CASE STUDY

Enterprise Password Rotation

Customer Vertical

Independent Software Vendor (ISV)

Problem Background

Password rotation refers to the changing/resetting of a password(s). Limiting the lifespan of a password reduces the risk from and effectiveness of password-based attacks and exploits, by condensing the window of time during which a stolen password may be valid. Password rotation not only applies to user passwords, but the predominant issue is non-centralised managed passwords (local usernames / administrators, API passwords, appliance passwords, application administrator passwords etc.).

Problem Statement

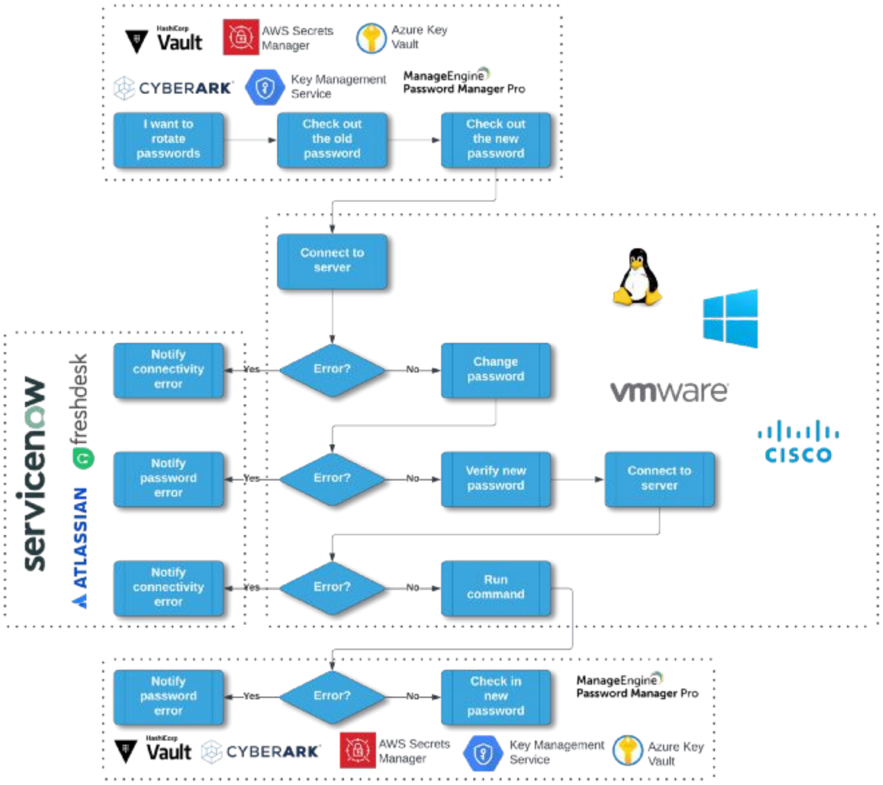
Prevent unauthorized access due to password rotation policies not consistently implemented across the IT environment.

Problem Impact

Data leakage has a financial impact (financial institutions can incur fines from regulatory bodies), reputational damage, legal action or loss of sensitive data.

Solution

Using **Direktiv** as a scheduler (initially), password rotation workflows for Linux, network infrastructure, VMware applications and APIs and storage infrastructure was created specifically. The password rotation policies were repeatable micro-workflows and would also create a new password in HashiCorp Vault, change the password on the target and then validate the changed password. If the validation checks were successful, the password would be stored in Vault. If not, an incident would be created in Servicenow.com and the old/new password combination is stored for troubleshooting. The password storage workflow was also later extended to support AWS Secrets Manager and CyberArk.



Business Outcome

Effort estimation savings 4 days FTE effort / month, guaranteed compliance of password rotation policies, error reduction in multi-technology password management.

Read more about Direktiv.io