LEGAL DISCLAIMER

This presentation contains materials that can be potentially damaging or dangerous.

These materials are for educational and research purposes only.

All tools provided are open source and CyberArk is not associated with any tools provided. Do not attempt to violate the law with anything contained here. If this is your intention, then **LEAVE NOW!** Neither the authors of this material, CyberArk, or anyone else affiliated in the content in any way, is going to accept responsibility for your actions.

We promote hacking, but do not promote CRIME! We are documenting the ways criminals steal and perform their nefarious acts, so you can defend yourself and your organization.

AGENDA

- Introduction
- CYBR Blueprint
- Cloud Attack Vectors
- Defense Controls

ANDY THOMPSON

Andy.Thompson@CyberArk.com

- Linkedin: in/andythompsoninfosec
- GitHub: github.com/binarywasp
- Twitter: @R41nMkr

- CyberArk Labs Advisor
- SSCP/CISSP
- GPEN Pen-tester
- Dallas TX Hacker Scene
- Travel-Hacker

51%

of security pros says there is no relationship between IT security and business innovation

50%

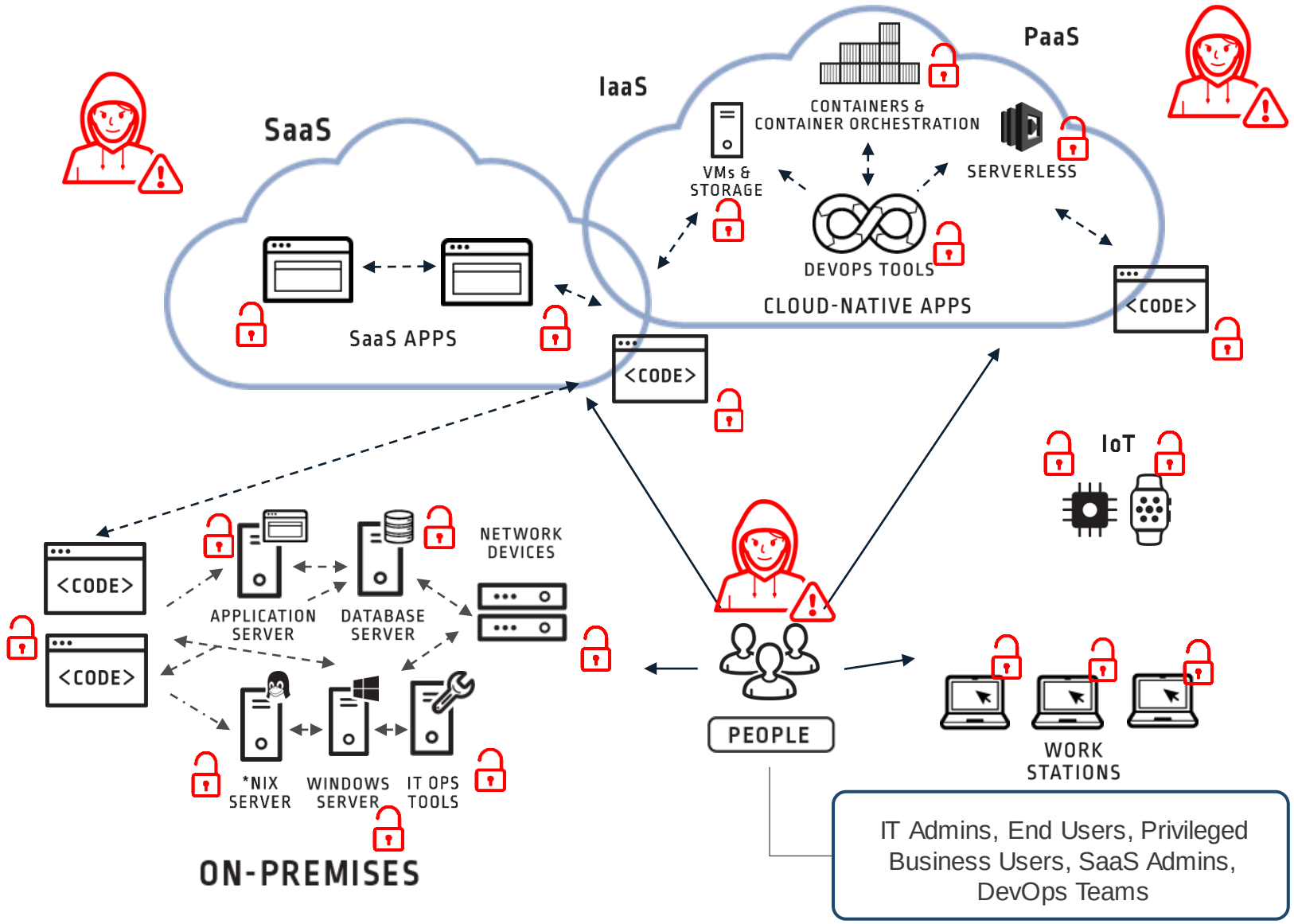
Don’t have a privileged account security strategy in place for Cloud

75%

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

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

THE NEW NORM: MORE RISK



More Infrastructure

More Applications

More Privileged Actors

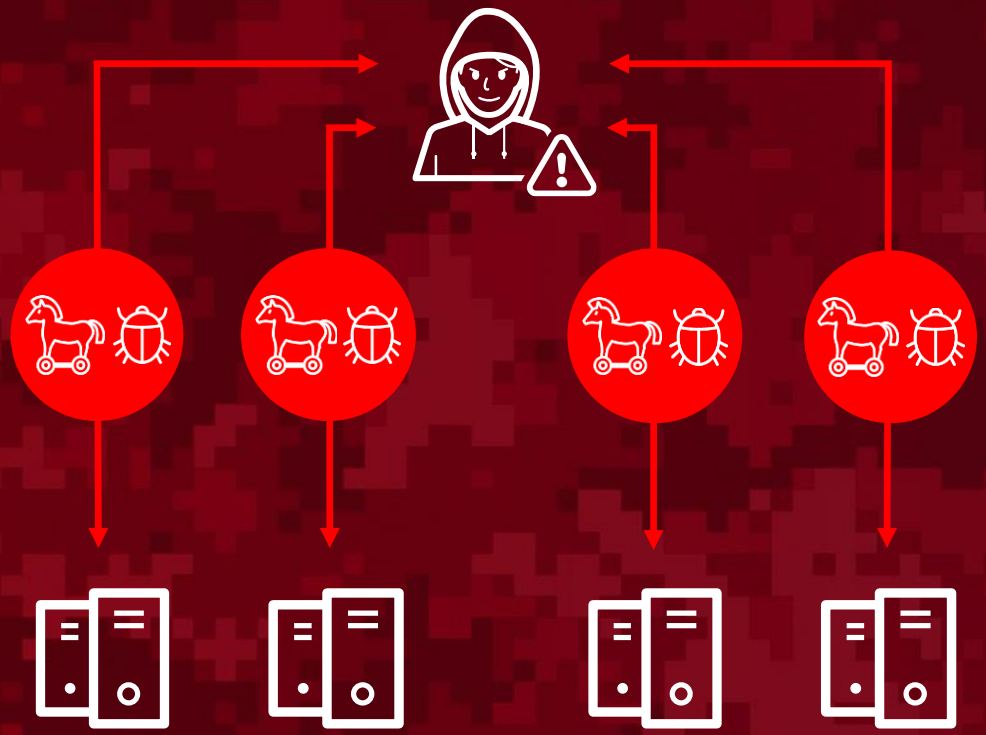
More Automation

More Privileged Security Risk!

THE POWER OF PRIVILEGE IN THE CLOUD

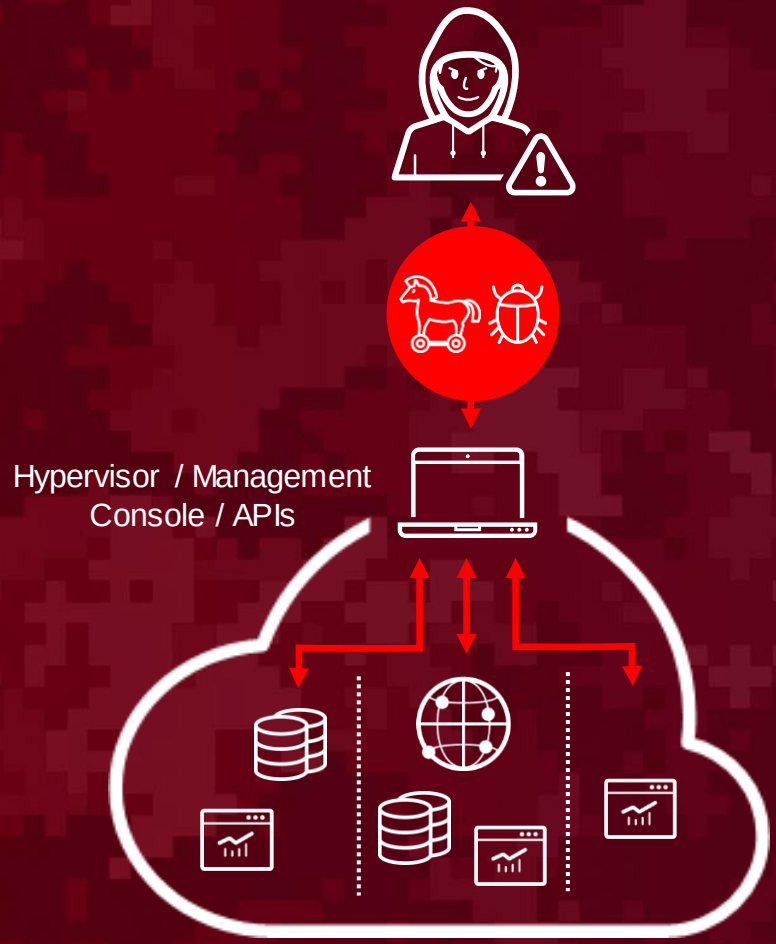
OLD WAY

Compromise a system, then another, then another, then own a domain



NEW WAY

Compromise one user, then own Cloud infrastructure



BLUEPRINT: 3 GUIDING PRINCIPLES

PREVENT CREDENTIAL THEFT

STOP LATERAL & VERTICAL MOVEMENT

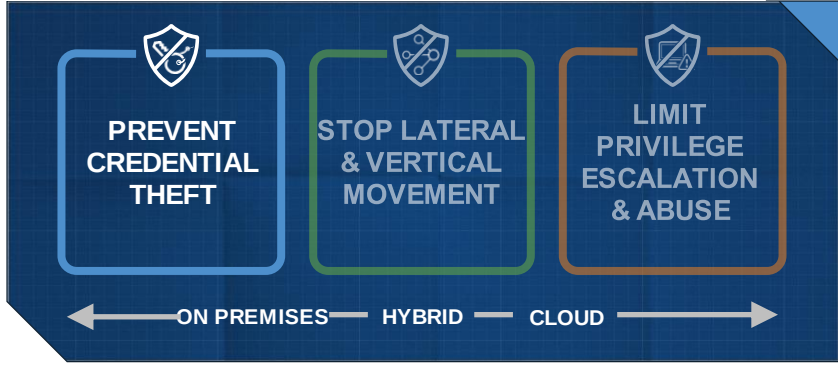
LIMIT PRIVILEGE ESCALATION & ABUSE

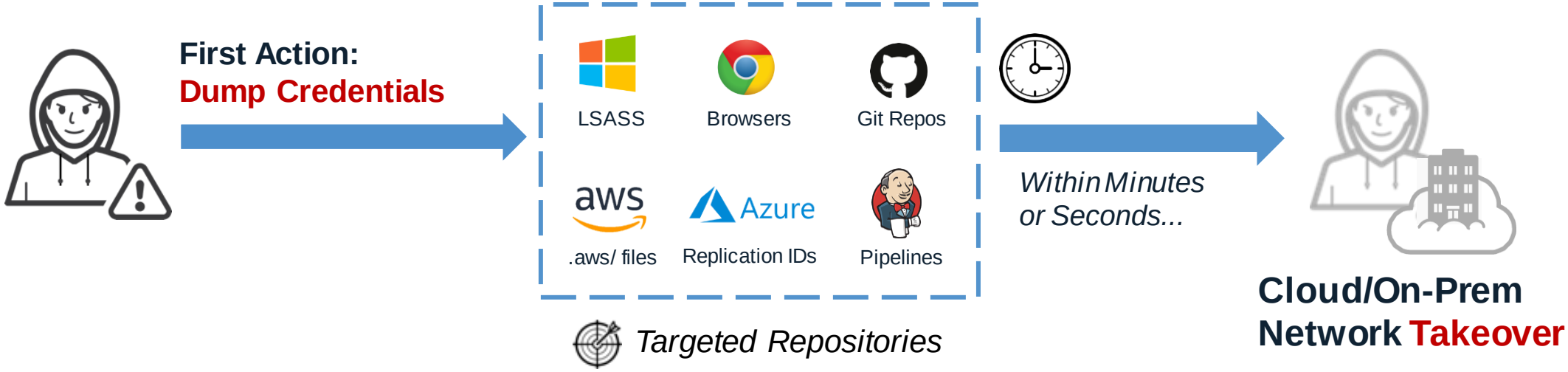
ON PREMISES — **HYBRID** — **CLOUD**

Risk based program designed to secure privileged access across all environments

GUIDING PRINCIPLE ON RISK MITIGATION

PREVENT CREDENTIAL THEFT





BLUEPRINT RECOMMENDATIONS

- ❑ Use **Session Isolation** to prevent credential residue from hitting machines
- ❑ **Remove Hard Coded Creds** from apps, scripts, and code repositories
- ❑ **Detect & Block** threats that are trying to access credential stores on endpoints

GUIDING PRIN

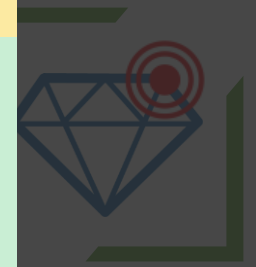
STOP LATERA

STOP LATERAL & VERTICAL MOVEMENT

LIMIT PRIVILEGE ESCALATION & ABUSE

ISES — HYBRID — CLOUD

Low Trus



Number of Characters	Numbers Only	Upper/Lower Case Letters	Upper/Lower Case Letters Mixed	Numbers, Upper- & Lower-Case Letters	Numbers, Upper & Lower Case Letters, Symbols
3	Instantly	Instantly	Instantly	Instantly	Instantly
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	3 Secs	10 Sec
6	Instantly	Instantly	8 Secs	3 Min	13 Min
7	Instantly	Instantly	5 Min	3 Hours	17 Hours
8	Instantly	13 Min	3 Hours	10 Days	57 Days
9	4 Secs	6 Hours	4 Days	1 Year	12 Years
10	40 Secs	6 Days	169 Days	106 Years	928 Years
11	6 Min	169 Days	16 Years	6K Years	71K Years
12	1 Hour	12 Years	600 Years	108K Years	5M Years
13	11 Hours	314 Years	21K Years	25M Years	423M Years
14	4 Days	8K Years	778K Years	1Bn Years	5Bn Years
15	46 Days	212K Years	28M Years	97Bn Years	2Tn Years
16	1 Year	512M Years	1Bn Years	6Tn Years	193Tn Years
17	12 Years	143M Years	36Bn Years	374Tn Years	14Qd Years
18	126 Years	3Bn Years	1Tn Years	23Qd Years	1Qt Years

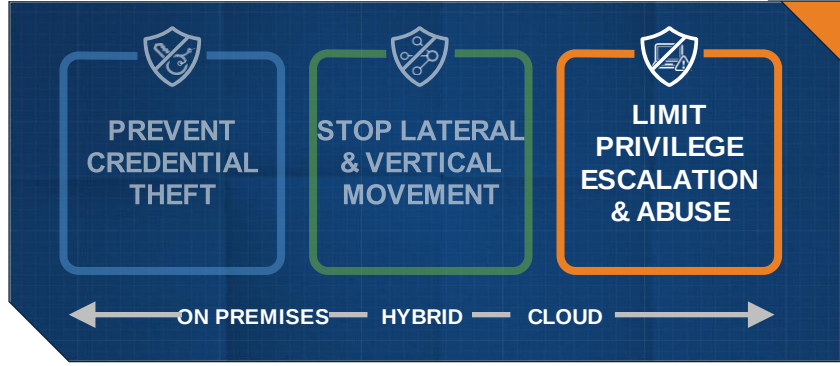
- **Randomize creden**
  eliminate account r
  reduce the overall time to live

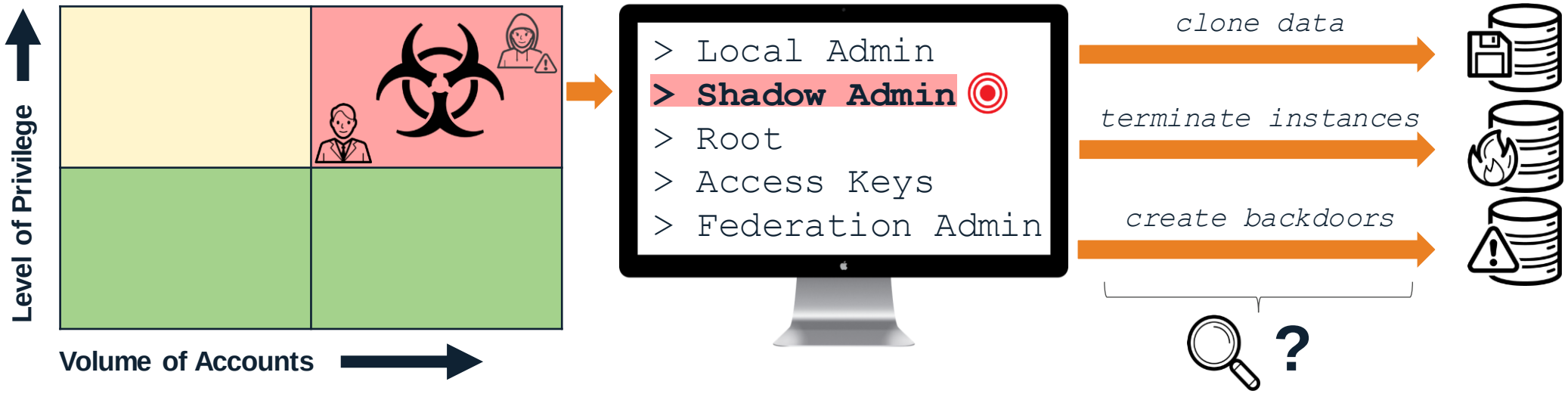
attacker's range of motion

st in Time
T) by providing
privilege only when needed

GUIDING PRINCIPLE ON RISK MITIGATION

LIMIT PRIVILEGE ESCALATION & ABUSE





BLUEPRINT RECOMMENDATIONS

- ❑ Enforce **Least Privilege** to reduce the attack surface and control elevation
- ❑ **Analyze Session** activities to look for signs of anomalous or malicious activity
- ❑ Apply **Adaptive Response** controls based on user activity to stop threats early

DEEP PRESCRIPTIVE GUIDANCE

STAGE 1 – RAPID RISK MITIGATION

RAPID RIS

On Prem/S

Hypervis
- ❑ Isola
- ❑ Rota

All Enviro
- ❑ Doma
- ❑ Win S
- ❑ Apply
- ❑ Servic
- ❑ C³ All
  Autom
- ❑ Creat
- ❑ Apply
- ❑ Devel

CYBERAR

STAGE 2 – UNIVERSAL TECHNOLOGIES

SECURING

On Prem/Sta

Win Work
Loosely Conn
- ❑ Vault

All Environm
- ❑ Active
- ❑ Service
- ❑ *nix roo
- ❑ Sessio
- ❑ Enviror
  - ❑ Se
- ❑ C³ Allia
  secrets
- ❑ Automa

CYBERARK

STAGE 3 – ENTERPRISE FOCUS

PIVOTING TO

On Prem/Stati

Out of Ban
- ❑ Isolate
- ❑ Rotate

All Environme
- ❑ Credenti
- ❑ One Tim
- ❑ *nix "roo
- ❑ Databas
- ❑ 3rd Party
- ❑ Session
- ❑ Adaptive
- ❑ Automat
- ❑ IT Admin
- ❑ Automat
- ❑ Full IAM

CYBERARK

STAGE 4 – MATURE THE PROGRAM

MATURING

On Prem/Stat

Network De
- ❑ Isolate

Static Appl
- ❑ Secrets

Critical Bus
- ❑ Vault &

All Environme
- ❑ Named
- ❑ Windows
  - ❑ Leas
  - ❑ Cred
  - ❑ App
- ❑ Windows
- ❑ Detailed
- ❑ Automat
- ❑ Ticketing

CYBERARK

STAGE 5 – ADVANCED SECURITY

SHORING UP PRIVILEGED ACCESS

On Prem/Static

Mainframe/Mid-Range
- ❑ Isolate & Rotate

Static Applications
- ❑ Advanced Authentication

Business Applications
- ❑ Vault & Isolate

Cloud/Dynamic

Web Applications
- ❑ Vault Credentials
- ❑ Isolate Sessions

All Environments
- ❑ **Windows Service IDs:** Rotate credentials
- ❑ **Kerberos Attack Detection** for Windows ENVs
- ❑ **Windows Servers**
  - ❑ Credential Theft Blocking
  - ❑ Application Elevation Whitelisting
- ❑ **Windows/Mac Wks:** App elevation whitelisting
- ❑ **Domain Controllers:** Least Privilege
- ❑ ***Nix Servers:** Least Privilege (*sudo replacement*)
- ❑ **Automatic Discovery** of Windows service IDs
- ❑ **Automated Dashboards** to track program KPIs

Stage 5 Guiding Principle: Look for new opportunities to shore up privileged access

Food For Thought
- Ask for partnership opportunities on product betas
- Provide guidance on new C3 Alliance integrations

CYBERARK

CLOUD ATTACK VECTORS

CLOUD ATTACK VECTORS

Locally Stored Cloud Credentials

Embedded Cloud Credentials in Code & Scripts

Credentials from the Cloud VM's Metadata

Cloud Misconfigs and Shadow Admins

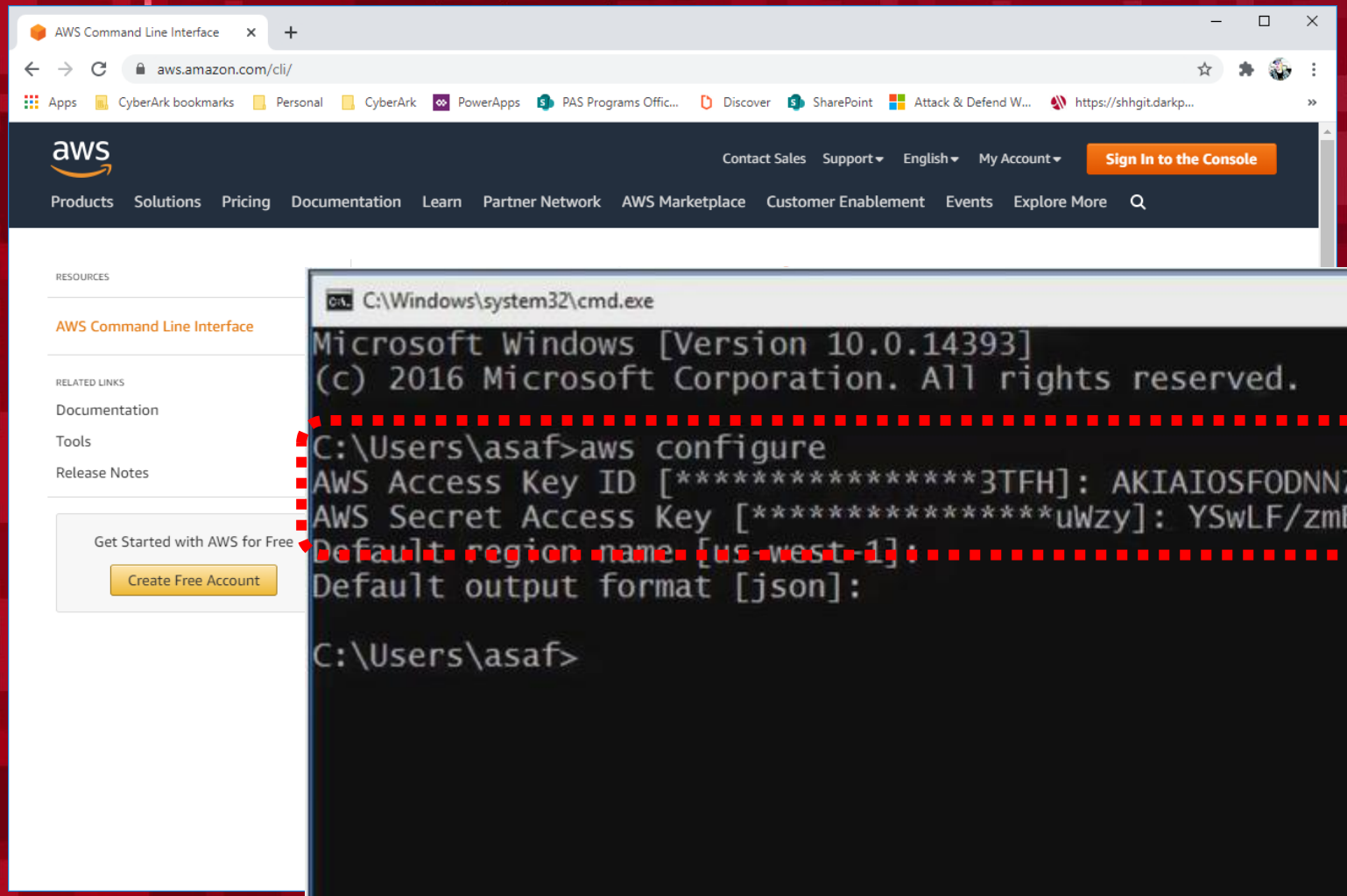
IAM and Federation Solutions to the cloud

LOCALLY STORED CLOUD CREDENTIALS

- Built almost entirely on AWS.
  - EBS snapshots
  - S3 buckets
  - AMI's
  - EBS instances
  - etc.
- Attacker accessed the AWS control panel.
- Extortion attempted
  - Did not comply.
- Game Over!

https://www.infoworld.com/article/2608076/murder-in-the-amazon-cloud.html

CLOUD CLI TOOLS



CLI EXAMPLE: AWS

In AWS, more than 5,000 different API calls, like:

- Create a new user
- Run a new VM instance
- Read files from S3 buckets
- etc.

add-client-id-to-open-id-connect-provider

add-role-to-instance-profile

add-user-to-group

attach-group-policy

attach-role-policy

attach-user-policy

change-password

create-access-key

create-account-alias

create-group

create-instance-profile

create-login-profile

create-open-id-connect-provider

create-policy

create-policy-version

create-role

create-saml-provider

create-service-linked-role

create-service-specific-credential

create-user

create-virtual-mfa-device

deactivate-mfa-device

delete-access-key

AND MANY MORE

LOCALLY STORED CLOUD CREDENTIALS

By default: The Cloud credentials saved in clear text!

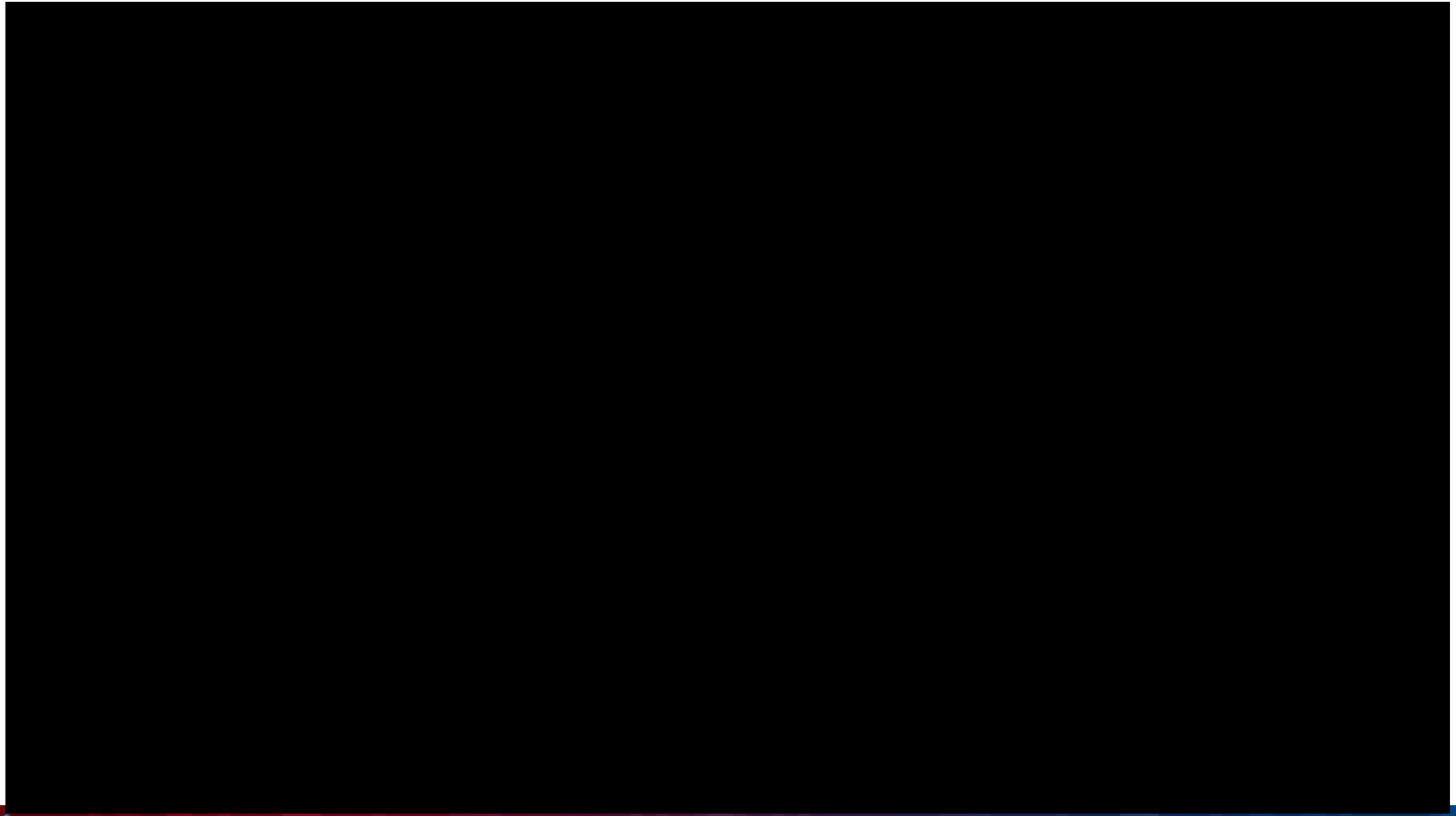
Under the “Users” folder:

AWS CLI:

1. C:\Users\{UserName}\.aws\credentials (Windows)
2. /home/{UserName}/.aws/credentials (Linux & MacOS)

Azure CLI:

1. C:\Users\{UserName}\.azure\accessTokens.json
2. C:\Users\{UserName}\.azure\azureProfile.json



HOW CAN CYBERARK HELP?

- **Secure Connect to AWS, Azure, and GCP CLI**
  - Using PSM when recording is needed.
- **For a Native Experience:**
  - PSM for SSH as bastion to manage workload in the cloud.
- **Manage and Rotate AWS IAM and Azure AD users**
- **Manage Cloud Platform Root Accounts**

SECURE ACCESS AND MANAGE THE CONSOLE

Google Cloud Platform

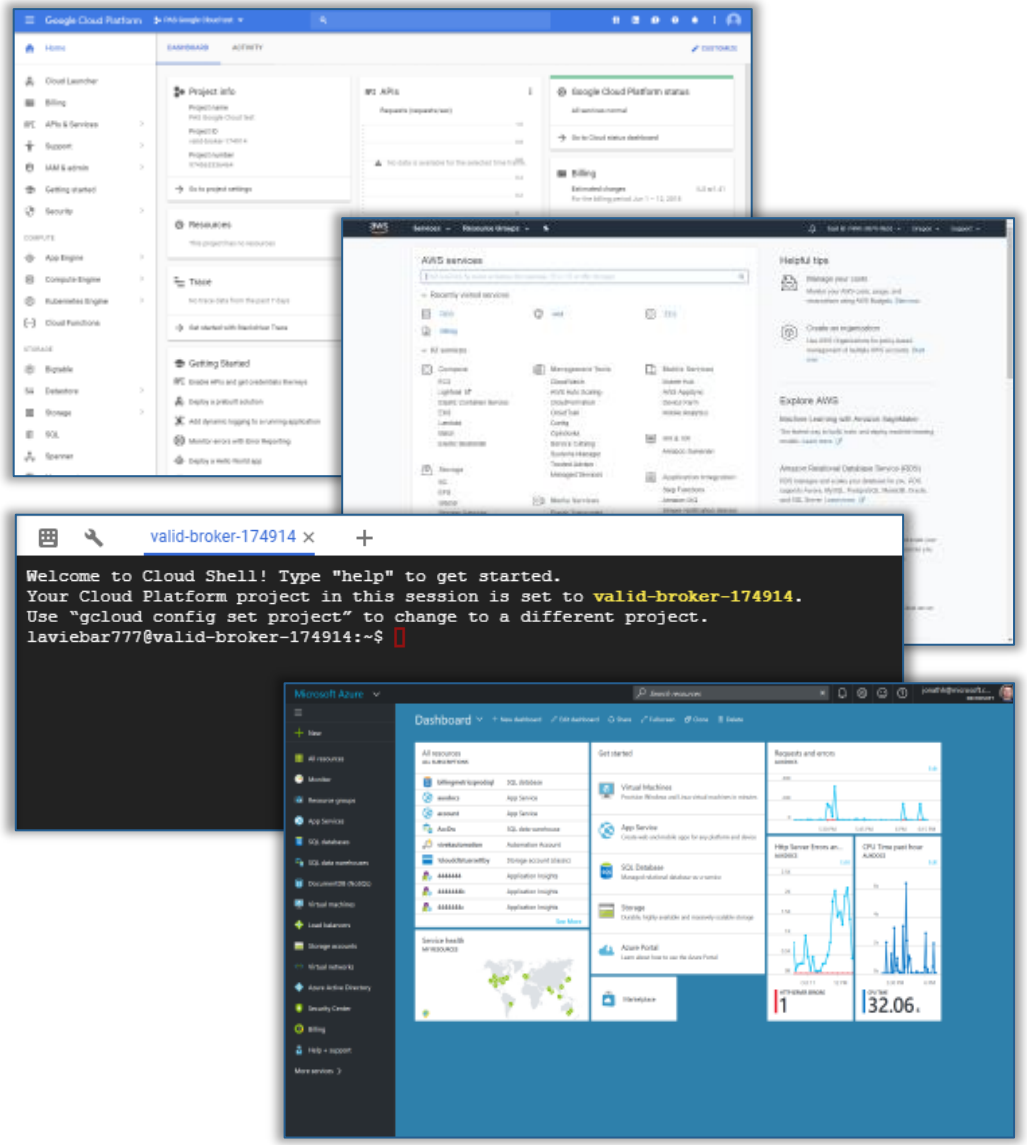
- Secure access to the Web Console and Web CLI

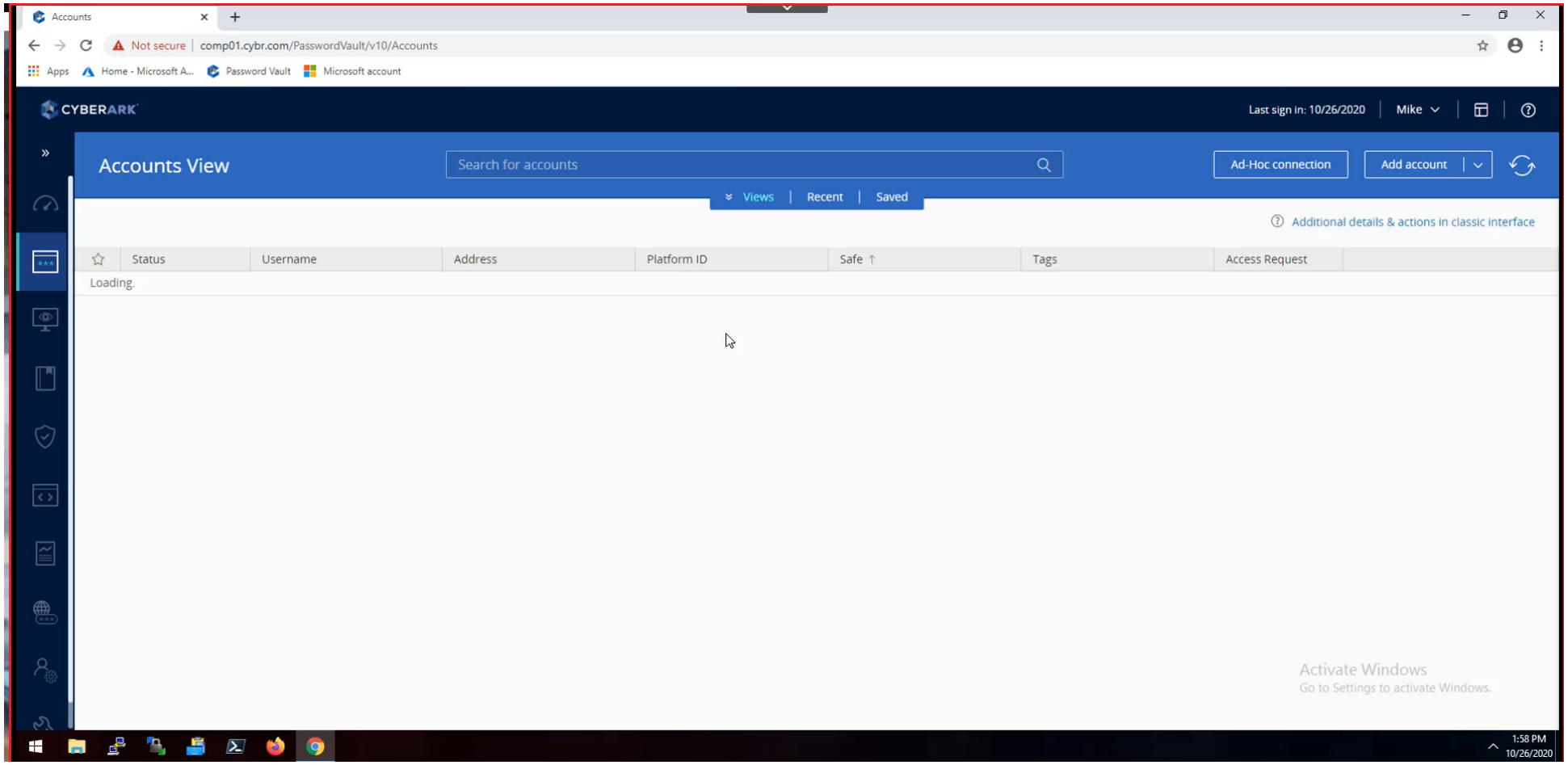
aws

- Protect and manage the root account
- Access to Console with root via PSM
- Manage IAM accounts
- Temporary access with AWS STS (AssumeRole and Federation)

Azure

- Manage Azure AD privileged accounts
- Secure access to Azure portal and Office365




Accounts
Not secure | comp01.cybr.com/PasswordVault/v10/Accounts
Apps
Home - Microsoft A...
Password Vault
Microsoft account
CYBERARK
Last sign in: 10/26/2020
Mike
Accounts View
Search for accounts
Ad-Hoc connection
Add account
Views
Recent
Saved
Additional details & actions in classic interface
Status
Username
Address
Platform ID
Safe
Tags
Access Request
Loading.
Activate Windows
Go to Settings to activate Windows.
1:58 PM
10/26/2020

EMBEDDED CLOUD CREDENTIALS IN CODE AND SCRIPTS

EMBEDDED CLOUD CREDENTIALS IN CODE & SCRIPTS

AWS Credential Structure:

1) Access ID. 20 alpha-numeric characters.
   (Always starts with AKIA)
   AKIAF06E7MXBSEXAMPLE

2) Secret Access Key. 40 alpha-numeric-slash-plus characters.
   kWcrlUX5JEDGM/LtmEENl/aVmYvHNif5zEXAMPLE

CREDS IN CODE & SCRIPTS

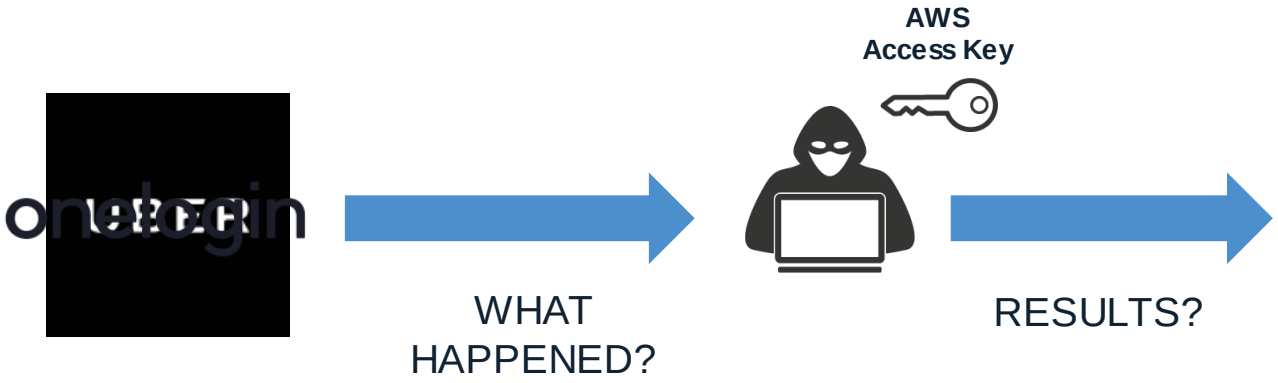
```
$policies = Get-IAMpolicyList -AccessKey AKIA4SMUA7B3AY - SecretKey t8#sb46aj2lf92jfolgbwo1x
$number = $managedPolicies.Count
Write-host "Discovered $numberPolicies policies"
```

```
$AccessKey = AKIA4SMUA7B3AY
$SecretKey = t8#sb46aj2lf92jfolgbwo1x

$policies = Get-IAMPolicyList - AccessKey #accessKey - SecretKey $secretKey
$number = $managedPolicies.Count
Write-host "Discovered $numberPolicies policies"
```

THE RISKS ARE REAL…

It only takes **one privileged credential** to **Hack a Datacenter** !!



Uber concealed massive hack that exposed data of 57m users and drivers

Firm paid hackers $100,000 to delete data and keep breach quiet

June 02, 2017

OneLogin hacker swiped AWS keys, can decrypt stolen data

OneLogin is reporting its recent data breach was made possible when a hacker obtained access to a set of Amazon Web Service keys through a third-party vendor. With this, the hacker was enabled entry into its U.S. data center compromising all its records.

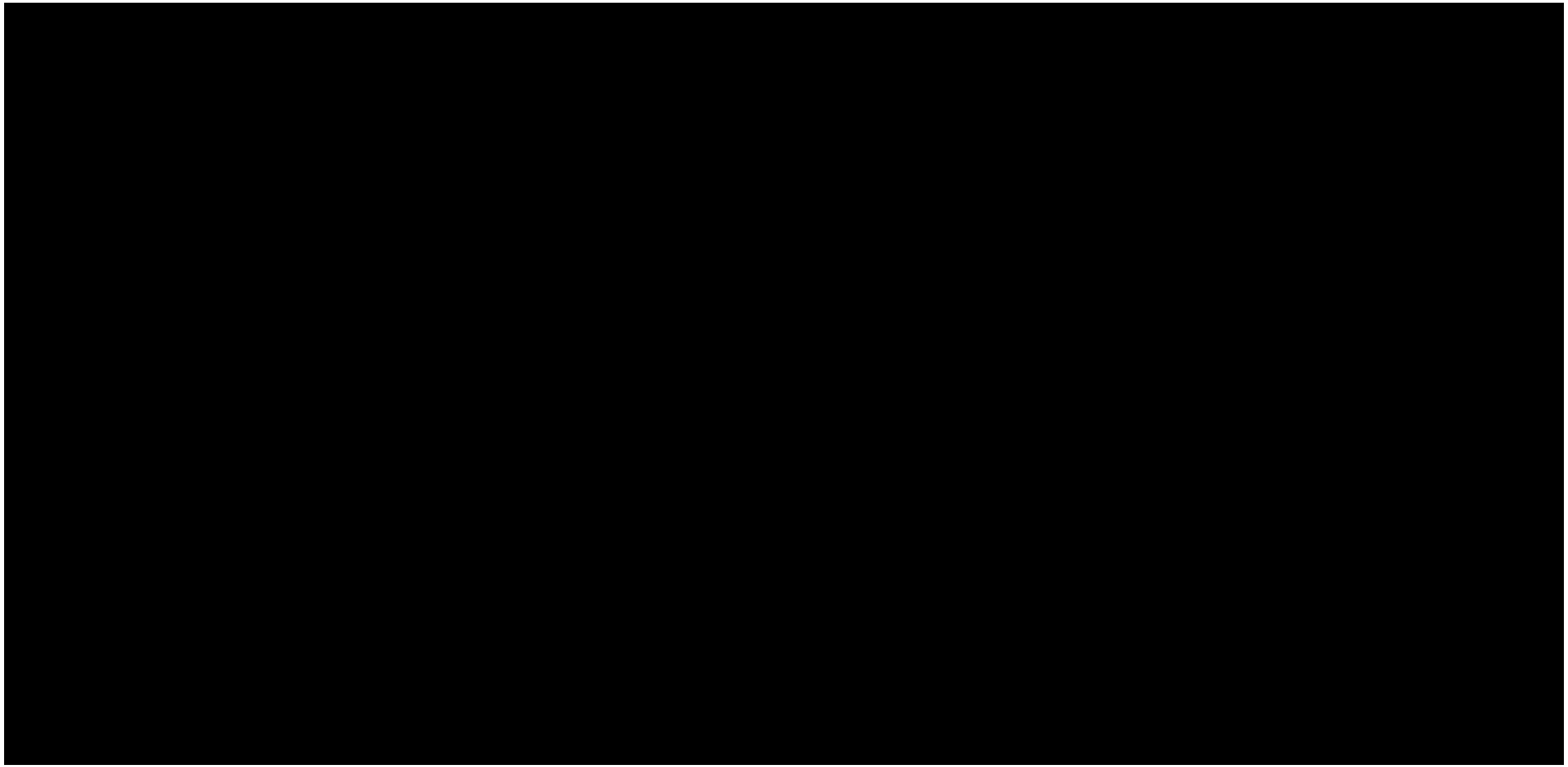
Companies should maintain direct control of their keys, said cybersecurity experts.

The password management firm said the stolen keys gave the intruder access through the AWS API, something industry experts say could have been averted if OneLogin maintained control of its keys. There could possibly be a design flaw, some say.

▲ Uber's CEO, Dara Khosrowshahi, said: 'None of this should have happened, and I will not make excuses for it.' Photograph: Andrew Caballero-Reynolds/AFP/Getty Images

https://www.theguardian.com/technology/2017/nov/21/uber-data-hack-cyber-attack

https://www.scmagazine.com/onelogin-hacker-swiped-aws-keys-can-decrypt-stolen-data/article/666112/

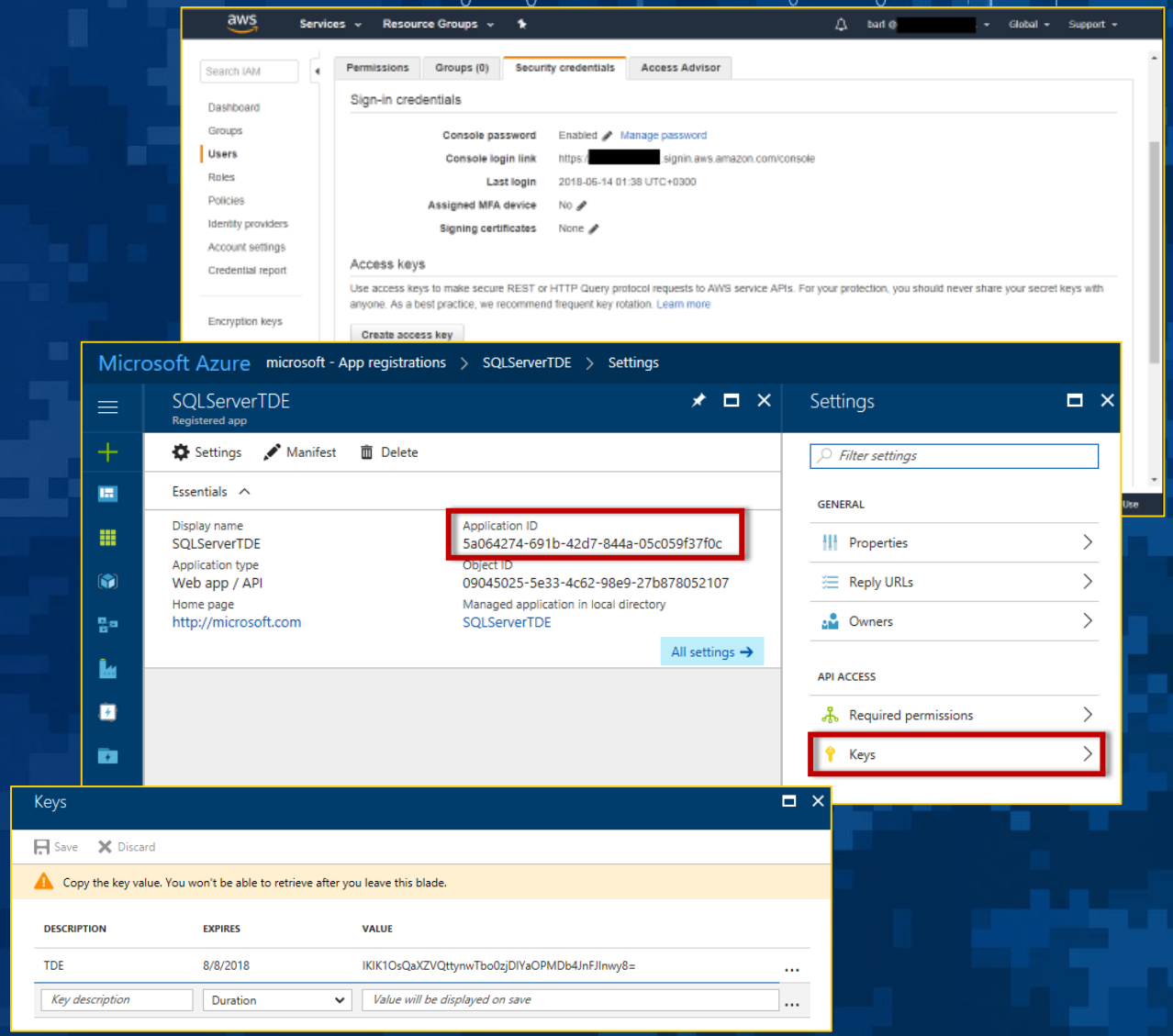


GUARD THE API KEYS

Risk: One hardcoded, unmanaged secret can takedown the entire network

Solution:

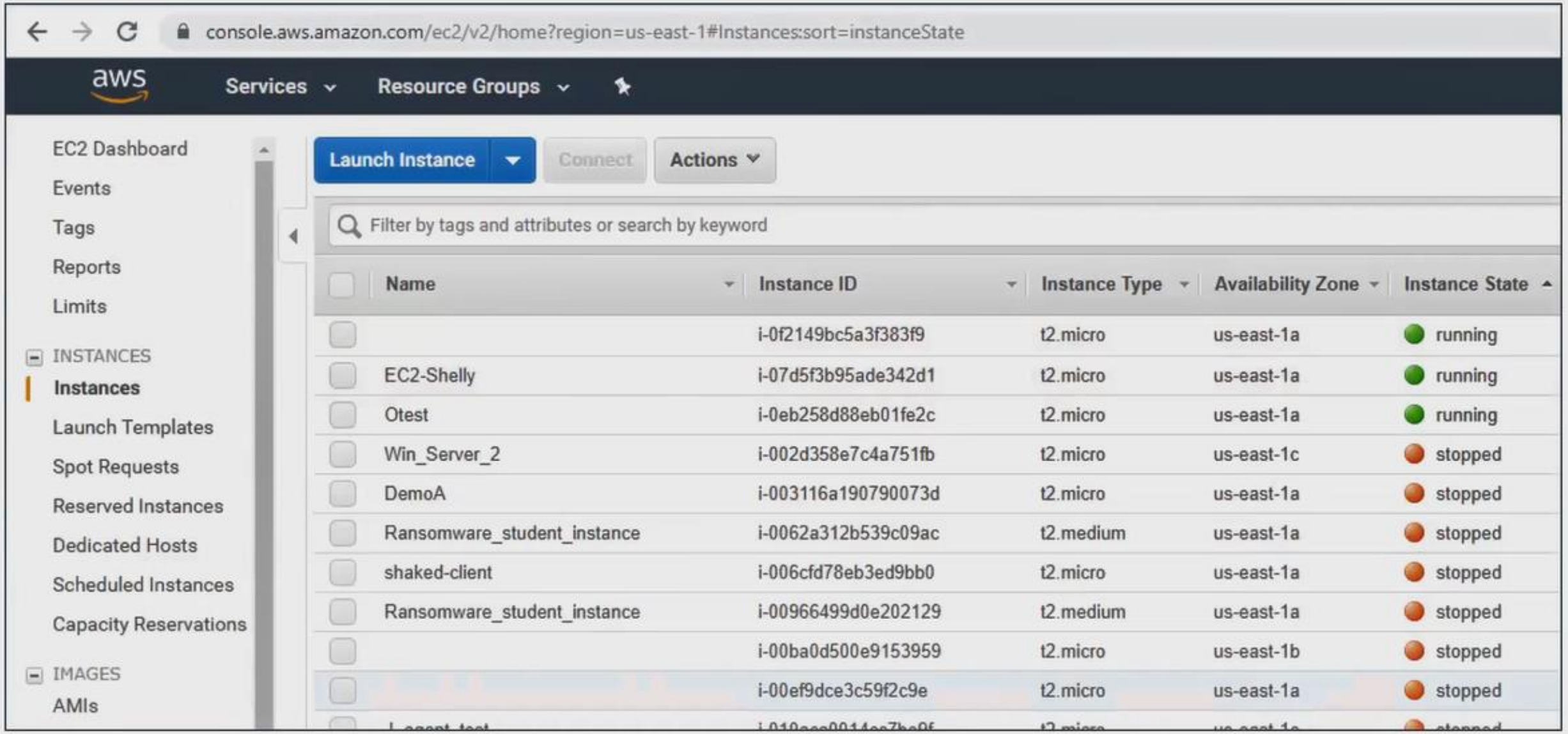
- Manage AWS Access Keys
- Manage Azure Service Principle
- Manage GCP Service Accounts
- Support developers and applications
  - AAM for development
  - Core PAS and AAM for key rotation management




ANDTGT01
CYBERARK
ATTACK & DEFEND
SERIES
Activate Windows

CREDENTIALS FROM THE CLOUD VM'S METADATA

AWS EC2 SERVICE – VIRTUAL MACHINES IN THE CLOUD

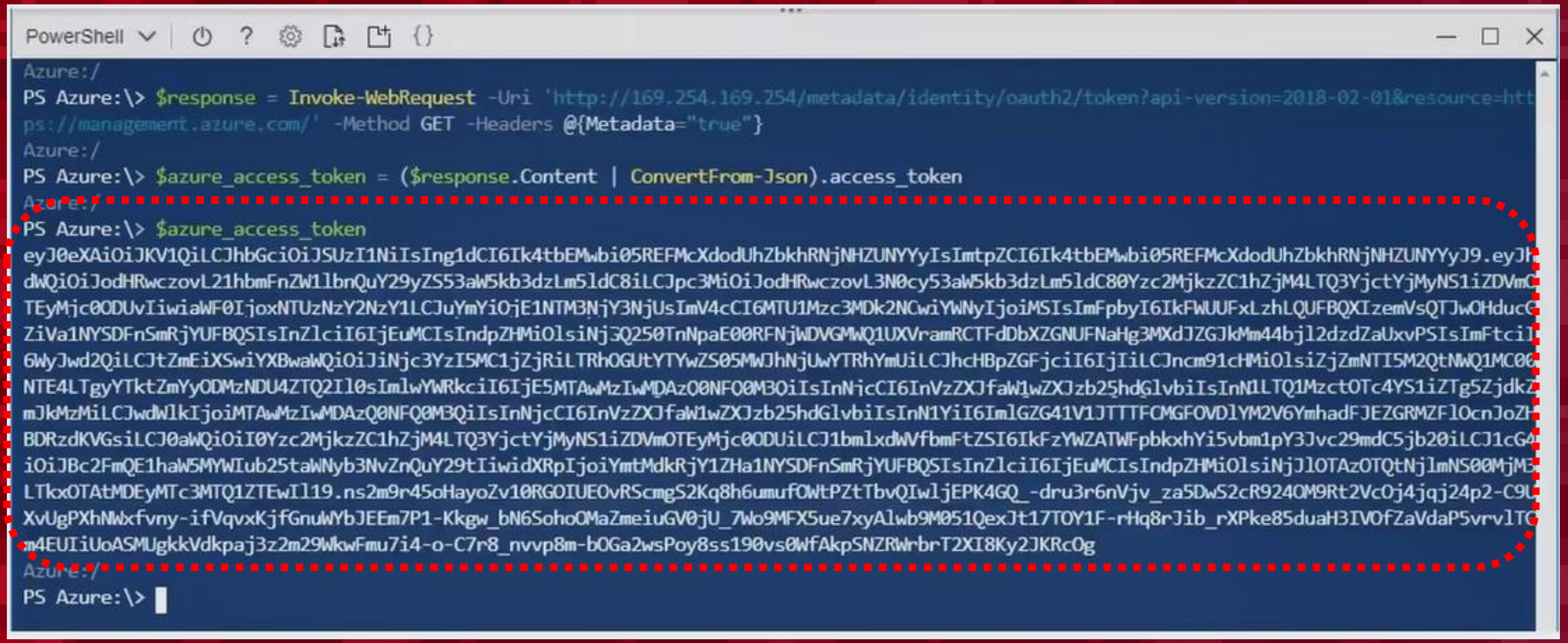


DEMO – RETRIEVING CREDS FROM EC2 INSTANCE'S METADATA

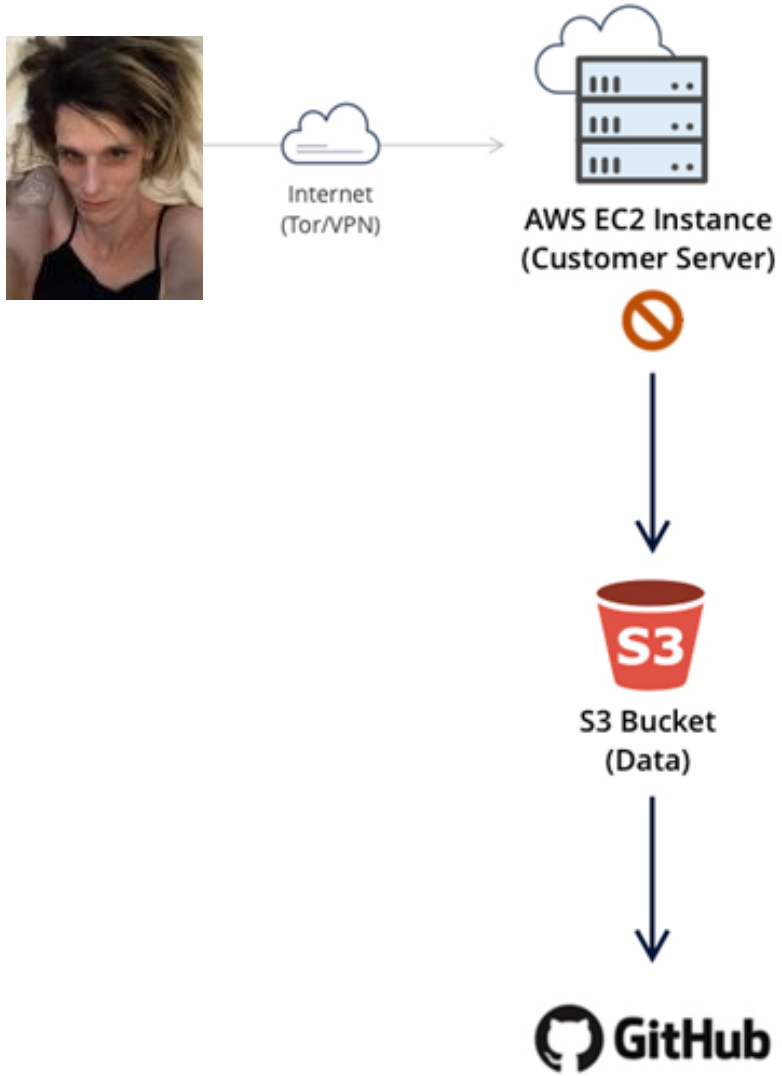
curl http://169.254.169.254/lates/meta-data/identity-credentials/ec2/security-credentials/ec2-instance


```
ec2-user@ip-172-31-62-19:~
[ec2-user@ip-172-31-62-19 ~]$ curl http://169.254.169.254/latest/meta
ity-credentials/ec2/security-credentials/ec2-instance
{                                                                    yint.net
  "Code" : "Success",
  "LastUpdated" : "2019-08-18T15:23:51Z",
  "Type" : "AWS-HMAC",
  "AccessKeyId" : "ASIAWDQ3G7DIK3COPLUB",
  "SecretAccessKey" : "mtqLIcssAtnxepcT7Wyc7UVOgF
  "Token" : "AgoJb3JpZ2luX2VjEOD//////////wEaCXVz
xNpzm1GVELEKwnIjBNyFTQH/hMELKAiA2cntKjkjPGsm0ZiCJbTkDT77MgIrPywKN9yO1k2//8iryAwh
5EAMaDDQxOTg5MDEzMzIwMCIMec7PvgeXyAIUyKJgKs8DwyL5TnxYdXG/pmNs/3CPs6ROqgx8CWGew6B
AbQazZNNdT38LYawOXKQVDws72SxUFWulP+xkaEcA3ZapGc9nAkpVhnZa/ZfbQy8aJm+uhmqvQPEZoHv
KYtwePV/MTzhMBoGYO5ZKGCKT+g1dyZr+B8kLL9lNSYm9DyaIly40YjvdIM7KpHbkqc7ghr6eYv06XS/
e+0YARWVcvViW6h3hKS+kumQWImPyiGVXyUJmY/Ay4XWflwClFGNmrplJ3VckR+adb8MGEbzr6gwyEWI
lLMe+IS5bbfZSx4Cz66OsciXQNCNa0eROCU5VYdTEuSIkV62LHlncfnQlZ5H1h6aG3MtxrqRE9iMhK5z
pkqnrg6mvpK8w6P45Prof1Vqc4Rh6kpq9OPFCVFnuBsOxiW0u8Ozli4+/WKhBGVMqQNEhn/Qz+Rxg2ga
4pTXbiStR3rDOkXJ/sxxOF2tNS3YZc+CQxNo9eUWVwXOlgOC3jq0TC50YFi24wSpaEF6
5yEeoYjYaRpGryc4Slv7oM4ynKX1SrXouQbOucc7CJ9i+Wg8Ci5DSd/Cpaod/tdDx5tN
RRwnIdYYp9pLeBl+maK2p3TDg2uXqBTq1Adxh5kPqpn5J5Akf1pORxvXyXKjIeqnMhqC
Ln0vUzEFI2/Mwy1wtVfy2XoNMtzMGJ+AeZOZHh4HxaJh4Jf+K9kr2/GQ67k0ff6uoA5N
+2q77hI/G/xOrBtEel+LEWtrCjmUnthauO6yHDWso8miORCzQvs7229hefadJY4+GScll
nFKV4citsNXRN1v35xh0vWXKTrDoJr2PbnC8=",
  "Expiration" : "2019-08-18T21:40:09Z"
}[ec2-user@ip-172-31-62-19 ~]$
```

EXAMPLE FROM AZURE

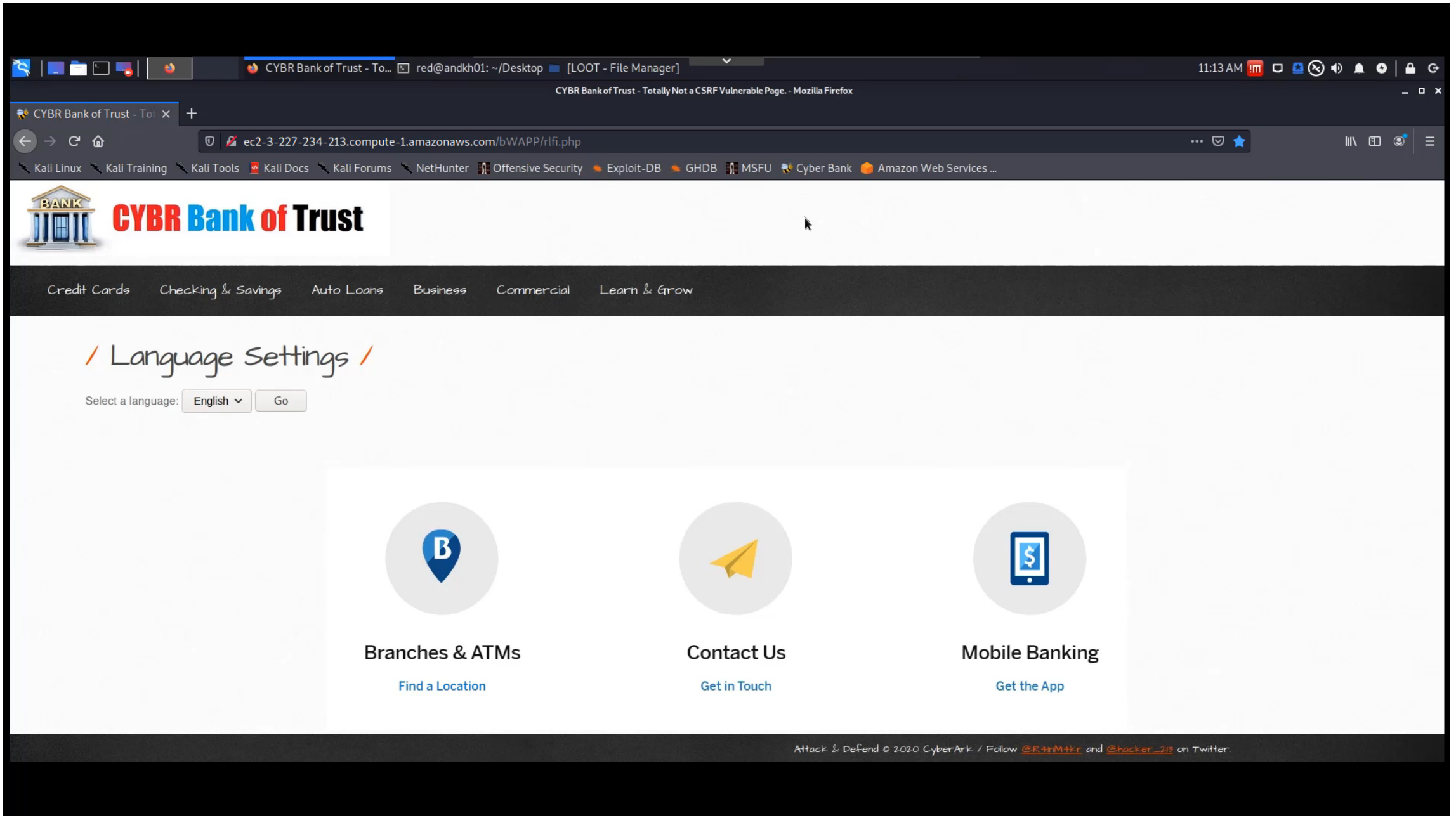


CAPITAL ONE DATA BREACH



1. Attacker's IP address allowed to connect. (Firewall misconfiguration)
2. Exploit SSRF vulnerability of NGINX.
3. Access EC2 instance metadata.

Stay tuned for **PART II…**


CYBR Bank of Trust - To...
red@andkh01: ~/Desktop
[LOOT - File Manager]
11:13 AM
CYBR Bank of Trust - Totally Not a CSRF Vulnerable Page. - Mozilla Firefox
CYBR Bank of Trust - To
ec2-3-227-234-213.compute-1.amazonaws.com/bWAPP/rlfi.php
Kali Linux
Kali Training
Kali Tools
Kali Docs
Kali Forums
NetHunter
Offensive Security
Exploit-DB
GHDB
MSFU
Cyber Bank
Amazon Web Services ...
BANK
CYBR Bank of Trust
Credit Cards
Checking & Savings
Auto Loans
Business
Commercial
Learn & Grow
/ Language Settings /
Select a language:
English
Go
Branches & ATMs
Find a Location
Contact Us
Get in Touch
Mobile Banking
Get the App
Attack & Defend © 2020 CyberArk / Follow @R4inM4kr and @hacker_213 on Twitter.

HOW CAN CYBERARK HELP?

- Application Development Best Practices
- IMS v2.0
- Restrict access to IMS via PSM.
- Least Privilege
- Updates and Patching

CLOUD MISCONFIGURATIONS AND SHADOW ADMINS

Cloud IAM services do not enforce Least Privileged policies

- Security and Operations lack consistent **cross-platform visibility.**
- Growing environments rapidly add permissions that **expand the attack surface.**
- **Unused and excessive** permissions that violate least privilege.
- **Incorrect configurations** expose to **higher risk**

According to a source with direct knowledge of the breach investigation, the problem stemmed in part from a misconfigured open-source Web Application Firewall (WAF) that Capital One was using as part of its operations hosted in the cloud with Amazon Web Services (AWS).

Known as "ModSecurity," this WAF is deployed along with the open-

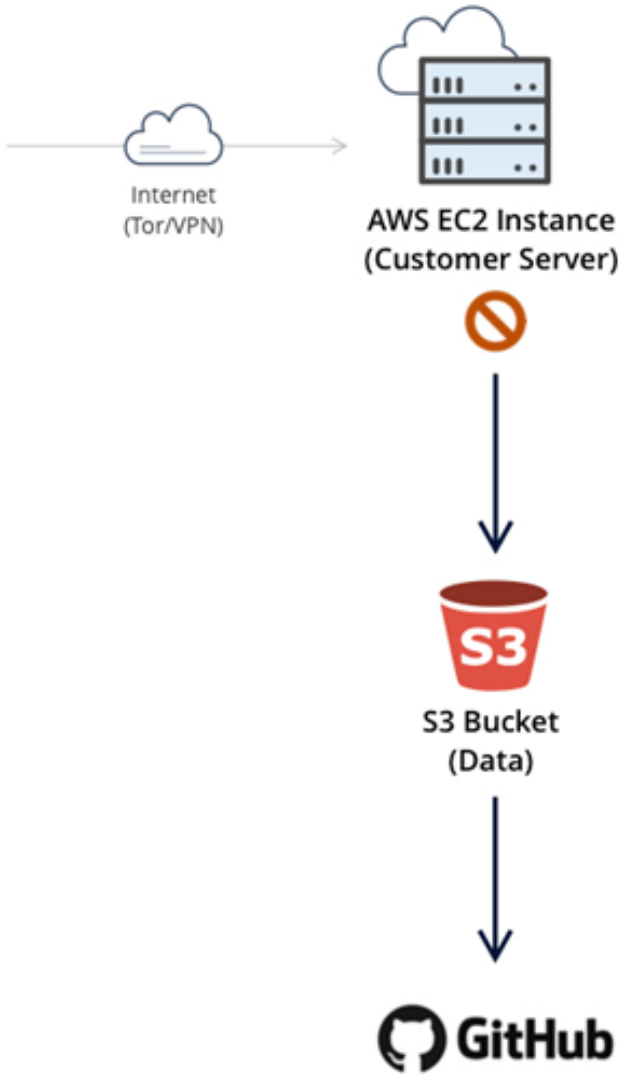
In AWS, exactly what those credentials can be used for hinges on the permissions assigned to the resource that is requesting them. In Capital One's case, the misconfigured WAF for whatever reason was assigned too many permissions, i.e. it was allowed to list all of the files in any buckets of data, and to read the contents of each of those files.

In AWS, exactly what those credentials can be used for hinges on the permissions assigned to the resource that is requesting them. In Capital One's case, the misconfigured WAF for whatever reason was assigned too many permissions, i.e. it was allowed to list all of the files in any buckets of data, and to read the contents of each of those files.

EXAMPLE

```
{
  "Name": "Storage Team Leader",
  "Id": null,
  "IsCustom": true,
  "Description": "Allows a Storage Team Leader to do his work",
  "Actions": [
    "Microsoft.Storage/*",
    "Microsoft.StorageSync/*",
    "Microsoft.Sql/managedInstances/databases/*",
    "Microsoft.DBforMySQL/servers/databases/*",
    "Microsoft.Authorization/roleAssignments/*"
  ],
  "NotActions": [],
  "AssignableScopes": [
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a"
  ]
}
```

CAPITAL ONE DATA BREACH



PART ONE

1. *Attacker's IP address allowed to connect. (Firewall misconfiguration)*
2. *Exploit SSRF vulnerability of NGINX.*
3. *Access EC2 instance metadata.*

PART TWO

1. Assumed Role *****-WAF-Role
   (Role Permission Misconfiguration)
2. Execute Commands:
   - ListBucket:
     This permission shouldn't be allowed for the WAF-Role
   - SyncBucket
     Last execution for that Role > 7 months.

A NEW LAYER OF PRIVILEGED USER

- Specific Permissions Create a Full Azure Admin User
- Control Other Privileged Users
- Hidden in Masses of Permissions and Users

BETTER SUITABLE PERMISSIONS FOR TEAM LEADER

```
{
  "Name": "Restricted Storage Team Leader",
  "Id": null,
  "IsCustom": true,
  "Description": "Allows a Storage Team Leader to do his work",
  "Actions": [
    "Microsoft.Storage/*",
    "Microsoft.StorageSync/*",
    "Microsoft.Sql/managedInstances/databases/*",
    "Microsoft.DBforMySQL/servers/databases/*",
    "Microsoft.Authorization/roleAssignments/*"
  ],
  "NotActions": [],
  "AssignableScopes": [
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourceGroups/Storage-Resource-Group",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourceGroups/Labs/providers/Microsoft.Storage/storageAccounts/storageaccount1",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourceGroups/Labs/providers/Microsoft.Storage/storageAccounts/storageaccount2",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourceGroups/Labs/providers/Microsoft.Storage/storageAccounts/storageaccount3",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourcegroups/Labs/providers/Microsoft.Sql/servers/sqlservername1/databases/sqldatabase",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourcegroups/Labs/providers/Microsoft.Sql/servers/sqlservername2/databases/sqldatabase",
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourcegroups/Labs/providers/Microsoft.DBforMySQL/servers/mysql1"
    "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a/resourcegroups/Labs/providers/Microsoft.DBforMySQL/servers/mysql2"
  ]
}
```

```
"AssignableScopes": [
  "/subscriptions/6ec6070a-ded3-41bc-9541-14954bd22c3a"
]
```

The original

HOW CAN CYBERARK HELP?

- **RBAC to AWS**
  - Reduces attack surface and easier management of roles.
- **Detection and onboarding with Privilege Threat Analytics**
  - AWS integration and management with EPV/PSM
- **Cloud Entitlements Manager**

CLOUD ENTITLEMENT MANAGER

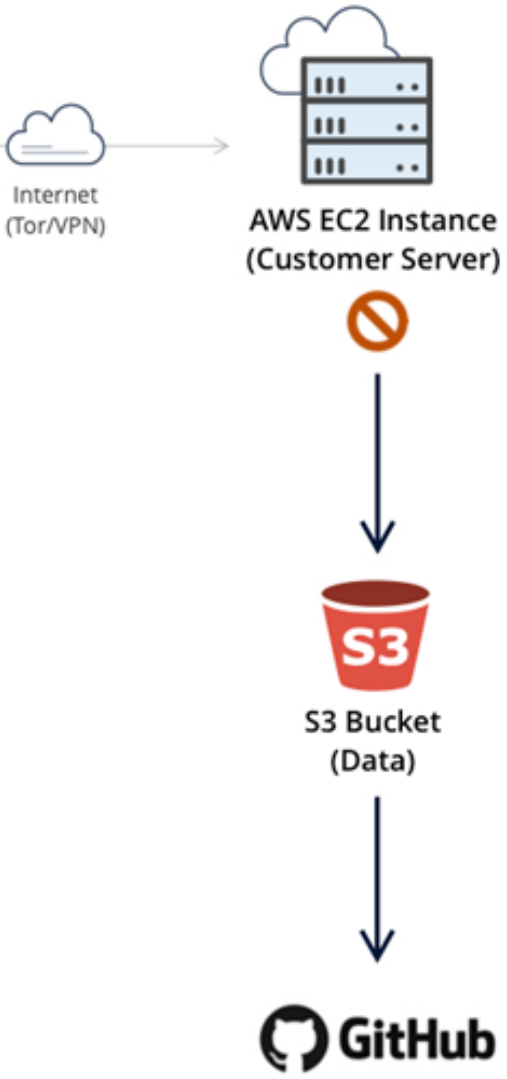
CEM a SaaS solution that reduces risk by implementing the Principle of Least Privilege in multi-cloud environments.

CEM centralizes visibility and control of permissions across an organization's cloud estate.

By:

- Analyzing granted permissions.
- Identifying unused and excessive permissions.
- Modeling exposure level.
- Actionable recommendations.
- Deployable remediations.

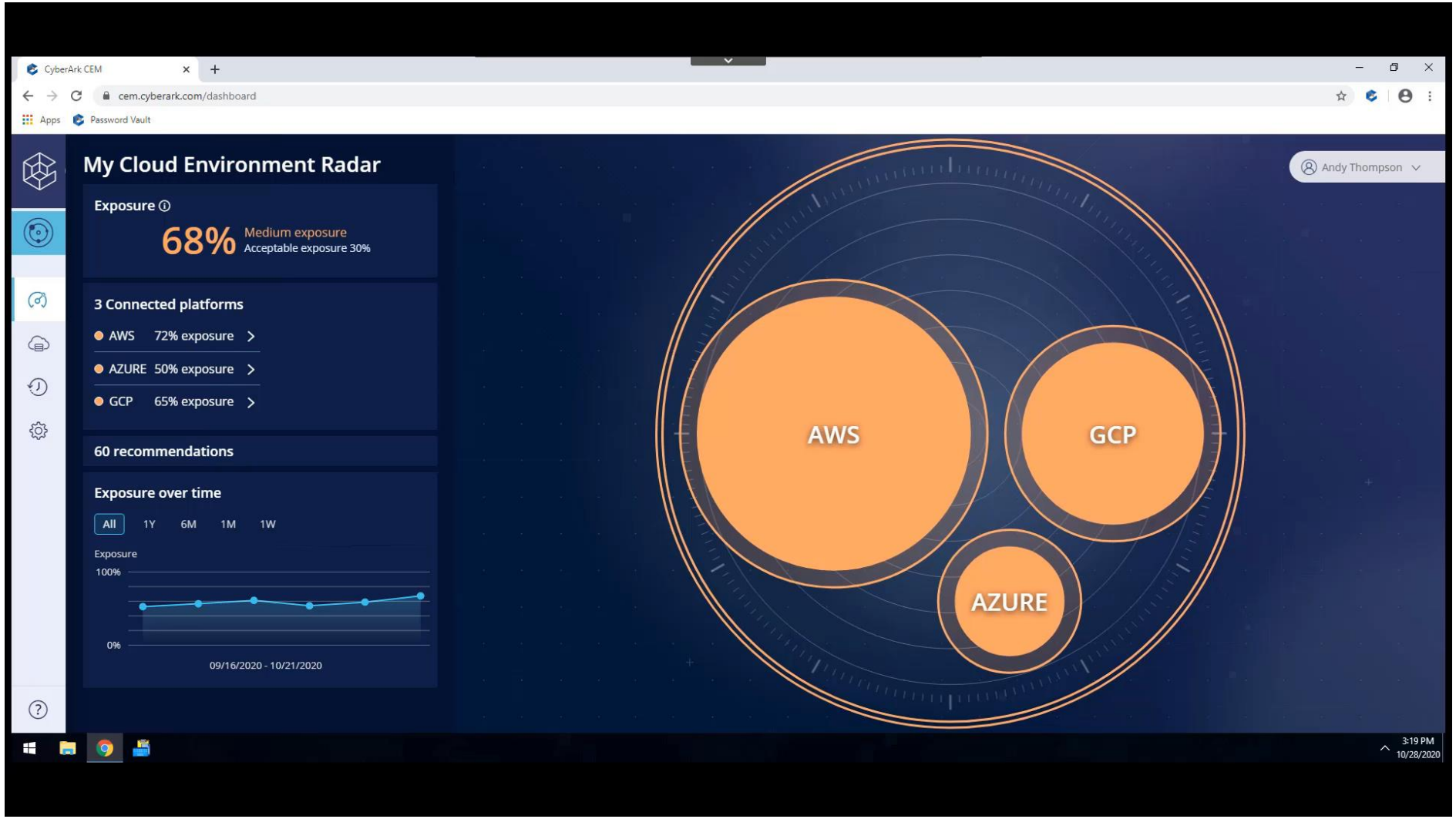
CAPITAL ONE DATA BREACH



1. Attacker's IP address allowed to connect (Firewall misconfiguration)
2. Assumed Role *****-WAF-Role **(Role Permission Misconfiguration)**
3. Execute Commands:
   - ListBucket:
     This permission shouldn't be allowed for the WAF-Role
   - SyncBucket
     Last execution for that Role > 7 months.

CyberArk can:

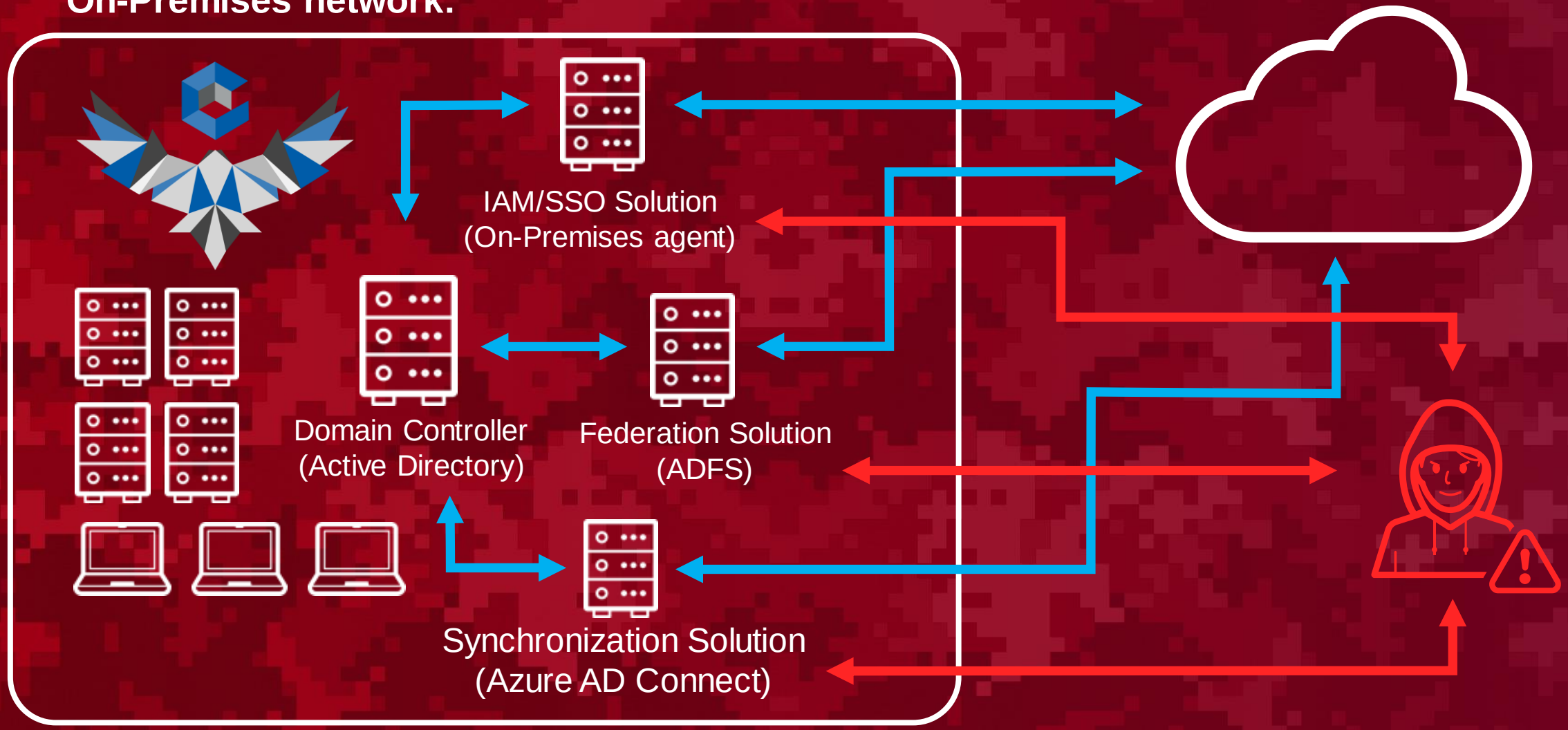
- Detect and Alert on excessive permission of the WAF-Role
- Clean up unused permissions
- Apply Least Privilege
- Block the attack early
- **With ZERO footprint and 5-minute setup.**

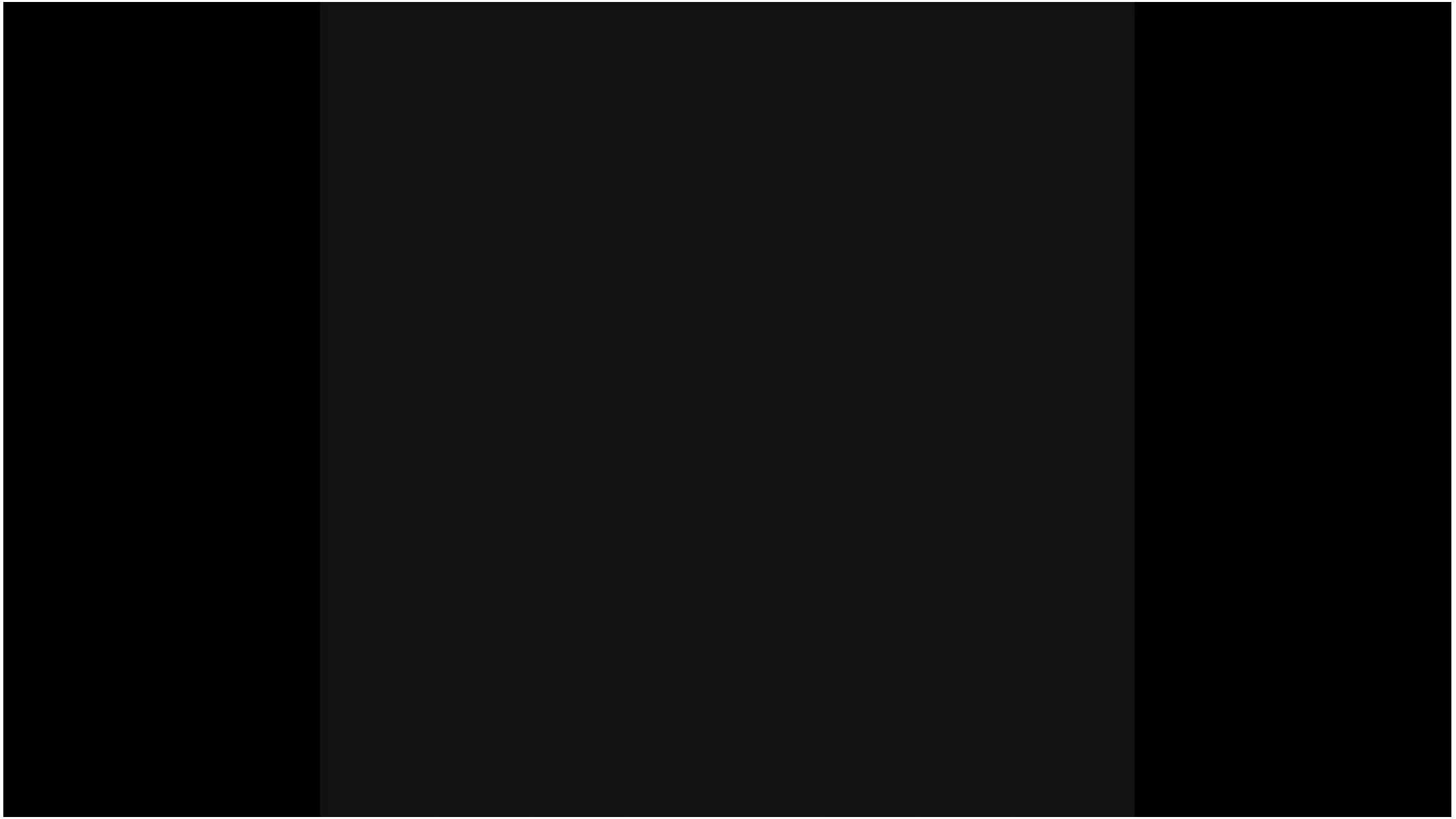

CyberArk CEM
cem.cyberark.com/dashboard
Apps
Password Vault
My Cloud Environment Radar
Andy Thompson
Exposure
68%
Medium exposure
Acceptable exposure 30%
3 Connected platforms
AWS 72% exposure
AZURE 50% exposure
GCP 65% exposure
60 recommendations
Exposure over time
All
1Y
6M
1M
1W
Exposure
100%
0%
09/16/2020 - 10/21/2020
AWS
GCP
AZURE
3:19 PM
10/28/2020

IAM AND FEDERATION SOLUTIONS TO THE CLOUD

TYPICAL HYBRID ORGANIZATION WITH IAM/SSO AND FEDERATION SOLUTION

On-Premises network:





HOW CAN CYBERARK HELP?

Enable CorePAS and EPM to protect against unauthorized privilege access and sophisticated attacks like Golden SAML.

SUMMARY: CLOUD ATTACKS

Cloud adoption is growing

No Zero-Days

Real Attack Scenarios

SUMMARY: CLOUD DEFENSE

Privilege is everywhere.

There is NOTHING new.

Follow the Blueprint.

PREVENT CREDENTIAL THEFT

STOP LATERAL & VERTICAL MOVEMENT

LIMIT PRIVILEGE ESCALATION & ABUSE

ON PREMISES — **HYBRID** — **CLOUD**

Risk based program designed to secure privileged access across all environments

SUMMARY: USING CYBERARK TO SECURE THE CLOUD

CYBERARK CAPABILITIES BY PLATFORM

	aws	Azure	Google Cloud Platform	Solution Examples
Console security	✓	✓	✓	PAS
Secure CLI	✓	✓	✓	PAS
IAM management	✓	✓		PAS
API Key Management	✓	✓		PAS
Onboarding w/ REST APIs	✓	✓	✓	PAS
Automatic Integrated Onboarding	✓			PAS
Secrets Mgmt.	✓	✓	✓	Conjur
Container Security	✓	✓	✓	PAS, OPM, Conjur

RED TEAM RESOURCES

Interested in learning more from the "Attacker" mindset?

- Red Team Services & Engagements
  - Red Team Customized TTP Sessions
- Participate in future virtual Attack & Defend events
- Check out our CyberArk Threat Research blog for the latest from our CyberArk Labs team

BLUE TEAM RESOURCES

Interested in learning more from the "Defender" mindset?

- Schedule a Blueprint Deep Dive session
- Privileged Risk Analysis
- Try our free trials!

Cloud Entitlements Manager
Endpoint Privilege Manager
CyberArk Alero

QUESTIONS?

THANK YOU.