Security Baseline

Go to Terms and Definitions

Discussion

A Security Baseline is a specialization of Baseline that establishes an approved reference for security controls, configuration values, constraints, and expected security characteristics.

The general concept of Baseline provides the controlled reference against which a subject can be compared, evaluated, changed, or restored.

A Security Baseline applies that concept to the security characteristics of a subject such as:

- An Infrastructure Environment
- A Machine Image
- An operating system
- A network
- A platform
- A software component
- A service
- A device
- An Artifact

A Security Baseline may identify:

- Required security controls
- Required configuration values
- Permitted services and protocols
- Prohibited services and protocols
- Identity and access settings
- Authentication requirements
- Authorization requirements
- Cryptographic requirements
- Logging and monitoring requirements
- Vulnerability-management settings
- Network-security settings
- Data-protection settings
- Applicable constraints
- Applicable Acceptance Criteria

A Security Baseline differs from a security policy:

- A security policy establishes governing security rules and objectives
- A Security Baseline establishes a controlled reference containing the security characteristics used to realize or evaluate those rules and objectives

A Security Baseline also differs from an observed security state:

- The Security Baseline identifies the approved reference state
- The observed security state identifies the security characteristics present in the evaluated subject

Comparing the observed security state with the Security Baseline may identify a Compliance Finding.

Definition

baseline that establishes an approved reference for the security controls, configuration values, constraints, and expected security characteristics of a subject

Source

Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

Note

A Security Baseline may derive from:

- Laws
- Regulations
- Standards
- Organizational policies
- Contractual obligations
- Threat assessments
- Risk assessments
- Platform-security guidance
- Operational requirements

A Security Baseline should have an identifiable revision so an evaluator can determine which reference applies to a particular assessment, deployment, or operational state.

Approval of a Security Baseline does not establish that every subject conforms to it. Conformance requires comparison of the subject with the applicable Security Baseline.

The term does not require a particular security framework, assessment method, configuration format, repository, tool, or implementation technology.

Example

A Security Baseline for a Red Hat Enterprise Linux Machine Image specifies permitted services, authentication settings, cryptographic settings, logging requirements, file permissions, network controls, and required security patches. An evaluator compares the resulting Machine Image with that

Security Baseline to determine whether the image satisfies the applicable security requirements.
