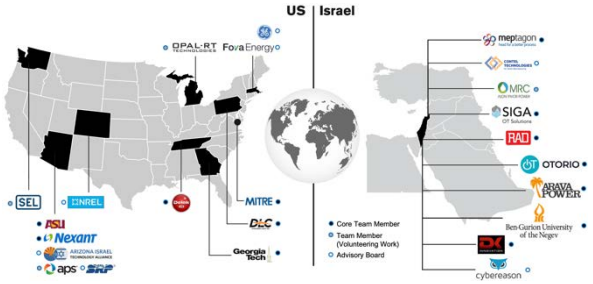

Converging Cybersecurity Solutions for Energy Systems to Practice

Meptagon Lab Dataset (2023-01-25) Description

Matan Dobrushin

OTORIO

February 22, 2023, 7:00 - 8:00 pm, Israeli time

(12:00-1:00 pm ET, 10:00-11:00 am MT/MST, 9:00 am-10:00 am PT)

Link: https://asu.zoom.us/j/6712258140

Abstract: To maximize the potential value of the algorithms developed in the BIRD ICRDE consortium, a physical lab built by Meptagon and Siga in the past, used as a real OT physical testbed to execute live attacks on it, and to later be analyzed by the Consortium members. During the last month, OTORIO collected data from the demonstrator including before, during, and after various attack scenarios.

The dataset includes full raw logs of both endpoint, network and OT (PLC), including all parts of the attack. The data sources include Raw PCAPs, I/O (time series) sensor data, Windows Event log including Sysmon monitoring, SNMP traps and more. This Dataset, unlike any other publicly available, contains data from IT/OT sensors, before during and after real attack scenarios actually used by attackers. This talk will explore the dataset collected from Meptagon, including the attacks that were executed, the structure of the raw logs, etc. for the benefits of all academic partners.

Bio:

Matan is a cyber security researcher with a vast experience in both Informational and Operational technologies, along with researching & implementing complex systems. These days, He manage more than a dozen top-notch security researchers that explore novel threats and OT technologies research projects that help position OTORIO as a leading OT research entity. Prior to OTORIO, Matan served as a commander in Israel's IDF elite cyber units.