Grid Cybersecurity Training Course

Professional Development Training Course Outline

Category	Renewable Energy	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Grid Cybersecurity Training Course is designed to strengthen the cyber resilience, operational technology (OT) security, critical infrastructure protection, and incident response capabilities required to defend modern electricity grids. As smart grids, distributed energy resources, Industrial Internet of Things (IIoT), digital substations, Advanced Metering Infrastructure (AMI), cloud platforms, and interconnected control systems continue to expand, utilities face increasingly sophisticated cyber threats, ransomware, supply-chain attacks, zero-day vulnerabilities, nation-state activity, and IT/OT convergence risks. This course equips professionals with the knowledge and practical skills to identify vulnerabilities, secure grid environments, protect SCADA and ICS architectures, implement Zero Trust security, strengthen identity and access management, and establish resilient cybersecurity controls across generation, transmission, distribution, and energy management environments.

Through hands-on labs, threat modeling, incident simulations, vulnerability assessments, tabletop exercises, and real-world case studies, participants learn how cybersecurity principles apply directly to critical power infrastructure. The course connects NERC CIP principles, IEC 62443 concepts, NIST Cybersecurity Framework practices, security monitoring, Security Operations Centers (SOC), SIEM, threat intelligence, network segmentation, encryption, endpoint protection, and cyber incident response to realistic utility scenarios. Participants will develop the confidence to detect, analyze, contain, and recover from cyber incidents while supporting business continuity, operational resilience, regulatory compliance, and secure digital transformation within the energy sector.

Programme Curriculum

Grid Cybersecurity Training Course

Introduction

Grid Cybersecurity Training Course is designed to strengthen the cyber resilience, operational technology (OT) security, critical infrastructure protection, and incident response capabilities required to defend modern electricity grids. As smart grids, distributed energy resources, Industrial Internet of Things (IIoT), digital substations, Advanced Metering Infrastructure (AMI), cloud platforms, and interconnected control systems continue to expand, utilities face increasingly sophisticated cyber threats, ransomware, supply-chain attacks, zero-day vulnerabilities, nation-state activity, and IT/OT convergence risks. This course equips professionals with the knowledge and practical skills to identify vulnerabilities, secure grid environments, protect SCADA and ICS architectures, implement Zero Trust security, strengthen identity and access management, and establish resilient cybersecurity controls across generation, transmission, distribution, and energy management environments.

Through hands-on labs, threat modeling, incident simulations, vulnerability assessments, tabletop exercises, and real-world case studies, participants learn how cybersecurity principles apply directly to critical power infrastructure. The course connects NERC CIP principles, IEC 62443 concepts, NIST Cybersecurity Framework practices, security monitoring, Security Operations Centers (SOC), SIEM, threat intelligence, network segmentation, encryption, endpoint protection, and cyber incident response to realistic utility scenarios. Participants will develop the confidence to detect, analyze, contain, and recover from cyber incidents while supporting business continuity, operational resilience, regulatory compliance, and secure digital transformation within the energy sector.

Course Duration

5 days

Course Objectives

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

1. Understand the grid cybersecurity threat landscape, including ransomware, malware, insider threats, nation-state attacks, and supply-chain compromise.
2. Analyze IT/OT convergence risks across modern power-generation, transmission, and distribution environments.
3. Secure SCADA, ICS, PLC, RTU, HMI, and industrial control systems against cyber threats.
4. Apply Zero Trust Architecture principles to critical energy infrastructure.
5. Perform OT vulnerability assessment, cyber risk assessment, and threat modeling for grid environments.
6. Implement effective network segmentation, secure remote access, firewalls, IDS/IPS, and industrial DMZs.
7. Apply NERC CIP, NIST CSF, IEC 62443, and critical-infrastructure cybersecurity concepts.
8. Strengthen identity and access management (IAM), privileged access management (PAM), and multi-factor authentication (MFA).
9. Develop capabilities for SIEM, SOC monitoring, threat detection, threat hunting, and cyber threat intelligence (CTI).
10. Design effective incident response, crisis management, containment, eradication, and recovery procedures.
11. Improve ransomware resilience, backup security, business continuity, and disaster recovery for grid operations.
12. Evaluate emerging risks from AI, cloud computing, IoT/IIoT, DERs, EV infrastructure, and smart-grid technologies.
13. Build an integrated cyber-resilience strategy that supports secure digital transformation and reliable power-grid operations.

Target Audience

1. Power-grid cybersecurity professionals
2. SCADA, ICS, and OT security engineers
3. IT security, SOC, and incident-response teams
4. Electrical and power-system engineers
5. Utility IT/OT managers and cybersecurity managers
6. Risk, compliance, audit, and governance professionals
7. Critical infrastructure and energy-sector consultants
8. CISOs, security architects, technology leaders, and government energy-security personnel

Course Modules

Module 1: Grid Cybersecurity Fundamentals & Threat Landscape

- Smart-grid cybersecurity
- Cyber threat landscape
- Critical infrastructure risk
- Threat modeling
- Case Study: Analyze the Ukraine power-grid cyberattacks to understand how attackers can move from initial access to operational disruption.

Module 2: SCADA, ICS & OT Security Architecture

- SCADA security
- IT/OT convergence
- ICS attack surfaces
- Secure architecture
- Case Study: Examine the Stuxnet incident to understand the consequences of targeted attacks against industrial control environments.

Module 3: Grid Vulnerability Assessment, Risk & Compliance

- OT vulnerability management
- Cyber risk assessment
- NERC CIP
- NIST CSF & IEC 62443
- Case Study: Conduct a simulated utility cyber-risk assessment involving critical assets, third-party connections, and remote engineering access.

Module 4: Network Security, Zero Trust & Secure Access

- Network segmentation
- Zero Trust Architecture
- Secure remote access.
- Intrusion detection
- Case Study: Respond to a simulated compromised vendor account attempting unauthorized access to a power-utility control network.

Module 5: Identity, Endpoint & Data Protection

- Identity and Access Management

- Privileged Access Management
- Endpoint security
- Data security
- Case Study: Investigate an insider-threat scenario involving excessive privileges and unauthorized changes to critical configuration files.

Module 6: SOC, SIEM, Threat Intelligence & Threat Hunting

- Security Operations Center
- SIEM
- Cyber Threat Intelligence
- Threat hunting
- Case Study: Perform a simulated ransomware investigation using SIEM alerts, endpoint evidence, network indicators, and threat intelligence.

Module 7: Incident Response, Ransomware & Cyber Resilience

- Incident response lifecycle
- Ransomware defense
- Tabletop exercises
- Business continuity
- Case Study: Manage a ransomware attack on a utility environment, balancing cybersecurity containment with continuous electricity-service requirements.

Module 8: Emerging Grid Technologies & Advanced Cyber Resilience

- AI and cybersecurity
- DER and smart-grid security
- Cloud and edge security
- Supply-chain cybersecurity
- Case Study: Develop a cyber-resilience strategy for a digitally connected smart-grid utility integrating DERs, cloud services, IoT devices, and remote operations.

Training Methodology

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call *+254769199797*

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com