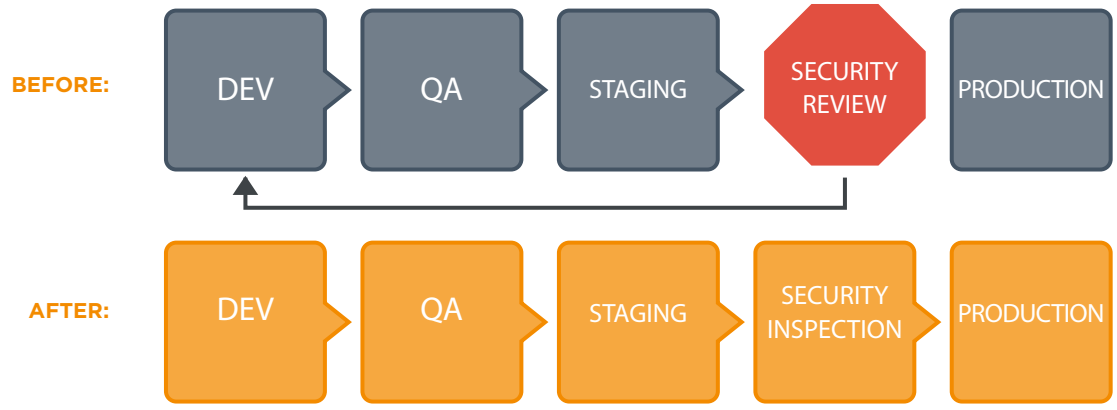
Chef in Government

Accelerate the ATO process using continuous compliance

IT practitioners and managers in the US government are challenged with delivering high-quality applications quickly while maintaining compliance with a plethora of federal standards and certifications such as FIPS 140-2, FISMA, FedRAMP, and more. Yet traditional approaches for ensuring standards compliance often involve slow, manual, post-build security scanning as part of an ATO (Authority to Operate) process. These processes catch compliance-related defects far too late, creating rework for engineers and resulting in budget overruns, schedule slippage, and unhappy users.



The Chef platform helps you solve these problems and achieve ATO faster, by incorporating compliance processes into every stage of the development cycle:

- The open-source InSpec language allows developers and systems engineers to replace lengthy & opaque security specification documents – written in PDF or Excel – with unambiguous tests that are easily readable by all parties involved: security engineers, auditors, systems administrators, and others.
- Chef provides a standard set of security baselines that you can easily customize and extend for your own use. Examples of baselines included are CIS Compliance Benchmarks and several DISA STIGs. Chef can also convert existing, hard-to-use formats like SCAP XCCDF and Microsoft SCCM XML to human-readable InSpec in order to take advantage of NIST baselines published in those formats.
- The open-source Chef configuration management language can be used to remediate any findings and keep systems in their correct, remediated state, thereby ensuring continuous compliance.

CHEF

619 Western Avenue Suite 400 | Seattle, WA 98104 | PH: 206.508.4799 | sales@chef.io | www.chef.io

Chef Automate's collaboration capabilities allow all parties involved in both an ATO process and production operations the ability to see, in real-time, the compliance status of any infrastructure. No longer do teams need to rely on expensive, infrequently-used tools accessible only to security engineers. With Chef, government IT can move from being reactive about compliance issues to always being compliant – and being able to prove it not just at ATO but any time.

EXAMPLE CONTROL DESCRIPTION FROM RHEL6 STIG:

ID: V-38551
ID Title: SRG-OS-000145
Severity: Medium
Title: The operating system must connect to external networks or information systems only through managed IPv6 interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.

CONTRAST WITH INSPEC RULE:

```
control 'RHEL-06-000106' do
  impact 0.5
  title 'The operating system must connect to external networks or information
systems only through managed IPv6 interfaces consisting of boundary protection
devices arranged in accordance with an organizational security architecture.'
  desc 'The "ip6tables" service provides the system\'s host-based firewalling
capability for IPv6 and ICMPv6.'
  tag group: 'SRG-OS-000145'
  tag vulid: 'V-38551'
  ref 'http://iasecontent.disa.mil/stigs/zip/U_RedHat_6_V1R15_STIG.zip'
  only_if { kernel_module('ipv6').loaded? }
  describe service('ip6tables') do
    it { should be_enabled }
    it { should be_running }
  end
end
```

"[Scanners are] slow and you can't run them all the time in production. They don't keep up very well... whereas with Chef Compliance, I can write a remediation for things that day & put them online. That's the kind of benefit you get when you go with Chef Compliance."

- John Ray, Senior Consultant, Shadow-Soft (GSA Schedule 70 partner)

Learn More at www.chef.io/federal

CHEF
619 Western Avenue Suite 400 | Seattle, WA 98104 | PH: 206.508.4799 | sales@chef.io | www.chef.io