



# Enterprise Compliance & Security with Ansible

Montreal, Canada  
August 20, 2019

---

JULIO VILLARREAL PELEGRINO  
CHIEF ARCHITECT, CLOUD & INFRASTRUCTURE  
@juliov01 | julio@redhat.com



This **WILL** be an interactive session...

Please register here to take part in the interactive parts of the session:

[PolleEV.com/redhat2018](http://PolleEV.com/redhat2018)

or

Text REDHAT2018 to **22333**

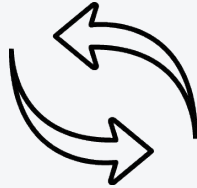
# Talking Points:

- ★ **Why All the FUD (fear, uncertainty, doubt)?**
- ★ **Why is Security and Compliance So Hard?**
- ★ **Simply Define Security**
- ★ **Raising the Bar**
- ★ **Crossing the barriers of “fear” and “intimidation”**



**SIMPLE**

+



**POWERFUL**

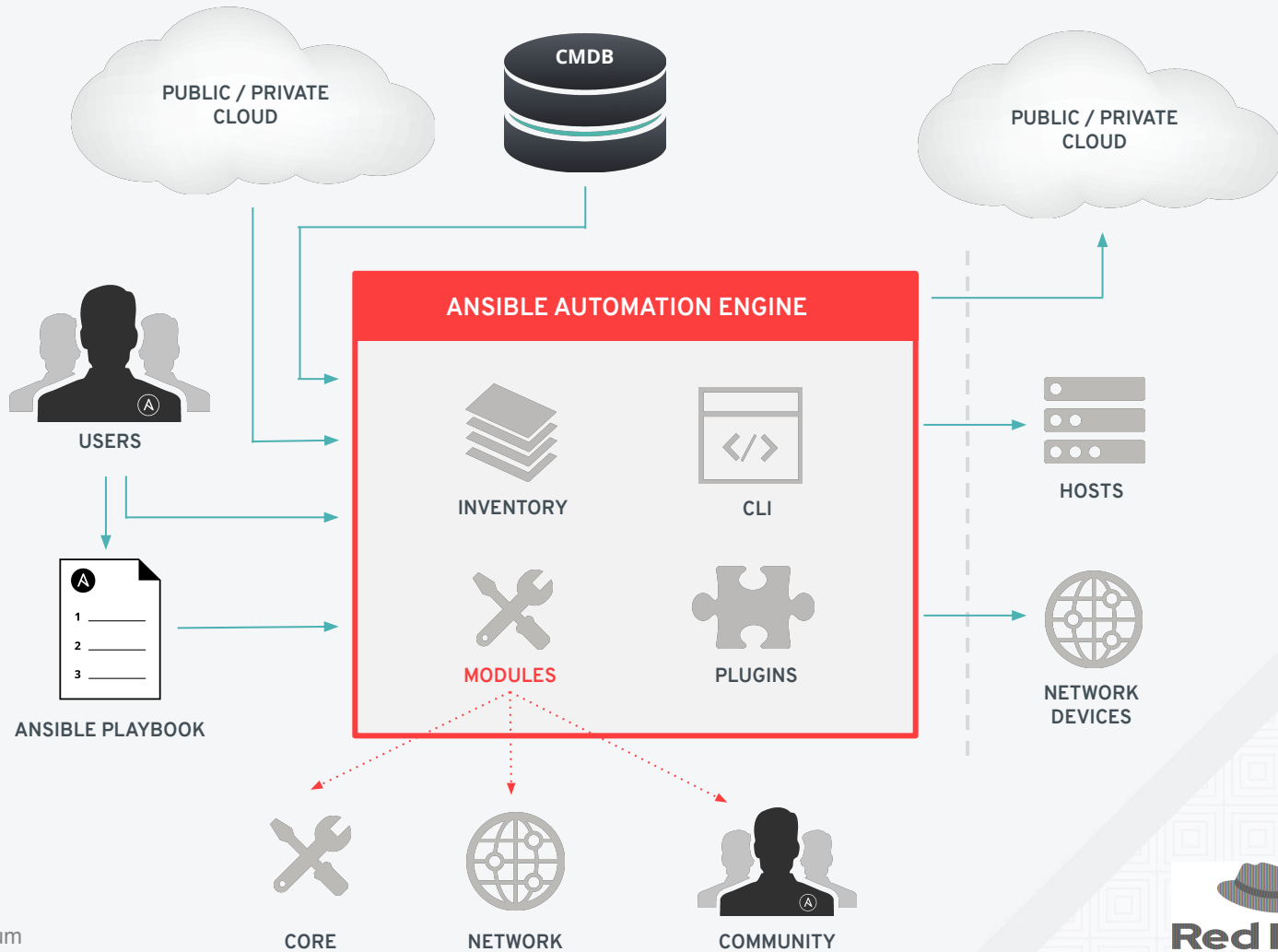
+



**AGENTLESS**

=

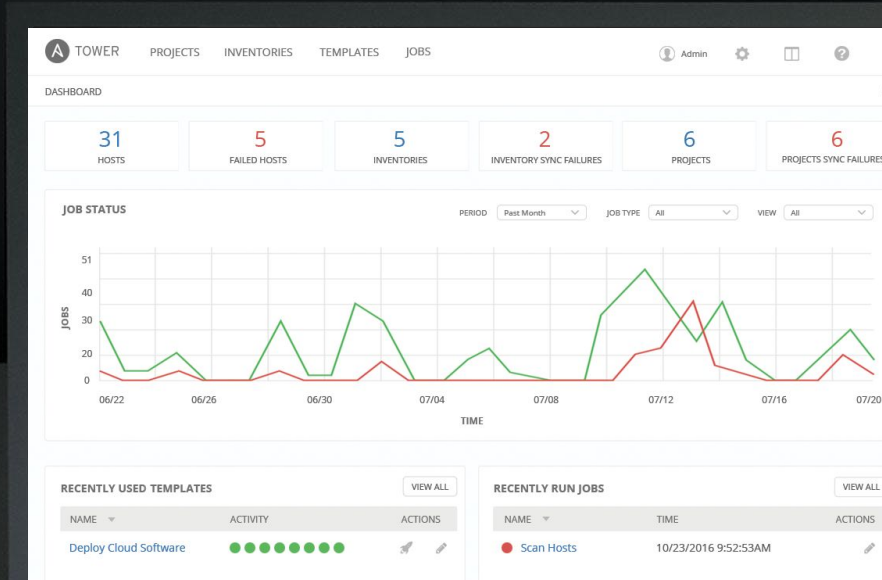






# RED HAT<sup>®</sup> ANSIBLE<sup>®</sup> Tower

- Building, managing dynamic inventory
- Organizing admin control with users and teams
- Leverage Ansible Workflows to break up tasks
- Support for Ansible privilege escalation plugins
- Support for deployment on, and management of, Red Hat Enterprise Linux<sup>®</sup> 8
- Enablement of Automation Insights
- Utilize the RESTful API for anything



# What is keeping you up at night?

# Why All The FUD?

(fear, uncertainty, and doubt)

---

## Security

Antivirus and Antimalware  
Software  
Application  
Data Loss Prevention  
Email

Firewalls  
Network Security, Access  
Control & Segmentation  
Web  
Endpoint

---

## Compliance

Software management (updates and patches)  
Vendor management  
User Access Controls/Tracking  
**AND all the security components above**

---



# Why is Security and Compliance so hard?

# Point Blank

## Security

- is practiced for its own sake, not to satisfy a third party's needs
- ~~is driven by the need to protect against constant threats to an organization's assets~~
- improved ~~is~~ finished and should be continuously maintained and improved

## Compliance

- ~~is practiced to satisfy external requirements and facilitate business operations~~
- is "done" when the third party is satisfied
- is driven by business needs rather than technical needs
- is "done" when the third party is satisfied

# What Does Security Look Like to You?

# Software Management

Scenario:

Your QSA is expected to come in and you are tasked with making sure all Linux systems packages are up to date

```
---  
## This role pushes software package patches for RHEL leveraging Satellite.  
  
- name: Check build status  
  stat:  
    path: /root/INITIAL_BUILD  
    register: bstat  
    changed_when: false  
  
- name: Set fact if yupdate is defined  
  set_fact:  
    ystate: "latest"  
  when: yupdate is defined  
  
- name: Set fact if yupdate is not defined  
  set_fact:  
    ystate: "present"  
  when: yupdate is not defined  
  
- name: Build Yum update  
  shell: yum -y update  
  when: bstat.stat.exists == true  
  
- name: Remove INITIAL_BUILD  
  file:  
    path: /root/INITIAL_BUILD  
    state: absent  
  when: bstat.stat.exists == true  
  
- name: restart machine  
  shell: sleep 2 && shutdown -r now "Ansible updates triggered"  
  async: 1  
  poll: 0  
  ignore_errors: true  
  when: bstat.stat.exists == true  
  
- name: wait for server reboot  
  local_action:  
    wait_for host: "{{ inventory_hostname }}"  
    state: started  
    port: 22  
    delay: 30  
    timeout: 300  
    connect_timeout: 15  
  when: bstat.stat.exists == true  
  
- name: Ensure Packages EL 5  
  yum:  
    state: '{{ ystate }}'  
    disable_gpg_check: yes  
    name:  
      - net-tools  
      - authconfig  
      - openldap-clients  
      - nscd  
      - xinetd
```

# Application

Scenario:

New web application was deployed and requires a new VIP pool and pool members need to be defined

```
---|
## This role configures an F5 based on the application requirements.

- name: Create F5 pool
  bigip_pool:
    server: "{{ f5 }}"
    user: "{{ f5_user }}"
    password: "{{ f5_pass }}"
    state: present
    validate_certs: no
    name: "{{ item.name }}"
    lb_method: "{{ item.lb_method }}"
    monitors: "{{ item.monitors }}"
  with_items: "{{ f5_portal_pools }}"
  tags:
    - f5

- name: Create F5 pool members
  bigip_pool_member:
    server: "{{ f5 }}"
    user: "{{ f5_user }}"
    password: "{{ f5_pass }}"
    state: present
    validate_certs: no
    host: "{{ hostvars[item].ansible_ssh_host }}"
    port: 80
    description: "{{ hostvars[item].ansible_ssh_host }}:80"
    pool: "{{ portal_pool }}"
  with_items: "{{ portal_hosts }}"
  tags:
    - f5

- name: Create F5 virtual server
  uri:
    url: "https://{{ f5 }}/mgmt/tm/ltn/virtual"
    method: POST
    user: "{{ f5_user }}"
    password: "{{ f5_pass }}"
    body: '{{ jsoncontent_portal }}'
    body_format: json
    force_basic_auth: yes
    validate_certs: no
  failed_when: no
  tags:
    - f5
```

# User Access Controls

Scenario:

Deploying a new private cloud platform and you need to setup/configure all of your security tools across 50-100 bare metals servers **AFTER** they have been already built

```
---  
## This role sets access for security service accounts.  
- name: Copy group file  
  copy:  
    src: sec-group.txt  
    dest: /usr/share/sec-group.txt  
- name: Add Security groups  
  shell: cat /usr/share/sec-group.txt >> /etc/group  
  args:  
    chdir: /usr/share  
- name: Create home directories  
  command: mkdir -p /home/qualys/.ssh /home/nessus/.ssh  
  ignore_errors: yes  
- name: Create Security user  
  user:  
    name: {{ item.value.name }}  
    comment: "{{ item.value.desc }}"  
    uid: {{ item.value.uid }}  
    group: {{ item.value.group }}  
    shell: {{ item.value.shell }}  
  with_dict: users  
  ignore_errors: yes  
- name: Copy shadow file  
  copy:  
    src: sec-shadow.txt  
    dest: /usr/share/sec-shadow.txt  
- name: Add sec users to shadow file  
  shell: cat /usr/share/sec-shadow.txt >> /etc/shadow  
  args:  
    chdir: /usr/share  
- name: Copy authorized keys  
  template:  
    src: sec-keys  
    dest: /home/{{ item.0 }}/.ssh/authorized_keys  
  with_together:  
    - user_id  
    - key  
- name: Set home directory permissions  
  command: chown -R 960:2023 /home/qualys  
- name: Set home directory permissions  
  command: chown -R 2996:2023 /home/nessus
```

# Firewall

Scenario:

Deploying a new vendor facing  
API and need to setup new  
Firewall rules to allow for secure  
connectivity

```
---  
- hosts: asa  
  gather_facts: false  
  connection: network_cli  
  
  vars:  
    asa_rule: a  
  
  tasks:  
    - name: Define Values From CSV File  
      set_fact:  
        source_group: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=1) }}"  
        src_1: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=2) }}"  
        src_2: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=3) }}"  
        destination_group: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=4) }}"  
        dst_1: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=5) }}"  
        dst_2: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=6) }}"  
        change_number: "{{ lookup('csvfile', asa_rule + ' file=csv_files/asa_rules.csv delimiter=', col=7) }}"  
      delegate_to: localhost  
  
    - name: jinja template  
      template:  
        src: templates/asa_rules.j2  
        dest: configs/asa_config.txt  
      delegate_to: localhost
```

# Raising The Bar



# Good Baseline

Red Hat provided + supported

Ansible playbooks

/usr/share/scap-security-guide/ansible



```
ssg-debian8-role-anssi_np_nt28_average.yml
ssg-debian8-role-anssi_np_nt28_high.yml
ssg-debian8-role-anssi_np_nt28_minimal.yml
ssg-debian8-role-anssi_np_nt28_restrictive.yml
ssg-debian8-role-common.yml
ssg-eap6-role-stig-eap6-disa.yml
ssg-fedora-role-common.yml
ssg-fedora-role-standard.yml
ssg-firefox-role-stig-firefox-upstream.yml
ssg-fuse6-role-common.yml
ssg-fuse6-role-stig-amq-upstream.yml
ssg-fuse6-role-stig-fuse6-upstream.yml
ssg-jre-role-stig-java-upstream.yml
ssg-opensuse-role-common.yml
ssg-rhel6-role-C25.yml
ssg-rhel6-role-common.yml
ssg-rhel6-role-CS2.yml
ssg-rhel6-role-CSCF-RHEL6-MLS.yml
ssg-rhel6-role-desktop.yml
ssg-rhel6-role-fisma-medium-rhel6-server.yml
ssg-rhel6-role-ftp-server.yml
ssg-rhel6-role-nist-cl-il-al.yml
ssg-rhel6-role-pci-dss.yml
ssg-rhel6-role-rht-ccp.yml
ssg-rhel6-role-server.yml
ssg-rhel6-role-standard.yml
ssg-rhel6-role-stig-rhel6-server-upstream.yml
ssg-rhel6-role-usgcb-rhel6-server.yml
ssg-rhel7-role-C25.yml
maty@localhost.localdomain:~ $
ssg-st7-role-cjis-rhel7-server.yml
ssg-st7-role-common.yml
ssg-st7-role-docker-host.yml
ssg-st7-role-nist-800-171-cui.yml
ssg-st7-role-ospp-rhel7.yml
ssg-st7-role-pci-dss.yml
ssg-st7-role-rht-ccp.yml
ssg-st7-role-standard.yml
ssg-st7-role-stig-ansible-tower-upstream.yml
ssg-st7-role-stig-http-disa.yml
ssg-st7-role-stig-ipa-server-upstream.yml
ssg-st7-role-stig-rhel7-disa.yml
ssg-st7-role-stig-rhev7-upstream.yml
ssg-st7-role-stig-satellite-upstream.yml
ssg-sle11-role-common.yml
ssg-sle11-role-server.yml
ssg-sle12-role-common.yml
ssg-ubuntu1404-role-anssi_np_nt28_average.yml
ssg-ubuntu1404-role-anssi_np_nt28_high.yml
ssg-ubuntu1404-role-anssi_np_nt28_minimal.yml
ssg-ubuntu1404-role-anssi_np_nt28_restrictive.yml
ssg-ubuntu1404-role-common.yml
ssg-ubuntu1604-role-anssi_np_nt28_average.yml
ssg-ubuntu1604-role-anssi_np_nt28_high.yml
ssg-ubuntu1604-role-anssi_np_nt28_minimal.yml
ssg-ubuntu1604-role-anssi_np_nt28_restrictive.yml
ssg-ubuntu1604-role-common.yml
ssg-webmin-role-common.yml
ssg-wrlinux-role-basic-embedded.yml
```

Community Authors > RedHatOfficial

RedHatOfficial  
Red Hat, Inc.  
<https://github.com/RedHatOfficial>

Roles

Name	Filter by Name...	Name	Downloads	Forks	Watchers	Stars	View content
manageiq_workers			132	0	7		
rhel7_c2s			26	1	3	0	
rhel7_cjis			3	0	3	0	
rhel7_disa_stig			115	0	3	1	

# Ansible + OpenSCAP

Ansible remediation playbooks provided (new with RHEL 7.5)

Generate based on DISA STIG:

```
$ oscap xccdf generate fix --fix-type ansible --profile  
xccdf org.ssgproject.content profile stig-rhel7-disa --output stig-rhel7-role.yml  
/usr/share/xml/scap/ssg/content/ssg-rhel7-ds.xml
```

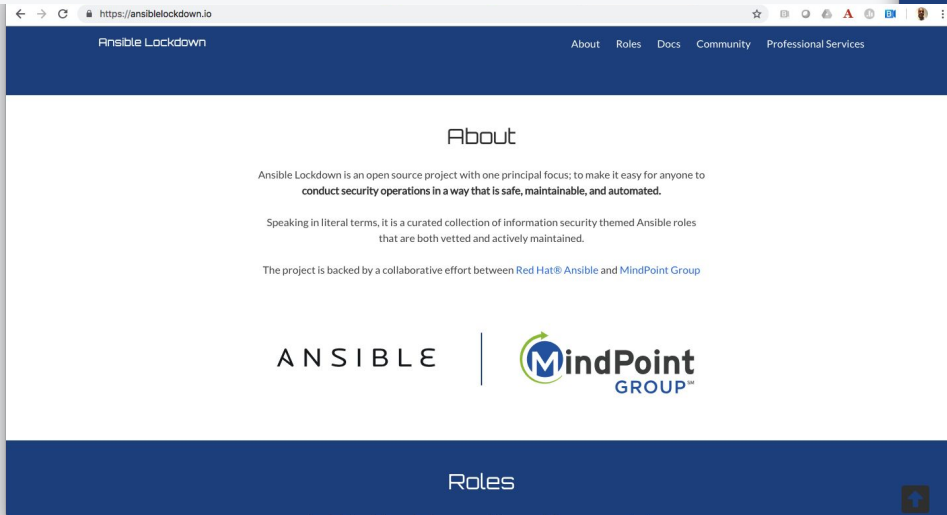
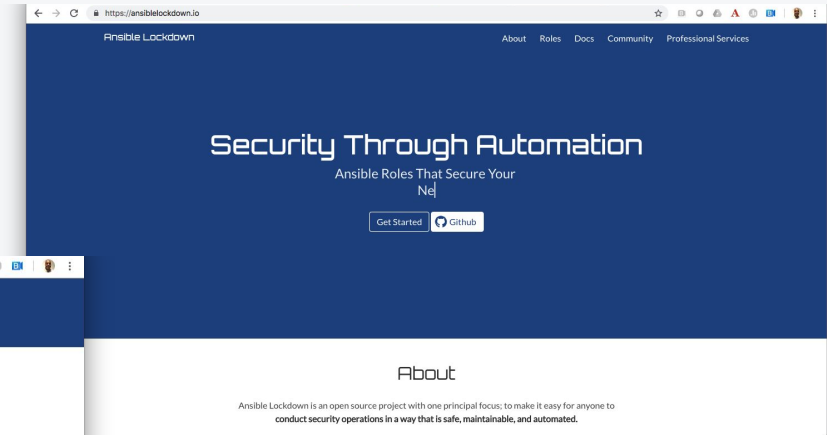
Generate based on a SCAN result:

```
$ oscap xccdf generate fix --fix-type ansible --result-id  
xccdf org.open-scap testresult xccdf org.ssgproject.content profile stig-rhel7-disa  
--output stig-playbook-result.yml results.xml
```

Apply:

```
ansible-playbook playbook.yml
```

# Ansiblelockdown.io



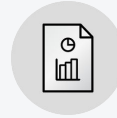
# Crossing the Barriers of “fear” and “intimidation”

# Be a **Security Jedi!**



# Ansible -> Security

Configuration Compliance

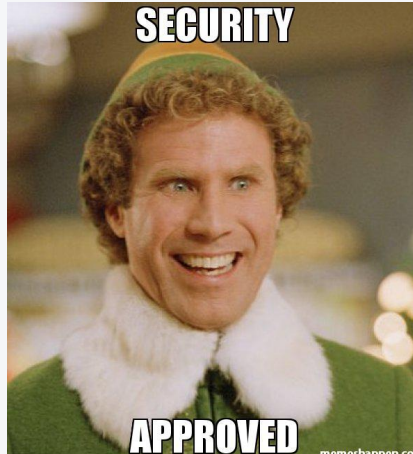


Enterprise Security  
Automation at Scale

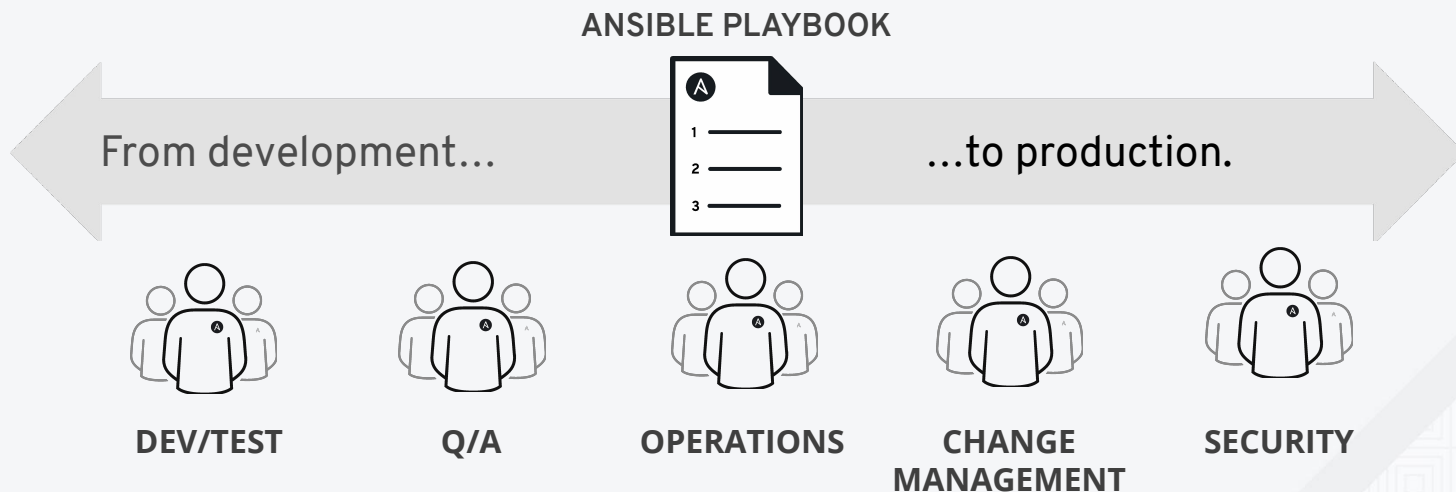
Remediation &  
Incident Response



Security as Code



# Use Ansible as the **common language**



# Quick examples



# Mitigating Meltdown and Spectre

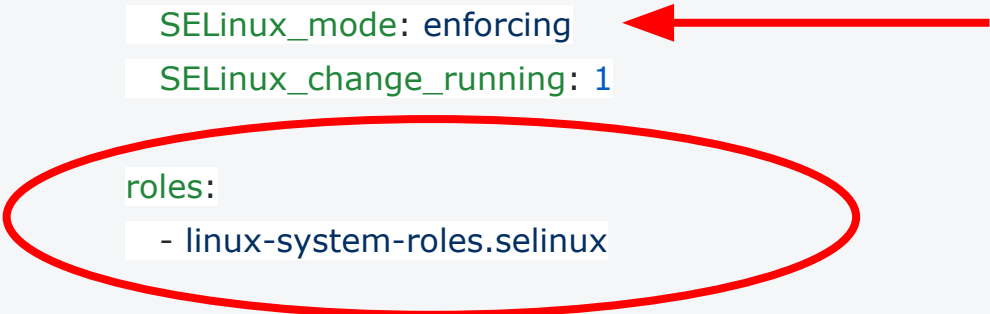
```
- name: Patch Linux systems against Meltdown and Spectre
hosts: "{{ target_hosts | default('all') }}"
become: yes

vars:
  reboot_after_update: no
  packages:
    # https://access.redhat.com/security/vulnerabilities/speculativeexecution
    RedHat7:
      - kernel-3.10.0-693.11.6.el7
      - microcode_ctl-2.1-22.2.el7
      - perf-3.10.0-693.11.6.el7
      - python-perf-3.10.0-693.11.6.el7
    RedHat6:
      - kernel-2.6.32-696.18.7.el6
      - kernel-firmware-2.6.32-696.18.7.el6
      - perf-2.6.32-696.18.7.el6
      - python-perf-2.6.32-696.18.7.el6

tasks:
  - name: RHEL | Install kernel updates
    yum:
      name: "{{ packages[ansible_os_family ~ ansible_distribution_major_version] }}"
      state: present
    when: ansible_pkg_mgr == 'yum'
    notify: reboot system
```

# SELinux prevention for ShellShock

```
---  
- hosts: all  
  become: true  
  become_user: root  
  vars:  
    SELinux_type: targeted  
    SELinux_mode: enforcing  
    SELinux_change_running: 1  
  roles:  
    - linux-system-roles.selinux
```



# Time to play!

# Is Ansible agentless?

Yes

No

# What are the languages behind Ansible?

Python and C

Python and  
YAML

Go and Python

Bash and Go

# What does Ansible solves when it comes to security?

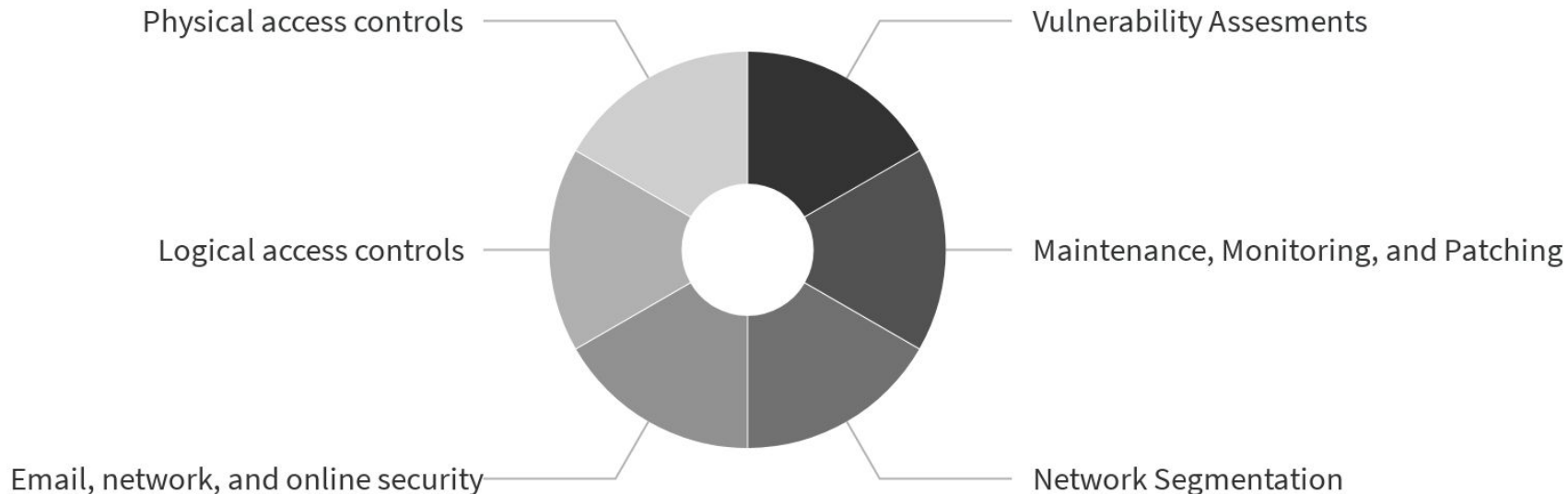
Set the standards

Helps define  
security

Secures everything  
auto-magically

# What are the security priorities in your organization?

Vulnerability Assesments **A**   Maintenance, Monitoring, and P... **B**   Network Segmentation **C**   Email, network, and online sec... **D**  
Logical access controls **E**   Physical access controls **F**



# Next Steps

- Speak with a Red Hat expert here at Security Symposium
- Look for the slides in a “Thank You” email from us in the next few days
- Stay up to date with Red Hat at [redhat.com/security](https://redhat.com/security)
- Visit [redhat.com/events](https://redhat.com/events) to find out about workshops and other events like this one coming to your area

Thank you for coming.

Feedback or questions?

[julio@redhat.com](mailto:julio@redhat.com)

@juliovp01







# Why Ansible

- Agentless
  - SSH/WinRM
- Desired State
- Extensible and Modular
- Push-based architecture
- Consistent

