CYBERARK®

# CUSTOMER FORUM BRUSSELS

CYBERARK®

# PRIVILEGED ACCOUNT SECURITY PROGRAM

# PAS HYGIENE PROGRAM GOALS

| | |
|---|---|
| **Step 1** | Focus first on eliminating irreversible network takeover attacks (e.g., Kerberos Golden Ticket). |
| **Step 2** | Control & secure well-known infrastructure accounts. |
| **Step 3** | Limit lateral movement. |
| **Step 4** | Protect 3rd party privileged accounts. |
| **Step 5** | Manage SSH keys on critical Unix servers. |
| **Step 6** | Defend cloud & DevOps processes accounts. |
| **Step 7** | Secure shared IDs for business users (integrate and accelerate adoption of MFA). |

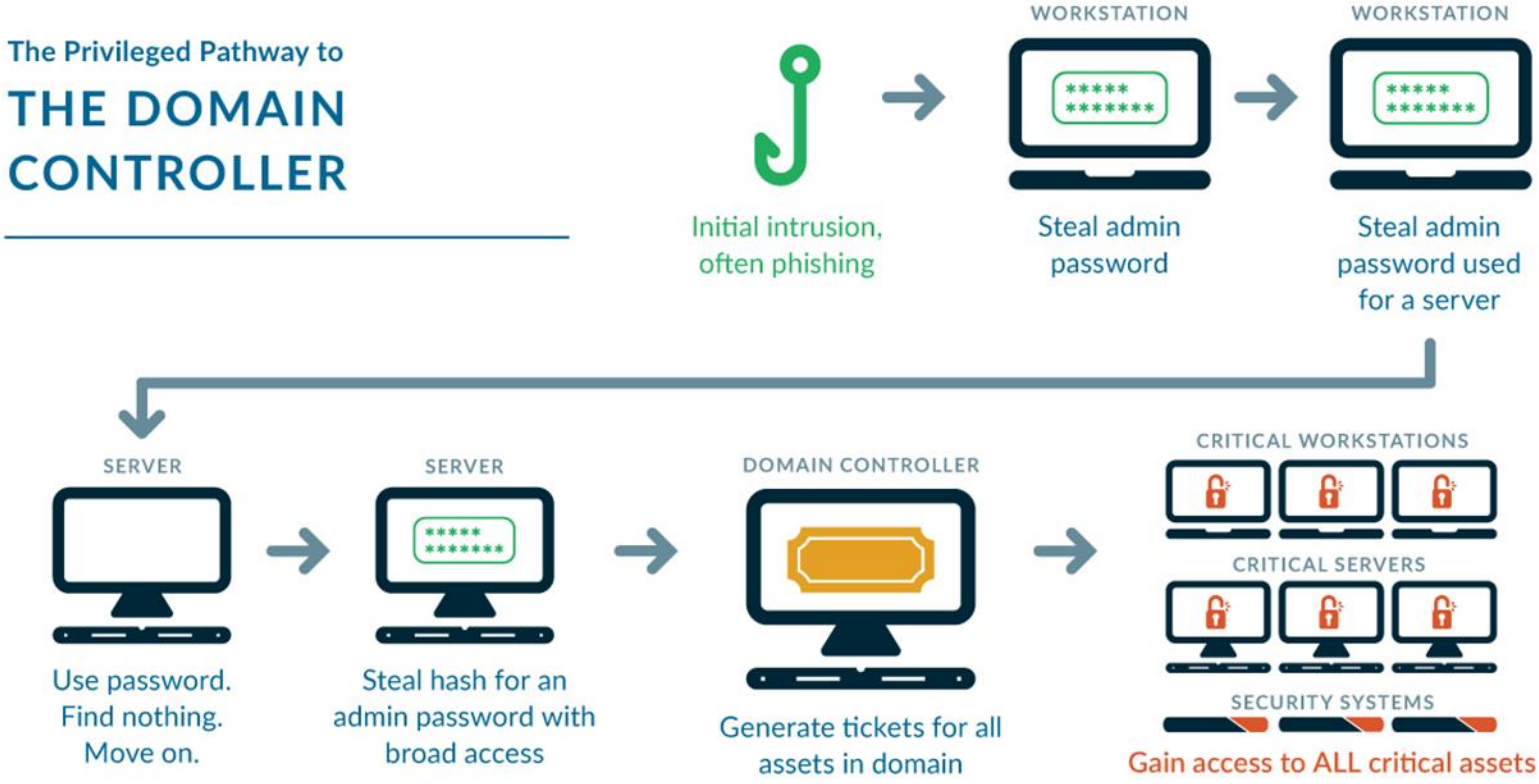
# IRREVERSIBLE NETWORK TAKEOVER ATTACKS

1

**ATTACKER'S MINDSET:**

Establish persistence in an organization by performing an attack that is not only hard to identify but also so intrusive that the business must rebuild to remove the attacker, e.g., a Kerberos attack such as a Golden ticket.

# GOLDEN TICKET ATTACK


The Privileged Pathway to
THE DOMAIN CONTROLLER
Initial intrusion, often phishing
WORKSTATION
*****
*******
Steal admin password
WORKSTATION
*****
*******
Steal admin password used for a server
SERVER
Use password. Find nothing. Move on.
SERVER
*****
*******
Steal hash for an admin password with broad access
DOMAIN CONTROLLER
Generate tickets for all assets in domain
CRITICAL WORKSTATIONS
CRITICAL SERVERS
SECURITY SYSTEMS
Gain access to ALL critical assets

# FUNDAMENTAL CONCEPTS

- **Separate Admin account for admin tasks**
- **Privileged Access Workstations (PAWs)**
- **Unique Local Admin Passwords for Workstations**
- **Unique Local Admin Passwords for Servers**
- **Time-bound privileges (no permanent administrators)**
- **Multi-factor for time-bound elevation**
- **Just Enough Admin (JEA) for DC Maintenance**
- **Attack Detection**

https://technet.microsoft.com/en-us/library/mt631194(v=ws.11).aspx

1

# IRREVERSIBLE NETWORK TAKEOVER ATTACKS

## PRESENT STATE

- Single factor Authentication for Domain Admins.
- Privileged credentials found on all machines in the network.
- Kerberos attacks on Domain Controller are not identified and blocked in progress.

## FUTURE STATE

- All privileged access to tier0 & tier1 is Isolated, and requires MFA.
- No hash residuals by design.
- Infrastructure account creation on tier0 is blocked.

## PATHWAY TO FUTURE STATE

- Allow CyberArk access only with MFA.
- Protect domain controllers and other valuable assets with PSM.
- Protect credential theft using EPM.
- Detect Kerberos attacks at real-time using PTA.

**PRIVILEGED SESSION MANAGER**

**PRIVILEGED THREAT ANALYTICS**

**ENDPOINT PRIVILEGE MANAGER**

# CONTROL & SECURE INFRASTRUCTURE AND ENDPOINT WELL-KNOWN INFRASTRUCTURE ACCOUNTS

## ATTACKER’S MINDSET:

Take ownership of an entire technology stack by compromising a single infrastructure account, and use the same credentials on similar assets.

2

# CONTROL & SECURE INFRASTRUCTURE AND ENDPOINT WELL-KNOWN INFRASTRUCTURE ACCOUNTS

## PRESENT STATE

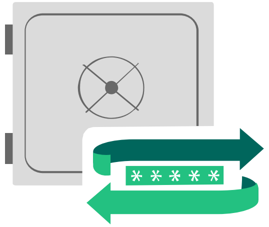
- Windows Servers: **some** Local Admins are Vaulted.
- Unix Servers: **some** root are Vaulted.
- Cisco: **some** enable are Vaulted.
- SQL Server: **some** sa are Vaulted.
- Oracle: **some** SYS & SYSTEM are Vaulted.

## FUTURE STATE

- Get to 100% managed accounts.

## PATHWAY TO FUTURE STATE

- Vault all well-known infrastructure accounts.
- Automatically rotate passwords periodically and after every use.



ENTERPRISE PASSWORD VAULT

3

# LIMIT LATERAL MOVEMENT

## ATTACKER’S MINDSET:

Stealing credentials and moving laterally to IT Windows workstation in order to steal elevated permissions.

3

# LIMIT LATERAL MOVEMENT

**PRESENT STATE**

- **Some** IT Windows workstations contain local admin rights for end point users.
- Credentials, such as hashes, allowing privileged access to Tier0 are found on **some** Tier1&2 machines.

**FUTURE STATE**

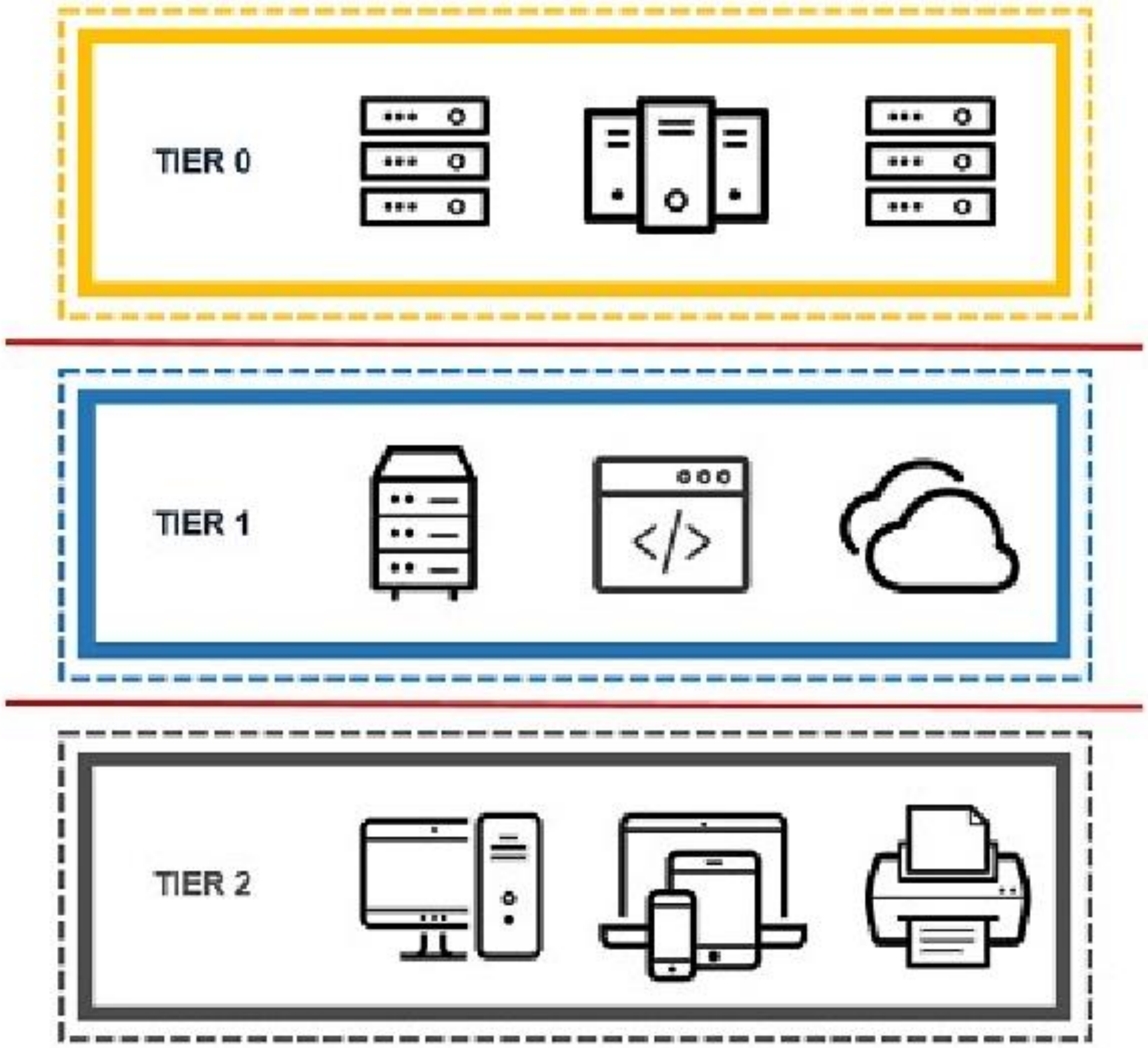
- Completely remove all end point users from the local admins group on IT Windows workstations.
- Network built in a tired module.

**PATHWAY TO FUTURE STATE**

- EPM IT Windows workstations in order to remove local admin rights, and to stop credential theft

**ENDPOINT PRIVILEGE MANAGER**

# TIER MODEL



# PROTECT 3RD PARTY PRIVILEGED APPLICATION ACCOUNTS

4

**ATTACKER’S MINDSET:**

Compromise 3rd party solutions that are used to perform operations such as deep scans, in order to steal the privileged credentials they are using.

# PROTECT 3RD PARTY PRIVILEGED APPLICATION ACCOUNTS

4

## PRESENT STATE

- Security solutions such as vulnerability scanners and inventory management products require highly privileged accounts with broad access to  the environment to perform operations.
- **Some** scan engines privileged accounts are Vaulted.
- **Some** inventory management privileged accounts are Vaulted.
- **Some** WebLogic/WebSphere/Tomcat/JBoss database passwords are Vaulted.

## FUTURE STATE

- **All** scan engines privileged accounts are Vaulted
- **All** inventory management privileged accounts are Vaulted
- **All** WebLogic/WebSphere/Tomcat/JBoss database passwords are Vaulted
- **All** of the above accounts are automatically changing after every usage

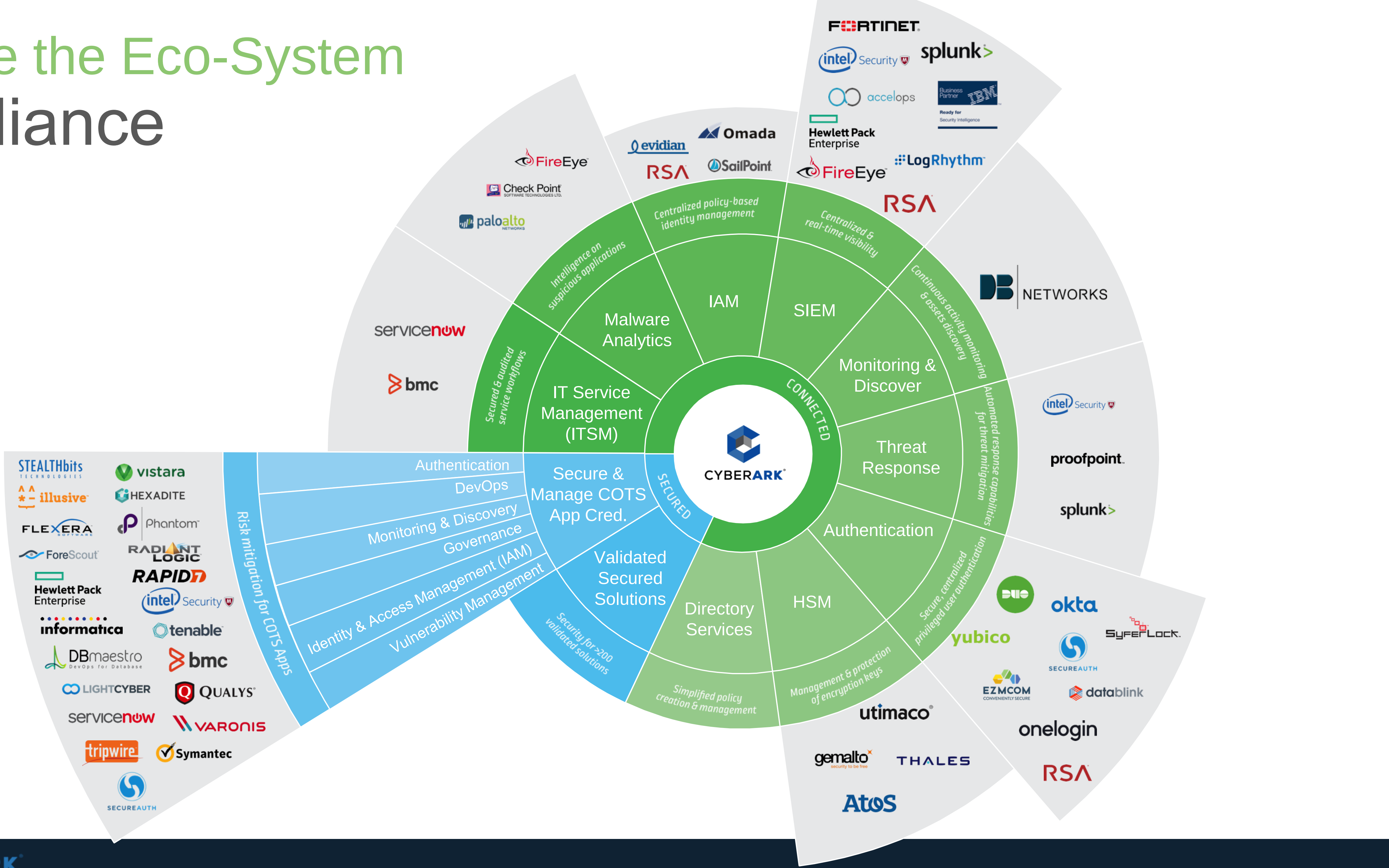
## PATHWAY TO FUTURE STATE

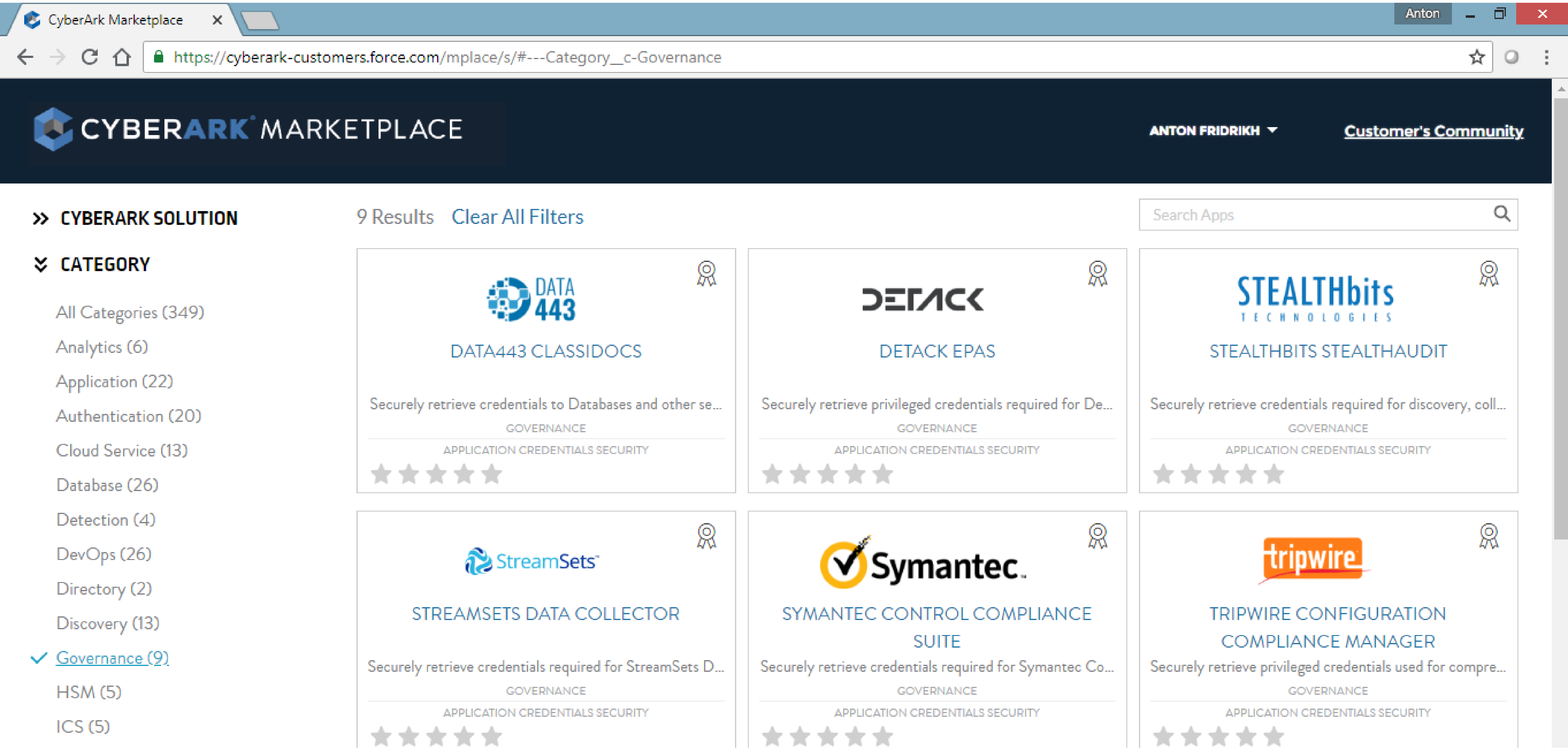
- Remove hard coded passwords on scan engines, inventory management agents & application servers with AIM (Application Identity Manager)

APPLICATION IDENTITY MANAGER

# Secure the Eco-System

## C3 Alliance


CYBERARK
CONNECTED
SECURED
IAM
Centralized policy-based identity management
Evidian
Omada
RSA
SailPoint
SIEM
Centralized & real-time visibility
FORTINET
intel Security
splunk
accelops
IBM Business Partner Ready for Security Intelligence
Hewlett Packard Enterprise
LogRhythm
FireEye
RSA
Monitoring & Discover
Continuous activity monitoring & assets discovery
DB NETWORKS
Threat Response
Automated response capabilities for threat mitigation
intel Security
proofpoint
splunk
Authentication
Secure, centralized privileged user authentication
DUO
okta
yubico
SyferLock
SECUREAUTH
EZMCOM
datablink
onelogin
RSA
HSM
Management & protection of encryption keys
utimaco
gemalto
THALES
Atos
Directory Services
Simplified policy creation & management
Validated Secured Solutions
Security for >200 validated solutions
Secure & Manage COTS App Cred.
Risk mitigation for COTS Apps
Authentication
DevOps
Monitoring & Discovery
Governance
Identity & Access Management (IAM)
Vulnerability Management
STEALTHbits TECHNOLOGIES
vistara
illusive
HEXADITE
FLEXERA SOFTWARE
Phantom
ForeScout
RADIANT LOGIC
Hewlett Packard Enterprise
RAPID7
intel Security
informatica
tenable
DBmaestro DevOps for Database
bmc
LIGHTCYBER
QUALYS
servicenow
VARONIS
tripwire
Symantec
SECUREAUTH
IT Service Management (ITSM)
Secured & audited service workflows
servicenow
bmc
Malware Analytics
Intelligence on suspicious applications
FireEye
Check Point SOFTWARE TECHNOLOGIES LTD.
paloalto NETWORKS



» CYBERARK SOLUTION

CATEGORY

- All Categories (349)
- Analytics (6)
- Application (22)
- Authentication (20)
- Cloud Service (13)
- Database (26)
- Detection (4)
- DevOps (26)
- Directory (2)
- Discovery (13)
- ✓ Governance (9)
- HSM (5)
- ICS (5)

9 Results Clear All Filters

DATA443 CLASSIDOCS
Securely retrieve credentials to Databases and other se...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

DETACK EPAS
Securely retrieve privileged credentials required for De...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

STEALTHBITS STEALTHAUDIT
Securely retrieve credentials required for discovery, coll...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

STREAMSETS DATA COLLECTOR
Securely retrieve credentials required for StreamSets D...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

SYMANTEC CONTROL COMPLIANCE SUITE
Securely retrieve credentials required for Symantec Co...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

TRIPWIRE CONFIGURATION COMPLIANCE MANAGER
Securely retrieve privileged credentials used for compre...
GOVERNANCE
APPLICATION CREDENTIALS SECURITY
☆☆☆☆☆

# MANAGE SSH KEYS ON CRITICAL UNIX SERVERS

**ATTACKER’S MINDSET:**

Leverage unmanaged SSH keys, in order to login with root access, and takeover the Unix technology stack.

5

# MANAGE SSH KEYS ON CRITICAL UNIX SERVERS

**PRESENT STATE**

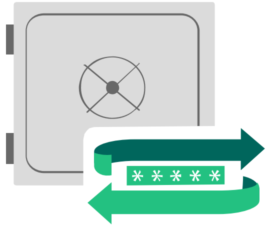
- Unmanaged SSH key-pairs found on **some** Unix production servers.

**FUTURE STATE**

- All SSH key-pairs on Unix production servers are Vaulted and rotated on a routine basis.

**PATHWAY TO FUTURE STATE**

- EPV SSH key-pairs on Unix production servers, and associate with SSH Key Manager policies.



**ENTERPRISE PASSWORD VAULT**

# DEFEND CLOUD & DEVOPS PROCESSES ACCOUNTS

## ATTACKER’S MINDSET:

Compromise high privileged API keys, embedded in code and CI/CD tools, in order to takeover the entire cloud environment.

6

# DEFEND CLOUD & DEVOPS PROCESSES ACCOUNTS

**PRESENT STATE**

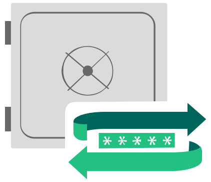
- AWS root accounts and API keys are not Vaulted.
- Ansible, Jenkins and other tools credentials are embedded in free text.
- DevOps secret are stored hard-coded in playbooks and configuration files.

**FUTURE STATE**

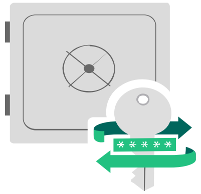
- AWS root accounts, keys and API keys are Vaulted and automatically rotated.
- Ansible, Jenkins and other tools credentials are secured in the Vault, retrieved on the fly, and automatically rotated.
- DevOps secrets are stored securely, access controlled, managed and monitored.

**PATHWAY TO FUTURE STATE**

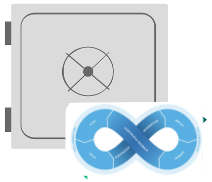
- EPV AWS root accounts, keys and API keys.
- AIM embedded credentials in CI/CD tools.
- Conjur DevOps secrets management.



**ENTERPRISE PASSWORD VAULT**



**APPLICATION IDENTITY MANAGER**



**Conjur**

# SECURE SAAS SHARED IDS FOR BUSINESS USERS

## ATTACKER’S MINDSET:

Steal credentials which are shared amongst business users, in order to get high level access into sensitive systems.

# SECURE SAAS SHARED IDS FOR BUSINESS USERS

7

## PRESENT STATE

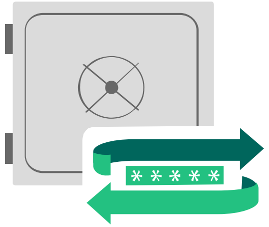
- Several high privileged IDs to Workday and financial institution websites are shared amongst business users at the finance department.
- Several high privileged IDs to BambooHR are shared amongst business users at the HR department.
- The above IDs are shared.  Hence, authentication does not utilize MFA.

## FUTURE STATE

- All access to shared IDs is Isolated, and requires MFA.

## PATHWAY TO FUTURE STATE

- Allow access to CyberArk only with MFA.
- Protect all shared IDs with PSM.

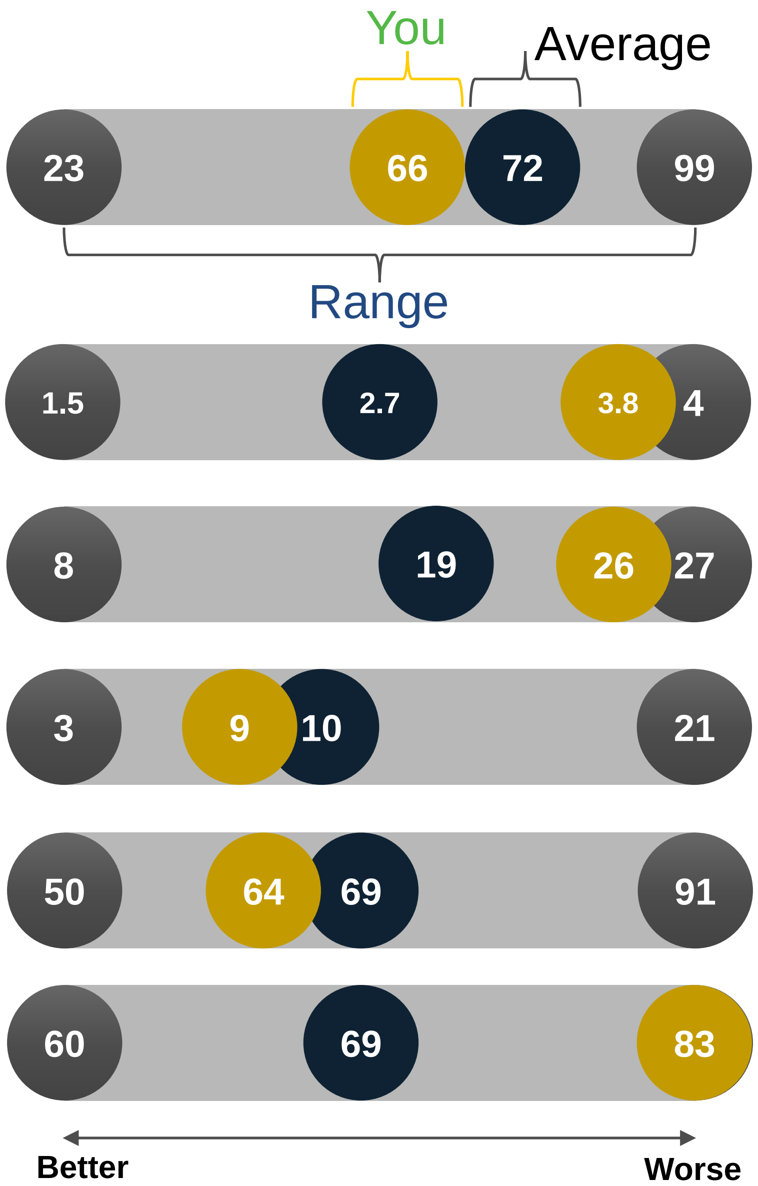


ENTERPRISE PASSWORD VAULT

# PAS HYGIENE PROGRAM GOALS

| Metrics for Success | How to Get There | Current State | Desired State |
|---|---|---|---|
| Measure progress | Periodic infrastructure scan to discover unprotected backdoors. | DNA scans are not performed systematically. | DNA scans are performed once a month.<br>PAS Assessment tool |
| Test and prove effectiveness against real world attacks | Periodic Red Team attack simulations. | Red Team simulations are not performed systematically. | CyberArk Red Team performs attack simulation post roll-out to verify effectiveness of controls. |
| Develop knowledge | Accelerate adoption by utilizing CyberArk expertise:<br>• Develop CyberArk certified workforce.<br>• Staff augmentation to accelerate program and knowledge transfer. | **SOME** vault SMEs are certified. | **ALL** vault SMEs are CyberArk certified. |

# ASSESS MATURITY, MEASURE SUCCESS



% of Local Admins Expired

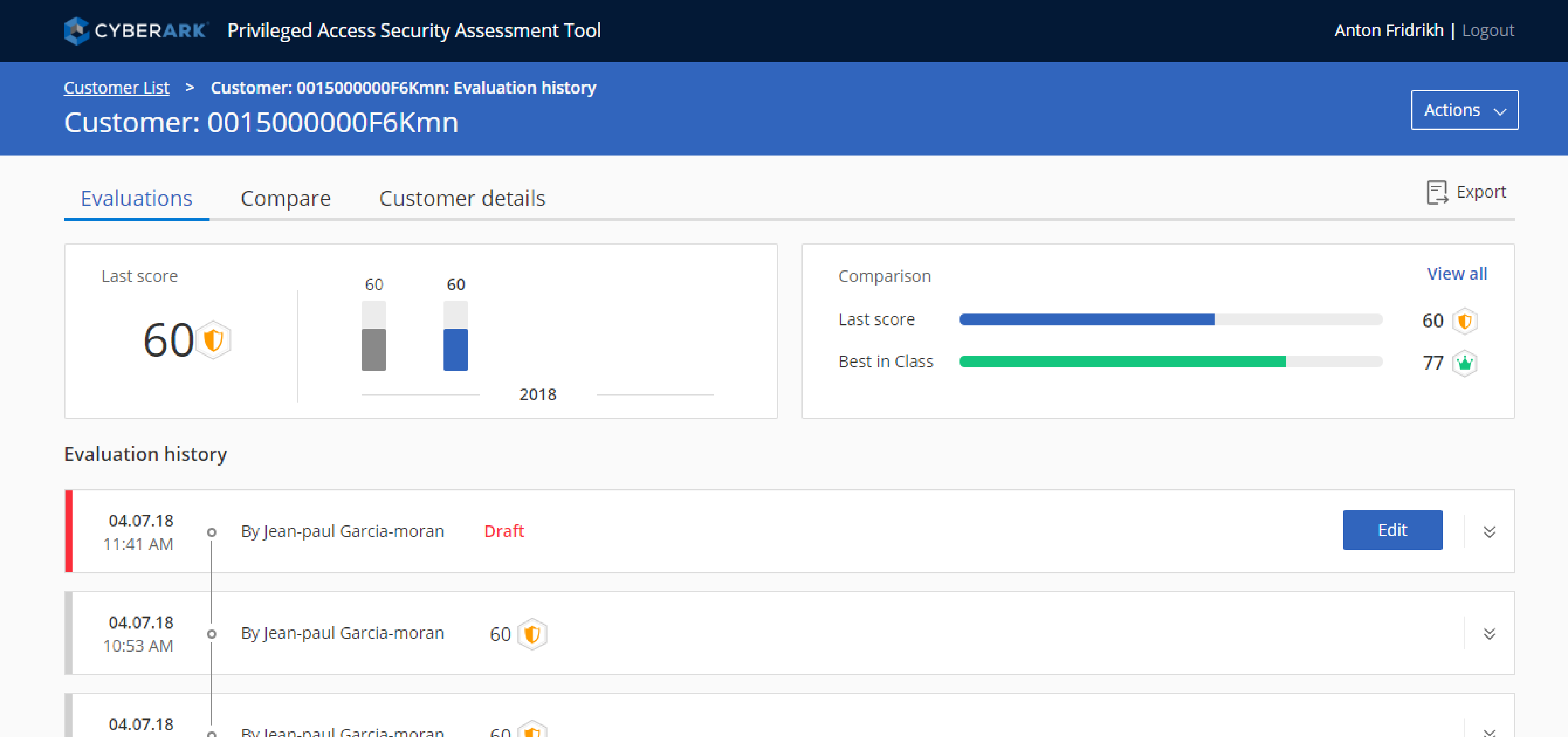
Average Local Admin Age (Years)

% of Privileged Domain IDs Expired

% of Privileged Domain IDs w/Access to >50% of scanned network

% of Service Accounts w/Admin Rights

% of Privileged Service Accounts Expired


CYBERARK
Privileged Access Security Assessment Tool
Anton Fridrikh | Logout
Customer List > Customer: 0015000000F6Kmn: Evaluation history
Actions
Evaluations
Compare
Customer details
Export
View all
2018
Edit

Customer: 0015000000F6Kmn

Last score

60

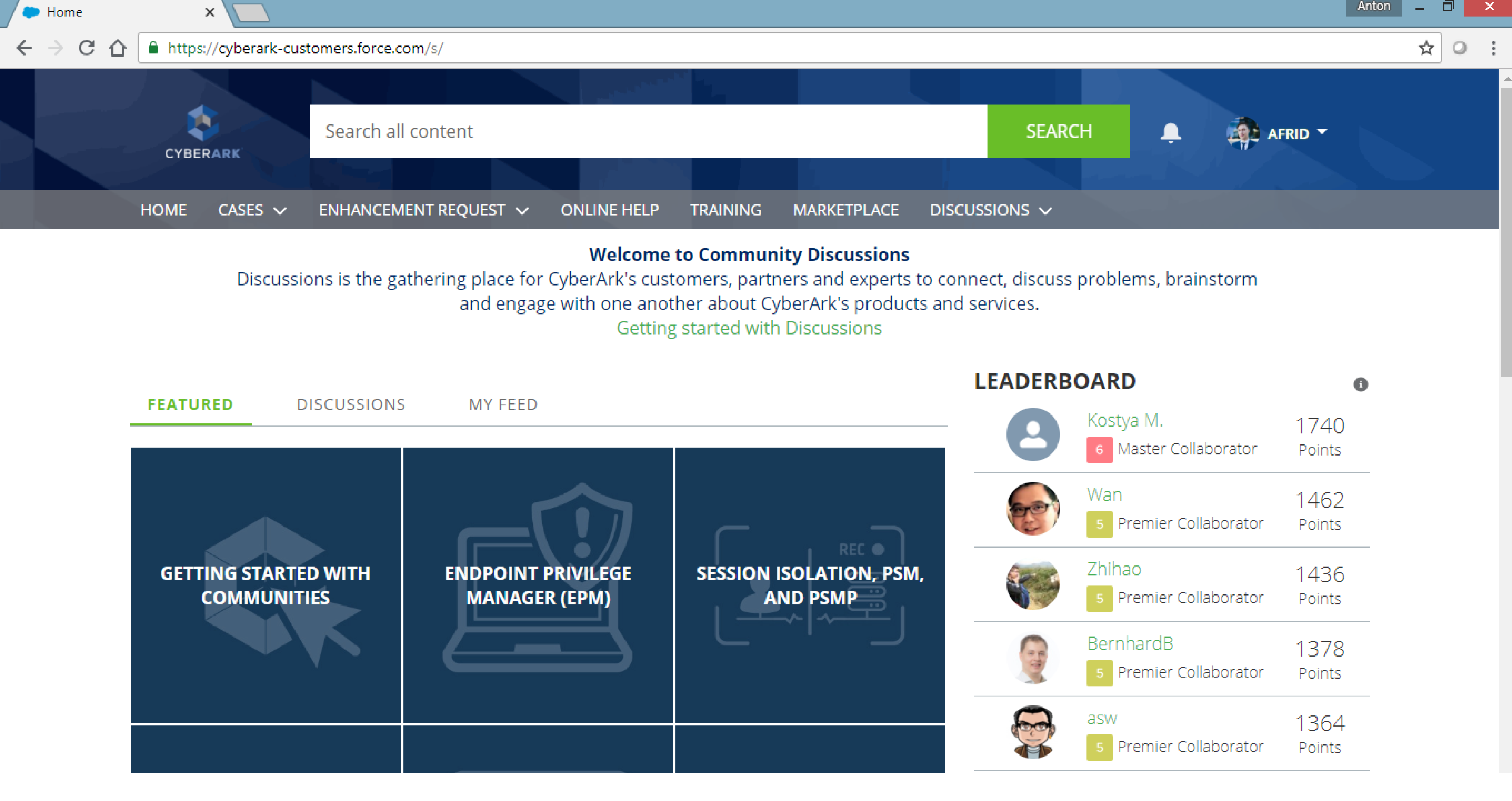
| | |
|---|---|
| 60 | 60 |

Comparison

| | |
|---|---|
| Last score | 60 |
| Best in Class | 77 |

Evaluation history

| | | |
|---|---|---|
| 04.07.18<br>11:41 AM | By Jean-paul Garcia-moran | Draft |
| 04.07.18<br>10:53 AM | By Jean-paul Garcia-moran | 60 |
| 04.07.18 | By Jean-paul Garcia-moran | 60 |



**Welcome to Community Discussions**

Discussions is the gathering place for CyberArk's customers, partners and experts to connect, discuss problems, brainstorm and engage with one another about CyberArk's products and services.

Getting started with Discussions

**LEADERBOARD**

| | | | |
|---|---|---|---|
| Kostya M. | 6 | Master Collaborator | 1740 Points |
| Wan | 5 | Premier Collaborator | 1462 Points |
| Zhihao | 5 | Premier Collaborator | 1436 Points |
| BernhardB | 5 | Premier Collaborator | 1378 Points |
| asw | 5 | Premier Collaborator | 1364 Points |

# THANK YOU