ALTERED SECURITY

Abusing Azure VMs:

When BitLocker Recovery Turns into an Attack Vector.

(Part of Altered Security Month of Azure Red Teaming 2026)

`whoami /all`

Hitesh Duseja (Twitter/X - @itsyobroda)

- Security Researcher @ Altered Security.
- Strong passion for Enterprise Cloud Security, and Red Teaming.
- Overall 7.5+ years of hands-on experience.
- Original research in Intune (now part of our Azure courses) and Hybrid Identity (not yet Public).

Altered Security

- Trained more than 50000 security professionals from more than 130 countries!
- Our Red Team Labs Platform enables labs to be:
  - Affordable
  - Easy to Access
  - Stable and provide great user experience
  - Fun to Solve
  - Big enough to feel enterprise-like

Red team labs	alteredsecurity.com/online-labs
Instructor-led bootcamps	alteredsecurity.com/bootcamps
GitHub	github.com/AlteredSecurity
Lab Platform	enterprisesecurity.io
Free Labs and Challenges	redlabs.enterprisesecurity.io

ALTERED SECURITY

Mission, Vision and Core Values

- Our Mission is to enable skill development of Red Team, Cloud Security and Security skills through practical way of learning, so that we can fulfil our vision of building a diverse global community of expert professionals who can take over the task of handling latest challenges in the Information Security industry.

- Our Core Values:
  - High Quality
  - Innovation
  - Empathy
  - Giving Back (This is why we have all gathered today in this webinar)

ALTERED SECURITY

What is Month of Azure Red Teaming(MoART)?

- We have observed that there is a lack of awareness about Azure and Entra ID Threat landscape. When Red Teaming is used in infosec discourse, it is usually limited to on-prem environments.

- Month of Azure Red Teaming is our way to bring a change by having meaningful discussions around Azure.

- It is absolutely not necessary to spend 1000s of $ to learn red teaming in Azure and Entra ID. For that, our Red Labs (https://redlabs.enterprisesecurity.io) are there to help you out.

Webinar Ground Rules

- You can ask questions on redlabs channel (#redlabs) on our Discord server (https://discord.com/invite/vcEwaRMwJe). We won't be able to monitor Zoom Chat.

- The lab will be made available to all users on the Red Labs platform for practice tomorrow (11th April 2026), so there is no follow along.

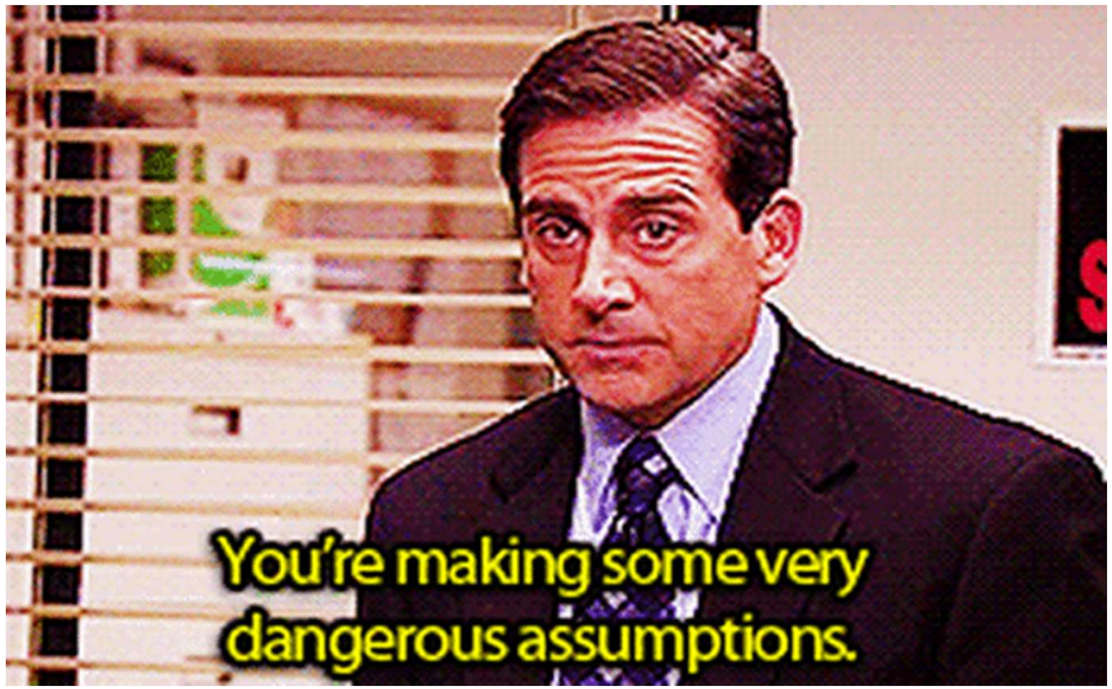
- To ensure a smooth experience, participants are not allowed to use their microphone.

- Please maintain professional conduct and a respectful atmosphere throughout the webinar.

ALTERED SECURITY

Assumptions

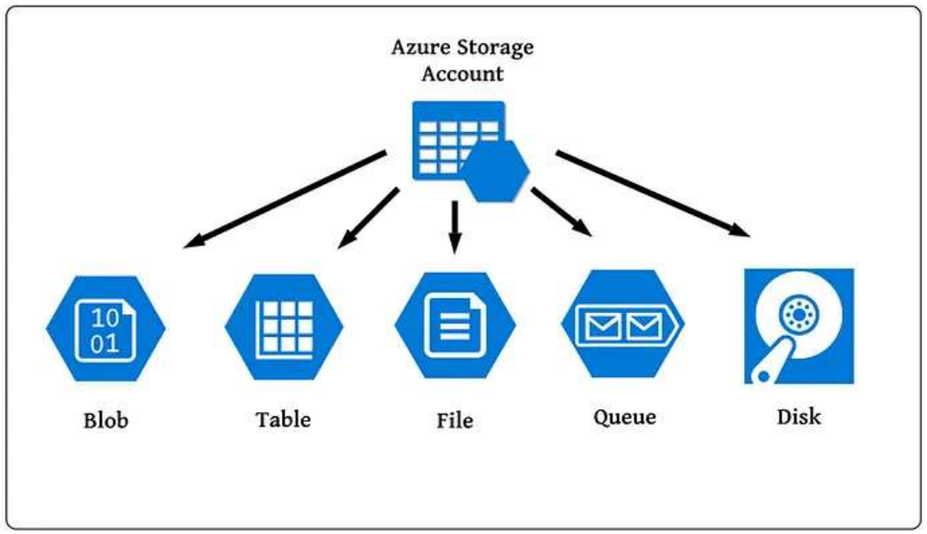
This webinar session assumes that the participant knows about the basics of Entra ID and Azure, both part of Microsoft's Cloud ecosystem.



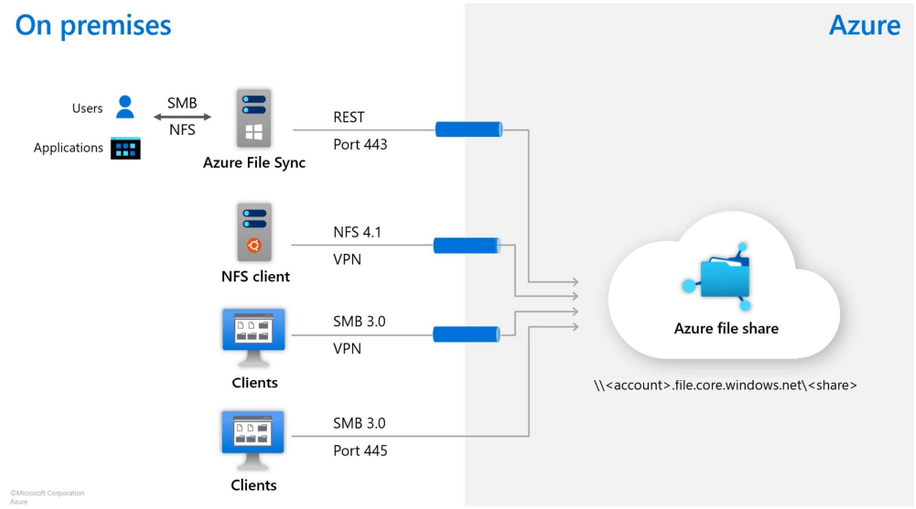
ALTERED SECURITY

Before we go any further,

Azure Storage Concepts



Source: https://miro.medium.com/v2/resize:fit:720/format:webp/0*QVoXPjNcmG-v5--n.png



Source: https://www.youtube.com/watch?v=MJEbmITLwwU

Source: https://www.youtube.com/watch?v=gPqD2P27pes

Today's Webinar Topic

- Our topic for today is about abusing VM via its Disk snapshots.

- To perform the abuse, we are shedding light on one of the lesser known features in Microsoft Entra ID, which is its capability to store BitLocker Keys. The use case is to support recovery or migration.

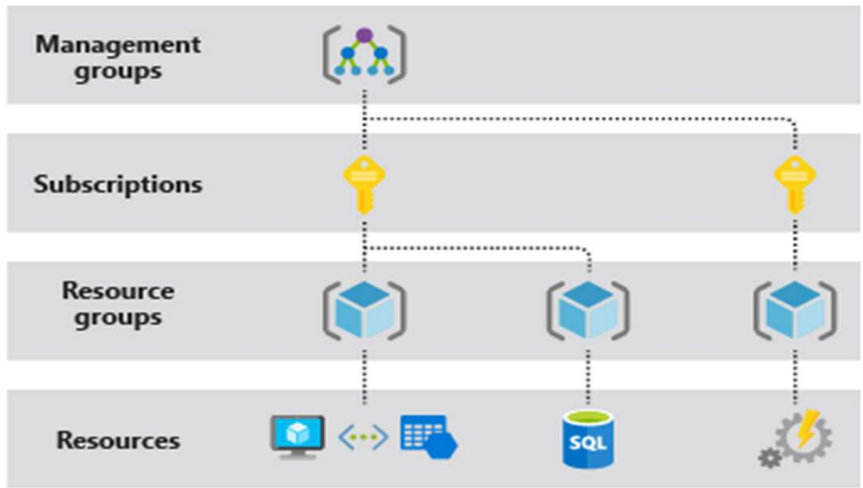
- Our attack path, thus will involve obtaining the BitLocker key of a device, using it to unlock Disk Snapshot, reading contents of the disk and finally, getting access to other Azure services, using certain tokens which the user of the VM has unknowingly left in it.

Lab Scenario

- Our lab scenario is that we are hired to do a Grey Box security assessment by a Fortune 500 organization that has hybrid infrastructure.

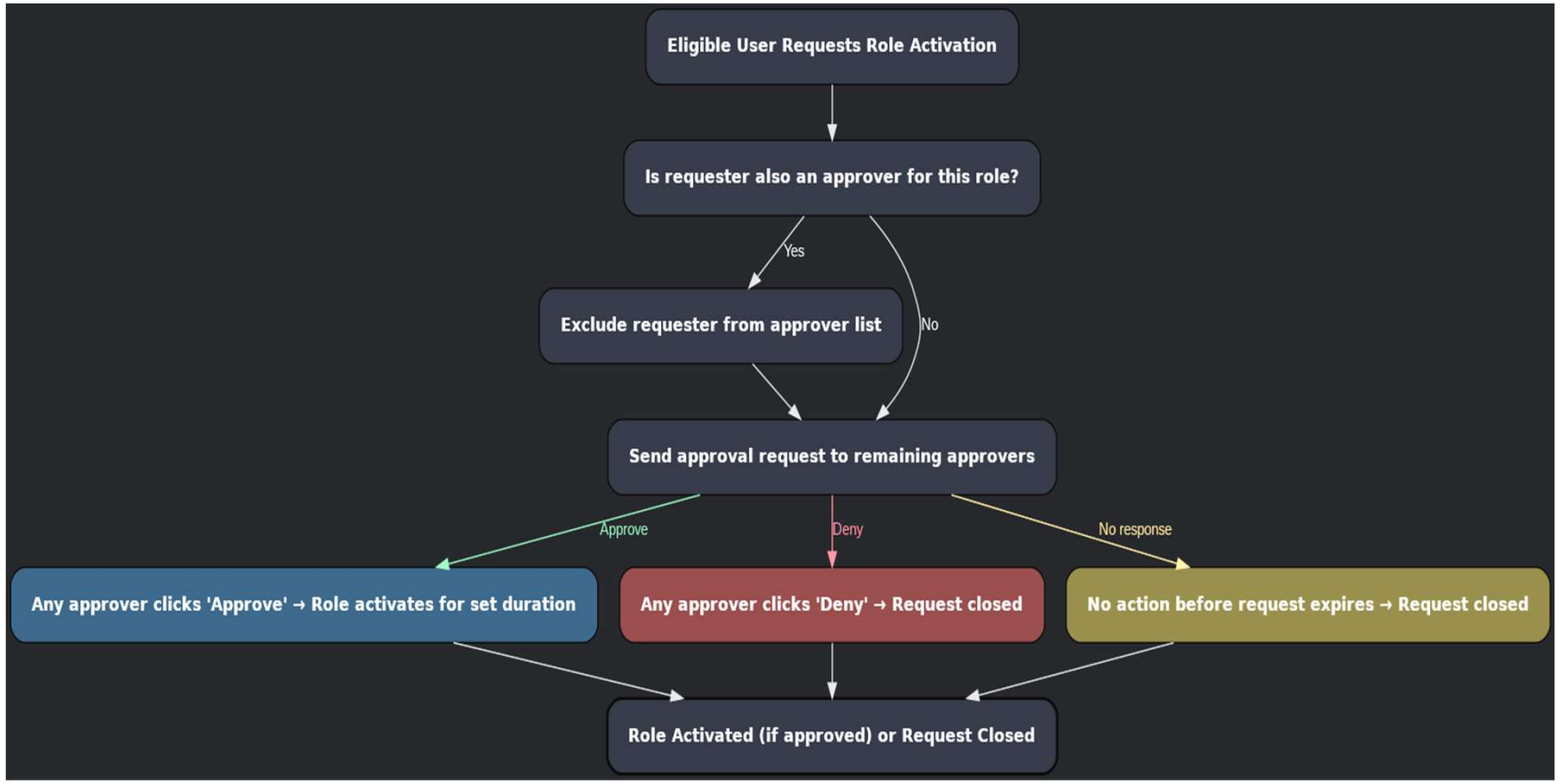
- Therefore as part of standard prerequisites, we have requested to provide us the Reader access at the subscription level.

- But since the scope that customer wanted us to assess was smaller, they have given equivalent access to one of their employees.




IT'S
DEMO TIME!

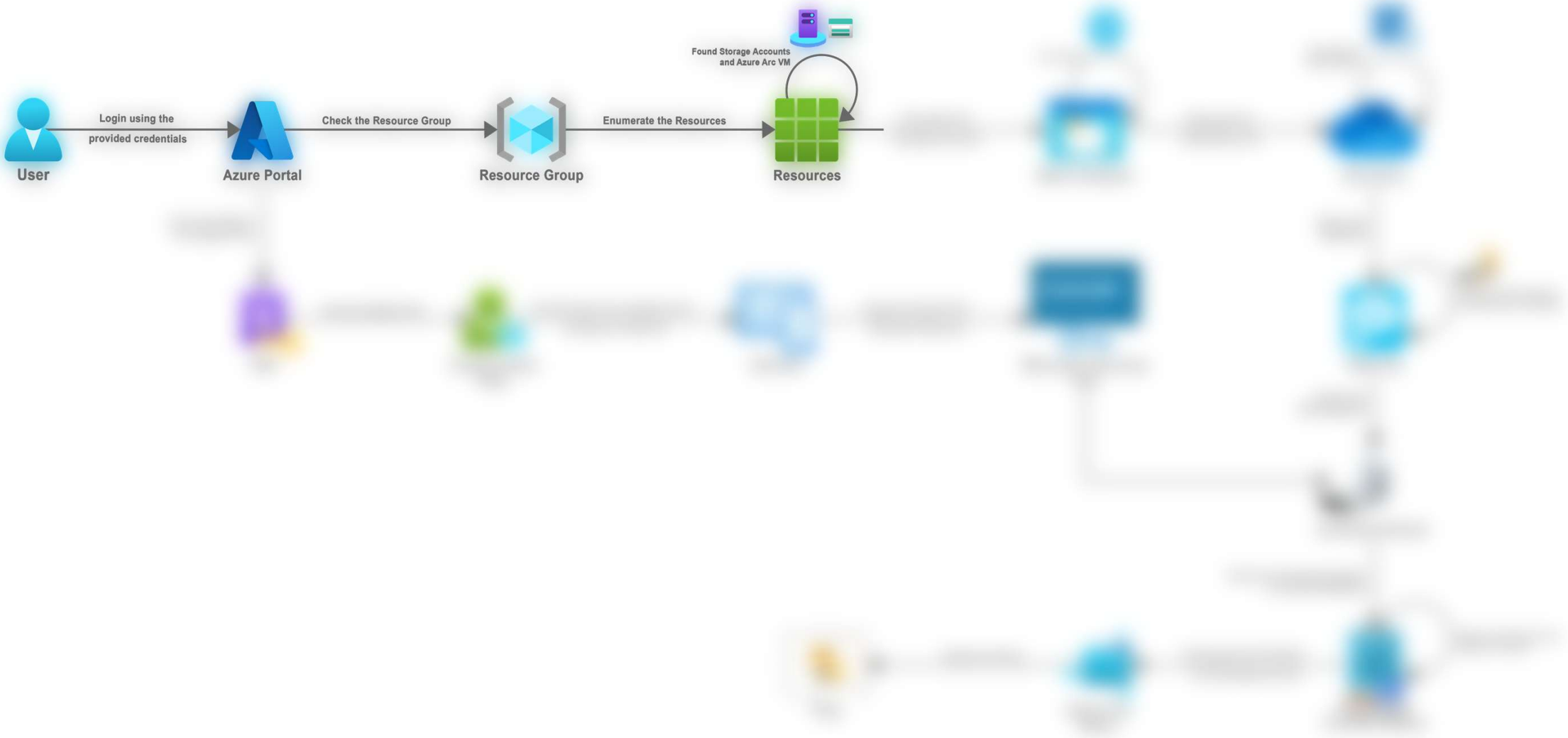
Privilege Identity Management

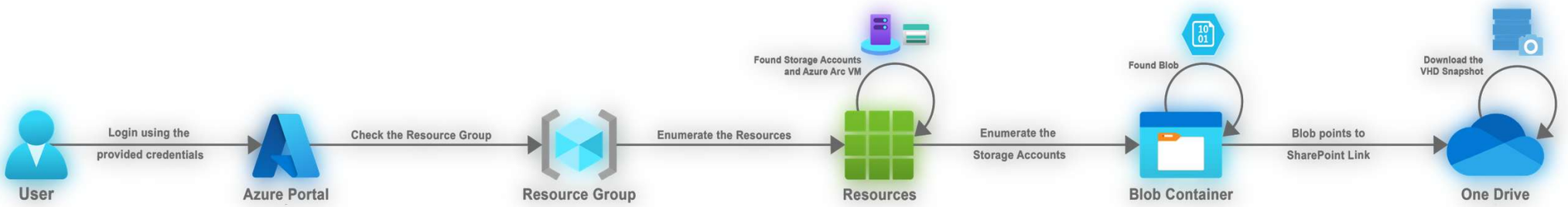


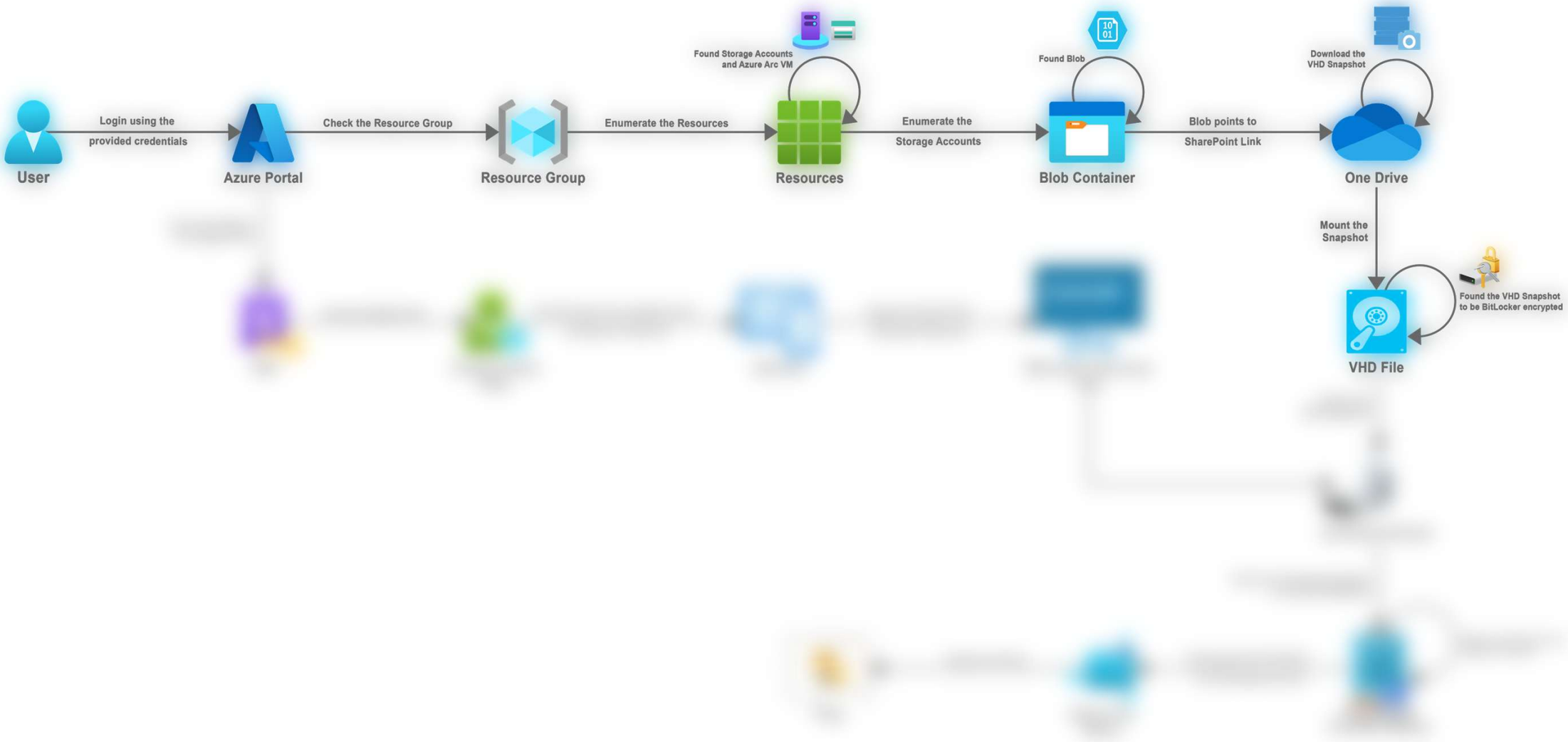
Source: https://images.squarespace-cdn.com/content/v1/687e9fc9122fdd14378717da/a726c218-f116-4ed8-9d2f-2377d45869a3/pim_approval_flow_darkgrey_friendly.png

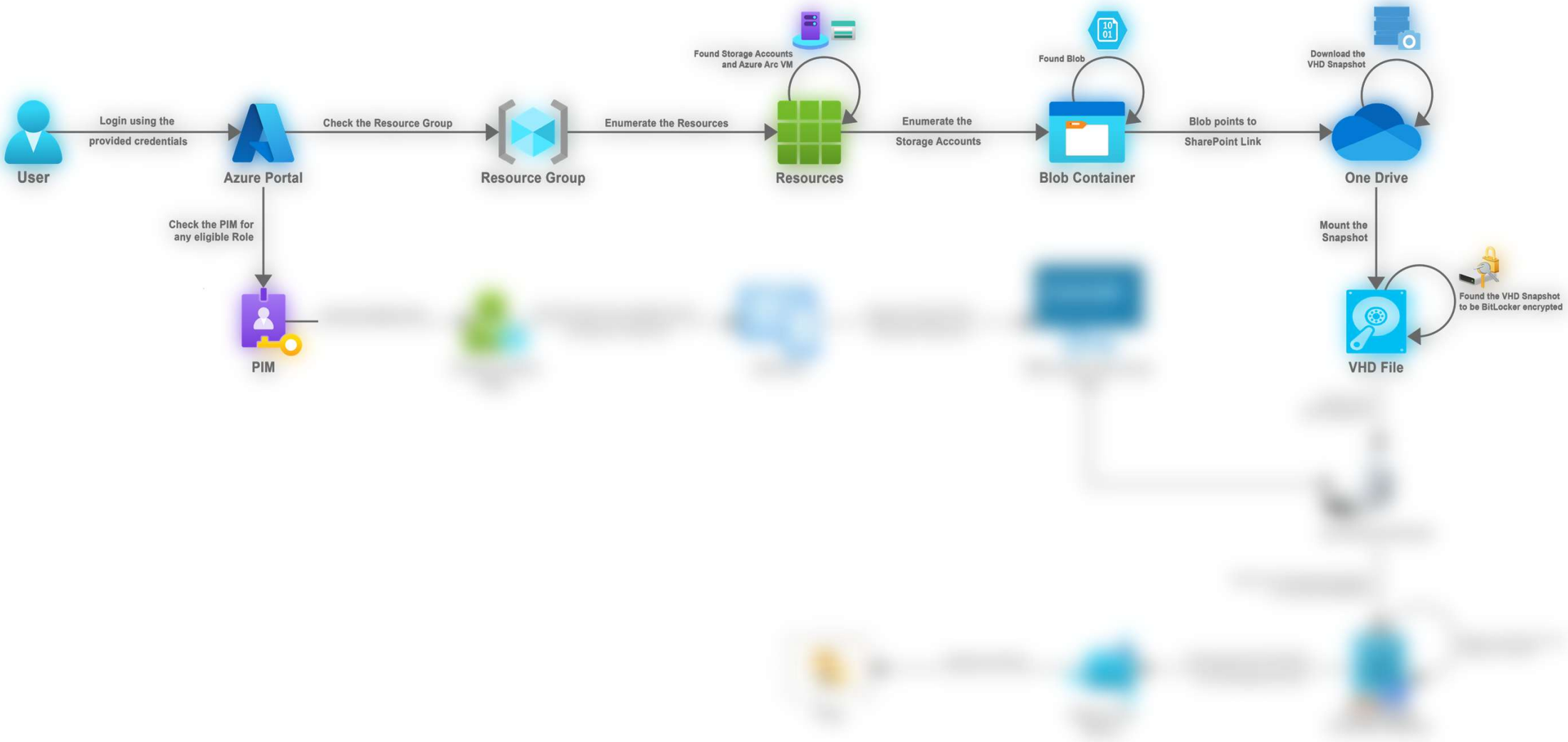

RECAP
TIME IT IS

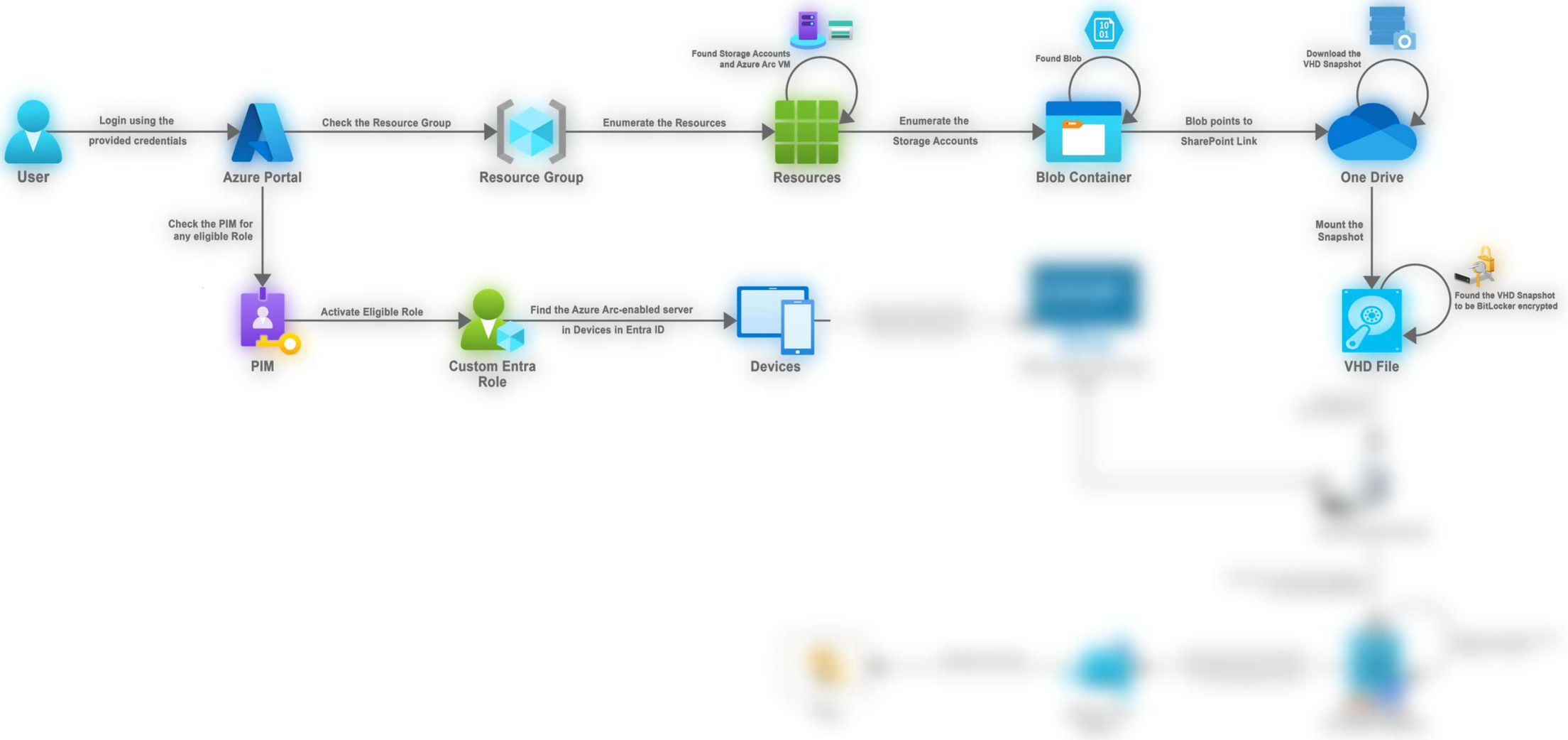

Login using the
provided credentials
User
Azure Portal

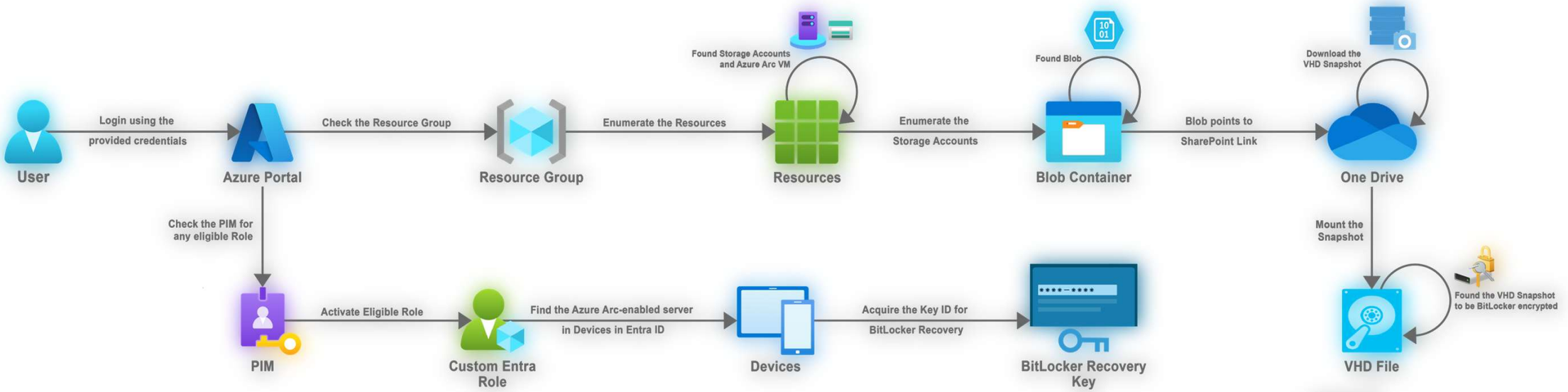

Found Storage Accounts
and Azure Arc VM
Login using the
provided credentials
Check the Resource Group
Enumerate the Resources
User
Azure Portal
Resource Group
Resources


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive

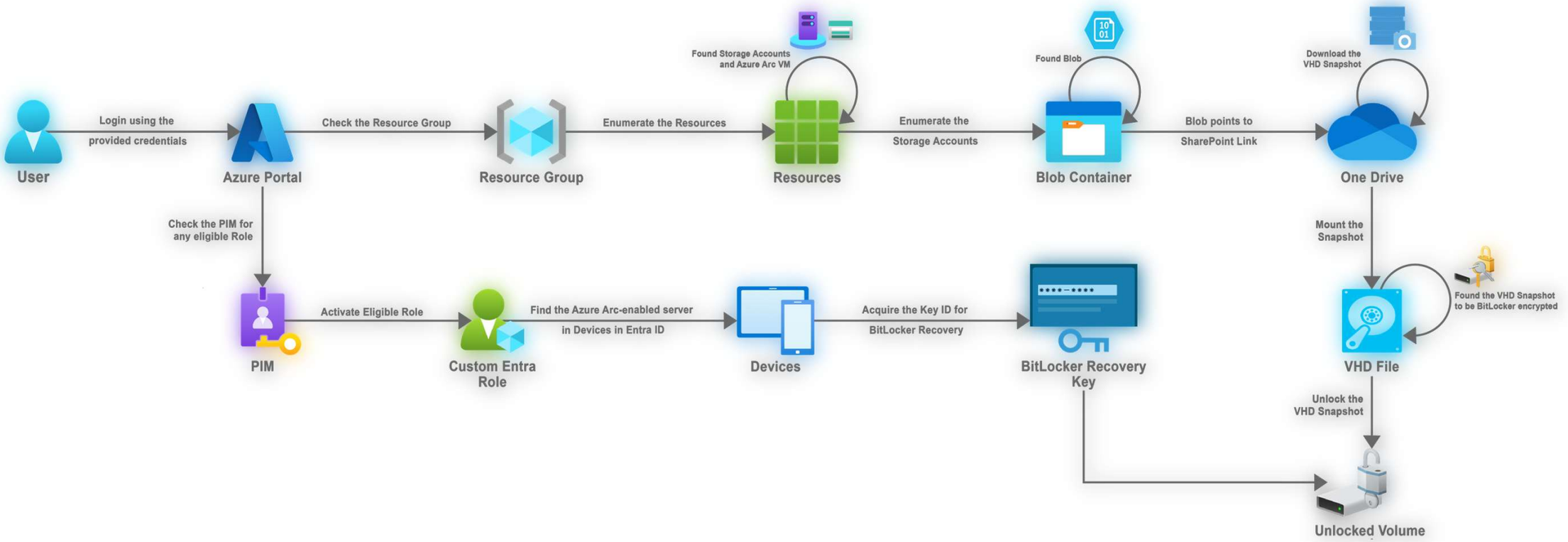

User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive
Mount the
Snapshot
Found the VHD Snapshot
to be BitLocker encrypted
VHD File


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive
Check the PIM for
any eligible Role
PIM
Mount the
Snapshot
Found the VHD Snapshot
to be BitLocker encrypted
VHD File

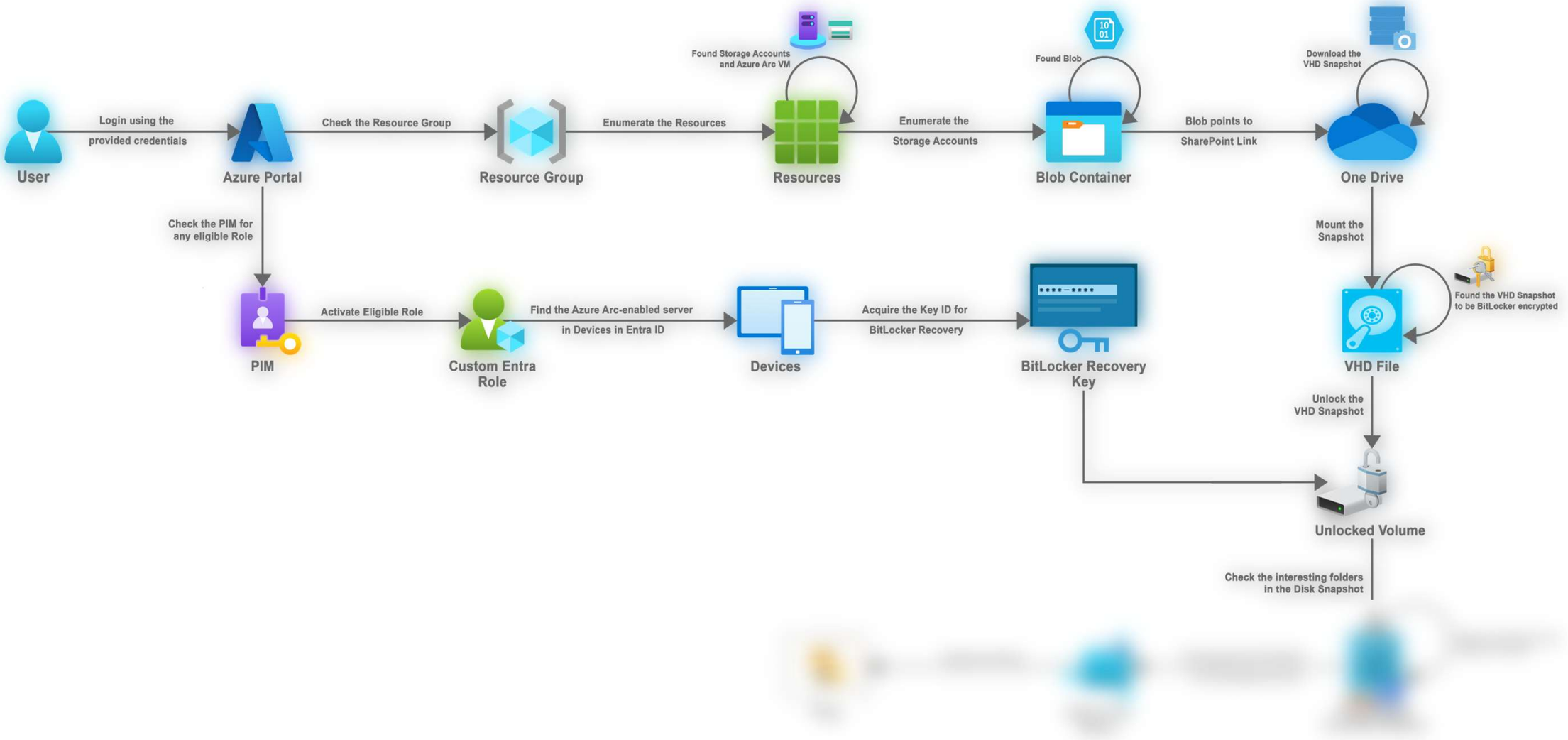

Login using the
provided credentials
User
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive
Check the PIM for
any eligible Role
PIM
Activate Eligible Role
Custom Entra
Role
Find the Azure Arc-enabled server
in Devices in Entra ID
Devices
Mount the
Snapshot
Found the VHD Snapshot
to be BitLocker encrypted
VHD File

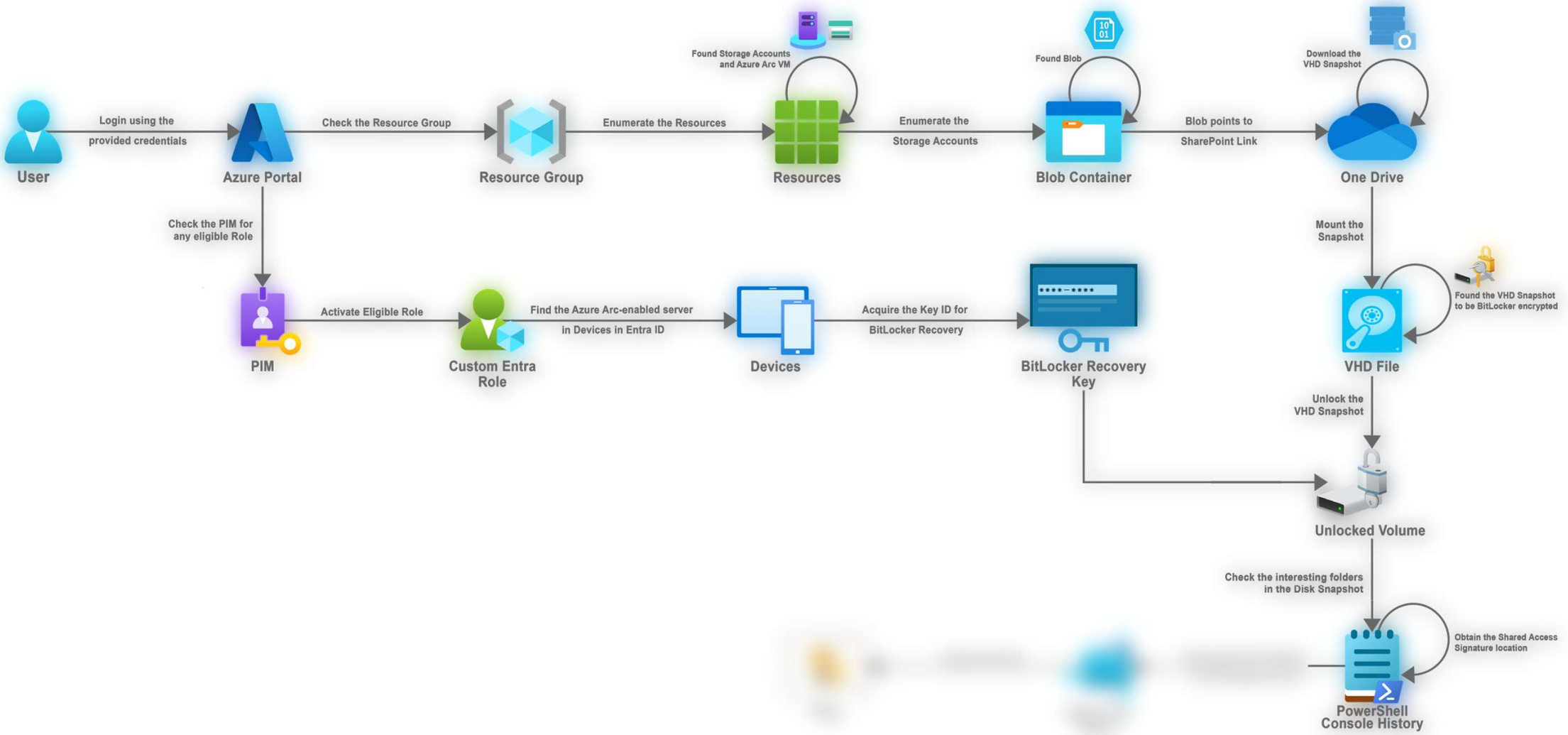


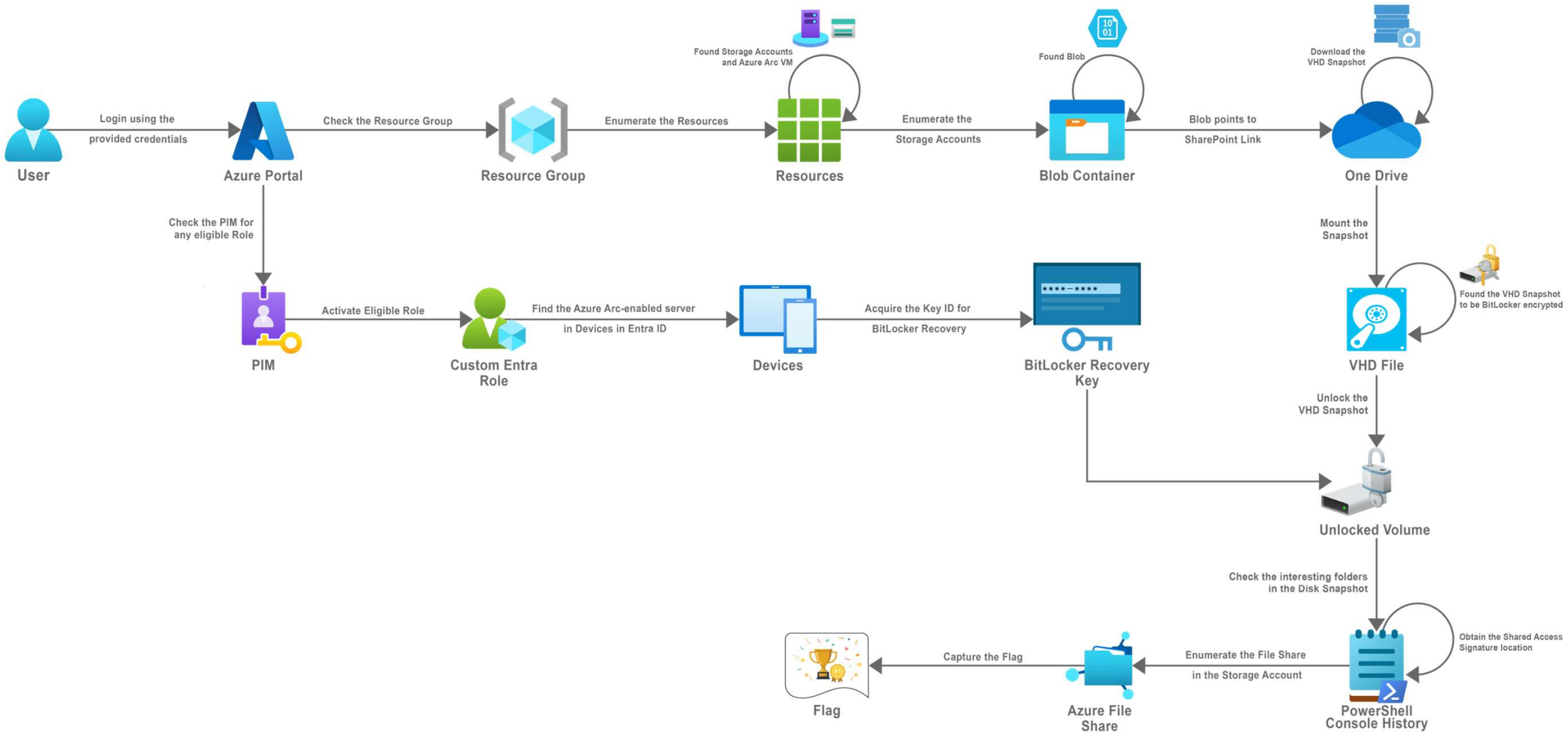
AlteredSecurity



AlteredSecurity


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive
Check the PIM for
any eligible Role
PIM
Activate Eligible Role
Custom Entra
Role
Find the Azure Arc-enabled server
in Devices in Entra ID
Devices
Acquire the Key ID for
BitLocker Recovery
BitLocker Recovery
Key
Mount the
Snapshot
Found the VHD Snapshot
to be BitLocker encrypted
VHD File
Unlock the
VHD Snapshot
Unlocked Volume
Check the interesting folders
in the Disk Snapshot


User
Login using the
provided credentials
Azure Portal
Check the Resource Group
Resource Group
Enumerate the Resources
Found Storage Accounts
and Azure Arc VM
Resources
Enumerate the
Storage Accounts
Found Blob
Blob Container
Blob points to
SharePoint Link
Download the
VHD Snapshot
One Drive
Check the PIM for
any eligible Role
PIM
Activate Eligible Role
Custom Entra
Role
Find the Azure Arc-enabled server
in Devices in Entra ID
Devices
Acquire the Key ID for
BitLocker Recovery
BitLocker Recovery
Key
Mount the
Snapshot
Found the VHD Snapshot
to be BitLocker encrypted
VHD File
Unlock the
VHD Snapshot
Unlocked Volume
Check the interesting folders
in the Disk Snapshot
Obtain the Shared Access
Signature location
PowerShell
Console History



AlteredSecurity

Bonus Demo

ALTERED SECURITY

Mitigations

- Limit access to users, who are capable of reading BitLocker keys, especially device owners for their own devices.
- Put approval process behind PIM activation as part of access reviews for all Entra roles capable of reading BitLocker Recovery keys.
- Don’t store sensitive data in Windows Temp folder as it can very well stay consistent even across reboots.
- Snapshots or any sensitive data stored should never be behind world readable access URLs.

For other premium red team labs:
https://www.alteredsecurity.com/online-labs

For bootcamps:
https://www.alteredsecurity.com/bootcamps

Join us at Discord -
https://discord.com/invite/vcEwaRMwJe