SYGNIA

HOW TO BUILD AN EFFECTIVE OT DETECTION STRATEGY

COURSE DESCRIPTION

Delivery Method:

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

Session Format:

- Focused exercise
- Strategic planning exercises

Learning Level:

- Intermediate
- Advanced

Course Summary:

This workshop provides students with a structured and field-proven approach to building a detection strategy tailored for their OT environments.

Participants will define visibility objectives, map detection use cases using ICS threat models, and build a phased roadmap aligned with their environment's operational constraints, safety priorities, and available technologies.

How We Do It:

Sygnia instructors provide guidance and best practice recommendations for students to effectively map their OT architecture and identify visibility gaps that currently inhibit their cyber defense capabilities.

An understanding of the dedicated ICS MITRE ATT&CK framework is established and then detections are prioritized based on the asset criticality of your environment's crown jewels and most common threat vectors.

Students will leverage existing tools to design use cases and layer detection capabilities that will improve their ability to help proactively prevent compromise.

The course will conclude with the creation of a scalable detection roadmap that provides clear and actionable milestones.

Course Outcomes:

After completing this workshop, participants will be able to:

- Map system architecture, boundaries, and critical assets across your OT environment
- Identify detection gaps and visibility blind spots based on above mapping
- Design prioritized use cases for detection in your OT environment
- Integrate detection efforts with SOC/IT monitoring tools
- Build a scalable, phased detection strategy with technical justification
- Communicate detection priorities effectively to management and executive teams

For Who:

- Security Operations (SOC) teams
- OT detection engineers
- IR teams
- CISOs
- OT cybersecurity architects

Prerequisites:

Familiarity with industrial environments and basic detection concepts

Duration:

2 hours minimum - 1 day maximum, depending on client objecives and environment maturity

Ideal Timeline:

This course is most beneficial when conducted:

- During onboarding of OT detection engineers, SOC analysts, or IR team members
- Prior to planning or upgrading an ICS/OT detection strategy
- Post-incident or following a detection failure