Security Plane

Go to Terms and Definitions

Discussion

A Security Plane is an architectural plane that coordinates security controls and security-related information across system components, services, environments, and other architectural planes.

The Security Plane may coordinate capabilities such as:

- Identity management
- Authentication
- Authorization
- Access control
- Credential management
- Cryptographic key management
- Secrets management
- Security policy enforcement
- Security configuration
- Security monitoring
- Security event recording
- Vulnerability management
- Compliance evaluation
- Security Evidence collection
- Incident response

The Security Plane may interact with:

- Control-plane components
- Data-plane components
- Management-plane components
- Infrastructure Environments
- Infrastructure Configurations
- Machine Images
- CI/CD Pipelines
- Operational services
- External security services

The Security Plane differs from an individual security control:

- A security control performs or enforces a bounded security function
- The Security Plane coordinates security concerns and controls across architectural elements

The Security Plane also differs from a Security Baseline:

- A Security Baseline establishes an approved reference for required security characteristics
- The Security Plane coordinates the capabilities that apply, enforce, observe, or evaluate

security characteristics

A Security Plane may be logically distinct without being implemented as a separate physical subsystem.

Definition

architectural plane that coordinates security controls and security-related information across architectural elements and other planes

Source

Dido Solutions, Inc. and Jackrabbit Consulting, Inc.

Note

The Security Plane may provide centralized, distributed, federated, or hybrid security capabilities.

An architectural element may participate in more than one plane. For example, a deployment service may perform deployment operations within a management or control plane while using the Security Plane for authorization, credential retrieval, and security event recording.

The Security Plane does not imply that security responsibilities belong only to components assigned to that plane. Every architectural element remains responsible for satisfying its applicable security requirements.

The term does not prescribe a particular security architecture, product, protocol, deployment topology, trust model, or implementation technology.

Example

The Security Plane authenticates a CI/CD Pipeline, authorizes access to an identified Infrastructure Configuration, supplies the credentials required for Infrastructure Deployment, records security-relevant events, and provides Evidence for a subsequent Compliance Assessment.
