CYBERARK®
The Identity Security Company™

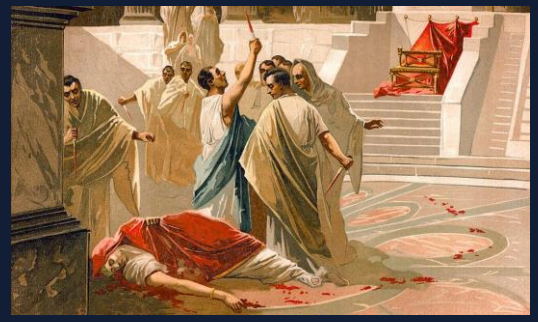
bako tech®

Evolution of Identity Security in the era of new Cyber Threats

Bartosz Kryński

Luke Przybylski

First trojan horse ~1200 B.C.



Assassination of Julius Ceasar 15.03.44 B.C.

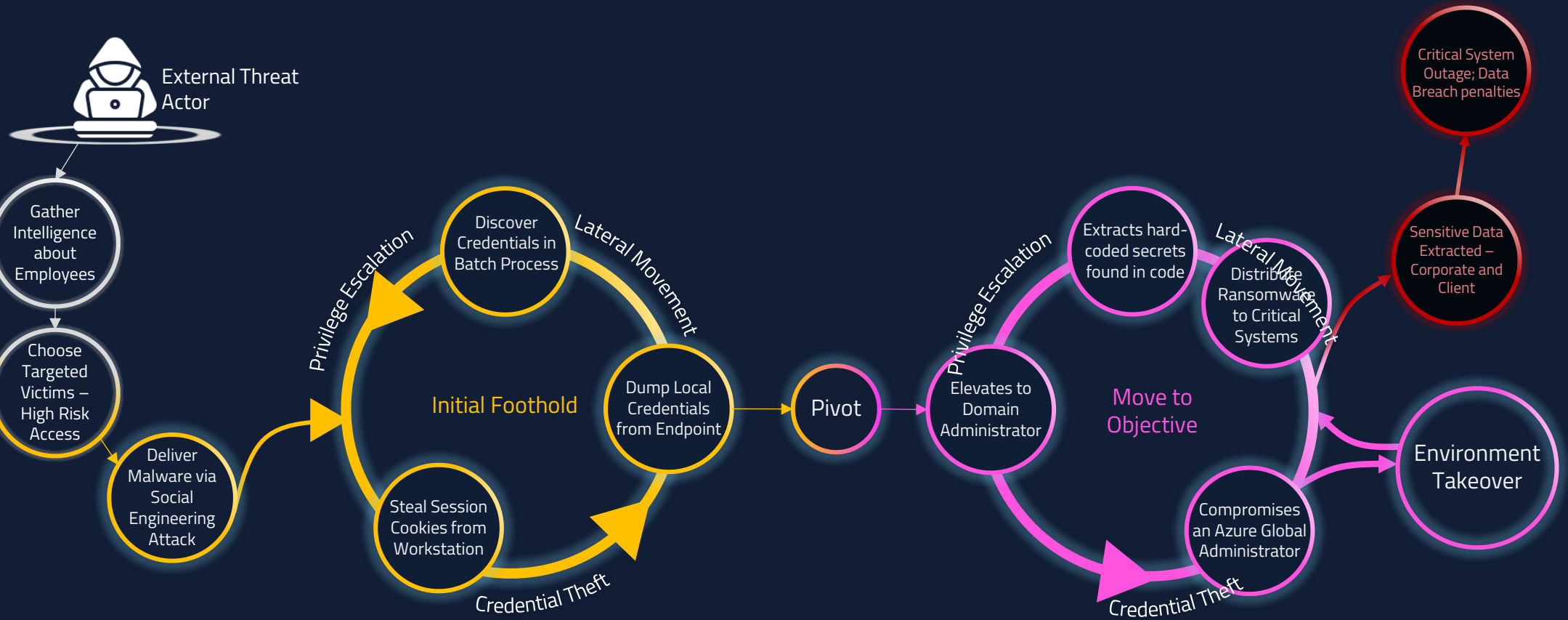
The Fall of Constantinople 1453 A.D.

Battle of the Bulge „Operation Grief" December 1944 A.D.

CYBERARK®

Recent Identity Security attacks

Attack chain

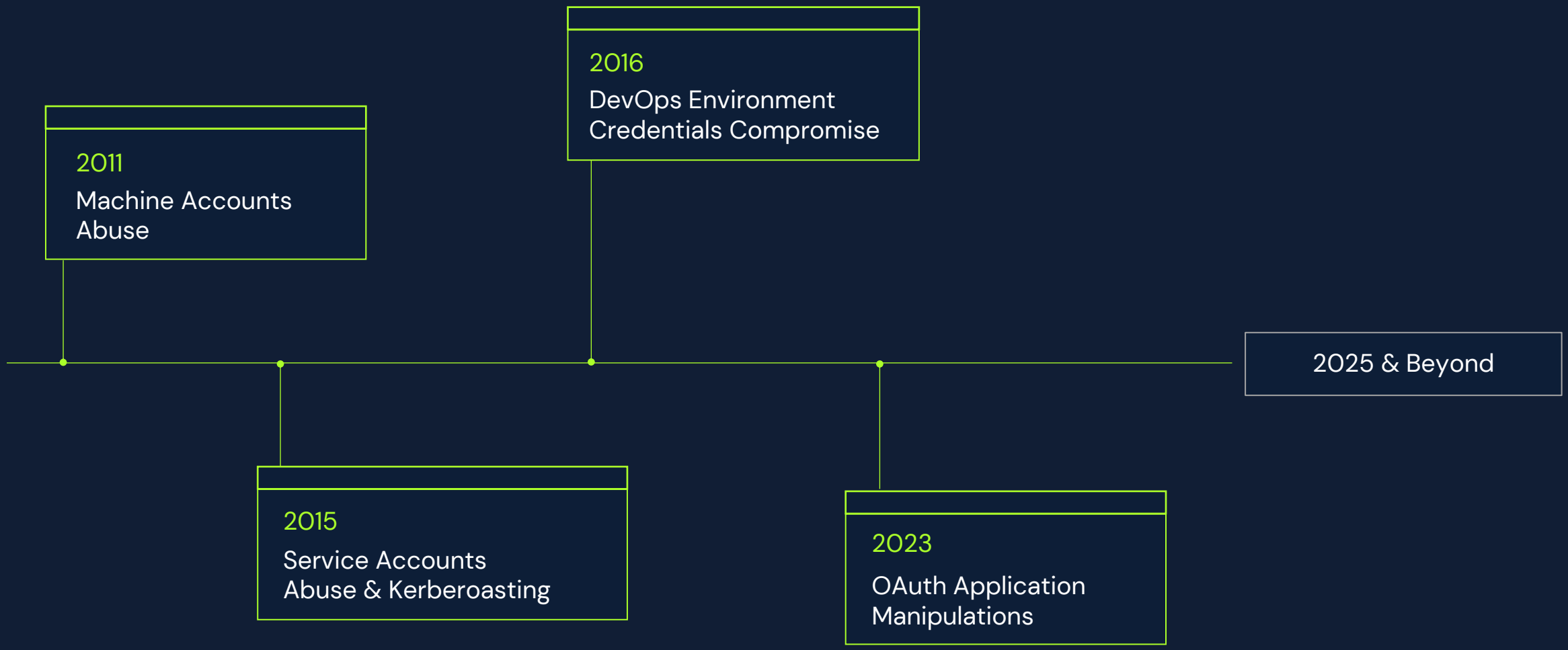


Reconnaissance, Resource Development, Initial Access, Execution, Persistence and Defence Evasion

Discovery, Collection, Command & Control, Exfiltration and Impact

CYBERARK®

Brief History of Machine Identities Threats



CYBERARK®


NEW IDENTITIES
NEW ENVIRONMENTS
NEW PARADIGMS
NEW ATTACK METHODS

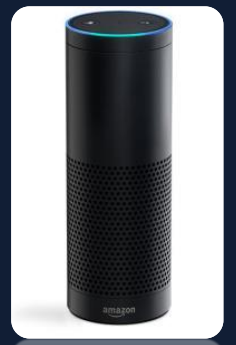
Privileged Access Management (PAM): Is it Still Relevant?

Year: 2000

HD size: 80GB

Year: 2007

HD size: 1 TB



Year: 2014

HD size: 10TB

Year: 2022

HD size: 20TB

CYBERARK®

Spectrum of Secured Environments
Zero Trust Access for All Identities

Standing Access

Access with personal admin account →

Access with shared account →

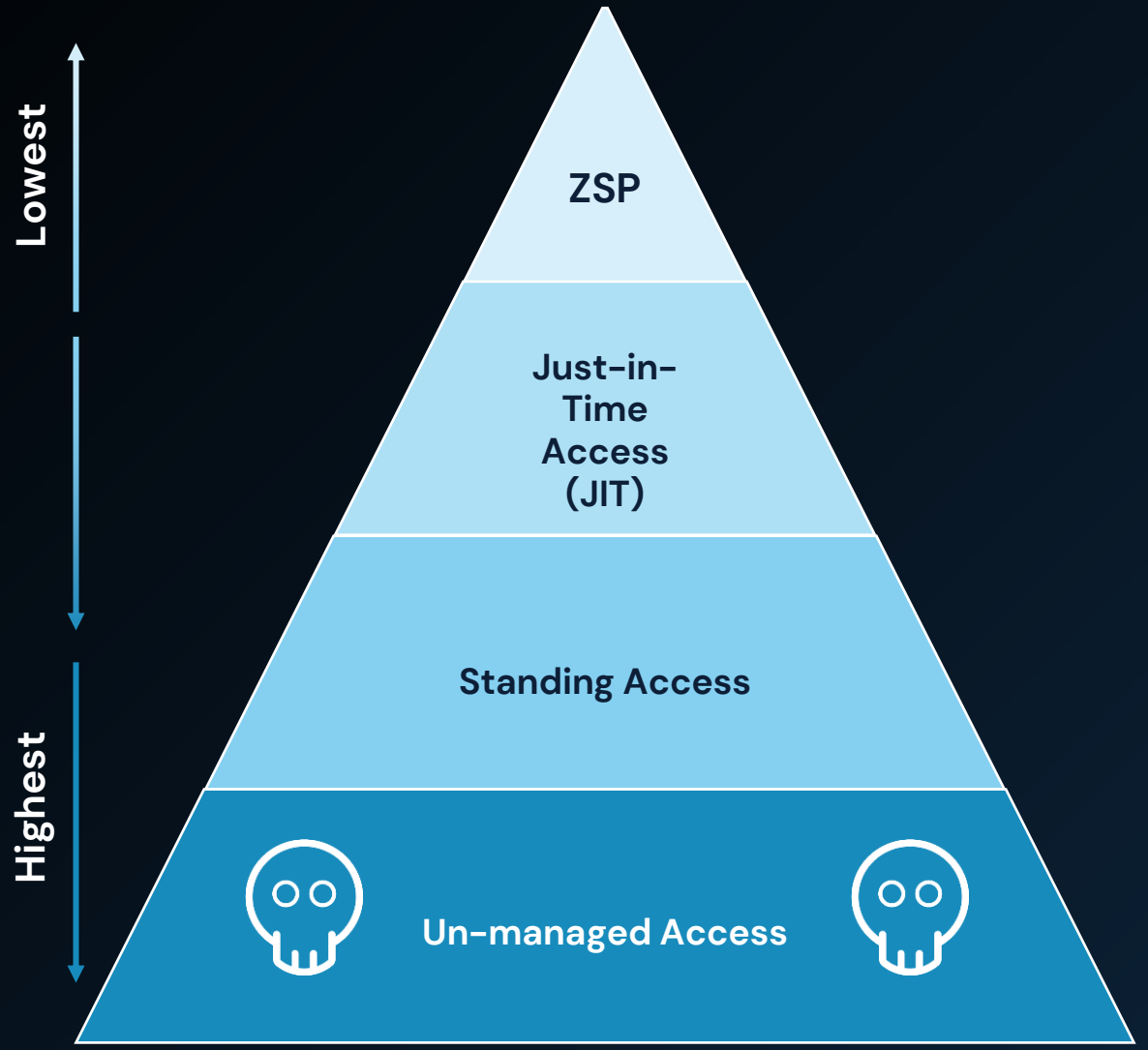
Federated Access

Assume admin role for elastic workloads →

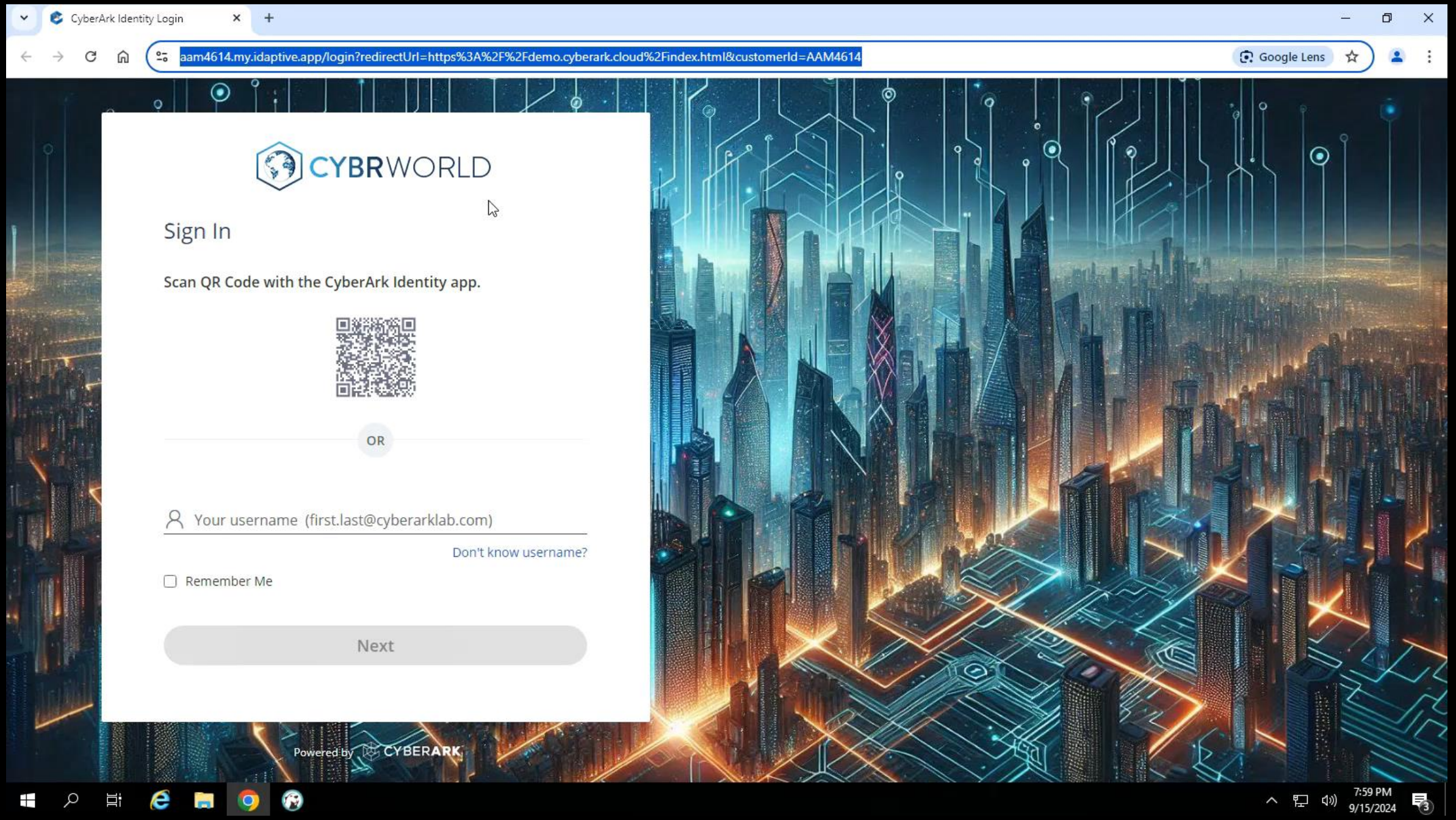
Assume admin role for cloud native services →

Assume admin role for web apps →

Risk Reduction Using Different Methods



CYBERARK®


CyberArk Identity Login
aam4614.my.idaptive.app/login?redirectUrl=https%3A%2F%2Fdemo.cyberark.cloud%2Findex.html&customerId=AAM4614
Google Lens
CYBRWORLD
Sign In
Scan QR Code with the CyberArk Identity app.
OR
Your username (first.last@cyberarklab.com)
Don't know username?
Remember Me
Next
Powered by CYBERARK
7:59 PM
9/15/2024

The challenge of cloud access

On Premise: Users OR Admins

*"Our applications run on **servers**"*

Windows Admin | Linux Admin | DB Admin

Require access to **servers**.

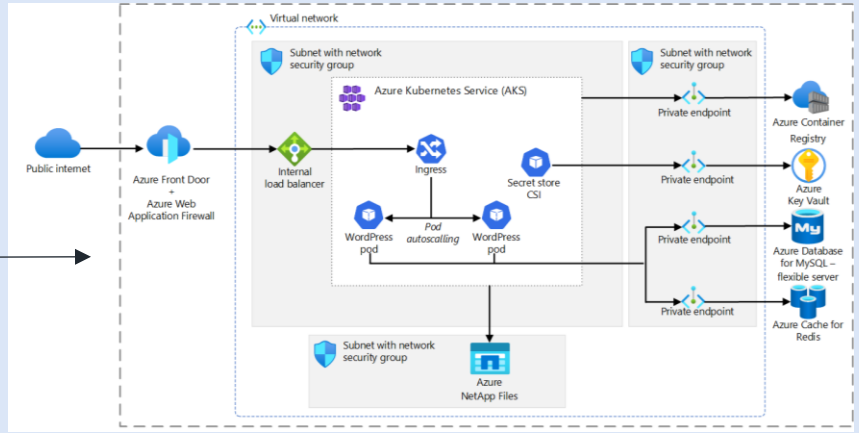
In the Cloud: Users ARE Admins

*"Our applications run on **services**"*

DevSecOps | Engineers | Data Scientists | Contract Developers

Require access to:

- Compute **services** and hosts
- Networking **services**
- Storage **services**
- Database + BigData **services**
- Deployment **services**
- … and more



Sample architecture – media app in Microsoft Azure

CYBERARK®

Secure Access to the Cloud Services

Who

Eva - Cloud Engineer

What

The cloud console, services and Infrastructure

Same scope/same Permission

Why

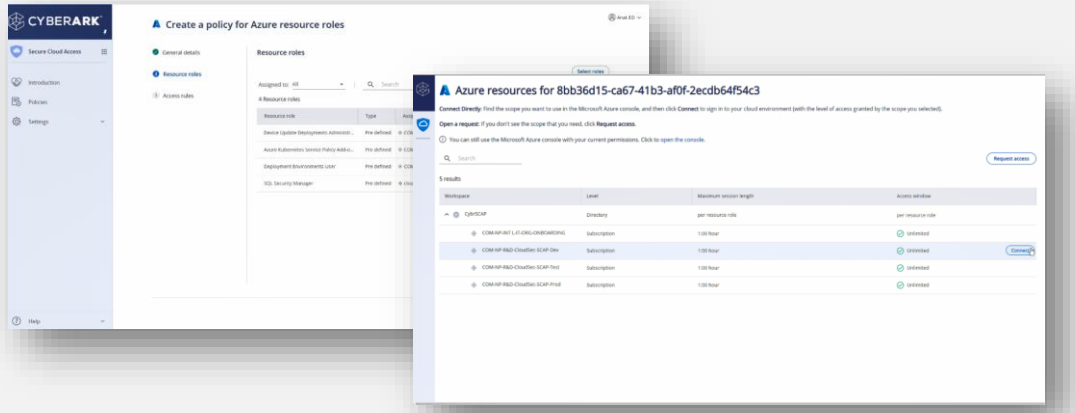
Build, Test, Deploy

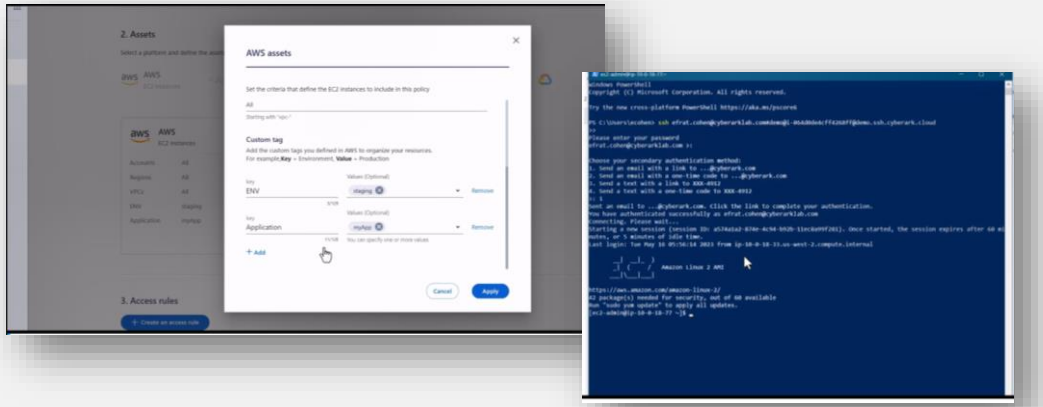
Frequency

Regular, Daily Use

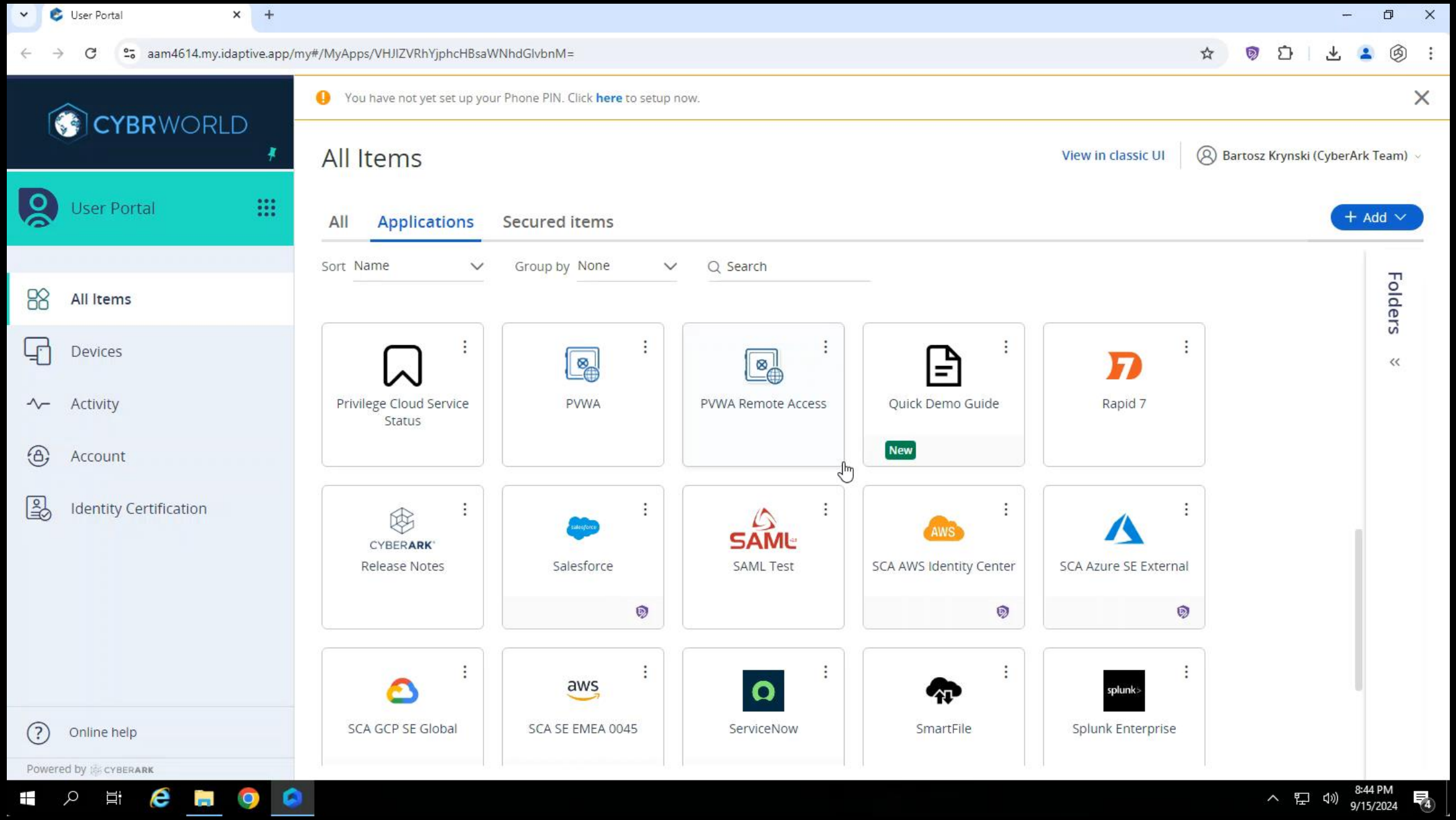
Expected experience: native access, no need to submit an access request

Policy-based access





CYBERARK


User Portal
aam4614.my.idaptive.app/my#/MyApps/VHJIZVRhYjphcHBsaWNhdGlvbnM=
CYBRWORLD
You have not yet set up your Phone PIN. Click here to setup now.
User Portal
All Items
Devices
Activity
Account
Identity Certification
Online help
Powered by CYBERARK
All Items
View in classic UI
Bartosz Krynski (CyberArk Team)
All
Applications
Secured items
Add
Sort Name
Group by None
Search
Folders
Privilege Cloud Service Status
PVWA
PVWA Remote Access
Quick Demo Guide
New
Rapid 7
CYBERARK Release Notes
Salesforce
SAML Test
SCA AWS Identity Center
SCA Azure SE External
SCA GCP SE Global
SCA SE EMEA 0045
ServiceNow
SmartFile
Splunk Enterprise
8:44 PM
9/15/2024

Virtual machines - Microsoft A | CyberArk Secure Web Sessions

portal.azure.com/?wa=wsignin1.0#browse/Microsoft.Compute%2FVirtualMachines

Microsoft Azure | Search resources, services, and docs (G+/) | Copilot | bartosz.krynski@demo-... COM-NP-INT L-SALES ENGINEER...

Home >

Virtual machines

COM-NP-Int L-Sales Engineering-Azure-External (cybrdemooutlook.onmicrosoft.com)

Create | Switch to classic | Reservations | Manage view | Refresh | Export to CSV | Open query | Assign tags | Start | Restart | Stop | Delete | Services | Maintenance

Filter for any field... | Subscription equals **all** | Type equals **all** | Resource group equals **all** | Location equals **all** | Add filter

Showing 0 to 0 of 0 records.

No grouping | List view

Name	Subscription	Resource group	Location	Status	Operating system	Size	Public IP address	Disks

No virtual machines to display

Create a virtual machine that runs Linux or Windows. Select an image from the marketplace or use your own customized image.

Create

Learn more about Windows virtual machines

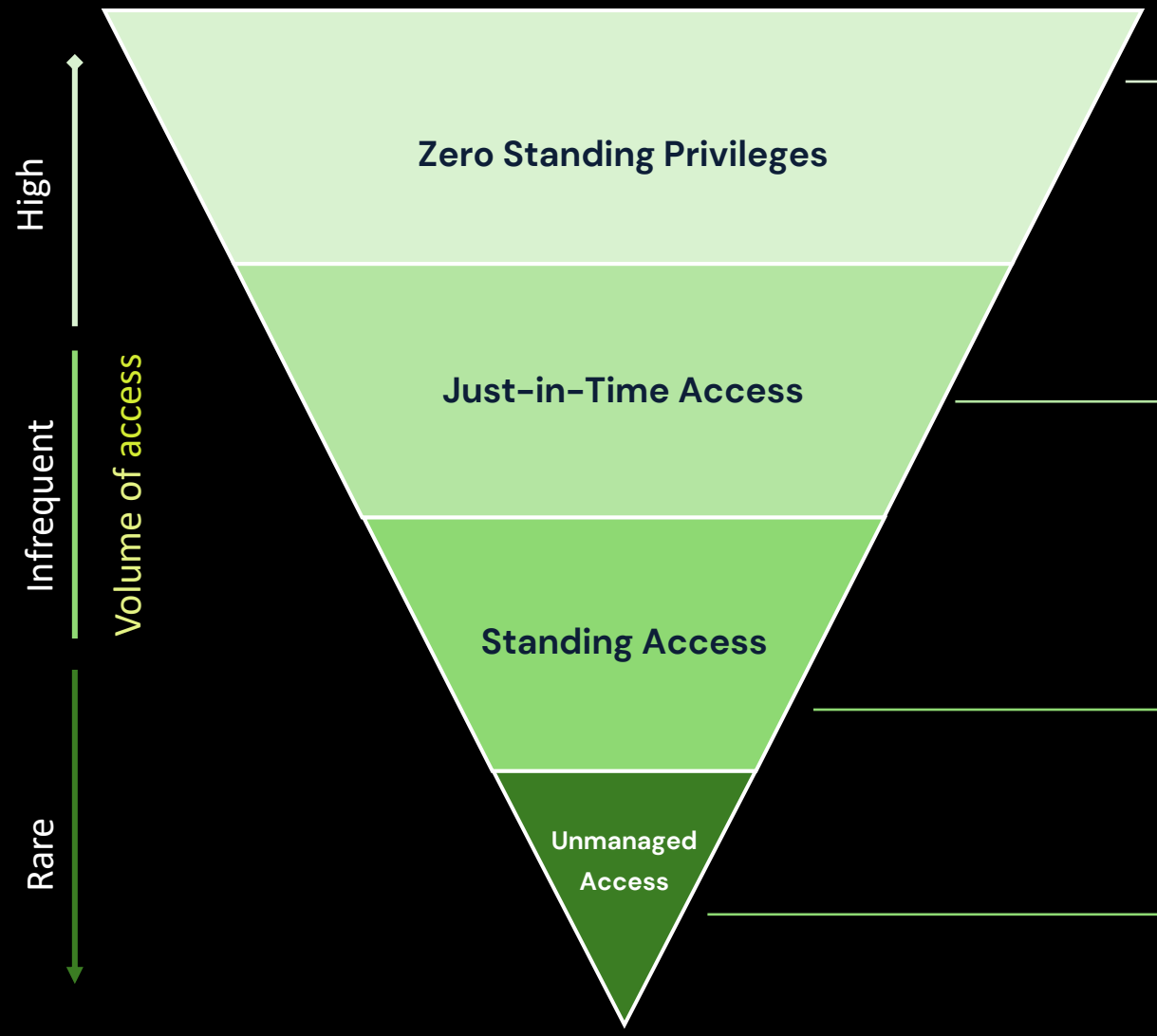
Learn more about Linux virtual machines

Give feedback

9:00 PM
9/15/2024


Documents
Downloads
Google Chrome
Computer Management
Registry Editor
WinSCP
CyberArk EPM Contr...
Username
Password
Login
DATA
AI
Type here to search
Downloads
CyberArk Endpoint ...
12:53 PM
9/15/2024

Prioritizing Privilege Controls



Zero Standing Privileges

- This should be your default method for privilege controls.
- Highest possible risk reduction with a lower effort to implement.
- This should be the highest volume of your privileged access.

Just-in-Time Access

- When ZSP controls are not possible – JIT is a good alternative control.
- Significant risk reduction is achieved by implementing access upon request.
- Use is subject to ZSP availability.

Standing Access - Secured by PAM – Vaulted and Isolated

- There will be system access. E.g. Cloud root accounts – You cannot neglect - Safe storage and privilege controls ALWAYS needed.
- Risk reduction is achieved through isolation and rotation of the accounts.
- This should be the lowest volume, representing a decreasing number of accounts.

Unmanaged Access

- This should not exist, but you should always track and account for any unmanaged access with the goal of putting them under management

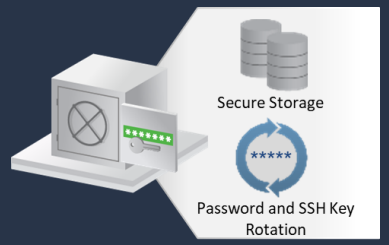
WORKFORCE

IT

DEVELOPERS

MACHINES

The Evolution of Securing Machines Pragmatically




```
Username = GetUserName()
Password = GetPassword()
Host = GetHost()
ConnectDatabase(Host, Username, Password)
```

Pre-2015

- CLI / BASH / PowerShell
- JAVA
- .NET
- C#
- MAINFRAME

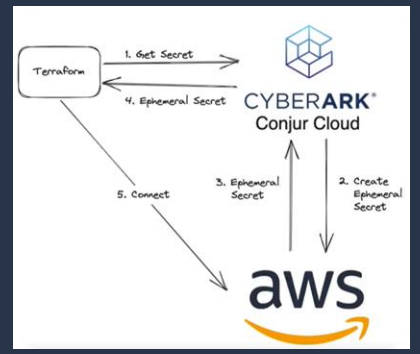
2017

- CI/CD Tools
- ANSIBLE
- k8s Cluster
- OpenShift

Conjur Cloud

2018-2023

- Cloud Native
- AKS / EKS / GKE
- Serverless



2023-Today

- Dynamic Secrets
- Cloud Key Vault
- Cloud Key Managament
- External Driver Operator

CYBERARK

Secure Certificates, PKI and Secrets. Automate and Prevent Outages

Expanded Capabilities Secure All Machine Identities

Secure Machine Identities

Machine Identity Security

Workloads | Apps | APIs | Infrastructure | Bots | IoT/OT

Certificate and PKI Management

- CLM (Certificate Lifecycle Management)
- PKI (Public Key Infrastructure)
- Certificate discovery
- Code signing

Secrets Management

- Centralized secrets management
- Secrets discovery
- Rotated and dynamic secrets

Secure Admin & IT Resource Access

Secure Access: Certificate & DevOps Admins, IT Resources

CyberArk PAM /CyberArk Identity Security Platform

CYBERARK®

What can I do here?

Dashboard

Share

All certificates **500** | Expired certificates **252** | Managed certificates **500** | Old certificates **248** | Retired certificates **0**

Expired certificates | High risk: 0 - 7 days expiration | Medium risk: 8 - 30 days expiration | Low risk: 31 - 60 days expiration | Healthy: > 60 days expiration

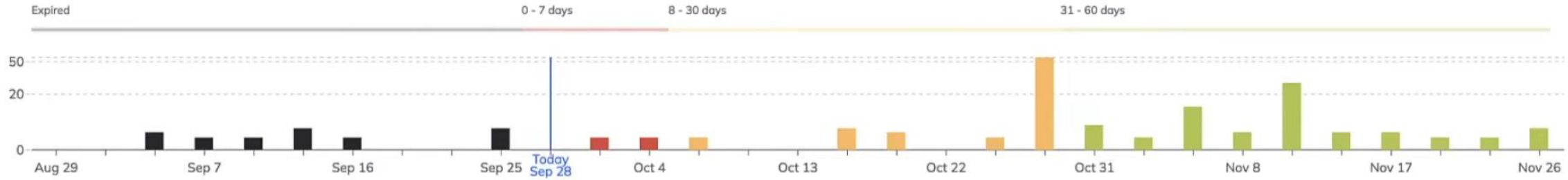
16 Certificates assigned to 3 Applications

Expired **12** | High Risk **1** | Medium Risk **0** | Low Risk **0** | Healthy **3**

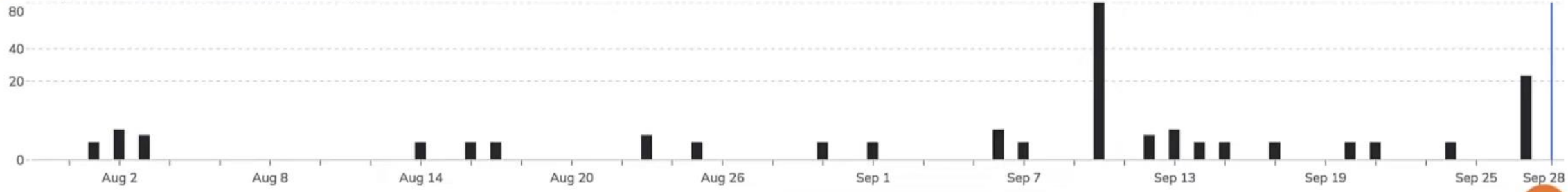
490 Certificates not assigned to Applications

Expired **246** | High Risk **1** | Medium Risk **42** | Low Risk **75** | Healthy **126**

132 Certificates expired, or about to expire



132 Newly added certificates for past 60 days

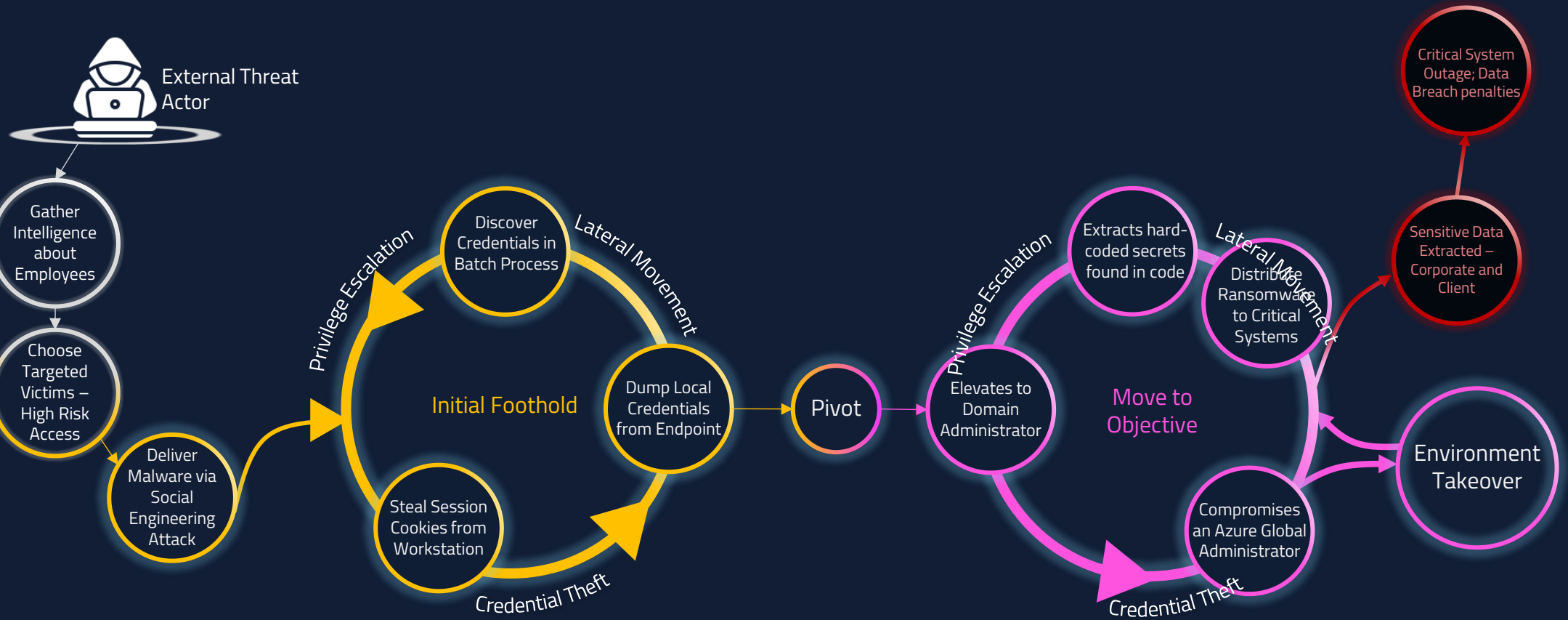


?

High risk certificates by Applications

Medium risk certificates by Applications

Attack chain reminder

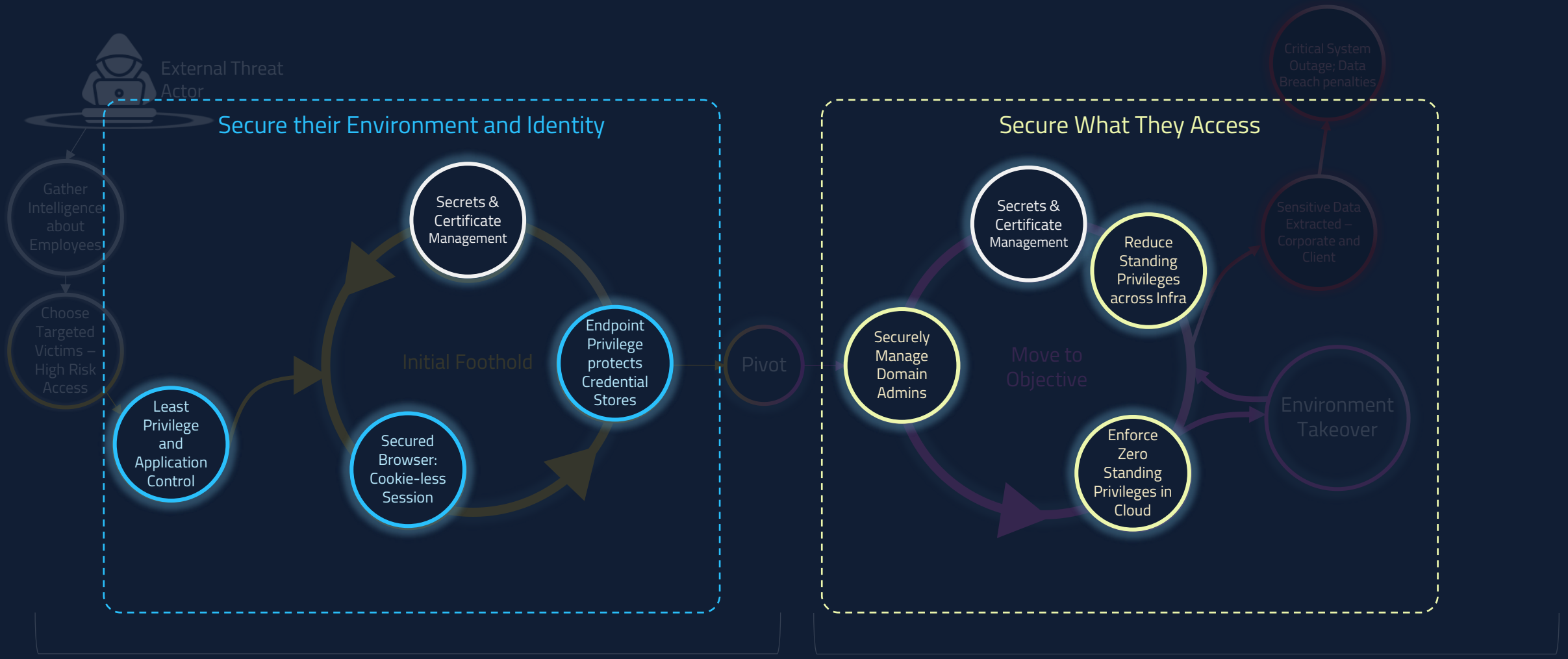


Reconnaissance, Resource Development, Initial Access, Execution, Persistence and Defence Evasion

Discovery, Collection, Command & Control, Exfiltration and Impact

CYBERARK®

Attack chain reminder



CYBERARK

CYBERARK®
The Identity Security Company™

bako tech®

Thank you!