RED HAT®
ANSIBLE®
Automation

Ansible Security Automation

Faz Sadeghi
Specialist Solution Architect
Red Hat Ansible Automation
faz@redhat.com

AGENDA

Information security

Why Ansible

Examples

Ansible Security Automation, ASA

Get involved

INFO SEC AREAS

Application Security

Network Security

Forensics

Incident Response

Penetration Testing

Fraud Detection and Prevention

Governance, Risk, Compliance

WHY IS INFO SEC COMPLICATED

ANSIBLE

People

Processes

Economics

Technology

redhat.

FLEXIBILITY IS CRUCIAL

WITH POWER COMES RESPONSIBILITY

NOT ZERO SUM

+

!= 0

WHAT CAN I DO WITH ANSIBLE?

Automate the deployment and management of your entire IT footprint.

Do this...

- Orchestration
- Configuration Management
- Application Deployment
- Provisioning
- Continuous Delivery
- Network Automation

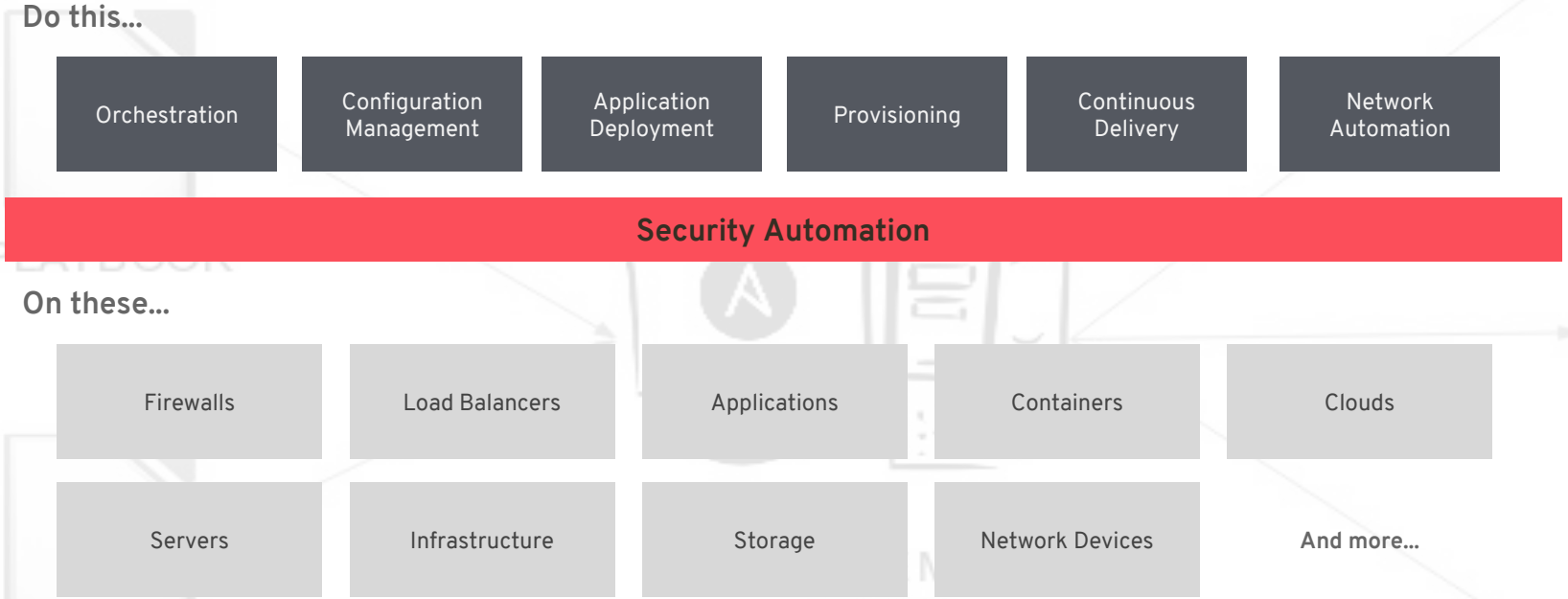
On these...

- Firewalls
- Load Balancers
- Applications
- Containers
- Clouds
- Servers
- Infrastructure
- Storage
- Network Devices
- And more...

WHAT CAN I DO WITH ANSIBLE?

ANSIBLE

Automate the deployment and management of your entire IT footprint.



redhat.

WHY ANSIBLE FOR SECURITY AUTOMATION?

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

WALLS OF SEPARATION

SECurity

Wants to ensure
Information Assurance

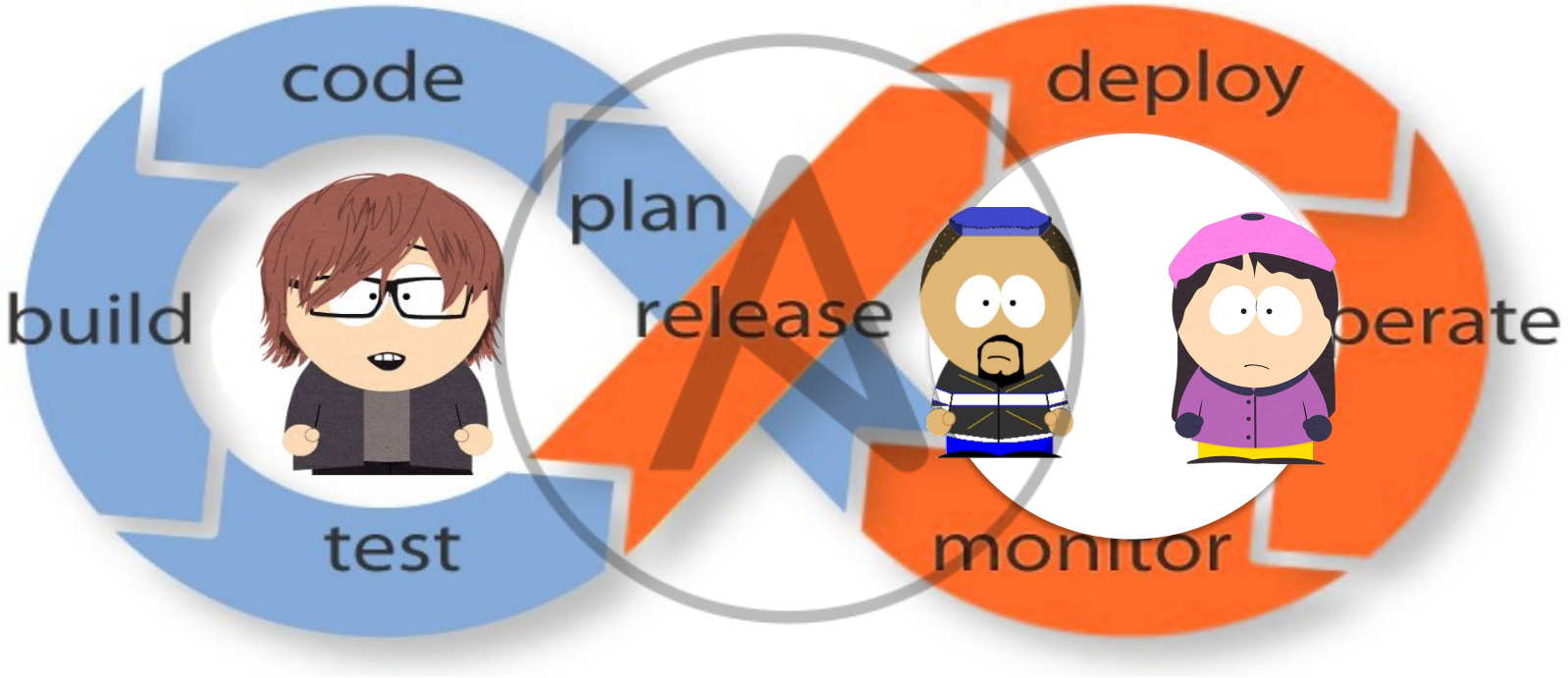
OPerationS

Wants to ensure
System Availability

DEVelopers

Wants to deliver
Applications Fast

ALL IN ALL, LET'S BREAK THE WALL



ANSIBLE TOWER

- Ansible Tower is an **enterprise framework** for controlling, securing and managing automation – with a **UI and RESTful API.**
- **Role-based access control**
- **Deploy** entire applications with **push-button deployment** access
- All automations are **centrally logged**

Self Service

- Enable operational teams
- Run on demand

Credentials

- Single repo
- Custom credentials
- AES 128

Roles

- Purpose and function focused
- Easy to build and publish

Version Control

- Single source of truth
- Security branch anyone

Linux, Windows and Networking, STIG Standard

Internal policy

PCI DSS requirement

Remediation

Incident Response

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":

PermitEmptyPasswords no

line

/etc/ssh/sshd_config

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
```

SECURITY POLICY - NETWORK

ANSIBLE

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 device from only 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
```


redhat.

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
```

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) }}"
```

Protect against he TCP "challenge ACK" side channel

```
- 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
```

Protect against MacOS High Sierra root bug

```
- name: Protect against MacOS High Sierra root bug
  hosts: macs
  become: yes

  tasks:
   - name: Change root password
     user:
       name: root
       update_password: always
       password: " { { root_password | password_hash( 'sha512' ) } } "

   - name: address CVE-2017-13872
     command: " softwareupdate  – i  ' Security Update 2017-001' "

   - name: reboot after security update
     reboot:
```

```
- 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
```

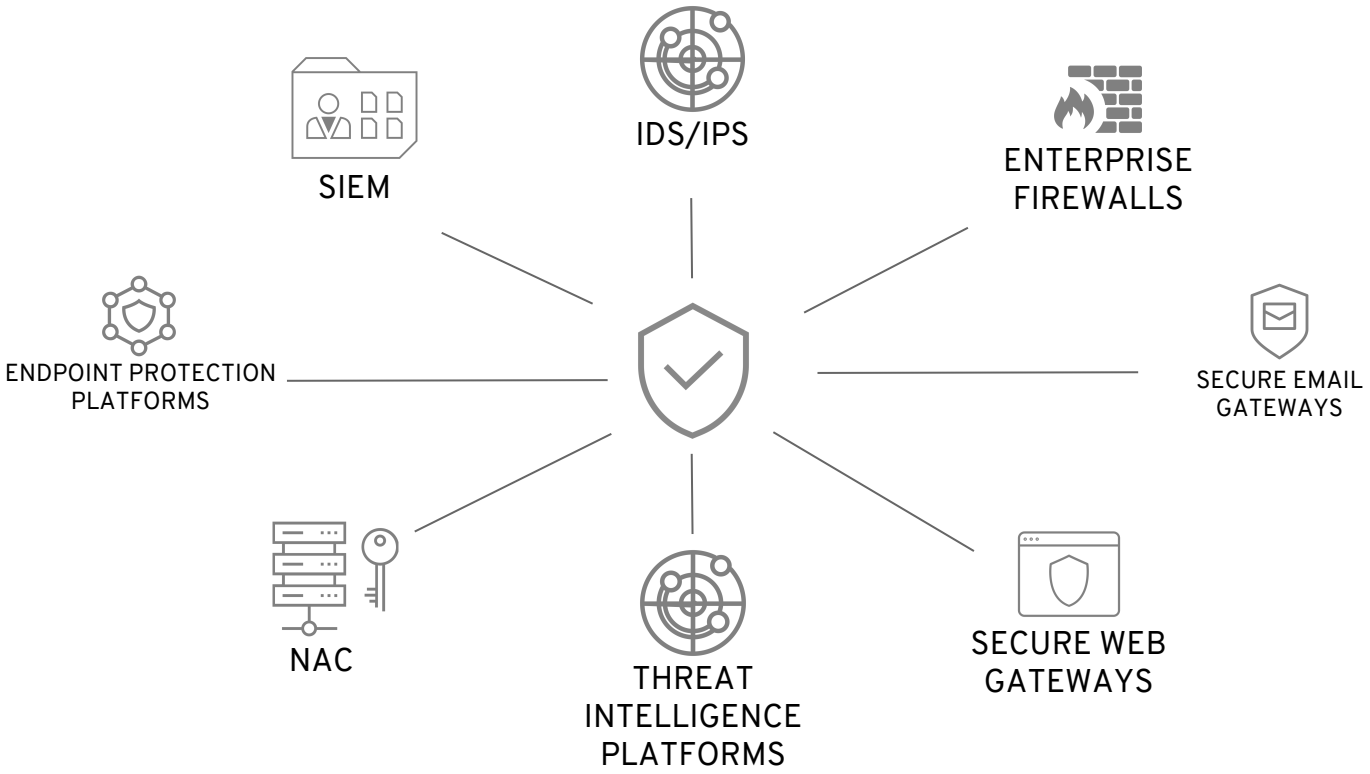
INCIDENT RESPONSE - LOGS

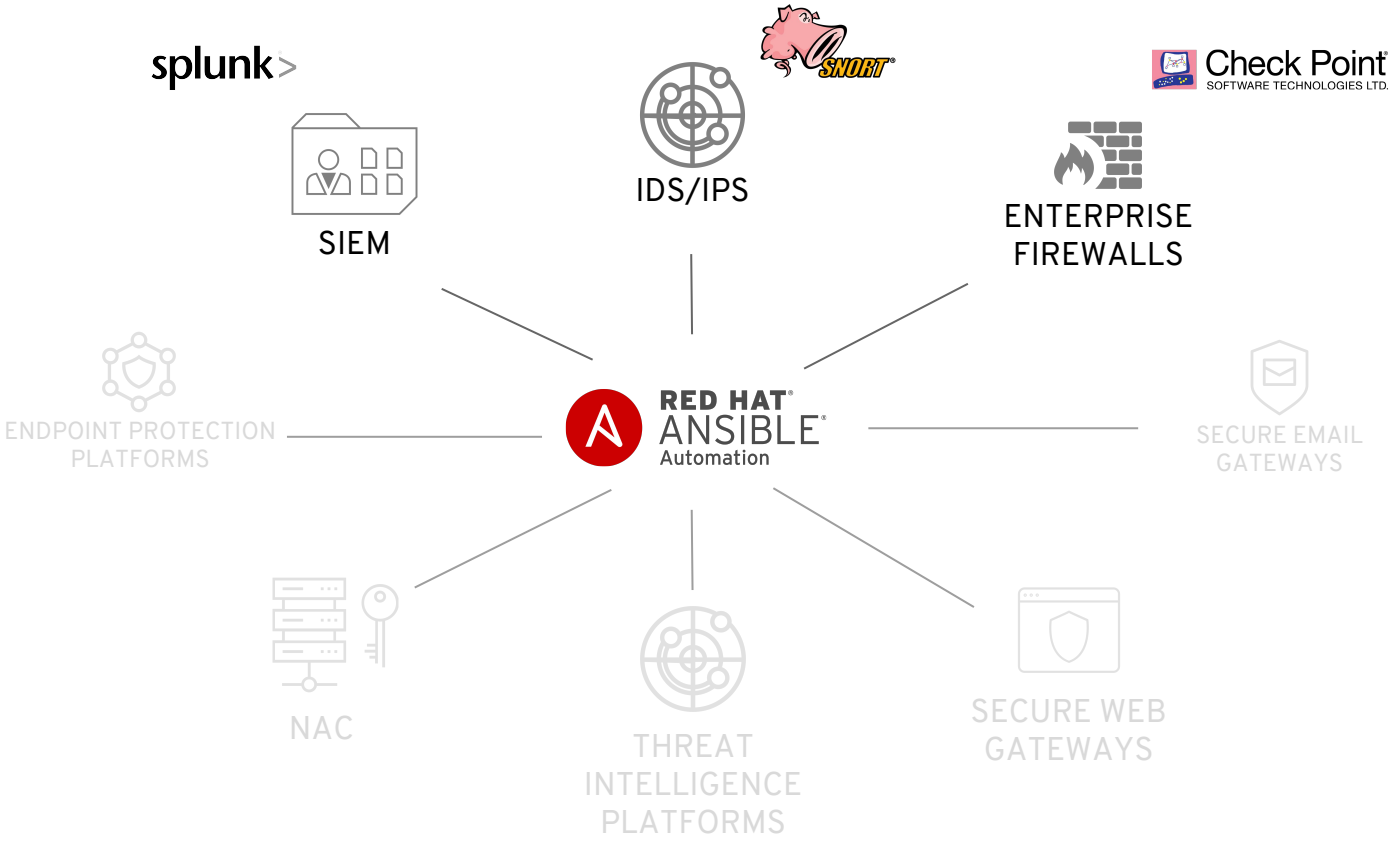

```
- name: Gather logs files from remote systems
  hosts: lab
  become: yes

  tasks:
    - name: Find logs
      find:
        paths: /var/log/
        patterns: '*.log'
        recurse: yes
      register: _logs

    - name: Fetch logs
      fetch:
        src: "{{ item.path }}"
        dest: logs
      with_items: "{{ _logs.files }}"
```

ANSIBLE SECURITY AUTOMATION, ASA


SIEM
IDS/IPS
ENTERPRISE FIREWALLS
ENDPOINT PROTECTION PLATFORMS
SECURE EMAIL GATEWAYS
NAC
THREAT INTELLIGENCE PLATFORMS
SECURE WEB GATEWAYS


splunk>
SNORT
Check Point
SOFTWARE TECHNOLOGIES LTD.
SIEM
IDS/IPS
ENTERPRISE
FIREWALLS
ENDPOINT PROTECTION
PLATFORMS
RED HAT
ANSIBLE
Automation
SECURE EMAIL
GATEWAYS
NAC
THREAT
INTELLIGENCE
PLATFORMS
SECURE WEB
GATEWAYS

Ansible Lockdown

Ansible Hardening

Mailing List

Ansible Galaxy

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

P2 www.projecttimes.com/articles/information-security-project-management.html
P4 https://vignette.wikia.nocookie.net/spongebob/images/6/63/Wet_Painters_108.png/revision/latest?cb=20161022071552
https://www.imdb.com/title/tt0206512/mediaviewer/rm3743357440
http://theadventuresofgarythesnail.wikia.com/wiki/File:Squilliam_Returns_013.jpg
https://i.imgflip.com/1hlgnj.jpg
P7 https://www.pinterest.co.uk/pin/795940934114843310/?lp=true
P9 https://medium.com/formcept/configuration-management-and-continuous-deployment-cd0892dce998
P12 https://www.niceideas.ch/roller2/badtrash/entry/devops-explained
P13 https://www.niceideas.ch/roller2/badtrash/entry/devops-explained
P15 https://www.digitalocean.com/community/tutorials/how-to-create-ansible-playbooks-to-automate-system-configuration-on-ubuntu