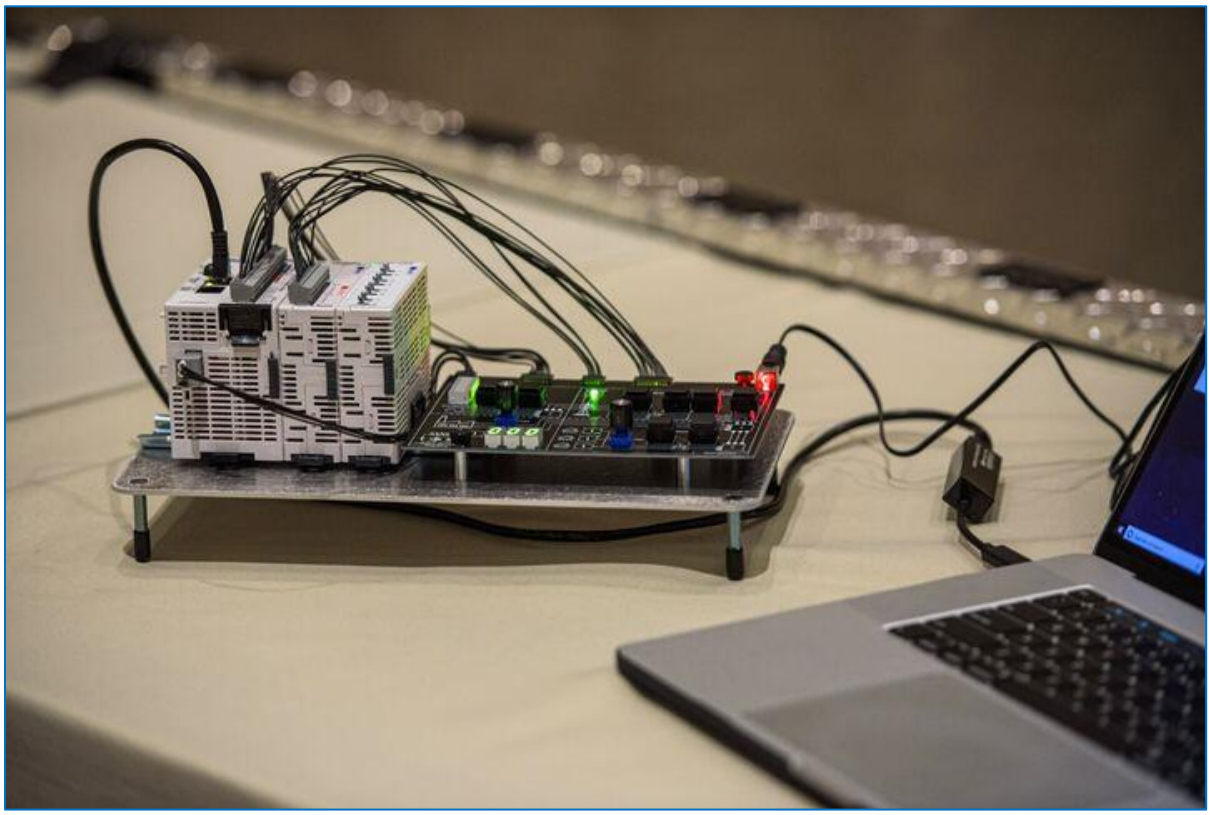
Tel No:+97126654546 | Fax No:+97126654182 | Email: training@cmc-me.com | www.cmc-me.com



IE293:
ICS Visibility, Detection & Response

Training Description:

Industrial Control Systems (ICS) are increasingly targeted by sophisticated cyber threats that can disrupt critical infrastructure, manufacturing, oil & gas, power generation, water treatment, transportation and other industrial operations. Unlike traditional IT environments, ICS networks require specialized visibility, monitoring and incident response approaches that maintain operational continuity while ensuring cybersecurity.

This intensive training course provides participants with the knowledge and practical skills required to establish effective ICS visibility, detect cyber threats across Operational Technology (OT) environments, and implement structured incident detection and response processes. Participants will learn modern OT security architectures, industrial protocols, asset discovery techniques, anomaly detection methods, threat intelligence integration, Security Operations Center (SOC) practices for OT and incident response aligned with international standards such as IEC 62443, NIST Cybersecurity Framework (CSF), NIST SP 800-82 and MITRE ATT&CK for ICS.

Training Objectives:

By the end of the training, participants will be able to:

- ✓ Understand ICS/SCADA and OT cybersecurity principles
- ✓ Identify unique threats targeting industrial environments
- ✓ Develop comprehensive OT asset visibility strategies
- ✓ Discover and classify industrial assets without operational disruption
- ✓ Understand industrial communication protocols and network behaviors
- ✓ Deploy passive monitoring solutions for ICS networks
- ✓ Detect cyber threats using behavioral analytics and anomaly detection
- ✓ Analyze industrial security events using OT-specific indicators
- ✓ Utilize MITRE ATT&CK for ICS during threat hunting activities
- ✓ Develop effective ICS incident detection and response procedures
- ✓ Integrate SOC operations with industrial cybersecurity monitoring
- ✓ Improve organizational cyber resilience for critical infrastructure

Training Designed for:

This training course is intended for ICS/SCADA Engineers, Control System Engineers, OT Cybersecurity Engineers, Security Operations Center (SOC) Analysts, Industrial Network Engineers, Control Room Operators, Plant Automation Engineers, Cybersecurity Analysts, Incident Response Teams, Risk Management Professionals, Industrial IT Administrators, Critical Infrastructure Security Personnel, Operations Managers, Reliability Engineers and Technical Managers responsible for OT environments.

Training Requirement:

"Hand's on practical sessions, equipment and software will be applied during the course if required and as per the client's request."

Contents can be adapted to your specific wishes. It is therefore possible to focus on specific modules of the training course as per client's learning needs and objectives. Further, it should be forwarded to us a month prior to the course dates.

Training Program:

DAY ONE:

FOUNDATIONS OF ICS VISIBILITY & OPERATIONAL TECHNOLOGY SECURITY

- Module 1: Introduction to ICS Cybersecurity
  - IT vs OT environments
  - Industrial control system architecture
  - ICS ecosystem overview
  - Purdue Enterprise Reference Architecture
  - SCADA, DCS, PLC, RTU, HMI fundamentals
  - Safety Instrumented Systems (SIS)
- Module 2: ICS Threat Landscape
  - Evolution of OT cyber attacks
  - Recent attacks on critical infrastructure
  - Threat actors targeting industrial environments
  - Common ICS attack vectors
  - Supply chain risks
  - Insider threats
- Module 3: Industrial Standards
  - IEC 62443 overview
  - NIST SP 800-82
  - NIST Cybersecurity Framework
  - ISO 27001 considerations
  - ISA/IEC security zones and conduits
- Module 4: ICS Asset Visibility
  - Importance of OT asset inventories
  - Passive asset discovery
  - Active discovery limitations
  - Identifying unmanaged assets
  - Firmware identification
  - Device fingerprinting
- Practical Exercises:
  - Building an OT asset inventory
  - Identifying industrial devices
  - ICS network mapping exercise

DAY TWO:

ICS NETWORK VISIBILITY & MONITORING

- Module 5: Industrial Network Architecture
  - Industrial Ethernet
  - Layer 2 and Layer 3 industrial communications
  - Segmentation strategies
  - Secure network design
  - Remote access security
- Module 6: Industrial Protocol Analysis

- Modbus TCP
- DNP3
- OPC UA
- Ethernet/IP
- Profinet
- BACnet
- IEC 61850
- MQTT in industrial environments

❖ Module 7: Passive Network Monitoring
- SPAN ports
- Network TAPs
- Deep Packet Inspection (DPI)
- OT network sensors
- Industrial packet capture

❖ Module 8: OT Visibility Platforms
Overview of leading OT monitoring solutions
- Nozomi Networks
- Claroty
- Microsoft Defender for IoT
- Dragos Platform
- Tenable.ot
- Armis

❖ Practical Exercises:
- Industrial traffic analysis
- Identifying abnormal communications
- Mapping communication paths
- Baseline creation

DAY THREE:

THREAT DETECTION & SECURITY MONITORING

❖ Module 9: Detection Engineering
- Indicators of Compromise (IOCs)
- Indicators of Attack (IOAs)
- Behavioral detection
- Signature-based detection
- Machine learning applications

❖ Module 10: Industrial Threat Hunting
- Threat hunting methodology
- MITRE ATT&CK for ICS
- Mapping adversary behaviors
- Lateral movement detection
- Privilege escalation indicators

❖ Module 11: Security Monitoring
- Security Information and Event Management (SIEM)
- OT log collection
- Event correlation

- Alarm tuning
- False positive reduction

❖ Module 12: Threat Intelligence
- ICS threat intelligence sources
- Industrial malware families
  - Stuxnet
  - Triton
  - Industroyer
  - BlackEnergy
  - Havex
  - Pipedream
- Intelligence-driven detection

❖ Practical Exercises:
- Creating detection rules
- SIEM event analysis
- ATT&CK mapping exercise
- Threat hunting simulation

DAY FOUR:

INCIDENT DETECTION & RESPONSE

❖ Module 13: ICS Incident Response Framework
- Preparing for incidents
- Incident lifecycle
- OT-specific response planning
- Safety considerations
- Business continuity

❖ Module 14: Detection & Investigation
- Alert triage
- Root cause analysis
- Timeline reconstruction
- Digital forensics considerations
- Evidence preservation

❖ Module 15: Responding to ICS Incidents
- Containment strategies
- Isolation procedures
- Recovery planning
- Operational coordination
- Crisis communications

❖ Module 16: SOC Operations for OT
- Building an OT SOC
- IT/OT collaboration
- Escalation procedures
- OT playbooks
- Reporting and documentation

❖ Practical Exercises:
- ICS incident simulation

- Response coordination exercise
- Incident reporting
- Executive briefing preparation

DAY FIVE:

ADVANCED DETECTION, RESILIENCE & CONTINUOUS IMPROVEMENT

- Module 17: Advanced Detection Technologies
  - Artificial Intelligence in OT monitoring
  - User and Entity Behavior Analytics (UEBA)
  - Extended Detection and Response (XDR)
  - Network Detection and Response (NDR)
  - Security Orchestration, Automation, and Response (SOAR)
- Module 18: Continuous Monitoring
  - Key Performance Indicators (KPIs)
  - Security metrics
  - Detection maturity assessment
  - Continuous improvement programs
- Module 19: Building a Cyber-Resilient ICS Environment
  - Zero Trust for OT
  - Defense-in-depth
  - Network segmentation validation
  - Backup and recovery
  - Secure remote maintenance
  - Vendor access management
- Module 20: Future of ICS Cybersecurity
  - IEC 62443 roadmap
  - Industrial IoT security
  - Edge computing security
  - Cloud-connected industrial systems
  - Emerging cyber threats
- Exercises:
  Participants work through a comprehensive ICS cyber incident scenario involving:
  - Asset identification
  - Network visibility analysis
  - Threat detection
  - Attack path identification
  - MITRE ATT&CK mapping
  - Incident investigation
  - Response planning
  - Recovery strategy
- Course Conclusion
- POST-ASSESSMENT and EVALUATION

Training Methodology:

This interactive training course includes the following training methodologies as a percentage of the total tuition hours:

- 30% Lectures, Concepts, Role Play
- 70% Workshops & Work Presentations, Techniques, Based on Case Studies & Practical Exercises, Gamification, Software & General Discussions
- Pre and Post Test

Training Certificate(s):

CMCT Internationally recognized certificate(s) will be issued to each participant who completed the course.

Training Fees:

USD$ TBA - This rate includes participant's manual, hand-outs, buffet lunch, coffee/tea on arrival, morning & afternoon of each day.

Note: The 5% VAT (Value Added Tax), will be effective starting 01st of January 2018 as per the new regulation from the UAE Government. The VAT applies for all quotation both for local and abroad.

Training Timings:

Daily Timings:

07:45 - 08:00	Morning Coffee / Tea
08:00 - 10:00	First Session
10:00 - 10:20	Recess (Coffee/Tea/Snacks)
10:20 - 12:20	Second Session
12:20 - 13:00	Recess (Prayer Break & Lunch)
13:00 - 14:00	Last Session

For training registrations or in-house enquiries, please contact:
Aisha Relativo - Training & Career Development Manager
aisha@cmc-me.com / training@cmc-me.com
Tel.: +971 2 665 3945 or +971 2 643 6653 | Mob.: +971 52 2954615