

# Cybersecurity Technology for Critical Power Infrastructure AI-Based Centralized Defense and Edge Resilience

## Quarterly Review Workshop III Agenda

August 24 - 25, 2022

Israel Time: 7-9 pm

US Time: 12 pm - 2 pm (EST), 9 am - 11 am (PST/MST)

### Purpose of Quarterly Review Workshop

Welcome to the BIRD-ICRDE cybersecurity project workshop III. We are delighted to have this opportunity to share with the consortium members some progress updates of this Israel-US binational joint project. The workshop will be on August 24-25. The Principal Investigator(s) of each task will present their research results and discuss plans for future quarters. The focus of the presentations will be on *tool development*, demonstration of the *practical values and potential impact* of the research solutions for early cyberattack stages, and *commercialization* in collaboration with industry partners. The workshop will be conducted via zoom video conferencing and recorded for future reference. Please use the link below to join the workshop.

<https://asu.zoom.us/j/6712258140>

**Agenda** (Moderator: Yang Weng) (all times are in Israeli time):

August 24 (Wed):

- |           |  |
|-----------|--|
| 7:00-7:15 | Task 10: Multi-layer anomaly detection framework<br>Nir Nissim, Asaf Shabtai, Robert Moskovitch (BGU), Ron Insler (RAD)                        |
| 7:15-7:30 | Task 12: Explainable cyber A.I. analytics<br>Liat Antwarg, Nir Nissim (BGU)  |
| 7:30-7:50 | Task 2: Digital rep. of physical processes & operational process modelling<br>Task 15: Self-healing and auto-remediation<br>Asaf Shabtai (BGU) |
| 7:50-8:00 | Task 1: Realization of advanced energy management applications<br>Yang Weng (ASU), John Dirkman (Resource Innovations)                         |
| 8:00-8:15 | Task 3: Data collection and aggregation  |

Matan Dobrushin (OTORIO), Rami Puzis (BGU)  
 8:15-8:30 Task 4: Multi-level threat intelligence knowledge base  
 Lior Rokach, Rami Puzis (BGU)  
 8:30-8:45 Task 6: Threat hunting  
 Rami Puzis (BGU)  
 8:45-9:00 Task 17: ICS security by design  
 Yuval Elovici (BGU), Ron Insler (RAD)

August 25 (Thu):

7:00-7:20 Task 5: GANs for generating adversarial attacks  
 Task 8: Detect event mimicking attacks  
 Lalitha Sankar (ASU)  
 7:20-7:35 Task 7: Malware threats mitigation  
 Wenke Lee (GIT)  
 7:35-7:50 Task 9: False data injection  
 Hagai Galili, Ilan Gendelman (SIGA)  
 7:50-8:00 Task 11: AI based intrusion detection  
 Ying-Cheng Lai (ASU), Yisroel Mirsky (BGU)  
 8:00-8:10 Task 16: Reinforcement learning control for cyber physical systems  
 Ying-Cheng Lai (ASU)  
 8:10-8:25 Task 13: Firmware verification  
 Yossi Oren (BGU)  
 8:25-8:40 Task 14: Cyberattack tolerance  
 Sukarno Mertoguno (GIT)  
 8:40-8:50 Task 18: Hardware-in-the-loop validation  
 Yang Weng (ASU)  
 8:50-9:00 Task 19: Innovation, education, coordination, and marketing Programs  
 Dan Bloomberg (BGU)

ICRDE Management Team (Yang Weng, Rami Puzis, Aviad Elyashar, Chin-Woo Tan, Shuman Luo)

