Hardened Image

Go up to Terms and Definitions

Discussion

A Hardened Image is a Machine Image configured to reduce security exposure and satisfy defined security requirements or benchmarks.

The hardening process may remove or disable unnecessary services, restrict access, strengthen authentication, configure auditing, apply security policies, update packages, enforce secure defaults, and remediate identified findings.

A Hardened Image reflects a defined security configuration at the time of its build. Continued security depends on controlled updates, vulnerability management, configuration management, monitoring, and operation within an appropriate environment.

Within Crucible, hardening and compliance scanning occur as controlled image-build activities, and the resulting findings and evidence remain associated with the image and its Provenance.

Definition

machine image configured to reduce security exposure and satisfy defined security requirements or benchmarks

Source

Generalized from cybersecurity, operating-system hardening, secure configuration, compliance engineering, and machine-image usage and specialized for the Crucible architecture and operational model.

Note

A Hardened Image is not necessarily accredited, authorized, vulnerability-free, or suitable for every operating context.

The applicable hardening criteria depend on the operating system, threat model, compliance baseline, workload, and target environment.

Example

Crucible applies a DISA STIG profile to a Red Hat Enterprise Linux (RHEL) 9 Guest Image, remediates applicable findings, disables unnecessary services, configures auditing, and produces a Hardened Image with associated compliance evidence.
