

# REVERSE ANALYSIS - OT - LEVEL 2



Trainees will find, research and suggest ways to bring back the environment to full function with the tools in hand - Sysinternals, Wireshark, Engineering Station. The trainees will create a timeline of the attacks.

**Days: 2**

Trainees: 12

Level: Advanced

**Topic: Forensic**

Sector: OT

Sub Sector: Generation

## Description

Reverse Analysis is an advanced forensics training that starts 1 day before the trainees arrive. The red team attacks the arena and when the trainees arrive to the arena, it has already been hacked for some time. The mission of the trainees is to analyze and suggest actions to solve the hack and restore the system to activity. Attack creates a fake PLC and creates a "man in the middle" between the HMI and the real PLC. The APT starts in the IT environment.

## Target Audience

- IT/OT Professional
- Junior OT security personnel in process of qualification
- Technical personnel in the fields of OT
- SOC Analyst

## Training Outcomes

- Ability to execute well-designed procedures during an actual cyberattacks
- Acquire critical knowledge required to successfully manage a cyber crisis
- Acquiring theoretical knowledge and first-hand experience in monitoring and protecting critical infrastructure in an OT-centric organization.
- Ability to analyze a hacked system and create a timeline of the attack

### Mandatory Prerequisites



- · Basic SIEM operation and configuration knowledge
- · Basic background knowledge of information security concepts and solutions
- · Be familiar with computer and Operating Systems architecture and internals
- · OT background
- · IR principal Tactics training
- · IR advanced Tactics training



## Contact information

For any inquiries on this course, reach out to:

[info@cyberpax.eu](mailto:info@cyberpax.eu)

+30 210 7525 363