The Practitioner's Guide to the NIST Cyber Security Framework (CSF) v2

This course is for the technical people, who live and breathe cyber security. We'll strip away the jargon and deliver a deep, hands-on exploration of the NIST Cyber Security Framework (CSF) v2, showing you exactly how to translate its principles into actionable, technical controls. From hardening systems to architecting resilient networks, automating detection, and streamlining incident response, you'll gain the practical expertise to leverage CSF v2 as your ultimate blueprint for securing digital assets. Get ready to level up your technical capabilities and drive real, measurable improvements in your organisation's cyber posture.

High-Level Outline:

1. Introduction to NIST CSF v2
2. Govern (GV) - The Strategic Technical Blueprint
3. Identify (ID) & Protect (PR) - Building the Technical Foundation
4. Detect (DE), Respond (RS) & Recover (RC) - Operationalising Technical Resilience
5. Next steps and takeaways

Objectives:

Upon completion of this course, participants will be able to:

- Articulate the core principles of NIST CSF v2, including the new Govern function.
- Translate CSF v2 categories and subcategories into concrete technical requirements and implementation strategies.
- Apply the CSF v2 framework to assess, design, implement, and continuously improve an organisation's cybersecurity posture.
- Develop technical profiles and roadmaps for achieving target cybersecurity outcomes based on organisational risk tolerance and business objectives.
- Know which security tools, technologies, and best practices to operationalise each CSF v2 function effectively.

Learning Outcomes:

By the end of this course, attendees will be able to:

- Map organisational mission and objectives to technical cybersecurity requirements.
- Categorise and classify assets based on criticality, data sensitivity, and business impact.
- Design and implement robust technical controls to protect their endpoints, networks and cloud environments.
- Employ various technologies like IDS, SIEM and SOAR among others.
- Develop and test incident response plans for various cyberattack scenarios.
- Implement resilient architectures and procedures to ensure business resilience.

Course Duration: 6 Hours (Flexible, can be adapted)

Included: A plain English guide to the various controls required by NIST CSF v2, an IT Diary, suggestions for technical solutions to address some of the controls. Incident Response Plan, Business Impact Analysis, Business Continuity Plan, and IT Disaster Recovery Plan templates (in Word format). Also, a copy of the slides will be provided.

Audience: Technical staff, responsible for securing their company's systems.

Capacity: Maximum 10 attendees