Security Technical Implementation Guide (STIG)

Go up to Terms and Definitions

Discussion

A Security Technical Implementation Guide (STIG) specifies security configuration requirements for an information technology product, system, service, platform, or technology.

The Defence Information Systems Agency (DISA) publishes STIGs for the United States Department of Defence information systems. A STIG translates applicable security controls and risk-management expectations into product-specific or technology-specific configuration requirements and assessment checks.

A STIG may identify required settings, prohibited configurations, vulnerability identifiers, severity categories, check procedures, remediation instructions, and references to associated security controls.

STIGs may be distributed in human-readable and machine-processable forms. Machine-processable content may support automated assessment through technologies such as the Security Content Automation Protocol (SCAP) and tools such as OpenSCAP.

Within Crucible, a STIG may form part of a Compliance Baseline or Compliance Posture. Crucible may apply STIG remediation during an Image Build, assess the resulting Hardened Image, and preserve the findings and evidence associated with the assessment.

Definition

security configuration guide that specifies implementation and assessment requirements for an information technology product, system, service, platform, or technology

Source

Generalised from the Security Technical Implementation Guides published by the United States Department of Defence and the Defence Information Systems Agency, and specialised for the Crucible architecture and operational model.

DISA identifies STIGs as security guidance for Department of Defence information technology systems and describes them as a bridge between NIST SP 800-53 and the Risk Management Framework.

Note

A STIG applies to a defined product, technology, version, or operating context. The applicable STIG and release should therefore be identified explicitly.

For example, a STIG for RHEL 9 applies to the Red Hat Enterprise Linux major version 9 family. The exact STIG release, selected profile, tailoring decisions, and applicable exceptions may affect the assessment result.

Applying a STIG does not by itself grant accreditation or an Operational Approval. The responsible authority evaluates the resulting configuration, findings, risks, and supporting Evidence within the applicable operating context.

Example

A Crucible Image Baseline identifies a DISA STIG for RHEL 9. During the Image Build, Crucible applies the selected remediation settings, runs a compliance assessment, records the findings, and associates the resulting evidence with the Hardened Image.
