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
- 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
WHY SECURITY AUTOMATION?
WHY SECURITY AUTOMATION?

“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)."

MICHAEL CALLAHAN, AWAKE SECURITY
WHY SECURITY AUTOMATION?

“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)
WHY SECURITY AUTOMATION?

“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)
WHY SECURITY AUTOMATION?

“63% of respondents say their leaders understand that automaton, 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**
- Human readable automation
- No special coding skills needed
- Tasks executed in order
- Get productive quickly

**POWERFUL**
- Gather Information and Audit
- Configuration and System State management
- Workflow orchestration
- Manage ALL IT infrastructure

**AGENTLESS**
- 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.

<table>
<thead>
<tr>
<th>Rank</th>
<th>Repository</th>
<th>Contributors</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Microsoft/vscode</td>
<td>19k</td>
</tr>
<tr>
<td>2</td>
<td>facebook/react-native</td>
<td>10k</td>
</tr>
<tr>
<td>3</td>
<td>tensorflow/tensorflow</td>
<td>9.3k</td>
</tr>
<tr>
<td>4</td>
<td>angular/angular-cli</td>
<td>8.8k</td>
</tr>
<tr>
<td>5</td>
<td>MicrosoftDocs/azure-docs</td>
<td>7.8k</td>
</tr>
<tr>
<td>6</td>
<td>angular/angular</td>
<td>7.6k</td>
</tr>
<tr>
<td>7</td>
<td>ansible/ansible</td>
<td>7.5k</td>
</tr>
<tr>
<td>8</td>
<td>kubernetes/kubernetes</td>
<td>6.5k</td>
</tr>
<tr>
<td>9</td>
<td>npm/npm</td>
<td>6.1k</td>
</tr>
<tr>
<td>10</td>
<td>DefinitelyTyped/DefinitelyTyped</td>
<td>6.0k</td>
</tr>
</tbody>
</table>

96 Million+ Projects

[Octoverse 2018](https://github.com) - GitHub
ANSIBLE IS NOT ZERO SUM

(the list goes on and on)
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)
Ansible roles that **SECURE** your...

- Systems
- Servers
- Networks
- Cloud
- Desktops
- Middleware
ANSIBLE LOCKDOWN

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

- Official Subproject of Ansible done in partnership with MindPoint Group
  - https://github.com/ansible/ansible-lockdown
- Community focused mailing list
  - https://groups.google.com/forum/#!forum/ansible-lockdown
- 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
**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
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
```

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

Fix Text: Configure an ACL or filter to restrict management access to the device from only 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
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'"
INTERNAL STANDARDS

Chapter 8, Subsection 5: Login Standards:

- Change privileged passwords every 60 Days

```yaml
- 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) }}"
```

#redhat #rhsummit
REMEDIATION
**REMEDIAION**

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

```yaml
- 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 Migrations
  ○ Shell Shock Verify Vulnerability 1
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
  - Scans
  - Audits
  - Provides remediation recommendations/instructions
  - Defacto-standard in opensource/Linux land
  - [https://www.open-scap.org/](https://www.open-scap.org/)

- OpenSCAP + Ansible
  - OpenSCAP can audit and generate Ansible Playbooks for remediation
Red Hat Insights assesses your Red Hat Enterprise Linux environment to help you proactively identify and remediate threats, avoiding outages and unplanned downtime.
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
Recommended action
Increase CPU and/or memory reservation

Stability
Filesystem has exceeded 95% capacity
Recommended action
Increase free space on the host.
Red Hat Insights Compliance
Built on OpenSCAP reporting

**Assess and monitor** the degree/level of compliance to a policy for Red Hat products with operational ease

**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
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

- 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:
  - [https://galaxy.ansible.com/ansible_security](https://galaxy.ansible.com/ansible_security)
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
QUESTIONS?
THANK YOU

Adam Miller
Senior Principal Software Engineer
Ansible Engineering

maxamillion
@TheMaxamillion

linkedin.com/company/Red-Hat
youtube.com/user/RedHatVideos
facebook.com/RedHatInc
twitter.com/RedHat