I Get Paid To Hack Your Company and These Are The Controls I Hate Most!

Carlos García & Jeff Macko

June 14, 2022

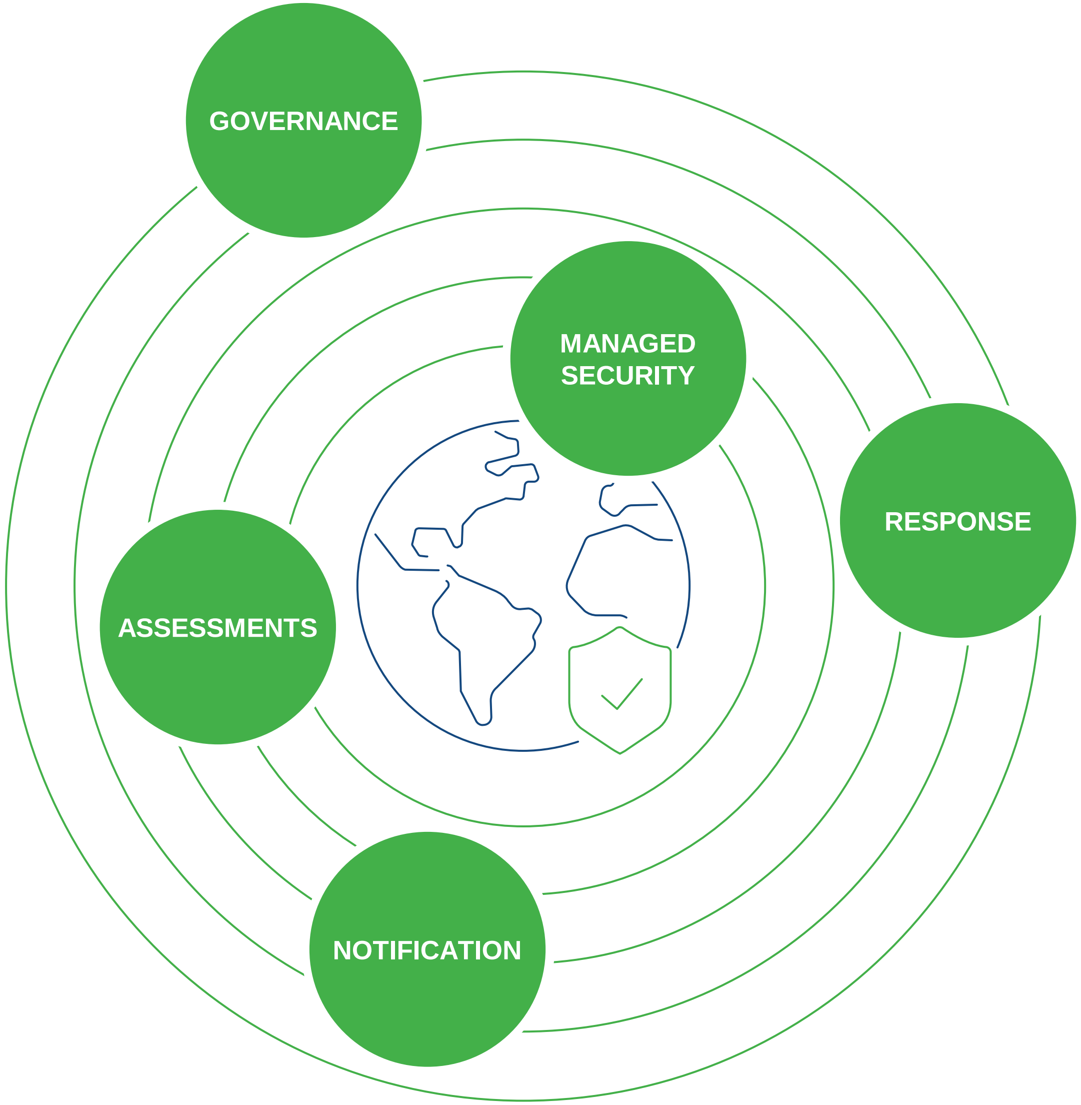
By The Numbers

3,200+
ENGAGEMENTS IN 2021

550+ PRACTITIONERS
ACROSS 18 COUNTRIES

FORTUNE 100 TO MEDIUM-SIZED BUSINESSES

WORKING WITH **60+** CYBER INSURANCE CARRIERS



Carlos García

Background

Carlos specializes in conducting penetration tests and vulnerability assessments against large, multinational / multi-site companies, with special focus on Active Directory environments.

Senior Vice President

Madrid, Spain

Jeff Macko

Background

Jeff leads Kroll's penetration testing services team in the US. He has over 30 years of experience in IT systems design, implementation, and management for a wide variety of industries with substantial experience in financial services, biotechnology, software development and e-commerce.

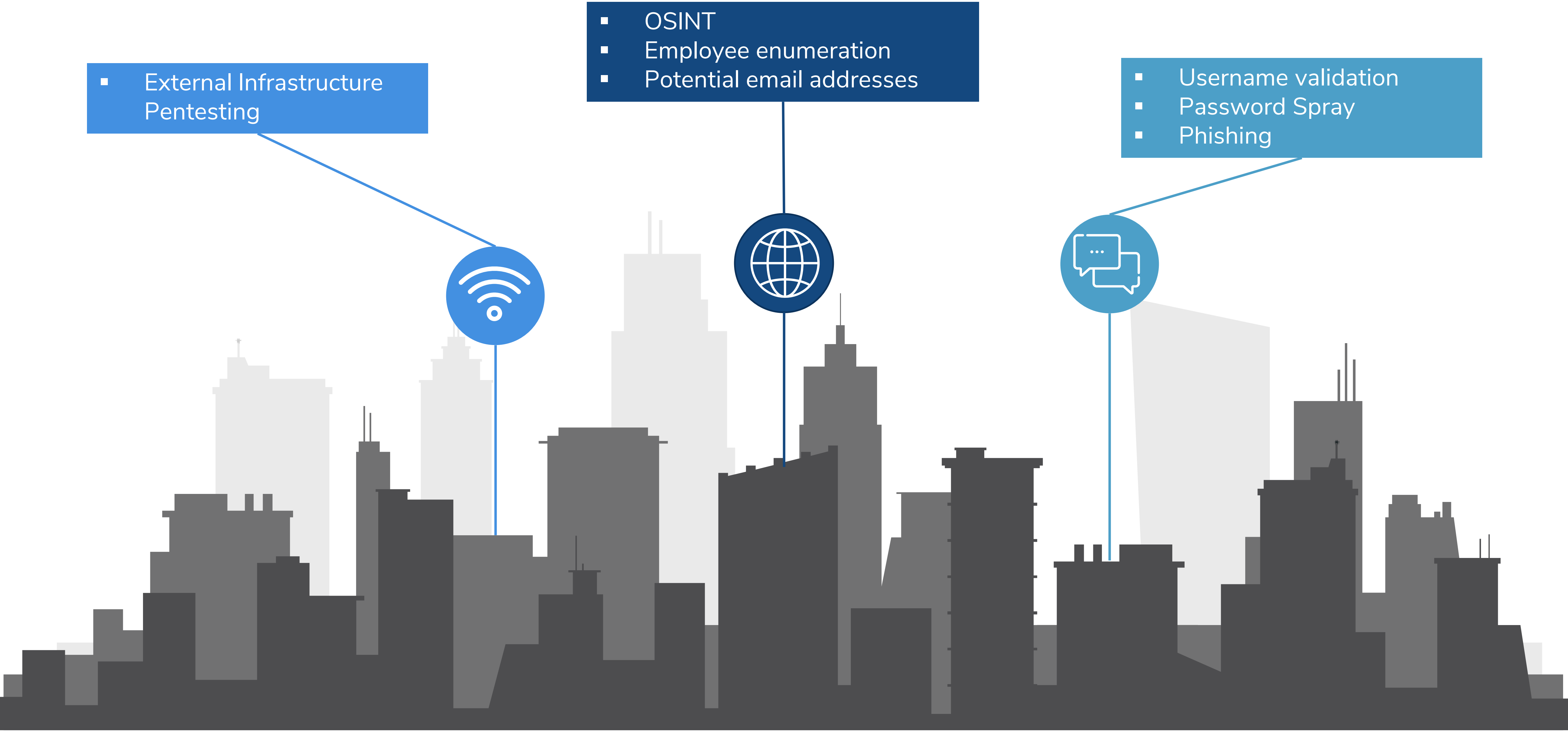
Associate Managing Director

North Carolina, USA

Today's Agenda

- Common External Attacks and Controls
- Common Internal Attacks and Controls

Common External Attacks and Controls

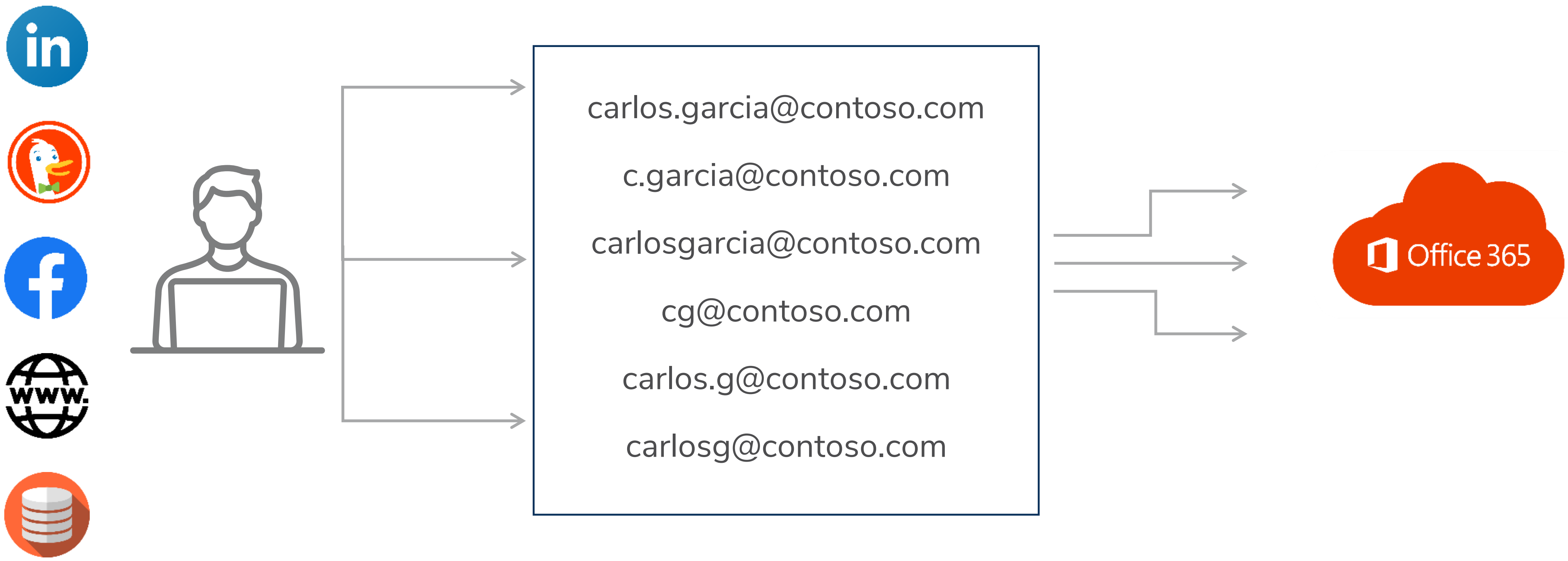


- External Infrastructure Pentesting

- OSINT
- Employee enumeration
- Potential email addresses

- Username validation
- Password Spray
- Phishing

Username Validation



carlos.garcia@contoso.com

c.garcia@contoso.com

carlosgarcia@contoso.com

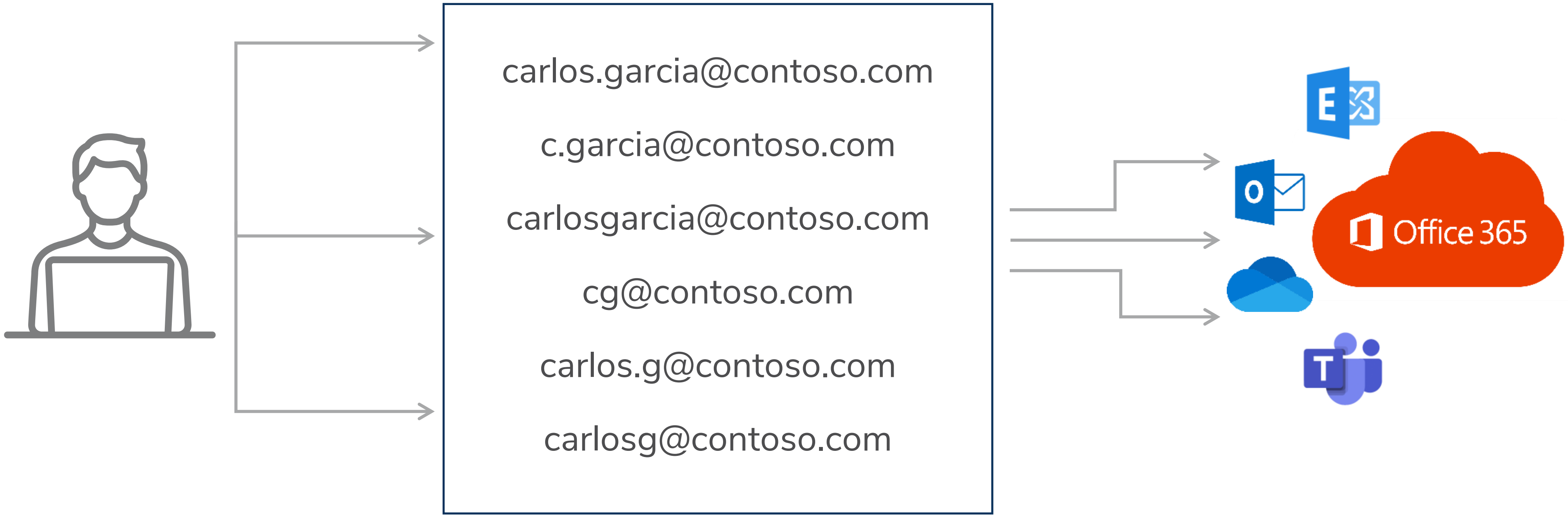
cg@contoso.com

carlos.g@contoso.com

carlosg@contoso.com

Username Validation

Microsoft is starting to make username validation ~~harder~~ more time consuming



carlos.garcia@contoso.com

c.garcia@contoso.com

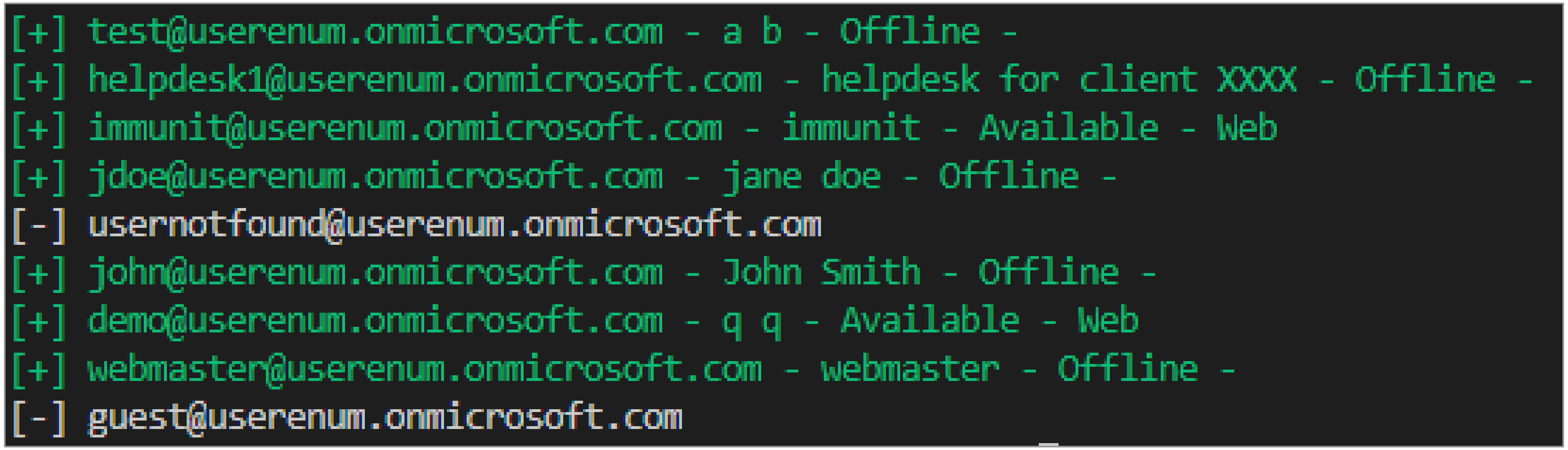
carlosgarcia@contoso.com

cg@contoso.com

carlos.g@contoso.com

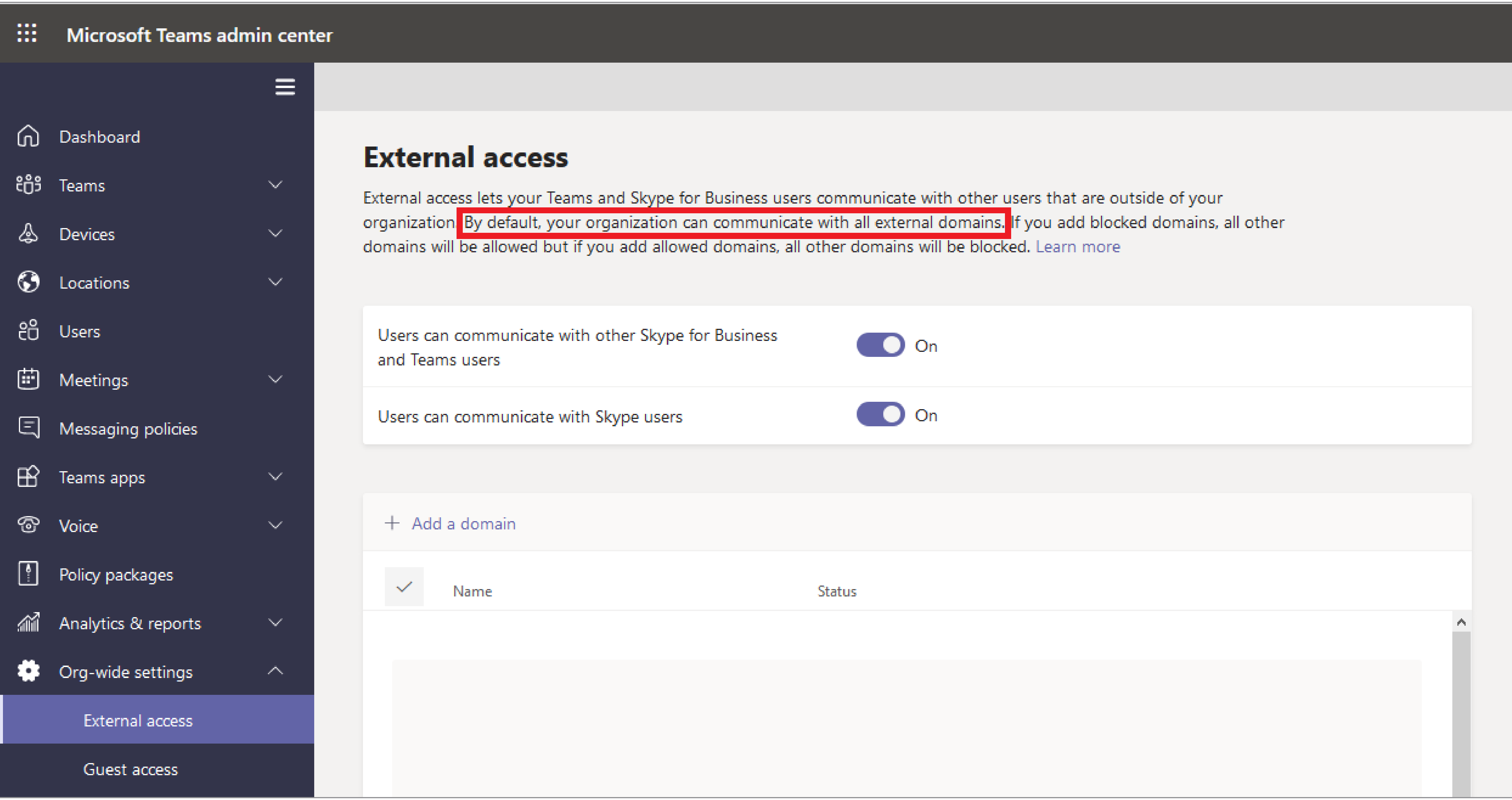
carlosg@contoso.com

User enumeration via MS Teams



```
[+] test@userenum.onmicrosoft.com - a b - Offline -
[+] helpdesk1@userenum.onmicrosoft.com - helpdesk for client XXXX - Offline -
[+] immunit@userenum.onmicrosoft.com - immunit - Available - Web
[+] jdoe@userenum.onmicrosoft.com - jane doe - Offline -
[-] usernotfound@userenum.onmicrosoft.com
[+] john@userenum.onmicrosoft.com - John Smith - Offline -
[+] demo@userenum.onmicrosoft.com - q q - Available - Web
[+] webmaster@userenum.onmicrosoft.com - webmaster - Offline -
[-] guest@userenum.onmicrosoft.com
```

References:
https://www.immunit.ch/blog/2021/07/05/microsoft-teams-user-enumeration/
https://github.com/vp40/TeamsUserEnum



External access

External access lets your Teams and Skype for Business users communicate with other users that are outside of your organization. By default, your organization can communicate with all external domains. If you add blocked domains, all other domains will be allowed but if you add allowed domains, all other domains will be blocked. Learn more

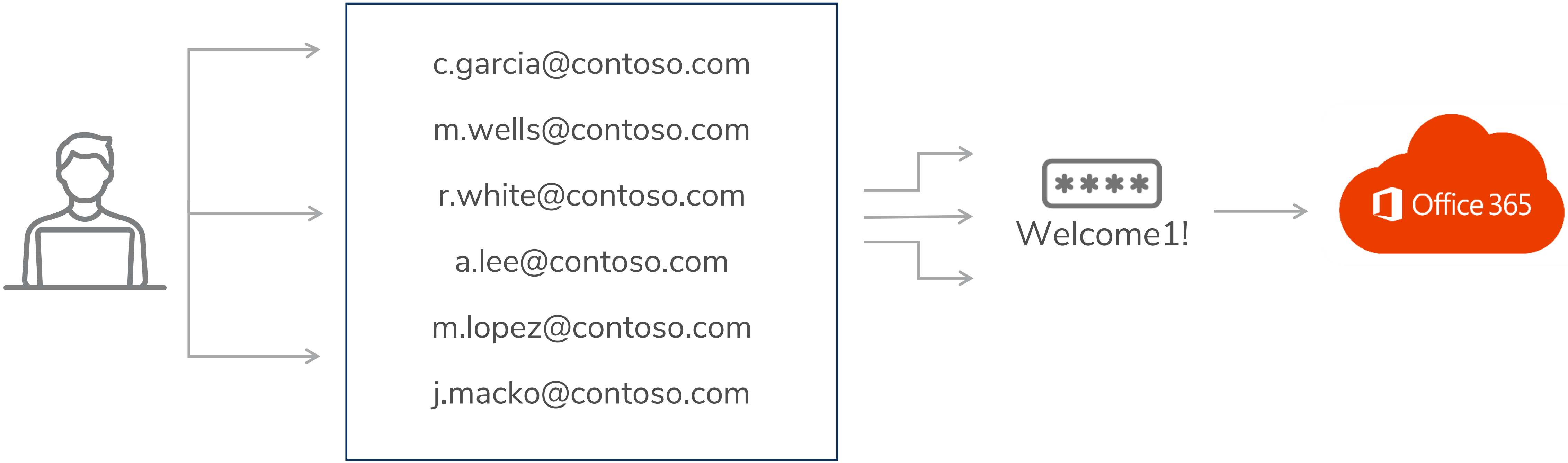
Users can communicate with other Skype for Business and Teams users: On

Users can communicate with Skype users: On

+ Add a domain

✓	Name	Status

Password Spray



c.garcia@contoso.com

m.wells@contoso.com

r.white@contoso.com

a.lee@contoso.com

m.lopez@contoso.com

j.macko@contoso.com

AD Password Audit

Use DSInternals to audit the passwords of your organization

- Accounts sharing the same (initial?) passwords
- Weak and guessable passwords
- Common patterns
- Accounts with passwords in a public database like HaveIBeenPwned or in a custom dictionary

References:
https://github.com/MichaelGrafnetter/DSInternals/blob/master/Documentation/PowerShell/Test-PasswordQuality.md#test-passwordquality

AD Password Audit

Online (DCSync)

```
Get-ADReplAccount -All -Server DC1-HOSTNAME |
   Test-PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-
ntlm.txt -IncludeDisabledAccounts
```

Offline (from ntds.dit copy)

script.ps1

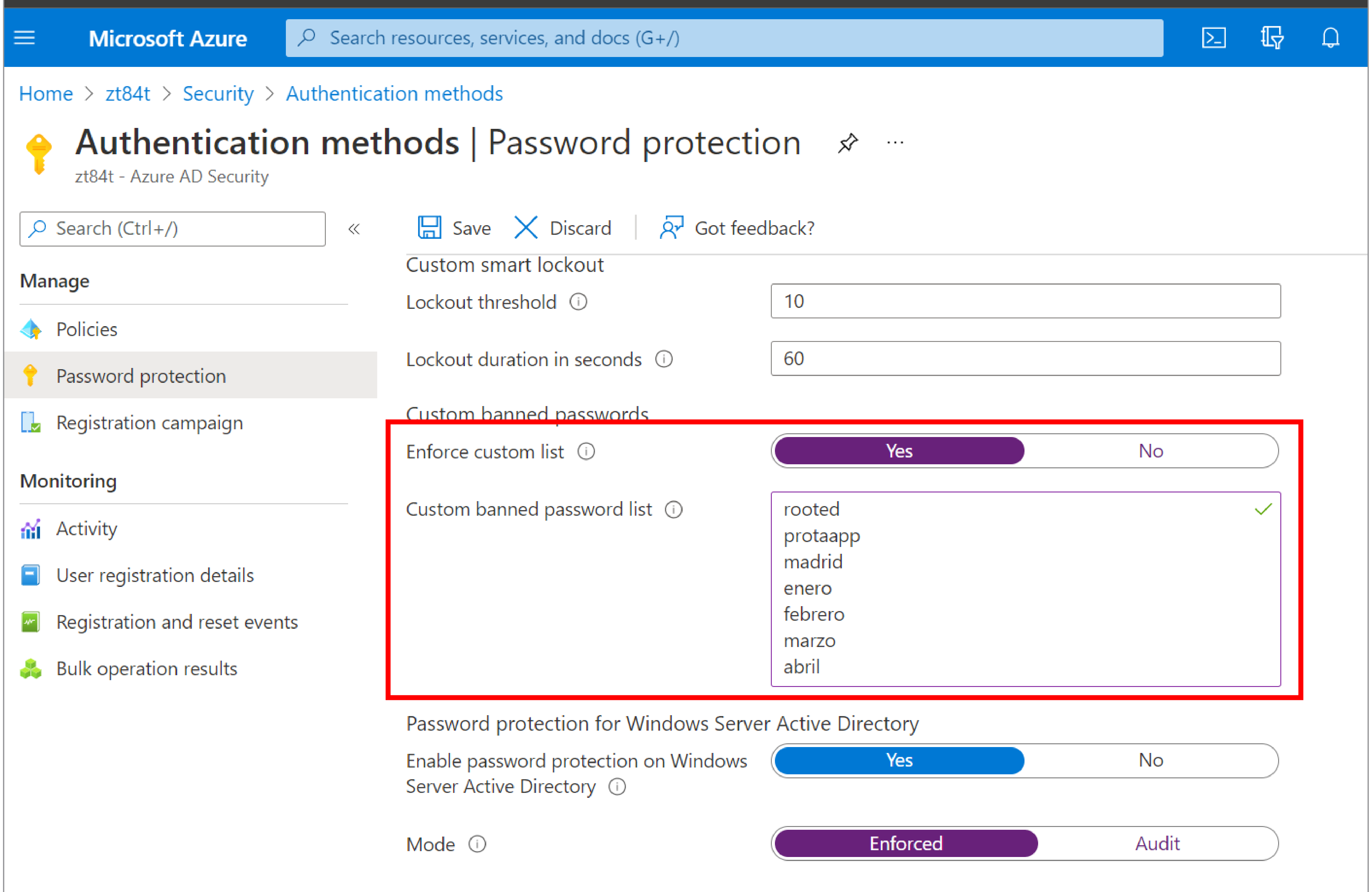
```
Import-Module $PSScriptRoot\DSInternals\DSInternals.psd1
$ntds_path = "$PSScriptRoot\ntds_files\ntds.dit"
$system_path = "$PSScriptRoot\ntds_files\SYSTEM"
$key = Get-BootKey -SystemHivePath $system_path
Get-ADDBAccount -All -DBPath $ntds_path -BootKey $key | Test-
PasswordQuality -WeakPasswordHashesFile .\pwned-passwords-ntlm.txt -
IncludeDisabledAccounts
```

References:
https://github.com/MichaelGrafnetter/DSInternals/blob/master/Documentation/PowerShell/Test-PasswordQuality.md#test-passwordquality

Deny list / Banned passwords

- Password Filter in AD
- Custom banned password list in Azure

References:
https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection
https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-password-ban-bad-on-premises-deploy
https://docs.microsoft.com/en-us/windows/win32/secmgmt/password-filters



Microsoft Azure
Search resources, services, and docs (G+/)
Home > zt84t > Security > Authentication methods

Authentication methods | Password protection

zt84t - Azure AD Security

Custom smart lockout

Lockout threshold: 10

Lockout duration in seconds: 60

Custom banned passwords

Enforce custom list: [✓ Yes] No

Custom banned password list:

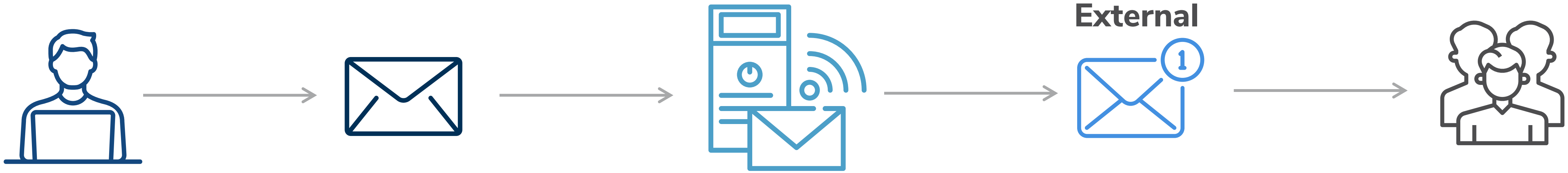
rooted
protaapp
madrid
enero
febrero
marzo
abril

Password protection for Windows Server Active Directory

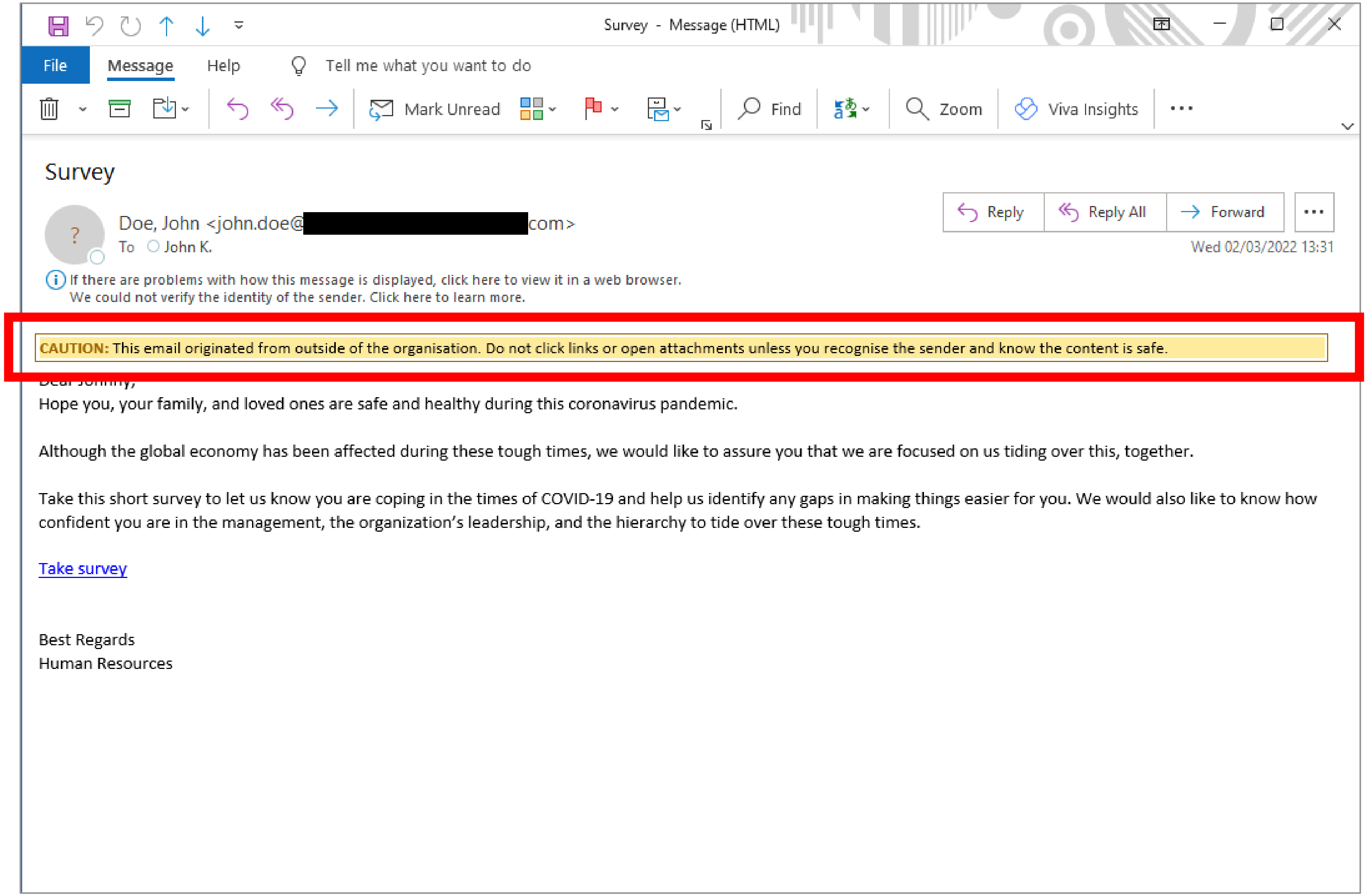
Enable password protection on Windows Server Active Directory: [✓ Yes] No

Mode: [✓ Enforced] Audit

External Email Warning Message



External Email Warning Message



Survey

Doe, John <john.doe@[redacted]com>

To John K.

Wed 02/03/2022 13:31

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.

CAUTION: This email originated from outside of the organisation. Do not click links or open attachments unless you recognise the sender and know the content is safe.

Dear Johnny,

Hope you, your family, and loved ones are safe and healthy during this coronavirus pandemic.

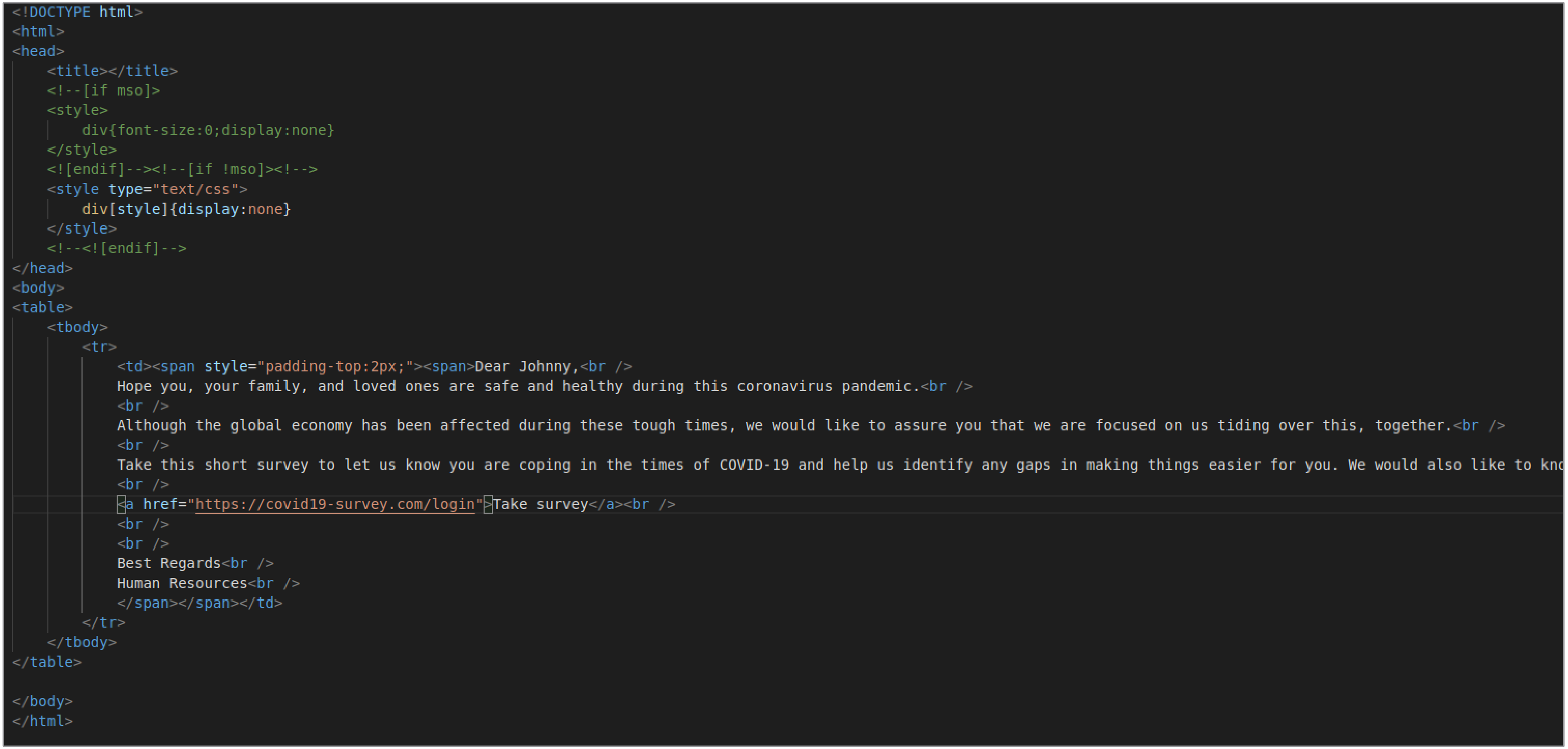
Although the global economy has been affected during these tough times, we would like to assure you that we are focused on us tiding over this, together.

Take this short survey to let us know you are coping in the times of COVID-19 and help us identify any gaps in making things easier for you. We would also like to know how confident you are in the management, the organization's leadership, and the hierarchy to tide over these tough times.

Take survey

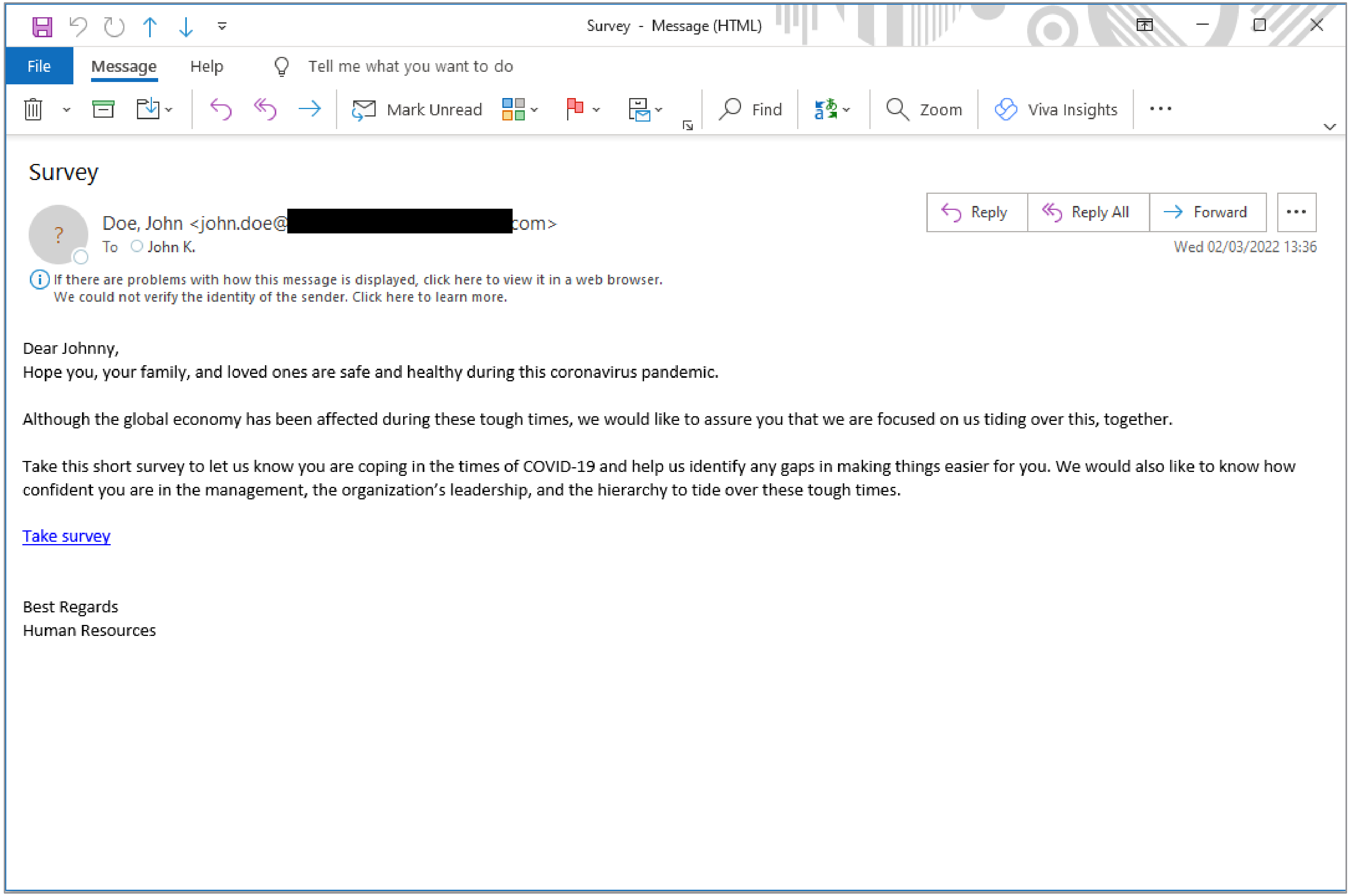
Best Regards
Human Resources

External Email Warning Message



```
<!DOCTYPE html>
<html>
<head>
    <title></title>
    <!--[if mso]>
    <style>
        div{font-size:0;display:none}
    </style>
    <![endif]--><!--[if !mso]><!-->
    <style type="text/css">
        div[style]{display:none}
    </style>
    <!--<![endif]-->
</head>
<body>
<table>
    <tbody>
        <tr>
            <td><span style="padding-top:2px;"><span>Dear Johnny,<br />
            Hope you, your family, and loved ones are safe and healthy during this coronavirus pandemic.<br />
            <br />
            Although the global economy has been affected during these tough times, we would like to assure you that we are focused on us tiding over this, together.<br />
            <br />
            Take this short survey to let us know you are coping in the times of COVID-19 and help us identify any gaps in making things easier for you. We would also like to kno
            <br />
            <a href="https://covid19-survey.com/login">Take survey</a><br />
            <br />
            <br />
            Best Regards<br />
            Human Resources<br />
            </span></span></td>
        </tr>
    </tbody>
</table>

</body>
</html>
```

Prepend Email Subject



Survey

Doe, John <john.doe@[redacted]com>
To John K.

Wed 02/03/2022 13:36

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.

Dear Johnny,
Hope you, your family, and loved ones are safe and healthy during this coronavirus pandemic.

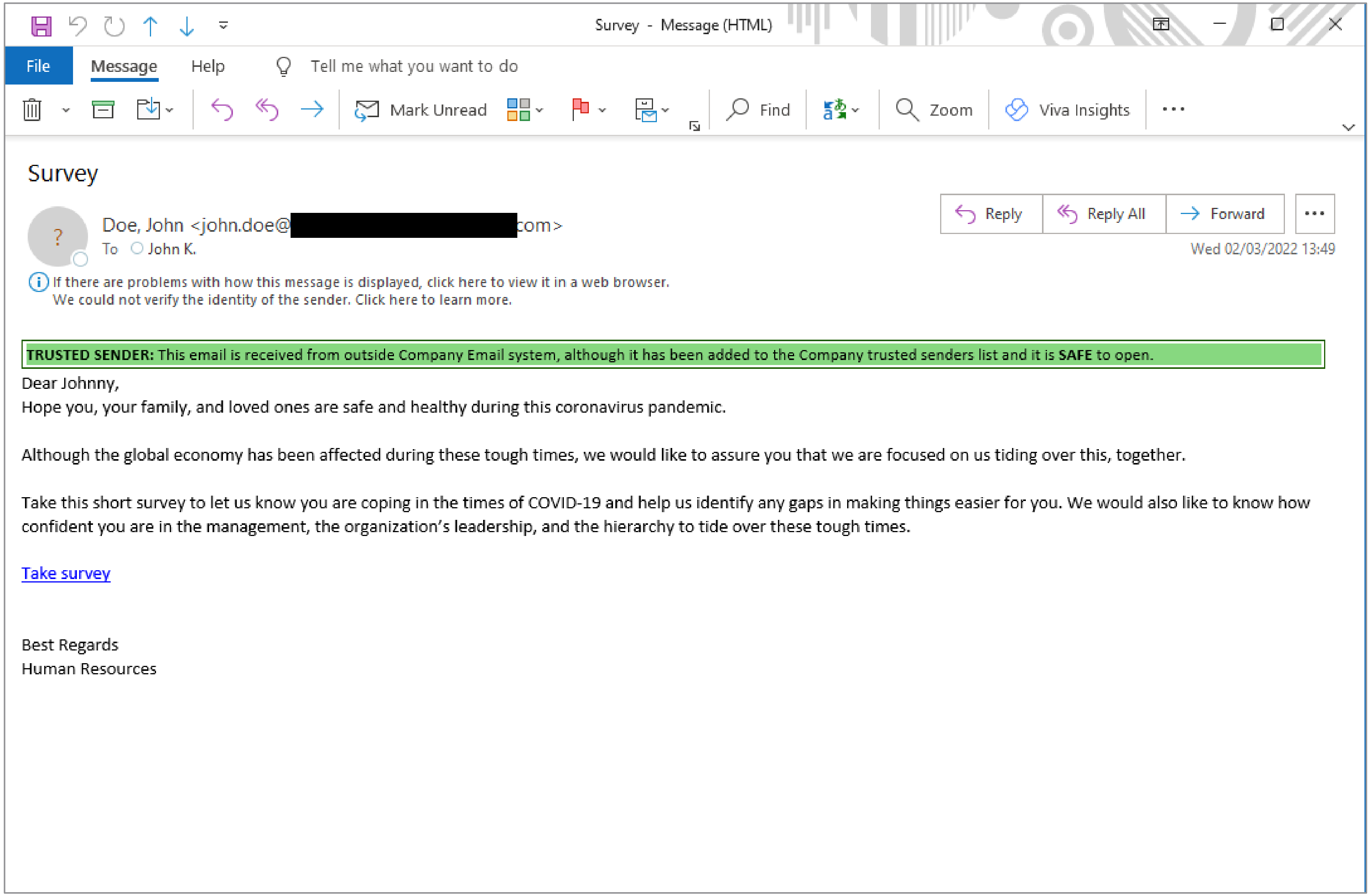
Although the global economy has been affected during these tough times, we would like to assure you that we are focused on us tiding over this, together.

Take this short survey to let us know you are coping in the times of COVID-19 and help us identify any gaps in making things easier for you. We would also like to know how confident you are in the management, the organization's leadership, and the hierarchy to tide over these tough times.

Take survey

Best Regards
Human Resources

Prepend Email Subject



Survey

Doe, John <john.doe@[redacted]com>

To John K.

Wed 02/03/2022 13:49

If there are problems with how this message is displayed, click here to view it in a web browser.
We could not verify the identity of the sender. Click here to learn more.

TRUSTED SENDER: This email is received from outside Company Email system, although it has been added to the Company trusted senders list and it is **SAFE** to open.

Dear Johnny,
Hope you, your family, and loved ones are safe and healthy during this coronavirus pandemic.

Although the global economy has been affected during these tough times, we would like to assure you that we are focused on us tiding over this, together.

Take this short survey to let us know you are coping in the times of COVID-19 and help us identify any gaps in making things easier for you. We would also like to know how confident you are in the management, the organization's leadership, and the hierarchy to tide over these tough times.

Take survey

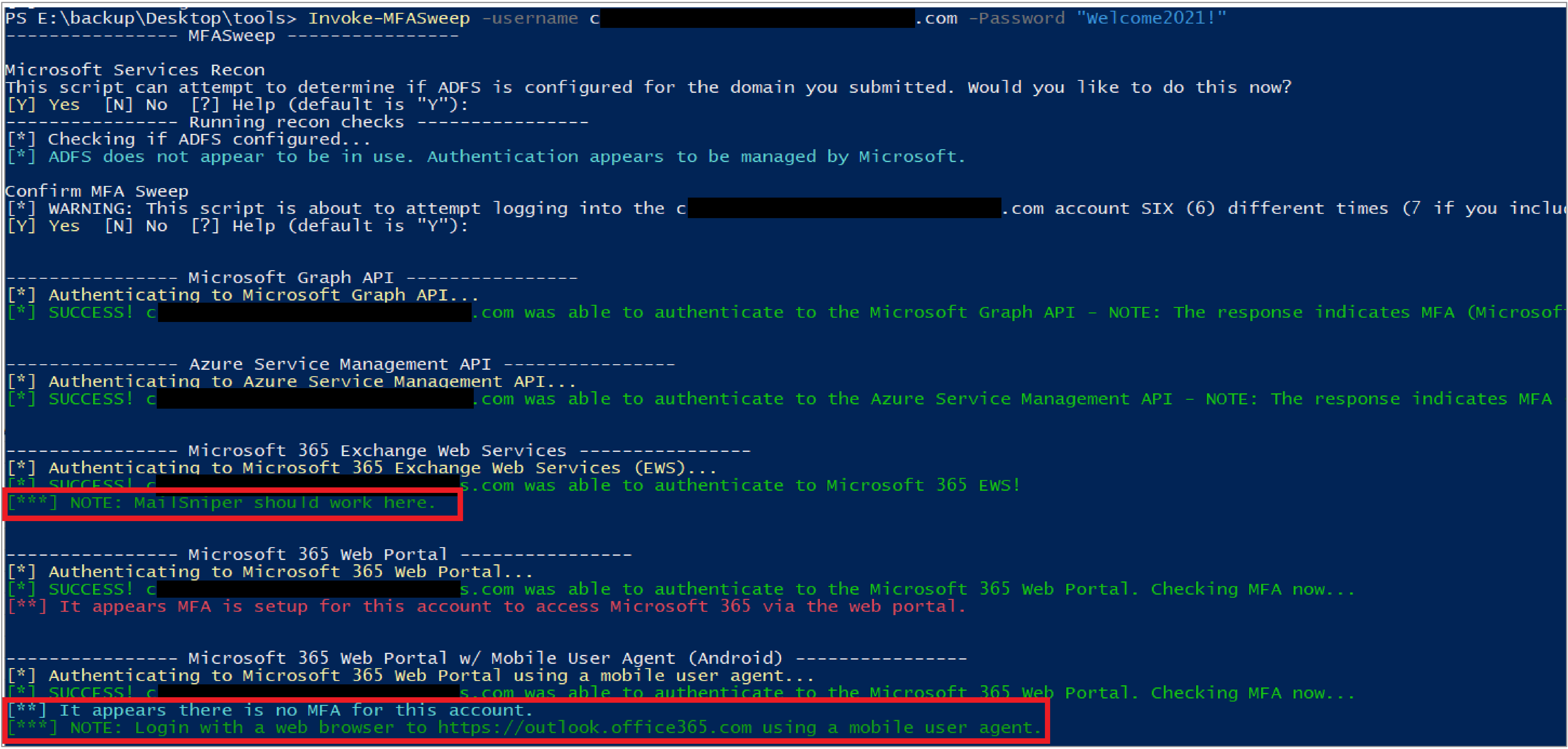
Best Regards
Human Resources

What if attackers manage to compromise valid username:password?

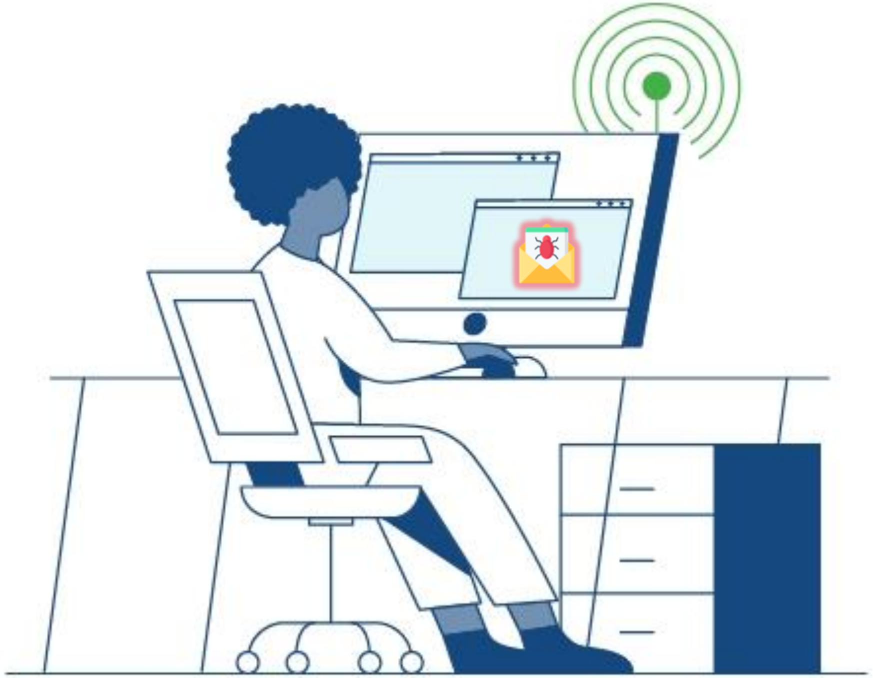
Multifactor Authentication

- Enabled on every external portal
  - 3rd party products – VPN, ticket, Mimecast

- Enabled on every protocol
  - Disable protocols that do not allow it
  - Conditional Access. **Implement it well!**



```
PS E:\backup\Desktop\tools> Invoke-MFASweep -username c[redacted].com -Password "Welcome2021!"
---------------- MFASweep ----------------

Microsoft Services Recon
This script can attempt to determine if ADFS is configured for the domain you submitted. Would you like to do this now?
[Y] Yes  [N] No  [?] Help (default is "Y"):
---------------- Running recon checks ----------------
[*] Checking if ADFS configured...
[*] ADFS does not appear to be in use. Authentication appears to be managed by Microsoft.

Confirm MFA Sweep
[*] WARNING: This script is about to attempt logging into the c[redacted].com account SIX (6) different times (7 if you inclu
[Y] Yes  [N] No  [?] Help (default is "Y"):


---------------- Microsoft Graph API ----------------
[*] Authenticating to Microsoft Graph API...
[*] SUCCESS! c[redacted].com was able to authenticate to the Microsoft Graph API - NOTE: The response indicates MFA (Microsof

---------------- Azure Service Management API ----------------
[*] Authenticating to Azure Service Management API...
[*] SUCCESS! c[redacted].com was able to authenticate to the Azure Service Management API - NOTE: The response indicates MFA

---------------- Microsoft 365 Exchange Web Services ----------------
[*] Authenticating to Microsoft 365 Exchange Web Services (EWS)...
[*] SUCCESS! c[redacted]s.com was able to authenticate to Microsoft 365 EWS!
[***] NOTE: MailSniper should work here.

---------------- Microsoft 365 Web Portal ----------------
[*] Authenticating to Microsoft 365 Web Portal...
[*] SUCCESS! c[redacted]s.com was able to authenticate to the Microsoft 365 Web Portal. Checking MFA now...
[**] It appears MFA is setup for this account to access Microsoft 365 via the web portal.

---------------- Microsoft 365 Web Portal w/ Mobile User Agent (Android) ----------------
[*] Authenticating to Microsoft 365 Web Portal using a mobile user agent...
[*] SUCCESS! c[redacted]s.com was able to authenticate to the Microsoft 365 Web Portal. Checking MFA now...
[**] It appears there is no MFA for this account.
[***] NOTE: Login with a web browser to https://outlook.office365.com using a mobile user agent.
```



References: flaticon

Common Internal Attacks and Controls

Kerberoasting

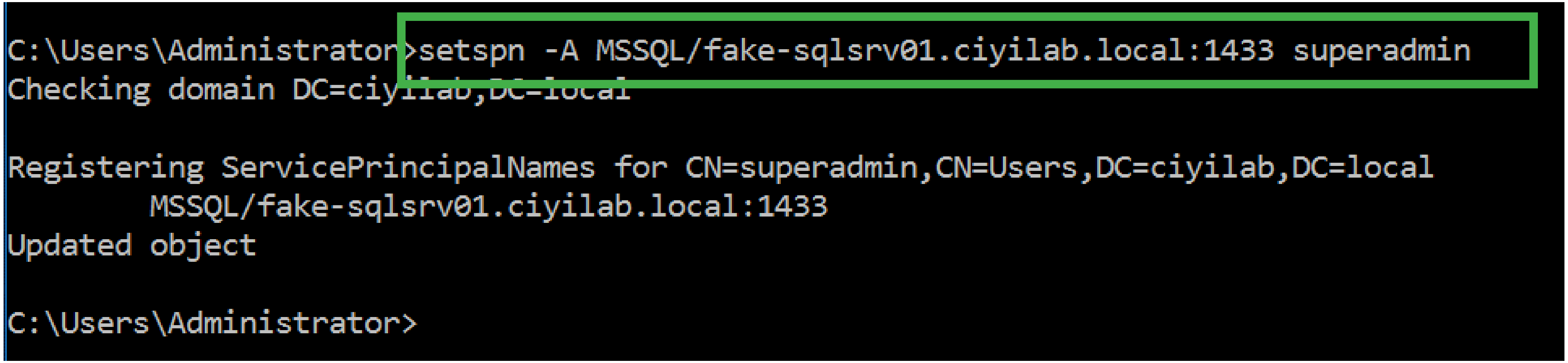
- Search for user accounts with Kerberos Service Principal Names (SPN)
- SPN is a reference to a specific service, the hostname that runs the instance and which port it is running on
- Service Ticket is encrypted with the user account’s password hash
- Most attackers will:
  - Enumerate all users in the domain
  - Look for users where their SPN attribute is not null
  - Attackers usually request them all (or interesting ones) and crack them offline

Harden Kerberoast Accounts

- List all the available SPN associated to user accounts
- Remove unnecessary services
- Follow the principle of minimum privileges
- Set REALLY strong password or use GMSA

Harden Kerberoast Accounts

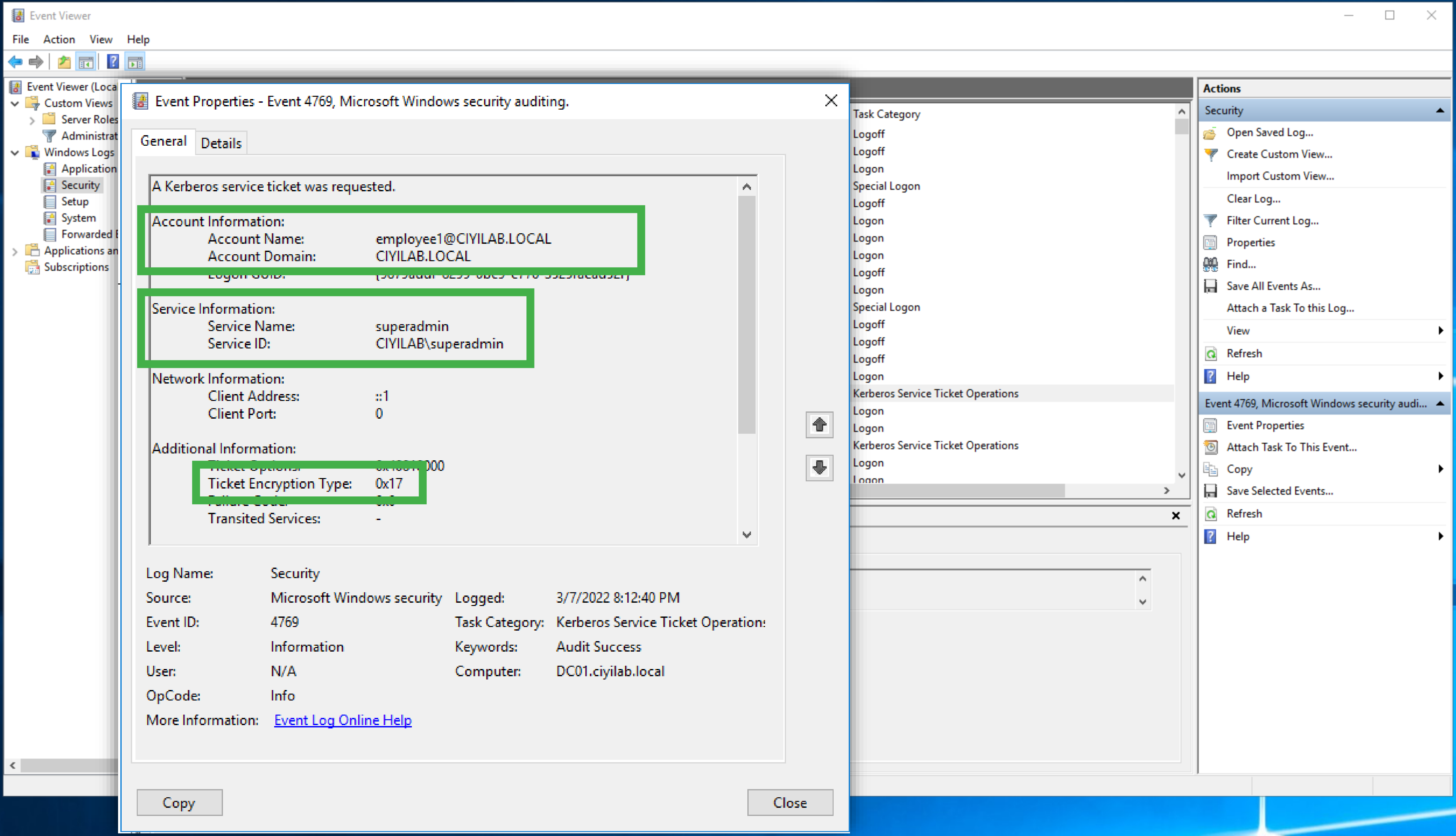
- Create a **Honey Kerberoast account**
  - Make it look like an interesting account
  - Set a REALLY strong password
  - Associate an SPN



```
C:\Users\Administrator>setspn -A MSSQL/fake-sqlsrv01.ciyilab.local:1433 superadmin
Checking domain DC=ciyilab,DC=local

Registering ServicePrincipalNames for CN=superadmin,CN=Users,DC=ciyilab,DC=local
        MSSQL/fake-sqlsrv01.ciyilab.local:1433
Updated object

C:\Users\Administrator>
```

- Monitor event 4769

References:
https://adsecurity.org/?p=3458



```
Task Category
Logoff
Logoff
Logon
Special Logon
Logoff
Logon
Logon
Logon
Logoff
Logon
Special Logon
Logoff
Logoff
Logoff
Logon
Kerberos Service Ticket Operations
Logon
Logon
Kerberos Service Ticket Operations
Logon
Logon
```

Event Properties - Event 4769, Microsoft Windows security auditing.

```
A Kerberos service ticket was requested.

Account Information:
        Account Name:           employee1@CIYILAB.LOCAL
        Account Domain:         CIYILAB.LOCAL
        Logon GUID:             {[illegible]}

Service Information:
        Service Name:           superadmin
        Service ID:             CIYILAB\superadmin

Network Information:
        Client Address:         ::1
        Client Port:            0

Additional Information:
        Ticket Options:         0x40810000
        Ticket Encryption Type: 0x17
        Failure Code:           0x0
        Transited Services:     -
```

Log Name: Security
Source: Microsoft Windows security
Logged: 3/7/2022 8:12:40 PM
Event ID: 4769
Task Category: Kerberos Service Ticket Operation:
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01.ciyilab.local
OpCode: Info
More Information: Event Log Online Help

Reconnaissance - User Hunting

1. Gets users groups and group members of each group
2. Lists domain computers
3. Lists active sessions on each computer
4. Obtains local admins for each computer
5. …

NetCease

References:
https://stealthbits.com/blog/making-internal-reconnaissance-harder-using-netcease-and-samri1o/

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

RestrictRemoteSAM

References:
https://stealthbits.com/blog/making-internal-reconnaissance-harder-using-netcease-and-samri1o/

https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls

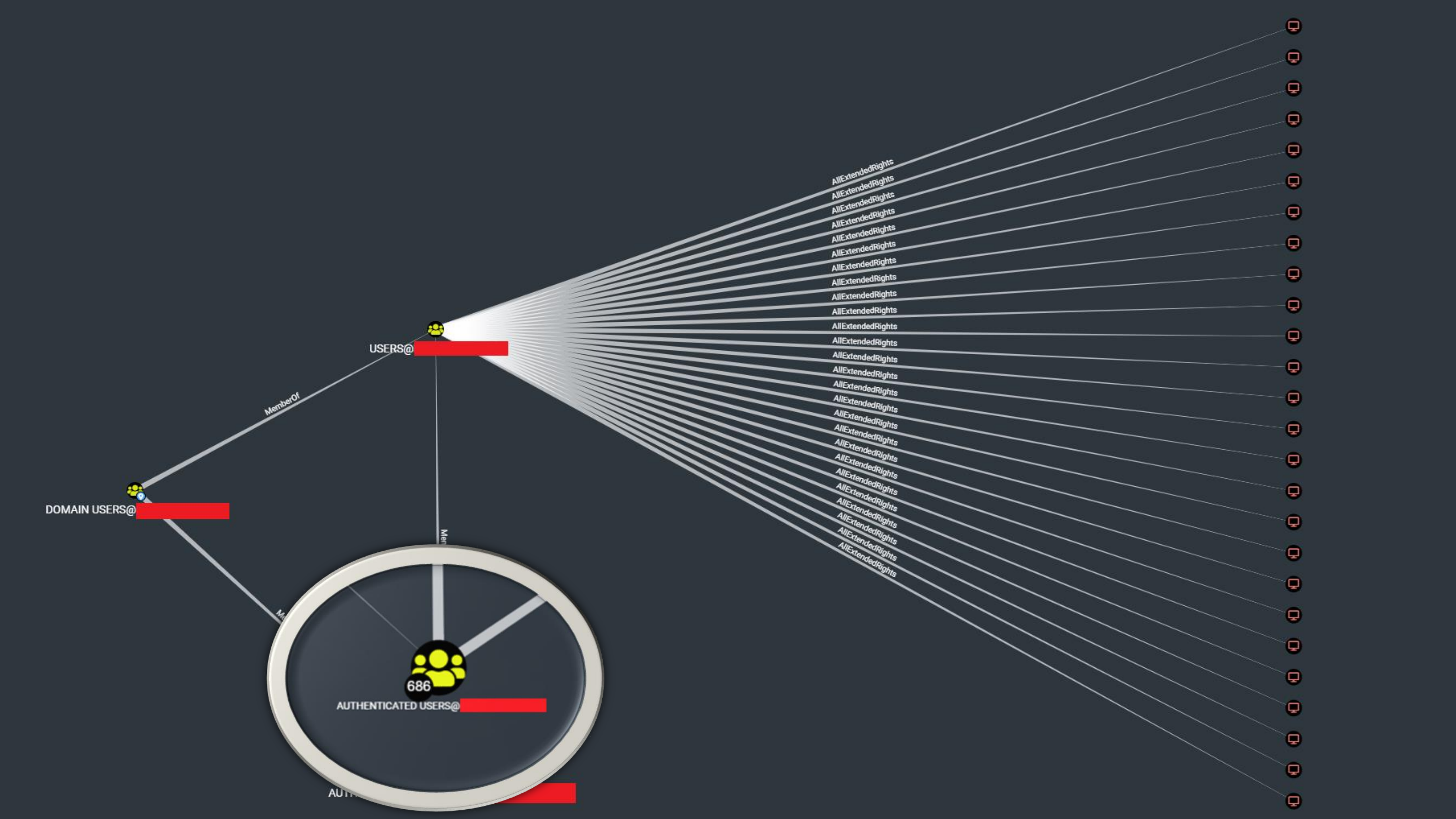
References: https://github.com/BloodHoundAD/BloodHound

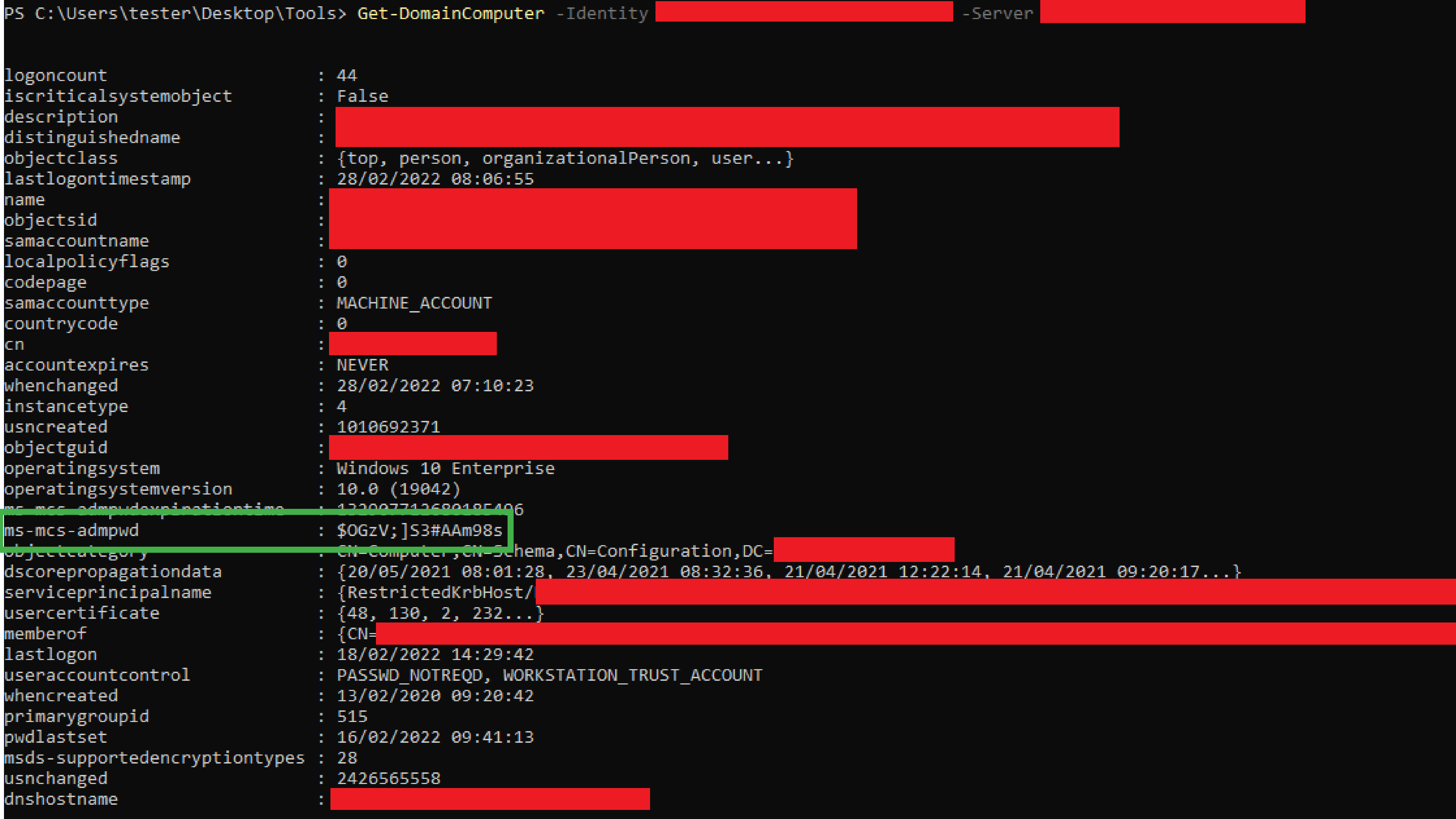
Harden Local Accounts

- Audit local accounts and remove unnecessary local accounts

- Deploy Local Administrator Password Solution (LAPS)
  - Passwords are stored in Active Directory (AD) and protected by ACL, so only eligible users can read it or request its reset
  - Deploy it well!

References:
https://www.microsoft.com/en-us/download/details.aspx?id=46899

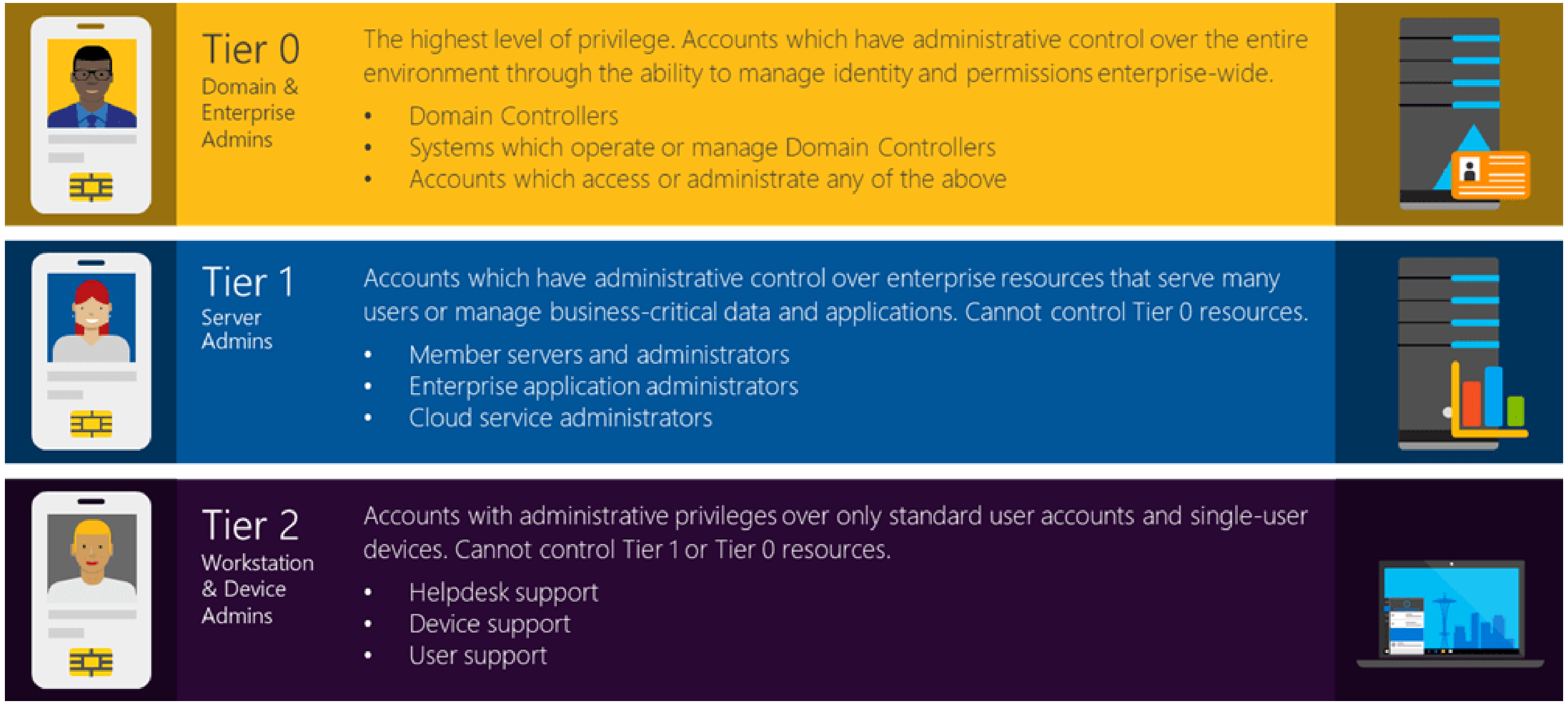

USERS@[redacted]
DOMAIN USERS@[redacted]
AUTHENTICATED USERS@[redacted]
686
AUT[redacted]
MemberOf
Mem
Me
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights
AllExtendedRights



```
PS C:\Users\tester\Desktop\Tools> Get-DomainComputer -Identity [redacted] -Server [redacted]


logoncount                    : 44
iscriticalsystemobject        : False
description                   : [redacted]
distinguishedname             :
objectclass                   : {top, person, organizationalPerson, user...}
lastlogontimestamp            : 28/02/2022 08:06:55
name                          : [redacted]
objectsid                     :
samaccountname                :
localpolicyflags              : 0
codepage                      : 0
samaccounttype                : MACHINE_ACCOUNT
countrycode                   : 0
cn                            : [redacted]
accountexpires                : NEVER
whenchanged                   : 28/02/2022 07:10:23
instancetype                  : 4
usncreated                    : 1010692371
objectguid                    : [redacted]
operatingsystem               : Windows 10 Enterprise
operatingsystemversion        : 10.0 (19042)
ms-mcs-admpwdexpirationtime   : 132907712680185406
ms-mcs-admpwd                 : $OGzV;]S3#AAm98s
objectcategory                : CN=Computer,CN=Schema,CN=Configuration,DC=[redacted]
dscorepropagationdata         : {20/05/2021 08:01:28, 23/04/2021 08:32:36, 21/04/2021 12:22:14, 21/04/2021 09:20:17...}
serviceprincipalname          : {RestrictedKrbHost/[redacted]
usercertificate               : {48, 130, 2, 232...}
memberof                      : {CN=[redacted]
lastlogon                     : 18/02/2022 14:29:42
useraccountcontrol            : PASSWD_NOTREQD, WORKSTATION_TRUST_ACCOUNT
whencreated                   : 13/02/2020 09:20:42
primarygroupid                : 515
pwdlastset                    : 16/02/2022 09:41:13
msds-supportedencryptiontypes : 28
usnchanged                    : 2426565558
dnshostname                   : [redacted]
```

Privileged Account Management

- Dual account model for privileged accounts
- Use Domain Admins accounts to ONLY logon to Domain Controllers
- Consider using the Protected Users group



Tier 0
Domain & Enterprise Admins

The highest level of privilege. Accounts which have administrative control over the entire environment through the ability to manage identity and permissions enterprise-wide.

- Domain Controllers
- Systems which operate or manage Domain Controllers
- Accounts which access or administrate any of the above

Tier 1
Server Admins

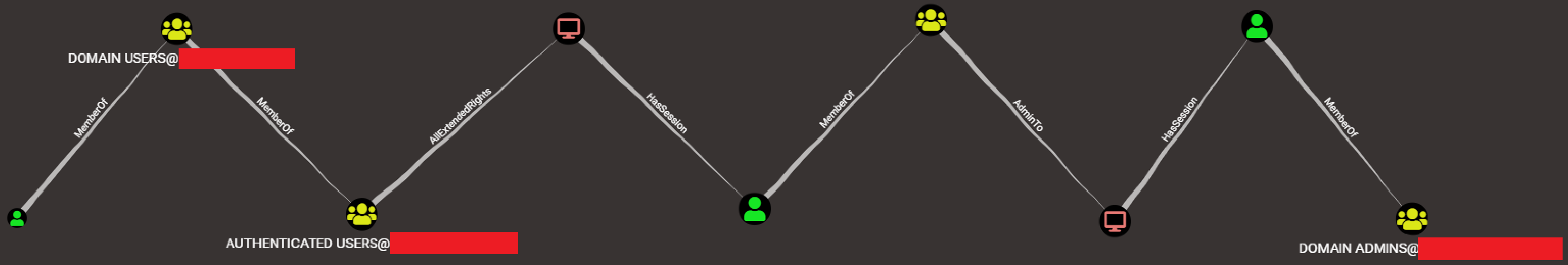
Accounts which have administrative control over enterprise resources that serve many users or manage business-critical data and applications. Cannot control Tier 0 resources.

- Member servers and administrators
- Enterprise application administrators
- Cloud service administrators

Tier 2
Workstation & Device Admins

Accounts with administrative privileges over only standard user accounts and single-user devices. Cannot control Tier 1 or Tier 0 resources.

- Helpdesk support
- Device support
- User support


MemberOf
DOMAIN USERS@[redacted]
MemberOf
AUTHENTICATED USERS@[redacted]
AllExtendedRights
HasSession
MemberOf
AdminTo
HasSession
MemberOf
DOMAIN ADMINS@[redacted]

SMB Shares Hygiene

Periodically audit accessible shares and their content

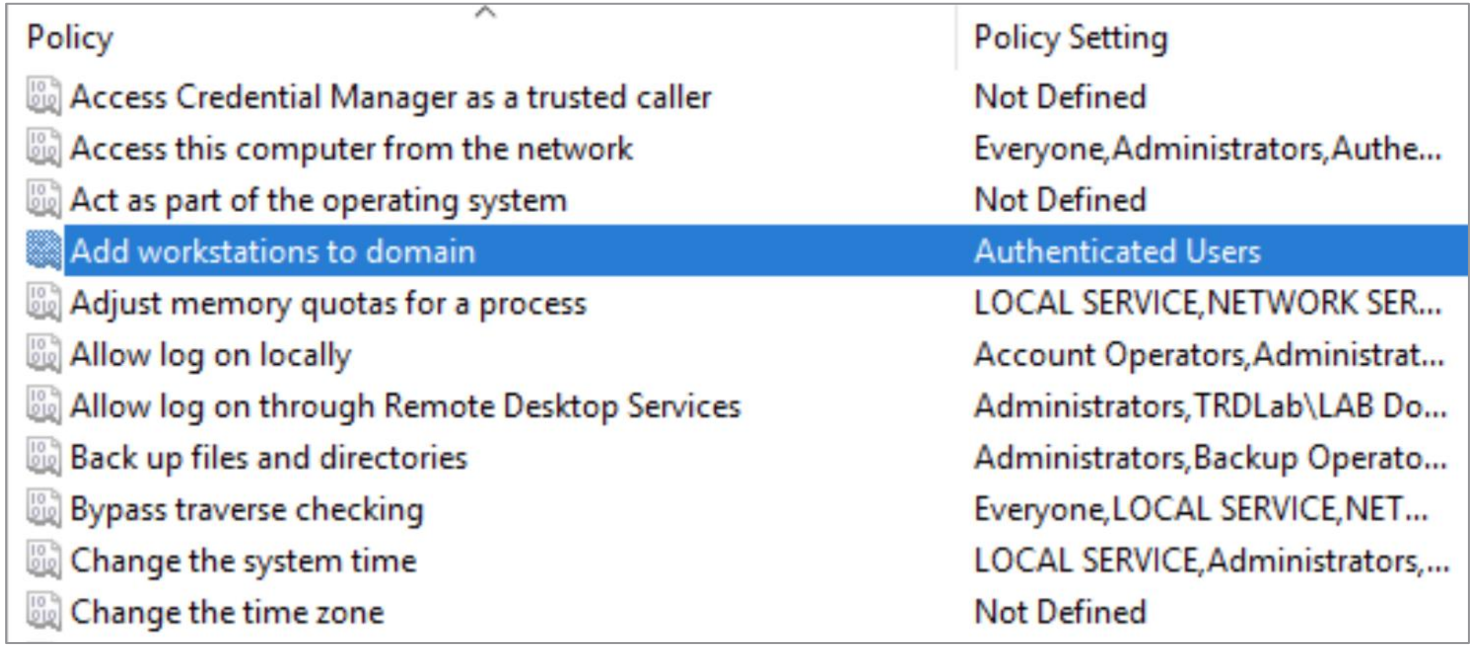
- Microsoft ShareEnum
- PingCastle
- PowerView:

```
Find-InterestingDomainShareFile -ComputerDomain DOMAIN -Server DC -include
@('*passw*', '*sensitive*', '*administrator*', '*administrador*', '*administrateur*',
'*login*', '*logon*', '*secret*', 'unattend*.xml', '*.vmdk', '*creds*',
'*credential*', '*.config', '*.ps1', '*.bat', '*.vbs', '*clave*', '*contrasena*',
'*contraseña*', 'WinSCP.ini', '*.kdbx', '*.cert', '*.pem', '*pwd*', '*heslo*',
'*.ova', '*.vhdx', '*.vhd', '*.vbe', '*.pfx', '*pass*.xls*', '*pass*.doc*',
'*pass*.txt', '*admin*.txt*') | Export-csv interesting_shares_files.csv
```

References:
https://docs.microsoft.com/en-us/sysinternals/downloads/shareenum
https://www.pingcastle.com
https://github.com/PowerShellMafia/PowerSploit/blob/master/Recon/PowerView.ps1

MS-DS-MachineAccountQuota

Domain level attribute that allows unprivileged users (Authenticated Users) to add up to 10 computers to an Active Directory (AD) domain by default



Policy	Policy Setting
Access Credential Manager as a trusted caller	Not Defined
Access this computer from the network	Everyone,Administrators,Authe...
Act as part of the operating system	Not Defined
Add workstations to domain	Authenticated Users
Adjust memory quotas for a process	LOCAL SERVICE,NETWORK SER...
Allow log on locally	Account Operators,Administrat...
Allow log on through Remote Desktop Services	Administrators,TRDLab\LAB Do...
Back up files and directories	Administrators,Backup Operato...
Bypass traverse checking	Everyone,LOCAL SERVICE,NET...
Change the system time	LOCAL SERVICE,Administrators,...
Change the time zone	Not Defined

MS-DS-MachineAccountQuota

- Harden it to help secure your AD against many AD attacks
  - Resource-Based Constrained Delegation
  - SamAccount Spoofing attack
  - KrbRelayUp
  - ...

- Restrict Default Domain Controllers policy or set attribute ms-DS-MachineAccountQuota = 0

References:
https://www.netspi.com/blog/technical/network-penetration-testing/machineaccountquota-is-useful-sometimes/
https://twitter.com/PyroTek3/status/1472707596234772486

A Summary of the Controls We Hate The Most

KROLL

External Controls We Hate The Most

- Map & reduce your attack surface
- Harden your Azure/O365 tenant
- Harden external reconnaissance possibilities
- Secure your MFA deployment
- Secure your External email warning
- Audit & harden your current password hygiene

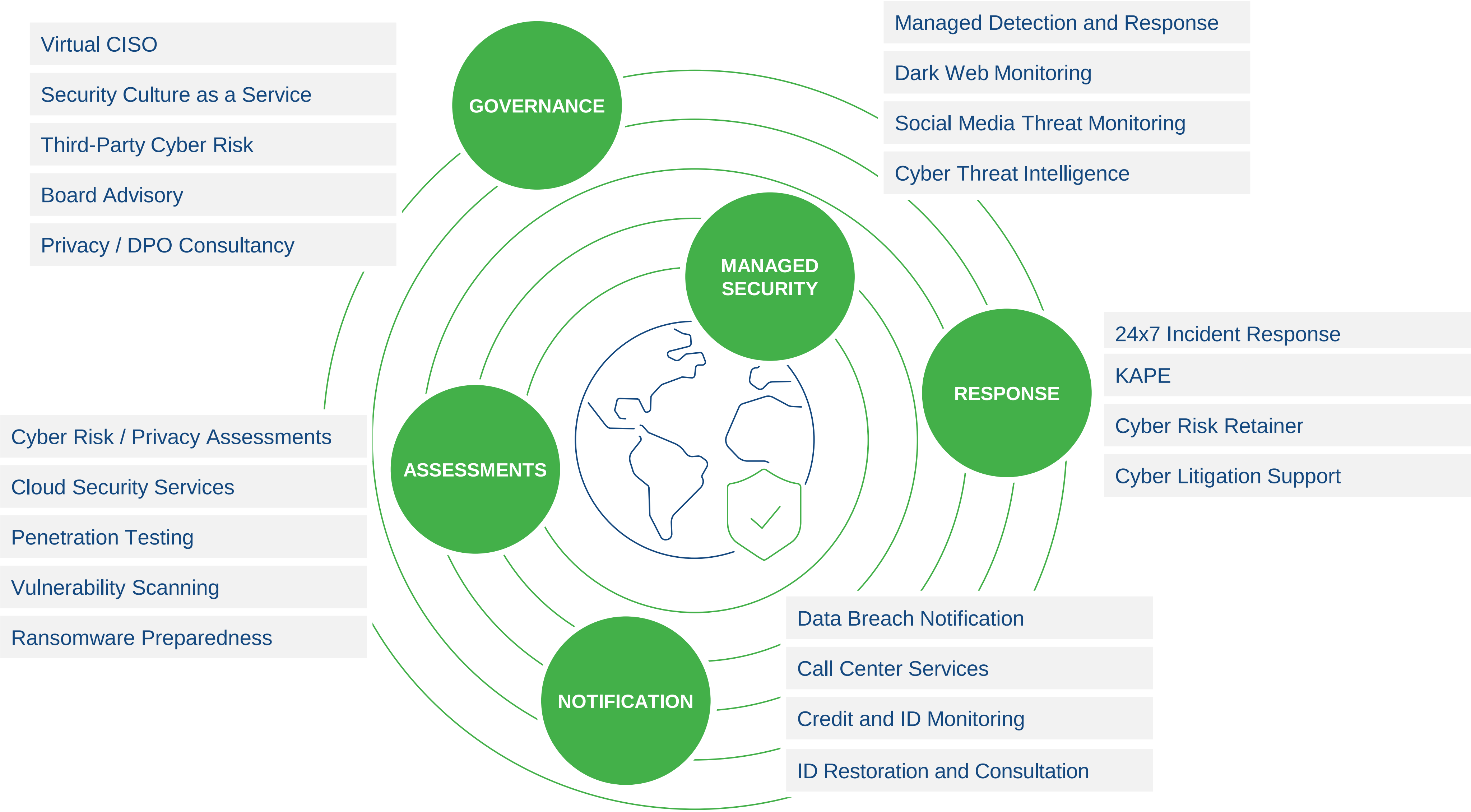
Internal Controls We Hate The Most

- Harden Kerberoast accounts (and pre-authentication)
- Harden reconnaissance possibilities
- Use BloodHound (& GoodHound & PlumHound)
- Keep a good hygiene of your SMB shares
- Disable obsolete protocols (and enable SMB & LDAP signing)
- Use privileged account management
- Extend your logging & auditing
- Harden and protect your endpoints

Thank You

Questions?

Global, End-to-End Cyber Risk Management



GOVERNANCE

- Virtual CISO
- Security Culture as a Service
- Third-Party Cyber Risk
- Board Advisory
- Privacy / DPO Consultancy

MANAGED SECURITY

- Managed Detection and Response
- Dark Web Monitoring
- Social Media Threat Monitoring
- Cyber Threat Intelligence

RESPONSE

- 24x7 Incident Response
- KAPE
- Cyber Risk Retainer
- Cyber Litigation Support

NOTIFICATION

- Data Breach Notification
- Call Center Services
- Credit and ID Monitoring
- ID Restoration and Consultation

ASSESSMENTS

- Cyber Risk / Privacy Assessments
- Cloud Security Services
- Penetration Testing
- Vulnerability Scanning
- Ransomware Preparedness

For more information, please contact:

Carlos García

Senior Vice President

carlos.garcia@kroll.com

Jeff Macko

Associate Managing Director

jeff.macko@kroll.com

About Kroll

Kroll is the world's premier provider of services and digital products related to valuation, governance, risk and transparency. We work with clients across diverse sectors in the areas of valuation, expert services, investigations, cyber security, corporate finance, restructuring, legal and business solutions, data analytics and regulatory compliance. Our firm has nearly 5,000 professionals in 30 countries and territories around the world. For more information, visit www.kroll.com.

M&A advisory, capital raising and secondary market advisory services in the United States are provided by Duff & Phelps Securities, LLC. Member FINRA/SIPC. Pagemill Partners is a Division of Duff & Phelps Securities, LLC. M&A advisory, capital raising and secondary market advisory services in the United Kingdom are provided by Duff & Phelps Securities Ltd. (DPSL), which is authorized and regulated by the Financial Conduct Authority. Valuation Advisory Services in India are provided by Duff & Phelps India Private Limited under a category 1 merchant banker license issued by the Securities and Exchange Board of India.