Arizona	ASU Nexant ARIZONA ISRAEL TECHNOLOGY ALLIANCE
Colorado	NREL
Georgia	Georgia Tech
Tennessee	Delek US
Massachusetts	Fova Energy
Michigan	OPAL-RT TECHNOLOGIES
Pennsylvania	DLC
Washington	SEL
Washington, DC	MITRE

Task 6

Threat hunting

Q2 - May. 9, 2022

meptagon head for a better process

CONTEL TECHNOLOGIES

MRC ALON TAVOR POWER

SIGA OT Solutions

Ben-Gurion University of the Negev

OTORIO

ARAVA POWER

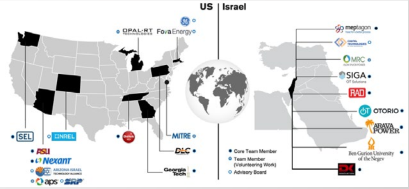
cybereason

RAD

DK INNOVATION

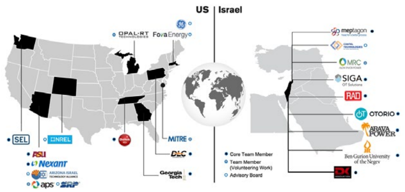
BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation

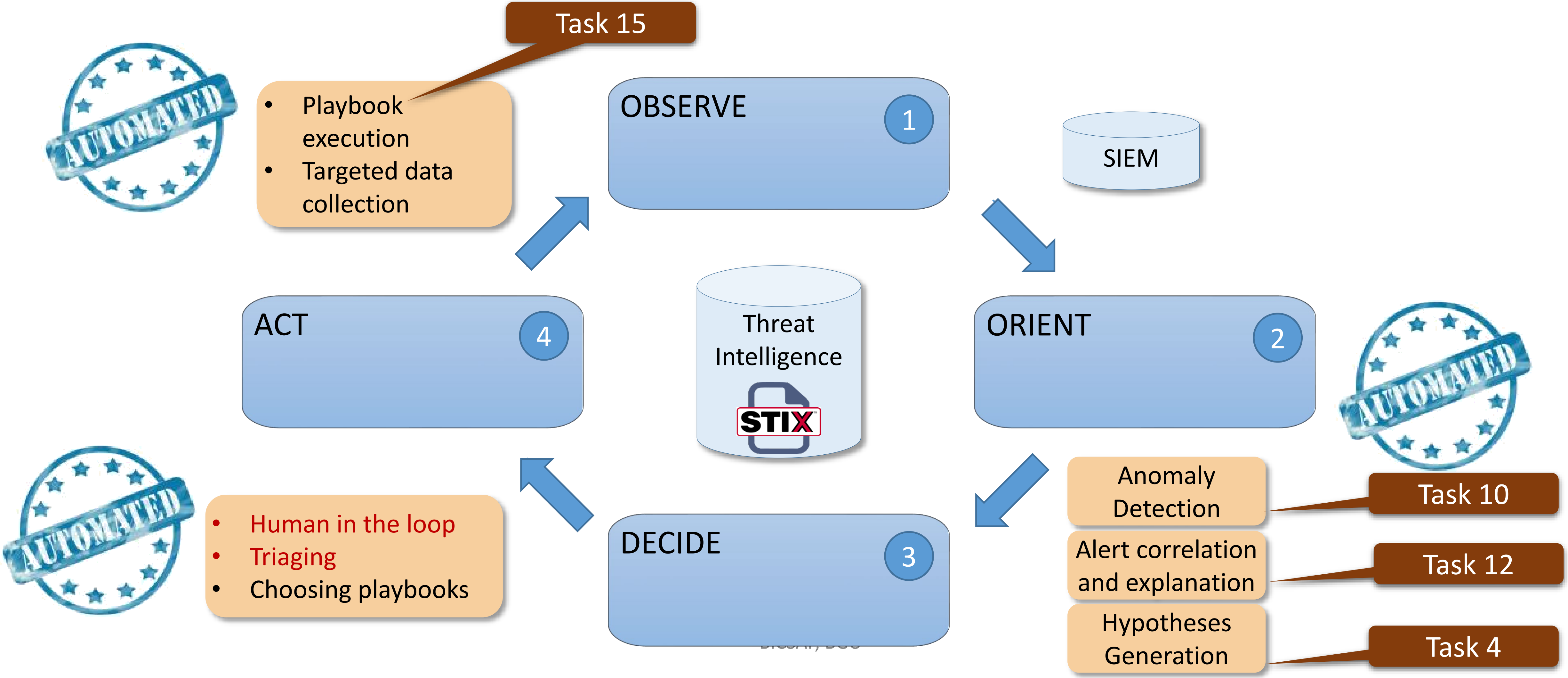
Cyber threat intelligence (CTI)



- 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

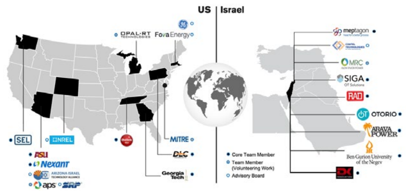
Anomaly Detection

Alert correlation and explanation

Hypotheses Generation

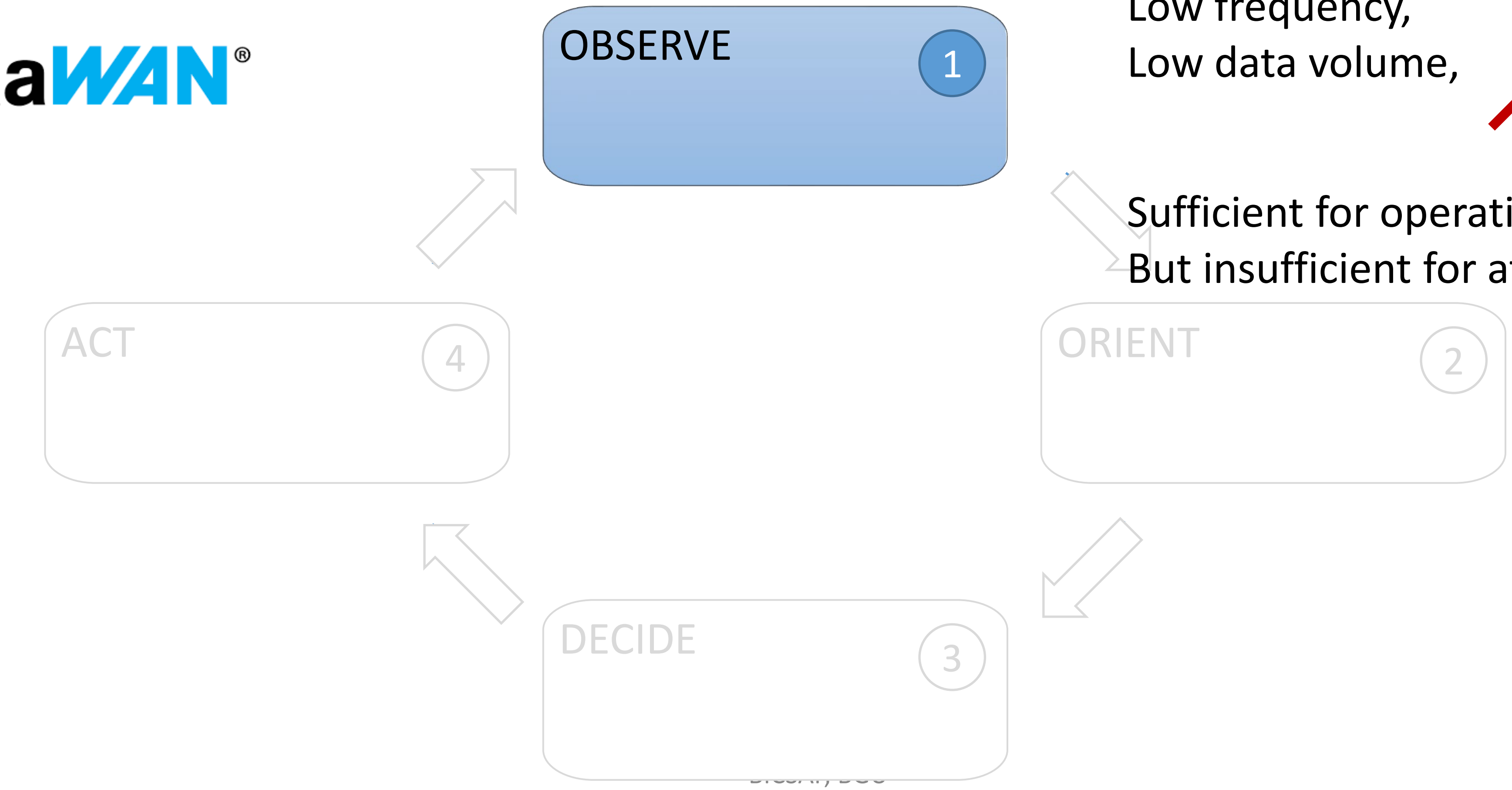
- Human in the loop
- Triaging
- Choosing playbooks

Low energy sensors in ICS



Low voltage, low energy, low power

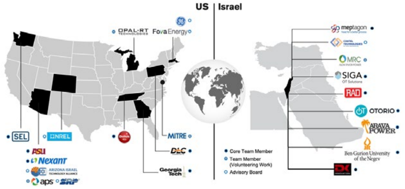
LoRaWAN®



Low frequency,
Low data volume,

Sufficient for operations management
But insufficient for attack investigation

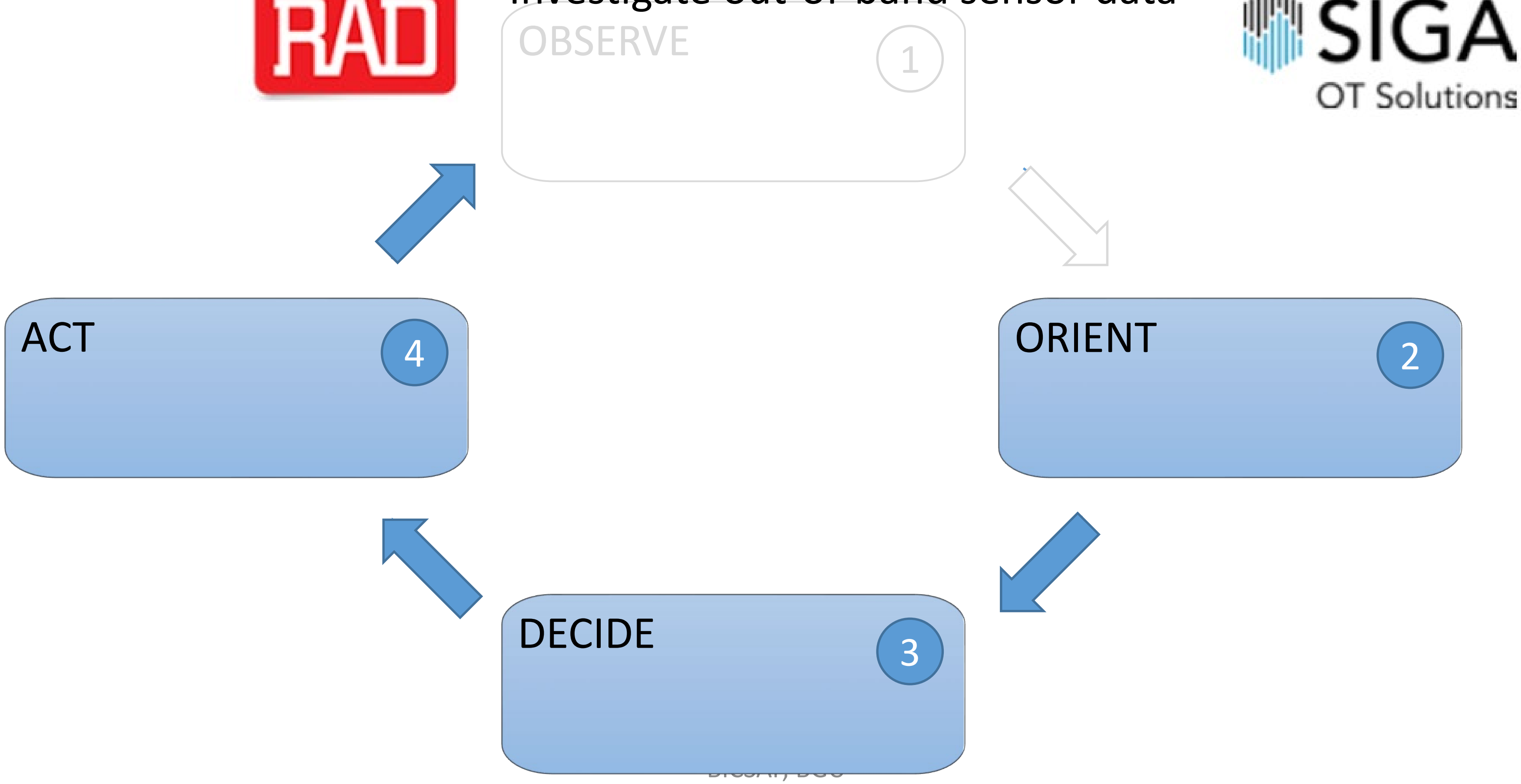
Activating additional sensors



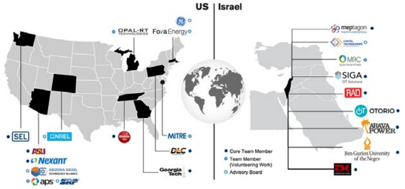
Trigger backup sensors to validate readings
Increase data collection frequency
Investigate out-of-band sensor data

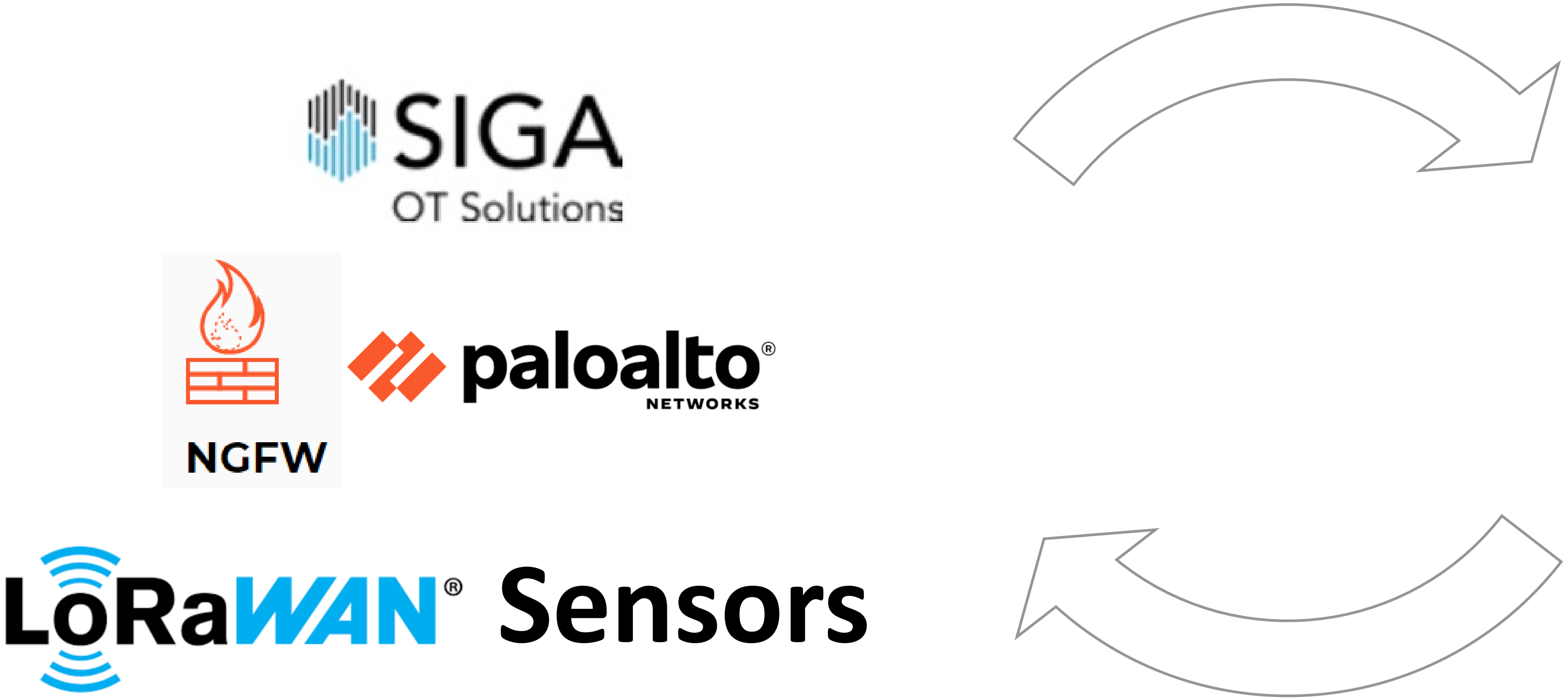
RAD

SIGA
OT Solutions



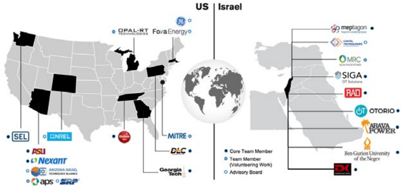
Industry relevance





sources of **sensory and security information** may be triggered/reconfigured by **security orchestration**

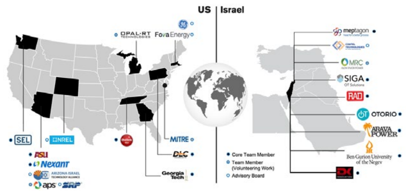
Plans

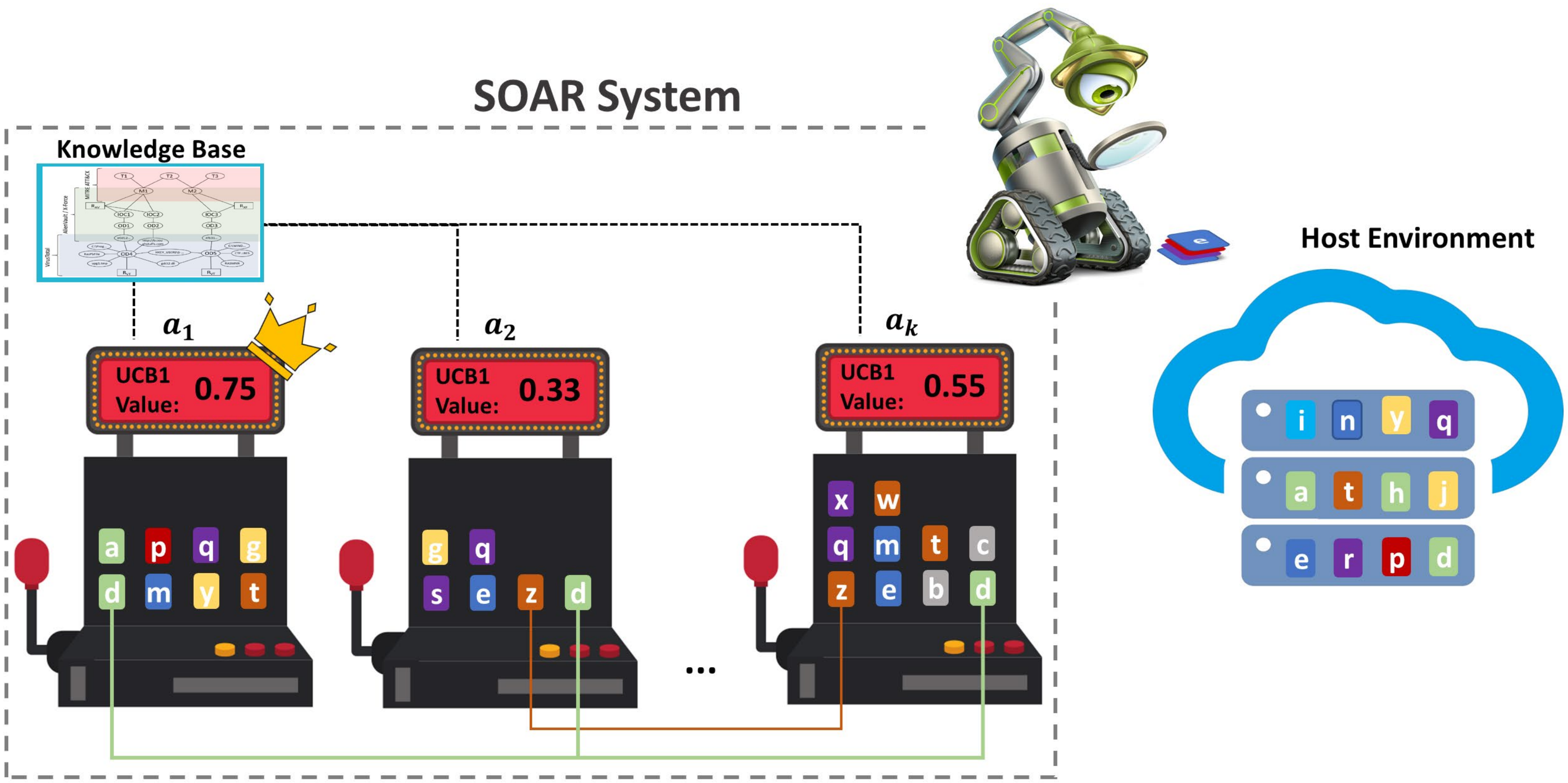


- Design reactive playbooks based on
  - must have and optional sensors specified in COPEs (from Task 2)
  - threat intelligence and adversary patterns (from Task 4)

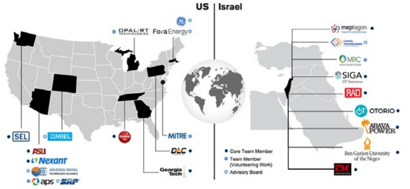
- Showcase the hunting process orchestration in the forthcoming Delek US Lab (from Task 3)
  1. Start the monitoring with limited resources
  2. Detect anomaly configured for high TPR high FPR (from Task 10)
  3. Automatically trigger additional monitoring capabilities relevant to the detected anomaly (from Task 12)
  4. Detect anomaly configured for low FPR (from Task 10)

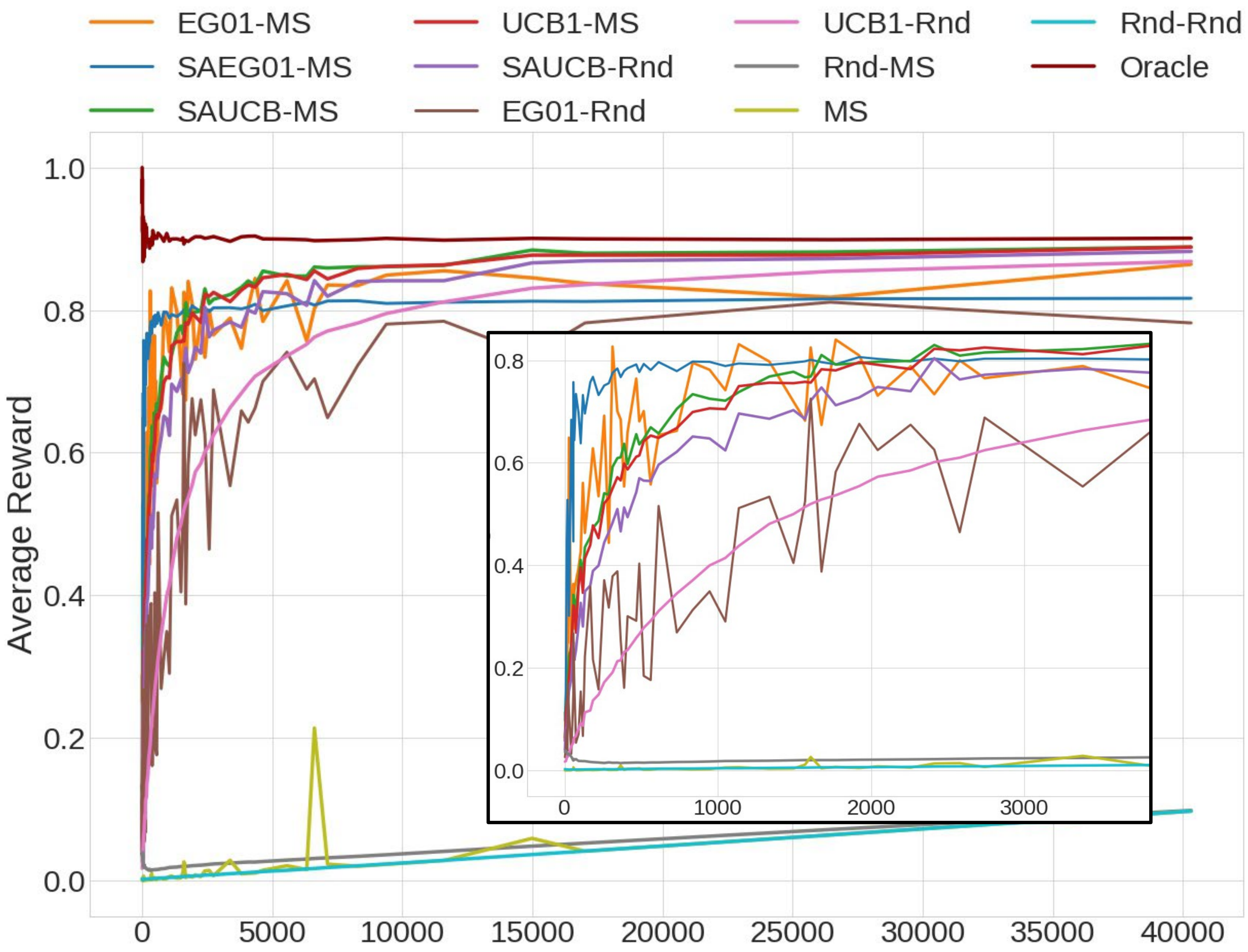
Exploration exploitation tradeoff in
security orchestration automation and response (SOAR)





Multi-armed bandit policies for threat hunting




EG01-MS
SAEG01-MS
SAUCB-MS
UCB1-MS
SAUCB-Rnd
EG01-Rnd
UCB1-Rnd
Rnd-MS
MS
Rnd-Rnd
Oracle
Average Reward