Security Domain

Go up to Terms and Definitions

Discussion

A Security Domain is an environment or context containing resources and entities governed by a common security policy, security model, or security architecture.

A Security Domain establishes a boundary within which defined rules govern:

- Information access
- Resource access
- Identity
- Authentication
- Authorization
- Information storage
- Information processing
- Information transmission
- Information marking
- Information release
- Audit and monitoring
- Administrative control

A Security Domain can include:

- Users
- Processes
- Services
- Devices
- Networks
- Applications
- Data stores
- Artifacts
- Infrastructure Resources
- Infrastructure Environments
- Deployment Targets

A Security Domain can be defined by:

- A Security Classification
- Information compartments
- Handling caveats
- Dissemination restrictions
- Organizational authority
- Mission purpose
- Legal or regulatory obligations
- Security architecture

- Access-control policy
- Information-release policy
- Connectivity restrictions

A Security Domain can exist within a:

- Classified Environment
- Unclassified Environment
- Connected Environment
- Disconnected Environment
- Air-Gapped Environment

Classification and connectivity do not independently define a Security Domain. A Security Domain also requires a common security policy or security architecture governing the resources and entities within its boundary.

A single Infrastructure Environment can contain more than one Security Domain when distinct resources or entities operate under different security policies.

Multiple Infrastructure Environments can also participate in one Security Domain when a common authority and security policy govern them.

Information movement within a Security Domain remains subject to the domain's Information Handling Rules.

Information movement from one Security Domain to another constitutes a Cross-Domain Transfer.

Definition

environment or context containing resources and entities governed by a common security policy, security model, or security architecture

Source

- NIST Computer Security Resource Center, Security Domain
- Committee on National Security Systems Instruction 4009, Committee on National Security Systems Glossary
- NIST Special Publication 800-53, Security and Privacy Controls for Information Systems and Organizations
- Dido Solutions, Crucible architecture and requirements terminology

Note

A Security Domain is not necessarily equivalent to:

- A network

- A subnet
- A Deployment Target
- An Infrastructure Environment
- A Security Classification
- An organizational unit

A physical or logical boundary can support enforcement of a Security Domain, but the common security policy defines the domain.

Two environments assigned the same Security Classification can remain separate Security Domains when different authorities, policies, compartments, missions, or release rules govern them.

A Security Domain can contain information at more than one classification or control level when the governing security policy and authorization permit that arrangement.

Example

A Classified Environment contains two Security Domains:

- A Secret mission domain available to all authorized mission personnel
- A Secret compartmented domain available only to personnel authorized for the compartment

Both domains operate at the Secret classification level, but different access and information-release policies make them separate Security Domains.
