CleanStart

STIG & OpenSCAP Compliance Architecture

Enabling audit – ready infrastructure for federal and regulated environments.

Executive Summary

Government compliance requirements such as DISA STIGs, NIST SP 800-53, and FedRAMP demand strict configuration controls across containerized infrastructure. Manual documentation and audit-based verification are no longer scalable in fast-moving environments where container images change daily or hourly.

This paper explains how **CleanStart** enables automated STIG enforcement and OpenSCAP-driven validation through infrastructure-native integration. By embedding hardened baselines and compliance verification at build and runtime, CleanStart removes manual effort and enables continuous compliance across enterprise and government environments.

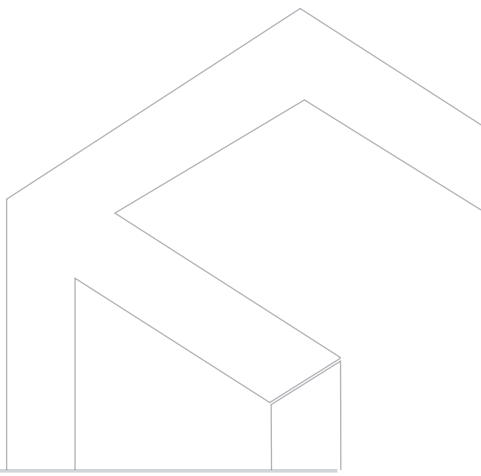
The Compliance Challenge

Container infrastructure introduces complexity when applying DISA STIG requirements across distributed environments. Manual STIG configuration, SCAP scanning, and spreadsheet-based documentation quickly become unreliable.

Organizations face several limitations:

- Configurations drift between environments
- Manual STIG documentation becomes outdated
- OpenSCAP scans are treated as one-time checks
- Evidence generation requires significant effort during audits
- Developers must research STIG requirements instead of building solutions

As container adoption increases, compliance must evolve from static documentation to real-time validation.



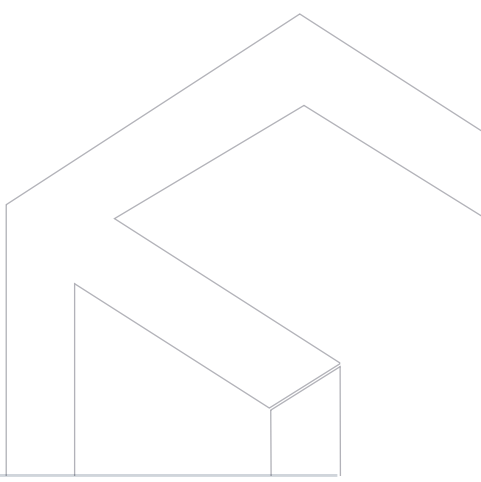
The CleanStart Solution

CleanStart transforms STIG compliance into an integrated capability built into the infrastructure layer. Rather than retrofitting compliance after deployment, CleanStart enables compliance by design through validated operating system baselines and automated SCAP workflows.

CleanStart integrates:

- **Pre-hardened STIG-compliant OS images**
- **Embedded SCAP validation at build time**
- **Config lockdown and policy enforcement**
- **Continuous drift detection and reporting**
- **Automated evidence generation for audit readiness**

This shifts compliance from manual effort to scalable enforcement across enterprise and government deployments.



Key Capabilities

STIG Baselines	Pre-hardened images aligned with DISA STIG requirements
OpenSCAP Automation	SCAP-based rule validation at build and runtime
Drift Detection	Configuration monitoring to prevent non-compliant states
Evidence Generation	Automated compliance attestation and reporting
CI/CD Integration	Native support for GitHub Actions and pipeline enforcement

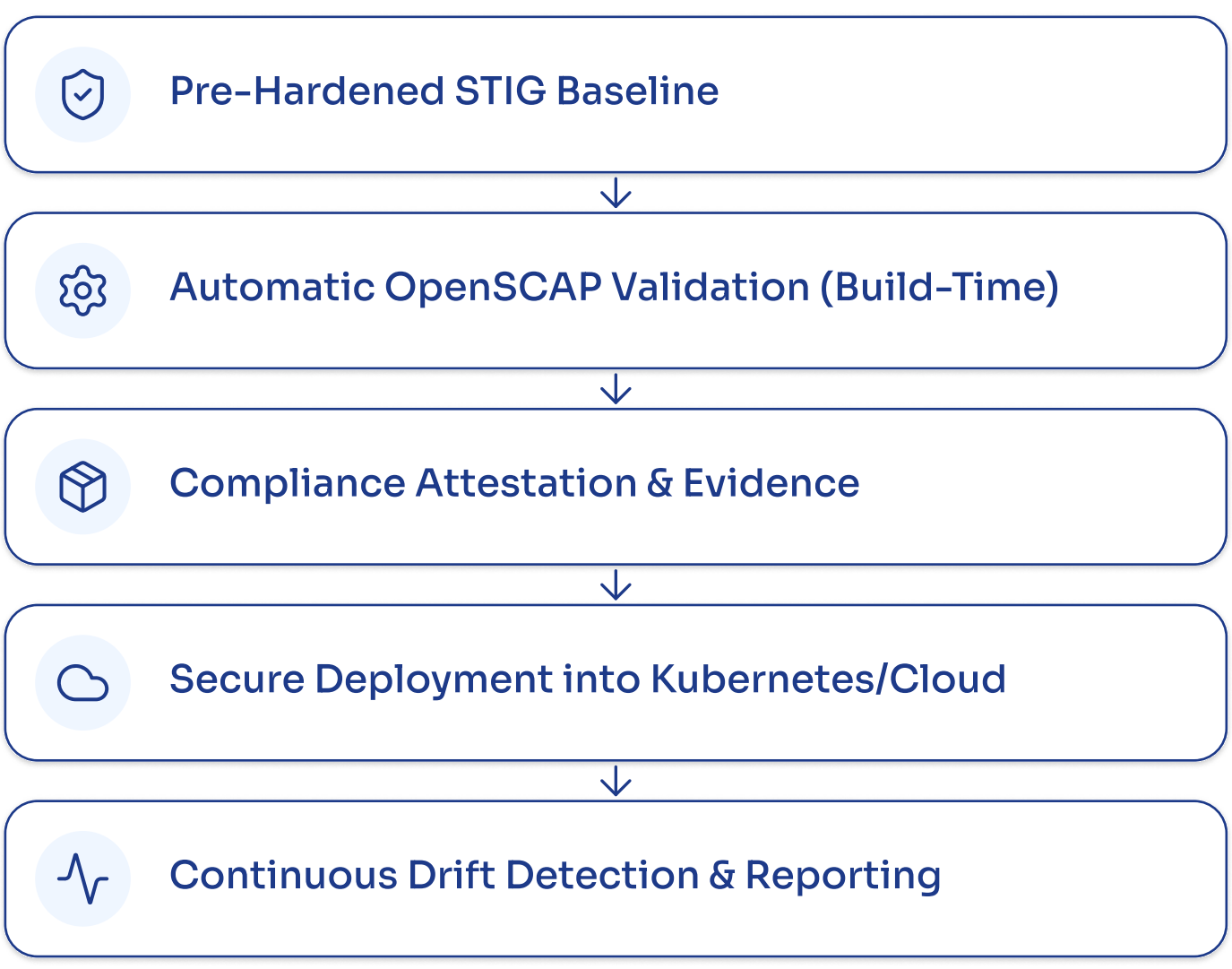
How CleanStart Works

CleanStart aligns security, compliance, and operations teams through infrastructure-native enforcement.

- Start from a pre-hardened STIG-based CleanStart image
- Apply security configurations during build
- Run OpenSCAP scanning automatically
- Generate compliance attestation and reports
- Deploy securely into Kubernetes or cloud-native environments

This approach ensures that compliance is consistent, repeatable, and production-ready from the start.

CleanStart STIG & OpenSCAP Compliance Workflow



CleanStart STIG Compliance Workflow - from pre - hardened baseline to continious OpenSCAP validation & real - time compliance assurance

Why CleanStart

Benefit	Outcome
Reduced audit effort	Compliance evidence generated automatically
Consistent enforcement	No configuration drift between environments
Lower operational cost	Eliminates manual scanning and remediation
Developer-friendly	No need to research STIG controls
Scales to government workloads	FedRAMP and DoD-ready baseline included

Integration and Availability

Integrates with:

Kubernetes, GitHub Actions, OpenShift, OpenSCAP, Terraform

Supported Standards:

DISA STIG, NIST SP 800-53, FedRAMP ConMon, SCAP 1.3

References

Simplify Implementation and Maintenance with Actionable Tips.

Documents OpenSCAP NIST certification for SCAP 1.2 support.

OpenSCAP Overview: Security Scanning for Docker Images and Containers.

Highlights the need for continuous security compliance in rapidly changing environments

Detailed SSG collaboration with DISA FSO

Automated compliance checks as a top three priority for 52 percent of respondents.

SCAP Security and Compliance Scanning of Docker Images in GitHub Actions and GitLab CI.