Implementing the NIST Cybersecurity Framework (CSF)

**CSF Goals**
- Define current and target state
- Identify and prioritize opportunities for improvement
- Assess progress and communicate across organization
- Complement existing processes and programs

**Cavirin automates the suggested NIST process**

**Desired process**
- The suggested NIST Cavirin automates

**Red Hat Enterprise Linux 7**
- Function 1: Automate
- Function 2: Automate
- Function 3: Automate
- Function 4: Automate

**Identify (ID)**
- **Objective**: Develop the organizational understanding to identify the assets, risk, and capabilities.
- **Subcategories**:
  - **ISA**: Asset vulnerabilities are identified and documented.
  - **ID**: Supplier relationships are identified and documented.
  - **ID**: Threats, both internal and external, are identified and documented.
  - **ID**: Cyber threat intelligence and vulnerability information is received from external information sharing forums and sources.
  - **ID**: Key vulnerabilities and impacts are used to determine risk likelihoods.

**Protect (PR)**
- **Objective**: Prevent or contain the possibility of incidents occurring or spreading.
- **Subcategories**:
  - **PR**: Access Control
  - **PR**: Awareness and Training
  - **PR**: Data Security
  - **PR**: Maintenance

**Respond (RS)**
- **Objective**: Identify and prioritize opportunities for improvement
- **Subcategories**:
  - **RS**: Awareness and Training
  - **RS**: Communications
  - **RS**: Response Planning

**Recover (RC)**
- **Objective**: Plan for recovery and continuity
- **Subcategories**:
  - **RC**: Business Contingency Planning
  - **RC**: Data Loss Prevention

**Cavrin curated policy packs do the heavy lifting in mapping the framework to actionable recommendations**

**Cavrin Implementation**

**Prioritize and Scope**

**Conduct Risk Assessment**

**Assess and Prioritize Gaps**

**Create Current Profile**

**Implement Action Plan**