



OT Security Information and Event Management (SIEM)

Course Introduction:

This course provides a comprehensive overview of OT SIEM, focusing on its importance in securing industrial environments. Participants will learn about the principles, tools, and best practices for implementing and managing SIEM systems in OT settings.

Course Objectives:

Upon the successful completion of this course, each participant will be able to:-

- Understand the fundamentals of OT security and the role of SIEM.
- Learn about the architecture and components of SIEM systems.
- Develop skills in configuring and managing SIEM tools for OT environments.
- Familiarize with incident detection, response, and reporting using SIEM.
- Explore best practices for optimizing SIEM performance and effectiveness.

Who Should Attend?

- OT security professionals
- IT security personnel
- Network administrators
- Compliance and risk management staff
- Anyone involved in OT security operations

Course Outline:

Day 1: Introduction to OT Security

- **Morning Session**
 - Overview of Operational Technology (OT) and its importance
 - Key differences between IT and OT security
- **Afternoon Session**
 - Understanding threats and vulnerabilities in OT environments
 - Importance of SIEM in OT security management

Day 2: SIEM Fundamentals

- **Morning Session**
 - Introduction to Security Information and Event Management (SIEM)
 - Key components and architecture of SIEM systems
- **Afternoon Session**
 - Data sources for SIEM: logs, events, and alerts from OT systems

- Overview of common SIEM tools and technologies

Day 3: Implementing SIEM in OT Environments

- **Morning Session**
 - Steps for deploying a SIEM solution in OT settings
 - Configuring data collection and normalization processes
- **Afternoon Session**
 - Creating security policies and rules for event correlation
 - Hands-on exercise: Setting up a SIEM tool for OT data

Day 4: Incident Detection and Response

- **Morning Session**
 - Understanding incident detection methodologies using SIEM
 - Analyzing alerts and prioritizing incidents
- **Afternoon Session**
 - Incident response procedures and best practices
 - Hands-on exercise: Responding to simulated security incidents

Day 5: Optimization and Best Practices

- **Morning Session**
 - Evaluating SIEM performance and effectiveness
 - Techniques for tuning and optimizing SIEM systems
- **Afternoon Session**
 - Best practices for continuous improvement in OT security
 - Group discussions on case studies and lessons learned
 - Conclusion and distribution of certificates of completion

Course Methodology:

A variety of methodologies will be used during the course that includes:

- (30%) Based on Case Studies
- (30%) Techniques
- (30%) Role Play
- (10%) Concepts
- Pre-test and Post-test
- Variety of Learning Methods

- Lectures
- Case Studies and Self Questionnaires
- Group Work
- Discussion
- Presentation

Course Certificate:

International Center for Training & Development (ICTD) will award an internationally recognized certificate(s) for each delegate on completion of training.

Course Fees:

To be advised as per course locations. This rate includes participant's manual, Hand-Outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Course Timings:

Daily Course Timings:

08:00 - 08:20	Morning Coffee / Tea
08:20 - 10:00	First Session
10:00 - 10:20	Coffee / Tea / Snacks
10:20 - 12:20	Second Session
12:20 - 13:30	Lunch Break & Prayer Break
13:30 - 15:00	Last Session