



**REAL EYES, REALIZE,
REAL LIES**

Beating Deception Technologies

Matan Hart

@machosec
matan@cymptom.com





**REAL EYES, REALIZE,
REAL LIES**

Beating Deception Technologies

Matan Hart

@machosec

matan@cymptom.com



***“The greatest deception men suffer
is from their own opinions”***

Leonardo da Vinci

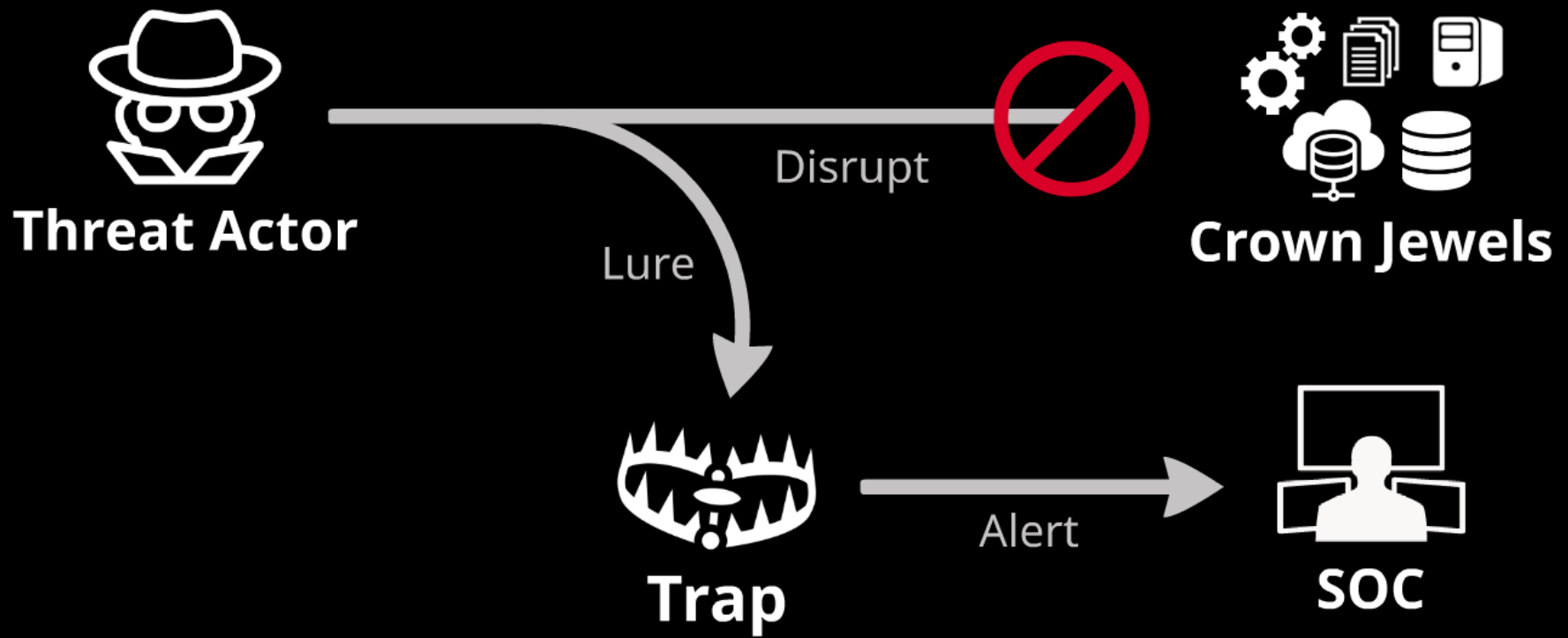


WHO AM I

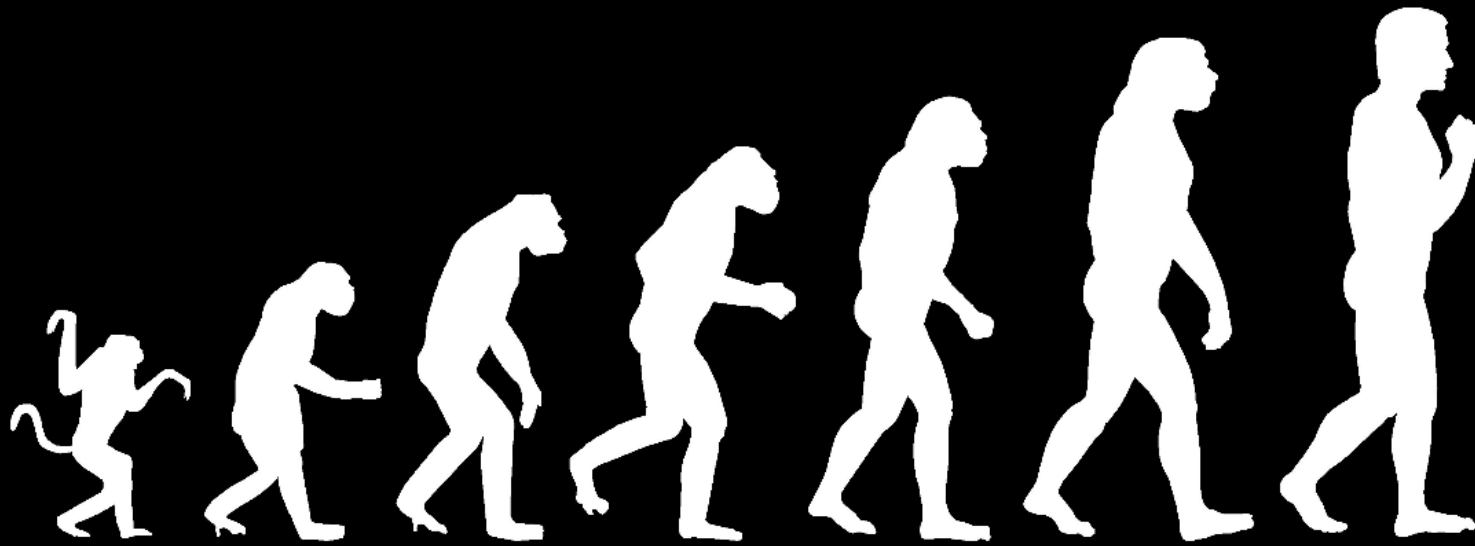
- **Co-Founder and CEO @ Cymptom**
 - Still at stealth :)
- **Speaker**
 - Black Hat, BSides
- **Addictions**
 - Poker, TV shows



DECEPTION



EVOLUTION



1993

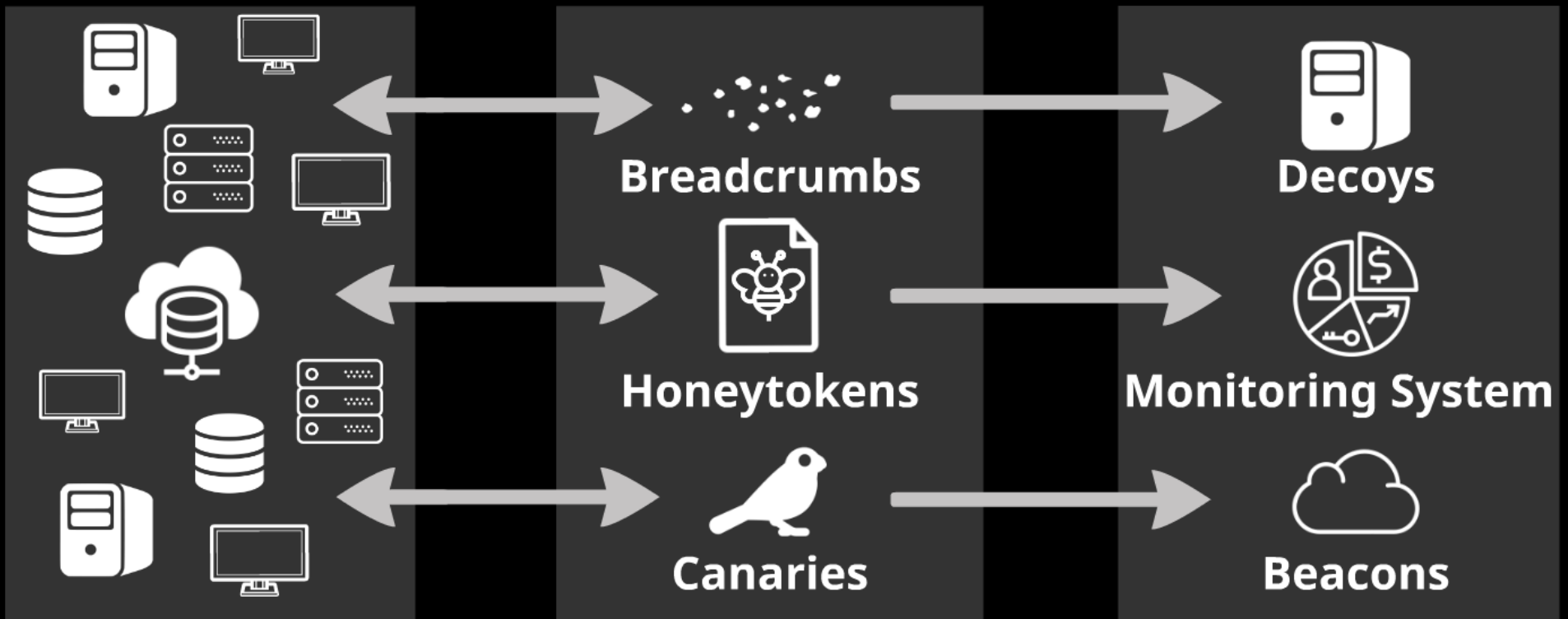
2018

ARCHITECTURE

"Real" Assets

Bait

Detection



EFFECTIVENESS



Confrontation



Network



Endpoint



Credentials



Application



Data



Believability

☰ ARP, DNS and DHCP records

☰ Active Directory entries

🔦 High interaction services

🌐 OSINT information



Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
<https://www.wellobtusa.com/pages/dc2e4f0a10a00a>

Confrontation



Network



Endpoint



Credentials



Application



Data

EFFECTIVENESS



Confrontation



Network



Endpoint



Credentials



Application



Data



Believability

☰ ARP, DNS and DHCP records

☰ Active Directory entries

🔍 High interaction services

🌐 OSINT information



Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
<https://www.wellobscure.com/pages/dc2e4f0a0d0a0a>

Believability

 **ARP, DNS and DHCP records**

 **Active Directory entries**

 **High interaction services**

 **OSINT information**

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT

<https://www.wallofsheep.com/pages/dc26#hyudovich>

EFFECTIVENESS



Confrontation



Network



Endpoint



Credentials



Application



Data



Believability

☰ ARP, DNS and DHCP records

☰ Active Directory entries

🔍 High interaction services

🌐 OSINT information



Success Rate

TURNING DECEPTION OUTSIDE-IN: TRICKING ATTACKERS WITH OSINT
<https://www.wellobtusa.com/pages/dc2e4f9a5d0a0>

COUNTER-DECEPTION



DO NOT COUNT ON:

- Your gut feeling
- Storyline plot holes
- Predictable patterns
- Endpoint isolation



***"DON'T PLAY THE ODDS
PLAY THE MAN"***

Harvey Specter, Suits



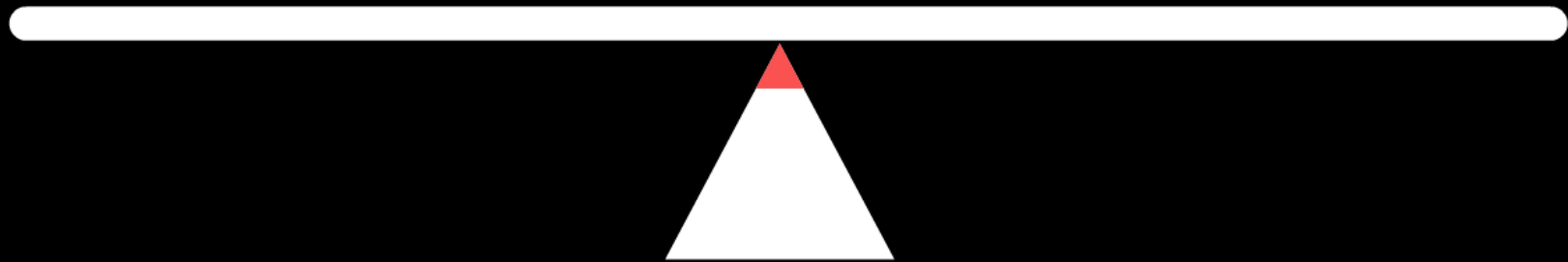
ACHILLES' HEEL



Authenticity

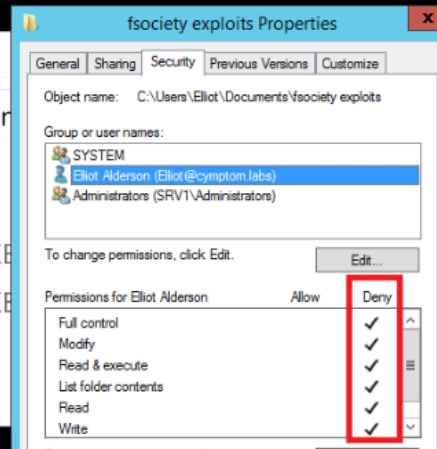
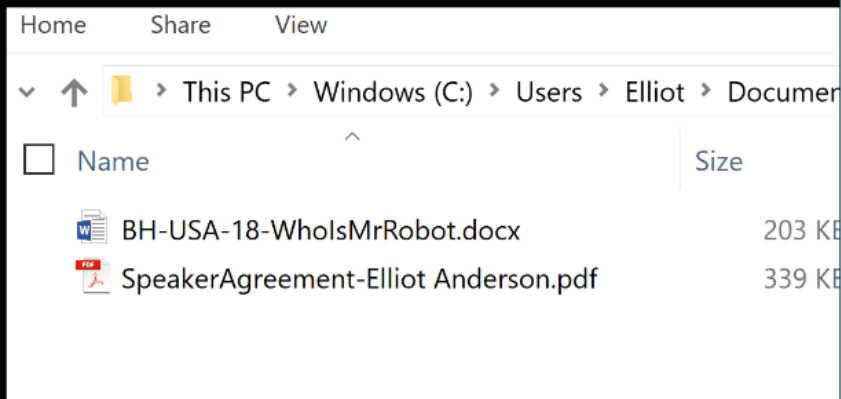


Disruption Risk

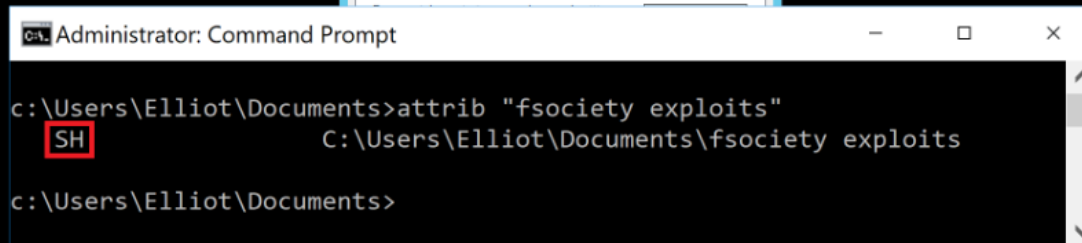
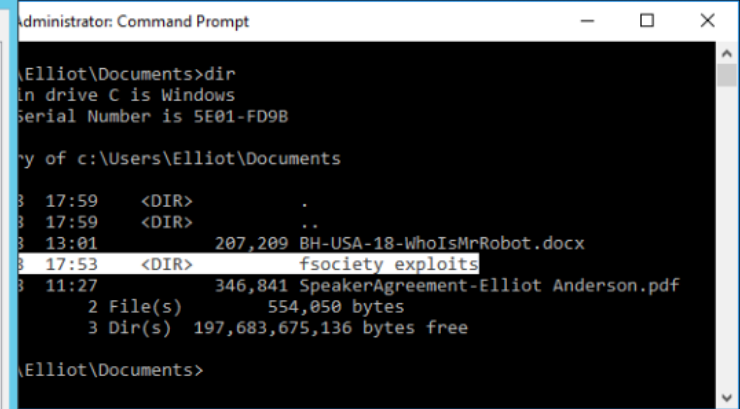


AVOIDING DISRUPTION

User's view



Attacker's view



Which one is fake?

The image displays three screenshots from a Windows environment. The top-left screenshot shows the command prompt output for creating a user named 'MR.Robot'. The 'Workstations allowed' property is set to 'All', which is circled in red. The top-right screenshot shows the command prompt output for creating a user named 'Elliot'. The 'Workstations allowed' property is also set to 'All'. The bottom screenshot is a PowerShell window showing a script that compares the 'LogonWorkstations' property of 'MR.Robot' and 'Elliot'. The output of the comparison is 'False', which is also circled in red. The PowerShell window also shows the user 'MR.Robot' is a member of the '*Domain Admins' group.

```
c:\>net user MR.Robot /domain
The request will be processed at a domain controller for domain cymptom.labs.

User name                MR.Robot
Full Name                 Mr. Robot
Comment                  We are all living in each other's paranoia
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

Password last set        7/16/2018 8:07:43 PM
Password expires         8/27/2018 8:07:43 PM
Password changeable      7/17/2018 8:07:43 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
Last logon

Logon hours allowed

Local Group Memberships
Global Group memberships
The command completed successfully

c:\>_
```

```
c:\>net user Elliot /domain
The request will be processed at a domain controller for domain cymptom.labs.

User name                Elliot
Full Name                 Elliot Alderson
Comment                  I don't even know what's real is any more
User's comment
Country/region code      000 (System Default)
Account active            Yes
Account expires           Never

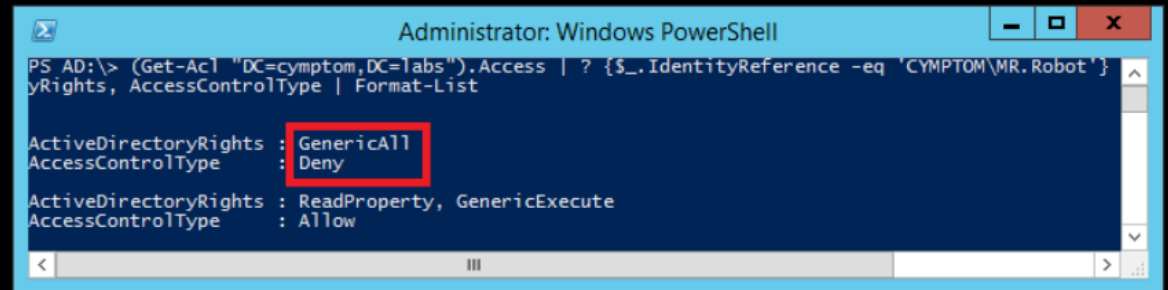
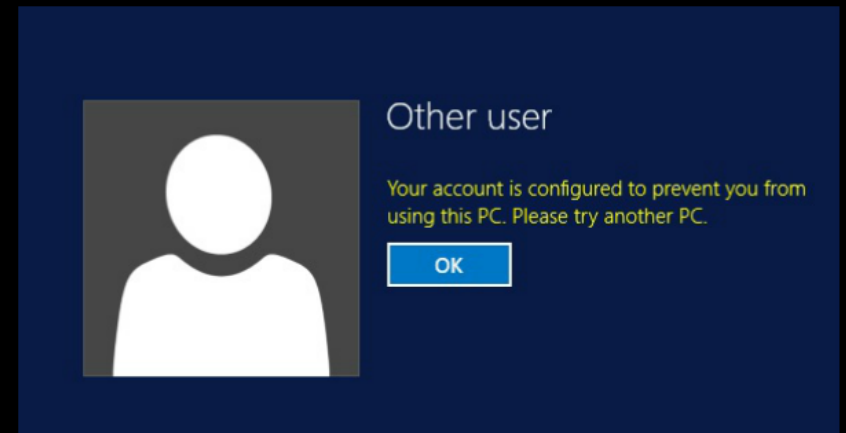
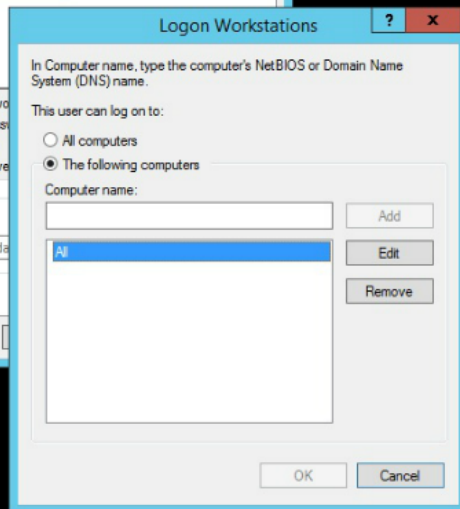
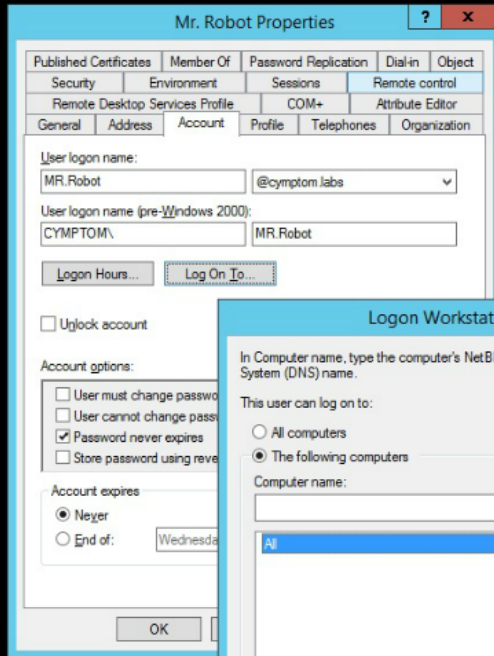
Password last set        7/16/2018 8:05:34 PM
Password expires         8/27/2018 8:05:34 PM
Password changeable      7/17/2018 8:05:34 PM
Password required        Yes
User may change password Yes

Workstations allowed     All
Logon script
User profile
Home directory
```

```
Windows PowerShell
PS C:\> $MRRobot = Get-ADUser MR.Robot -Properties LogonWorkstations
PS C:\> $Elliot = Get-ADUser Elliot -Properties LogonWorkstations
PS C:\> $MRRobot.LogonWorkstations -eq $Elliot.LogonWorkstations
False
PS C:\>

*Domain Admins
```

MINIMIZING RISK



THE TOOL

Reveal effective rights



- **Users (local/domain)**
- **Files/Folders**
- **Emails**
- **Registry**
- **Processes**
- **Active Directory objects**
- **Shares/Printers**

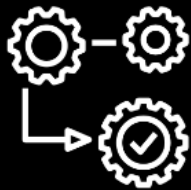


“True success requires sacrifice”

Rick Riordan



SOUND BYTES



**Effective deception requires
Believability and Diversity**



**Deception's achilles' heel lies in
practical business trade-offs**



**Beat deception by exploiting
disruption and risk precautions**

THANKS!

Assume Nothing. Question Everything.



@machosec



matan@cymptom.com



CYMP TOM