SYGNIA

FOUNDATIONAL OT SECURITY BEST PRACTICES

COURSE DESCRIPTION

Delivery Method:

- Instructor-led
- On-site guided workshops
- Remote web-based

Session Format:

- Knowledge sharing
- Focused exercises

Learning Level:

- Basic
- Intermediate

Course Summary:

This foundational workshop is designed to raise awareness and promote secure practices for security and cross-functional industrial teams.

Students will explore OT-specific threat scenarios, common vulnerabilities, and essential security practices needed to improve their cyber resilience across legacy and modern industrial control systems.

Participants will gain understanding of the operational consequences attached to OT cyber risk and foster an improved collaboration across critical engineering and cyber defense teams.

How We Do It:

Sygnia instructors share field-proven security best practices developed from real-world use cases seen on the frontlines, including ransomware attacks and well-known OT breaches like Colonial Pipeline, TRISIS, and BlackEnergy.

Students are guided through the OT cyber kill chain and common attacker pathways that illustrate the security challenges of these tailored scenarios.

Practical recommendations are provided for remote access, backup strategies, network segmentation, patch management, and third-party vendor handling.

Course Outcomes:

After completing this workshop, participants will be able to:

- Identify cyber risks relevant to their OT environments
- Apply essential security practices that address your specific threat landscape
- Strengthen secure remote access, change control, and recovery measures
- Collaborate more effectively across OT & IT functions

For Who:

- Security teams
- CISOs
- OT cybersecurity owners
- OT engineers
- Control system integrators
- Site managers
- Asset operators

Prerequisites:

None required; content is designed for cross-functional participation

Duration:

2 hours minimum - 1 day maximum depending on client needs

Ideal Timeline:

This course is most beneficial when conducted:

- During onboarding of new OT engineers or security team members
- Prior to deploying or upgrading ICS/OT architecture or security controls
- Prior to a regulatory audit or compliance-driven assessment
- In accordance with digital transformation projects, particularly those involving new connectivity, remote access, or third-party integrations