



# Ansible Security Automation

Faz Sadeghi  
Specialist Solution Architect  
Red Hat Ansible Automation  
[faz@redhat.com](mailto:faz@redhat.com)



# WHY SECURITY AUTOMATION

ANSIBLE








**Ansible use cases**  
**Information security pillars**  
**Why Ansible?**  
**Examples**  
**Get involved**





**Application Security**  
**Network Security**  
**Forensics**  
**Incident Response**  
**Penetration Testing**  
**Fraud Detection and Prevention**  
**Governance, Risk, Compliance**

## Automate the deployment and management of your entire IT footprint.

Do this...

Orchestration

Configuration  
Management

Application  
Deployment

Provisioning

Continuous  
Delivery

On these...

Firewalls

Load Balancers

Applications

Containers

Clouds

Servers

Infrastructure

Storage

Network Devices

And more...

## Automate the deployment and management of your entire IT footprint.

Do this...

Orchestration

Configuration  
Management

Application  
Deployment

Provisioning

Continuous  
Delivery

Security Automation

On these...

Firewalls

Load Balancers

Applications

Containers

Clouds

Servers

Infrastructure

Storage

Network Devices

And more...



# WHY IS INFO SEC COMPLICATED

ANSIBLE





# FLEXIBILITY IS CRUCIAL

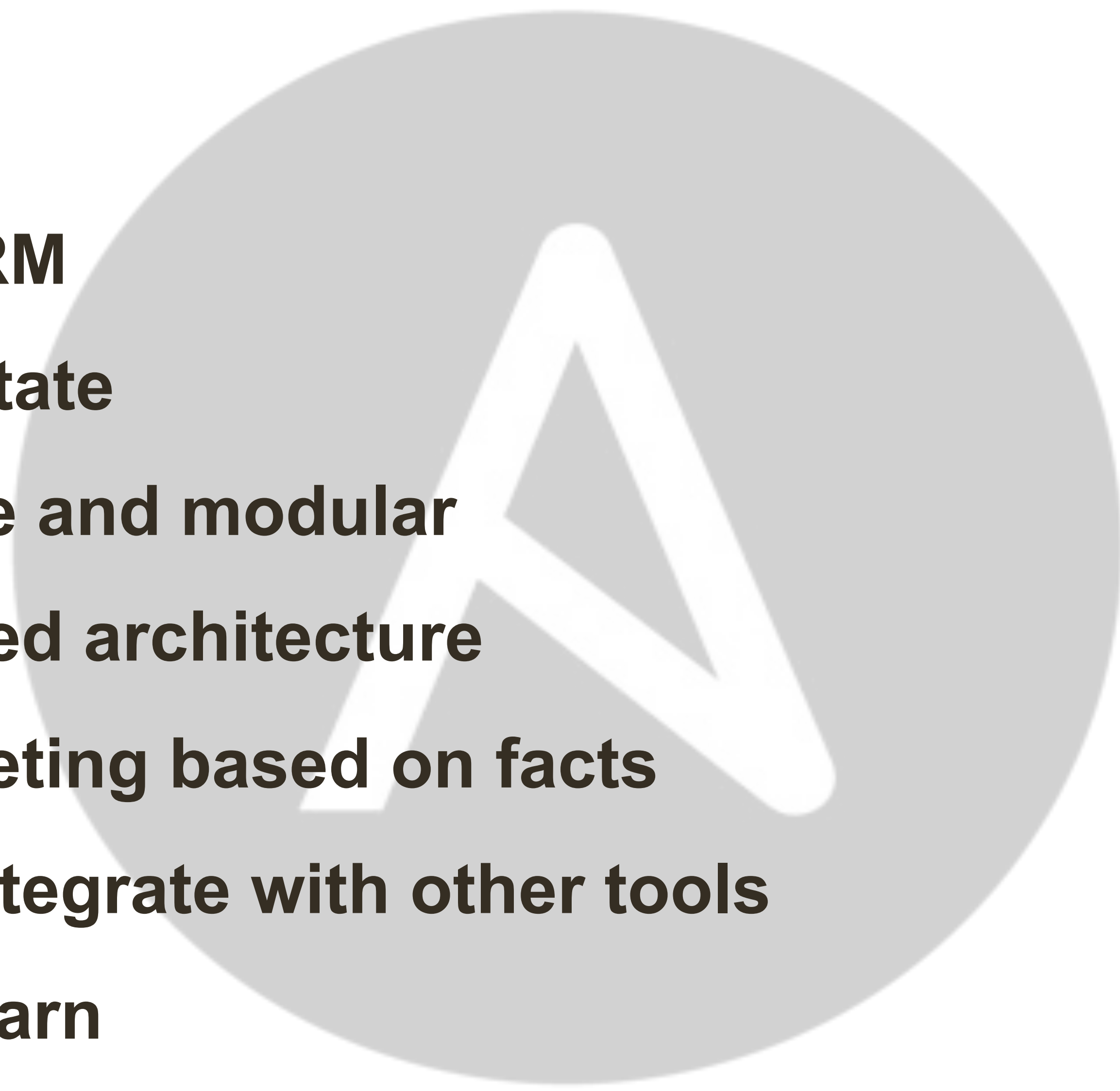
ANSIBLE









- 
- **Agentless**
  - **SSH/WinRM**
  - **Desired State**
  - **Extensible and modular**
  - **Push-based architecture**
  - **Easy targeting based on facts**
  - **Easy to integrate with other tools**
  - **Easy to learn**



# WHAT IS ANSIBLE TOWER?

Ansible Tower is an **enterprise framework** for controlling, securing and managing your Ansible automation – with a **UI and RESTful API**.

- **Role-based access control**
- **Deploy** entire applications with **push-button deployment** access
- All automations are **centrally logged**





## WALLS OF SEPARATION

**SECurity**



Wants to ensure Information Assurance

**OPerationS**



Wants to ensure System Availability

**DEVelopers**

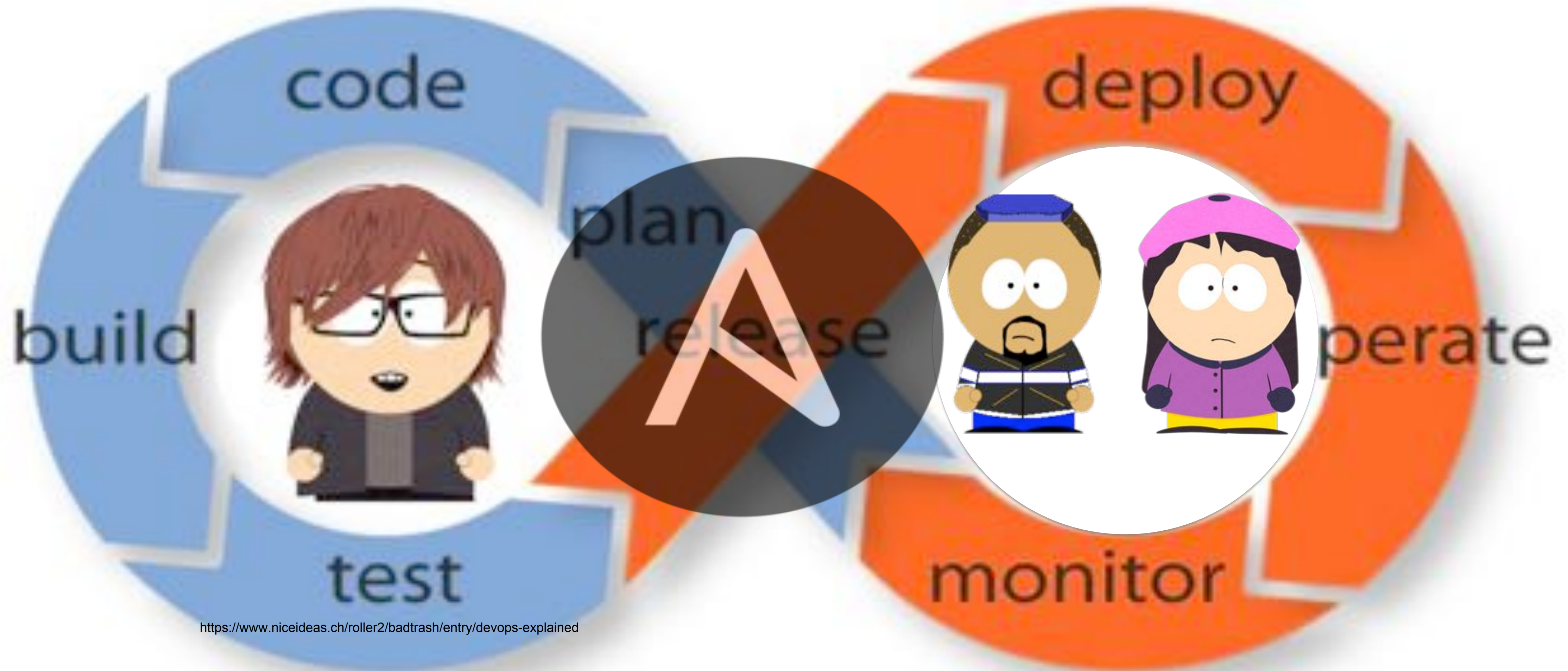


Wants to deliver Applications Fast

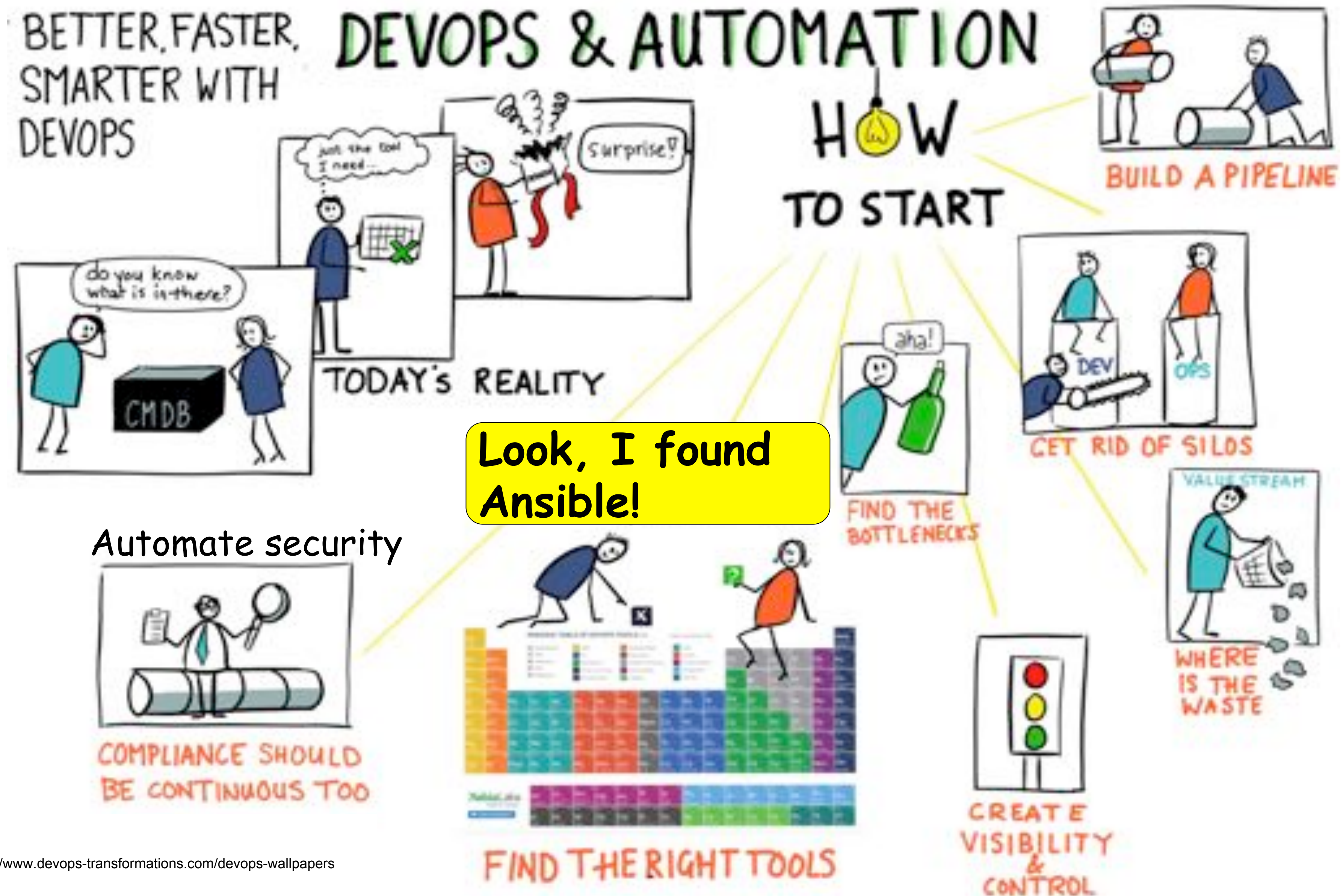


# ALL IN ALL, LET'S BREAK THE WALL

ANSIBLE









## Security Playbook Examples



Rule Title: The SSH daemon must not allow authentication using an empty password  
Linux servers .

Rule Title: Anonymous enumeration of shares must be restricted on Windows servers.

Rule Title: The network element must only allow management connections for administrative access from hosts residing in to the management network.

Rule Title: Change root password on all servers, according to policy every 60 days.

Rule Title: Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches.

Install critical security patches within one month of release.

Rule Title: Protect against CVE-2016-5696.

Rule Title: Fix and test shellshock.

.....

.....

Rule Title: The SSH daemon must not allow authentication using an empty password.

Fix Text: To explicitly disallow remote logon from accounts with empty passwords, add or correct the following line in "/etc/ssh/sshd\_config":

line

/etc/ssh/sshd\_config

PermitEmptyPasswords no

PermitEmptyPasswords no

- name: "HIGH | RHEL-07-010270 | PATCH | The SSH daemon must not allow authentication using an empty password."

**lineinfile:**

state: present

dest: /etc/ssh/sshd\_config

regexp: ^#?PermitEmptyPasswords

line: PermitEmptyPasswords no

validate: sshd -tf %s

notify: restart sshd



Rule Title: The operating system must implement address space layout randomization to protect its memory from unauthorized code execution.

Fix Text:

Check the kernel setting for virtual address space randomization with the following command:

```
# /sbin/sysctl kernel.randomize_va_space  
kernel.randomize_va_space=2  
kernel.randomize_va_space=2
```

- name: "MEDIUM | RHEL-07-020190 | PATCH |  
The operating system must implement address space layout randomization to protect its memory from unauthorized code execution."

```
sysctl:  
  name: kernel.randomize_va_space  
  value: 2  
  state: present  
  reload: yes  
  ignoreerrors: yes  
  notify: reboot system
```

Rule Title: The network element must only allow management connections for administrative access from hosts residing in to the management network.

Fix Text: Configure an ACL or filter to restrict management access to the management network

ACL or filter

management network

- hosts: ios
- connection: local

tasks:

- name: Create management ACL

**ios\_config:**

parents: ip access-list mgmnt

before: no ip access-list mgmnt

lines:

- 10 permit ip host 192.168.1.99 log
- 20 permit ip host 192.168.1.121 log

- name: Harden VTY lines

**ios\_config:**

parents: line vty 0 15

lines:

- exec-timeout 15
- transport input ssh
- access mgmnt in



Rule Title: Anonymous enumeration of shares must be restricted.

Fix Text: Configure the policy value for Computer Configuration -> Windows Settings -> Security Settings -> Local Policies -> Security Options -> "Network access: Do not allow anonymous enumeration of SAM accounts and shares" to "Enabled".

- **hosts:** windows

**tasks:**

- **name:** Restrict enumeration of shares

**win\_regedit:**

**key:** 'HKLM:

**\System\CurrentControlSet\Control\Lsa'**


**value:** RestrictAnonymous

**data:** 1

**datatype:** dword



6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor- supplied security patches. Install critical security patches within one month of release.

- name: RHEL | Install updates  
**yum:**  
  name: "\*"   
  state: latest  
  exclude: "mysql\* httpd\* nginx\*"   
  when: "ansible\_os\_family == 'RedHat'" 
- name: DEBIAN | Install updates  
**apt:**  
  update\_cache: yes  
  cache\_valid\_time: 7200  
  name: "\*"   
  state: latest  
  when: "ansible\_os\_family == 'Debian'" 



Change root password every 60 days

---

```
- name: Change root password
  hosts: all
  become: yes
  vars:
    root_password: "{{ vault_root_password }}"
    root_password_salt: "{{ vault_root_password_salt }}"
  tasks:
    - name: Change root password
      user:
        name: root
        password: "{{ root_password |
password_hash(salt=root_password_salt) }}"
```

```
- name: Protect against CVE-2016-5696
hosts: all
become: yes
become_user: root

tasks:
  - name: CVE-2016-5696 | Limit TCP challenge ACK limit
    sysctl:
      name: net.ipv4.tcp_challenge_ack_limit
      value: 999999999
      sysctl_set: yes
```



- Database hardening
- Web Shell Inspection
- Hardening a host firewall
- Hardening Web Servers
- Enable SSL on Content Management System
- Enabling Encrypted Storage Backups
- Web Application Security Testing
- And so many more...

Ansible Lockdown

Ansible Hardening

Ansible Galaxy

Mailing List

<https://github.com/samdoran/demo-playbooks>



# THANK YOU



[plus.google.com/+RedHat](https://plus.google.com/+RedHat)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[twitter.com/RedHatNews](https://twitter.com/RedHatNews)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)