NIST Cybersecurity Framework

A Comprehensive Guide for Organizations

Overview

The NIST Cybersecurity Framework provides a policy framework of computer security guidance for how private sector organizations in the United States can assess and improve their ability to prevent, detect, and respond to cyber attacks.

Core Functions

1. IDENTIFY (ID)
   - Asset Management
   - Business Environment
   - Governance
   - Risk Assessment
   - Risk Management Strategy

2. PROTECT (PR)
   - Identity Management and Access Control
   - Awareness and Training
   - Data Security
   - Information Protection Processes
   - Maintenance
   - Protective Technology

3. DETECT (DE)
   - Anomalies and Events
   - Security Continuous Monitoring
   - Detection Processes

4. RESPOND (RS)
   - Response Planning
   - Communications
   - Analysis
   - Mitigation
   - Improvements

5. RECOVER (RC)
   - Recovery Planning
   - Improvements
   - Communications

Implementation Tiers

Tier 1: Partial - Risk management practices are not formalized
Tier 2: Risk Informed - Risk management practices are approved
Tier 3: Repeatable - Risk management practices are formally approved and expressed as policy
Tier 4: Adaptive - Organization adapts its cybersecurity practices based on lessons learned

Framework Profiles

Current Profile: Current state of cybersecurity activities
Target Profile: Desired cybersecurity outcomes