Implementing NIST Cybersecurity Framework

Duration: 2 Days

COURSE DESCRIPTION

This course will guide participants through the NIST Cybersecurity Framework (CSF) 2.0, providing the knowledge and tools necessary to adopt and adapt the CSF effectively within their organizations. The course focuses on understanding the framework's structure, its core functions, profiles, and tiers—and on applying this knowledge through practical workshops that simulate real-world implementation scenarios.

COURSE OBJECTIVES

Participants will:

- Gain a deep understanding of the CSF 2.0's components: Core, Profiles, and Tiers.
- Develop skills to map their organization's current cybersecurity posture to the CSF and identify areas for improvement.
- Learn to create actionable plans for integrating CSF into their cybersecurity risk management programs.
- Engage in hands-on exercises that simulate the application of CSF in various organizational scenarios.

COURSE OUTLINE

Day 1: Introduction to NIST CSF and Understanding the Framework Core

Morning Session: Understanding the CSF Core

- Overview of NIST CSF 2.0
- Detailed review of CSF Functions: Identify, Protect, Detect, Respond, Recover
- **Workshop:** Participants will map their organization's current cybersecurity measures to the CSF Core functions.

Afternoon Session: Creating and Using CSF Profiles

- Introduction to CSF Profiles: Current and Target Profiles
- **Workshop:** Develop a Current Profile for your organization.
- **Workshop:** Design a Target Profile that addresses identified gaps from the Current Profile.

Day 2: Implementing and Managing Cybersecurity Improvements

Morning Session: CSF Tiers and Their Application

- Overview of CSF Tiers: Understanding maturity levels
- **Workshop:** Assess the organization's current tier and discuss strategies to advance to higher tiers.

Afternoon Session: Integrating CSF with Organizational Practices and Continuous Improvement

- Strategies for integrating CSF into existing policies and governance structures
- **Workshop:** Develop an integration plan for CSF implementation including stakeholder engagement, communication strategies, and setting up continuous improvement metrics.
- **Workshop:** Scenario-based exercise on using CSF to manage a cybersecurity incident from detection to recovery.

Closing and Evaluation

- Recap of the workshop and open discussion on implementation challenges.
- Feedback collection and provision of additional resources for ongoing learning.

This training is designed to not only convey theoretical knowledge but also to ensure practical, actionable understanding through continuous interaction and application of the NIST CSF 2.0 in various organizational contexts. This approach helps solidify learning and prepares participants to effectively implement and manage cybersecurity improvements using the framework.

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

WHO SHOULD ATTEND

- CISOs, Security Managers, and IT Managers
- Risk Management Professionals
- Compliance Officers
- Network and Systems Administrators
- Information Security Analysts

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th