1.2 Scope

Go to 1. Introduction

Crucible addresses the controlled construction, hardening, assessment, transfer, deployment, operation, maintenance, verification, and reproduction of software and Infrastructure Environments.

In Scope

The scope of Crucible includes:

- Definition, selection, reuse, and composition of version-controlled Baselines
- Use of Declarative Descriptions to identify intended environments, inputs, providers, compliance criteria, and lifecycle operations
- Construction, hardening, signing, verification, promotion, and replacement of Machine Images
- Construction and management of container images
- Definition and deployment of infrastructure through Infrastructure as Code (IaC)
- Separation of provider-independent intent from provider-specific implementation through Provider Abstraction
- Dependency Capture and preservation of Build Dependencies in a Dependency Store
- Preparation, export, import, and controlled transfer of Transfer Bundles
- Population of Offline Repositories within Disconnected Environments
- Deployment and validation of infrastructure resources, virtual machines, Kubernetes clusters, containerized workloads, and platform services
- Deployment rollback
- Automated Compliance Assessment using Compliance as Code (CaC)
- Generation and preservation of Compliance Findings, Provenance, Traceability, and Evidence
- Support for security-control implementation Evidence used in Security Control Traceability Matrix, Risk Management Framework, and Authority to Operate activities
- Reproduction of controlled environments from identified inputs and recorded lifecycle information
- Integration with Git-based Workflows, GitOps Workflows, and CI/CD Pipelines
- Access through a Command-Line Interface and a Web-Based User Interface
- Extension through provider, platform, image, compliance, and tooling integration points

Crucible applies across Cloud Environments, On-Premises Environments, Hybrid Environments, Connected Environments, Disconnected Environments, and Air-Gapped Environments.

Out of Scope

The scope of Crucible does not include:

- Definition or implementation of the mission-specific functionality that distinguishes a product or delivers its mission value
- Definition of the legal, regulatory, contractual, or organizational criteria governing a particular system or deployment

- Granting Accreditation, Operational Approval, or an Authority to Operate (ATO)
- Replacement of the responsible governance, assessment, compliance, or authorizing authorities
- Mandating a particular cloud provider, infrastructure platform, operating system, compliance scanner, package manager, build tool, or automation technology
- Elimination of product-specific configuration, Baselines, security criteria, provider integrations, or operational decisions
- Assumption of responsibility for product-specific risk acceptance, deployment approval, or operational authorization

The responsible authorities, standards bodies, policies, contracts, and governance organizations establish the criteria that apply to a particular system or deployment.

Crucible produces and preserves controlled artifacts, assessment results, Traceability, Provenance, and Evidence that support accreditation, approval, and authorization determinations, but Crucible does not make those determinations.

Different implementations can use different technologies while preserving the defined architectural contracts, lifecycle controls, Evidence obligations, and provider-independent behavior.
