Arizona

Colorado

Georgia

Tennessee

Massachusetts

Michigan

Pennsylvania

Washington

Washington, DC

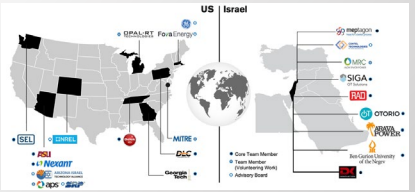
Task 6

Threat hunting

Q1 - Jan. 24, 2022

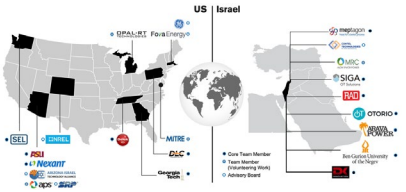
BIRD
Israel-U.S.
Binational Industrial Research
and Development Foundation

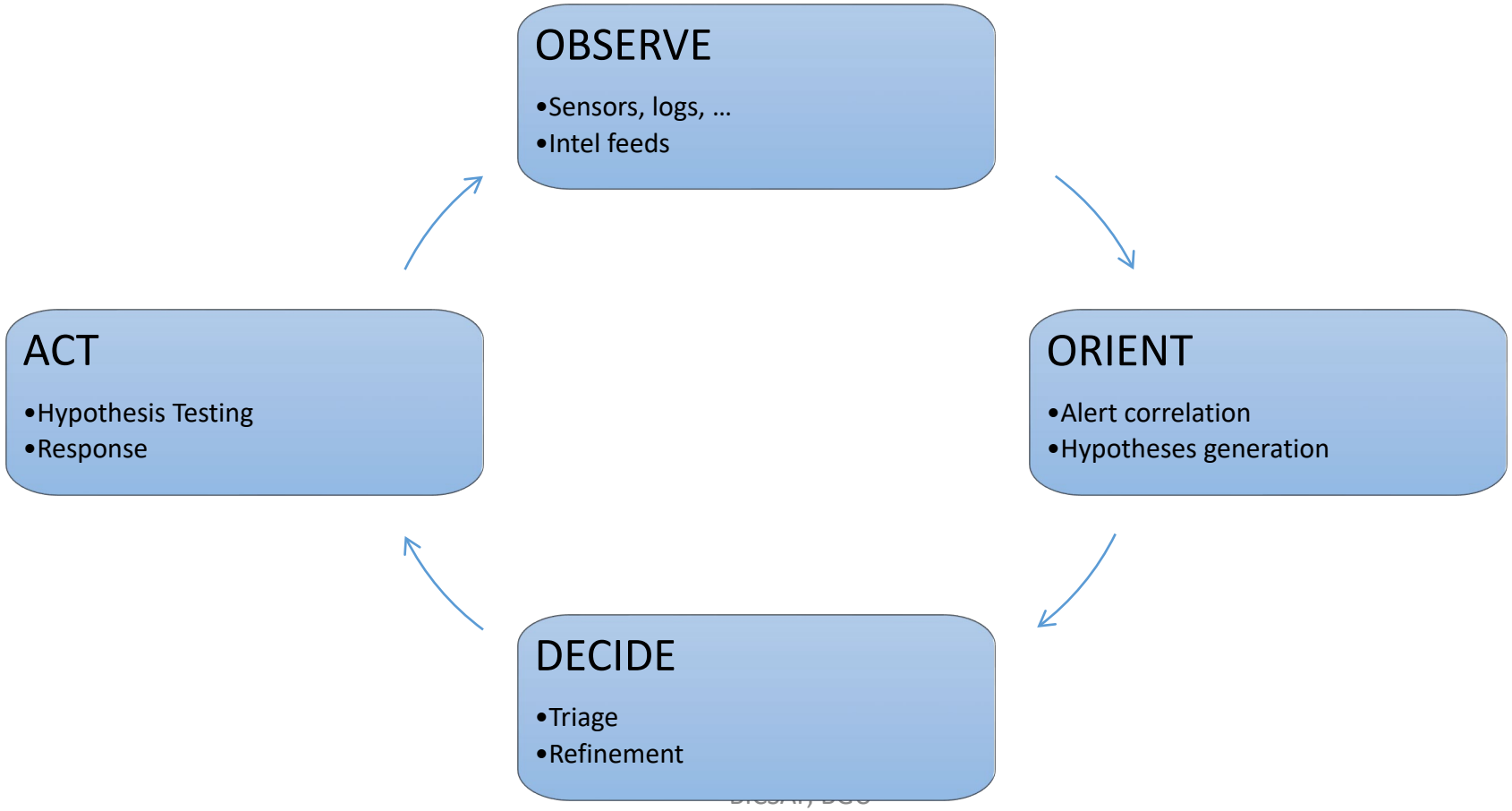
Cyber threat intelligence (CTI)



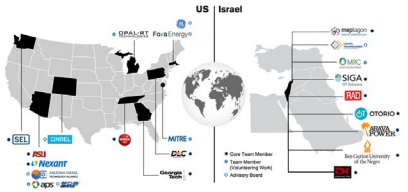
- Structured and actionable information for identifying adversaries and their motives, goals, capabilities, resources, and tactics
- Evidence-based knowledge in the form of measurable events and the context for the events' interpretation.

The OODA loop in Threat Hunting





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



- Playbook execution
- Targeted data collection

OBSERVE 4

SIEM

ACT 3

Threat Intelligence

STIX

ORIENT 1

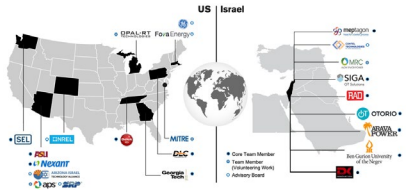
- Choosing playbooks

DECIDE 2

Hypotheses Generation

Task 4

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



- Playbook execution
- Targeted data collection

OBSERVE 1

SIEM

ORIENT 2

- Anomaly Detection → Task 10
- Alert correlation and explanation → Task 12
- Hypotheses Generation → Task 4

DECIDE 3

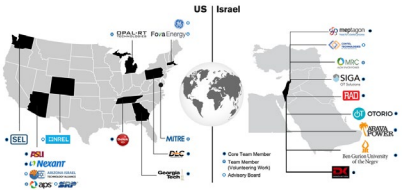
- Human in the loop
- Triaging
- Choosing playbooks

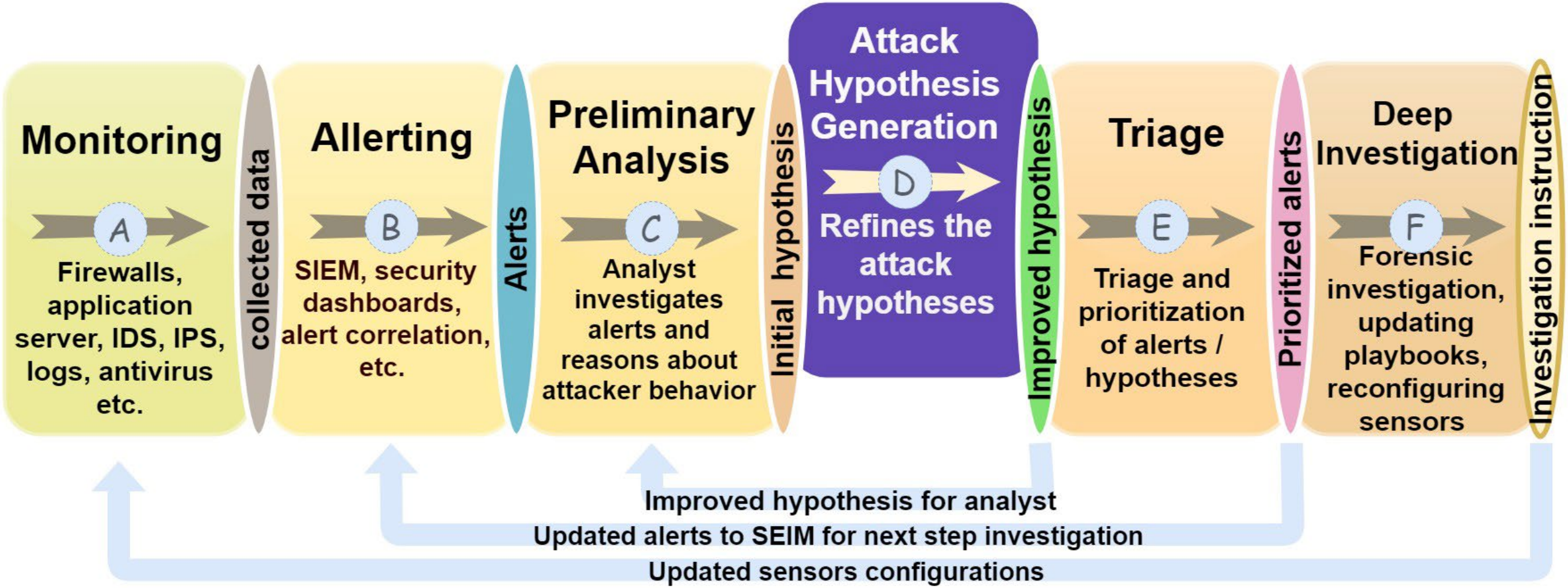
ACT 4

Threat Intelligence

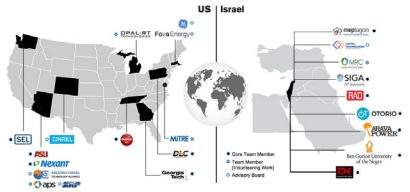
STIX

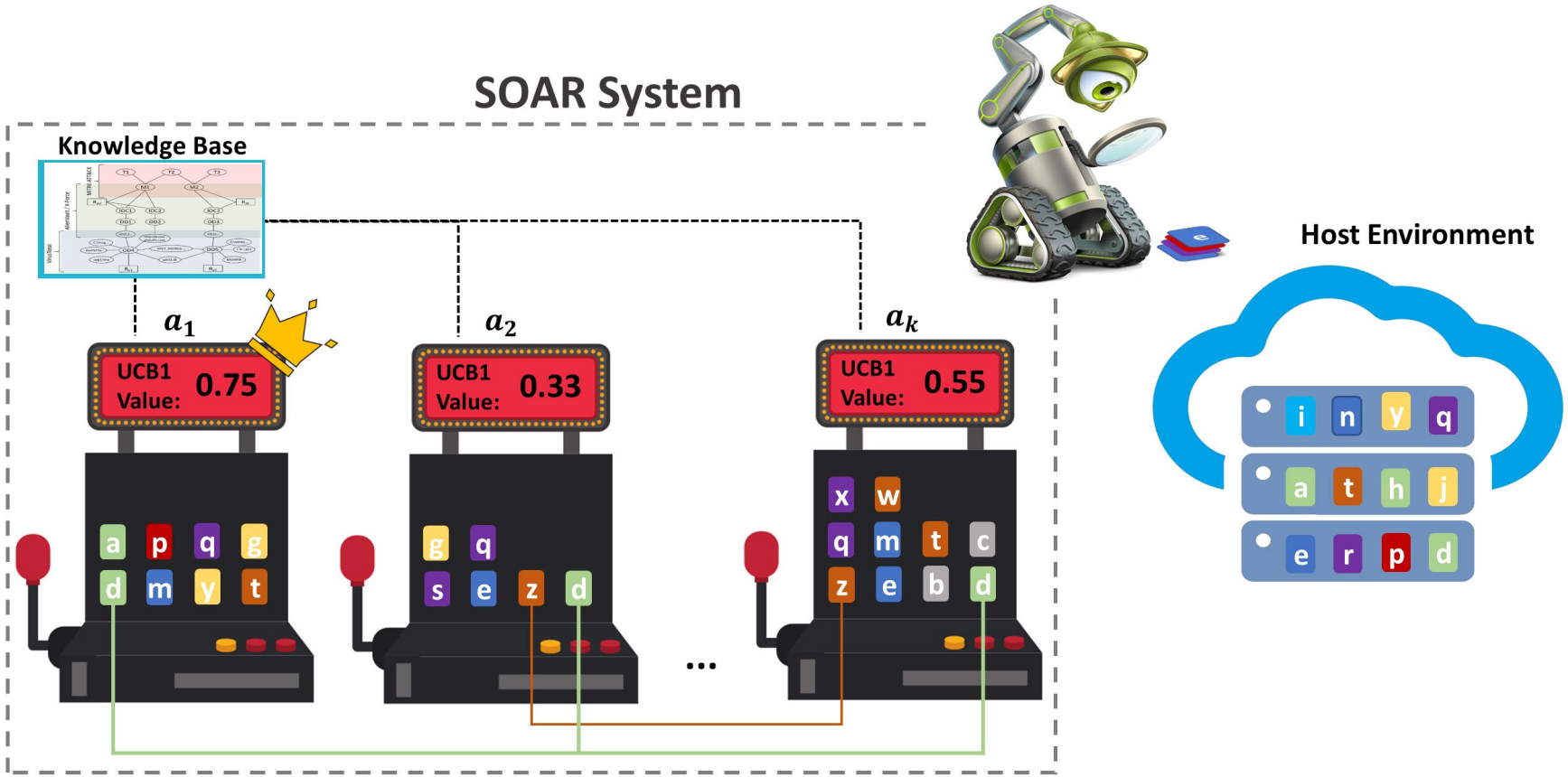
Attack Hypotheses Generation



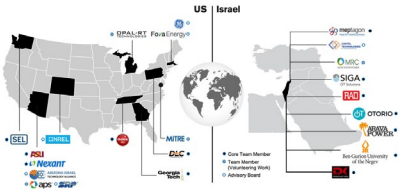


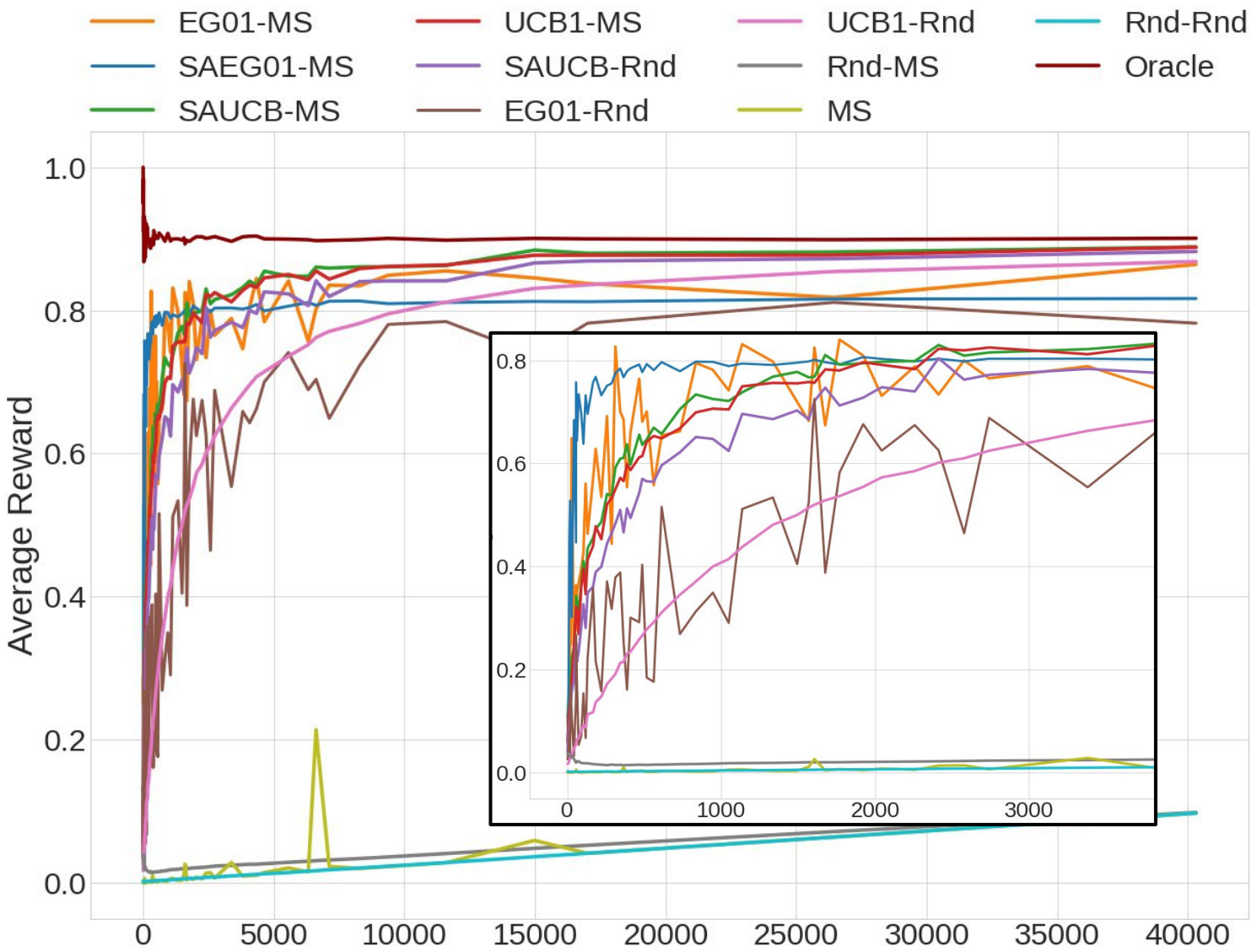
Exploration exploitation tradeoff in
security orchestration automation and response (SOAR)





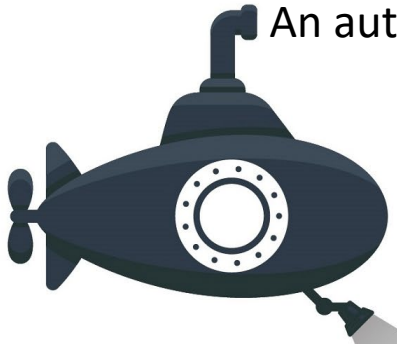
Multi-armed bandit policies for threat hunting





An autonomous deep dive into for advanced cyber-security forensics

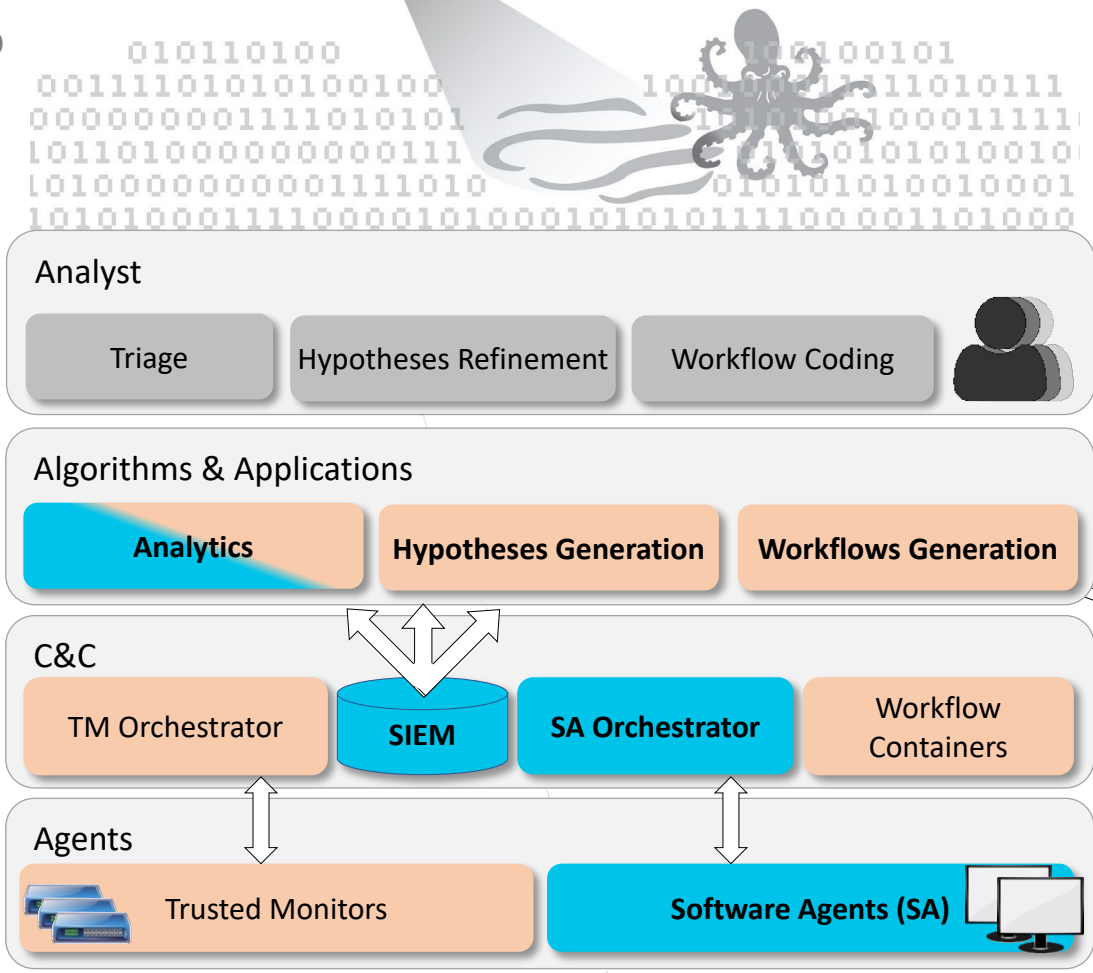
BICSAF

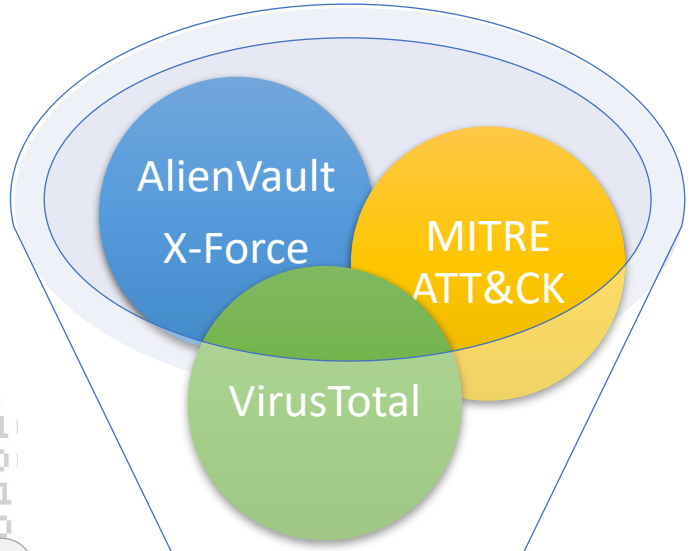


Do not sit back and wait for the Intrusion Detection Systems to raise alerts.

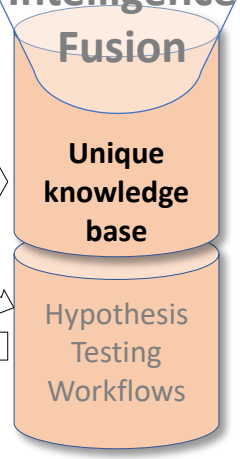
Actively hunt down artifacts that will lead to the attacker.

Agile and adaptive data collection process feeds on **attack hypotheses** constantly generated by BICSAF. **Hunting workflows** (a.k.a. playbooks) are **automatically generated** relaying on a unique **knowledge base** constructed relying on multiple threat intelligence sources.





Threat Intelligence Fusion



CBG Cyber@ Ben-Gurion University of the Negev

BICSAF distributed architecture for managed security services