Implementing a secure hybrid cloud using security and compliance automation

Lucy Kerner
Director, Security Global Strategy and Evangelism
Red Hat

Justin Lacey
Solutions Architect
Red Hat
“" Fully deploying security automation can reduce the average cost of a breach by 95%, but only 16% of organizations have done so.

The average security team typically examines less than 5% of alerts.

Source:
“”

The Bad Guys use Automation

Fight Fire with Fire

---

Forrester

Sources:
Reduce Risk and Improve Security Through Infrastructure Automation (Forrester, June 2018)
How Automation Solves Today’s Security Challenges

- Speed
- Reduce Human Errors
- Consistency
Automation for Improved Security and Compliance

- Bake Security into Dev & Ops
- Infrastructure, Security, and Compliance as Code = Repeatable, Shareable, Verifiable
- Continuous Monitoring
  Automated Response to Alerts
  Automated Controlled Remediations
Implementing Consistent Automation Strategy Across Organization

Infrastructure

Applications

Security Operations
Common automation language across the organization

From development... ANSIBLE PLAYBOOK ...to production.

DEV/TEST  Q/A  OPERATIONS  CHANGE MANAGEMENT  SECURITY

#securitysymposium
# Common Automation Language For Hybrid Cloud

<table>
<thead>
<tr>
<th>Traditional code development &amp; deployment tooling</th>
<th>CI/CD Pipelines &amp; Code Repositories</th>
</tr>
</thead>
<tbody>
<tr>
<td>Databases</td>
<td>Application Lifecycle Management</td>
</tr>
<tr>
<td>Middleware</td>
<td>Kubernetes Container Orchestration Platforms</td>
</tr>
<tr>
<td>VMs</td>
<td>OS</td>
</tr>
<tr>
<td>Bare metal</td>
<td>Network and storage infrastructure</td>
</tr>
<tr>
<td>OS</td>
<td>X-cloud Portability &amp; Integrations</td>
</tr>
<tr>
<td>SaaS/PaaS</td>
<td>Private Clouds</td>
</tr>
</tbody>
</table>

- Service catalogs & governance
- Full stack monitoring
- Root cause Analytics
- Capacity Optimization
- Cloud Financial Mgt
- Security & Compliance
- Config & Provision
- Patch & Remediate
- ITSM & CMDB Integration

Red Hat

#securitysymposium
Automation Enables Holistic DevSecOps

It’s not just about the application CI/CD pipeline!

Application pipeline:
- Write App Code
- Build App
- Unit Test
- Package App
- Deploy App

Supply chain:
- Images & artifacts

Development:
- Write Infa Code
- Build Images
- Validate Infra
- Automate Infra
- Deploy Infra

Test environments:
- Automate Infra

Production:
- Deploy Infra

Deployment infrastructure pipeline

#securitysymposium
**Why Ansible?**

**Simple**
- Human readable automation
- No special coding skills needed
- Tasks executed in order
- Usable by every team
- Get productive quickly

**Powerful**
- App deployment
- Configuration management
- Workflow orchestration
- Network automation
- Orchestrate the app lifecycle

**Agentless**
- Agentless architecture
- Uses OpenSSH & WinRM
- No agents to exploit or update
- Get started immediately
- More efficient & more secure
Ansible for Security and Compliance

Issue Detection
Issue Resolution
Operation Knowledge
Cost to Implement

#securitysymposium
What Is Ansible Automation Platform?

Ansible Automation Platform is Red Hat’s enterprise automation platform to automate the provisioning and configuration of modern enterprise IT environments, from compute resources, like VMs and containers, to networks, all the way to the application layer.
Ansible Collections

module > azure_rm_securitygroup

Manage Azure network security groups

Synopsis
- Parameters
- Notes
- Examples
- Return Values

Synopsis
- Create, update or delete a network security group.
- A security group contains Access Control List (ACL) rules that allow or deny network traffic to subnets or individual network interfaces.
- A security group is created with a set of default security rules and an empty set of security rules.
- Shape traffic flow by adding rules to the empty set of security rules.

Requirements
- python >= 2.7
- azure >= 2.0.0
Security and Compliance Automation for Infrastructure Operations
Automated Security & Compliance for Infrastructure Operations

DevSecOps in Baby Steps: Starting with securing Infrastructure Operations

Vulnerability & Compliance scanning

Host hardening

Enforcing automated compliance

Automated Patching of hosts

Automation & Analytics are the key to effective Security & Compliance

More details here: https://red.ht/securitylabs
Full Stack Patch Automation

**Build**
- Build Inventory List
- Build Integration with Monitoring, Change Control, and Notifications
- Build Application Automation

**Test**
- Test Playbooks
- Test Integration
- Test App Automation

**Resolve**
- Update Inventory based on Tests
- Reduce Manual Touch
- Increase Efficiency and Reduce Downtime

Updated host
Example: Networking

Scenario:
F5 load balancer management interface needs to comply with corporate security standards.
Example:
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 metal servers AFTER they have been already built

```yaml
- name: add security groups
  group:
    name: "{{ item.name }}"
    gid: "{{ item.gid }}"
  loop:
    - { name: 'secdev', gid: 5002 }
    - { name: 'appdev', gid: 5003 }
    - { name: 'auditcomp', gid: 6000 }

- name: add security users
  user:
    name: "{{ item.name }}"
    uid: "{{ item.uid }}"
    group: "{{ item.group }}"
  loop:
    - { name: 'nessus', uid: 10001, group: 'secdev' }
    - { name: 'qualys', uid: 10002, group: 'auditcomp' }

- name: add authorized keys for security users
  authorized_key:
    user: "{{ item.name }}"
    state: present
    key: "{{ lookup('file', item.pub_key) }}"
  loop:
    - { name: 'nessus', pub_key: 'keys/nessus_id_rsa.pub' }
    - { name: 'qualys', pub_key: 'keys/qualys_id_rsa.pub' }
```
Example: Security agent install and config (Splunk)

Scenario:
How do you ensure that your Splunk Universal Forwarder is installed and configured properly to send all relevant logs for analysis?
Ansible Roles for Security Compliance Automation

RHEL Compliance to industry standard or custom security baselines

https://galaxy.ansible.com/RedHatOfficial

Ansible playbooks provided and supported by Red Hat

And easily editable for your agency’s needs

#securitysymposium
Automate the Validation of Your Baseline with OpenSCAP

- Create Ansible remediation playbooks directly from the scan results
- Run automatically, scheduled, or manually

Standards

Security Content Automation Protocol (SCAP) is a U.S. standard maintained by National Institute of Standards and Technology (NIST). The OpenSCAP project is a collection of open source tools for implementing and enforcing this standard, and has been awarded the SCAP 1.2 certification by NIST in 2014.
Example: Ansible remediation playbook created from OpenSCAP scan

```bash
# Inserts/replaces the rule in /etc/audit/audit.rules
#
name: Inserts/replaces the fchown rule in audit.rules when on x86_64
lineinfile:
  line: "-a always,exit -F arch=b64 -S fchown -F auid=>1000 -F auid!=unset -F key=perm_mod"
state: present
dest: /etc/audit/audit.rules
create: yes
when: audit_arch == 'b64' and (ansible_virtualization_role != "guest" or ansible_virtualization_type != "docker")
tags:
  - audit_rules_dac_modification_fchown
  - medium_severity
  - restrict_strategy
  - low_complexity
  - low_disruption
  - CCE-27356-5
  - NIST-800-53-AC-17(7)
  - NIST-800-53-AU-1(b)
  - NIST-800-53-AU-2(a)
  - NIST-800-53-AU-2(c)
  - NIST-800-53-AU-2(d)
  - NIST-800-53-AU-12(a)
  - NIST-800-53-AU-12(c)
  - NIST-800-53-IR-5
  - NIST-800-171-3.1.7
  - PCI-DSS-Req-18.5.5
  - CJIS-5.4.1.1
  - DISA-STIG-RHEL-07-038380
```
Security and Compliance Automation for Application Development

#securitysymposium
Secure Application Lifecycle Management with Ansible

DevSecOps with Ansible

- Cucumber
- Arquillian
- JUnit

AUTOMATED QUALITY

Trusted Repositories

- Sonarqube
- Sonatype
- Fortify
- Twistlock
- Blackduck

- Synopsys
- Aqua

CCB
RAPID ATO

CM CS
sysdig
StackRox

PROD

#securitysymposium
Security and Compliance Automation for Security Operations
Automating Security Operations with Ansible

### Investigation Enrichment
Enabling programmatic access to log configurations such as destination, verbosity, etc.

### Threat Hunting
Automating alerts, correlation searches and signature manipulation

### Incident Response
Creating new security policies to whitelist, blacklist or quarantine a machine
## Ansible automates technologies you use

Time to automate is measured in minutes, 50+ **certified** platforms

<table>
<thead>
<tr>
<th>Cloud</th>
<th>Virt &amp; Container</th>
<th>Windows</th>
<th>Network</th>
<th>Security</th>
<th>Monitoring</th>
</tr>
</thead>
<tbody>
<tr>
<td>AWS</td>
<td>Docker</td>
<td>ACLs</td>
<td>Arista</td>
<td>Checkpoint</td>
<td>Dynatrace</td>
</tr>
<tr>
<td>Azure</td>
<td>Kubernetes</td>
<td>Files</td>
<td>Aruba</td>
<td>Cisco</td>
<td>Datadog</td>
</tr>
<tr>
<td>Digital Ocean</td>
<td>OpenStack</td>
<td>Packages</td>
<td>Bigswitch</td>
<td>CyberArk</td>
<td>LogicMonitor</td>
</tr>
<tr>
<td>Google</td>
<td>OpenShift</td>
<td>IIS</td>
<td>Cisco</td>
<td>F5</td>
<td>New Relic</td>
</tr>
<tr>
<td></td>
<td>VMware</td>
<td>Registry</td>
<td>Ericsson</td>
<td>FRR</td>
<td></td>
</tr>
<tr>
<td></td>
<td>+more</td>
<td>Shares</td>
<td></td>
<td>Juniper</td>
<td></td>
</tr>
<tr>
<td>AWS</td>
<td>Docker</td>
<td>Services</td>
<td></td>
<td>Meraki</td>
<td></td>
</tr>
<tr>
<td>AWS</td>
<td>Kubernetes</td>
<td>Configs</td>
<td>FRR</td>
<td>OpenSwitch</td>
<td></td>
</tr>
<tr>
<td>AWS</td>
<td>OpenStack</td>
<td>Users</td>
<td>Juniper</td>
<td>Ruckus</td>
<td>Dynatrace</td>
</tr>
<tr>
<td>AWS</td>
<td>OpenShift</td>
<td>Domains</td>
<td></td>
<td>VyOS</td>
<td>Datadog</td>
</tr>
<tr>
<td>AWS</td>
<td>VMware</td>
<td>Updates</td>
<td></td>
<td>+more</td>
<td>LogicMonitor</td>
</tr>
<tr>
<td>AWS</td>
<td>+more</td>
<td></td>
<td></td>
<td></td>
<td>New Relic</td>
</tr>
</tbody>
</table>

### Red Hat Products
- **RHEL**
- **Satellite Insights**
- **Pure Storage**
- **Infinidat**
- **Netapp**
- **Pure Storage**
- **+more**

### Devops
- **Jira**
- **GitHub**
- **Vagrant**
- **Jenkins**
- **Slack**
- **+more**

#securitysymposium
Consistent Automation Strategy Across Organization

Infrastructure

Applications

Security Operations

Questions? Email us!

lkerner@redhat.com

jlacey@redhat.com
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.