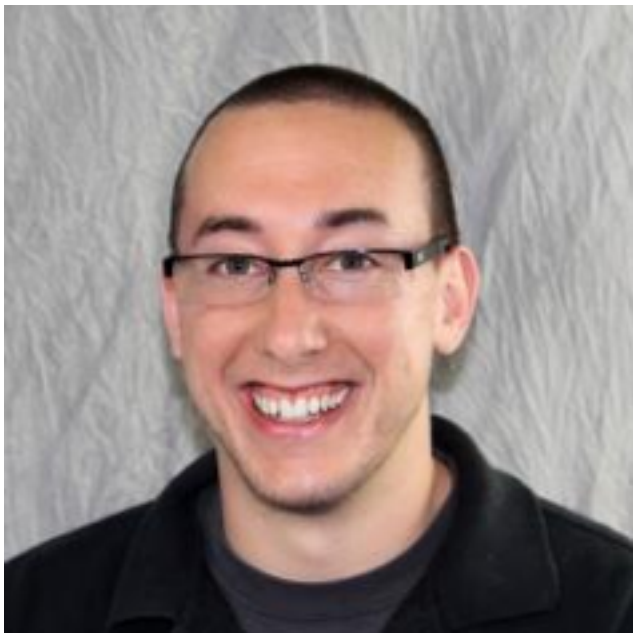


Peeling Back the Onion: Drupal Security and Compliance



CivicActions

Who are we...



CivicActions is ...

Open

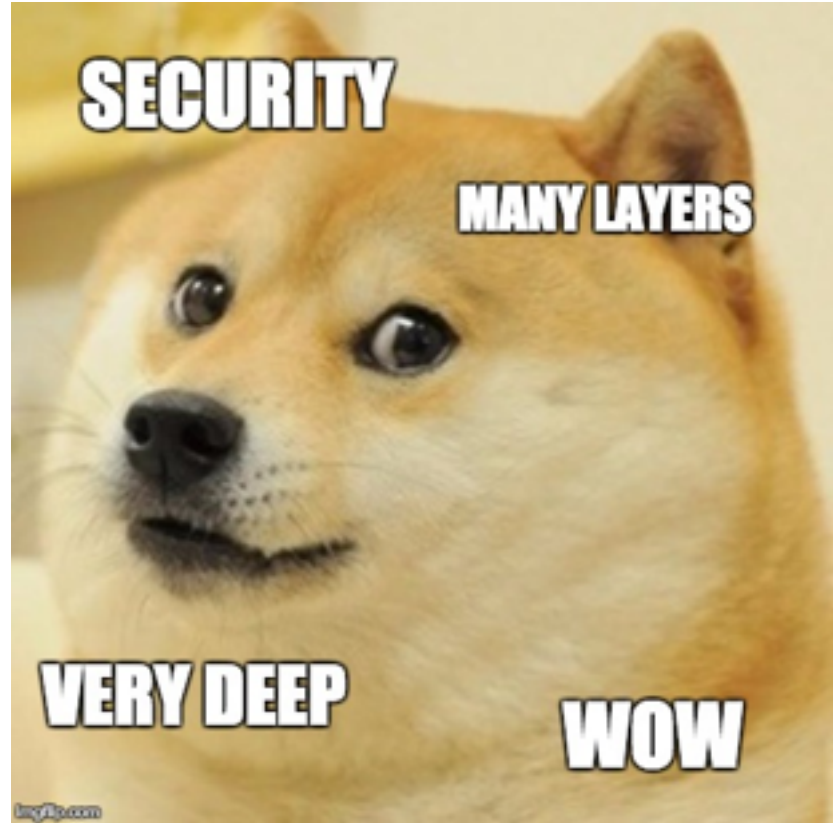
Agile

Transparent

What is security?

WHAT ARE THE GOALS OF SECURITY?

Problem of Security



WHAT ARE THE GOALS OF SECURITY?

**Security Objective:
Practical, preventative
measures for mitigating risk**

COMPLIANCE DOES NOT MEAN SECURITY

Goals of Security



Information Assurance

Image courtesy of the book:

Information Security Principles of Success
Breithaupt and Merkow, 2014

WHAT ARE THE GOALS OF SECURITY?

**The practice changes for
each system and need**

WHAT ARE THE GOALS OF SECURITY?

Let's evaluate some guiding principles to achieve the outlined goals

COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

- 1. Least Privilege / Access Control**
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation

COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
- 2. Complete Mediation**
3. Attack Vectors
4. Logging, Auditing, Monitoring
5. Nonrepudiation

COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
- 3. Attack Vectors**
4. Logging, Auditing, Monitoring
5. Nonrepudiation

COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
- 4. Logging, Auditing, Monitoring**
5. Nonrepudiation

COMPLIANCE DOES NOT MEAN SECURITY

Security Principles

1. Least Privilege / Access Control
2. Complete Mediation
3. Attack Vectors
4. Logging, Auditing, Monitoring
- 5. Nonrepudiation**

WHAT ARE THE GOALS OF SECURITY?

**Be proactive and test your
security practices**

Why Compliance?

**Compliance is not just a good idea,
*it's the law***



**Compliance is not just a good idea,
*it's the law***

When you're told that the new system has to be compliant





See also: CDM from DHS and GSA.

Control Types

- **Administrative**
 - Guidelines, procedures (Security Policy)
- **Technical**
 - Intrusion detection systems, ACLs (Least Privilege)
- **Physical**
 - Physical (USB, media) access (Separation of Duties)

Practical Benefits of Compliance

- Scanning regularly (CVEs, STIGs, ...)
- Keeping LAMP stack up-to-date
- Keeping Drupal up-to-date
- Reviewing logs
- Managing Access Control
- Incident Response Training
- Bastion SSH host and CDN

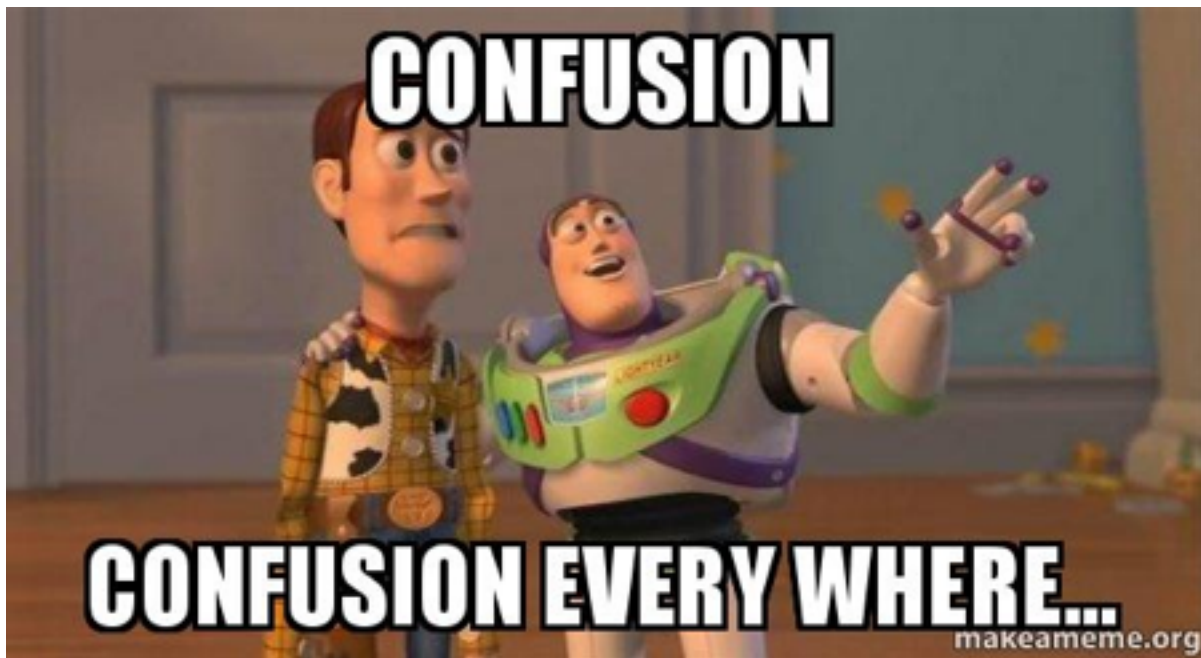
Compliance does not mean Security

COMPLIANCE DOES NOT MEAN SECURITY

How are they related?

**Compliance controls provide guidance,
but they do not prescribe security
practices.**

COMPLIANCE DOES NOT MEAN SECURITY



The Onion

COMPLIANCE DOES NOT MEAN SECURITY

- 1. Network - Ports, VPC, Monitor**
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem

COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
- 2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer**
3. Application - Drupal, Solr, HTTPD, JavaScript
4. Data - MySQL, Shared Filesystem

COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
- 3. Application - Drupal, Solr, HTTPD, JavaScript**
4. Data - MySQL, Shared Filesystem

COMPLIANCE DOES NOT MEAN SECURITY

1. Network - Ports, VPC, Monitor
2. Infrastructure - Instance OS, CDN, SSH proxy, Load Balancer
3. Application - Drupal, Solr, HTTPD, JavaScript
- 4. Data - MySQL, Shared Filesystem**

COMPLIANCE DOES NOT MEAN SECURITY

**Look at each tier of the
system to map controls to
security practices**

COMPLIANCE DOES NOT MEAN SECURITY

Making the onion tasty



COMPLIANCE DOES NOT MEAN SECURITY

**What are the most common
compliance controls you need
to be aware of?**

Typical Controls

- AC: Access Control
- IA: Identification and Authentication
- AU: Audit & Accountability
- CM: Configuration Management
- RA: Risk Assessment

The 18 RMF (Risk Management Framework) “Control Families”

Defined in NIST
SP 800-37 Rev 4

Control Families

Families
<u>AC - Access Control</u>
<u>AU - Audit and Accountability</u>
<u>AT - Awareness and Training</u>
<u>CM - Configuration Management</u>
<u>CP - Contingency Planning</u>
<u>IA - Identification and Authentication</u>
<u>IR - Incident Response</u>
<u>MA - Maintenance</u>
<u>MP - Media Protection</u>
<u>PS - Personnel Security</u>
<u>PE - Physical and Environmental Protection</u>
<u>PL - Planning</u>
<u>PM - Program Management</u>
<u>RA - Risk Assessment</u>
<u>CA - Security Assessment and Authorization</u>
<u>SC - System and Communications Protection</u>
<u>SI - System and Information Integrity</u>
<u>SA - System and Services Acquisition</u>

COMPLIANCE DOES NOT MEAN SECURITY

What is an example?

AC: Access Control

- AC-2 Account Management
- AC-2(5) Inactivity Logout
- AC-5 Separation of Duties
- AC-6 Least Privilege
- IA-5 Authenticator Management

AC: Drupal Solutions

- Roles and Perms
- Autologout
- Password Policy
- TFA / SimpleSAMLPHP
- * Permissions (Field Permissions, Taxonomy Access Control, etc)

Handout

We have a handout that outlines
additional security and compliance
recommendations

Current Challenges

CURRENT CHALLENGES

- 1. Poorly defined best practices**
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. Tools are not accessible
5. No magic bullet (security is relative to your system)

CURRENT CHALLENGES

1. Poorly defined best practices
- 2. Education of developers and reviewers**
3. Tools are not robust or comprehensive
4. Tools are not accessible
5. No magic bullet (security is relative to your system)

CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
- 3. Tools are not robust or comprehensive**
4. Tools are not accessible
5. No magic bullet (security is relative to your system)

CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
- 4. Tools are not accessible**
5. No magic bullet (security is relative to your system)

CURRENT CHALLENGES

1. Poorly defined best practices
2. Education of developers and reviewers
3. Tools are not robust or comprehensive
4. Tools are not accessible
- 5. No magic bullet (security is relative to your system)**

Fun Stuff

COMPLIANCE DOES NOT MEAN SECURITY

Where do we see security and compliance going?

COMPLIANCE DOES NOT MEAN SECURITY

Innovation at every tier of the onion



COMPLIANCE DOES NOT MEAN SECURITY

**The three year ATO cycle is
transforming into
continuous assurance**

COMPLIANCE DOES NOT MEAN SECURITY

Compliance is pushing more into DevOps

COMPLIANCE DOES NOT MEAN SECURITY

**Build small, discrete
components and automate**

COMPLIANCE DOES NOT MEAN SECURITY

Intrusion Detection

Isolate Threats

Minimize Damage

COMPLIANCE DOES NOT MEAN SECURITY

Artificial Intelligence: The Next Frontier

System predicts 85 percent of cyber-attacks using input from human experts

Virtual artificial intelligence analyst developed by the Computer Science and Artificial Intelligence Lab and PatternEx reduces false positives by factor of

5. <http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418>

Examples

OpenSCAP is free and open source, automated security scanning for operating systems* and selected applications.

*only Red Hat 6 & 7 for now, but can be extended

Compliance and Scoring

The target system did not satisfy the conditions of 43 rules! Please review rule results and consider applying remediation.

Rule results



Severity of failed rules



Score

Scoring system	Score	Maximum	Percent
um:xccdf:scoring:default	74.907738	100.000000	74.91%

Rule Overview

- ☒ pass
- ☒ fixed
- ☒ informational
- ☒ fail
- ☒ error
- ☒ unknown
- ☒ notchecked
- ☐ notselected
- ☒ notapplicable

Group rules by:

Default

Title	Severity	Result
▼ Guide to the Secure Configuration of Red Hat Enterprise Linux 7 43x fail 9x notchecked		
> Introduction		
▼ System Settings 43x fail 9x notchecked		
▼ Installing and Maintaining Software 1x fail 0x notchecked		
▼ Disk Partitioning 1x fail 1x notchecked		
Ensure /tmp Located On Separate Partition	low	fail
Ensure /var Located On Separate Partition	low	pass
Ensure /var/log/audit Located On Separate Partition	low	pass
Ensure /home Located On Separate Partition	low	pass
Encrypt Partitions	medium	notchecked
▼ Updating Software 0x notchecked		
Ensure Red Hat GPG Key Installed	high	pass
Ensure gpgcheck Enabled In Main Yum Configuration	high	pass
Ensure gpgcheck Enabled For All Yum Package Repositories	high	pass

COMPLIANCE DOES NOT MEAN SECURITY

A YAML-Powered Antidote To Bureaucracy

It's a powerfully simple idea.

It's a schema.

It's a set of tools and best practices.

It's a community.



A YAML-Powered Antidote To Bureaucracy

It's a powerfully simple idea.

To improve the quality of our software development, we use continuous integration. To improve the reliability of our deployment, we use continuous delivery. To improve the security of our systems, we can use continuous authorization.

Simply put, the tools that we use to develop and operate software, should also be used to generate and validate assessment and authorization packages.

Every commit runs the tests. Every passing build, updates the system security plan. Every deployment includes updates to continuous monitoring.

Software as Code.

Tests as Code.

Infrastructure as Code.

Compliance as Code.

It's a schema.

By adopting a standard approach to documenting "controls" (whether Technical, Operational, or Management) we can rapidly build a community of vendors and operators. You can see [the current \(and evolving\) OpenControl schema here](#).

COMPLIANCE DOES NOT MEAN SECURITY

Component Schema

Here is an example component schema:

```
# CloudFoundry-UAA.yaml
---
name: User Account and Authentication (UAA) Server
references:
- name: User Account and Authentication (UAA) Server
  url: http://docs.pivotal.io/pivotalcf/concepts/architecture/uaa.html
governors:
- name: Cloud Foundry Roles
  url: https://cf-pl-docs-prod.cfapps.io/pivotalcf/concepts/roles.html
satisfies:
  NIST-800-53:
    AC-2: Cloud Foundry accounts are managed through the User Account and Authentication (UAA) Server.
```

You can find the [complete file on github](#).

The GovReady Dashboard puts compliance info in a Drupal report.

*Alpha - Not yet ready for production, but interesting work.

2
Module updates
Drupal Core security update!
8 total modules >

June 9th 2017
Next domain renewal
No SSL active
Domains + SSL >

2
super admins
4 total accounts >

System

OS	Linux 3.8.0-29-generic
PHP	PHP 5.5.36-1+donate.sury.org-trusty+1
APPLICATION	Drupal: 7.43
WEBSERVER	
DATABASE	MySQL:mysqlnd 5.0.11-dev - 20120503 - \$id: 15d5c781cfad91193dceae1d2cd1127674d8b3e \$

Recommended security modules

- ☐ Site Audit
- ☐ Security Review

Known vulnerabilities

- Drupal
- commerce
- webform

Manual Tasks

Track your manual tasks here. [See all.](#)

Upcoming / Past-due

Verify site monitoring

Due in 25 days

Verify offsite database backups

Due in 31 days

Server security updates

Due in 21 days

Recent Task Reports

Incident response practice	July 19th 2016
Verify offsite database backups	July 19th 2016
Verify site monitoring	July 19th 2016

Inactive Accounts

Are these users still in your organization? [Edit them](#), if not, [delete them](#).

USER	ROLES	LAST LOGIN
sketchy joe	authenticated user	November 8th 2015, 12:25:05 pm
fred coworker	authenticated user, administrator	April 8th 2016, 1:25:05 pm

Points of Contact to Maintain your Site

Keep this handy list [updated](#) with important contacts to maintain your site

WHAT TO CALL THEM FOR	EMAIL	PHONE	LAST CONFIRMED
Account access	greg@govready.com	123-345-2342	July 19th 2016
Content publishing	jane@example.com	657-645-5489	July 19th 2016
Site emergencies	dont-bother-	321-541-	July 19th

Call To Action

COMPLIANCE DOES NOT MEAN SECURITY

**We need to define best
practices and build the tools
to support it**

COMPLIANCE DOES NOT MEAN SECURITY

Open Concept's Guide: Drupal Security Best Practices

COMPLIANCE DOES NOT MEAN SECURITY

Details

README

ansible-role-govready

Role to install [GovReady](#).

GovReady is a super easy to use commandline toolkit for running security scans on open source servers and software. Technically, GovReady is a bash wrapper around [OpenSCAP](#), a NIST certified SCAP toolkit.

GovReady depends upon: - [OpenSCAP role](#) must be installed on all instances - [SCAP Security Guide role](#) must be installed on the GovReady "dashboard" instance.

COMPLIANCE DOES NOT MEAN SECURITY

Drupal 8 Security Review

New Plugin System

Code Sprint

Thank you.