Course Outline

NIST Cybersecurity Framework (NCSF) Boot Camp

Course Summary

Description

The three-day NIST Cybersecurity Bootcamp course is a combination of the NIST Cybersecurity Framework (NCSF) Foundation and Practitioner Training courses. The bootcamp provides a deep dive into the components of the NIST CSF and NIST Risk Management Framework (RMF) and how they align to risk management. The course will follow the principles of the NIST Cybersecurity Framework to design and implement (or improve) a cybersecurity program to protect critical assets. The bootcamp details defense in depth, creation of a Written Information Security Program, and implementing ongoing assessments for a continuous improvement plan. This course is suited for individuals working with and overseeing the cybersecurity of an organization, including CIOs, CISOs, IT Security workforce, and IT Directors/Managers/Personnel.

Topics

- Course Introduction
- The Basics of Cybersecurity
- A Holistic Study of the NIST Cybersecurity Framework
- Cybersecurity Activities: The Framework Core
- Risk Management Considerations: Framework Implementation Tiers
- Current and Desired Outcomes: Framework Profiles
- A Primer on the Seven Step Framework Implementation Process
- Risk Management in the NIST CSF and NIST RMF
- Real World Attacks
- The Components of the NIST Cybersecurity Framework
- Defense in Depth and the NIST Cybersecurity Framework
- Assessing Cybersecurity in the Subcategories
- Creating a Written Information Security Program
- A Practitioner's Deep Dive into Creating or Improving a Cybersecurity Program
- Continuous Cybersecurity Improvement

Audience

This course is suited for individuals working with and overseeing the cybersecurity of an organization, including CIOs, CISOs, IT Security workforce, and IT Directors/Managers/Personnel.

Prerequisites

There are no prerequisites for this course. Basic computing skills and security knowledge will be helpful.

Duration

Three days

Course Outline

NIST Cybersecurity Framework (NCSF) Boot Camp

Course Outline

I. Course Introduction
- A. Provides the student with information relative to the course and the conduct of the course in the classroom, virtual classroom, and course materials.

II. The Basics of Cybersecurity
- A. What is cybersecurity?
- B. Types of attackers
- C. Vulnerabilities
- D. Exploits
- E. Threats
- F. Controls
- G. Frameworks
- H. Risk-Based Cybersecurity

III. A Holistic Study of the NIST Cybersecurity Framework
- A. History
  1. EO 13636
  2. Cybersecurity Enhancement Act of 2014
  3. EO 13800
- B. Uses and Benefits of the Framework
- C. Attributes of the Framework
- D. Framework Component Introduction
  1. Framework Core
  2. Framework Profiles
  3. Framework Implementation Tiers

IV. Cybersecurity Activities: The Framework Core
- A. Purpose of the Core
- B. Core Functions, Categories, and Subcategories
- C. Informative References

V. Risk Management Considerations: Framework Implementation Tiers
- A. Purpose of the Tiers
- B. The Three Tiers
- C. Components of the Tiers
- D. Compare and contrast the NIST Cybersecurity Framework with the NIST Risk Management Framework

VI. Current and Desired Outcomes: Framework Profiles
- A. Purpose of the Profiles
- B. The Two Profiles
- C. Interrelationships between the Framework Components

VII. A Primer on the Seven Step Framework Implementation Process
- A. Prioritize and Scope
- B. Orient
- C. Create a Current Profile
- D. Conduct a Risk Assessment
- E. Create a Target Profile
- F. Determine, Analyze, and Prioritize Gaps
- G. Implement Action Plan

THE PRACTITIONER COURSE IS ORGANIZED AS FOLLOWS:

VIII. Course Introduction

IX. Risk Management in the NIST CSF and NIST RMF
- A. Risk Management in the NIST Cybersecurity Framework
- B. Analyzing the NIST Risk Management Framework
  1. Introduction and History
  2. Purpose and Use Cases
  3. Six Steps
     a) Categorize System
     b) Select Controls
     c) Implement Controls
     d) Assess Controls
     e) Authorize System
     f) Monitor Controls
- C. Integrating the Frameworks

X. Real World Attacks
- A. Major Cybersecurity Attacks and Breaches
- B. Cyber Kill Chain
- C. MITRE ATT&CK Matrices

XI. The Components of the NIST Cybersecurity Framework
- A. Tiers and Tier selection
- B. Current and Target Profiles and the Framework Core
- C. Deep dive in Informative References
  1. Center for Internet Security 20 Critical Security Controls
  2. ISO 27001:2013 Information Security Management System (ISMS)
  3. ISO 27002:2013 Code of Practice

Supply Chain Risk Management in the Enterprise

Course Outline

NIST Cybersecurity Framework (NCSF) Boot Camp

Course Outline (cont'd)

XII. Defense in Depth and the NIST Cybersecurity Framework
- A. Informative References, Subcategories, and Defense in Depth
- B. Aligning vendor Controls with Subcategories
- C. Security Operations Center (SOC) activities and Security Information and Event Management solutions in relation to the Framework

XIII. Assessing Cybersecurity in the Subcategories
- A. Creating an Assessment Project
- B. Tiers, Threats, Risks, Likelihoods, and Impact

XIV. Creating a Written Information Security Program
- A. The Intersection of Business and Technical Controls
- B. What is a Written Information Security Program (WISP)?
- C. Creating a WISP Template
- D. Aligning Current Profile with a WISP

XV. A Practitioner's Deep Dive into Creating or Improving a Cybersecurity Program
- A. Step 1: Prioritize and Scope
  1. Identifying organizational priorities
  2. Aiding and influencing strategic cybersecurity implementation decisions
  3. Determining scope of the implementation
  4. Planning for internal adaptation based on business line/process need
  5. Understanding risk tolerance
- B. Step 2: Orient
  1. Identifying systems and applications which support organizational priorities
  2. Working with compliance to determine regulatory and other obligations
  3. Planning for risk responsibility
- C. Step 3: Create a Current Profile
  1. Cybersecurity Assessment options
  2. How to measure real world in relation to the Framework
  3. Qualitative and quantitative metrics
  4. Current Profile and Implementation Tiers
- D. Step 4: Conduct a Risk Assessment
  1. Risk assessment options (3rd party vs internal)
  2. Organizational vs. system level risk assessment
  3. Risk assessment and external stakeholders
- E. Step 5: Create a Target Profile
  1. Target Profile and Steps 1-4
  2. External stakeholder considerations
  3. Adding Target Profiles outside the Subcategories
- F. Step 6: Determine, Analyze, and Prioritize Gaps
  1. Defining and determining Gaps
  2. Gap analysis and required resources
  3. Organizational factors in creating a prioritized action plan
- G. Step 7: Implement Action Plan
  1. Implementation team design from Executives to Technical Practitioners
  2. Assigning tasks when priorities conflict
  3. Considering compliance and privacy obligations
  4. Taking action
  5. Reporting and reviewing

XVI. Continuous Cybersecurity Improvement
- A. Creating a continuous improvement plan
- B. Implementing ongoing assessments