

### Security Automation with Ansible

#### Bridging the Automation Gap in SecOps

Adam Miller Senior Principal Software Engineer Ansible Engineering

Red Hat Summit 2019

# **INFORMATION SECURITY**

#### **KEY SUBJECT AREAS**

- Application Security
- Network Security
- Digital Forensics

#redhat #rhsummit

- Incident Response
- Penetration Testing
- Fraud Detection and Prevention
- Intrusion Detection and Prevention
- Governance, Risk, Compliance

### SECURITY VS OPERATIONS

# SEC VS OPS

#### IT OPERATIONS VS SECURITY TEAM

- Traditionally disjoint roles and responsibilities
- IT Operations (should) harden systems
  - Manages infrastructure
  - Deploys and maintains systems
- Security Operations Team
  - Tracks ongoing threats
  - Intrusion Detection/Prevention
  - Firewall management
  - Auditing
  - Red Team/Blue Team (maybe?)

#### SECURITY IS EVERYBODY'S RESPONSIBILITY

"For one, **security teams are overwhelmed**. The average security team typically examines less than 5% of the alerts flowing into them every day (and in many cases, much less than that). "



#### "Having **insufficient skilled personnel** dedicated to cybersecurity was the second biggest barrier to cyber resilience, with only 29% having the ideal staffing level."

The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

"57% of respondents said the

#### time to resolve an incident has increased

65% reported the

#### severity of attacks has increased"

The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

#redhat #rhsummit

"63% of respondents say their leaders understand that **automation**, machine learning, artificial intelligence and **orchestration** strengthens cyber resilience."

The Third Annual Study on the Cyber Resilient Organization - Ponemon Institute (Sponsored by IBM)

### WHY ANSIBLE?

#### SIMPLE

#### POWERFUL

### AGENTLESS

Human readable automation

No special coding skills needed

Tasks executed in order

Get productive quickly

Gather Information and Audit

Configuration and System State management

Workflow orchestration

Manage ALL IT infrastructure

Agentless architecture

Uses native connection protocols (SSH, HTTPS, etc)

No agents to exploit or update

More efficient & more secure

# WHY ANSIBLE?

#### ANSIBLE IS AN AUTOMATION TOOL

- IT Security is something we (should) do for all systems and technologies
- This leads to repetitive work as you:
  - Bring systems online
  - Take systems offline
  - Face new threats
  - Deploy new apps
  - Modify firewall rules
  - Threat hunt
  - Remediate

#### Security is not special, it's just another thing to automate

### ANSIBLE IS THE UNIVERSAL LANGUAGE



# ANSIBLE IS PERVASIVE

#### Top open source projects

VS Code, React, and Tensorflow once again top our list of open source projects by contributor count. New to the list are projects that manage containerized applications, share Azure documentation, and consolidate TypeScript type definitions: Kubernetes, Azure Docs, and DefinitelyTyped. \*

## 96 Million+ Projects

Octoverse 2018 - GitHub

		Contributors	
1	<u>Microsoft/vscode</u>	<b>19</b> ĸ	
2	facebook/react-native	<b>10</b> ĸ	
3	tensorflow/tensorflow	<b>9.3</b> ĸ	
4	<u>angular/angular-cli</u>	<b>8.8</b> ĸ	
5	<u>MicrosoftDocs/azure-docs</u>	<b>7.8</b> κ	
6	<u>angular/angular</u>	<b>7.6</b> κ	
7	<u>ansible/ansible</u>	<b>7.5</b> κ	
8	kubernetes/kubernetes	<b>6.5</b> ĸ	••
9	<u>npm/npm</u>	<b>6.1</b> κ	
10	DefinitelyTyped. DefinitelyTyped	<b>6.0</b> κ	

Contributore

### ANSIBLE IS NOT ZERO SUM



### SYSTEM HARDENING

# COMPLIANCE

- Federal Information Processing Standards (FIPS)
  - Standards developed by the United States federal government for use in computer systems by non-military government agencies and government contractors
  - FIPS 140 Security requirements for cryptography modules
  - FIPS 153 (3D graphics)
  - FIPS 197 (Rijndael / AES cipher)
  - FIPS 199 Standards for Security Categorization of Federal Information and Information Systems
  - FIPS 201 Personal Identity Verification for Federal Employees and Contractors

# GUIDANCE

- Security Technical Implementation Guide (STIG)
  - Configuration standards for DOD IA and IA-enabled devices/systems
  - Comes from the Defense Information Systems Agency (DISA), part of the United States Department of Defense.
  - The guide is released with a public domain license and it is commonly used to secure systems at public and private organizations around the world.
  - System and Version/Release specific
    - RHEL 7 STIG Version 1, Release 3 (Published on 2017-10-27)
    - RHEL 7 STIG Version 1, Release 1 (Published on 2017-02-27)
    - RHEL 7 STIG Version 1, Release 4 (Published on 2018-01-26)



# ansiblelockdown.io

#### Ansible roles that **SECURE** your...

- Systems
- Servers
- Networks

- Cloud
- Ø Desktops
- Ø Middleware





# ANSIBLE LOCKDOWN

Ansible Lockdown (https://ansiblelockdown.io/)

- Official Subproject of Ansible done in partnership with MindPoint Group
  - <u>https://github.com/ansible/ansible-lockdown</u>
- Community focused mailing list
  - <u>https://groups.google.com/forum/#!forum/ansible-lockdown</u>
- Covers STIG for the following Operating Systems
  - RHEL 6
  - RHEL 7
  - Windows Server 2012 DC
  - Windows Server 2012 MS
  - Windows Server 2008R2 MS

### SYSTEM HARDENING EXAMPLES

## STIG - RHEL7

**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

# STIG - RHEL7

**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

"/et line sshd\_config": /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



# **STIG - NETWORK**

**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.

# **STIG - NETWORK**

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

Fix Text: Configure a ACL or filter device device the 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

# PCI DSS

6.2 Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendorsupplied 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'"

# INTERNAL STANDARDS

Chapter 8, Subsection 5: Login Standards:

Change privileged passwords
 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) }}"
```

### REMEDIATION

# REMEDIATION

- Mitigate CVEs in the wild
- Example:
  - Protect against CVE-2016-5696

```
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
```

# **REMEDIATION - FIX AND VERIFY**

- Mitigate and Verify Mitigation of CVEs in the Wild
- Example:
  - Shell Shock Migiations
  - Shell Shock Verify Vulnerability 1

```
name: Fix and test shellshock
  hosts: all
  tasks:
    - name: Update bash
      yum:
        name: bash
        state: latest
        update_cache: yes
    - name: Test vulnerability 1
      shell: 'env x=''() { :;}; echo
vulnerable'' bash -c "echo this is a test"'
      executable: /bin/bash
      register: vulntest1
      failed when: vulntest1.stdout
search('vulnerable')
      ignore_errors: yes
      changed_when: no
```

# REMEDIATION - FIX AND VERIFY (CON'T)

- Mitigate and Verify Mitigation of CVEs in the Wild
- Example:
  - Shell Shock Verify Vulnerability 2

```
- name: Test vulnerability 2
      shell: 'env X=''() { (a)=>'' bash -c
''echo date'':'
      executable: /bin/bash
      register: vulntest2
      failed when:
        not vulntest2.stderr | search('error
importing function definition')
      ignore_errors: yes
      changed when: no
    - name: Cleanup after vulnerability test 2
      file:
        path: ~/echo
        state: absent
```

### AUDITING AND REPORTING

### SCAP

Security Content Automation Protocol (SCAP)

- Method for using specific standards to enable the automated vulnerability management, measurement, and policy compliance evaluation of systems
  - Common Vulnerabilities and Exposures (CVE)
  - Common Configuration Enumeration (CCE) (prior web-site at MITRE)
  - Common Platform Enumeration (CPE)
  - Common Vulnerability Scoring System (CVSS)
  - Extensible Configuration Checklist Description Format (XCCDF)
  - Open Vulnerability and Assessment Language (OVAL)
  - Open Checklist Interactive Language (OCIL) Version 2.0
  - Asset Identification (AID)
  - Asset Reporting Format (ARF)
  - Common Configuration Scoring System (CCSS)
  - Trust Model for Security Automation Data (TMSAD)

# OpenSCAP

- OpenSCAP
  - An implementation of SCAP
  - $\circ$  Scans
  - Audits
  - Provides remediation recommendations/instructions
  - Defacto-standard in opensource/Linux land
  - <u>https://www.open-scap.org/</u>
- OpenSCAP + Ansible
  - OpenSCAP can audit and generate Ansible Playbooks for remediation
  - <u>https://access.redhat.com/documentation/en-us/red\_hat\_enterprise\_lin</u> <u>ux/7/html/security\_guide/sect-using\_openscap\_with\_ansible</u>

### **RED HAT INSIGHTS**

### **RED HAT**<sup>®</sup> INSIGHTS

Red Hat Insights assesses your Red Hat Enterprise Linux environment to help you proactively identify and remediate threats, avoiding outages and unplanned downtime.

### **RED HAT**<sup>®</sup> INSIGHTS

#### PREDICT RISK. GET GUIDANCE. STAY SECURE.

#### **PREDICTIVE I.T. ANALYTICS**

#### **AUTOMATED EXPERT ASSESSMENT**

SIMPLE REMEDIATION

## **KEY RISKS DISCOVERED**

#### Tailored resolution steps included for resolution



Performance issue Network interface is not performing at maximum speed Recommended action Check cable, connections, and remote switch settings



Security risk detected Privilege escalation

Recommended action Apply mitigation and update the kernel



Availability OpenShift operations fail if insufficient CPU or memory



Stability Filesystem has exceeded 95% capacity Recommended action Increase CPU and/or memory reservation

Recommended action Increase free space on the host.



### Red Hat Insights Compliance

Built on OpenSCAP reporting

#### **COMPLIANCE OFFERS**



Remediate known issues of non-compliance in the Red Hat environment via **Ansible** playbooks based on business risk & relevance Ability to generate JavaScript Object Notation and CSV view-based reports to keep relevant stakeholders informed

Ansible Security Automation is the automation glue between disjoint systems and security appliances that have little to no integrations. Security Operators can utilize Ansible Security Automation to be more productive, adapt to the growing demand of the modern IT landscape, ensure consistency in their IT environments, and respond to security incidents faster.



- Ansible Security Automation
  - Supported set of Ansible modules, roles and playbooks designed to unify the security response to cyberattacks in a new way
  - **Orchestrating** the activity of multiple classes of security solutions that wouldn't normally integrate with each other.
  - **Be the "Automation Glue" between disjoint technologies** and solutions targeting SecOps workflows
- Currently in Tech Preview:
  - <u>https://galaxy.ansible.com/ansible\_security</u>





# USE CASES

- Detection and Triage of suspicious activities
  - For example, Ansible can automatically enable logging or increase the log verbosity across enterprise firewalls and IDS to enrich the alerts received by a SIEM for an easier triage.
- Threat Hunting
  - For example, Ansible can automatically create new IDS rules to investigate the origin of a firewall rule violation, and whitelist those IP addresses recognized as non threats.
- Incident Response
  - For example, Ansible can automatically validate a threat by verifying an IDS rule, trigger a remediation from the SIEM solution, and create new enterprise firewall rules to blacklist the source of an attack.

# WHO IS IT FOR?

Ansible Security Automation extends the Ansible agentless, modular and easy to use enterprise automation platform to support the following industry constituencies:

- End-user organizations' security teams in charge of Security Operations Centres (SOCs)
- Managed security service providers (MSSPs) responsible for the governance of thousands of enterprise security solutions across their whole customer base
- Security ISVs offering security orchestration and automation (SOAR) solutions currently using custom-made automation frameworks



**#ANSIBLE**FEST ATLANTA **2019** 



ANSIBLE

## QUESTIONS?



#### THANK YOU



linkedin.com/company/Red-Hat



youtube.com/user/RedHatVideos





facebook.com/RedHatinc

maxamillion
 maxamillion



Senior Principal Software Engineer Ansible Engineering

Adam Miller