CYBERARK®

HOW TO HANDLE "OFFICE SPACE" MOMENTS AND MOVE FORWARD WITH YOUR PAS PROGRAM

October 26, 2018 – Raleigh InfoSeCon

AGENDA

- Part 1: Building a business case for prioritizing PAS
- Part 2: Broadening your organization’s use of PAS across more parts of the organization
- Part 3: Turning PAS skeptics into advocates

MMMKAY YA…

WE NEED TO SECURE OUR PRIVILEGED ACCOUNTS

CASE STUDY:
BUILDING A BUSINESS CASE FOR PRIORITIZING PAS

FEDERAL GOVERNMENT SERVICE PROVIDER

- **COMPANY OVERVIEW**
  - Government, Trust, & Technology Services Group
  - Provide critical applications and services to customers
  - Require high levels of data protection and privacy to meet security mandates and regulations like NIST 800-171
- **CHALLENGES**
  - Existing solution was causing expensive outages
  - Applications failing, team members working nights & weekends to triage problems, costing. $160k / year in extraneous hours
  - Manual and disjoined workflows
  - Needed to invest in strong PAS platform, one that could grow with organization needs and scale to meet future use cases

CASE STUDY: **BUILDING A BUSINESS CASE FOR PRIORITIZING PAS**

FEDERAL GOVERNMENT SERVICE PROVIDER

- **SOLUTION**
  - Evaluated 7 privileged account security products
  - Overcame internal pushback with proof-of-concept and focused on finding solid, centralized solution that the team could rely on for the long term
  - Selected the CyberArk Core Privileged Access Security Solution
- **RESULTS**
  - Replaced unreliable PAS system
  - Quickly deployed and began vaulting and rotation of critical credentials to replace existing solution
  - Improved workflows across the organization
  - Taking advantage of PSM to combat insider threats
  - Expanding with AIM to secure Qualys, Ansible, AWS, and other critical apps
  - Other business units taking notice

WHAT’S NEXT?

- Secure software development lifecycle
- Automation with API to track certs
- Continuous improvements with health checks and DNA
- Insider Threat – Identifying critical accounts for session isolation
- Information and best practices sharing with CyberArk (sanitized)

WE NEED TO TALK ABOUT YOUR FLAIR

CASE STUDY

EXPANDING PAS ACROSS THE ORGANIZATION

- **COMPANY OVERVIEW**
  - Fortune 250 Financial Services Firm – banking, securities, asset management, mortgage, insurance
  - 2,000 branches across multiple domestic regions
  - Complex IT environment, segregated systems

- **CHALLENGES**
  - Initial project driver: Regulatory and audit requirements
  - # of users with privileged access seemed unbelievable
  - Needed to transform the management of privileged access
  - Needed to prioritize managing the riskiest accounts/users

PROGRAM GOALS & OBJECTIVES

1. **Reduce attack surface**
   - Reduce overall # of accounts
   - Secure, manage, and review these accounts
   - Rotate account credentials
2. **Reduce lateral movement**
   - Unique credentials per server in Platinum
   - Privileged credential separation (Administrative Tier Model)
3. **Enforce least privileged**
   - Entitle safes based on roles and business functions
4. **Prevent account hijacking**
   - Monitor and record session activity
   - Enforce multi factor authentication (via RSA)
   - Automatically rotate and cycle credentials

PROTECTION LEVELS

GOLD PROTECTION LEVEL FOR INDIVIDUAL ACCOUNTS

- Active directory and human access accounts
- Provide individual user accounts with access across various authorized servers
- Ability to identify who retrieved privileged account and when
- Rotate account credentials frequently (2 days on unix, 3 days on windows.)

PLATINUM PROTECTION LEVEL FOR SHARED ACCOUNTS

- Limit: small set of shared accounts for each function on Platinum host (e.g. App support, DB ops, Web Ops, OS ops etc.)
- Real time monitoring of activity on servers
- Audit logs produced, and securely stored
- Rotate account credentials (after each use)

BUILDING A STRATEGIC PROGRAM & PLANNING

- Program Support

“What project are we going to charge for this work?”

“What is your time-line for implementation? “

“How will we request access?”

  - Dedicated Project with Project Manager to help with rollout
  - Leverage internal communications resources to help with how-to guides, 1-page request process pdfs
  - Partner with your account team to see if Customer Success support is an option for what you are trying to accomplish
  - Leverage professional services to deepen the technical depth of your team at critical times like installs and upgrades

BUILDING A STRATEGIC PROGRAM & PLANNING

- Build Trust with Users

“Does that mean you’re going to manage ALL accounts on the servers?”

  - Fear that applications will stop working
  - Reduce scope if needed to target lower hanging fruit

“How is this going to impact ongoing build and operations?”

  - When using existing accounts, adding accounts to the vault will have no effect on entitlements.
  - If transitioning to new privileged overlap old and new access

  - Phased Approach & Steady Rollout = Better User Adoption

BUILDING A STRATEGIC PROGRAM & PLANNING

- Objectives and Priorities

“Why is this more important than the other things my team is working”

  - Tie benefits to Goals, for example educate on risks associates with lateral movement,
  - Gain management backing if you don’t already have it.
  - Identify “crown jewel” application hosts for most resource intensive access management.

- Operations and Management

“How are we going to be able to administer a user community of thousands with lean resources?”

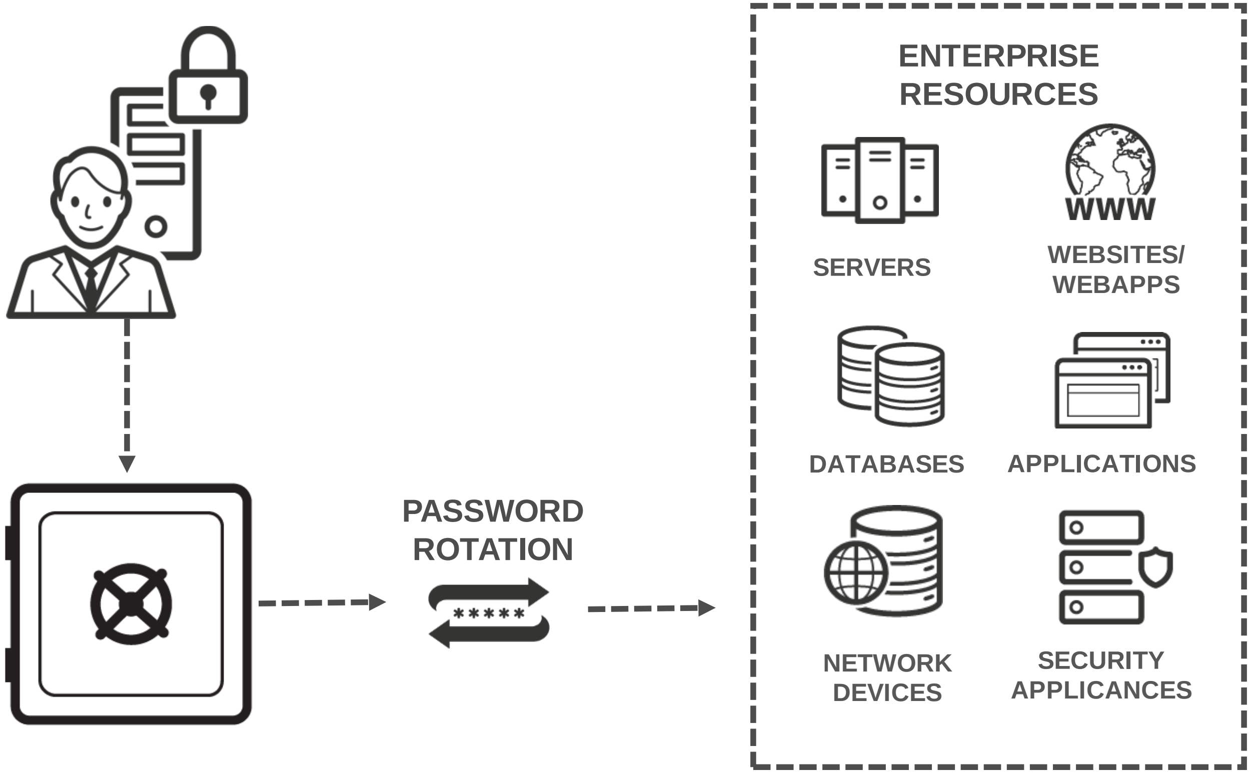
  - Streamline Onboarding with Automation
  - Leverage seed files from reliable sources (eg A.D. accounts lists)

```
Get-AdUser -Filter 'name -Like "*-Z"'
```

  - Automation yields uniform deployment

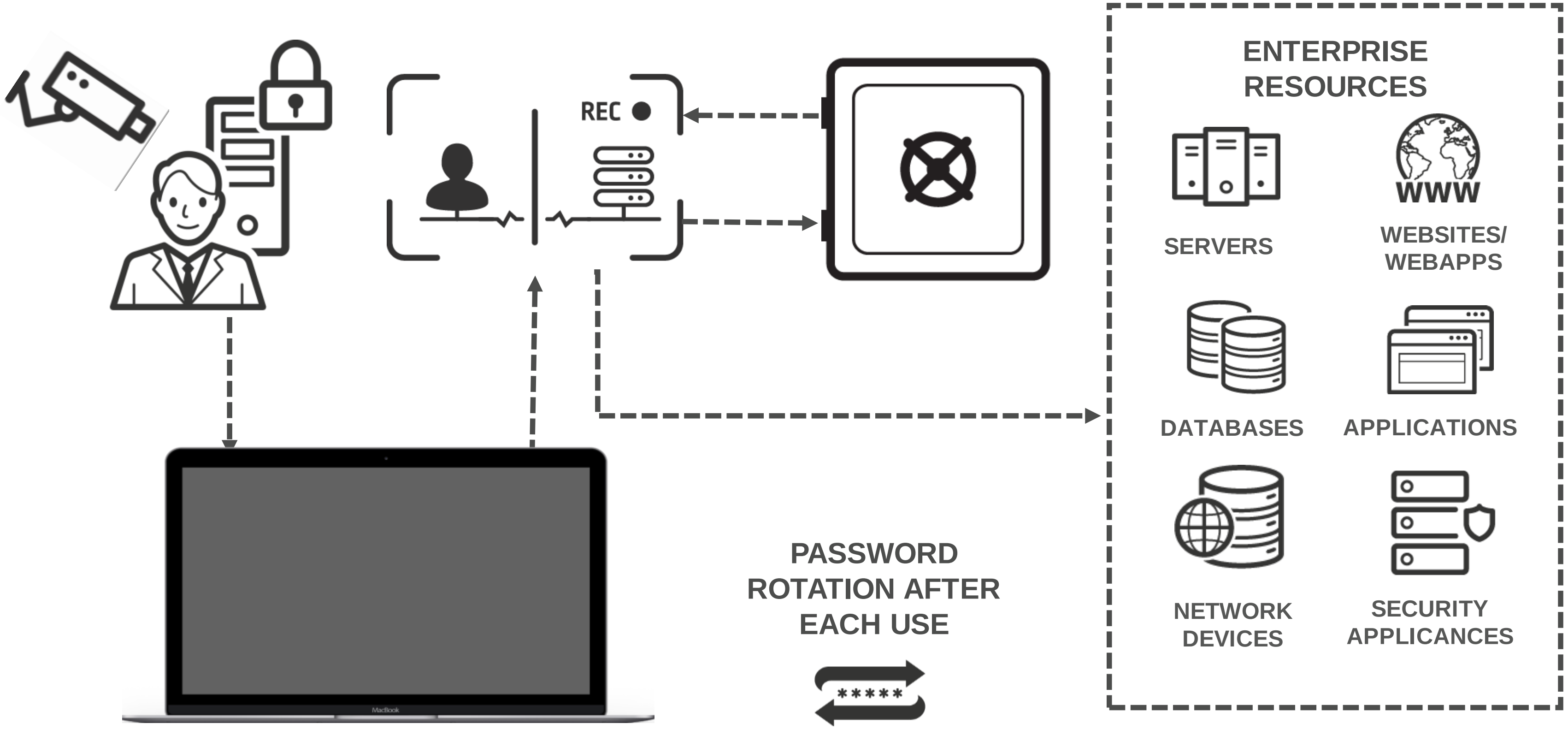
EXAMPLE: GOLD PROTECTION

- Admin user logs into CyberArk with individual privileged credentials to access a certain server
- User accesses target server from workstation (can copy and paste credentials from CyberArk)



EXAMPLE: PLATINUM PROTECTION

- Window Ops admin user logs into CyberArk, requests access to shared account for a server.
- System validates user permissions, and sends credential to target system – user cannot view/copy password.
- User access logged and session activity recorded.



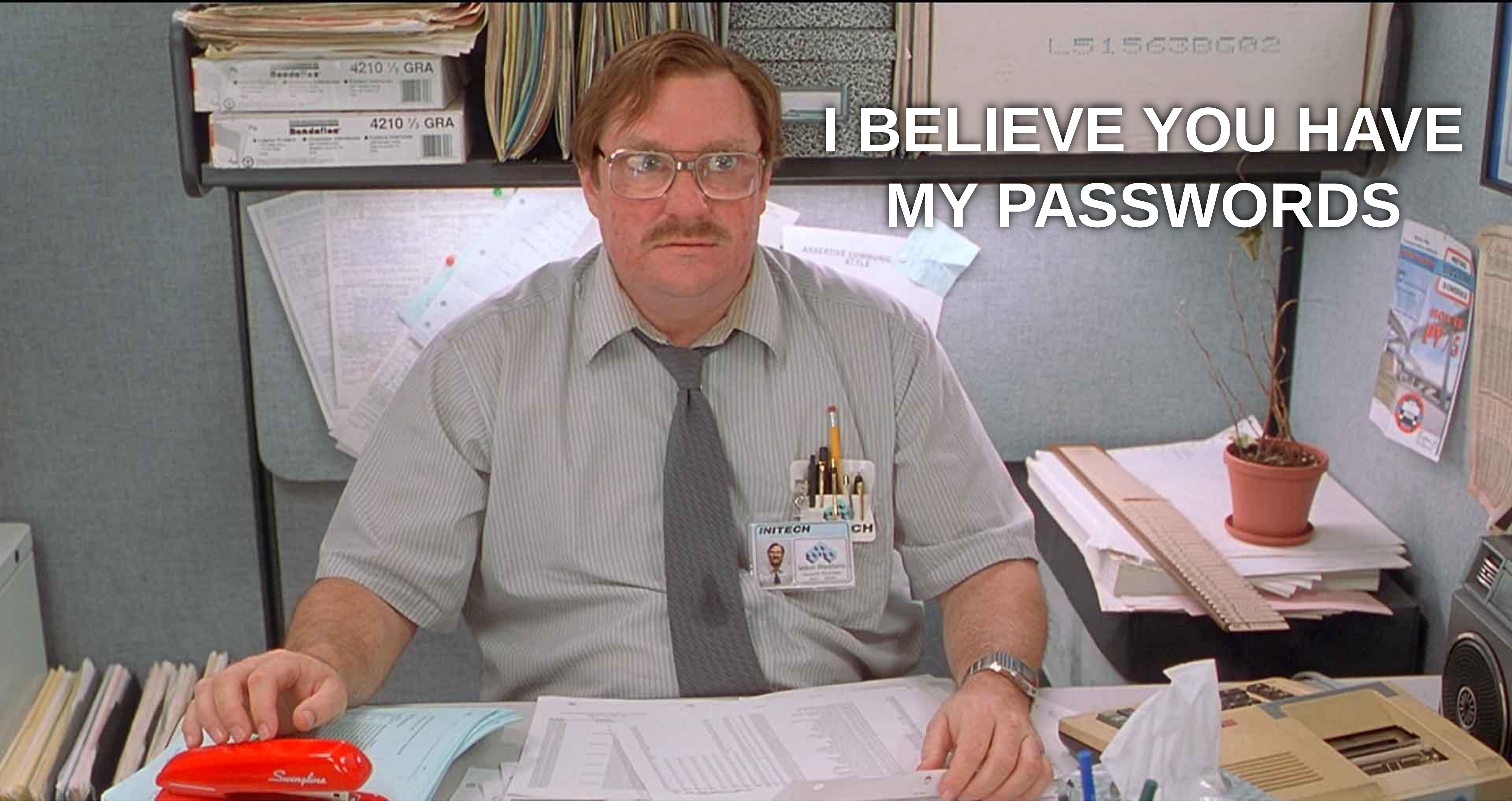
INITIAL RESULTS

- Reduced attack surface on Platinum servers
  - From hundreds of privileged users per server to ~10 per server
- Practically eliminated lateral movement to Platinum servers using server specific shared human accounts
- On boarded 1600 individual privileged human accounts, approximated 25% of the population of privileged users
  - Gold: Individual account onboarding
  - Platinum: Server specific shared human accounts

SUCCESS BASED EXPANSION

- Success based growth of Gold and Platinum account access
  - Gold expanding to 100% of Individual privileged accounts
  - Platinum server base growing 150%
  - Replicating core implementation to segmented network

  - Expanding to service accounts... many flavors so scoping carefully


I BELIEVE YOU HAVE MY PASSWORDS
4210 ½ GRA
4210 ½ GRA
INITECH
Swingline

TIPS FOR HANDLING PAS SKEPTICS

Change can be hard. Preconceived notions can be strong.

1. Practice your pitch – communicate a compelling PAS vision with confidence.
2. Listen to stakeholders – earn their trust, alleviate fears.
3. Ensure their needs are taken into consideration, while also demonstrating how the vision will equate to tangible benefits and improvements.

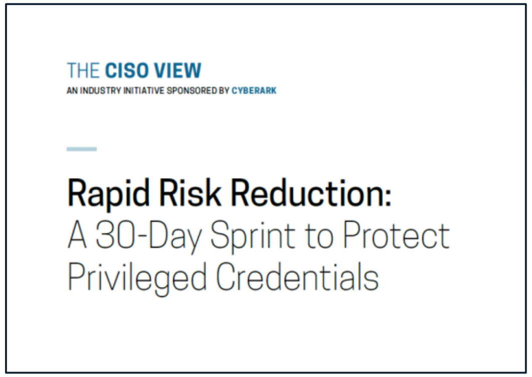
LEVERAGE TOOLS AND TRAINING RESOURCES

METHODOLOGIES & TOOLS

- 30 Day Sprint
- Hygiene Program
- PAS Maturity Assessment Tool
- Discover & Audit (DNA) Tool

CYBERARK WHITE PAPER

CYBERARK PRIVILEGED ACCOUNT SECURITY CYBER HYGIENE PROGRAM



THE CISO VIEW

AN INDUSTRY INITIATIVE SPONSORED BY CYBERARK

Rapid Risk Reduction: A 30-Day Sprint to Protect Privileged Credentials

TRAINING

- Variety of training options and certifications
- Free, online Introduction to PAS course
  - For any professionals who will be part of a CyberArk project (Project Managers, IT personnel, Network Engineers, etc.)

SUMMARY & NEXT STEPS

- Visit the CyberArk booth
- Scan your network with CyberArk DNA
- Free Online Training & Certification:
  - Introduction to CyberArk Privileged Account Security Course
  - Trustee Certification Exam
- And… visit the BB&T booth
  - explore career opportunities
  - pick up some swag!