Peeling Back the Onion: Drupal Security and Compliance

CivicActions

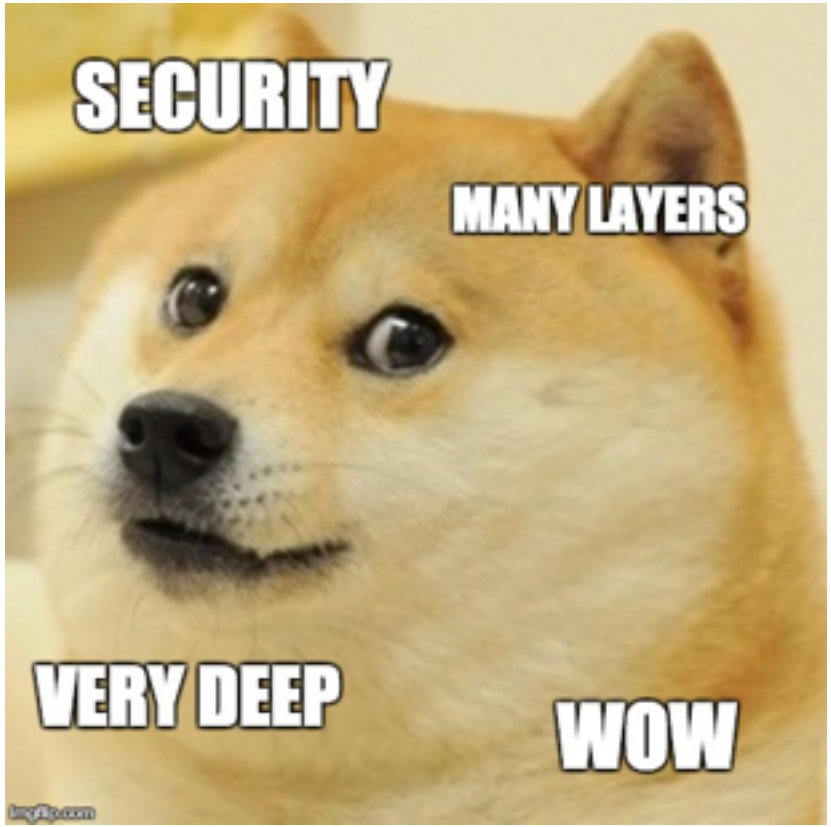
Who are we...

CivicActions is …

Open
Agile
Transparent

What is security?

Problem of Security



Security Objective: Practical, preventative measures for mitigating risk

Goals of Security

Information Assurance

Image courtesy of the book:

Information Security Principles of Success
Breithaupt and Merkow, 2014

The practice changes for each system and need

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

Security Principles

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

Security Principles

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

Security Principles

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

Security Principles

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

Security Principles

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

Be proactive and test your security practices

Why Compliance?

CivicActions

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

The Risk Management Framework

Continuous Monitoring is to be implemented by 2017 per OMB M-14-03.

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

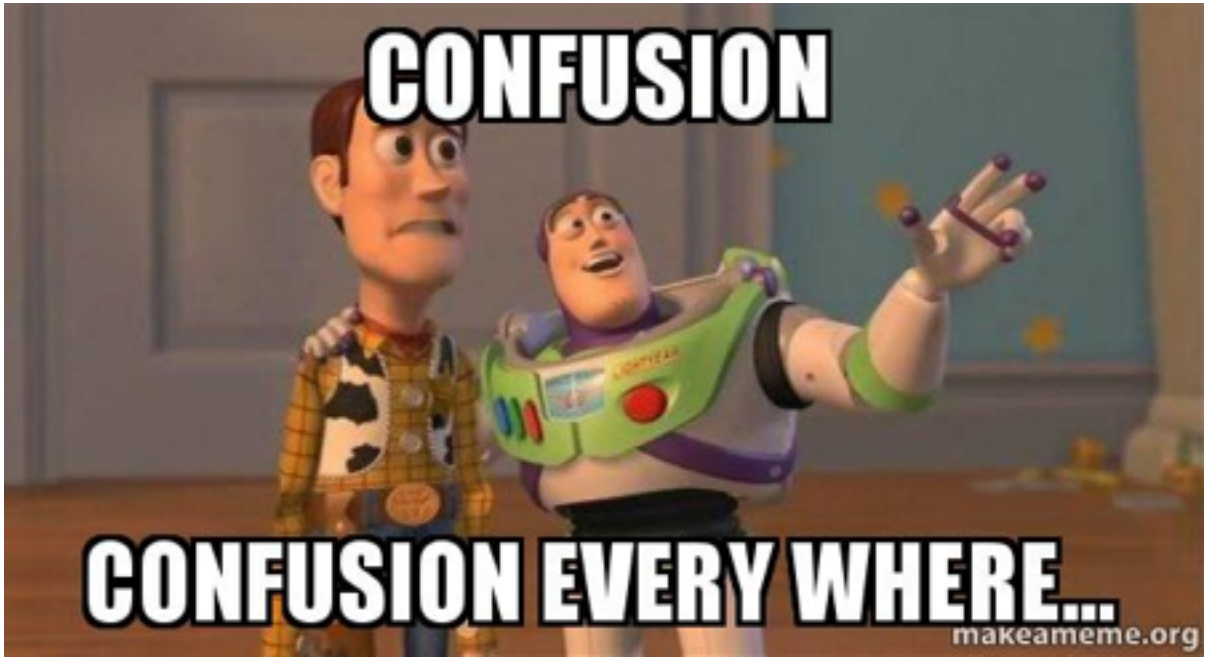
Compliance does not mean Security

CivicActions

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**

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

Making the onion tasty

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

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

Where do we see security and compliance going?

Innovation at every tier of the onion

The three year ATO cycle is transforming into continuous assurance

Compliance is pushing more into DevOps

Build small, discrete components and automate

Intrusion Detection
Isolate Threats
Minimize Damage

Artificial Intelligence: The Next Frontier

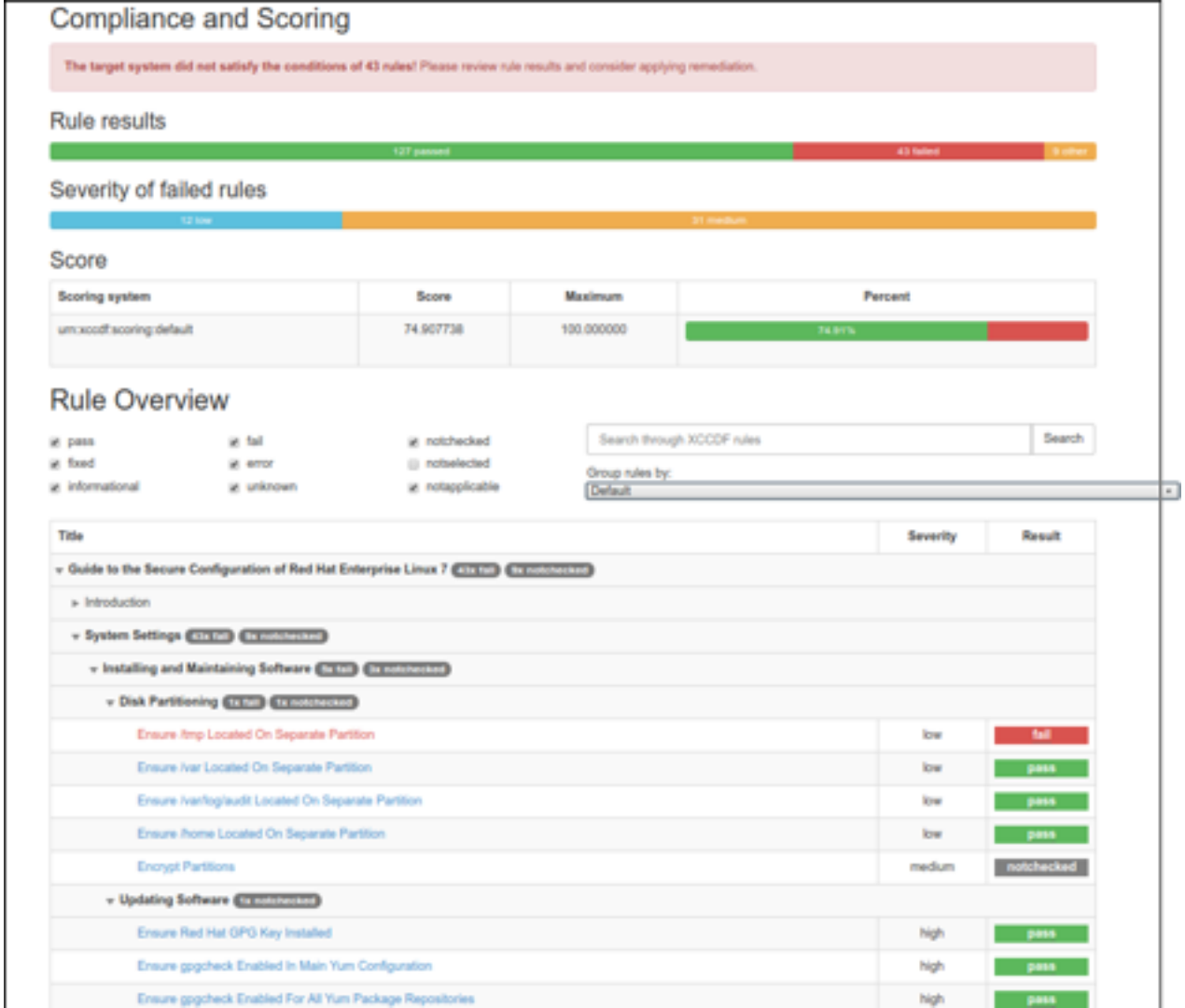
System predicts 85 percent of cyber-attacks using input from human experts

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 DOES NOT MEAN SECURITY

COMPLIANCE DOES NOT MEAN SECURITY

Component Schema

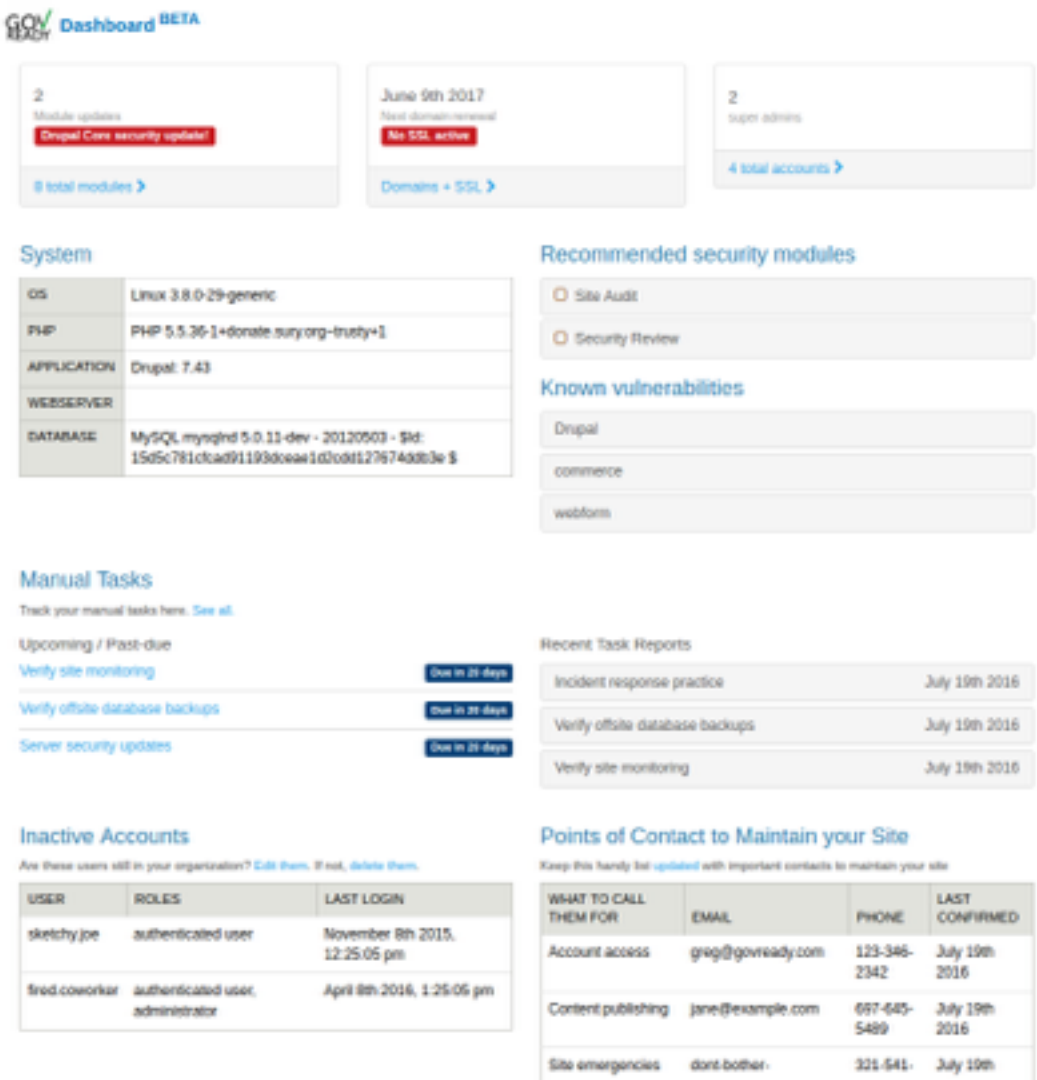
Here is an example component schema:

```
# 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-p1-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.



Call To Action

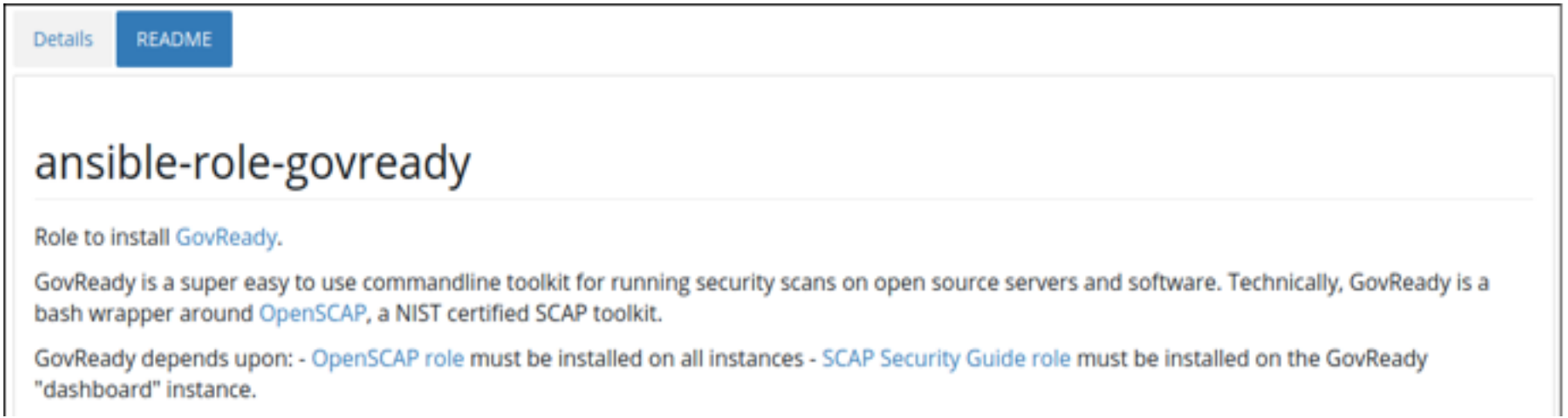
COMPLIANCE DOES NOT MEAN SECURITY

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



COMPLIANCE DOES NOT MEAN SECURITY

Drupal 8 Security Review New Plugin System Code Sprint

CivicActions

Thank you.

CivicActions