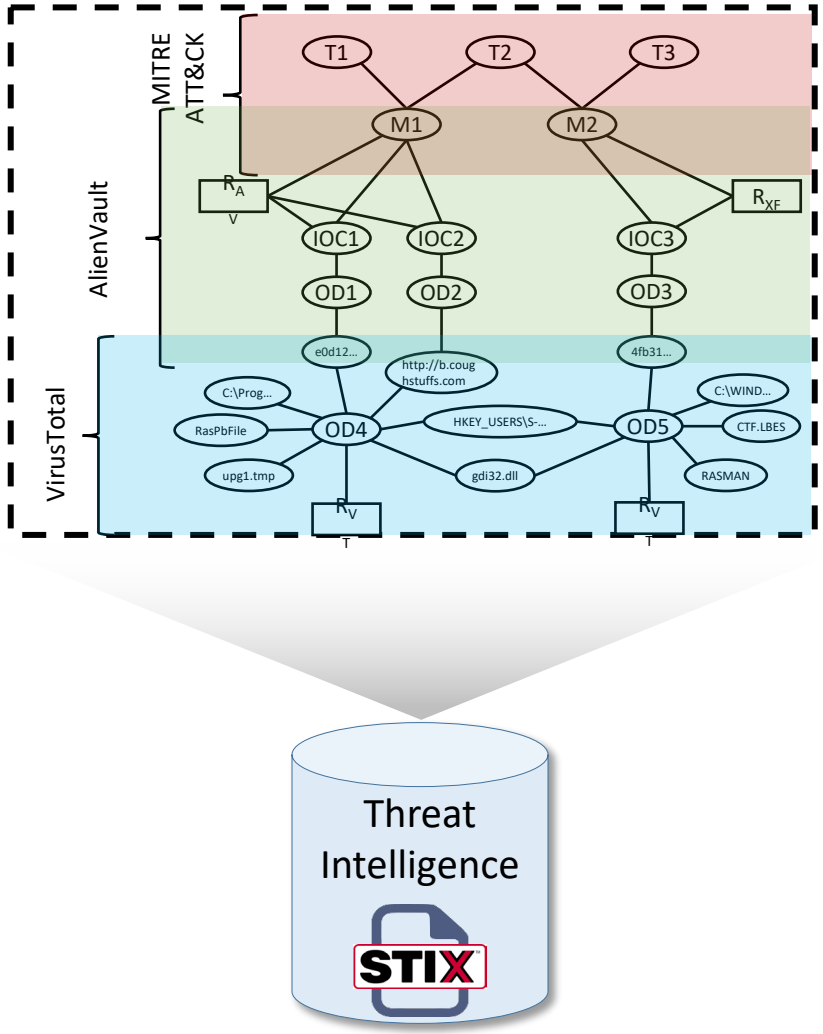
Task 12

Hypotheses Generation

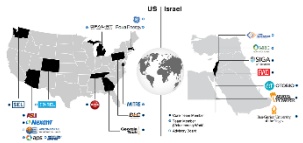
Engagement 5 (Transparent Computing)



- DARPA Engagement 5 of the DARPA Transparent Computing program
- Open data for development and testing
- Capture The Flag activity funded by DARPA
- Includes benign enterprise activity before end during the attacks
- A set of attack scenarios that were generated and recorded by multiple teams
- Mimic new and existing APTs
- Ground truth data is provided for reference
- Can it be used with our Enterprise Knowledge Base?



Engagement 5 (Transparent Computing)

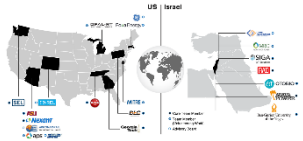


- DARPA Engagement 5 of the DARPA Transparent Computing program
- Open data for development and testing
- Ca… …y DARPA
- In… …before e…
- A… g… …e teams
- Mimic new and existing…
- Ground truth data is provided for reference
- Can it be used with our Enterprise Knowledge Base?

Prof. Wenke Lee,
Did THEIA generate data that can be reused in this consortium?

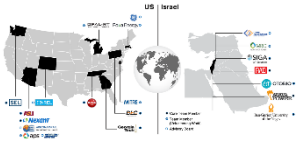
- ≈20 attack scenarios on Windows, Linux, Android environments
- Span over about two weeks of activity
- Recorded events from the attacked machines, formatted in a specific AVRO format
- About 1.5TB of data
- Interesting data features:
  - Registry keys
  - Process trees
  - Files

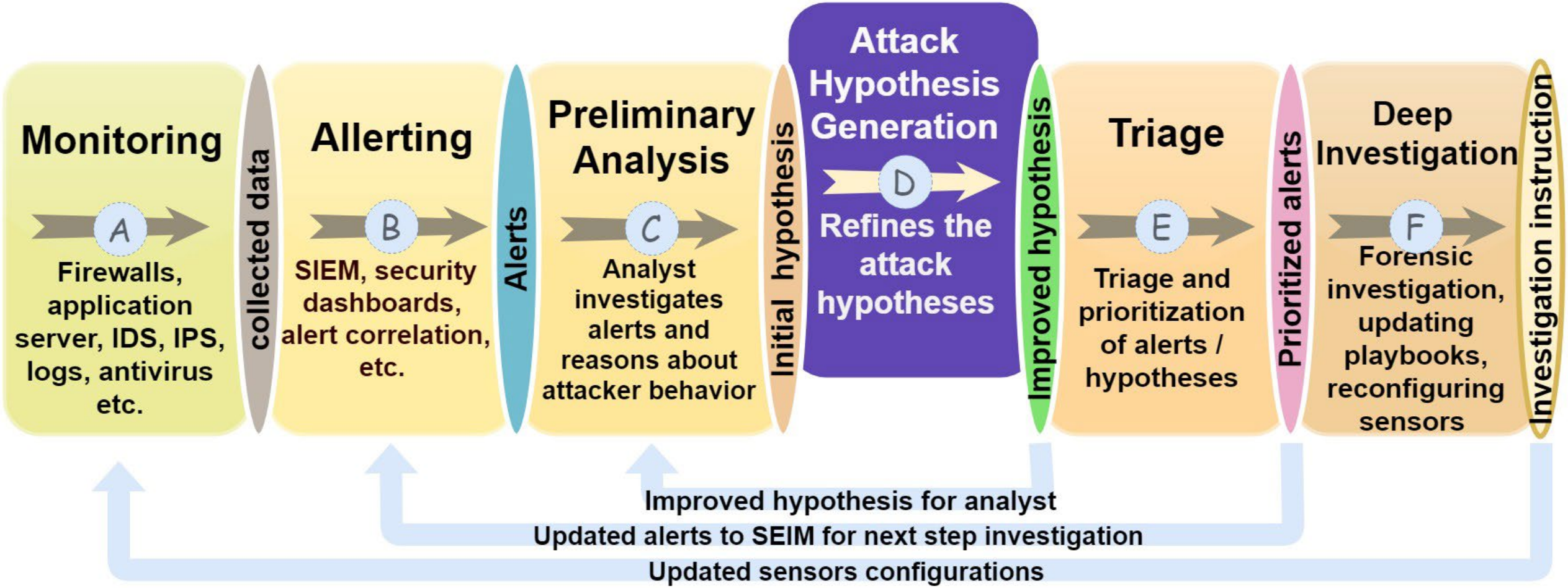
Engagement 5 usage



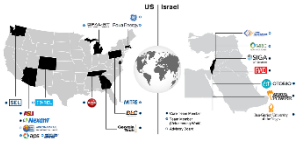
- Use the data in Engagement 5 together with our Enterprise KB
- Intersect the reported data items in the two repositories to see if there is enough common ground to build our algorithms on
  - This is still WIP
- Develop a Threat Hunting Hypothesis Generation Algorithm on top of the Engagement 5 and the Enterprise KB data

Attack Hypothesis Generation

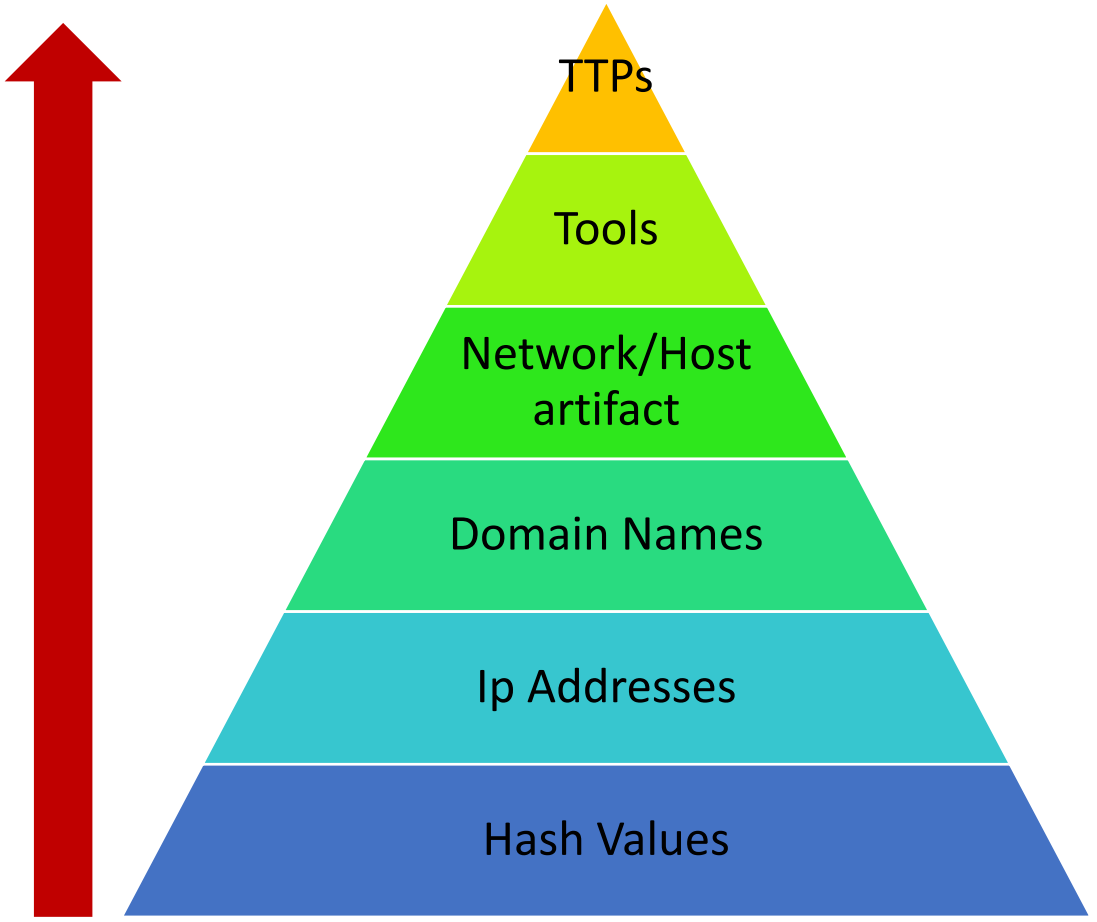




Attack Techniques Classification

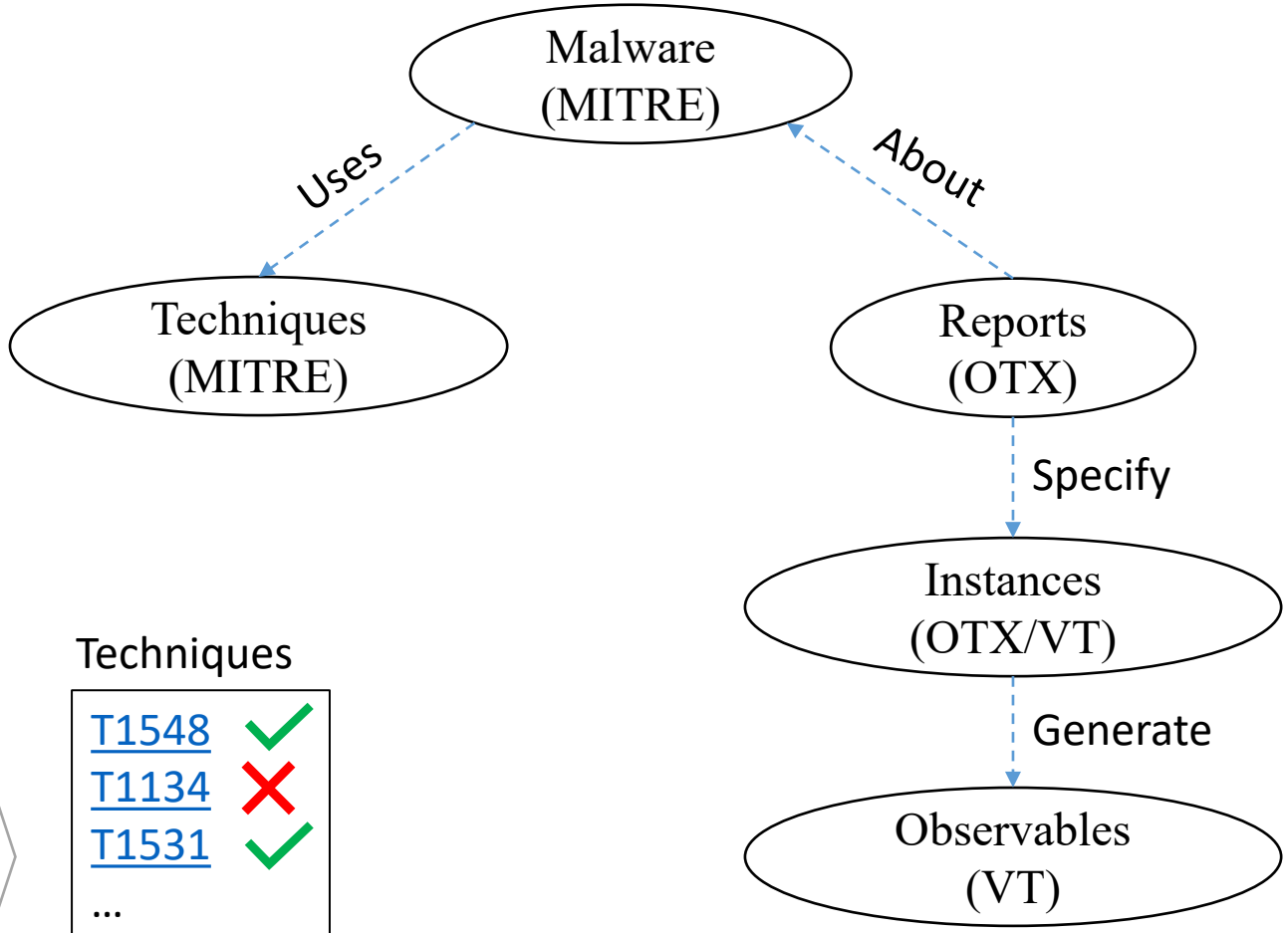


- An essential step in Threat Hunting is to identify the techniques being used by the attacker
- We want to use observed artifacts to find the techniques that generated them
- That means we want to get from bottom to top in the Pyramid of Pain



Attack Techniques Classification - approach

- 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



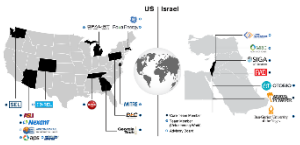
ML multi-label classification

Techniques

T1548 ✓
T1134 ✗
T1531 ✓
...
T1220 ✗

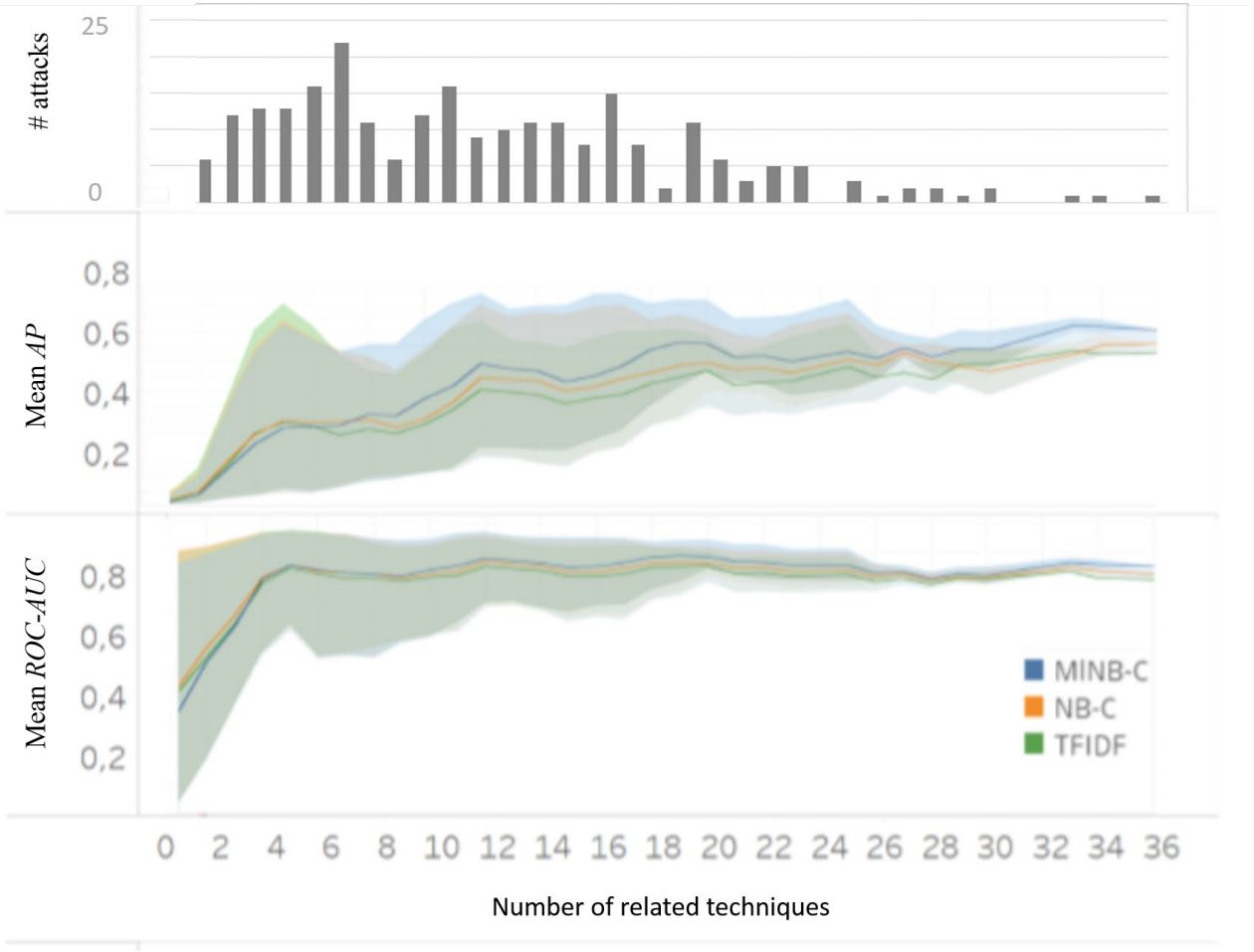
Attack Hypotheses Generation Based on Threat Intelligence Knowledge Graph

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



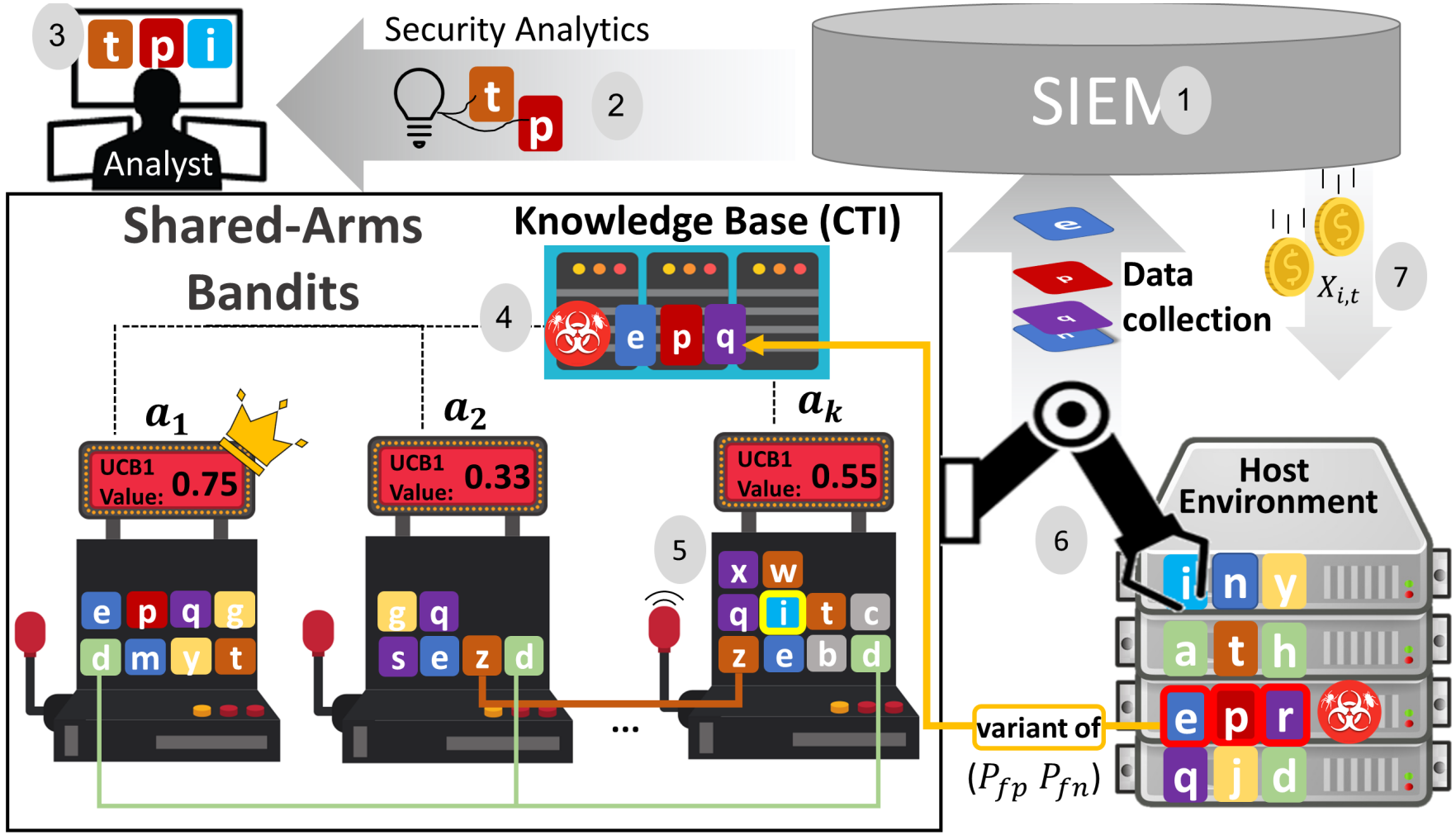
- Pending major revision
- IEEE transactions on dependable and secure computing (IF=7.329)

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

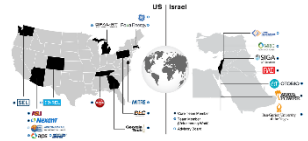


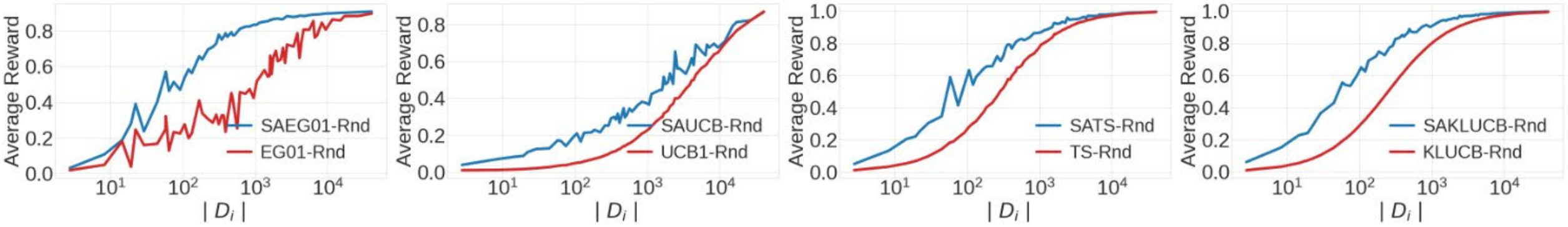
MABAT: A Multi-Armed Bandit Approach for Threat-Hunting

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



The average reward as a function of the available CTI

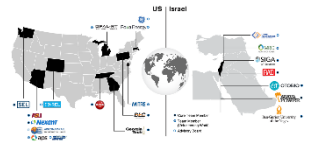


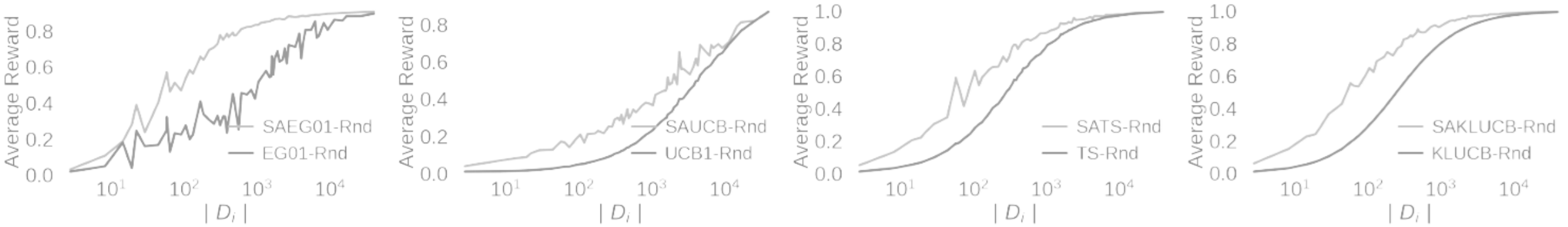


(a) EG01 (b) UCB1 (c) TS (d) KL-UCB

Consider observables shared by multiple malware families

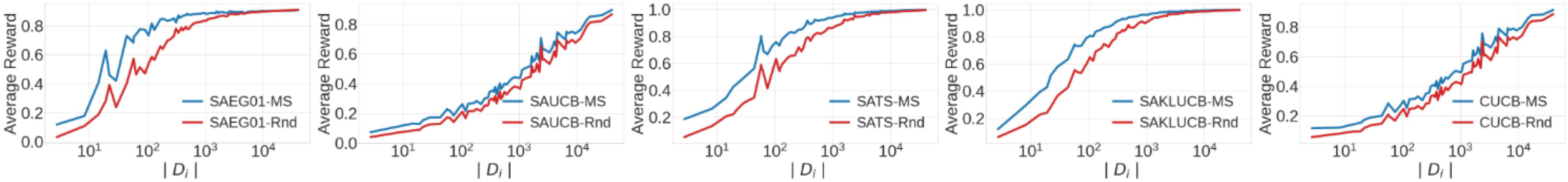
The average reward as a function of the available CTI





(a) EG01 (b) UCB1 (c) TS (d) KL-UCB

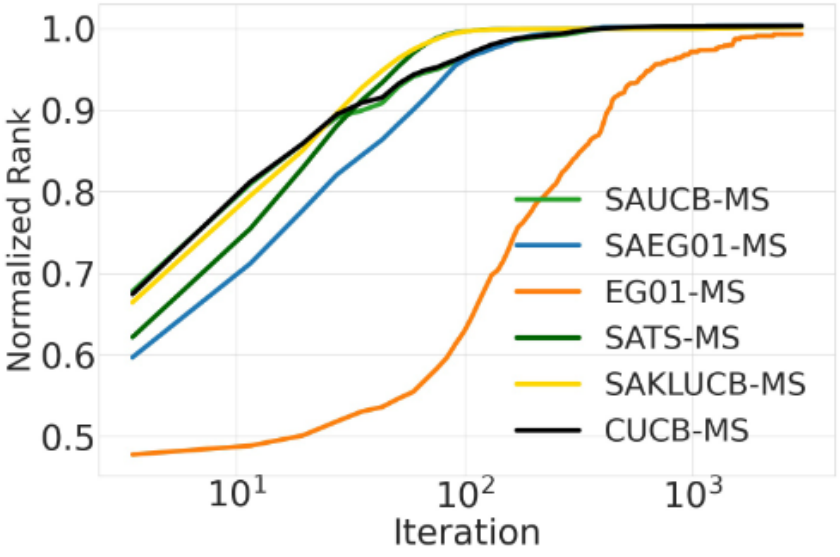
Consider observables shared by multiple malware families



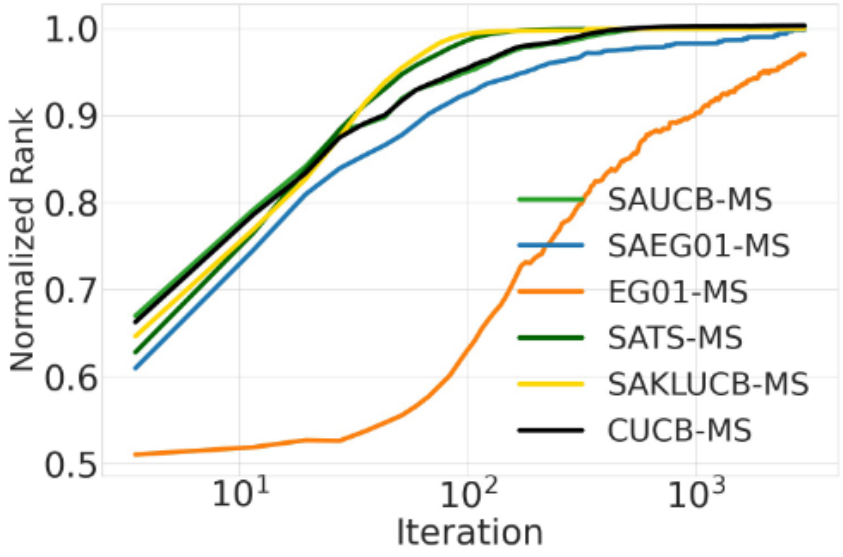
(a) SAEG01 (b) SAUCB (c) SATS (d) SAKLUCB (e) CUCB

Prioritize most shared observables

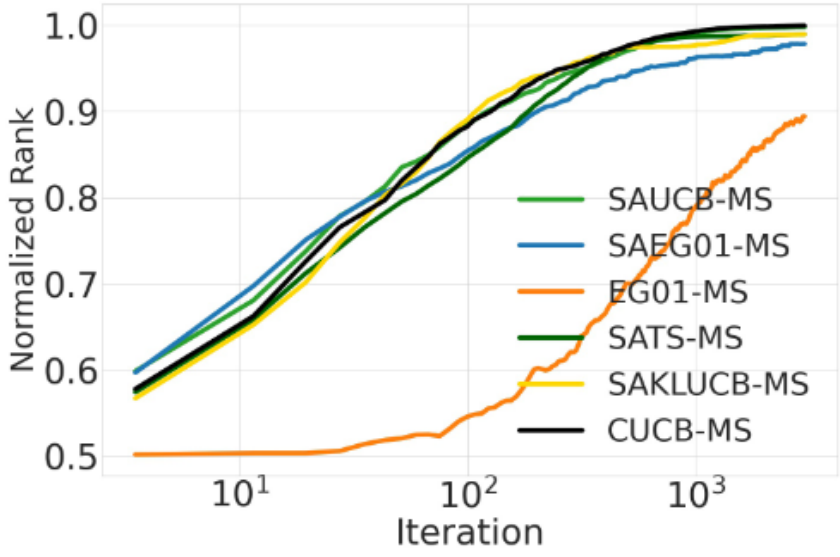
Attack ranking (detection) with varying CTI quality



(a) $P_{fp} = 0,\ P_{fn} = 0$



(b) $P_{fp} = 0.01,\ P_{fn} = 0.1$



(c) $P_{fp} = 0.05,\ P_{fn} = 0.5$

- Accepted with minor revision in
- IEEE Transactions on Information Forensics and Security
- IF=7.178