CICI: RSSD: DISCERN:
Datasets to Illuminate Suspicious Computations on Engineering Research Networks

PI: Brian Kocoloski – bkocolos@isi.edu Co-PI: Jelena Mirkovic – mirkovic@isi.edu

Problem

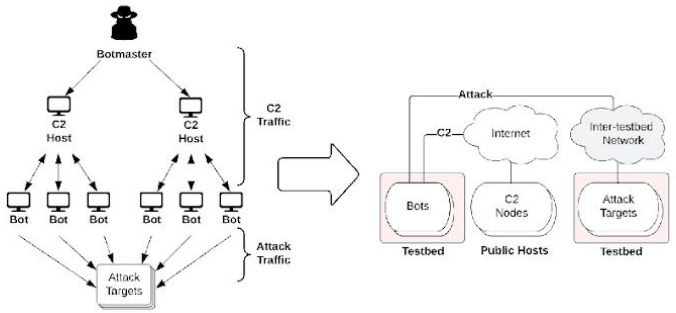
We need better datasets reflecting how ***modern attack scenarios*** play out on ***modern cyberinfrasturctures***

How can we enable easier and more representative ***assessment of the cybersecurity posture*** of modern cyberinfrastructures?

(Future Work)
Can we ***build confidence in ability to transition cybersecurity research*** to modern cyberinfrastructures?

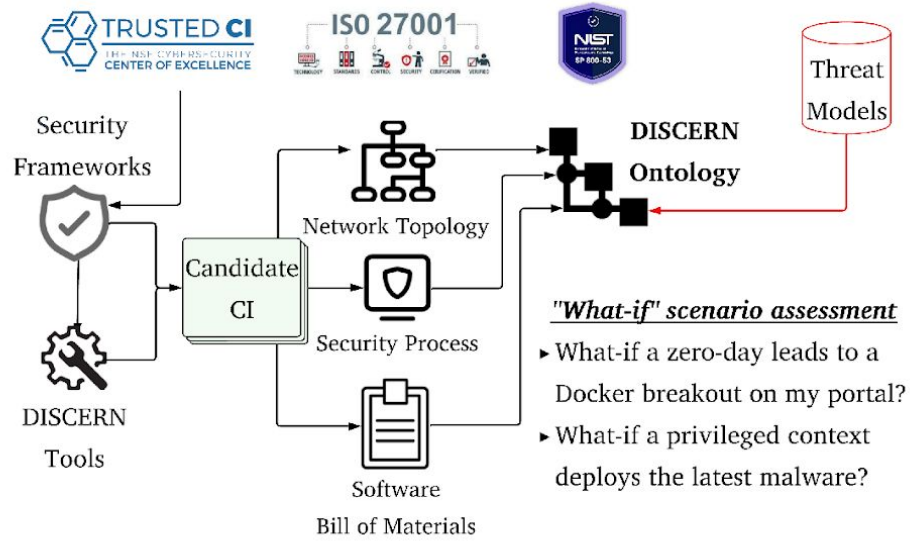
Approach

- Run controlled cyberattacks against SPHERE CI
  - Scanning, spamming, cryptojacking, data exfiltration, ransomware, DDoS, etc.
- Develop plugins to monitor system behavior
  - User interfaces, OSes, networks
  - Bare metal nodes, hypervisors, switches



Logical Attack Model *Realistic Deployment*

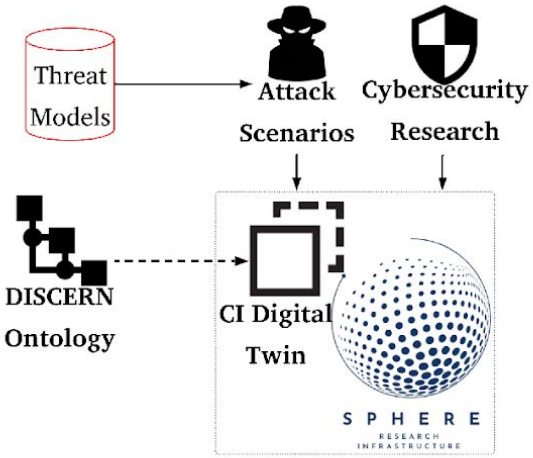
- Security "frameworks" improve awareness, but they put the onus on operators to assess their security posture and require significant time investment



"What-if" scenario assessment

- What-if a zero-day leads to a Docker breakout on my portal?
- What-if a privileged context deploys the latest malware?

- Transition DISCERN CI ontologies and threat models onto SPHERE research infrastructure
- Evaluate security research through digital twinning



Impact

- Datasets capturing benign and malicious workload characteristics on a modern CI platform
- Portable tools to enable collection of CI usage datasets on other community CI
- Ontology + DSL to describe CI implementations
- Tools to infer CI ontologies through passive and active measurement
- Datasets describing (1) modern CI implementations using the DISCERN DSL, with (2) what-if threat model CI evaluations
- Test and evaluation of cybersecurity research transitioned on modern CIs