SPECTEROPS

Keep only those privileges that speak to your heart

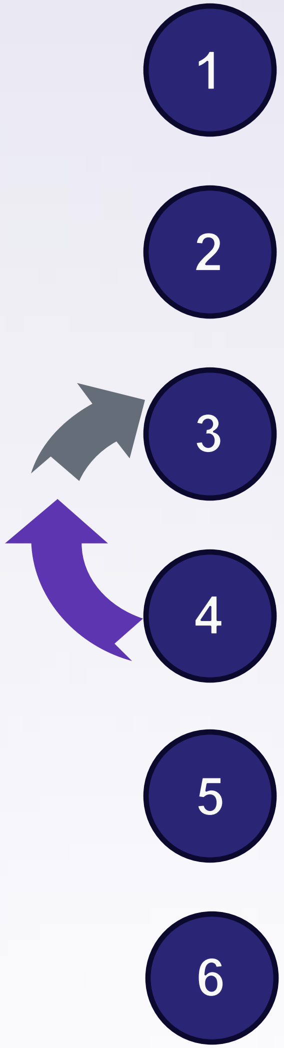
Automating Active Directory Privilege Clean-up

Luis F Monge Martinez

Journey

People cannot change their tidying habits without first changing their way of thinking.

Marie Kondo



1. Realizing we have a problem/s
2. Understanding “The problem”
3. Understanding how it affect us
4. Prioritize our problems
5. Help others
6. Pray and/or annoy

Luis F Monge Martínez

Endpoint and Active Directory security in EEAS.
Former Incident Handler, Incident Responder, Thread Hunter, Forensic Analyst, Cybersecurity Investigator, IT admin, IT supp., communications operator…

Data analysis lover and in love with Jupyter Notebooks.

Medium: @luckyluk3
GitHub: lucky-luk3

Realizing we have a problem

The wake up!

The wake up

From routine to incertitude

The wake up

From routine to incertitude

The wake up

From routine to incertitude

How many admins do we have on our systems?

The wake up

From routine to incertitude

Domain admins?
Schema admins?
Local admins?
DB admins?

The wake up

From routine to incertitude

The wake up

From routine to incertitude

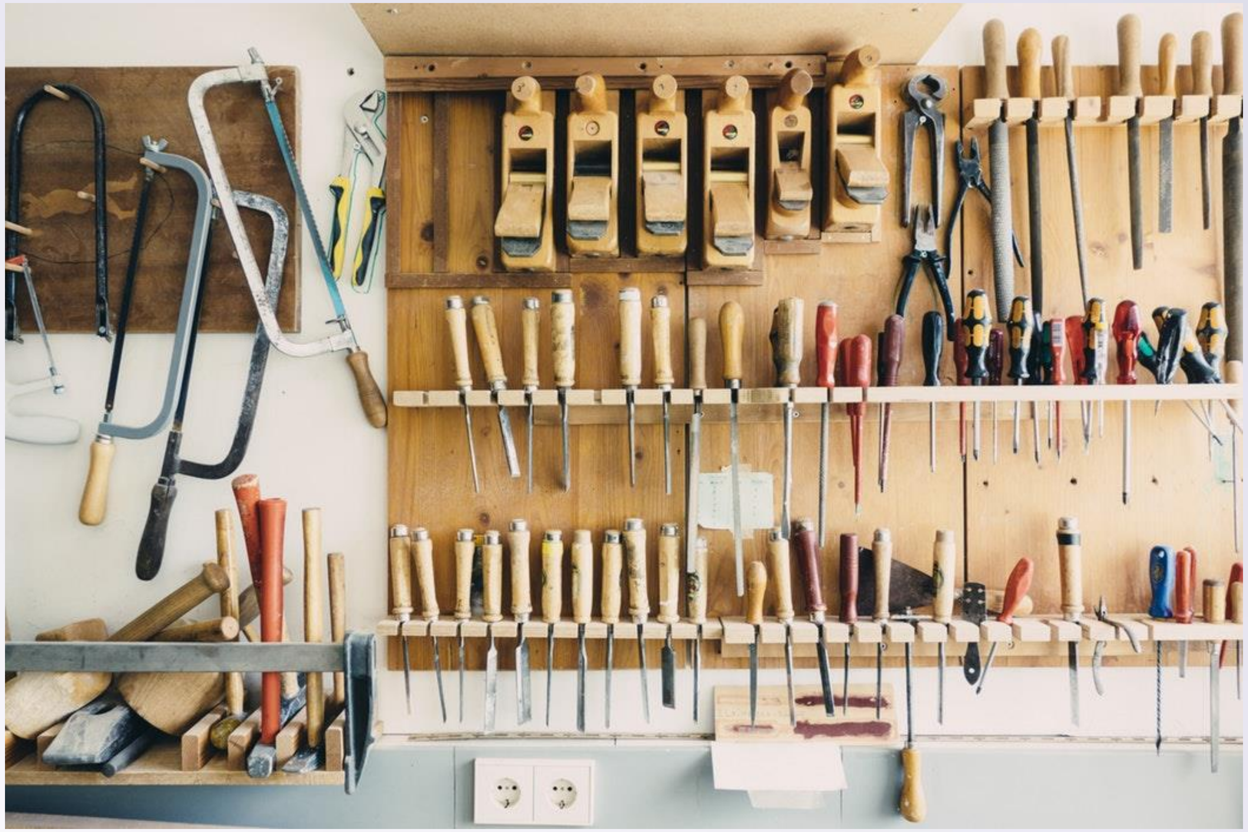
What does admin mean?
Is everyone admin in some way?
Am I the admin of myself?

The wake up

From routine to incertitude

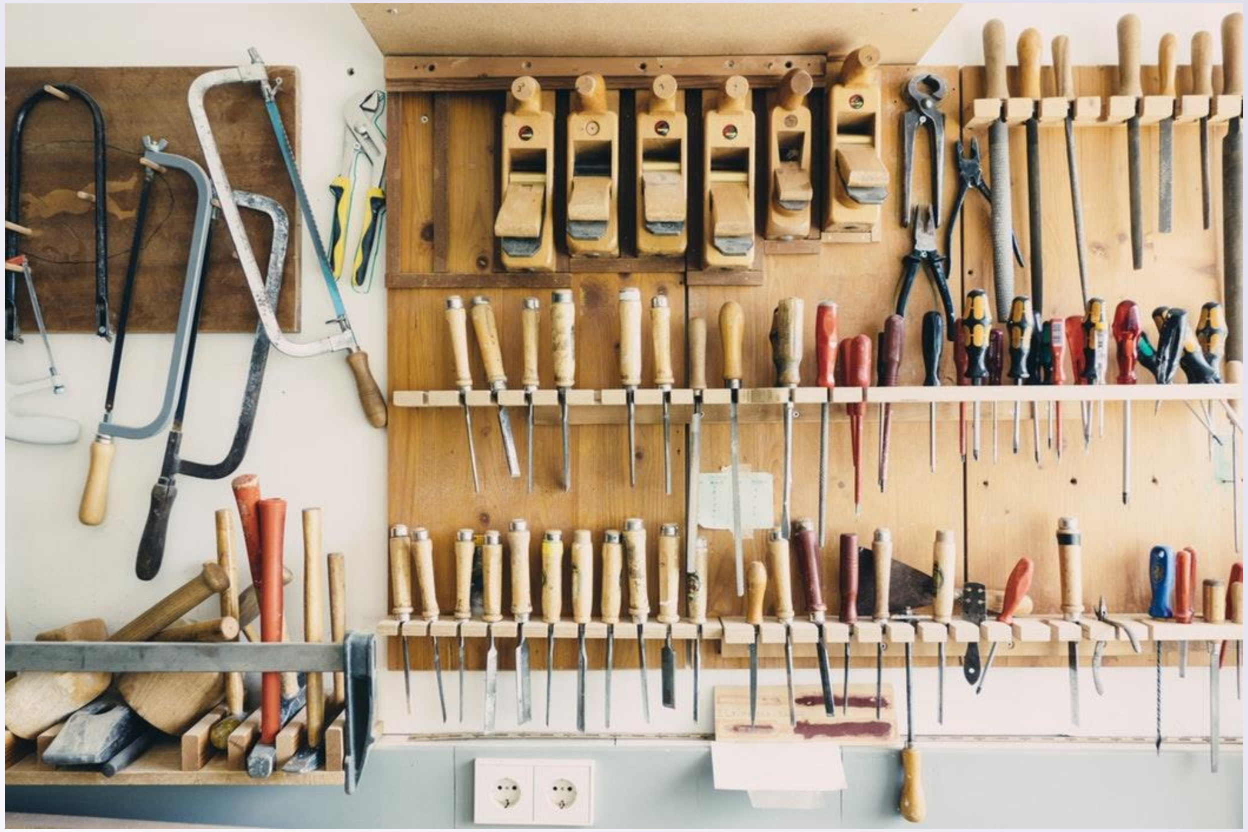
Understanding “The problem”

Let´s focus on Active Directory



The problem

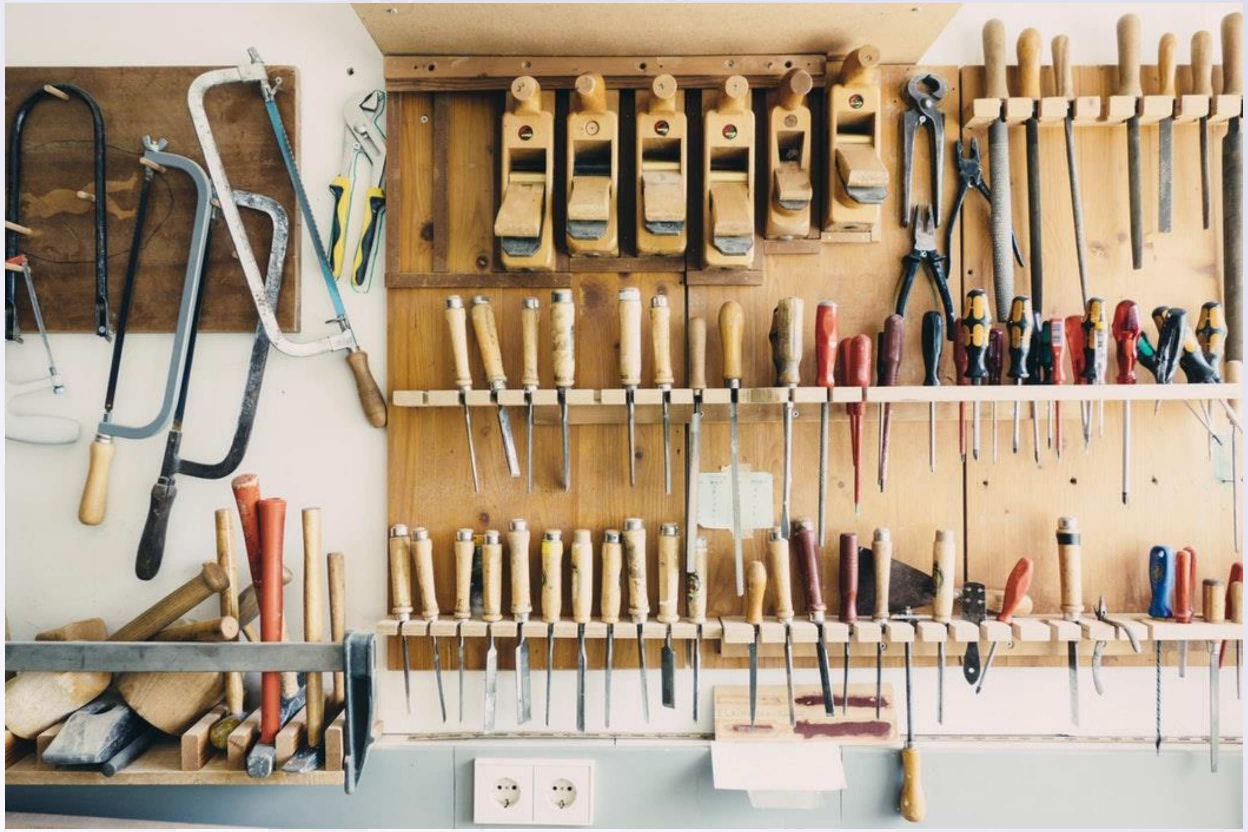
If you think the solution to a problem is only technical, you are not understanding the problem.



The problem

A fool with a tool is still a fool.

Grady Booch



The problem

Lack of knowledge

- Even if everybody uses AD almost nobody really understands it.
- Excessive rights by default.
- Impact in case of compromise.

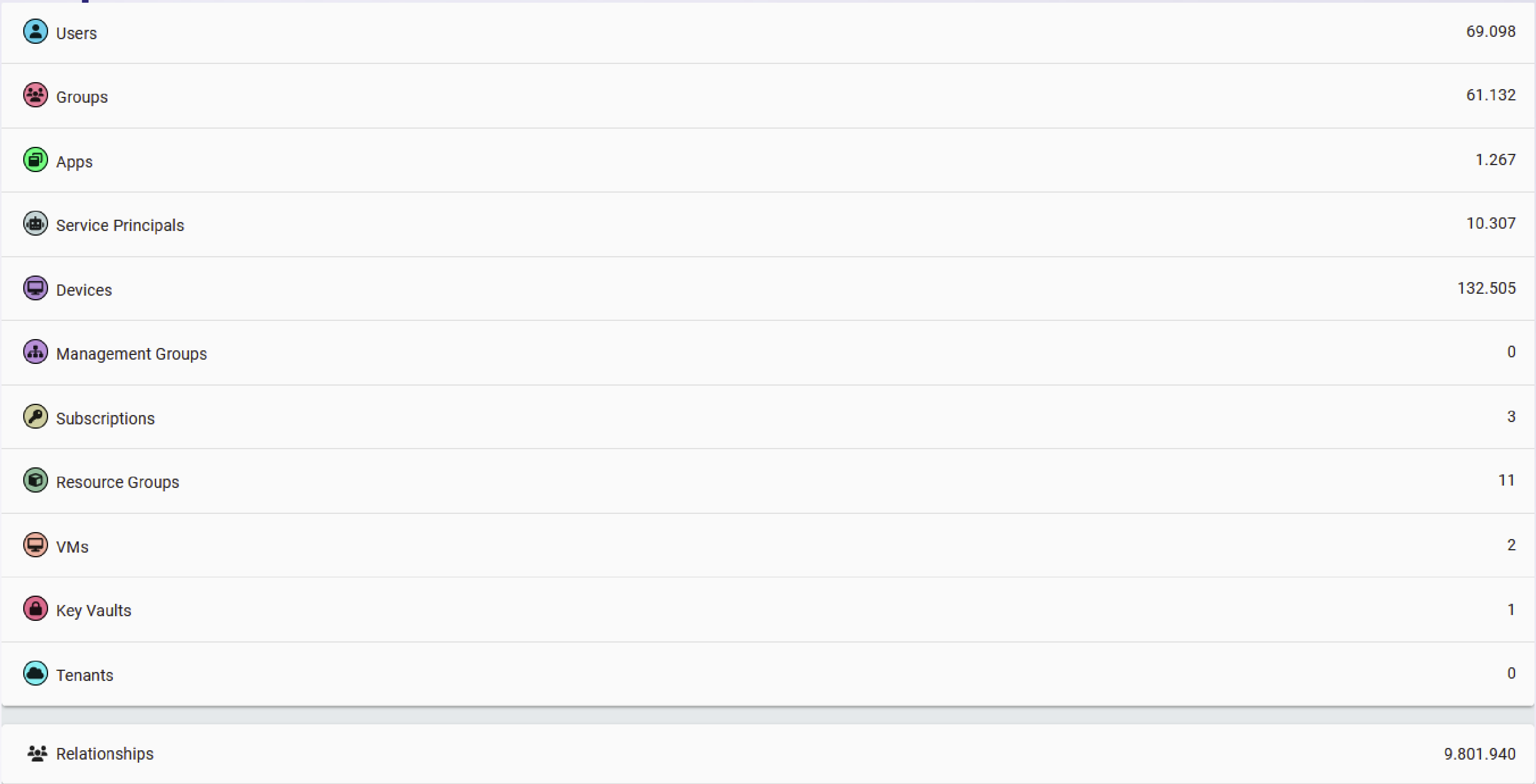
Show must go on!

- An excessive focus on operations.
- The most over privileged the easiest for operations.
- Security in AD is time demanding and problematic.

Lack of tools

- Native tools…
- Commercial tools focus on compliance.
- Open Source or free tools focused in AD configurations.
- EDRs somehow.
- Now BloodHound Enterprise!! Finally!

The problem



Users	69.098
Groups	61.132
Apps	1.267
Service Principals	10.307
Devices	132.505
Management Groups	0
Subscriptions	3
Resource Groups	11
VMs	2
Key Vaults	1
Tenants	0
Relationships	9.801.940

Understanding “our” problem

Get on with it!

Our problem

Increasing visibility

Our problem

Increasing visibility

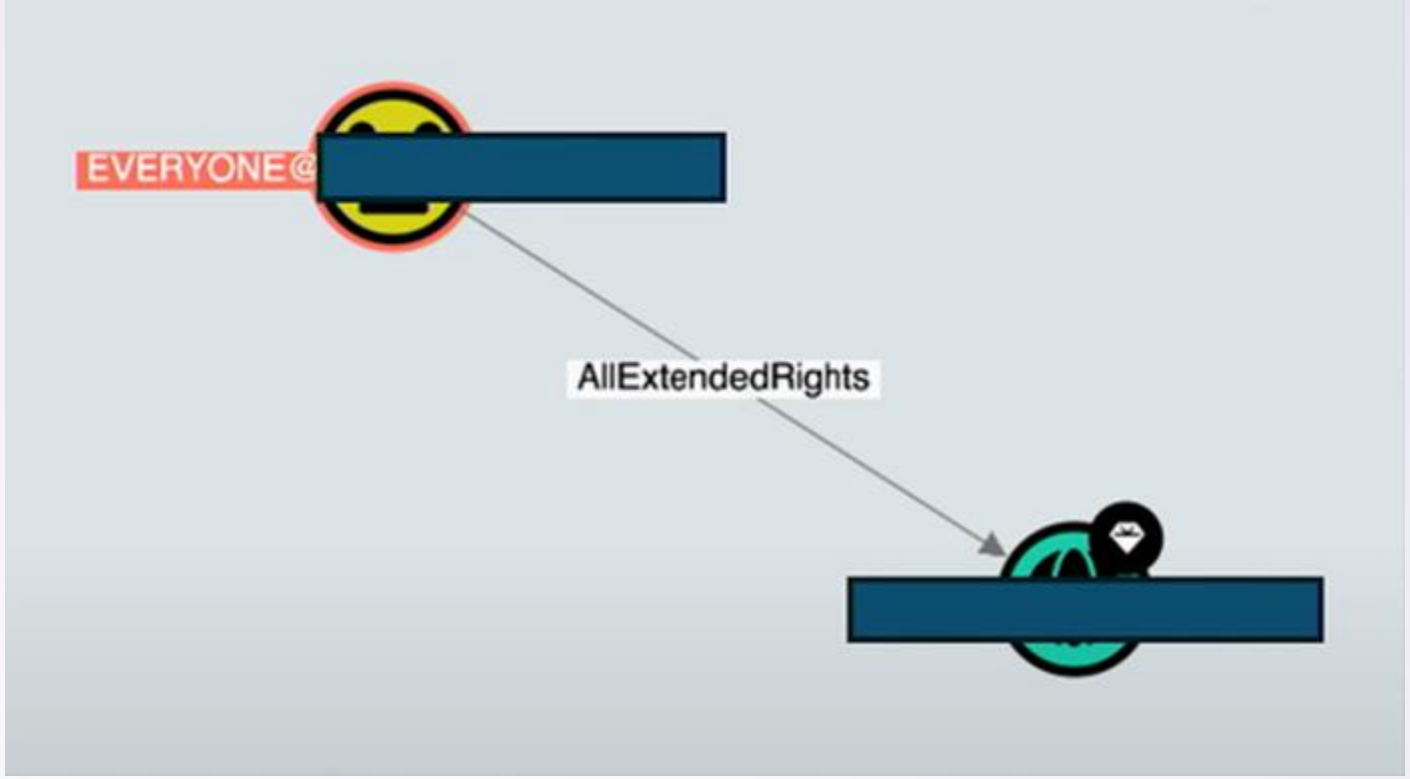
BLOODHOUND
COMMUNITY EDITION

Easy to deploy
https://github.com/SpecterOps/bloodhound-cli

Remove these today:
https://www.linkedin.com/pulse/find-fix-three-common-ad-issues-andy-robbins/

Our problem

Increasing visibility



Our problem

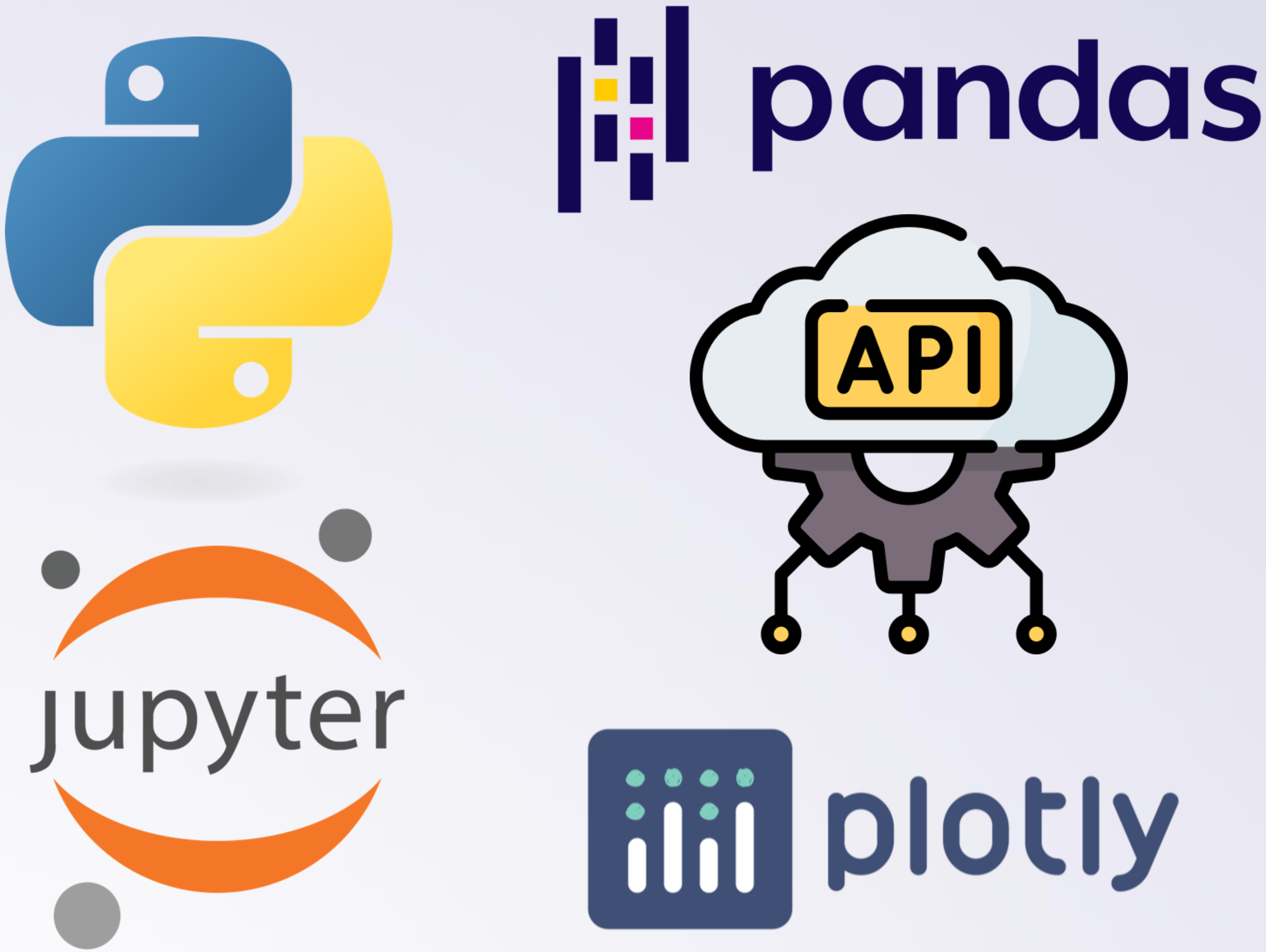
Increasing visibility

Justin Kohler
The BloodHound Enterprise State of Attack Path Management
https://youtu.be/mm5LU3cX6lU?si=yW6xTYR2x3TfgjTV

BLOODHOUND
ENTERPRISE

Our problem

Increasing visibility



Our problem

Our data - SharpHound

- Aces
- admincount
- allowedtodelegate
- ContainedBy
- description
- displayname
- distinguishedname
- domain
- DomainSID
- dontreqpreauth
- email
- enabled
- encryptedtextpwdallowed
- gmsa
- HasSIDHistory
- hasspn
- homedirectory
- IsACLProtected
- IsDeleted
- lastlogon
- lastlogontimestamp
- lockedout
- logonscript
- logonscriptenabled
- name
- ObjectIdentifier
- passwordcantchange
- passwordexpired
- passwordnotreqd
- PrimaryGroupSID
- profilepath
- pwdlastset
- pwdneverexpires
- reconcile
- samaccountname
- sensitive
- serviceprincipalnames
- sfupassword
- sidhistory
- smartcardrequired
- SPNTargets
- supportedencryptiontypes
- title
- trustedtoauth
- UnconstrainedDelegation
- unicodepassword
- unixpassword
- usedeskeyonly
- useraccountcontrol
- userpassword
- whencreated

Our problem

Our data - SharpHound

- Aces
- admincount
- allowedtodelegate
- ContainedBy
- description
- displayname
- distinguishedname
- domain
- DomainSID
- dontreqpreauth
- email
- enabled
- encryptedtextpwdallowed
- gmsa
- HasSIDHistory
- hasspn
- homedirectory
- IsACLProtected
- IsDeleted
- lastlogon
- lastlogontimestamp
- lockedout
- logonscript
- logonscriptenabled
- name
- ObjectIdentifier
- passwordcantchange
- passwordexpired
- passwordnotreqd
- PrimaryGroupSID
- profilepath
- pwdlastset
- pwdneverexpires
- reconcile
- samaccountname
- sensitive
- serviceprincipalnames
- sfupassword
- sidhistory
- smartcardrequired
- SPNTargets
- supportedencryptiontypes
- title
- trustedtoauth
- UnconstrainedDelegation
- unicodepassword
- unixpassword
- usedeskeyonly
- useraccountcontrol
- Userpassword
- whencreated

Our problem

Our data - BloodHound

- admincount
- adminRights
- allowedtodelegate
- constrainedDelegation
- controllables
- controllers
- dcomRights
- description
- displayname
- distinguishedname
- domain
- domainsid
- dontreqpreauth
- email
- enabled
- encryptedtextpwdallowed
- gmsa
- gpos
- groupMembership
- hasspn
- highvalue
- homedirectory
- isaclprotected
- lastlogon
- lastlogontimestamp
- lastseen
- lockedout
- logonscript
- logonscriptenabled
- name
- objectid
- passwordcantchange
- passwordexpired
- passwordnotreqd
- profilepath
- psRemoteRights
- pwdlastset
- pwdneverexpires
- rdpRights
- samaccountname
- sensitive
- serviceprincipalnames
- sessions
- sidhistory
- smartcardrequired
- sqlAdmin
- supportedencryptiontypes
- system_tags
- title
- trustedtoauth
- unconstraineddelegation
- usedeskeyonly
- useraccountcontrol
- whencreated

Our problem

Our data - BloodHound

admincount	enabled	logonscriptenabled	sessions
adminRights	encryptedtextpwdallowed	name	sidhistory
allowedtodelegate	gmsa	objectid	smartcardrequired
constrainedDelegation	gpos	passwordcantchange	sqlAdmin
controllables	groupMembership	passwordexpired	supportedencryptiontypes
controllers	hasspn	passwordnotreqd	system_tags
dcomRights	highvalue	profilepath	title
description	homedirectory	psRemoteRights	trustedtoauth
displayname	isaclprotected	pwdlastset	unconstraineddelegation
distinguishedname	lastlogon	pwdneverexpires	usedeskeyonly
domain	lastlogontimestamp	rdpRights	useraccountcontrol
domainsid	lastseen	samaccountname	whencreated
dontreqpreauth	lockedout	sensitive	
email	logonscript	serviceprincipalnames	

Our problem

Our data – Processing data

Scan with SharpHound

Process JSON data extracting names, UID, ACES and Properties

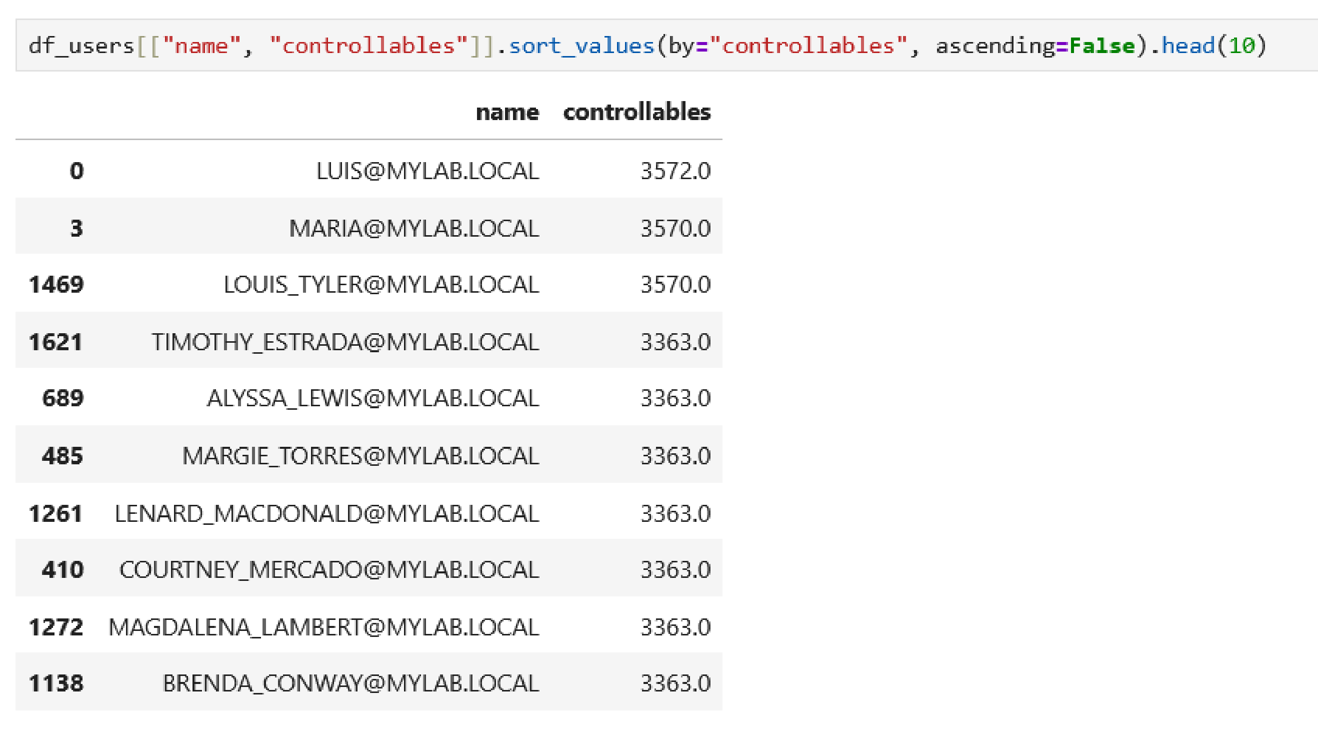
Ask BHCE API for extender info

Create Pandas Dataframe

Our problem

Making the correct questions

- What are the most privileged Users/Groups?
  - Controllables
  - Filtering
  - Name convention
  - Grouping
  - Plotting
  - Export to SCV
  - …



```
df_users[["name", "controllables"]].sort_values(by="controllables", ascending=False).head(10)
```

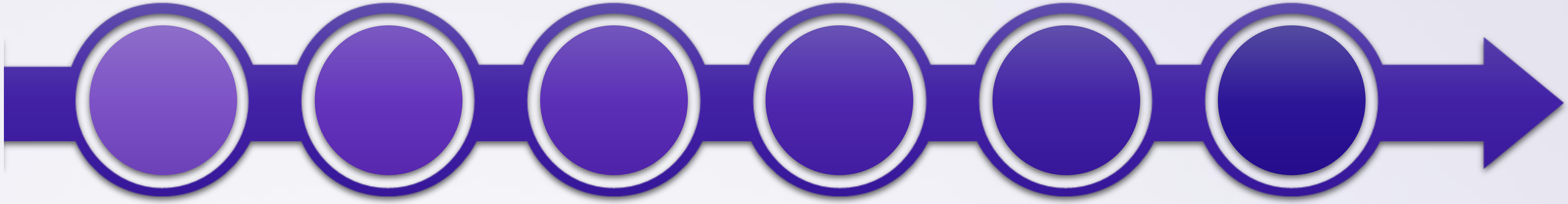
	name	controllables
0	LUIS@MYLAB.LOCAL	3572.0
3	MARIA@MYLAB.LOCAL	3570.0
1469	LOUIS_TYLER@MYLAB.LOCAL	3570.0
1621	TIMOTHY_ESTRADA@MYLAB.LOCAL	3363.0
689	ALYSSA_LEWIS@MYLAB.LOCAL	3363.0
485	MARGIE_TORRES@MYLAB.LOCAL	3363.0
1261	LENARD_MACDONALD@MYLAB.LOCAL	3363.0
410	COURTNEY_MERCADO@MYLAB.LOCAL	3363.0
1272	MAGDALENA_LAMBERT@MYLAB.LOCAL	3363.0
1138	BRENDA_CONWAY@MYLAB.LOCAL	3363.0

Prioritize problems

Let´s make this more professional

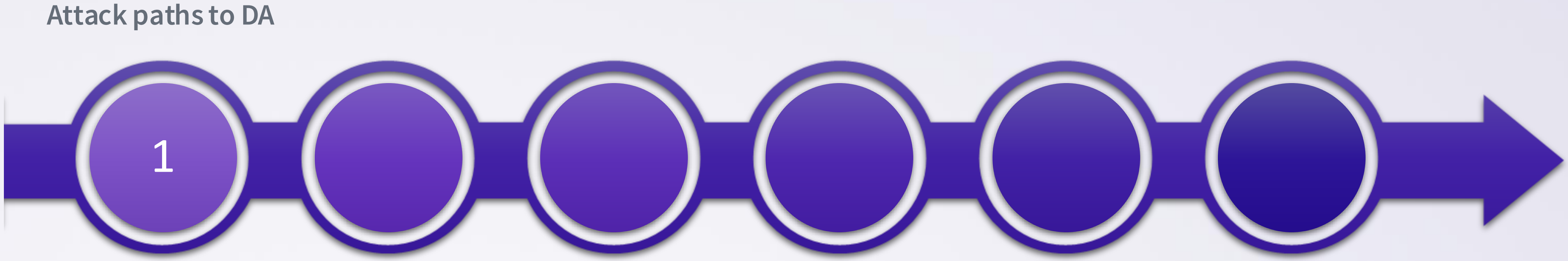
Risk process

From mess to order



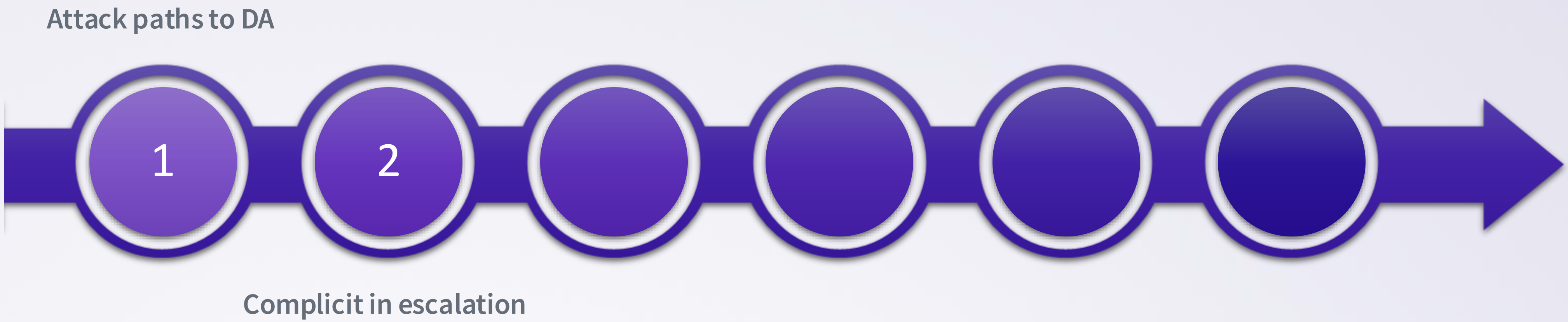
Risk process

From mess to order



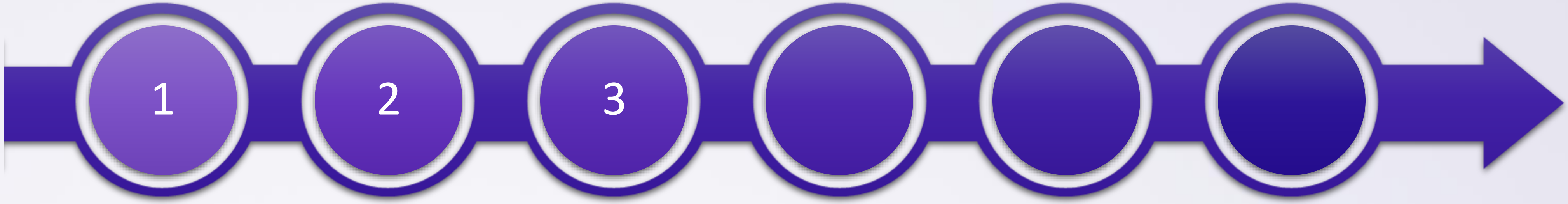
Risk process

From mess to order



Risk process

From mess to order



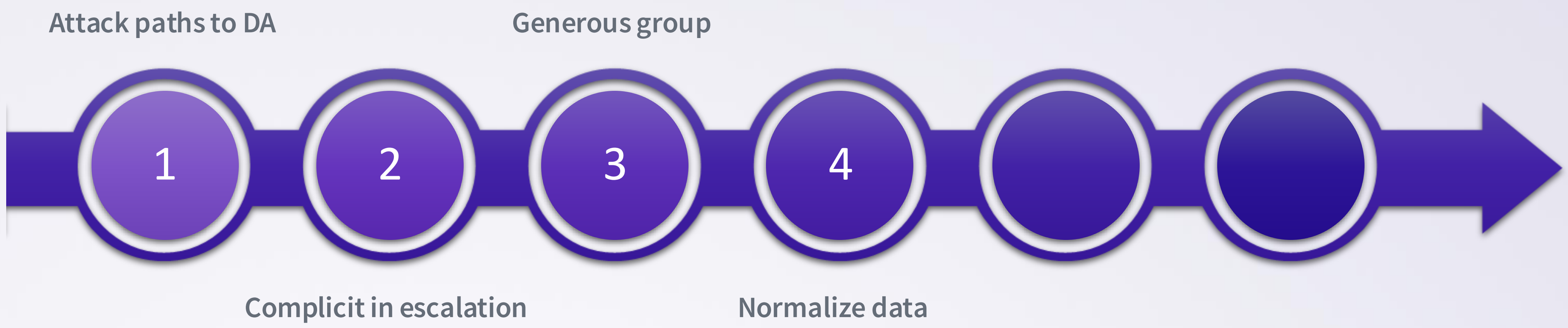
Attack paths to DA

Complicit in escalation

Generous group

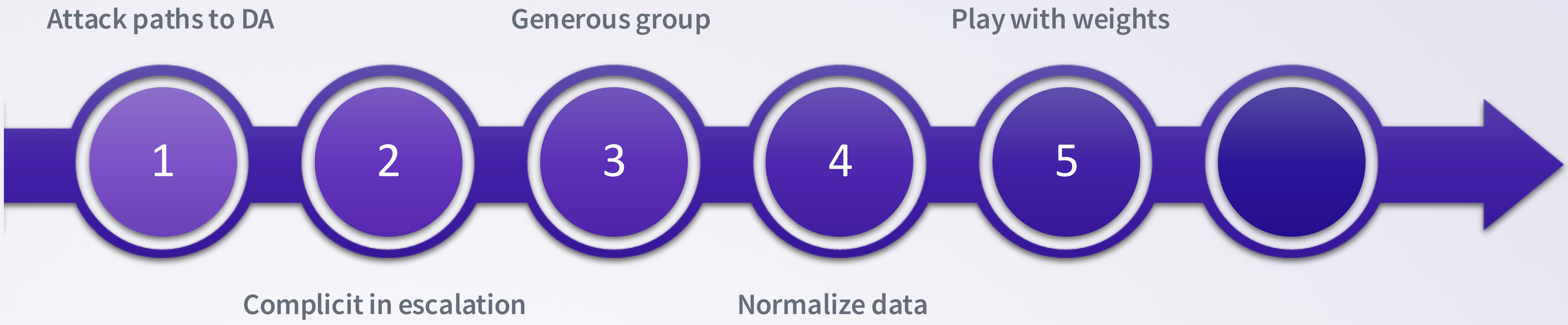
Risk process

From mess to order



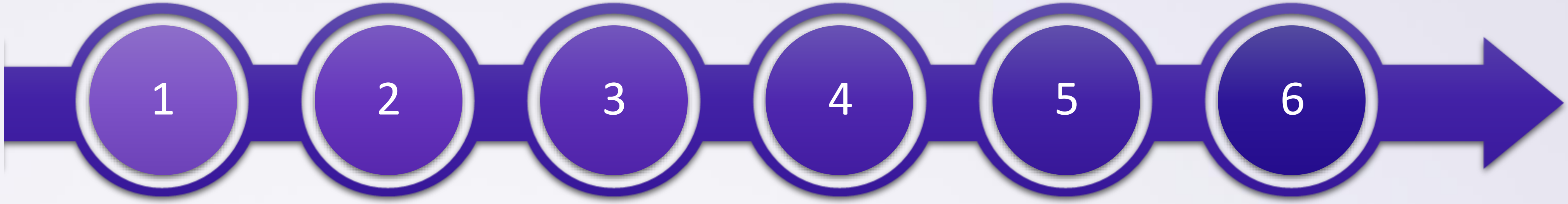
Risk process

From mess to order



Risk process

From mess to order



Attack paths to DA

Complicit in escalation

Generous group

Normalize data

Play with weights

Calculate risk

Risk process

From mess to order

Users

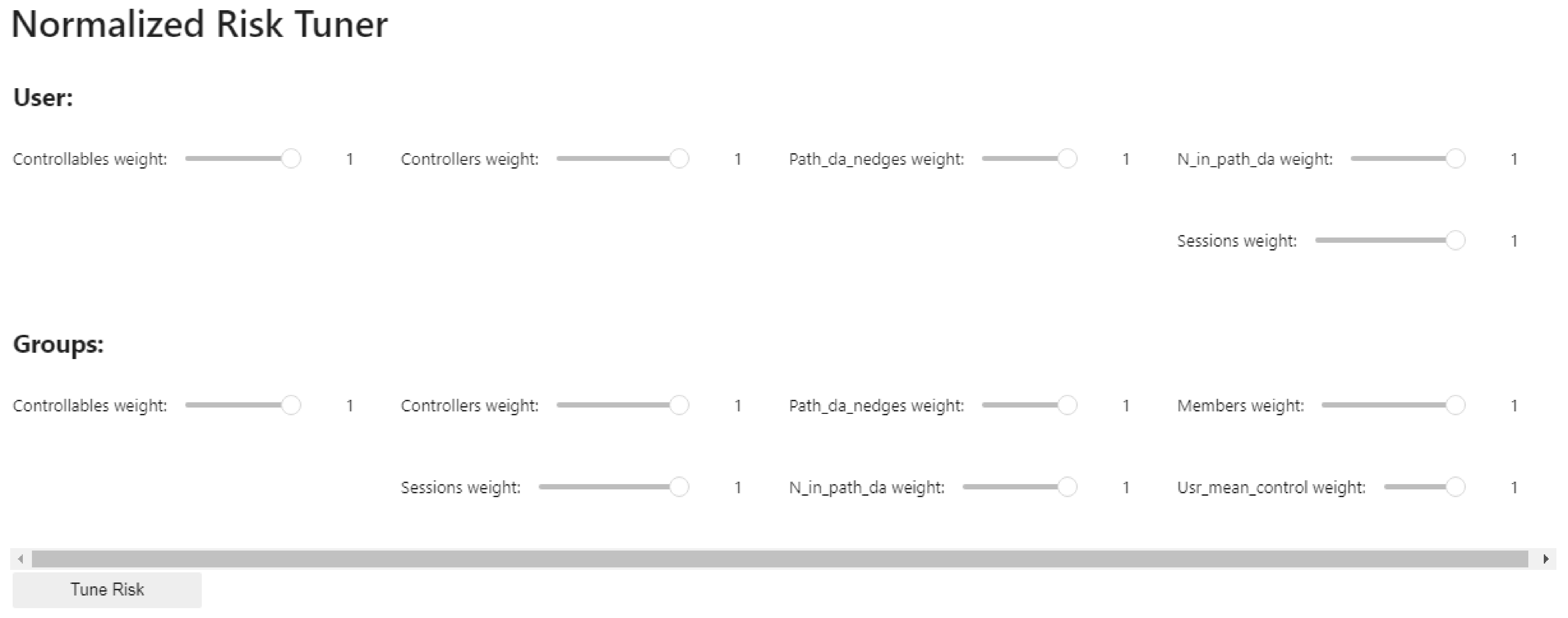
- **Controllables**
- **Controllers**
- **Path to Domain Admins (Number of Edges)**
- **In path to Domain Admins (Number)**
- **Sessions**

Groups

- **Controllables**
- **Controllers**
- **Path to Domain Admins (Number of Edges)**
- **In path to Domain Admins (Number)**
- **Sessions**
- **Members**
- **Mean members controllers – Group controllers (Inverted)**

Risk process

From mess to order



Normalized Risk Tuner

User:

Controllables weight: 1

Controllers weight: 1

Path_da_nedges weight: 1

N_in_path_da weight: 1

Sessions weight: 1

Groups:

Controllables weight: 1

Controllers weight: 1

Path_da_nedges weight: 1

Members weight: 1

Sessions weight: 1

N_in_path_da weight: 1

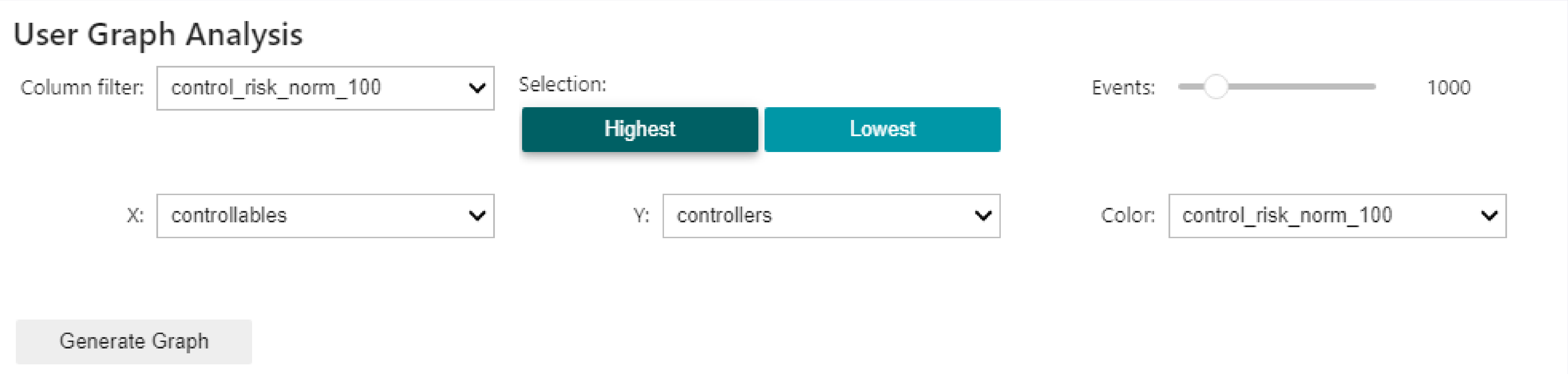
Usr_mean_control weight: 1

Understanding “our” problem

Again and better

The complicated problems

The need of understanding the data



User Graph Analysis

Column filter: control_risk_norm_100

Selection:

Events: 1000

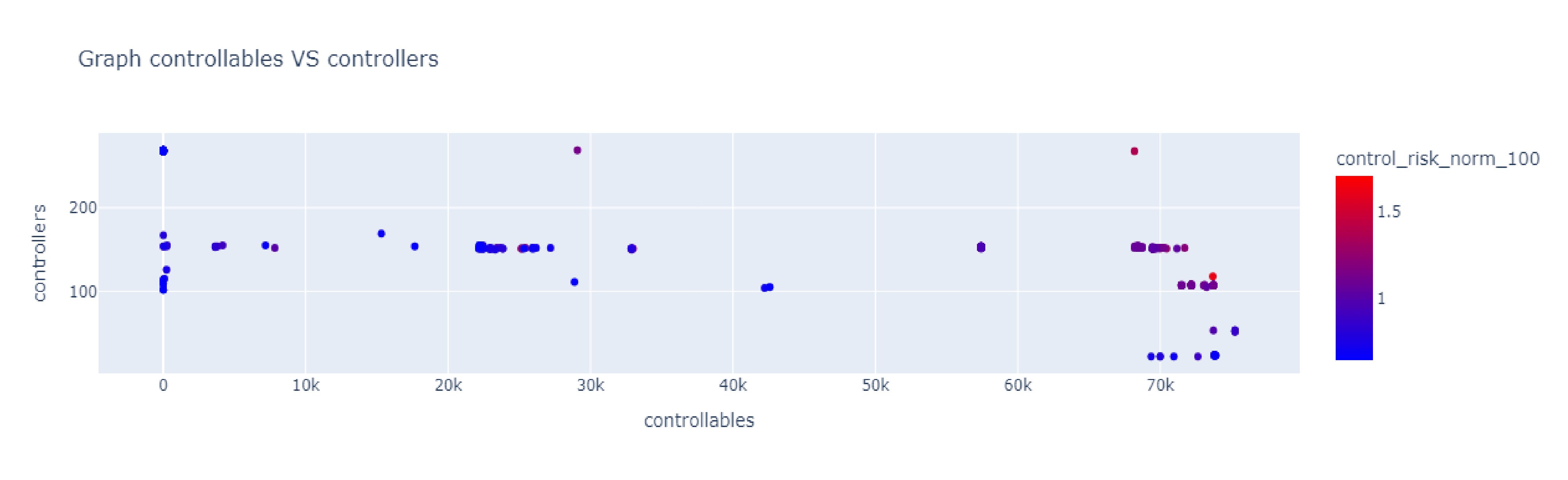
X: controllables

Y: controllers

Color: control_risk_norm_100

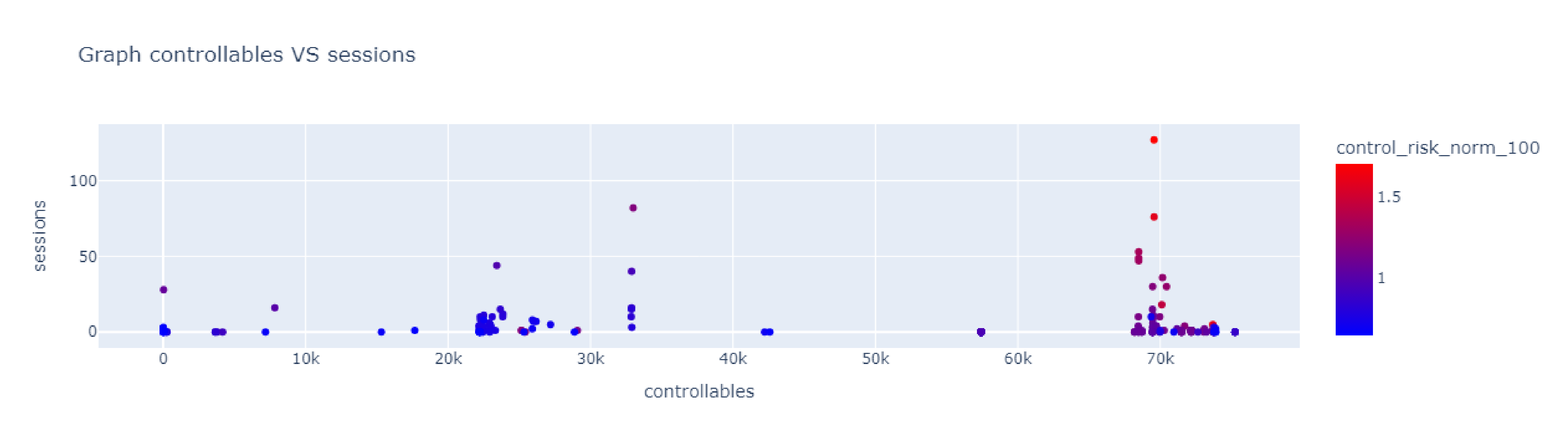
The complicated problems

The need of understanding the data



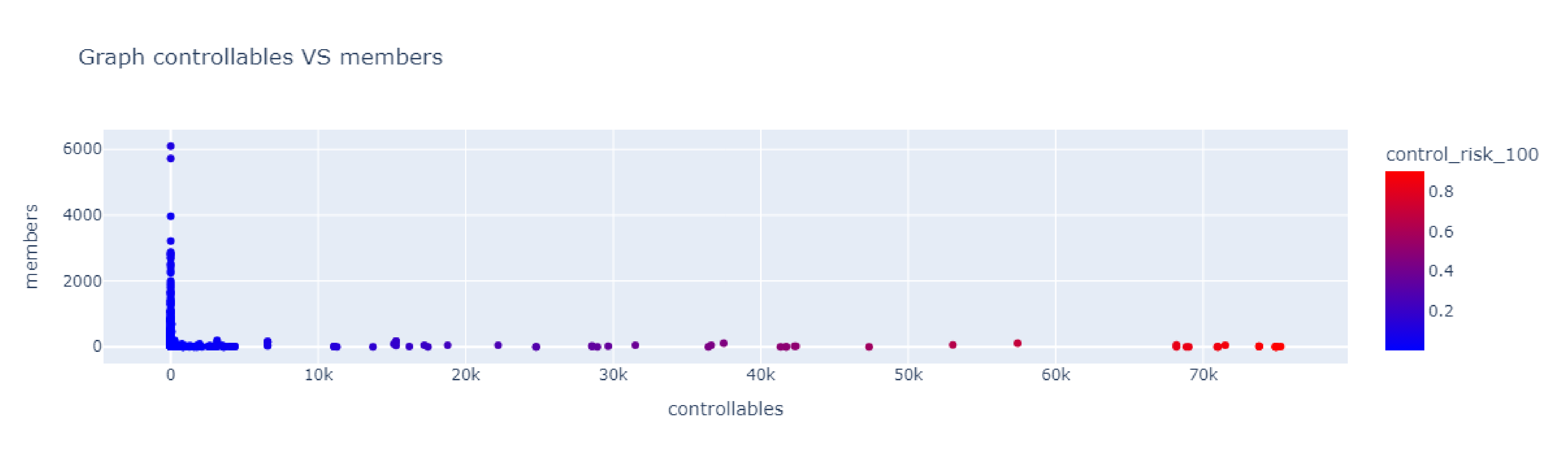
The complicated problems

The need of understanding the data



The complicated problems

The need of understanding the data



The complicated problems

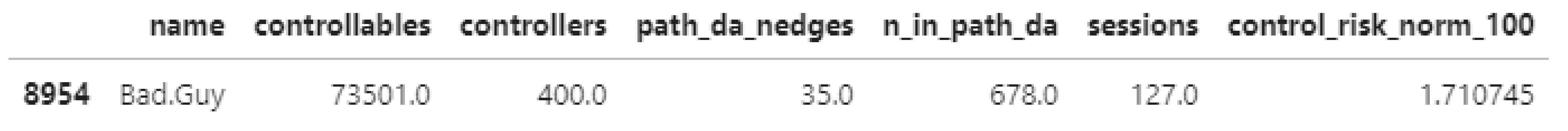
The need of understanding the data

Helping others (Optional)

Understanding the problem. Yes, again.

Helping others

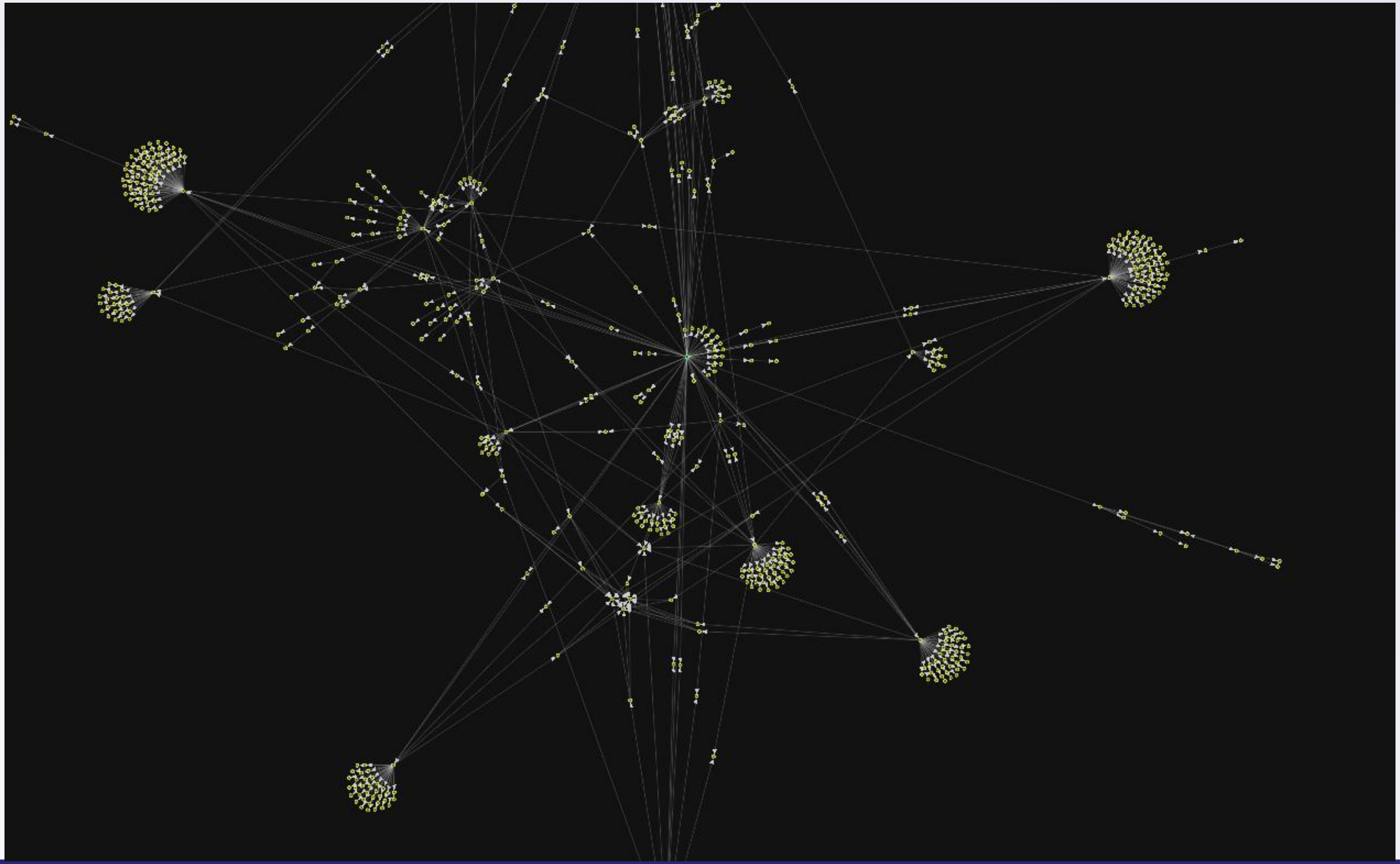
Understanding the root cause



	name	controllables	controllers	path_da_nedges	n_in_path_da	sessions	control_risk_norm_100
8954	Bad.Guy	73501.0	400.0	35.0	678.0	127.0	1.710745

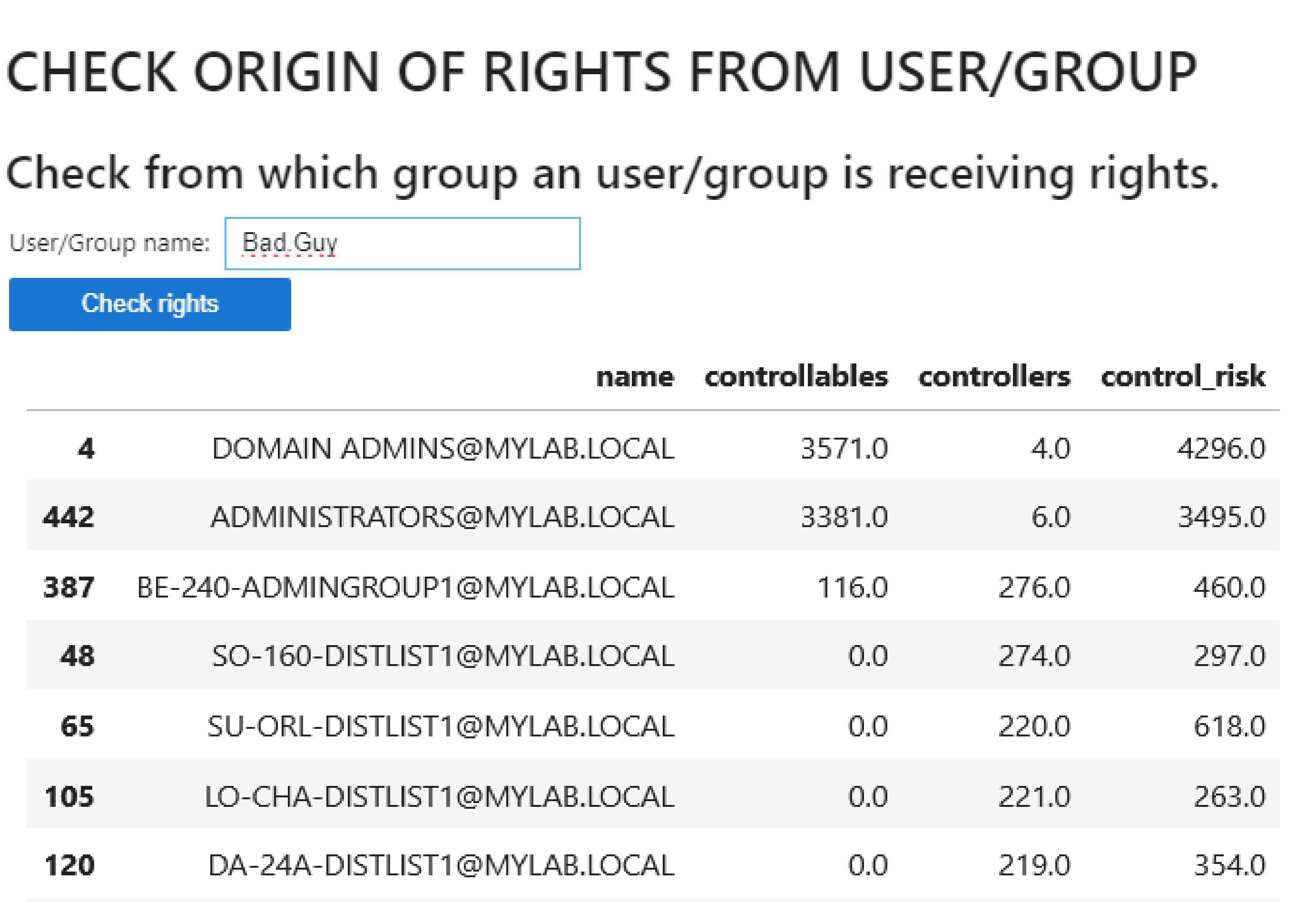
Helping others

Understanding the root cause



Helping others

Understanding the root cause



CHECK ORIGIN OF RIGHTS FROM USER/GROUP

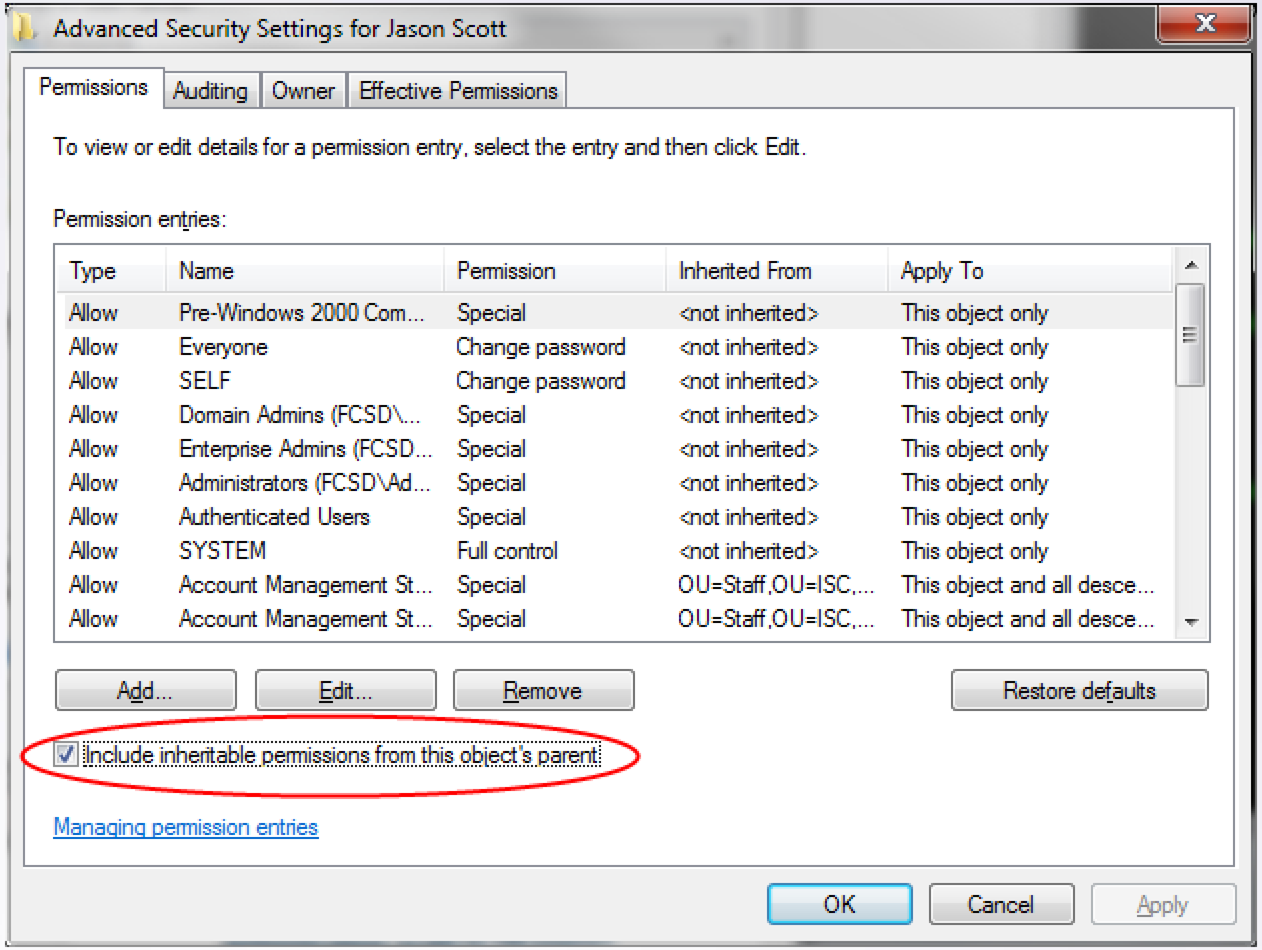
Check from which group an user/group is receiving rights.

User/Group name: Bad.Guy

	name	controllables	controllers	control_risk
4	DOMAIN ADMINS@MYLAB.LOCAL	3571.0	4.0	4296.0
442	ADMINISTRATORS@MYLAB.LOCAL	3381.0	6.0	3495.0
387	BE-240-ADMINGROUP1@MYLAB.LOCAL	116.0	276.0	460.0
48	SO-160-DISTLIST1@MYLAB.LOCAL	0.0	274.0	297.0
65	SU-ORL-DISTLIST1@MYLAB.LOCAL	0.0	220.0	618.0
105	LO-CHA-DISTLIST1@MYLAB.LOCAL	0.0	221.0	263.0
120	DA-24A-DISTLIST1@MYLAB.LOCAL	0.0	219.0	354.0

Helping others

Understanding the root cause



Advanced Security Settings for Jason Scott

To view or edit details for a permission entry, select the entry and then click Edit.

Permission entries:

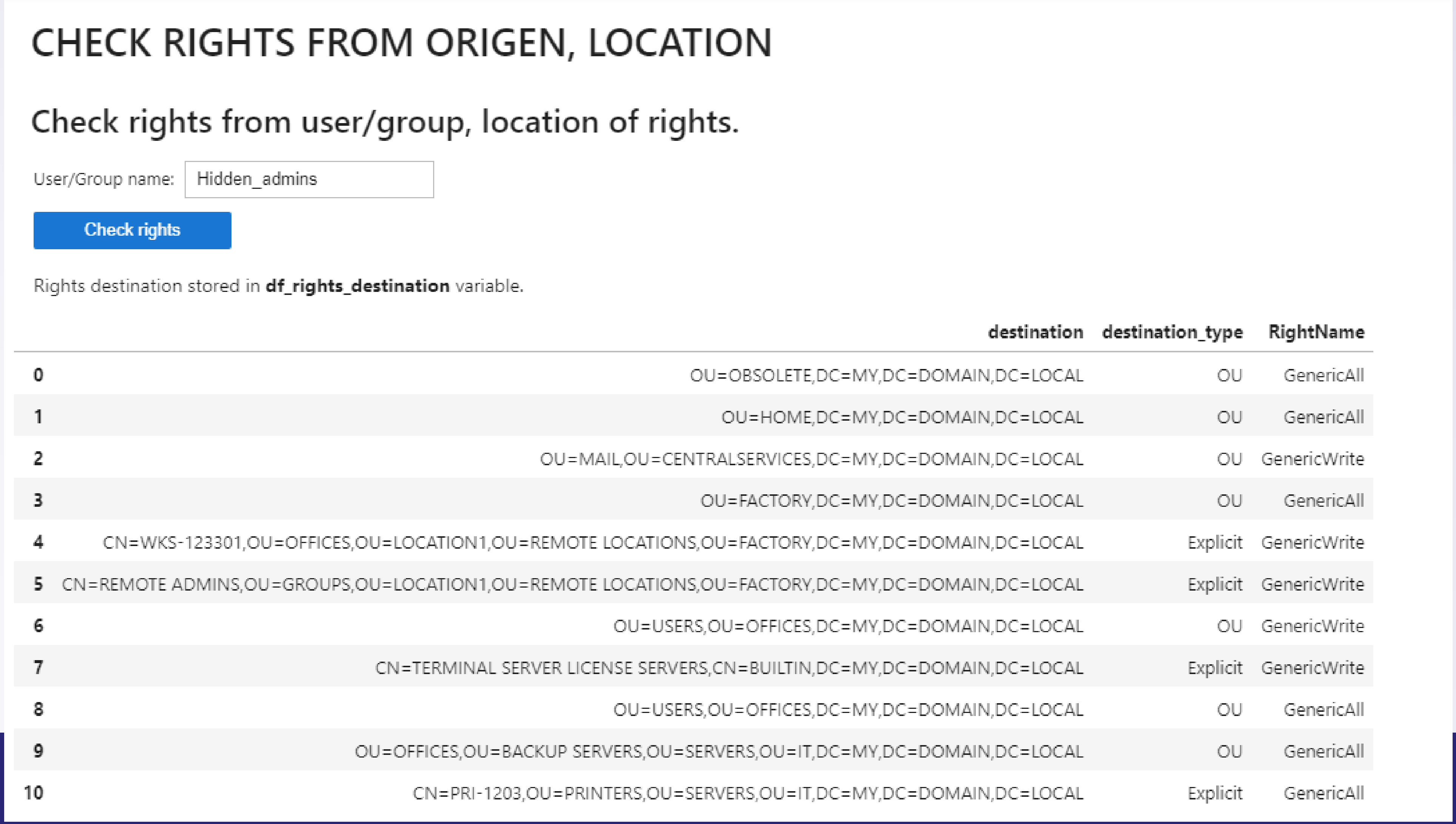
Type	Name	Permission	Inherited From	Apply To
Allow	Pre-Windows 2000 Com...	Special	<not inherited>	This object only
Allow	Everyone	Change password	<not inherited>	This object only
Allow	SELF	Change password	<not inherited>	This object only
Allow	Domain Admins (FCSD\...	Special	<not inherited>	This object only
Allow	Enterprise Admins (FCSD...	Special	<not inherited>	This object only
Allow	Administrators (FCSD\Ad...	Special	<not inherited>	This object only
Allow	Authenticated Users	Special	<not inherited>	This object only
Allow	SYSTEM	Full control	<not inherited>	This object only
Allow	Account Management St...	Special	OU=Staff,OU=ISC,...	This object and all desce...
Allow	Account Management St...	Special	OU=Staff,OU=ISC,...	This object and all desce...

☑ Include inheritable permissions from this object's parent

Managing permission entries

Helping others

Understanding the root cause



CHECK RIGHTS FROM ORIGEN, LOCATION

Check rights from user/group, location of rights.

User/Group name: Hidden_admins

Rights destination stored in **df_rights_destination** variable.

	destination	destination_type	RightName
0	OU=OBSOLETE,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
1	OU=HOME,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
2	OU=MAIL,OU=CENTRALSERVICES,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericWrite
3	OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
4	CN=WKS-123301,OU=OFFICES,OU=LOCATION1,OU=REMOTE LOCATIONS,OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericWrite
5	CN=REMOTE ADMINS,OU=GROUPS,OU=LOCATION1,OU=REMOTE LOCATIONS,OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericWrite
6	OU=USERS,OU=OFFICES,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericWrite
7	CN=TERMINAL SERVER LICENSE SERVERS,CN=BUILTIN,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericWrite
8	OU=USERS,OU=OFFICES,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
9	OU=OFFICES,OU=BACKUP SERVERS,OU=SERVERS,OU=IT,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
10	CN=PRI-1203,OU=PRINTERS,OU=SERVERS,OU=IT,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericAll

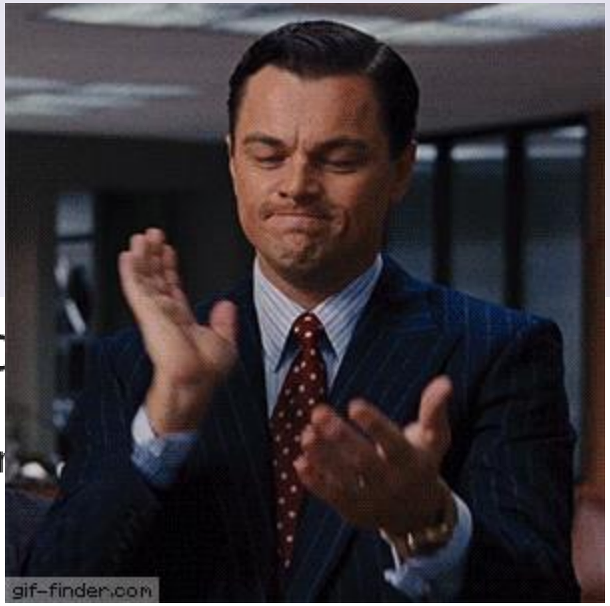
Helping others

Understanding the root cause

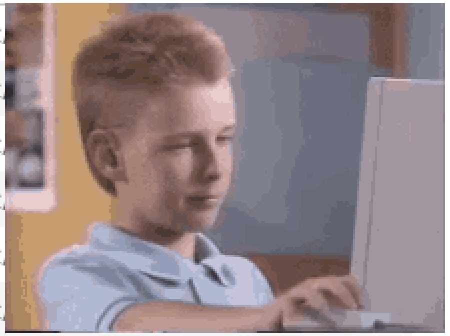
HTS FROM ORIGEN, LOC

om user/group, location of r

n_admins



Rights destination stored in **df_rights_destination** variable.



	destination	destination_type	RightName
0	OU=OBSOLETE,DC=MY,DC=DOMAIN,DC=LOC		
1	OU=HOME,DC=MY,DC=DOMAIN,DC=LOC		
2	MAIL,OU=CENTRALSERVICES,DC=MY,DC=DOMAIN,DC=LOC		
3	OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOC		
4	CN=WKS-123301,OU= TE LOCATIONS,OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOC		
5	CN=REMOTE ADMINS,OU= TE LOCATIONS,OU=FACTORY,DC=MY,DC=DOMAIN,DC=LOC		
6	OU=USERS,OU=OFFICES,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericWrite
7	ICENSE SERVERS,CN=BUILTIN,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericWrite
8	OU=USERS,OU=OFFICES,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
9	OU=OFFICES,OU=BACKUP SERVERS,OU=SERVERS,OU=IT,DC=MY,DC=DOMAIN,DC=LOCAL	OU	GenericAll
10	CN=PRI-1203,OU=PRINTERS,OU=SERVERS,OU=IT,DC=MY,DC=DOMAIN,DC=LOCAL	Explicit	GenericAll

Pray and/or annoy

Annoy!

The solution

People don't do what you expect but what you inspect.

Louis V. Gerstner

The solution

If you want to go fast, go alone. If you want to go far, go together.

African proverb

Demo!

Sum up

- Educate our admins.
  - Policies.
  - Project admin ≠ AD admin.
  - Temporary rights.
  - Rights segregations.
- Use data visualization.
- Try to help others.

Sum up

- Educate our admins.
  - Policies.
  - Project admin ≠ AD admin.
  - Temporary rights.
  - Rights segregations.
- Use data visualization.
- Try to help others.

If you don´t know your domain, nobody will do it for you.

Thank you

Questions?

Luis F Monge Martinez