Enhancing Secrets Management in Ansible with CyberArk Application Identity Manager
TODAY’S PRESENTERS:

Chris Smith
Moderator
DevOps Product Marketing, CyberArk

Naama Schwartzblat
Application Identity Manager
Senior Product Manager
CyberArk

Kyle Benson
Global Alliance Architect,
Red Hat
TODAY’S IT ARCHITECTURES are continually changing and must be infinitely flexible.
IT OPERATIONS BEARS THE BURDEN

CEO
LINE OF BUSINESS
DEVELOPERS
IT OPERATIONS
EFFECTIVE MANAGEMENT & AUTOMATION MUST SPAN CLOUD, CONTAINERS AND TRADITIONAL I.T.

<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>Kubernetes Container Orchestration Platforms</td>
</tr>
<tr>
<td>Middleware</td>
<td>Container packaging platforms</td>
</tr>
<tr>
<td>Bare metal</td>
<td></td>
</tr>
<tr>
<td>OS</td>
<td></td>
</tr>
<tr>
<td>Network and storage infrastructure</td>
<td></td>
</tr>
<tr>
<td>X-cloud Portability &amp; Integrations</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SaaS/PaaS</th>
<th>Private Clouds</th>
<th>AWS</th>
<th>Azure</th>
<th>Google</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>IT Automation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service catalogs &amp; governance</td>
</tr>
<tr>
<td>Full stack monitoring</td>
</tr>
<tr>
<td>Root cause Analytics</td>
</tr>
<tr>
<td>Capacity Optimization</td>
</tr>
<tr>
<td>Cloud Financial Mgt</td>
</tr>
<tr>
<td>Security &amp; Compliance</td>
</tr>
<tr>
<td>Config &amp; Provision</td>
</tr>
<tr>
<td>Patch &amp; Remediate Hosts</td>
</tr>
<tr>
<td>ITSM &amp; CMDB Integration</td>
</tr>
</tbody>
</table>
WHAT IS ANSIBLE AUTOMATION?

The Ansible project is an open source community sponsored by Red Hat. It’s also a **simple automation language** that perfectly describes IT application environments in **Ansible Playbooks**.

**Ansible Engine** is a **supported product** built from the Ansible community project.

Ansible Tower is an **enterprise framework** for controlling, securing, managing and extending your Ansible automation (community or engine) with a UI and RESTful API.
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
SHARING IS CARING

Modular approaches help teams respect each others’ standards of operations.

SCM is key to spreading Ansible best practices and helping cross-train newcomers to the Orchestration table.
HOW TO DETERMINE WHAT ANSIBLE CAN DO FOR YOU
PROBLEM SOLVING STARTS WITH TRIAGE, NOT TOOLS

- What am I doing?
- Who is involved?
- How does this scale or grow?
- What is the plan for ongoing management?
- Is there built-in capability to my tools, or am I creating something from scratch?
Ansible solves the problem of automating and orchestrating.

Does not address bigger picture security/compliance.

Tower spotlights security considerations and provides predictability.

Role-based access control and secure credential storage.

API integrations, accountability and execution history.
SECURITY CONSIDERATIONS
Only respects security in place at host user level

No abstraction of remote host or cloud credentials from user

No guarantee of execution parameters or integrity of playbook as designed by the team

Creates an isolated runtime environment to control execution of Ansible

Abstracts security credentials and specifics (ssh keys, username+passwords, etc.) from end user

 Guarantees execution parameters and execution is as designed for the playbook
Multiple Inventories may be needed
- Network automation may not need to have app/cache/db hosts in their inventory
- Multiple Cloud Dynamic Sources will overwrite each other

Things that “just work” for CLI may need consideration in Tower
- Execution isolation means config files at ~/.* need to be placed for AWX user in Tower
- PRoot isolates Tower runs to project/Playbook directory (can’t write to /tmp locally, etc.)

SCM is to your advantage:
- Playbook projects for different teams/orgs can utilize forks, branch tags
- Roles don’t need one monolithic repository
UTILIZE OUR PARTNERSHIPS

CyberArk
Integrate with Enterprise Credential Management

Splunk
Get your logs out of Ansible Tower and making meaningful decisions at scale

GitHub & Atlassian
Use your existing source control tools to manage your infrastructure like code
BUT..... DEVOPS PIPELINES MAY NOT BE FULLY SECURED

Cyberark Advanced Threat Landscape - 2018 Report, indicated:

- 75% organizations do not have a privileged account security strategy for DevOps
- Fewer than half report that DevOps and security teams consistently work together
- Nearly all (99%) of security pros and DevOps respondents failed to identify all places where privileged accounts or secrets exist
DEVOPS EXPANDS THE SECURITY CHALLENGES

Must Protect The Pipeline!

- Unwatched environment
- Massive Amounts of Corporate IP
- POWERFUL Credentials
- Accessed, changed and modified by people and code constantly!
Islands Of Security In Access Management Create Challenges

Native tool solutions for secrets: Create “Security Islands”

- Provide a specific and different solution for each tool
- Not built with security in mind -- Secret repository only
  - No rotation of secrets
  - No audit
- Have limited integration capabilities
- No central view of Privileged Account Security
TYPICAL CHALLENGES OF THE CI/CD TOOLS

• Unmanaged and distributed secrets and credentials
• Usually Master server needs super user privileges to gain access to many secrets
• Security islands: duplicate secrets management for different platforms
• Lack of audit
• Lack of compliance visibility
• Lack of Segregation of Duty
Global Energy Company

Requirements/Solution

• Enable Ansible to checkout credentials from CyberArk Enterprise Vault via Application Identity Manager (AIM)

• Execute an automation task in Ansible using the checked-out credentials

• Limit and control use of checked-out credentials within Ansible
Eliminates embedded application credentials for improved security and compliance
SECRET MANAGEMENT WITH CYBERARK CREDENTIAL PROVIDER (CP)

Key Feature:
- Strong authentication
- Local cache
- Full audit
- Secret rotation

Authentication:
- IP/DNS/Hostname
- OS User
- App Path
- App Hash

Resiliency:
- Agent based
1. Automatic Secure Credential Retrieval
2. No Security islands - secrets are managed centrally in the Vault
3. Enable Secret rotation
4. Auditability
Whenever Ansible Requires Privileged Credentials:

1. Standard python ‘lookup’ executed from within Playbook

2. Lookup utilizes AIM CLIPasswordSDK to communicate with Credential Provider installed on Ansible Control Node to retrieve credentials

3. Credentials stored in variables and used throughout playbook to access assets, APIs, configure systems, install applications, etc.
• CyberArk AIM module for Ansible has been approved by the community and is merged into the core Ansible product

• Ansible v.2.4 shipped in mid-Sept 2017 includes the AIM integration.

Add a CyberArk password lookup plug in – allows retrieval of credentials from vault
SECURE THE CONFIGURATION MANAGEMENT TOOL WITH CYBERARK

Critical steps for securing your CI/CD Tools

❖ Secure Master / Playbook by removing the hard coded/unmanaged credentials from the jobs and retrieving them in a secure way using Application Identity Manager

❖ Secure the managed Nodes by establishing an identity during orchestration to be used for secrets retrieval in a secure way using Conjur

❖ Protect the tool console by monitor and record any Interactive Access with Privileged Session Manager

❖ Secure the tool credentials by managing and rotating them based on policies using Central Policy Manager

❖ Auto discover hidden hard coded credentials in the tool Playbooks, Roles, Tasks by using DNA

Leverage the CyberArk PAS suite to secure across the full environment
SECURE ANSIBLE WITH CYBERARK-CONJUR

- Secrets managed by CyberArk and Conjur are delivered securely to Ansible hosts
- Least privilege enforced on Ansible hosts
- Security Teams enabled to bring best practices to Ansible and meet compliance requirements
- Removes the need to duplicate Secrets Management functionality across multiple platforms.
- Audit privileged activity on Ansible hosts
DNA: INTEGRATION WITH ANSIBLE AUTOMATES DISCOVERY

• Automates discovery of hidden credentials in Ansible (Playbooks, Roles, Tasks) by using CyberArk Discovery & Audit

• Customer Value
  • Improves security and reduces risk for CI/CD pipeline by automating discovery
  • Gives CISO a powerful tool to help discover and understand the risks of hidden credentials in DevOps environments
  • Helps customers drive additional value from existing CyberArk solutions
**Key Takeaways**

- Use CyberArk – Ansible plugin to secure your Ansible playbook

**Where to Start**

- Visit [https://galaxy.ansible.com/cyberark-bizdev/](https://galaxy.ansible.com/cyberark-bizdev/)
- Download AIM lookup plugin from [https://galaxy.ansible.com/cyberark-bizdev/password_lookup_plugin/](https://galaxy.ansible.com/cyberark-bizdev/password_lookup_plugin/)
- CyberArk Conjur - Free and Open Source version of Conjur is available at [conjur.org](http://conjur.org).
- Visit us at [www.cyberark.com/conjur](http://www.cyberark.com/conjur)
  
  Audit capabilities are available only in [Conjur Enterprise](http://Conjur Enterprise).
- CyberArk Conjur Ansible Role & Lookup Plug-in are available on [GitHub](http://GitHub) and [Ansible Galaxy](http://Ansible Galaxy).
- Use CyberArk DNA to identify hidden credentials in Ansible
GET STARTED

Learn more about Ansible:
ansible.com/it-automation

Download an Ansible Tower trial:
ansible.com/tower-trial
Q&A