abhisam

Understanding OT Cybersecurity & IEC 62443- Training Workshop

Venue: Mumbai

Date: 2nd & 3rd August 2024

abhisam

What is this training event all about?

OT is short for Operational Technology. These are computer based systems that control physical objects and parameters in the real world. Although these systems do process data, their main function is to monitor and control physical objects and parameters. Some examples of OT systems include:

* Industrial Automation and Control Systems (including DCS/PLC/SCADA/SIS)
* Building Automation Systems
* Heating, Ventilation & Airconditioning (HVAC) Control Systems
* Ship Steering & Control Systems
* Marine Port cranes
* Automated Warehouse Stacking Systems

There are more such systems and they are in many different industrial sectors.

Real Life Exercises

This training event is not all talk.

Participate in real life exercises in the workshop including the following:

a) Evaluate an OT architecture for cyber resilience-spot weaknesses and vulnerabilities.
b) Modify it to become more resilient
c) Develop a new OT CSMS (Cyber Security Management System)
d) Conduct a Cyber Risk Assessment for your OT System

Some Participants in earlier workshops & feedback

Participants from marquee organizations such as GACL, Toyo Engg, Thyssenkrupp, HCL Technologies, Schneider, Worley and others have participated in earlier workshops.

 sales@abhisam.com

Abhisam's OT Cybersecurity workshops and self-paced e-learning courses have seen participation from several hundreds of professionals from all over the world including from several marquee organizations. Here's a sampling of the excellent feedback from participants.

Thanks to this workshop, I will now be able to define cybersecurity requirements & specifications very well for my client for the next project as well conduct risk assessments effectively
Participant from Worley

Great knowledge gained about OT Security. It will help protect our DCS from cyber attacks
Participant from Gujarat Alkalies and Chemicals

I was able to very well understand the different parts of IEC 62443 and how to apply the clauses of different parts-
Participant from Thyssenkrupp

Exciting real life examples and Case Studies-
Participant from Toyo Engineering

Why is OT Cybersecurity different from IT cybersecurity?

Both OT systems and IT systems are computer based systems that may be vulnerable to cyberattacks. A cyber attack on an IT system may result in loss of data, information and perhaps money; however **an attack on an OT system may result in not only loss or theft of data, but may also lead to physical consequences such as fires, explosions, loss of containment, equipment damage, harm to people and harm to the environment.**

Many OT systems that exist today are insecure from the design stage itself, since it was never envisaged that they would be the target of cyberattacks. Additionally, the priorities of defending OT systems and IT systems are

 sales@abhisam.com

different, so the strategies and techniques are also different. For IT systems confidentiality of data is a priority whereas for OT systems, availability & safety are priorities. Furthermore, OT systems may be a few generations older than IT systems and the cyber security tools commonly used to protect IT systems may not be suitable for protecting OT systems.

Additionally, the standards that govern OT systems (such as IEC 62443) are different from IT cybersecurity standards.

Who Should attend?

Any technical professional who has some work experience in working with any IT system or OT system can attend. Participants should have a basic understanding of computers, networking and preferably be familiar with typical industrial operations.

Some typical attendee profiles are:

* Instrumentation & Automation Professionals from end users, EPC companies, Automation vendors, system integrators, engg consultants
* IT Heads (CIOs) from manufacturing or Critical Infrastructure or Marine operations or Transportation or similar organizations having cyber-physical systems
* IT Cybersecurity Professionals including CISOs who wish to understand OT security in more detail
* IT Cybersecurity Auditors
* Process Safety Professionals
* Industrial Plant or Process Engineers
* Management Consultants

 sales@abhisam.com

abhisam

What will be covered?

The following topics will be covered.

1. Introduction to Operational Technology (OT) systems.
2. Differences between OT security and IT security.
3. Basic Concepts of OT security- Threats, Vulnerabilities & Attacks
4. Case Study of an OT attack
5. Evaluating OT System architectures for vulnerabilities and weaknesses
6. Introduction to CSMS
7. Overview of different standards related to OT cybersecurity
8. Introduction to IEC 62443 & **Changed Structure in 2024**
9. Overview of following (published) parts of IEC 62443
   - IEC 62443-1-1
   - IEC 62443-2-1
   - IEC 62443-2-3
   - IEC 62443-2-4
   - IEC 62443-3-1
   - IEC 62443-3-2
   - IEC 62443-3-3
   - IEC 62443-4-1
   - IEC 62443-4-2
10. Carrying out an OT Security Risk Assessment
11. Tabletop Exercise- Red Team & Blue Team

Few Discounted Early Bird tickets are available up to 15th July 2024. Click here to book.

Registration will close immediately after all tickets (Early Bird and Regular) are sold.
Book now to get a seat.

How to Register?

Please visit the link below. A few Early Bird discounted tickets available ONLY until 7th July 2024. For organizations wishing to nominate, please contact us.

https://www.explara.com/e/understanding-ot-cyber-security-and-iec-62443

More Information?

Contact us at sales@abhisam.com or Call/WhatsApp on +91 9664404771 OR Call us/Telegram us on +91 7208060349