System Security Engineering Capability Maturity Model

Overview

The System Security Engineering Capability Maturity Model (SSE-CMM) is a process-oriented methodology used to develop secure systems based on the Software Engineering Capability Maturity Model.

Model

The SSE-CMM is organized into processes and maturity levels. Generally speaking, the processes define what needs to be accomplished by the security engineering process, and the maturity levels categorize how well the process accomplishes its goals.

Def: A *process capability* is the range of expected results that can be achieved by following the process. It is a predictor of future project outcomes.

Def: *Process performance* is a measure of the actual results achieved.

Def: *Process maturity* is the extent to which a process is explicitly defined, managed, measured, controlled, and effective.

The SSE-CMM contains 11 process areas. The definition of each of the process areas below contains a goal for the process area and a set of base processes that support the process area.

- Administer Security Controls
- Assess Impact
- Assess Security Risk
- Assess Threat
- Assess Vulnerability
- Build Assurance Argument
- Coordinate Security
- Monitor System Security Posture
- Provide Security Input
- Specify Security Needs
- Verify and Validate Security

The five Capability Maturity Levels that represent increasing process maturity are:

1. Performed Informally
   Base processes are performed.

2. Planned and Tracked
   Project-level definition, planning, and performance verification issues are addressed.

3. Well-Defined
   The focus is on defining and refining a standard practice and coordinating it across the organization.

4. Quantitatively Controlled
   This level focuses on establishing measurable quality goals and objectively managing their performance.

5. Continuously Improving
   At this level, organizational capability and process effectiveness are improved.

Usage

Application of the SSE-CMM is a straightforward analysis of existing processes to determine which base processes have been met and the maturity levels they have achieved. The same process can help an organization determine which security engineering processes they may need but do not currently have in practice.