OT/ICS Cyber Range Argentina

Turning the industrial cybersecurity into practice

KPMG has set up an OT/ICS Cyber rage lab, using production grade equipment to simulate in a controlled manner scale-model version of the industrial processes. The OT/ICS Range will allow our clients to establish secure remote connections through our infrastructure, with the purpose of performing hands-on training sessions, cyber-attacks simulations, proof-of-concepts (PoCs), and develop industrial cybersecurity-related research. By leveraging on our unique industrial ecosystem, our specialists will be up-to-date regarding any industrial cybersecurity practice-related subject, with the goal to offer tailored and comprehensive solutions to our clients.

2 Oil Treatment Plant

A narrowed version of a treatment plant, where the crude is processed and separated from the gas, and send them to Gas processing plants and Refineries.

3 Gas-fired Power Plant

A simulated gas-fired power plant, which reproduces the activation of the turbine vanes caused by the influx of gas injected from the gas processing plant output pipeline.

1 Artificial Lift (Oil & Gas)

A production scale model of an artificial Lift set up designed with a PCP (progressing Cavity Pump), is measuring multiple operational variables such as: pressure, flow and temperature.

Industrial multi-vendor ecosystem with production-grade equipment and virtualized systems commonly used in the major industries.

Full visibility and fundamental controls for industrial networks

CLAROTY

Nowadays many organizations don't have full and continuous visibility of the ongoing cyber events in their OT network.

To streamline the adoption process of a cybersecurity solution for the visibility and continuous cyber-event monitoring, our lab is equipped with an on-premise Claroty CTD Architecture, that will ease up the experience of understanding Claroty's capabilities, such as: asset discovery and threat detection.

Capabilities

Protect
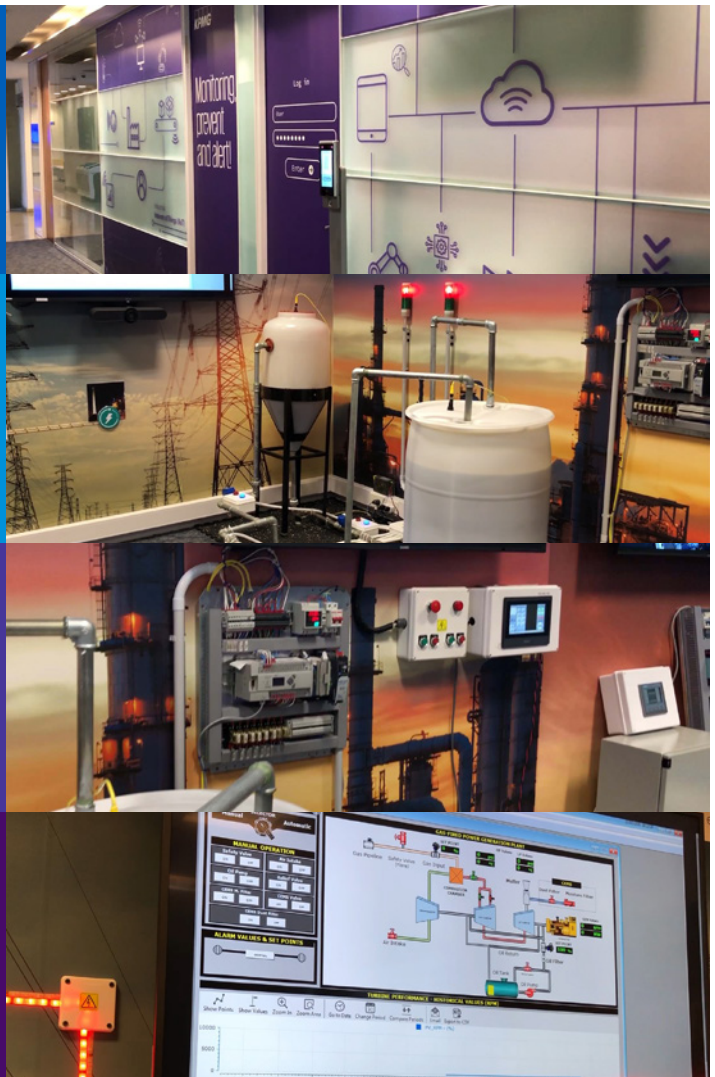Detect vulnerabilities, insecure configurations, and unauthorized connections.

Control
Enforce network segmentation and manage remote access.

Detect
Continuously monitor and detect malicious activity.

Respond
Receive context rich alerts for rapid triage and investigation.

OT/ICS Cyber Range Use Cases

1 OT Cybersecurity Hands-On Training Sessions

Performing online training sessions with production-grade equipment, in order to solidify OT/ICS Cybersecurity concepts to establish a mind-shift within the audience supporting them to perform their daily tasks in a cybersafe way.

2 OT Cybersecurity Tool demos

The goal of the hands-on demos of Cybersecurity tools is to better understand the technical capabilities of the tool and evaluate them on multiple scenarios. The demos can be requested without restrictions through our communication channels detailed in the "Contact Us" section.

4 OT Cybersecurity Remediations Testing

Prior the implementation of a cybersecurity remediation plan, our local team of specialist could perform testing procedures to validate and review that effectiveness and reliance of the workaround in a similar architecture.
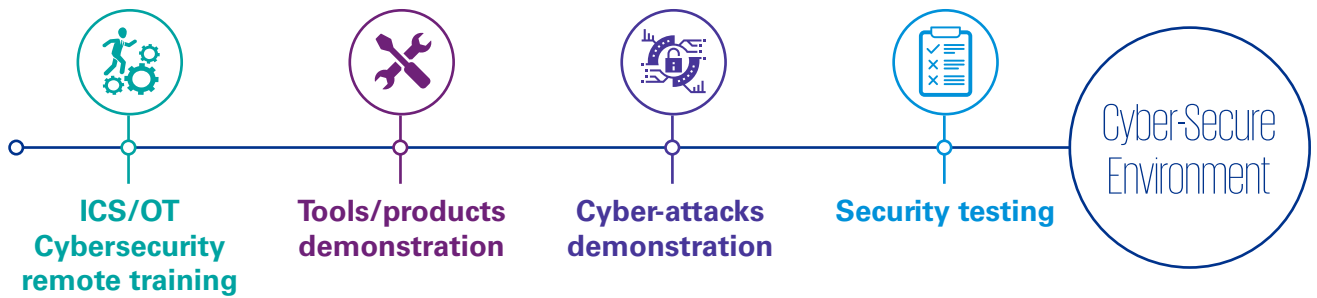
3 OT Cyber-Attack demos

Through on multiple cyber attack scenarios applied on the industrial environment we pretend to show how OT assets function can be crippled. Also, the details related to the attacks such as vulnerabilities to exploit, potential damage caused to the equipment, among other topics will be discussed.

ICS/OT
Cybersecurity
remote training

Tools/products
demonstration

Cyber-attacks
demonstration

Security testing

Cyber-Secure
Environment

Contact us:

Walter Risi
Global Cyber IoT Lead
and Consulting Partner
wrisi@kpmg.com.ar
KPMG in Argentina

Pablo Almada
Director IT Advisory
palmada@kpmg.com.ar
KPMG in Argentina

kpmg.com.ar