RISE OF THE MACHINES: DEVOPS AND THE ROLE OF SECRETS MANAGEMENT

Elizabeth Lawler
Vice President, DevOps Security
CyberArk
@ElizabethLawler
@CyberArk
Code Delivery = Revenue Growth

Companies with faster code delivery were 62% more likely to see YoY revenue growth of 25% or more.

BUT

51% of security pros say there is no relationship between IT security and business innovation

75% of organizations don’t have a privileged account security strategy in place for DevOps

50% don’t have a privileged account security strategy in place for Cloud

Sources: F5 “The Evolving Role of CISOs and the Importance to the Business”
CyberArk “2018 Threat Landscape Report”
PROTECT THE PIPELINE

“Unmanned” Environment

Powerful Rights

Accessed, Changed, and Modified by People and Code Constantly

Massive Amounts of Corporate IP
The New Norm: Customer And Industry Realities

- More Infrastructure
- More Applications
- More Privileged Actors
- More Automation
The Expanded Attack Surface

- More Infrastructure
- More Applications
- More Privileged Actors
- More Automation
- More Privileged Security Risk

IT Admins, End Users, Privileged Business Users, SaaS Admins, DevOps Teams
Security Islands: Different Locations & Rules

Islands of Security

- Puppet Hiera
- Ansible Vault
- Chef Databags
- DockerSecrets
- Kubernetes Secrets
- AWS IAM / KMS
- Microsoft Azure IAM/KMS / KMS
- Google Cloud IAM / KMS
- OpenShift Secrets

PRIVILEGED ACCESS MANAGEMENT

AD/LDAP
Managing Secrets in One Flow

1. Administer
2. Rotate
3. App Enrollment
4. Cluster Enrollment
5. Secret 0
6. Audit
7. Connect
Vault Cluster Architecture and Secret Rotation

Diagram showing the architecture and secret rotation process with labels for Reset, Administer, Rotate, App Enrollment, Cluster Enrollment, Secret 0, Audit, and Connect.
Application Enrollment Flow for Secrets Retrieval
“Secret 0”
Use the Right Size Vault for the Environment
The Maturity Level of Secrets Solutions

DevOps Vault Product Evolution Generations

- **"0th"** – No strong encryption, robust authentication, authorization or audit
- **1st** – Encryption, authentication, authorization, CLI management and REST API, single-site HA
- **2nd** – Add declarative policy, user interface, multi-site HA, integrations with 3rd party tools
- **3rd** – Add extensible authentication (delegation of "Secret-0" root of trust), and enrollment workflows to support separation of duties
- **4th** – Remove developers and code from the secrets workflows. Secure the "last mile" delivery of connectivity to applications
Securing DevOps Initiatives is a Team Sport
Simple Steps to Secure DevOps

1. Assess secrets and management approaches across cloud and DevOps environments.
2. Mitigate poorly secrets as basic DevOps hygiene.
3. Embed security with developers and DevOps teams to facilitate better secrets management practices.
4. Embrace security engineering and security automation.
THANK YOU

Elizabeth Lawler
Vice President, DevOps Security
CyberArk
@ElizabethLawler
@CyberArk
Rotate, Repave and Repair

Rotate datacenter credentials every few minutes or hours

Repave every server and application every few hours from a known good state

Repair vulnerabilities consistently within hours of patch availability

BUT there are always exceptions.
No one has every environment set fully on automate.
If it is fit for purpose, use it.