

Security and Compliance Automation in Any Environment, on Any Platform

Chef InSpec leverages an open-source framework for defining security and compliance rules as executable code designed to be used at all stages of the software delivery process, from a developer's workstation all the way through to production.

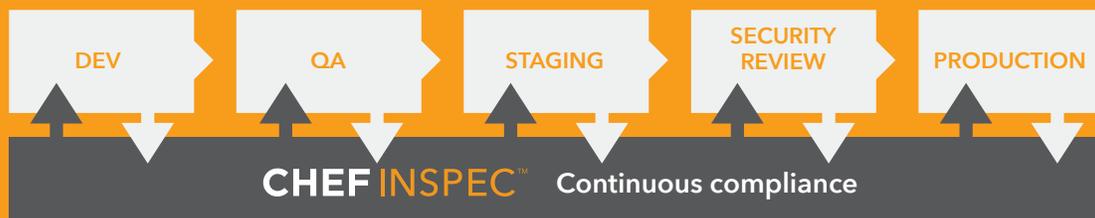
As more and more diverse technologies are deployed across data centers, hybrid or cloud estates, validating compliance organization-wide has become increasingly difficult. When defined with Chef InSpec, compliance, security, and other policy requirements become automated tests that can be run against traditional servers, containers, and cloud APIs, ensuring standards are enforced consistently in every managed environment.

Shift Security and Compliance Left

Before Chef InSpec



After Chef InSpec



Stop treating information security as an afterthought! Relying only on pre-production security scans slows down development process and creates rework. Chef InSpec allows organizations to build Security directly into every stage of development by turning compliance, security and other policy requirements into code.

Chef InSpec's breadth of coverage and ease of use allow it to be shared between software development, operations and security teams, enabling better collaboration throughout the software development lifecycle

It is only with a continuous compliance approach that organizations are able to ensure their applications, and underlying infrastructure, are compliant from the first day it's developed - not simply in the instant it is released to the world.

CIS	Coverage Level
-----	----------------

Operating Systems	
-------------------	--

Amazon Linux 2	Level 1 + 2 Server
CentOS 7	Level 1 + 2 Server
CentOS 6	Level 1 + 2 Server
RHEL 7	Level 1 + 2 Server
RHEL 6	Level 1 + 2 Server
Ubuntu 18.04	Level 1 + 2 Server
Windows Server 2016	Level 1 + 2 MS + DC
Windows Server 2012R2	Level 1 + 2 MS + DC
Windows Server 2012	Level 1 + 2 MS + DC

Cloud Platforms	
-----------------	--

Google Cloud	Level 1 + 2
AWS Fundamentals	Level 1 + 2
Azure Foundations	Level 1 + 2

DISA STIG	Coverage Level
-----------	----------------

Operating Systems	
-------------------	--

RHEL 7	Cat 1/2/3
RHEL 6	Cat 1/2/3
Windows 2019	Cat 1/2/3
Windows 2016	Cat 1/2/3
Windows Memberserver 2012/2012R2	Cat 1/2/3

Transform Compliance and Security into Simple Code

Chef Automate supplies built-in Chef InSpec profiles for standards like the Center for Internet Security (CIS) benchmarks, Defense Information System Agency (DISA) Security Technical Implementation Guides (STIG's) and more, to allow quick start and applying continuous compliance to your infrastructure.

Build on predefined profiles, or write your own, to codify your organization's requirements with Chef InSpec's extensible language.

Use Chef InSpec for:

- **Security Automation:** Secure, audited infrastructure across entire software delivery lifecycle. Define policies as code, detect issues before production, and discover non-compliance for fast remediation.
- **Compliance Auditing:** Make audits painless by augmenting built-in InSpec profiles with organization-specific exceptions & requirements and continuously scanning your entire fleet.
- **Government Compliance Automation:** Predefined DISA STIG and CIS Benchmarks profiles help Accelerate the Authority-To-Operate (ATO) in highly regulated federal organizations

For more information visit: chef.io/inspec

“Chef InSpec has helped us unify our compliance, security and DevOps teams and streamlined audits, reducing the thousands of staff hours usually required by as much as 95 percent.”

- Jon Williams, CTO, Niu Solutions

