Change Auditor Cyberattack Mitigation Best Practices

Searches | Protection Templates

Quest®

Where Next Meets Now.

Change Auditor
Suggested Alerts / Searches

- Irregular Domain Controller Registration Events (DCShadow)
- Irregular Domain Replication Activity Events (DCSync)
- NTLMv1 & NTLM v2 (Needs Logon Activity Module)
- Kerberos user ticket events that exceed the maximum ticket lifetime (Golden Ticket) (Needs Logon Activity Module)
- Changes by Human vs. IAM
- Service account used out of band
- Changes to Membership of local “administrators” group
- DACL changes on Domain container
- SPN added
- Searches for unconstrained and constrained delegation
- Searches for changes to Protected objects
- ALL Protection templates discussed in next section

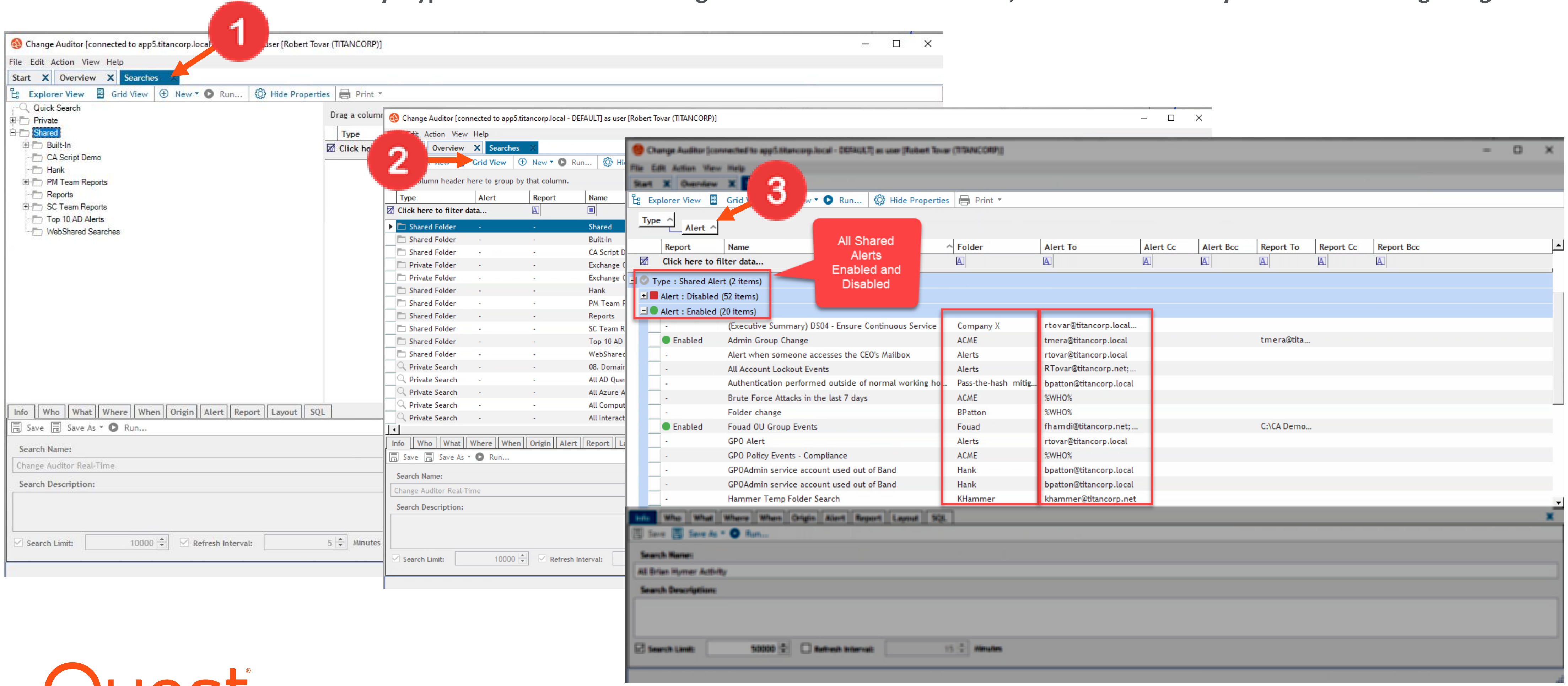
Quest®
Where Next Meets Now.

How to use the “Searches” Tab

Quest™

Searches: Grid View – Find those hidden alerts

- The best practice is to keep alerts organized but in some cases they will be stored in multiple containers. Finding them all can be difficult.
  - Sort by ‘Type’ then ‘Alert’ while using the ‘Grid View’ to find alerts, what container they live in and who’s getting the alerts.



1
2
3
Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]
File Edit Action View Help
Start Overview Searches
Explorer View Grid View New Run... Hide Properties Print
Quick Search
Private
Shared
Built-In
CA Script Demo
Hank
PM Team Reports
Reports
SC Team Reports
Top 10 AD Alerts
WebShared Searches
Info Who What Where When Origin Alert Report Layout SQL
Save Save As Run...
Search Name:
Change Auditor Real-Time
Search Description:
Search Limit: 10000
Refresh Interval: 5 Minutes
Drag a column header here to group by that column.
All Shared Alerts Enabled and Disabled

Type	Alert	Report	Name
Shared Folder	-	-	Shared
Shared Folder	-	-	Built-In
Shared Folder	-	-	CA Script D
Private Folder	-	-	Exchange C
Private Folder	-	-	Exchange C
Shared Folder	-	-	Hank
Shared Folder	-	-	PM Team R
Shared Folder	-	-	Reports
Shared Folder	-	-	SC Team R
Shared Folder	-	-	Top 10 AD
Shared Folder	-	-	WebShared
Private Search	-	-	08. Domain
Private Search	-	-	All AD Quer
Private Search	-	-	All Azure A
Private Search	-	-	All Comput
Private Search	-	-	All Interact

Type : Shared Alert (2 items)

🟥 Alert : Disabled (52 items)

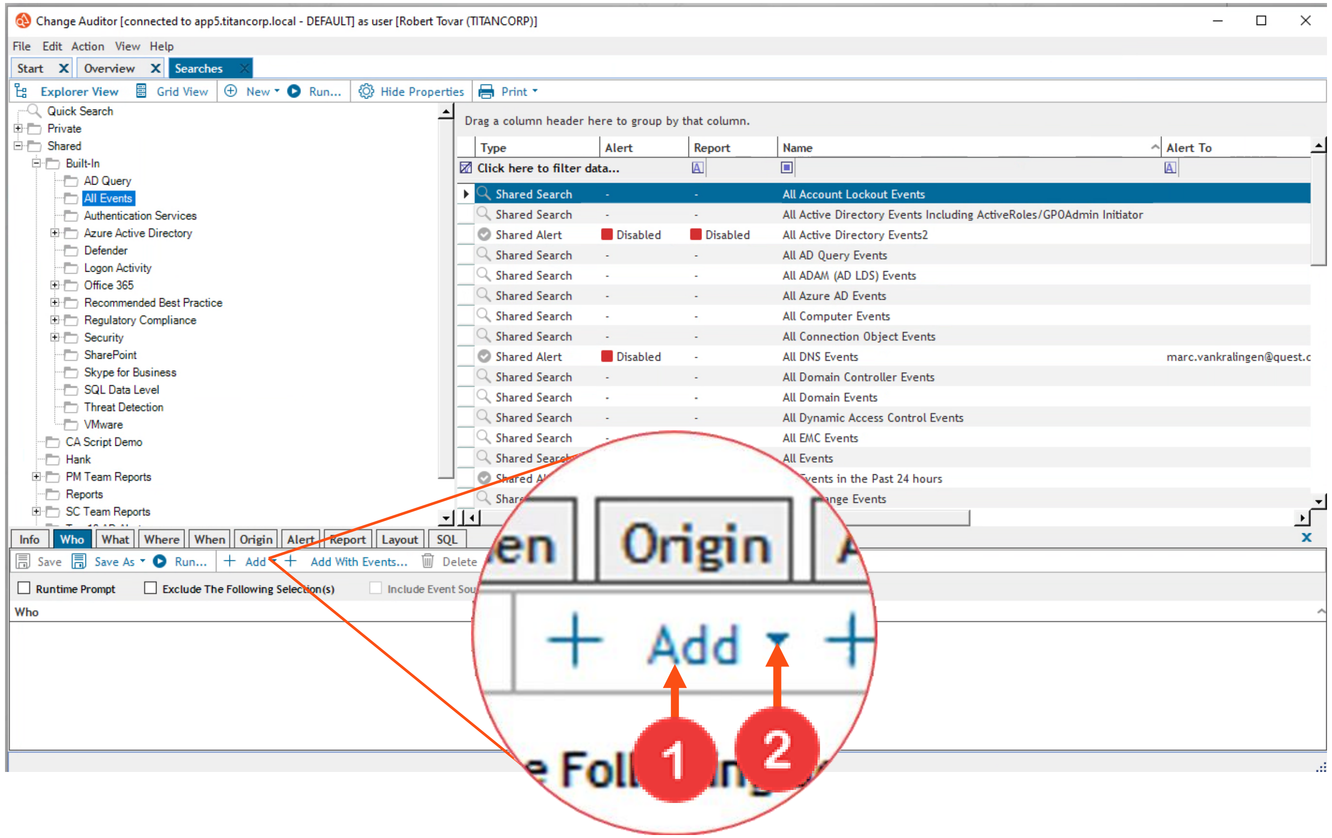
● Alert : Enabled (20 items)

Report	Name	Folder	Alert To	Alert Cc	Alert Bcc	Report To	Report Cc	Report Bcc
-	(Executive Summary) DS04 - Ensure Continuous Service	Company X	rtovar@titancorp.local...					
● Enabled	Admin Group Change	ACME	tmera@titancorp.local			tmera@tita...		
-	Alert when someone accesses the CEO's Mailbox	Alerts	rtovar@titancorp.local					
-	All Account Lockout Events	Alerts	RTovar@titancorp.net;...					
-	Authentication performed outside of normal working ho...	Pass-the-hash mitig...	bpatton@titancorp.local					
-	Brute Force Attacks in the last 7 days	ACME	%WHO%					
-	Folder change	BPatton	%WHO%					
● Enabled	Fouad OU Group Events	Fouad	fhamdi@titancorp.net;...			C:\CA Demo...		
-	GPO Alert	Alerts	rtovar@titancorp.local					
-	GPO Policy Events - Compliance	ACME	%WHO%					
-	GPOAdmin service account used out of Band	Hank	bpatton@titancorp.local					
-	GPOAdmin service account used out of Band	Hank	bpatton@titancorp.local					
-	Hammer Temp Folder Search	KHammer	khammer@titancorp.net					

Where Next Meets Now.

Searches: Who Tab – There are 2 parts to the ‘Add’ button

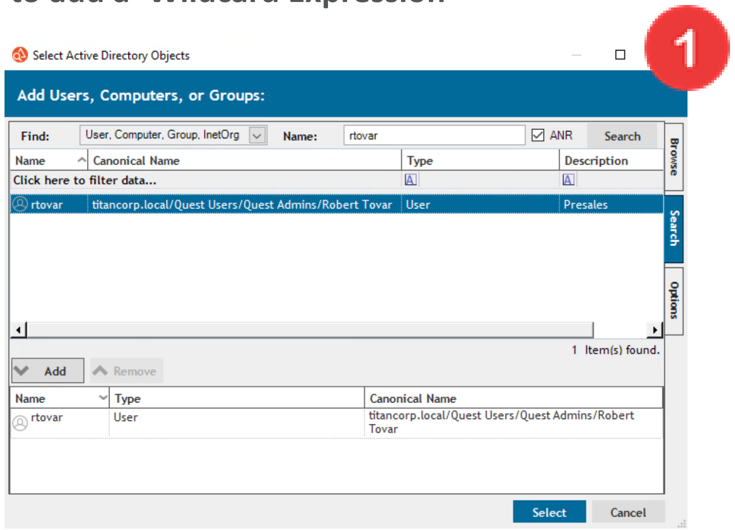
- ‘Add’ vs the tiny arrow button next to the ‘Add’ button, what’s the difference?
    1. ‘Add’ allows you to ‘Browse’ or ‘Search’ for the user, users or group/s.
    2. The arrow button next to the word ‘Add’ is a separate button that allows to add a ‘Wildcard Expression’



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]
File Edit Action View Help
Start Overview Searches
Explorer View Grid View New Run... Hide Properties Print
Quick Search
Private
Shared
Built-In
AD Query
All Events
Authentication Services
Azure Active Directory
Defender
Logon Activity
Office 365
Recommended Best Practice
Regulatory Compliance
Security
SharePoint
Skype for Business
SQL Data Level
Threat Detection
VMware
CA Script Demo
Hank
PM Team Reports
Reports
SC Team Reports
Info Who What Where When Origin Alert Report Layout SQL
Save Save As Run... Add Add With Events... Delete
☐ Runtime Prompt ☐ Exclude The Following Selection(s) ☐ Include Event Sou
Who
en Origin A
Add
e Foll n
1
2

Drag a column header here to group by that column.

Type	Alert	Report	Name	Alert To
Click here to filter data...				
Shared Search	-	-	All Account Lockout Events	
Shared Search	-	-	All Active Directory Events Including ActiveRoles/GPOAdmin Initiator	
Shared Alert	Disabled	Disabled	All Active Directory Events2	
Shared Search	-	-	All AD Query Events	
Shared Search	-	-	All ADAM (AD LDS) Events	
Shared Search	-	-	All Azure AD Events	
Shared Search	-	-	All Computer Events	
Shared Search	-	-	All Connection Object Events	
Shared Alert	Disabled	-	All DNS Events	marc.vankralingen@quest.c
Shared Search	-	-	All Domain Controller Events	
Shared Search	-	-	All Domain Events	
Shared Search	-	-	All Dynamic Access Control Events	
Shared Search	-	-	All EMC Events	
Shared Searc			All Events	
Shared A			vents in the Past 24 hours	
Shar			nge Events	



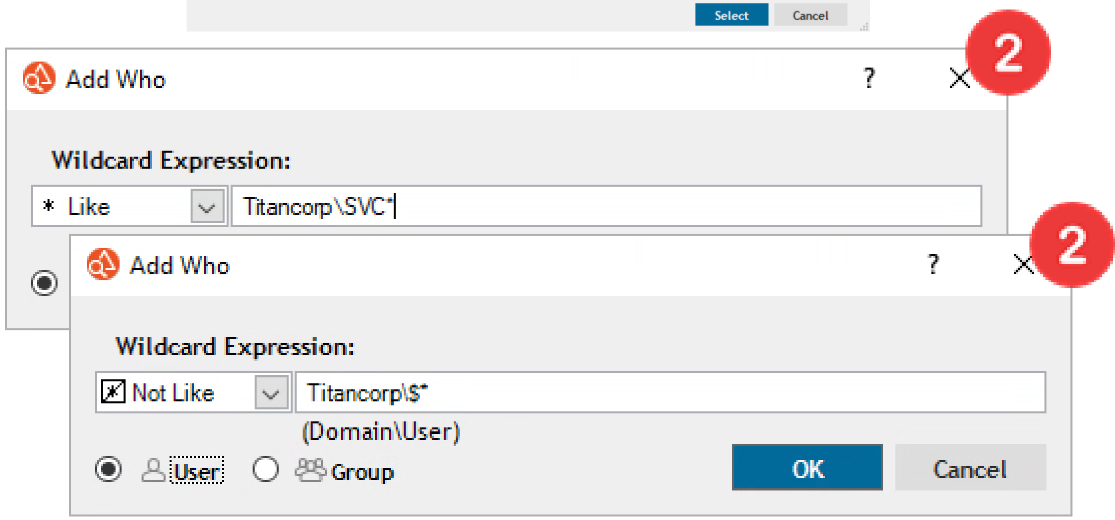
1
Select Active Directory Objects
Add Users, Computers, or Groups:
Browse
Search
Options
Add
Remove
Select
Cancel

Find: User, Computer, Group, InetOrg Name: rtovar ☑ ANR Search

Name	Canonical Name	Type	Description
Click here to filter data...			
rtovar	titancorp.local/Quest Users/Quest Admins/Robert Tovar	User	Presales

1 Item(s) found.

Name	Type	Canonical Name
rtovar	User	titancorp.local/Quest Users/Quest Admins/Robert Tovar



Wildcard Expression:

* Like Titancorp\SVC*

Wildcard Expression:

Not Like Titancorp\$*

(Domain\User)

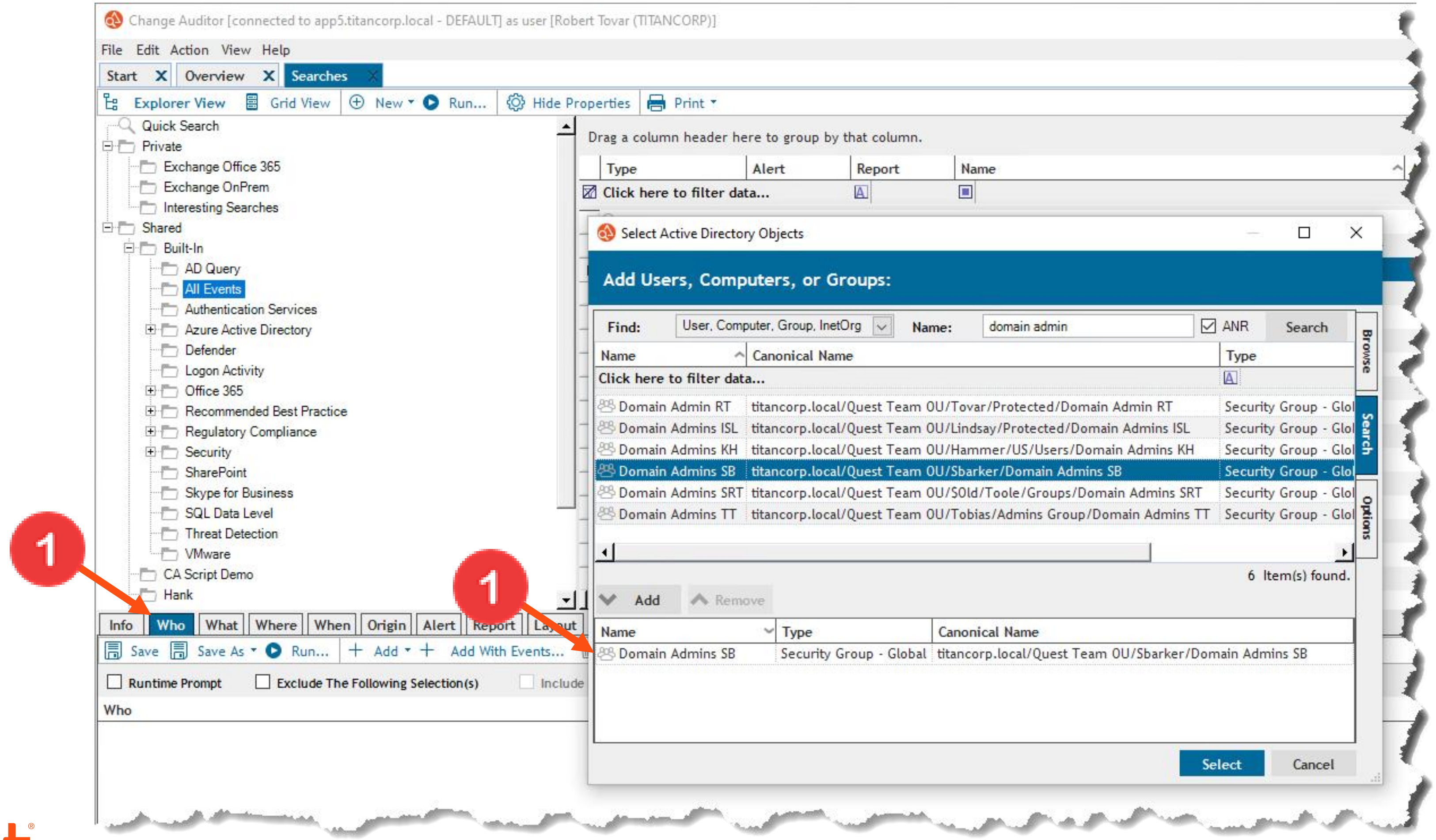
● User ○ Group

Quest

quest.com | confidential

Searches: Who Tab – Add group/s to the who tab

- You can add groups to the 'Who' tab to add all members of a group
  1. Add group or groups to the who tab



Find: User, Computer, Group, InetOrg   Name: domain admin   ☑ ANR   Search

Name	Canonical Name	Type
Domain Admin RT	titancorp.local/Quest Team OU/Tovar/Protected/Domain Admin RT	Security Group - Glol
Domain Admins ISL	titancorp.local/Quest Team OU/Lindsay/Protected/Domain Admins ISL	Security Group - Glol
Domain Admins KH	titancorp.local/Quest Team OU/Hammer/US/Users/Domain Admins KH	Security Group - Glol
Domain Admins SB	titancorp.local/Quest Team OU/Sbarker/Domain Admins SB	Security Group - Glol
Domain Admins SRT	titancorp.local/Quest Team OU/SOld/Toole/Groups/Domain Admins SRT	Security Group - Glol
Domain Admins TT	titancorp.local/Quest Team OU/Tobias/Admins Group/Domain Admins TT	Security Group - Glol

6 Item(s) found.

Add   Remove

Name	Type	Canonical Name
Domain Admins SB	Security Group - Global	titancorp.local/Quest Team OU/Sbarker/Domain Admins SB

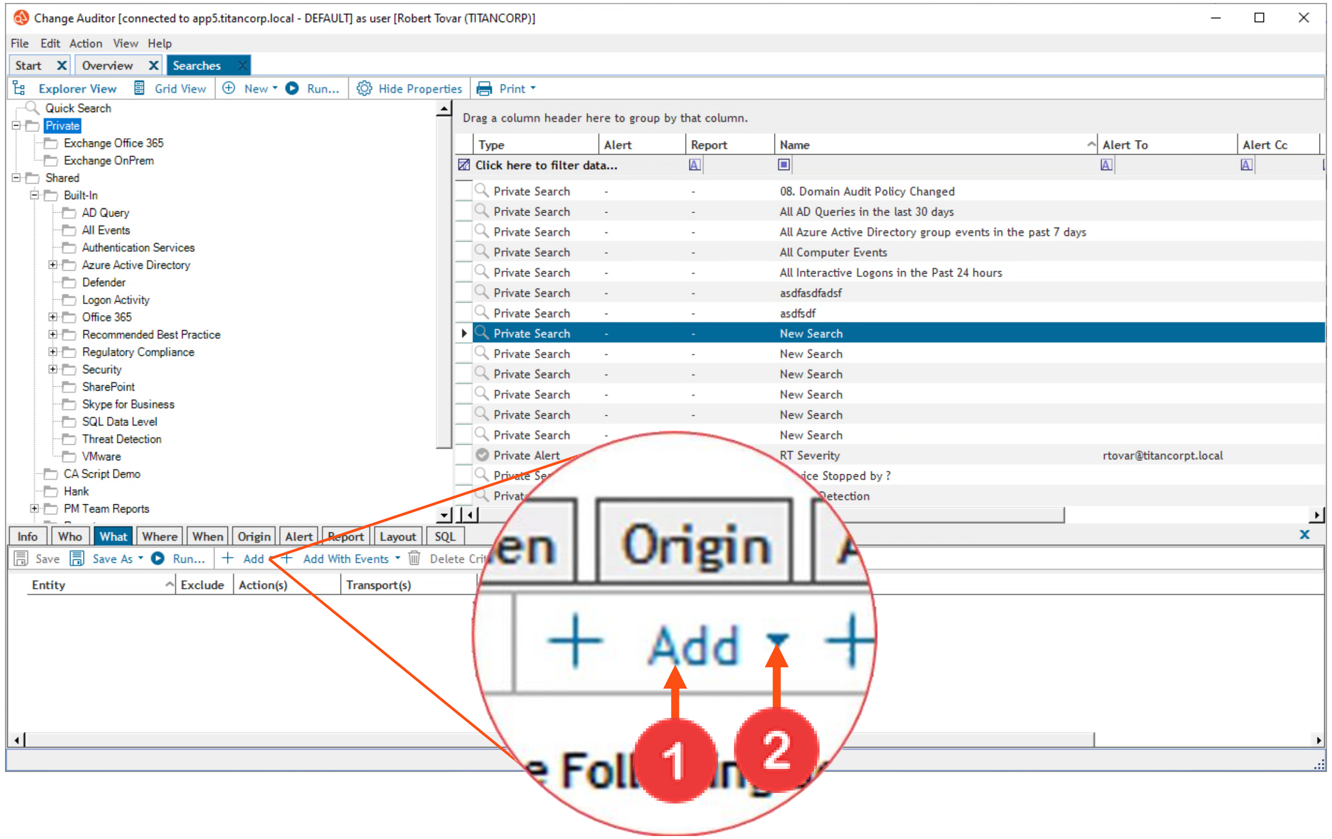
Select   Cancel

Quest

Where Next Meets Now.

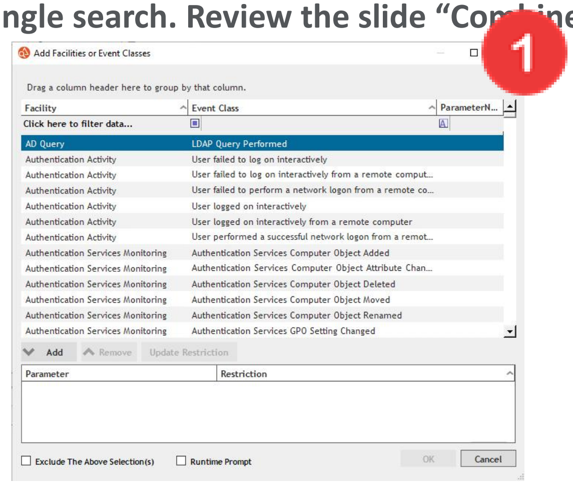
Searches: What Tab – There are 2 parts to the ‘Add’ button

- ‘Add’ vs the tiny arrow button next to the ‘Add’ button, what’s the difference?
  1. ‘Add’ allows you to select from all of the possible events Change Auditor can produce. The search will focus on the activity.
  2. The arrow button next to the word ‘Add’ is a separate button that allows to select the objects/activity you want the search to focus on.
  3. You can search based on the object and the event within a single search. Review the slide “Combine the specific activity and object”



Drag a column header here to group by that column.

Type	Alert	Report	Name	Alert To	Alert Cc
Click here to filter data...					
Private Search	-	-	08. Domain Audit Policy Changed		
Private Search	-	-	All AD Queries in the last 30 days		
Private Search	-	-	All Azure Active Directory group events in the past 7 days		
Private Search	-	-	All Computer Events		
Private Search	-	-	All Interactive Logons in the Past 24 hours		
Private Search	-	-	asdfasdfadsf		
Private Search	-	-	asdfsdf		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Alert			RT Severity	rtovar@titancorpt.local	
Private Se			ice Stopped by ?		
Privat			Detection		

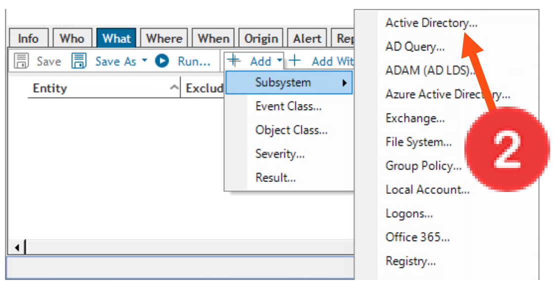


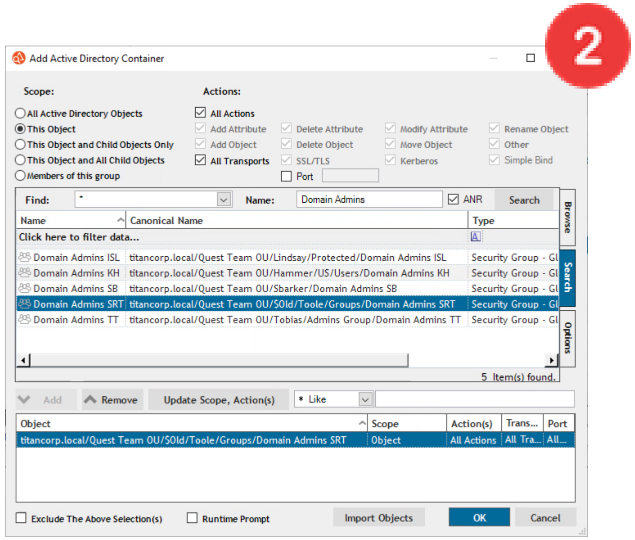
Drag a column header here to group by that column.

Facility	Event Class	ParameterN...
Click here to filter data...		
AD Query	LDAP Query Performed	
Authentication Activity	User failed to log on interactively	
Authentication Activity	User failed to log on interactively from a remote comput...	
Authentication Activity	User failed to perform a network logon from a remote co...	
Authentication Activity	User logged on interactively	
Authentication Activity	User logged on interactively from a remote computer	
Authentication Activity	User performed a successful network logon from a remot...	
Authentication Services Monitoring	Authentication Services Computer Object Added	
Authentication Services Monitoring	Authentication Services Computer Object Attribute Chan...	
Authentication Services Monitoring	Authentication Services Computer Object Deleted	
Authentication Services Monitoring	Authentication Services Computer Object Moved	
Authentication Services Monitoring	Authentication Services Computer Object Renamed	
Authentication Services Monitoring	Authentication Services GPO Setting Changed	

Parameter	Restriction

☐ Exclude The Above Selection(s) ☐ Runtime Prompt





Scope:
○ All Active Directory Objects
● This Object
○ This Object and Child Objects Only
○ This Object and All Child Objects
○ Members of this group

Actions:
☑ All Actions
☑ Add Attribute ☑ Delete Attribute ☑ Modify Attribute ☑ Rename Object
☑ Add Object ☑ Delete Object ☑ Move Object ☑ Other
☑ All Transports ☑ SSL/TLS ☑ Kerberos ☑ Simple Bind
☐ Port

Find: * Name: Domain Admins ☑ ANR

Name	Canonical Name	Type
Click here to filter data...		
Domain Admins ISL	titancorp.local/Quest Team OU/Lindsay/Protected/Domain Admins ISL	Security Group - Gl
Domain Admins KH	titancorp.local/Quest Team OU/Hammer/US/Users/Domain Admins KH	Security Group - Gl
Domain Admins SB	titancorp.local/Quest Team OU/Sbarker/Domain Admins SB	Security Group - Gl
Domain Admins SRT	titancorp.local/Quest Team OU/$Old/Toole/Groups/Domain Admins SRT	Security Group - Gl
Domain Admins TT	titancorp.local/Quest Team OU/Tobias/Admins Group/Domain Admins TT	Security Group - Gl

5 Item(s) found.

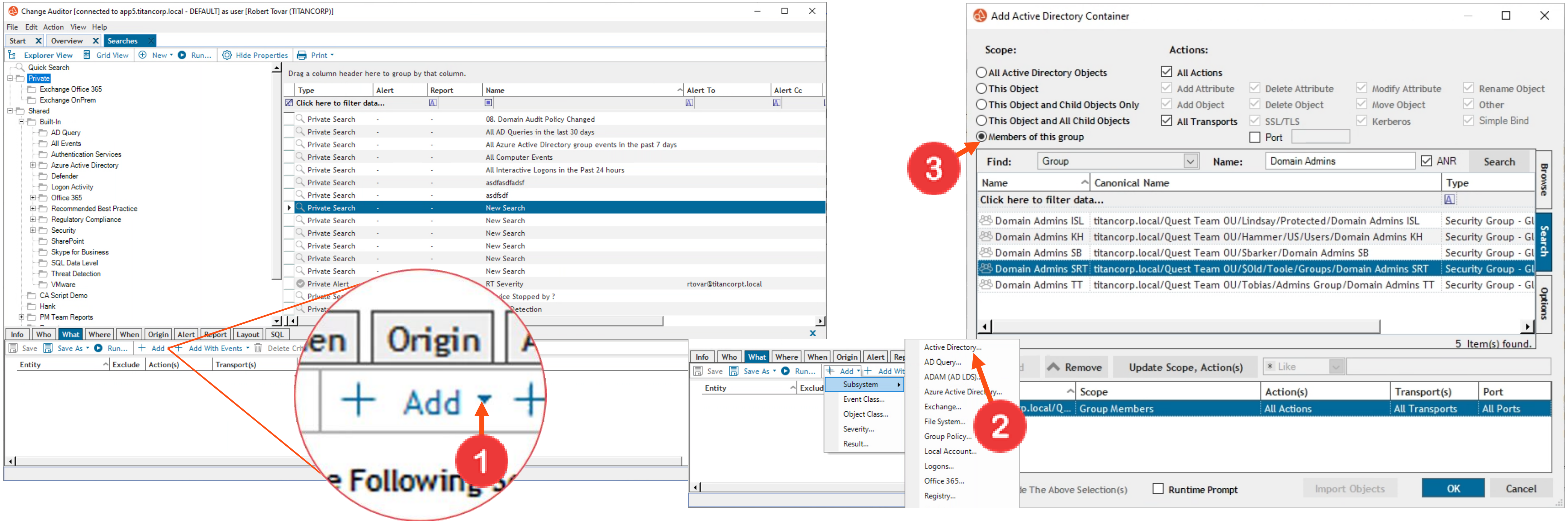
* Like

Object	Scope	Action(s)	Trans...	Port
titancorp.local/Quest Team OU/$Old/Toole/Groups/Domain Admins SRT	Object	All Actions	All Tra...	All...

☐ Exclude The Above Selection(s) ☐ Runtime Prompt

Searches: What Tab – Activity performed against all members of this group

1. The arrow button next to the word ‘Add’ is a separate button that allows to select the objects/activity you want the search to focus on.
2. You can search based on the members of a group.
3. Members of this group - select this option to show changes made to users in a specified group.
   1. Nested groups are not supported.



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]

Drag a column header here to group by that column.

Type	Alert	Report	Name	Alert To	Alert Cc
Private Search	-	-	08. Domain Audit Policy Changed		
Private Search	-	-	All AD Queries in the last 30 days		
Private Search	-	-	All Azure Active Directory group events in the past 7 days		
Private Search	-	-	All Computer Events		
Private Search	-	-	All Interactive Logons in the Past 24 hours		
Private Search	-	-	asdfasdfadsf		
Private Search	-	-	asdfsdf		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Alert			RT Severity	rtovar@titancorpt.local	

Add Active Directory Container

Scope:
- ○ All Active Directory Objects
- ○ This Object
- ○ This Object and Child Objects Only
- ○ This Object and All Child Objects
- ● Members of this group

Actions:
- ☑ All Actions
- ☑ Add Attribute ☑ Delete Attribute ☑ Modify Attribute ☑ Rename Object
- ☑ Add Object ☑ Delete Object ☑ Move Object ☑ Other
- ☑ All Transports ☑ SSL/TLS ☑ Kerberos ☑ Simple Bind
- □ Port

Find: Group Name: Domain Admins ☑ ANR Search

Name	Canonical Name	Type
Domain Admins ISL	titancorp.local/Quest Team OU/Lindsay/Protected/Domain Admins ISL	Security Group - Gl
Domain Admins KH	titancorp.local/Quest Team OU/Hammer/US/Users/Domain Admins KH	Security Group - Gl
Domain Admins SB	titancorp.local/Quest Team OU/Sbarker/Domain Admins SB	Security Group - Gl
Domain Admins SRT	titancorp.local/Quest Team OU/SOld/Toole/Groups/Domain Admins SRT	Security Group - Gl
Domain Admins TT	titancorp.local/Quest Team OU/Tobias/Admins Group/Domain Admins TT	Security Group - Gl

5 Item(s) found.

	Scope	Action(s)	Transport(s)	Port
p.local/Q...	Group Members	All Actions	All Transports	All Ports

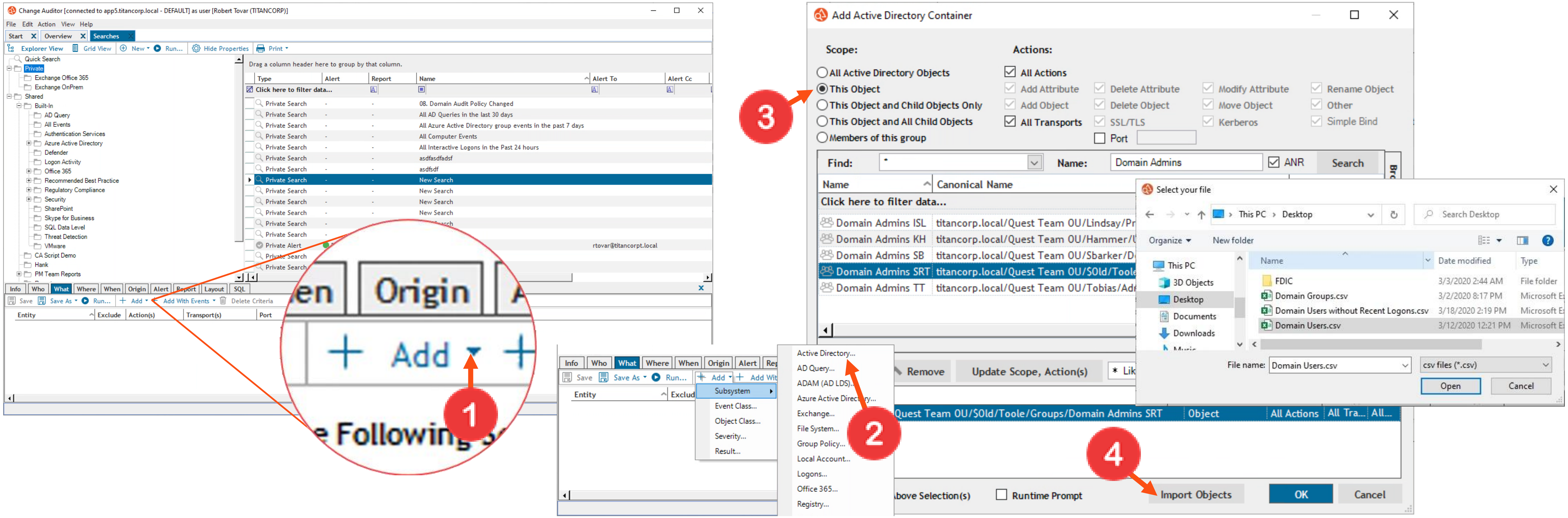
□ Runtime Prompt

Quest

Where Next Meets Now.

Searches: What Tab – Bulk import objects from CSV file

1. The arrow button next to the word ‘Add’ is a separate button that allows to select the objects/activity you want the search to focus on.
2. You can search based on a list of AD objects.
3. Click on the ‘This Object’ option
4. Click on ‘Import Objects’



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]

Type	Alert	Report	Name	Alert To	Alert Cc
Private Search	-	-	08. Domain Audit Policy Changed		
Private Search	-	-	All AD Queries in the last 30 days		
Private Search	-	-	All Azure Active Directory group events in the past 7 days		
Private Search	-	-	All Computer Events		
Private Search	-	-	All Interactive Logons in the Past 24 hours		
Private Search	-	-	asdfasdfadsf		
Private Search	-	-	asdfsdf		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Search	-	-	New Search		
Private Alert				rtovar@titancorpt.local	

Add Active Directory Container

Scope:
○ All Active Directory Objects
● This Object
○ This Object and Child Objects Only
○ This Object and All Child Objects
○ Members of this group

Actions:
☑ All Actions
☑ Add Attribute ☑ Delete Attribute ☑ Modify Attribute ☑ Rename Object
☑ Add Object ☑ Delete Object ☑ Move Object ☑ Other
☑ All Transports ☑ SSL/TLS ☑ Kerberos ☑ Simple Bind
□ Port

Find: * Name: Domain Admins ☑ ANR

Name	Canonical Name
Domain Admins ISL	titancorp.local/Quest Team OU/Lindsay/Pr
Domain Admins KH	titancorp.local/Quest Team OU/Hammer/U
Domain Admins SB	titancorp.local/Quest Team OU/Sbarker/D
Domain Admins SRT	titancorp.local/Quest Team OU/SOld/Toole
Domain Admins TT	titancorp.local/Quest Team OU/Tobias/Ad

Quest Team OU/SOld/Toole/Groups/Domain Admins SRT | Object | All Actions | All Tra… | All…

Select your file

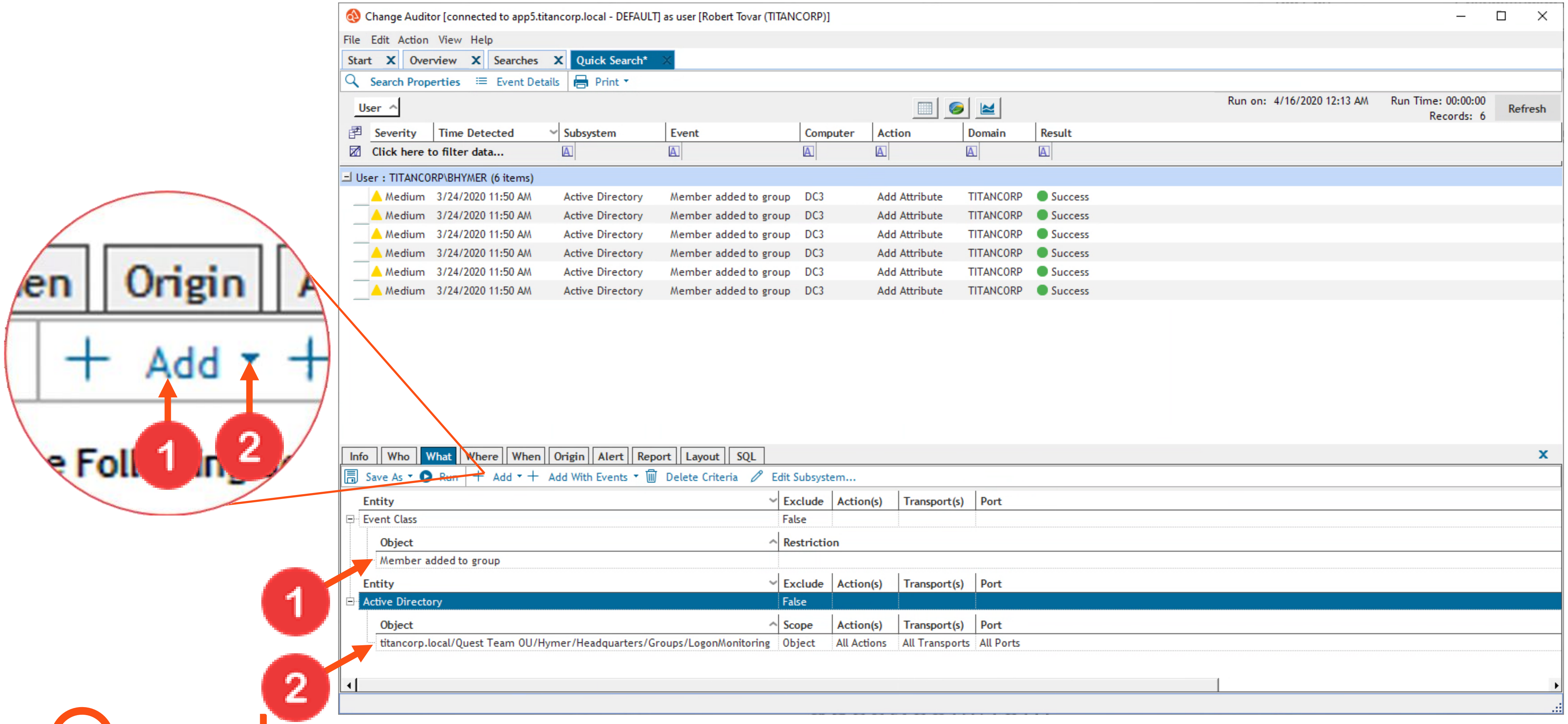
This PC › Desktop

Name	Date modified	Type
FDIC	3/3/2020 2:44 AM	File folder
Domain Groups.csv	3/2/2020 8:17 PM	Microsoft E
Domain Users without Recent Logons.csv	3/18/2020 2:19 PM	Microsoft E
Domain Users.csv	3/12/2020 12:21 PM	Microsoft E

File name: Domain Users.csv csv files (*.csv)

Searches: What Tab – Combine the specific activity and object

1. ‘Add’ allows you to select from all of the possible events Change Auditor can produce. The search will focus on the activity.
2. The arrow button next to the word ‘Add’ is a separate button that allows to select the objects you want the search to focus on.
3. You can combine the activity and the object of interest within the ‘What’ tab to get filtered results.


Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]
File Edit Action View Help
Start Overview Searches Quick Search*
Search Properties Event Details Print
User
Refresh
Click here to filter data...
Info Who What Where When Origin Alert Report Layout SQL
Save As Run Add Add With Events Delete Criteria Edit Subsystem...
en Origin
Add
Foll
1
2

Run on: 4/16/2020 12:13 AM Run Time: 00:00:00 Records: 6

User : TITANCORP\BHYMER (6 items)

Severity	Time Detected	Subsystem	Event	Computer	Action	Domain	Result
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	Success

Entity	Exclude	Action(s)	Transport(s)	Port
Event Class	False			

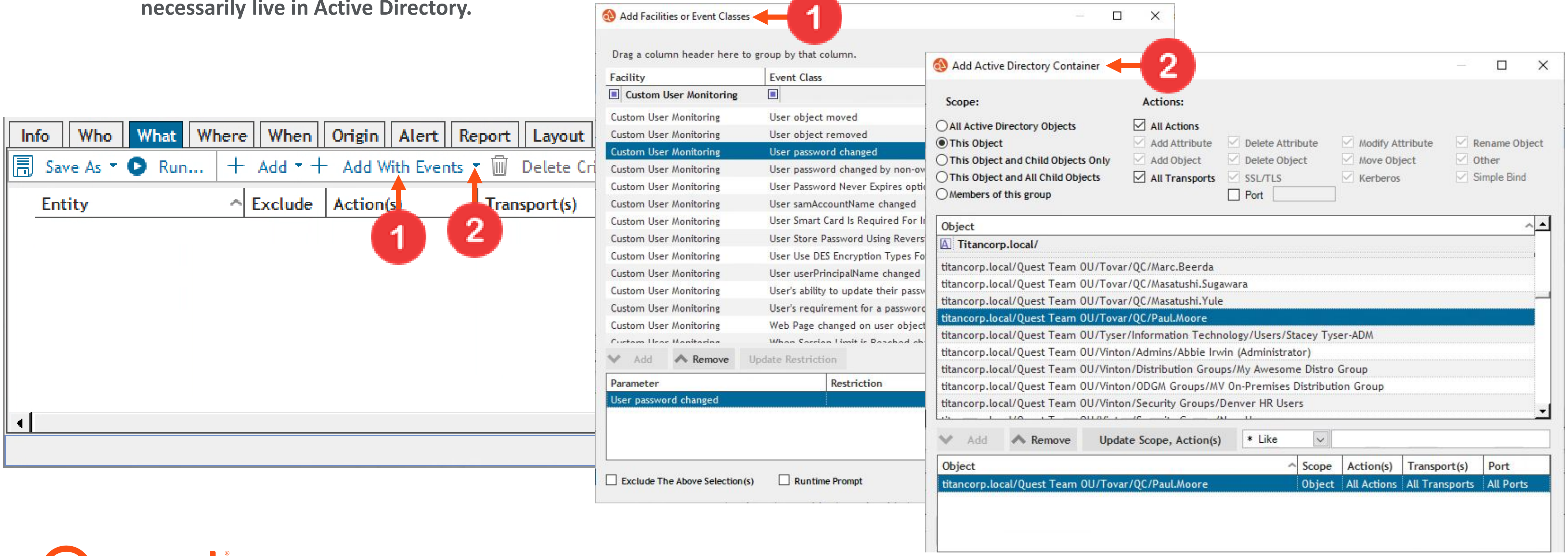
Object	Restriction
Member added to group	

Entity	Exclude	Action(s)	Transport(s)	Port
Active Directory	False			

Object	Scope	Action(s)	Transport(s)	Port
titancorp.local/Quest Team OU/Hymer/Headquarters/Groups/LogonMonitoring	Object	All Actions	All Transports	All Ports

Searches: ’Add With Events’ within the Who / What tab. What does it do?

- The ‘Add With Events’ button allows you to add events and/or objects that live within the database but not necessarily in Active Directory
- If you need to search for an object that may have been deleted from Active Directory searching via the ‘Add’ button is not an option.
  1. The ‘Add With Events’ button will provide a list of events that have been generated in your environment and exist in the DB
  2. The arrow button next to the ‘Add With Events’ button allows you to focus a search from the list of objects that live within the DB but may not necessarily live in Active Directory.



Add Facilities or Event Classes

Drag a column header here to group by that column.

Facility	Event Class
Custom User Monitoring	
Custom User Monitoring	User object moved
Custom User Monitoring	User object removed
Custom User Monitoring	User password changed
Custom User Monitoring	User password changed by non-ow
Custom User Monitoring	User Password Never Expires optic
Custom User Monitoring	User samAccountName changed
Custom User Monitoring	User Smart Card Is Required For Ir
Custom User Monitoring	User Store Password Using Revers
Custom User Monitoring	User Use DES Encryption Types Fo
Custom User Monitoring	User userPrincipalName changed
Custom User Monitoring	User's ability to update their passw
Custom User Monitoring	User's requirement for a passworc
Custom User Monitoring	Web Page changed on user object

Parameter	Restriction
User password changed	

□ Exclude The Above Selection(s) □ Runtime Prompt

Add Active Directory Container

Scope:

○ All Active Directory Objects
● This Object
○ This Object and Child Objects Only
○ This Object and All Child Objects
○ Members of this group

Actions:

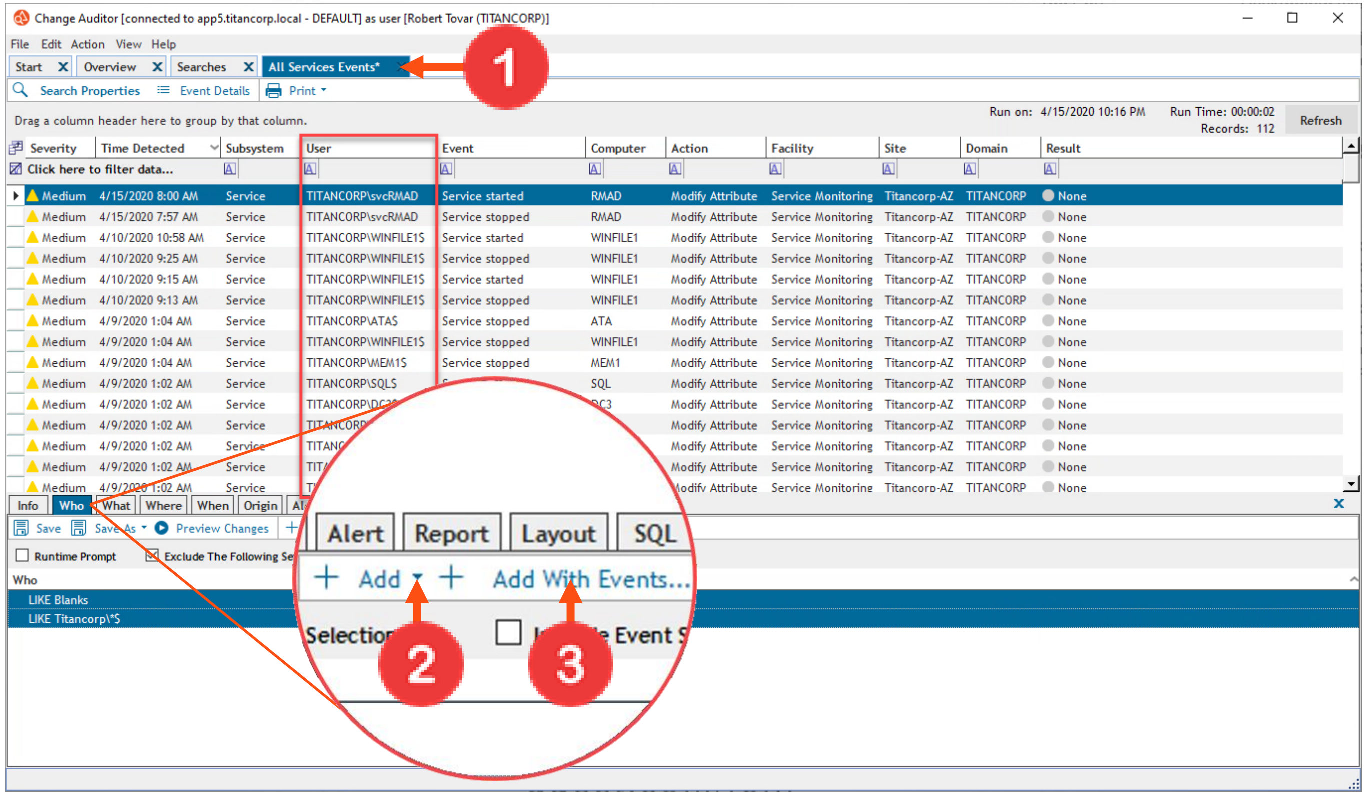
☑ All Actions
☑ Add Attribute ☑ Delete Attribute ☑ Modify Attribute ☑ Rename Object
☑ Add Object ☑ Delete Object ☑ Move Object ☑ Other
☑ All Transports ☑ SSL/TLS ☑ Kerberos ☑ Simple Bind
□ Port

Object
Titancorp.local/
titancorp.local/Quest Team OU/Tovar/QC/Marc.Beerda
titancorp.local/Quest Team OU/Tovar/QC/Masatushi.Sugawara
titancorp.local/Quest Team OU/Tovar/QC/Masatushi.Yule
titancorp.local/Quest Team OU/Tovar/QC/Paul.Moore
titancorp.local/Quest Team OU/Tyser/Information Technology/Users/Stacey Tyser-ADM
titancorp.local/Quest Team OU/Vinton/Admins/Abbie Irwin (Administrator)
titancorp.local/Quest Team OU/Vinton/Distribution Groups/My Awesome Distro Group
titancorp.local/Quest Team OU/Vinton/ODGM Groups/MV On-Premises Distribution Group
titancorp.local/Quest Team OU/Vinton/Security Groups/Denver HR Users

Object	Scope	Action(s)	Transport(s)	Port
titancorp.local/Quest Team OU/Tovar/QC/Paul.Moore	Object	All Actions	All Transports	All Ports

Searches: Wildcard Expressions – Filtering out the noise

- Certain activities are performed by user accounts and computer accounts – filtering out computer accounts can single out the users
  1. Run the ‘All Services Events’ search and you will see a lot of computer accounts in the ‘User’ column
  2. In the ‘Who’ tab exclude via a ‘Wildcard Expression’ to filter out computer accounts: **$
  3. In the ‘Who’ tab exclude ‘blank’ entries to further clear out non user events: ‘Add With Events’



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]

Drag a column header here to group by that column.

Run on: 4/15/2020 10:16 PM Run Time: 00:00:02 Records: 112

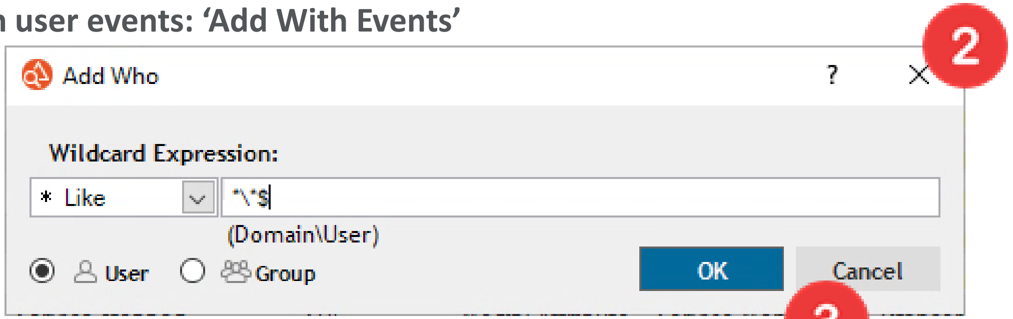
Click here to filter data...

Severity	Time Detected	Subsystem	User	Event	Computer	Action	Facility	Site	Domain	Result
Medium	4/15/2020 8:00 AM	Service	TITANCORP\svcRMAD	Service started	RMAD	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/15/2020 7:57 AM	Service	TITANCORP\svcRMAD	Service stopped	RMAD	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/10/2020 10:58 AM	Service	TITANCORP\WINFILE1$	Service started	WINFILE1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/10/2020 9:25 AM	Service	TITANCORP\WINFILE1$	Service stopped	WINFILE1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/10/2020 9:15 AM	Service	TITANCORP\WINFILE1$	Service started	WINFILE1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/10/2020 9:13 AM	Service	TITANCORP\WINFILE1$	Service stopped	WINFILE1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:04 AM	Service	TITANCORP\ATA$	Service stopped	ATA	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:04 AM	Service	TITANCORP\WINFILE1$	Service stopped	WINFILE1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:04 AM	Service	TITANCORP\MEM1$	Service stopped	MEM1	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	TITANCORP\SQL$		SQL	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	TITANCORP\DC3		DC3	Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	TITANCORP			Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	TITANC			Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	TIT			Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None
Medium	4/9/2020 1:02 AM	Service	T			Modify Attribute	Service Monitoring	Titancorp-AZ	TITANCORP	None

☐ Runtime Prompt ☑ Exclude The Following Se

Selection ☐ I e Event S

Who
LIKE Blanks
LIKE Titancorp*$



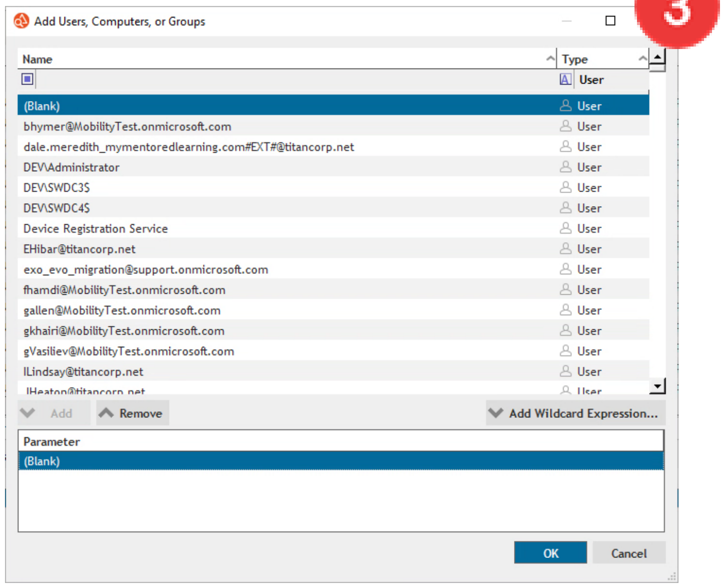
Add Who

Wildcard Expression:

* Like **$

(Domain\User)

● User ○ Group



Add Users, Computers, or Groups

Name	Type
	User
(Blank)	User
bhymer@MobilityTest.onmicrosoft.com	User
dale.meredith_mymentoredlearning.com#EXT#@titancorp.net	User
DEV\Administrator	User
DEV\SWDC3$	User
DEV\SWDC4$	User
Device Registration Service	User
EHibar@titancorp.net	User
exo_evo_migration@support.onmicrosoft.com	User
fhamdi@MobilityTest.onmicrosoft.com	User
gallen@MobilityTest.onmicrosoft.com	User
gkhairi@MobilityTest.onmicrosoft.com	User
gVasiliev@MobilityTest.onmicrosoft.com	User
lLindsay@titancorp.net	User
lHeaton@titancorp.net	User

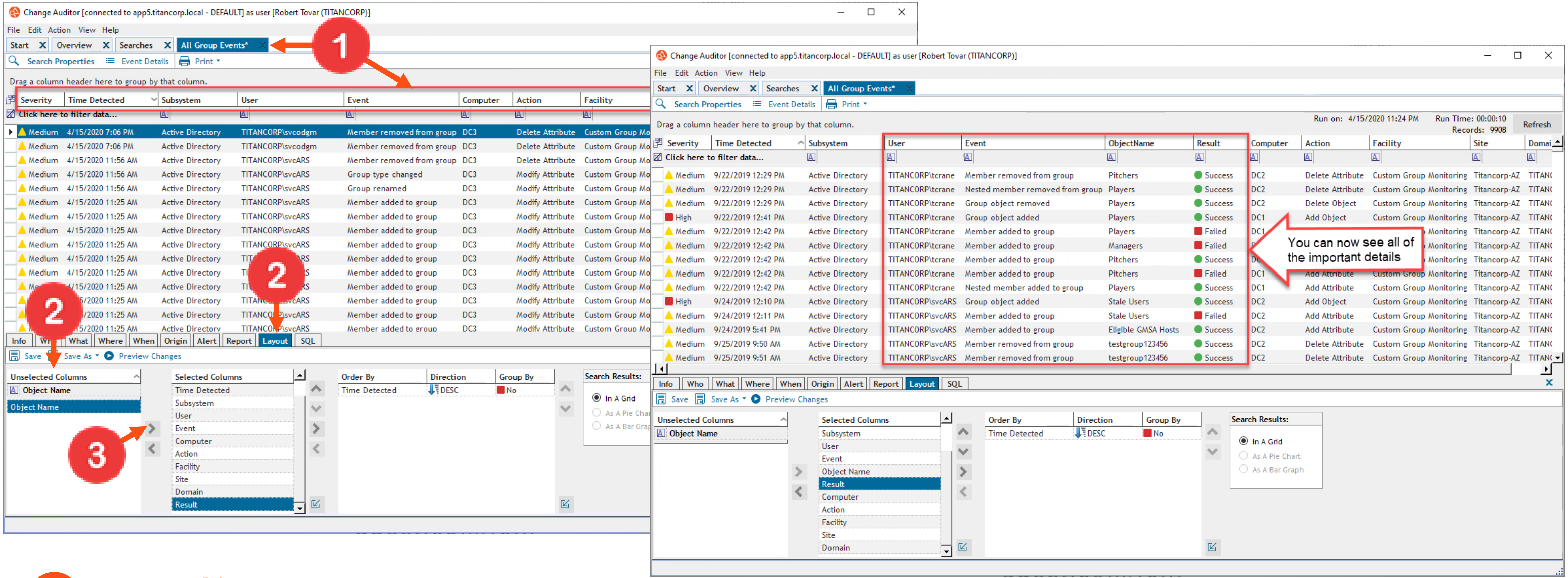
Parameter
(Blank)

Quest

Where Next Meets Now.

Searches: Layout Tab – Add/Remove columns to provide detailed data

- By default, some event details can only be seen by clicking on the event. Modify the search to include additional columns.
  1. In the 'All Group Events' search you can see the user that made the change and activity performed but you can't see the group modified.
  2. With the 'Layout' tab under the 'Unselected Columns' type in 'Object Name'
  3. Add the 'Object Name' column to the 'Selected Columns' and rerun the search.



Drag a column header here to group by that column.

Severity	Time Detected	Subsystem	User	Event	Computer	Action	Facility
Click here to filter data...							
Medium	4/15/2020 7:06 PM	Active Directory	TITANCORP\svcodgm	Member removed from group	DC3	Delete Attribute	Custom Group Mo
Medium	4/15/2020 7:06 PM	Active Directory	TITANCORP\svcodgm	Member removed from group	DC3	Delete Attribute	Custom Group Mo
Medium	4/15/2020 11:56 AM	Active Directory	TITANCORP\svcARS	Member removed from group	DC3	Delete Attribute	Custom Group Mo
Medium	4/15/2020 11:56 AM	Active Directory	TITANCORP\svcARS	Group type changed	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:56 AM	Active Directory	TITANCORP\svcARS	Group renamed	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	TITANCORP\svcARS	Member added to group	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	TITANCORP\svcARS	Member added to group	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	TITANCORP\svcARS	Member added to group	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	TITANCORP\svcARS	Member added to group	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo
Medium	4/15/2020 11:25 AM	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo
[illegible]	4/15/2020 11:25 AM	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo
[illegible]	[illegible]	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo
[illegible]	[illegible]	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo
[illegible]	[illegible]	Active Directory	[illegible]	Member added to group	DC3	Modify Attribute	Custom Group Mo

Unselected Columns
Object Name
Object Name

Selected Columns
Time Detected
Subsystem
User
Event
Computer
Action
Facility
Site
Domain
Result

Order By	Direction	Group By
Time Detected	DESC	No

Search Results:
● In A Grid
○ As A Pie Char
○ As A Bar Grap

Run on: 4/15/2020 11:24 PM Run Time: 00:00:10
Records: 9908

Drag a column header here to group by that column.

Severity	Time Detected	Subsystem	User	Event	ObjectName	Result	Computer	Action	Facility	Site	Domai
Click here to filter data...											
Medium	9/22/2019 12:29 PM	Active Directory	TITANCORP\tcrane	Member removed from group	Pitchers	Success	DC2	Delete Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:29 PM	Active Directory	TITANCORP\tcrane	Nested member removed from group	Players	Success	DC2	Delete Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:29 PM	Active Directory	TITANCORP\tcrane	Group object removed	Players	Success	DC2	Delete Object	Custom Group Monitoring	Titancorp-AZ	TITAN
High	9/22/2019 12:41 PM	Active Directory	TITANCORP\tcrane	Group object added	Players	Success	DC1	Add Object	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:42 PM	Active Directory	TITANCORP\tcrane	Member added to group	Players	Failed	DC1	[illegible]	[illegible] Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:42 PM	Active Directory	TITANCORP\tcrane	Member added to group	Managers	Failed	[illegible]	[illegible]	[illegible] Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:42 PM	Active Directory	TITANCORP\tcrane	Member added to group	Pitchers	Success	[illegible]	[illegible]	[illegible] Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:42 PM	Active Directory	TITANCORP\tcrane	Member added to group	Pitchers	Failed	DC1	Add Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/22/2019 12:42 PM	Active Directory	TITANCORP\tcrane	Nested member added to group	Players	Success	DC1	Add Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
High	9/24/2019 12:10 PM	Active Directory	TITANCORP\svcARS	Group object added	Stale Users	Success	DC2	Add Object	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/24/2019 12:11 PM	Active Directory	TITANCORP\svcARS	Member added to group	Stale Users	Failed	DC2	Add Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/24/2019 5:41 PM	Active Directory	TITANCORP\svcARS	Member added to group	Eligible GMSA Hosts	Success	DC2	Add Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/25/2019 9:50 AM	Active Directory	TITANCORP\svcARS	Member removed from group	testgroup123456	Success	DC2	Delete Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN
Medium	9/25/2019 9:51 AM	Active Directory	TITANCORP\svcARS	Member removed from group	testgroup123456	Success	DC2	Delete Attribute	Custom Group Monitoring	Titancorp-AZ	TITAN

You can now see all of the important details

Unselected Columns
Object Name

Selected Columns
Subsystem
User
Event
Object Name
Result
Computer
Action
Facility
Site
Domain

Order By	Direction	Group By
Time Detected	DESC	No

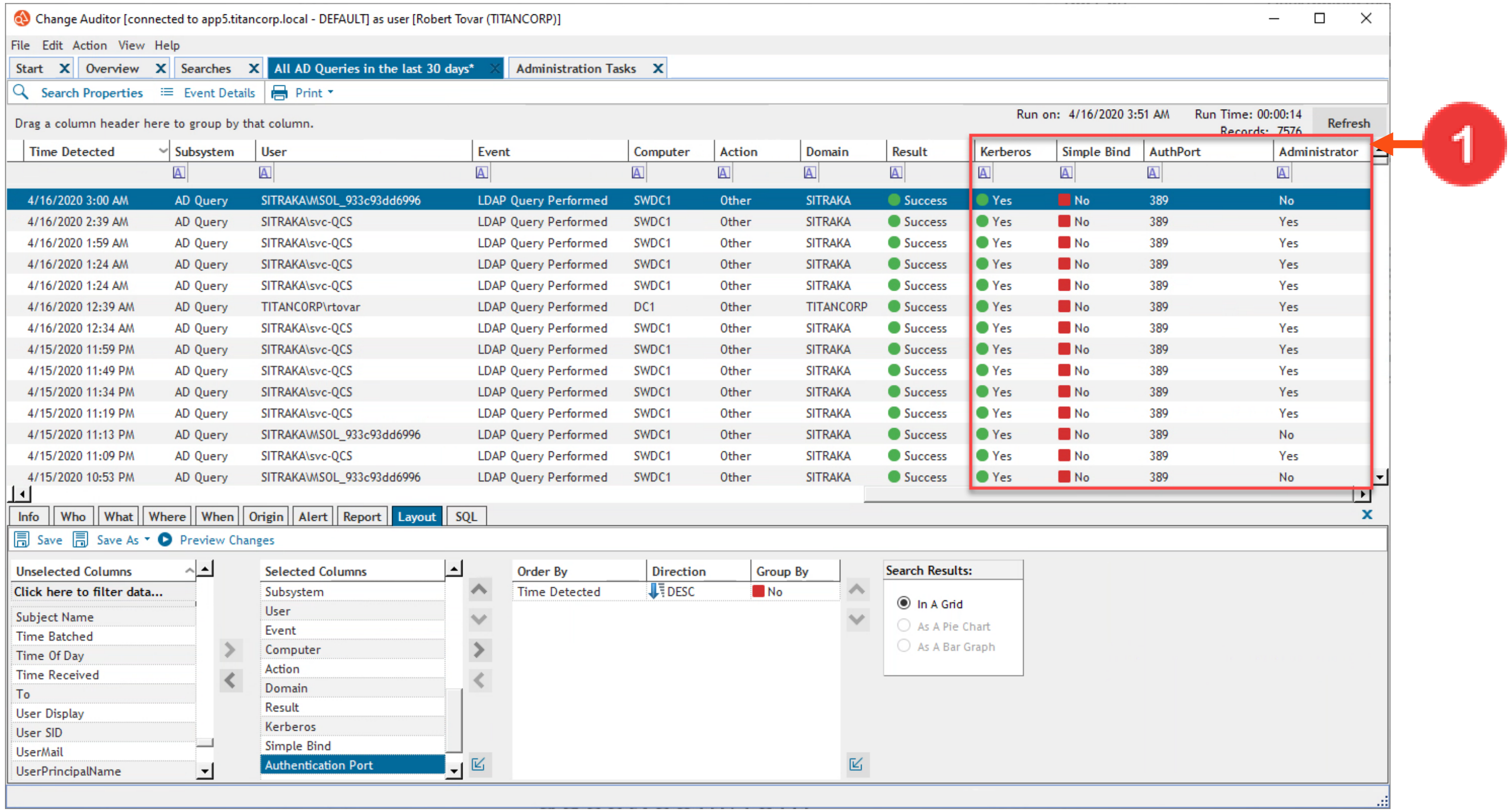
Search Results:
● In A Grid
○ As A Pie Chart
○ As A Bar Graph

quest.com | confidential

Where Next Meets Now.

Searches: AD Query – Display addition columns for AD Query report

- Add columns to the AD Query Search.
  1. Kerberos, Simple Bind, AuthPort, Administrator
  2. Many applications performing unsecure LDAP “simple binds” where credentials are transferred in clear text over the network.
  3. Those exposed credentials typically include the “service account” used to connect to LDAP, but also include the user credentials used during the application login.


Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]
File Edit Action View Help
Start
Overview
Searches
All AD Queries in the last 30 days*
Administration Tasks
Search Properties
Event Details
Print
Refresh
Info
Who
What
Where
When
Origin
Alert
Report
Layout
SQL
Save
Save As
Preview Changes
1

Drag a column header here to group by that column.

Run on: 4/16/2020 3:51 AM Run Time: 00:00:14 Records: 7576

Time Detected	Subsystem	User	Event	Computer	Action	Domain	Result	Kerberos	Simple Bind	AuthPort	Administrator
4/16/2020 3:00 AM	AD Query	SITRAKA\MSOL_933c93dd6996	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	No
4/16/2020 2:39 AM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/16/2020 1:59 AM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/16/2020 1:24 AM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/16/2020 1:24 AM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/16/2020 12:39 AM	AD Query	TITANCORP\rtovar	LDAP Query Performed	DC1	Other	TITANCORP	● Success	● Yes	🟥 No	389	Yes
4/16/2020 12:34 AM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 11:59 PM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 11:49 PM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 11:34 PM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 11:19 PM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 11:13 PM	AD Query	SITRAKA\MSOL_933c93dd6996	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	No
4/15/2020 11:09 PM	AD Query	SITRAKA\svc-QCS	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	Yes
4/15/2020 10:53 PM	AD Query	SITRAKA\MSOL_933c93dd6996	LDAP Query Performed	SWDC1	Other	SITRAKA	● Success	● Yes	🟥 No	389	No

Unselected Columns
Click here to filter data...
Subject Name
Time Batched
Time Of Day
Time Received
To
User Display
User SID
UserMail
UserPrincipalName

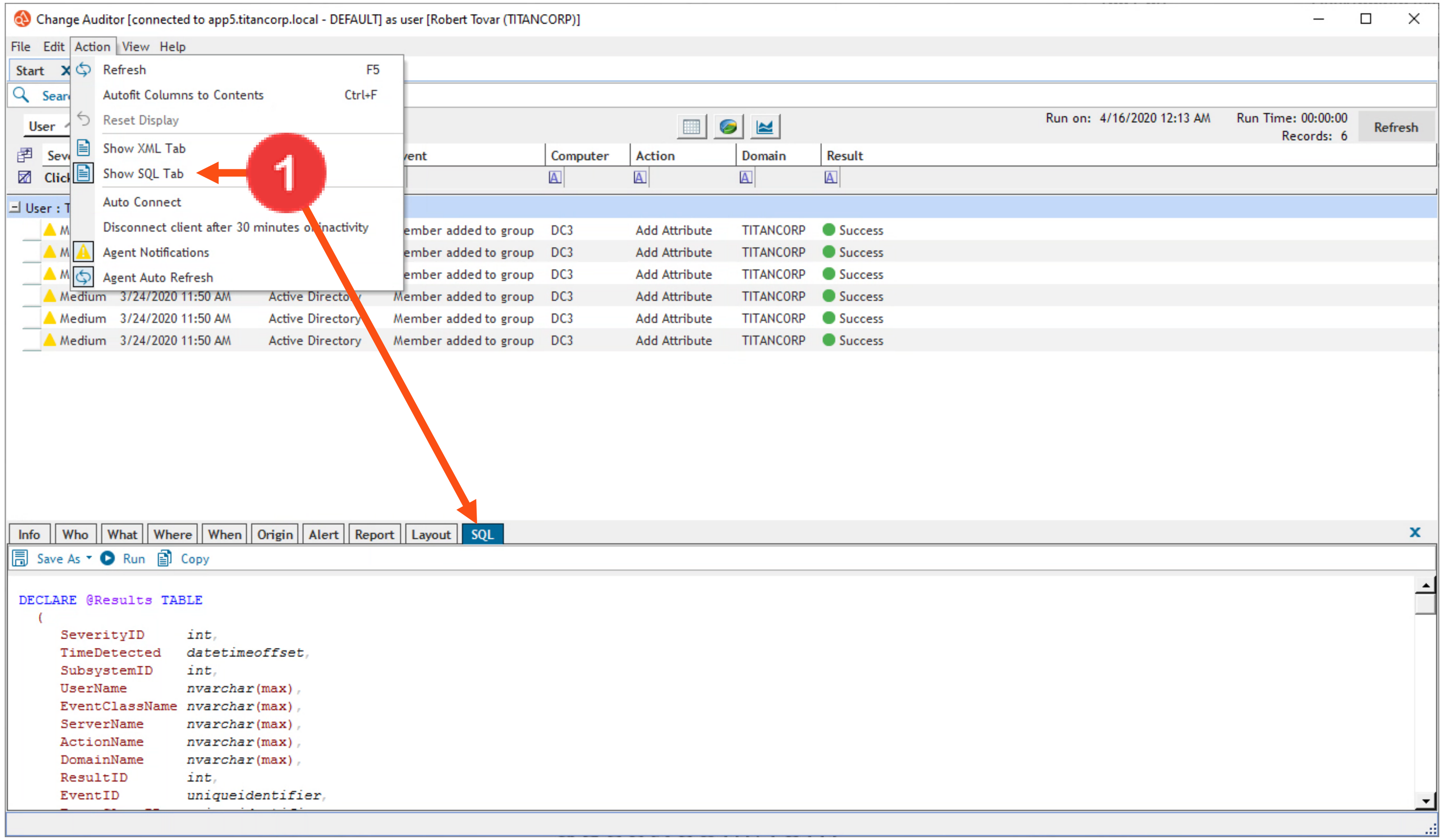
Selected Columns
Subsystem
User
Event
Computer
Action
Domain
Result
Kerberos
Simple Bind
Authentication Port

Order By	Direction	Group By
Time Detected	DESC	🟥 No

Search Results:
● In A Grid
○ As A Pie Chart
○ As A Bar Graph

Searches: SQL Tab – Display the SQL Query

- The SQL tab is not displayed by default.
    1. To display the SQL tab click on the ‘Action’ tab followed by ‘Show SQL Tab’



Run on: 4/16/2020 12:13 AM

Run Time: 00:00:00

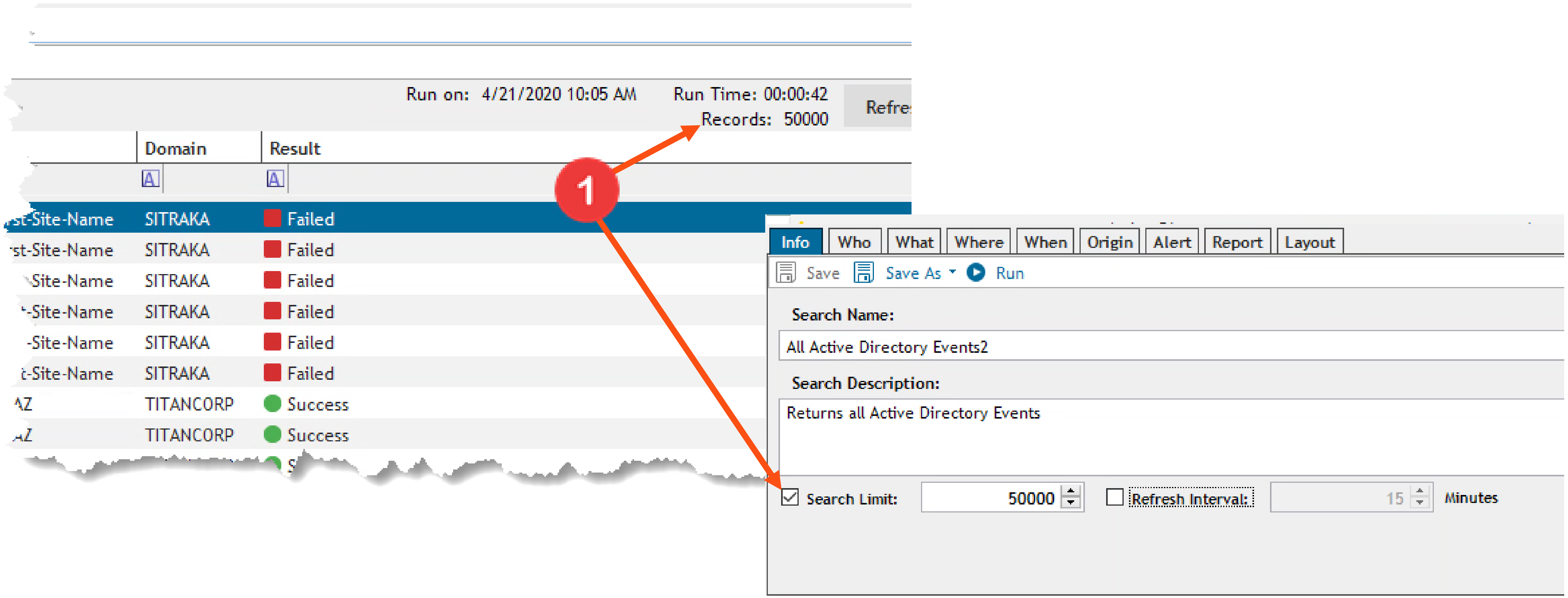
Records: 6

Sev			ent	Computer	Action	Domain	Result
M			ember added to group	DC3	Add Attribute	TITANCORP	● Success
M			ember added to group	DC3	Add Attribute	TITANCORP	● Success
M			ember added to group	DC3	Add Attribute	TITANCORP	● Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	● Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	● Success
Medium	3/24/2020 11:50 AM	Active Directory	Member added to group	DC3	Add Attribute	TITANCORP	● Success

```
DECLARE @Results TABLE
  (
     SeverityID     int,
     TimeDetected   datetimeoffset,
     SubsystemID    int,
     UserName       nvarchar(max),
     EventClassName nvarchar(max),
     ServerName     nvarchar(max),
     ActionName     nvarchar(max),
     DomainName     nvarchar(max),
     ResultID       int,
     EventID        uniqueidentifier,
```

Searches: Info Tab – Search limit

- Search Limit is set to 50,000 by default on all searches.
  1. When you search for events by date range you may reach the search limit.
     1. Adjust your date range or increase the search limit.



Run on: 4/21/2020 10:05 AM Run Time: 00:00:42
Records: 50000

	Domain	Result
st-Site-Name	SITRAKA	🟥 Failed
st-Site-Name	SITRAKA	🟥 Failed
Site-Name	SITRAKA	🟥 Failed
-Site-Name	SITRAKA	🟥 Failed
-Site-Name	SITRAKA	🟥 Failed
t-Site-Name	SITRAKA	🟥 Failed
AZ	TITANCORP	● Success
AZ	TITANCORP	● Success

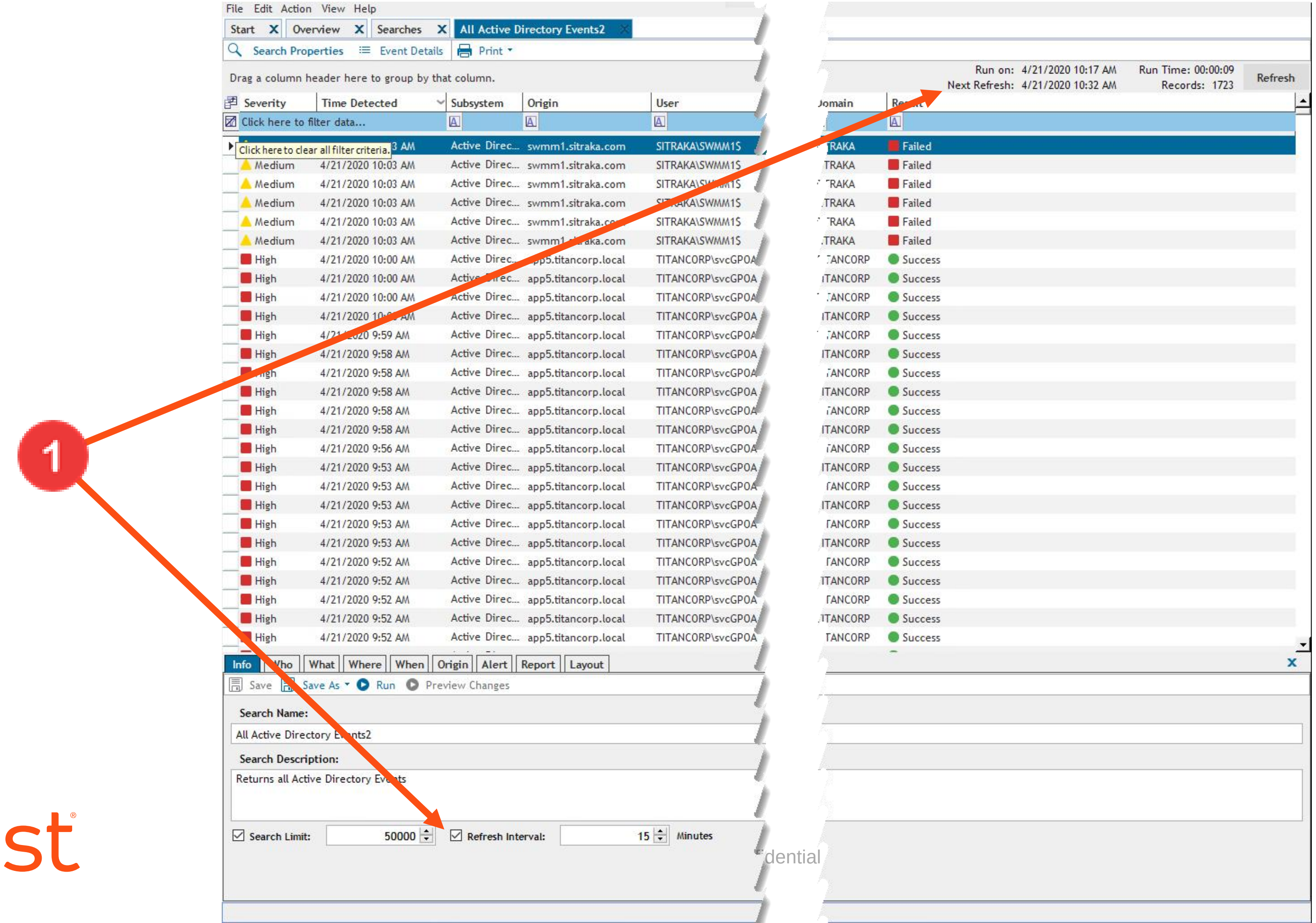
Search Name:
All Active Directory Events2

Search Description:
Returns all Active Directory Events

☑ Search Limit: 50000 □ Refresh Interval: 15 Minutes

Searches: Info Tab – Auto-Refresh Interval

1. Define an auto-refresh interval for any search.



Run on: 4/21/2020 10:17 AM Run Time: 00:00:09
Next Refresh: 4/21/2020 10:32 AM Records: 1723

Drag a column header here to group by that column.

Click here to filter data...

Click here to clear all filter criteria.

Severity	Time Detected	Subsystem	Origin	User	Domain	Result
	3 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	RAKA	🟥 Failed
▲ Medium	4/21/2020 10:03 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	TRAKA	🟥 Failed
▲ Medium	4/21/2020 10:03 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	TRAKA	🟥 Failed
▲ Medium	4/21/2020 10:03 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	TRAKA	🟥 Failed
▲ Medium	4/21/2020 10:03 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	TRAKA	🟥 Failed
▲ Medium	4/21/2020 10:03 AM	Active Direc...	swmm1.sitraka.com	SITRAKA\SWMM1$	TRAKA	🟥 Failed
🟥 High	4/21/2020 10:00 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 10:00 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 10:00 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 10:[illegible] AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:59 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:58 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:58 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:58 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:58 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:58 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:56 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:53 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:53 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:53 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:53 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:53 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:52 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:52 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:52 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:52 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success
🟥 High	4/21/2020 9:52 AM	Active Direc...	app5.titancorp.local	TITANCORP\svcGPOA	TANCORP	● Success

Search Name: All Active Directory Events2

Search Description: Returns all Active Directory Events

☑ Search Limit: 50000 ☑ Refresh Interval: 15 Minutes

Quest

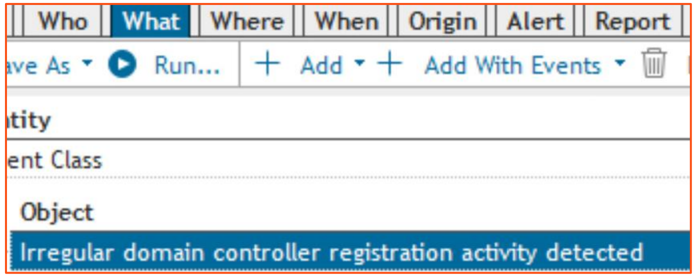
Where Next Meets Now.

Sample Attack Mitigation Searches

Irregular Domain Controller Registration Events (DCShadow)

This event shows replication changes occurring from a machine that is not a domain controller and hopefully will never generate an event. An alert should be configured for immediate notification if this is triggered. Here is an example of what the event looks like if you have DCShadow performed in your environment

Event Filter to run

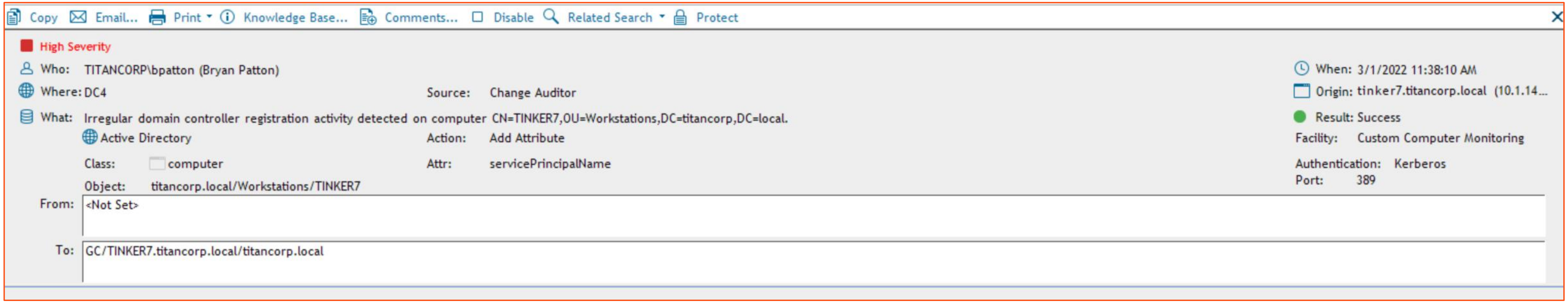


tity

ent Class

Object

Irregular domain controller registration activity detected



High Severity

Who: TITANCORP\bpatton (Bryan Patton)

When: 3/1/2022 11:38:10 AM

Where: DC4

Source: Change Auditor

Origin: tinker7.titancorp.local (10.1.14...

What: Irregular domain controller registration activity detected on computer CN=TINKER7,OU=Workstations,DC=titancorp,DC=local.

Result: Success

Active Directory

Action: Add Attribute

Facility: Custom Computer Monitoring

Class: computer

Attr: servicePrincipalName

Authentication: Kerberos

Port: 389

Object: titancorp.local/Workstations/TINKER7

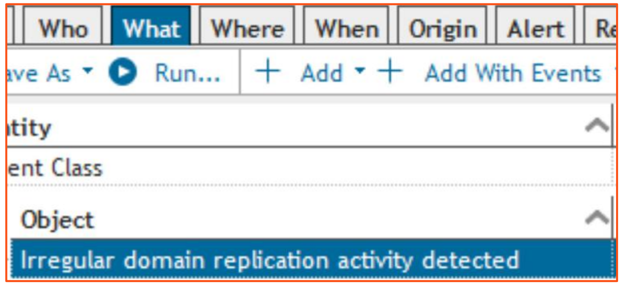
From: <Not Set>

To: GC/TINKER7.titancorp.local/titancorp.local

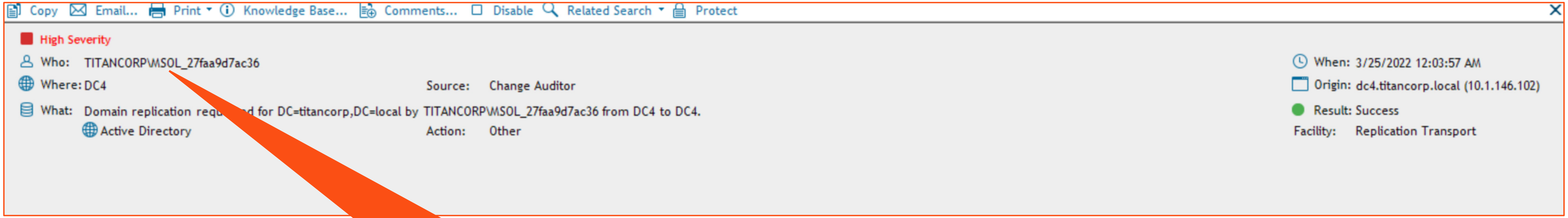
Irregular Domain Replication Activity Events (DCSync)

This event is triggered when password hashes are obtained. If using Azure AD Connect you will likely have many event generated by your MSOL_* account. After an event is generated, it is recommended to create an alert with a filter excluding your MSOL account to see the exceptions.

Event Filter to run



Irregular domain replication activity detected



High Severity

Who: TITANCORP\MSOL_27faa9d7ac36

Where: DC4

Source: Change Auditor

What: Domain replication requested for DC=titancorp,DC=local by TITANCORP\MSOL_27faa9d7ac36 from DC4 to DC4.

Active Directory

Action: Other

When: 3/25/2022 12:03:57 AM

Origin: dc4.titancorp.local (10.1.146.102)

Result: Success

Facility: Replication Transport

Exclude MSOL_* account

Quest

Where Next Meets Now.

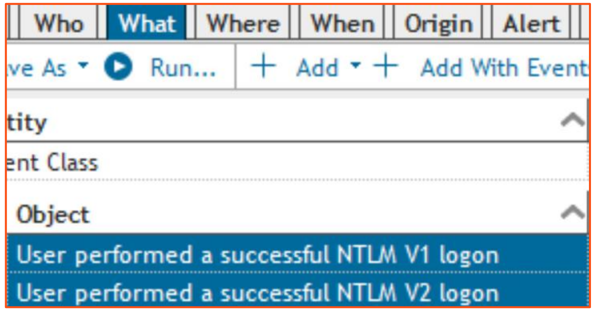
NTLMv1 & NTLM v2 (Needs Logon Activity Module)

NTLM is one of the most iconic and common attacks on Active Directory environments. In this attack, the attacker (Relay-er) captures an authentication and pass it to their desired server.

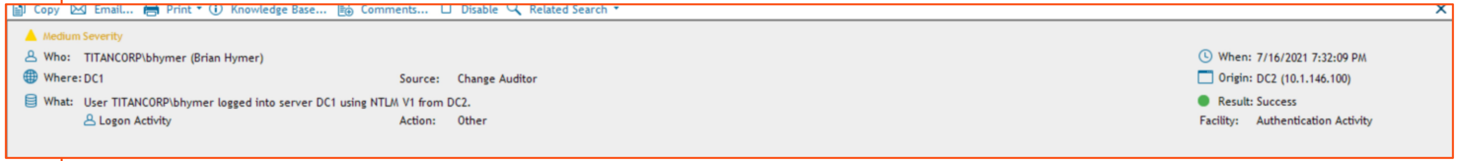
Change Auditor:

- By default, these event are disabled since NTLM activity it is chatty. It is recommended to enable this event for a period of 20 minutes to see if any NTLM traffic is being generated (Note that this feature is included with the Logon Activity User module of Change Auditor).
- It is also recommended to perform these activites for NTLMv1 first then move to NTLMv2
- After running a search, you can view the origin and see if there are any conflicts. We want to look for any origins that may be mission critical applications and once those have been resolved you can disable NTLM and then setup an alert in the event if NTLM is detected by Change Auditor. If no events are generated for 20 minutes, you can keep the event enabled. Once you are comfortable that no mission critical applications are using NTLM it is advisable to configure a GPO to disable the use of NTLM.

Event Filter to run



User performed a successful NTLM V1 logon
User performed a successful NTLM V2 logon



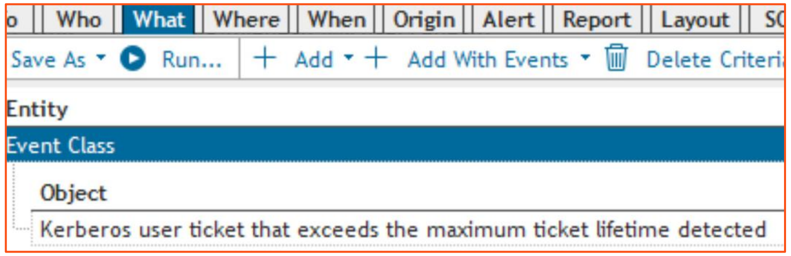
Medium Severity

Who: TITANCORP\bhymer (Brian Hymer)
Where: DC1
Source: Change Auditor
What: User TITANCORP\bhymer logged into server DC1 using NTLM V1 from DC2.
Logon Activity
Action: Other
When: 7/16/2021 7:32:09 PM
Origin: DC2 (10.1.146.100)
Result: Success
Facility: Authentication Activity

Kerberos user ticket events that exceed the maximum ticket lifetime (Needs Logon Activity Module)

Golden Ticket Attacks give attackers unrestricted access to networked resources and the ability to forge new tickets, allowing them to reside on networks indefinitely by being disguised as credentialed administrator-level users. While TGTs are usually valid for 10 hours by default, an attacker can make the TGT valid for any length of time up to 10 years.

Event Filter to run

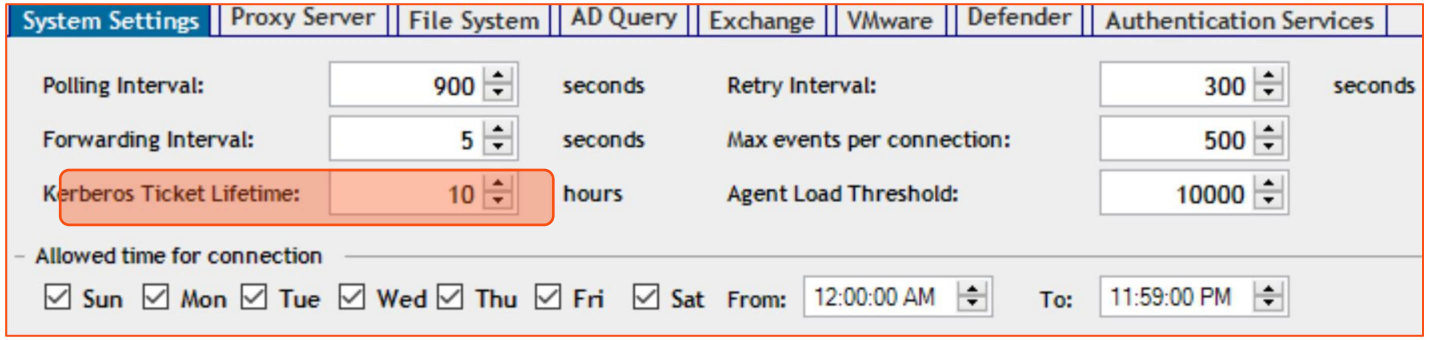


Entity

Event Class

Object

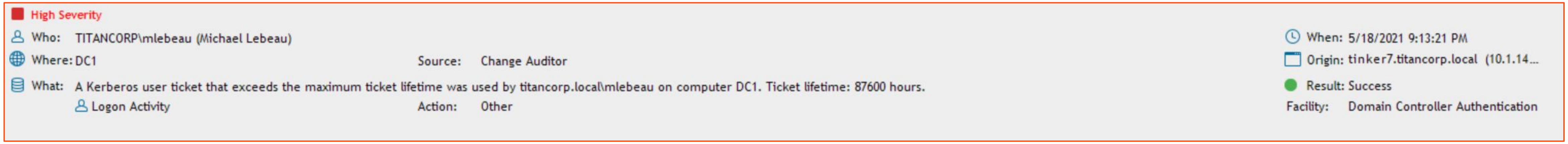
Kerberos user ticket that exceeds the maximum ticket lifetime detected



Polling Interval:	900	seconds	Retry Interval:	300	seconds
Forwarding Interval:	5	seconds	Max events per connection:	500	
Kerberos Ticket Lifetime:	10	hours	Agent Load Threshold:	10000	

Allowed time for connection

☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat From: 12:00:00 AM To: 11:59:00 PM



High Severity

Who: TITANCORP\mlebeau (Michael Lebeau)

When: 5/18/2021 9:13:21 PM

Where: DC1

Source: Change Auditor

Origin: tinker7.titancorp.local (10.1.14...

What: A Kerberos user ticket that exceeds the maximum ticket lifetime was used by titancorp.local\mlebeau on computer DC1. Ticket lifetime: 87600 hours.

Result: Success

Logon Activity

Action: Other

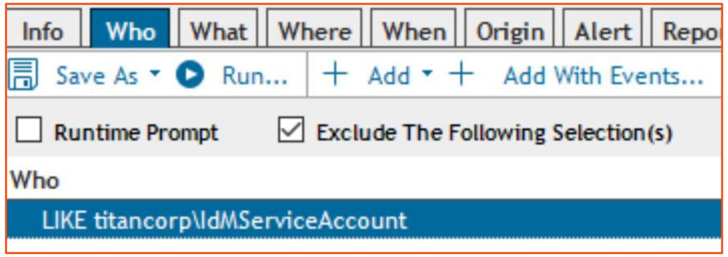
Facility: Domain Controller Authentication

Changes by Human vs. IAM

If Identity and Access Management (IAM) processes are in place, changes made by humans should be unusual. Monitoring for changes outside of the IAM process would only generate light alert noise as changes by humans should be an exception. It would be advantageous to have the ability to review alert emails and ignore if you know the change was valid.

If IAM product/process are not in place for AD, this may not be advisable as it would generate many alerts.

Event Filter to run



□ Runtime Prompt ☑ Exclude The Following Selection(s)

Who

LIKE titancorp\IdMServiceAccount

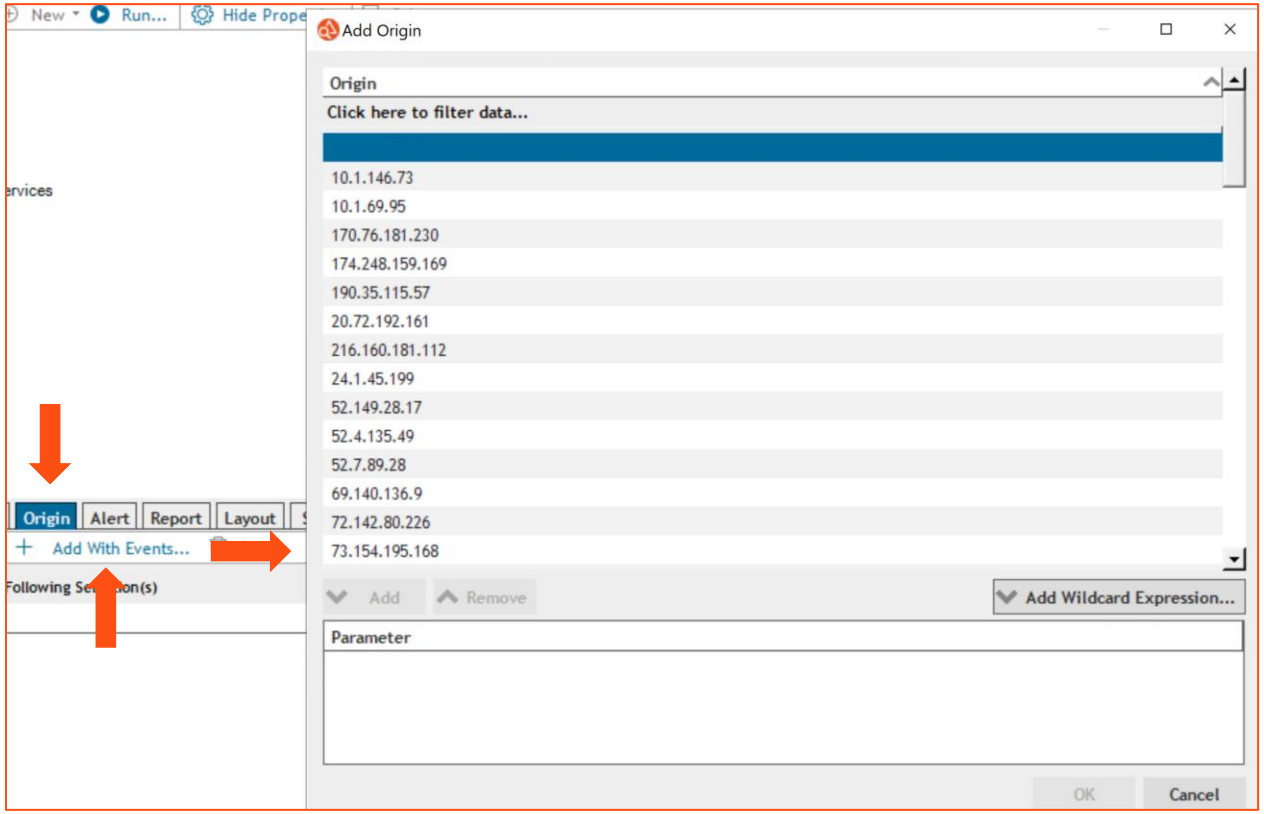
Where Next Meets Now.

Service account used out of band

Every service should have an origination defined of how that account is to be used. For example, with APPLICARION (GPOADmin) the account originating data should only ever be from the APPLICATION (GPOADmin) server. If change happens outside of that one server, alerts should be configured.

If you are using IAM, an alert could be configured when the IAM service account is made outside of the origin which should be the source server of your IAM system.

Event Filter to run



Origin
Click here to filter data...
10.1.146.73
10.1.69.95
170.76.181.230
174.248.159.169
190.35.115.57
20.72.192.161
216.160.181.112
24.1.45.199
52.149.28.17
52.4.135.49
52.7.89.28
69.140.136.9
72.142.80.226
73.154.195.168

Parameter

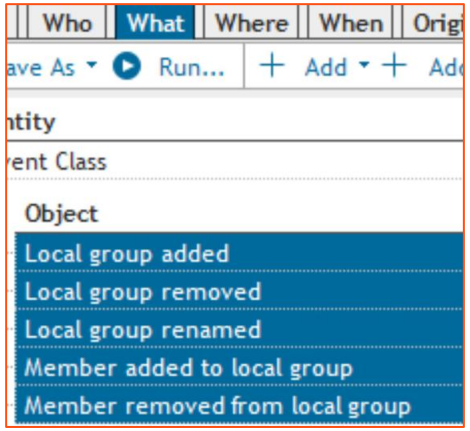
Quest

Where Next Meets Now.

Changes to Membership of local “administrators” group

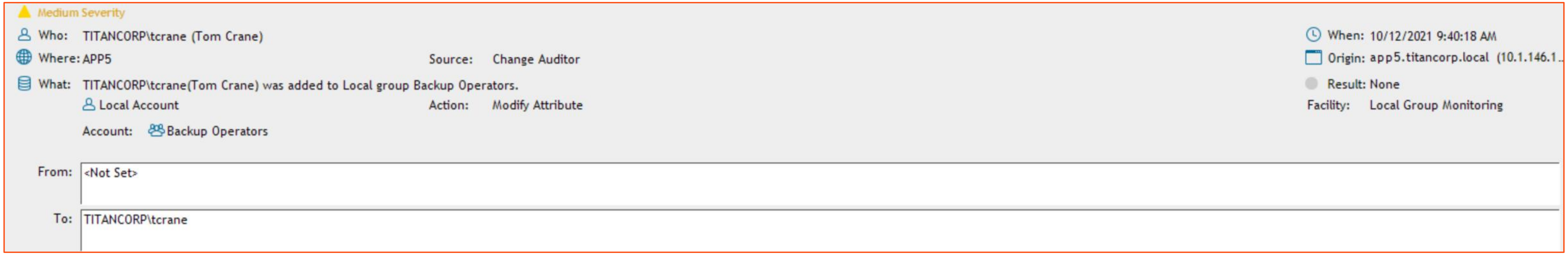
Being a member of the local administrator group gives those objects the ability to go into debug mode on that machine. This is commonly used with Mimikatz to extract information locally on those machines and should be monitored accordingly. Being a local admin gives object ability to execute “privilege::debug” locally on a machine with Mimikatz as default behavior. It’s possible to change this via GPO and make an exception group for debug permission.

Event Filter to run



ntity
ent Class

Object
Local group added
Local group removed
Local group renamed
Member added to local group
Member removed from local group



Medium Severity

Who: TITANCORP\tcrane (Tom Crane)

Where: APP5

Source: Change Auditor

What: TITANCORP\tcrane(Tom Crane) was added to Local group Backup Operators.

Local Account

Action: Modify Attribute

Account: Backup Operators

When: 10/12/2021 9:40:18 AM

Origin: app5.titancorp.local (10.1.146.1

Result: None

Facility: Local Group Monitoring

From: <Not Set>

To: TITANCORP\tcrane

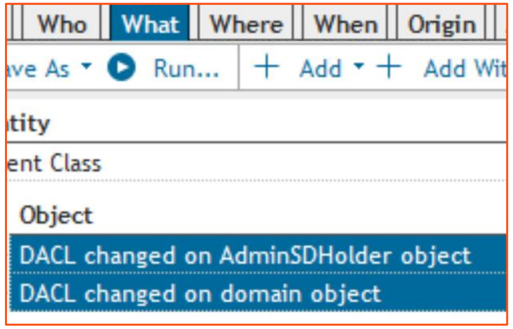
DACL changes on Domain container

DCSync is an attack that allows an adversary to simulate the behavior of a domain controller (DC) and retrieve password data via domain replication.

Generally, Administrators, Domain Admins and Enterprise Admins have the rights required to execute a DCSync attack. Specifically, the following rights are required:

- Replicating Directory Changes
- Replicating Directory Changes All

Event Filter to run



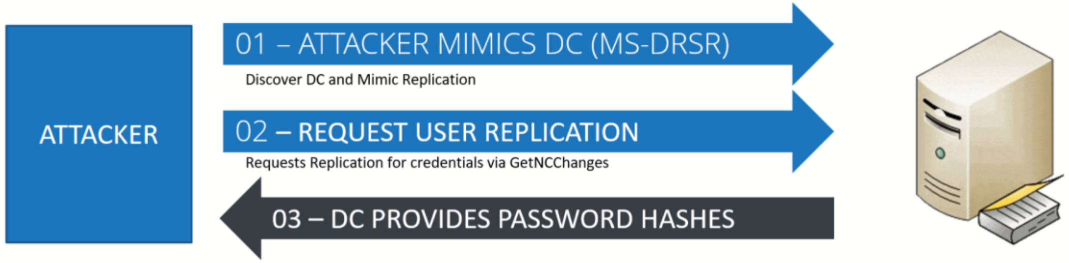
tity

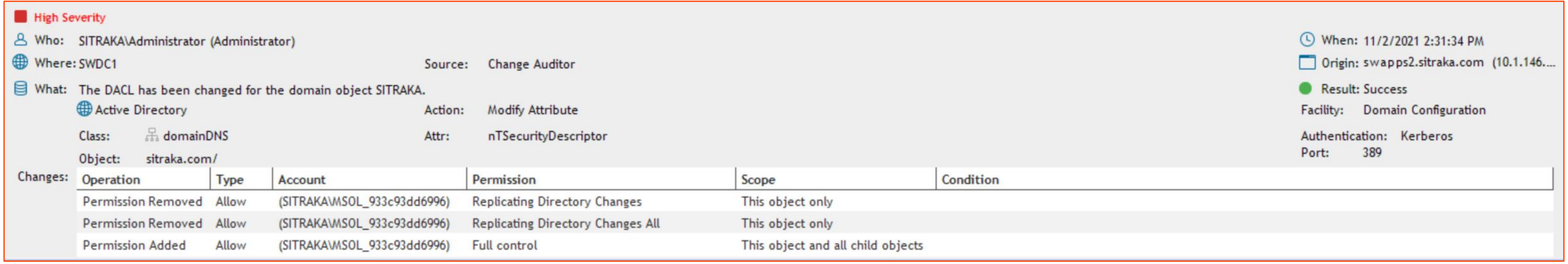
ent Class

Object

DACL changed on AdminSDHolder object

DACL changed on domain object


ATTACKER
01 – ATTACKER MIMICS DC (MS-DRSR)
Discover DC and Mimic Replication
02 – REQUEST USER REPLICATION
Requests Replication for credentials via GetNCChanges
03 – DC PROVIDES PASSWORD HASHES



High Severity

Who: SITRAKA\Administrator (Administrator)

Where: SWDC1

Source: Change Auditor

What: The DACL has been changed for the domain object SITRAKA.

Active Directory

Action: Modify Attribute

Class: domainDNS

Attr: nTSecurityDescriptor

Object: sitraka.com/

When: 11/2/2021 2:31:34 PM

Origin: swapps2.sitraka.com (10.1.146....

Result: Success

Facility: Domain Configuration

Authentication: Kerberos

Port: 389

Changes:

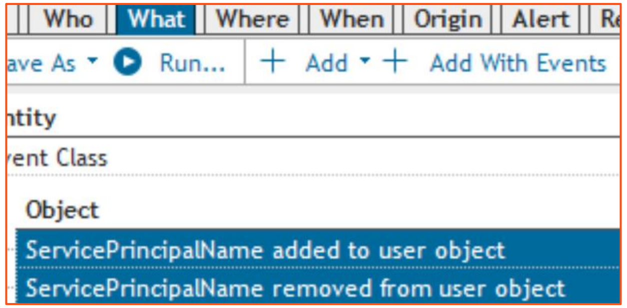
Operation	Type	Account	Permission	Scope	Condition
Permission Removed	Allow	(SITRAKA\MSOL_933c93dd6996)	Replicating Directory Changes	This object only	
Permission Removed	Allow	(SITRAKA\MSOL_933c93dd6996)	Replicating Directory Changes All	This object only	
Permission Added	Allow	(SITRAKA\MSOL_933c93dd6996)	Full control	This object and all child objects	

SPN added

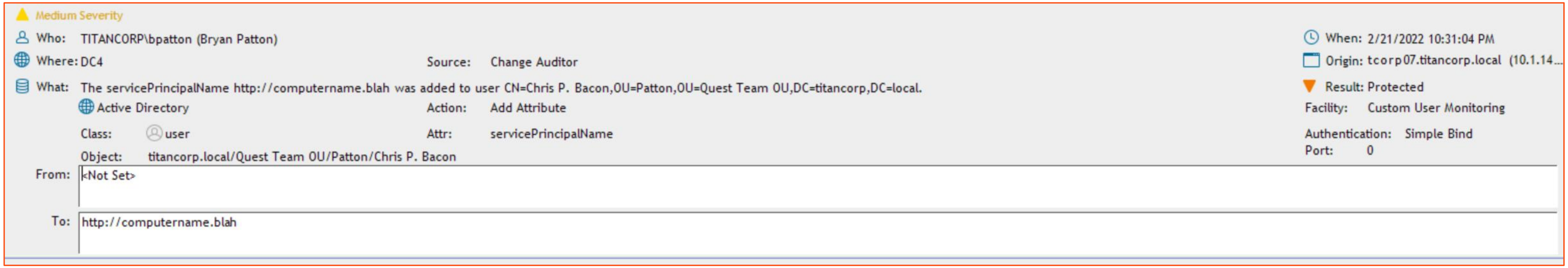
Silver Ticket Attack and Kerberoasting

Adversaries primarily target service or user accounts, since a successful takeover of such accounts can let an adversary brute-force the password to these accounts or add an arbitrary user to the group of administrator for that service

Event Filter to run



ServicePrincipalName added to user object
ServicePrincipalName removed from user object



Medium Severity

Who: TITANCORP\bpatton (Bryan Patton)

Where: DC4   Source: Change Auditor

What: The servicePrincipalName http://computername.blah was added to user CN=Chris P. Bacon,OU=Patton,OU=Quest Team OU,DC=titancorp,DC=local.

Active Directory   Action: Add Attribute

Class: user   Attr: servicePrincipalName

Object: titancorp.local/Quest Team OU/Patton/Chris P. Bacon

When: 2/21/2022 10:31:04 PM

Origin: tcorp07.titancorp.local (10.1.14...

Result: Protected

Facility: Custom User Monitoring

Authentication: Simple Bind

Port: 0

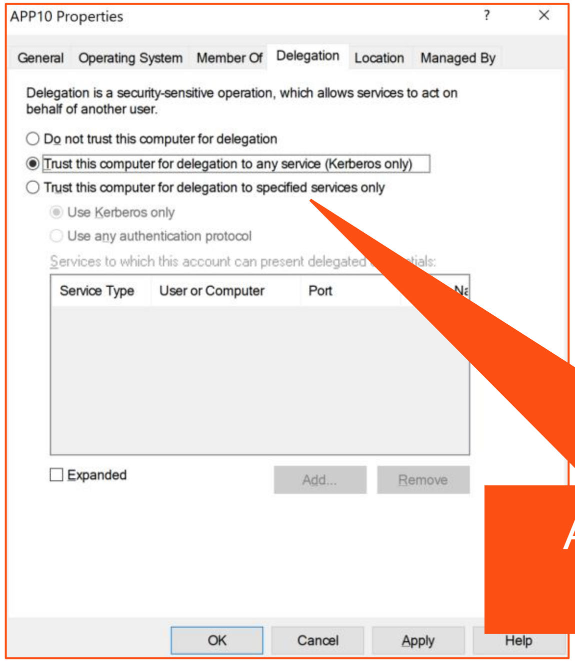
From: <Not Set>

To: http://computername.blah

Searches for unconstrained delegation

Credential Theft Leveraging Unconstrained Delegation

If an attacker finds a server with Kerberos Unconstrained Delegation, they can compromise the server via an admin or service account or Social engineer a Domain Admin to connect to any service on the server with unconstrained delegation.



APP10 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

● Trust this computer for delegation to any service (Kerberos only)

○ Trust this computer for delegation to specified services only

○ Use Kerberos only

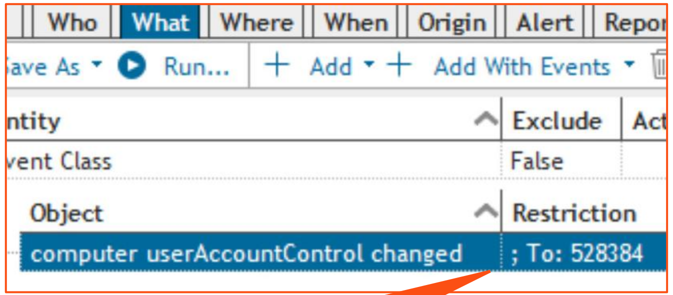
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Na

□ Expanded

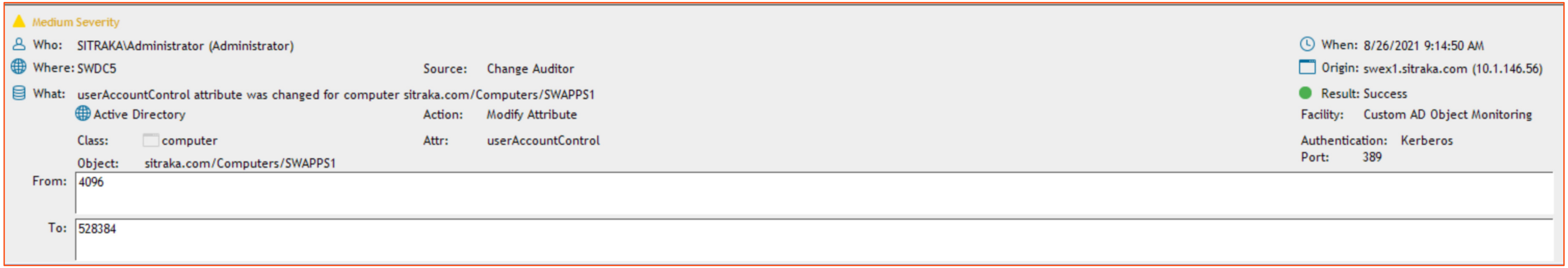
Event Filter to run



ntity	Exclude	Act
vent Class	False	

Object	Restriction
computer userAccountControl changed	; To: 528384

Action on left generates activity on right



Medium Severity

Who: SITRAKA\Administrator (Administrator)

Where: SWDC5

Source: Change Auditor

What: userAccountControl attribute was changed for computer sitraka.com/Computers/SWAPPS1

Active Directory

Action: Modify Attribute

Class: computer

Attr: userAccountControl

Object: sitraka.com/Computers/SWAPPS1

When: 8/26/2021 9:14:50 AM

Origin: swex1.sitraka.com (10.1.146.56)

Result: Success

Facility: Custom AD Object Monitoring

Authentication: Kerberos

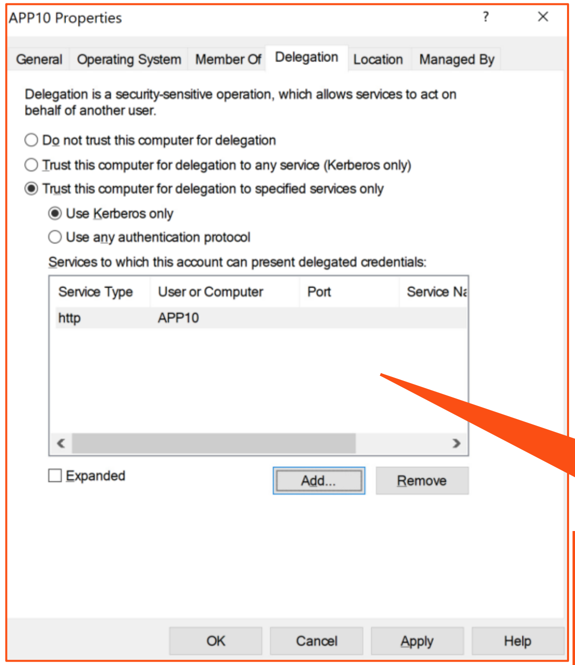
Port: 389

From: 4096

To: 528384

Searches for constrained delegation

Constrained Delegation allows you to configure which services an account can be delegated to. This, in theory, would limit the potential exposure if a compromise occurred



APP10 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation

○ Trust this computer for delegation to any service (Kerberos only)

● Trust this computer for delegation to specified services only

● Use Kerberos only

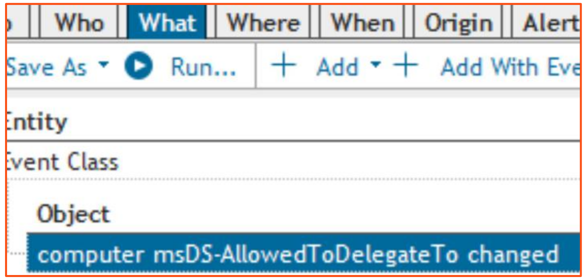
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer	Port	Service Na
http	APP10		

□ Expanded

Event Filter to run



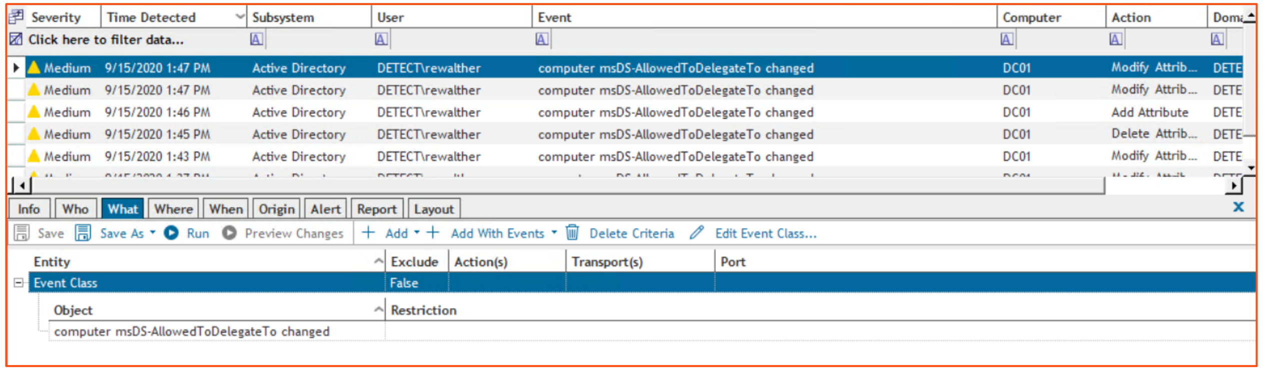
ntity

vent Class

Object

computer msDS-AllowedToDelegateTo changed

Action on left generates activity on right



Severity	Time Detected	Subsystem	User	Event	Computer	Action	Doma
Click here to filter data...							
Medium	9/15/2020 1:47 PM	Active Directory	DETECT\rewalther	computer msDS-AllowedToDelegateTo changed	DC01	Modify Attrib...	DETE
Medium	9/15/2020 1:47 PM	Active Directory	DETECT\rewalther	computer msDS-AllowedToDelegateTo changed	DC01	Modify Attrib...	DETE
Medium	9/15/2020 1:46 PM	Active Directory	DETECT\rewalther	computer msDS-AllowedToDelegateTo changed	DC01	Add Attribute	DETE
Medium	9/15/2020 1:45 PM	Active Directory	DETECT\rewalther	computer msDS-AllowedToDelegateTo changed	DC01	Delete Attrib...	DETE
Medium	9/15/2020 1:43 PM	Active Directory	DETECT\rewalther	computer msDS-AllowedToDelegateTo changed	DC01	Modify Attrib...	DETE

Entity	Exclude	Action(s)	Transport(s)	Port
Event Class	False			

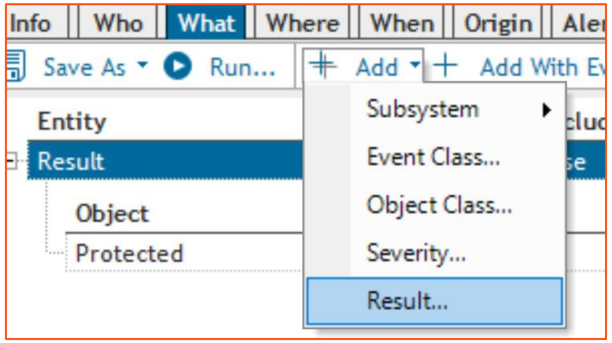
Object	Restriction
computer msDS-AllowedToDelegateTo changed	

Searches for changes to Protected objects

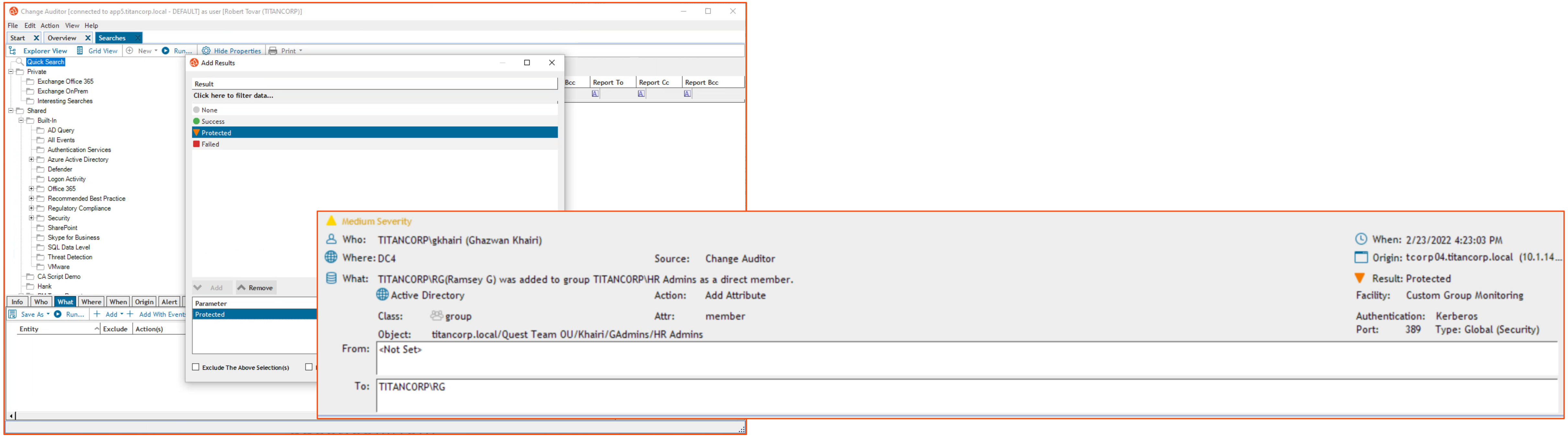
In general, all protected objects are usually critical objects and alerts should be defined.

Rather than create multiple alerts you can create a single alert that includes all existing and future protected objects.

Event Filter to run



Entity
Result
Object
Protected



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Robert Tovar (TITANCORP)]

- Quick Search
- Private
  - Exchange Office 365
  - Exchange OnPrem
  - Interesting Searches
- Shared
  - Built-In
    - AD Query
    - All Events
    - Authentication Services
    - Azure Active Directory
    - Defender
    - Logon Activity
    - Office 365
    - Recommended Best Practice
    - Regulatory Compliance
    - Security
    - SharePoint
    - Skype for Business
    - SQL Data Level
    - Threat Detection
    - VMware
  - CA Script Demo
  - Hank

Entity	Exclude	Action(s)

Add Results

Result

Click here to filter data...

- None
- Success
- Protected
- Failed

Parameter
Protected

□ Exclude The Above Selection(s)

Medium Severity

Who: TITANCORP\gkhairi (Ghazwan Khairi)

Where: DC4 Source: Change Auditor

What: TITANCORP\RG(Ramsey G) was added to group TITANCORP\HR Admins as a direct member.

Active Directory Action: Add Attribute

Class: group Attr: member

Object: titancorp.local/Quest Team OU/Khairi/GAdmins/HR Admins

From: <Not Set>

To: TITANCORP\RG

When: 2/23/2022 4:23:03 PM

Origin: tcorp04.titancorp.local (10.1.14...

Result: Protected

Facility: Custom Group Monitoring

Authentication: Kerberos

Port: 389 Type: Global (Security)

Change Auditor
Suggested Protection Templates

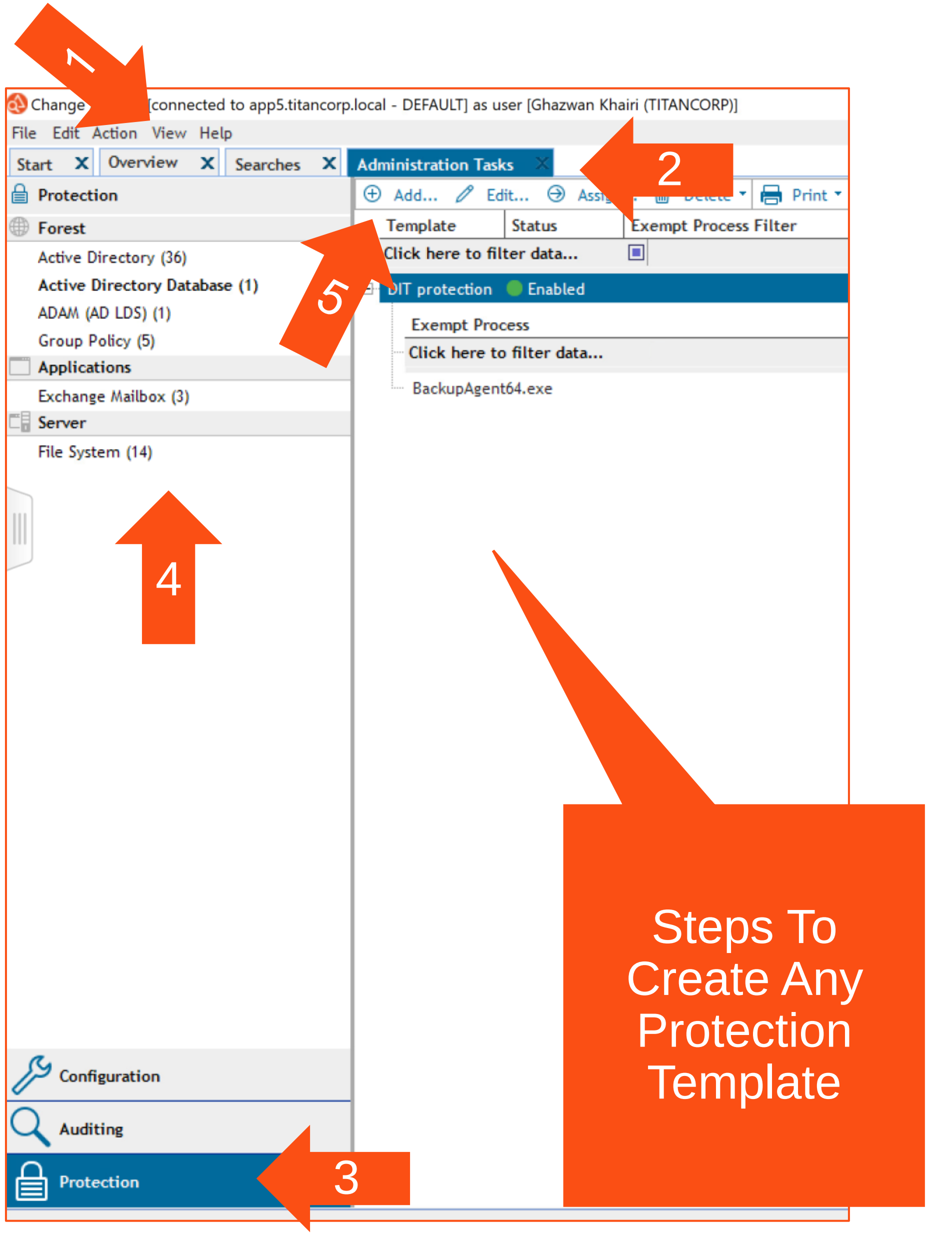
- ❖NTDS.DIT
- ❖Privileged Groups
- ❖AdminSDHolder
- ❖GPOs
- ❖GPO Linkage

Where Next Meets Now.

Setting Up Protection Templates Process

1. Start at the ‘View Menu’
2. Select Administration
3. From the administration task page, select Protection
   - You will see a list of all the entities you can apply a protection template against
4. Select the object from the list
   - Forest level
     - Active Directory
     - Active Directory Database
     - ADAM (AD LDS)
     - Group Policy
   - Applications
     - Exchange Mailbox
   - Server
     - File System
5. Click Add to start the protection template wizard
   - Based on your selections the screens maybe slightly different
   - Follow the screens

- **Use the examples from the next few slides as reference**



Steps To Create Any Protection Template

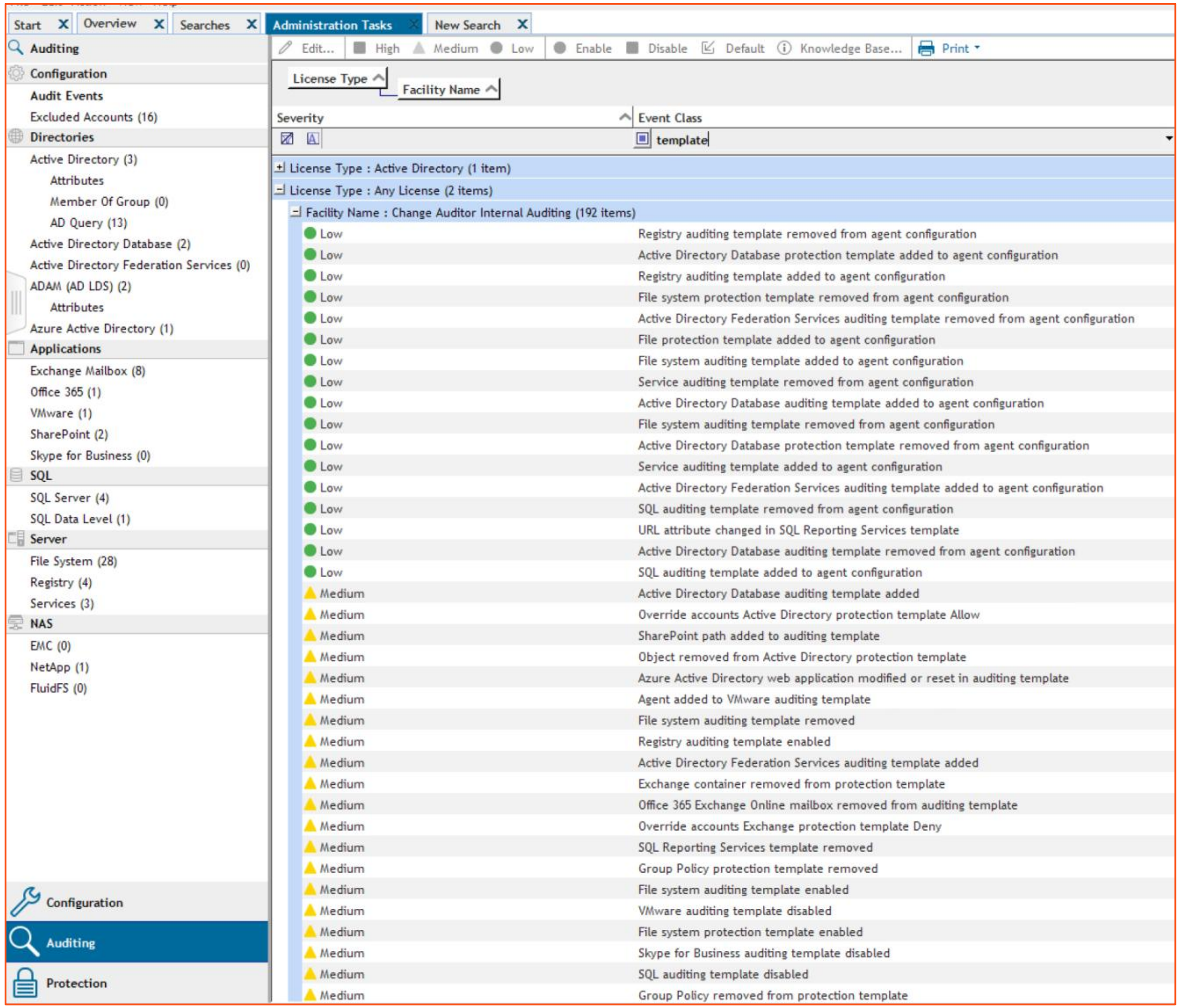
Collection Templates Changes Are Audited!

A. Change Auditor Internal Auditing captures any changes users trigger against protection templates.

B. So, if a user adds, edits, deletes, assigns the template to a configuration, removes the template from a configuration, an event is generated

C. These events, like all other Change Auditor events, can be searches, viewed, reported on, and most importantly alerted on

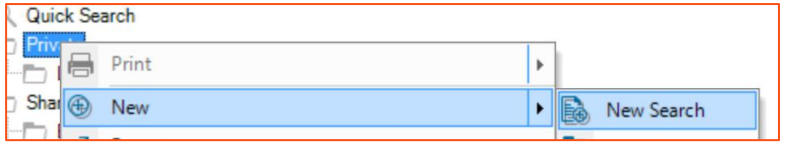
D. This ensures that protection of the various security measures and settings throughout your environment are constantly being applied.



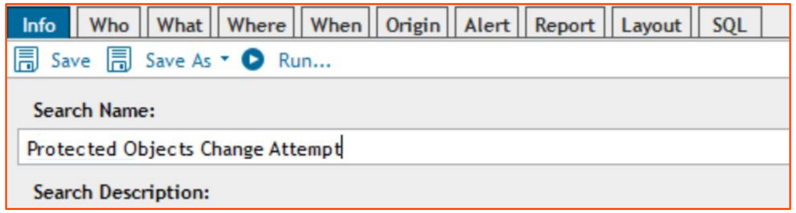
Severity	Event Class
	template
License Type : Active Directory (1 item)	
License Type : Any License (2 items)	
Facility Name : Change Auditor Internal Auditing (192 items)	
● Low	Registry auditing template removed from agent configuration
● Low	Active Directory Database protection template added to agent configuration
● Low	Registry auditing template added to agent configuration
● Low	File system protection template removed from agent configuration
● Low	Active Directory Federation Services auditing template removed from agent configuration
● Low	File protection template added to agent configuration
● Low	File system auditing template added to agent configuration
● Low	Service auditing template removed from agent configuration
● Low	Active Directory Database auditing template added to agent configuration
● Low	File system auditing template removed from agent configuration
● Low	Active Directory Database protection template removed from agent configuration
● Low	Service auditing template added to agent configuration
● Low	Active Directory Federation Services auditing template added to agent configuration
● Low	SQL auditing template removed from agent configuration
● Low	URL attribute changed in SQL Reporting Services template
● Low	Active Directory Database auditing template removed from agent configuration
● Low	SQL auditing template added to agent configuration
▲ Medium	Active Directory Database auditing template added
▲ Medium	Override accounts Active Directory protection template Allow
▲ Medium	SharePoint path added to auditing template
▲ Medium	Object removed from Active Directory protection template
▲ Medium	Azure Active Directory web application modified or reset in auditing template
▲ Medium	Agent added to VMware auditing template
▲ Medium	File system auditing template removed
▲ Medium	Registry auditing template enabled
▲ Medium	Active Directory Federation Services auditing template added
▲ Medium	Exchange container removed from protection template
▲ Medium	Office 365 Exchange Online mailbox removed from auditing template
▲ Medium	Override accounts Exchange protection template Deny
▲ Medium	SQL Reporting Services template removed
▲ Medium	Group Policy protection template removed
▲ Medium	File system auditing template enabled
▲ Medium	VMware auditing template disabled
▲ Medium	File system protection template enabled
▲ Medium	Skype for Business auditing template disabled
▲ Medium	SQL auditing template disabled
▲ Medium	Group Policy removed from protection template

Setting Up Alerts / Reports On Protected Objects Change Attempts

1. Create New Search



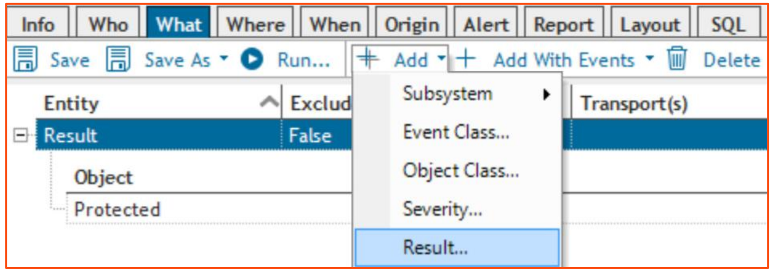
2. Provide Descriptive Name



Search Name: Protected Objects Change Attempt

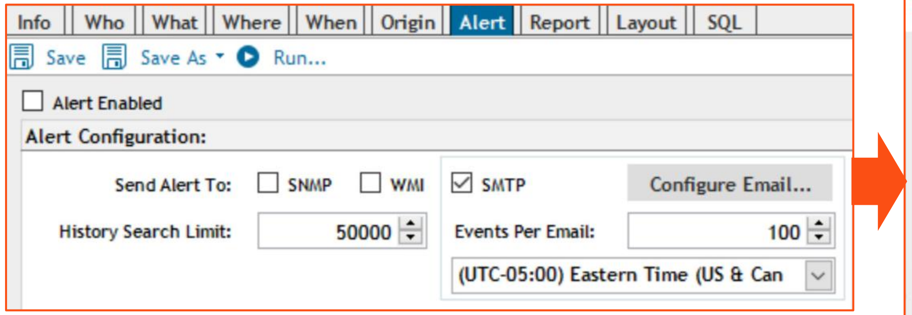
Search Description:

3. Filter Result = Protected



Entity	Exclud	Transport(s)
Result	False	
Object		
Protected		

4. Setup Alert



□ Alert Enabled

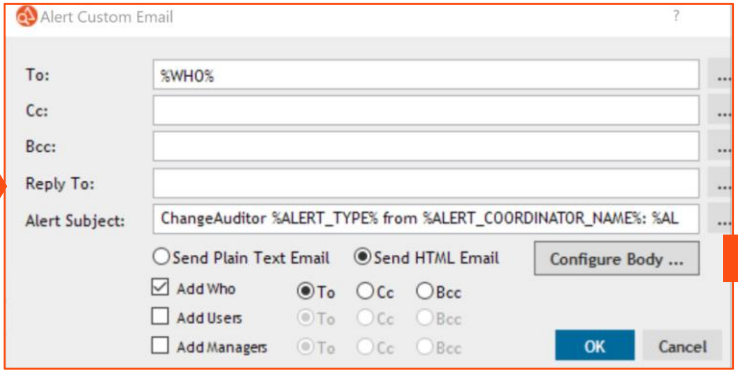
Alert Configuration:

Send Alert To: □ SNMP □ WMI ☑ SMTP

History Search Limit: 50000

Events Per Email: 100

(UTC-05:00) Eastern Time (US & Can



To: %WHO%

Cc:

Bcc:

Reply To:

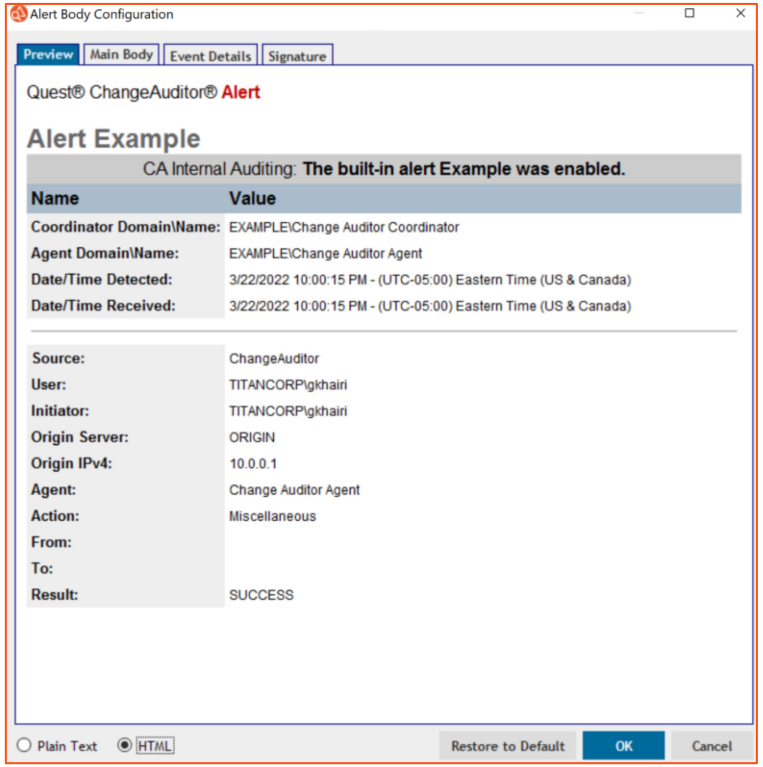
Alert Subject: ChangeAuditor %ALERT_TYPE% from %ALERT_COORDINATOR_NAME%: %AL

○ Send Plain Text Email ● Send HTML Email

☑ Add Who ● To ○ Cc ○ Bcc

□ Add Users ● To ○ Cc ○ Bcc

□ Add Managers ● To ○ Cc ○ Bcc



Quest® ChangeAuditor® **Alert**

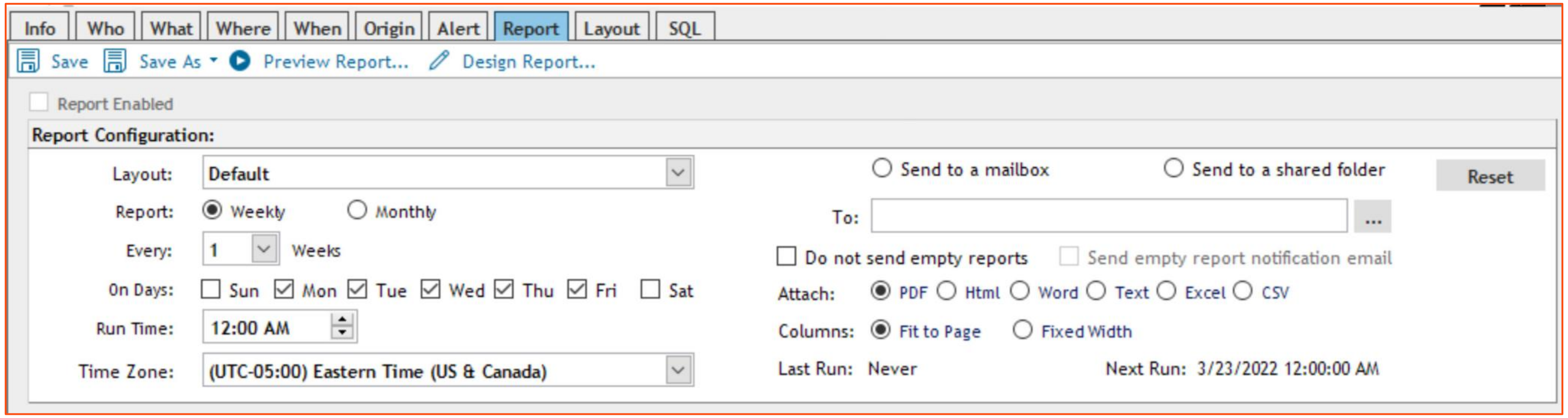
Alert Example

CA Internal Auditing: **The built-in alert Example was enabled.**

Name	Value
Coordinator Domain\Name:	EXAMPLE\Change Auditor Coordinator
Agent Domain\Name:	EXAMPLE\Change Auditor Agent
Date/Time Detected:	3/22/2022 10:00:15 PM - (UTC-05:00) Eastern Time (US & Canada)
Date/Time Received:	3/22/2022 10:00:15 PM - (UTC-05:00) Eastern Time (US & Canada)
Source:	ChangeAuditor
User:	TITANCORP\gkhairi
Initiator:	TITANCORP\gkhairi
Origin Server:	ORIGIN
Origin IPv4:	10.0.0.1
Agent:	Change Auditor Agent
Action:	Miscellaneous
From:	
To:	
Result:	SUCCESS

○ Plain Text ● HTML

5. Setup Report



□ Report Enabled

Report Configuration:

Layout: Default

Report: ● Weekly ○ Monthly

Every: 1 Weeks

On Days: □ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri □ Sat

Run Time: 12:00 AM

Time Zone: (UTC-05:00) Eastern Time (US & Canada)

○ Send to a mailbox ○ Send to a shared folder

To:

□ Do not send empty reports □ Send empty report notification email

Attach: ● PDF ○ Html ○ Word ○ Text ○ Excel ○ CSV

Columns: ● Fit to Page ○ Fixed Width

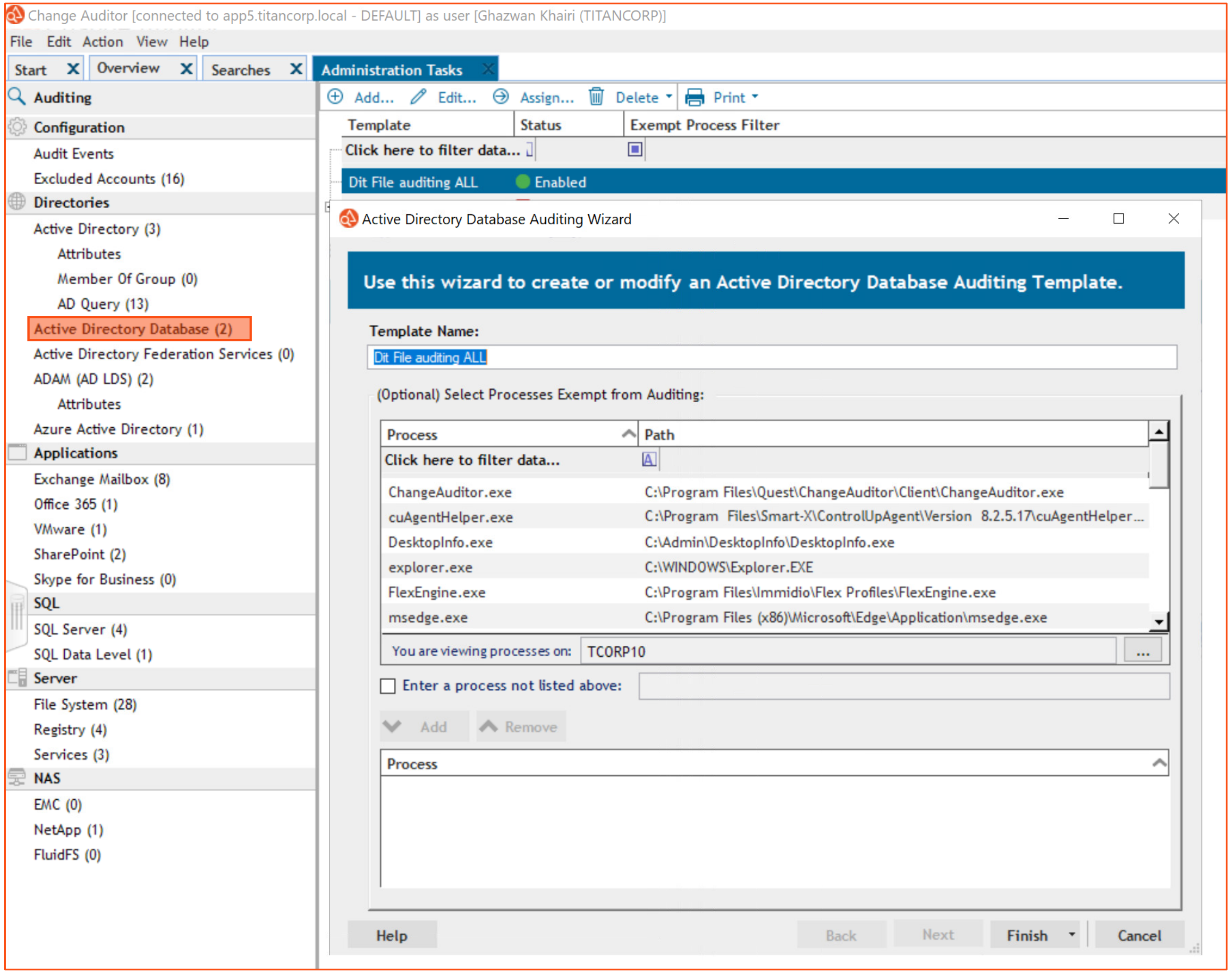
Last Run: Never

Next Run: 3/23/2022 12:00:00 AM

Enable NTDS.DIT File Auditing Template

Change Auditor has a feature to audit access to the NTDS.DIT database. Before these events are audited it must be configured.

From the Administration Configuration section, select Active Directory Database, Click Add and configure your template



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Ghazwan Khairi (TITANCORP)]

Template	Status	Exempt Process Filter
Click here to filter data...		
Dit File auditing ALL	Enabled	

Active Directory Database Auditing Wizard

Use this wizard to create or modify an Active Directory Database Auditing Template.

Template Name: Dit File auditing ALL

(Optional) Select Processes Exempt from Auditing:

Process	Path
Click here to filter data...	
ChangeAuditor.exe	C:\Program Files\Quest\ChangeAuditor\Client\ChangeAuditor.exe
cuAgentHelper.exe	C:\Program Files\Smart-X\ControlUpAgent\Version 8.2.5.17\cuAgentHelper...
DesktopInfo.exe	C:\Admin\DesktopInfo\DesktopInfo.exe
explorer.exe	C:\WINDOWS\Explorer.EXE
FlexEngine.exe	C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

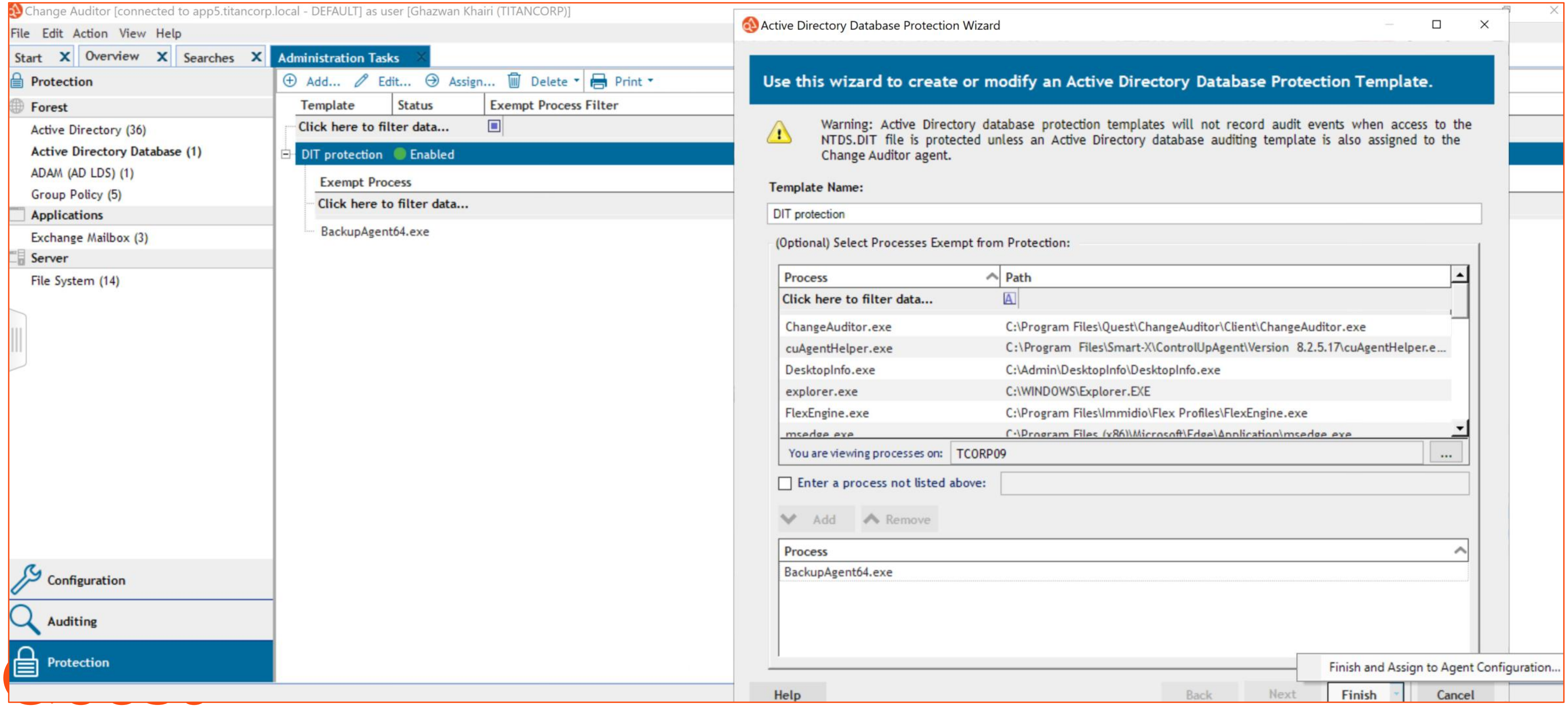
You are viewing processes on: TCORP10

□ Enter a process not listed above:

Protect NTDS.DIT File

Extraction of this file could lead to parsing of usernames and passwords resulting in a security breach

Read Notes Section



Template	Status	Exempt Process Filter
Click here to filter data...		
DIT protection	● Enabled	

Exempt Process
Click here to filter data...
BackupAgent64.exe

Use this wizard to create or modify an Active Directory Database Protection Template.

Warning: Active Directory database protection templates will not record audit events when access to the NTDS.DIT file is protected unless an Active Directory database auditing template is also assigned to the Change Auditor agent.

Template Name: DIT protection

(Optional) Select Processes Exempt from Protection:

Process	Path
Click here to filter data...	
ChangeAuditor.exe	C:\Program Files\Quest\ChangeAuditor\Client\ChangeAuditor.exe
cuAgentHelper.exe	C:\Program Files\Smart-X\ControlUpAgent\Version 8.2.5.17\cuAgentHelper.e...
DesktopInfo.exe	C:\Admin\DesktopInfo\DesktopInfo.exe
explorer.exe	C:\WINDOWS\Explorer.EXE
FlexEngine.exe	C:\Program Files\Immidio\Flex Profiles\FlexEngine.exe
msedge.exe	C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe

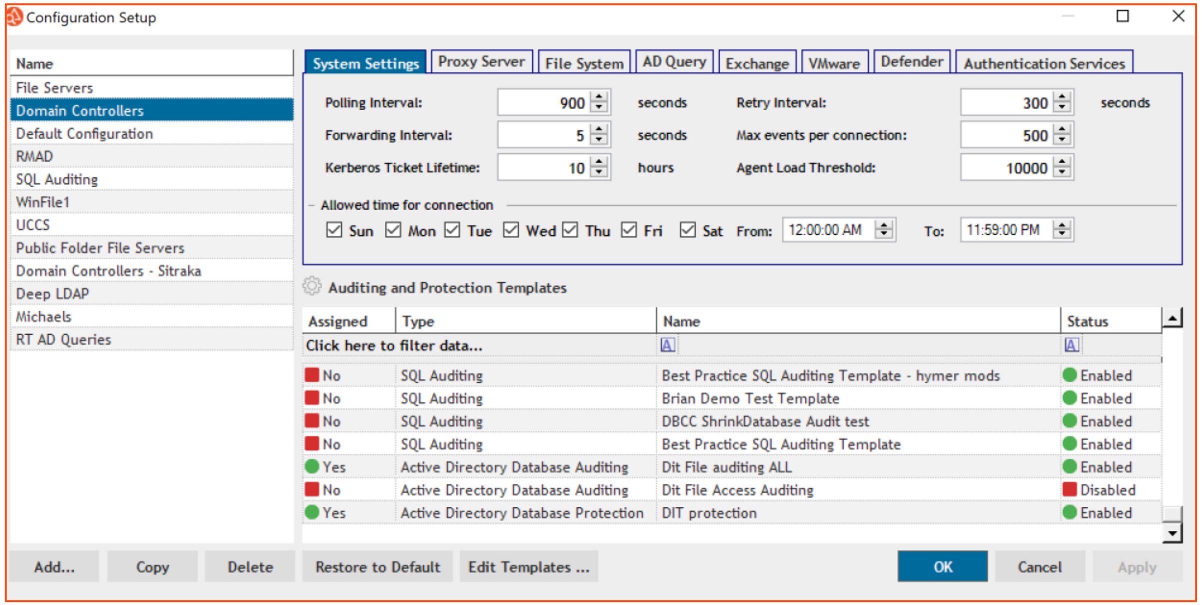
You are viewing processes on: TCORP09

□ Enter a process not listed above:

Process
BackupAgent64.exe

Protect NTDS.DIT File

1. Configure the protection template (as shown on previous slide)
    - Brainstorm other processes to exclude from the protection
        - Ex: Anti-Virus (read notes section below)
2. Finish and assign to configuration
3. Choose Default Configuration or Configuration that has the DCs in it



Name
- File Servers
- Domain Controllers
- Default Configuration
- RMAD
- SQL Auditing
- WinFile1
- UCCS
- Public Folder File Servers
- Domain Controllers - Sitraka
- Deep LDAP
- Michaels
- RT AD Queries

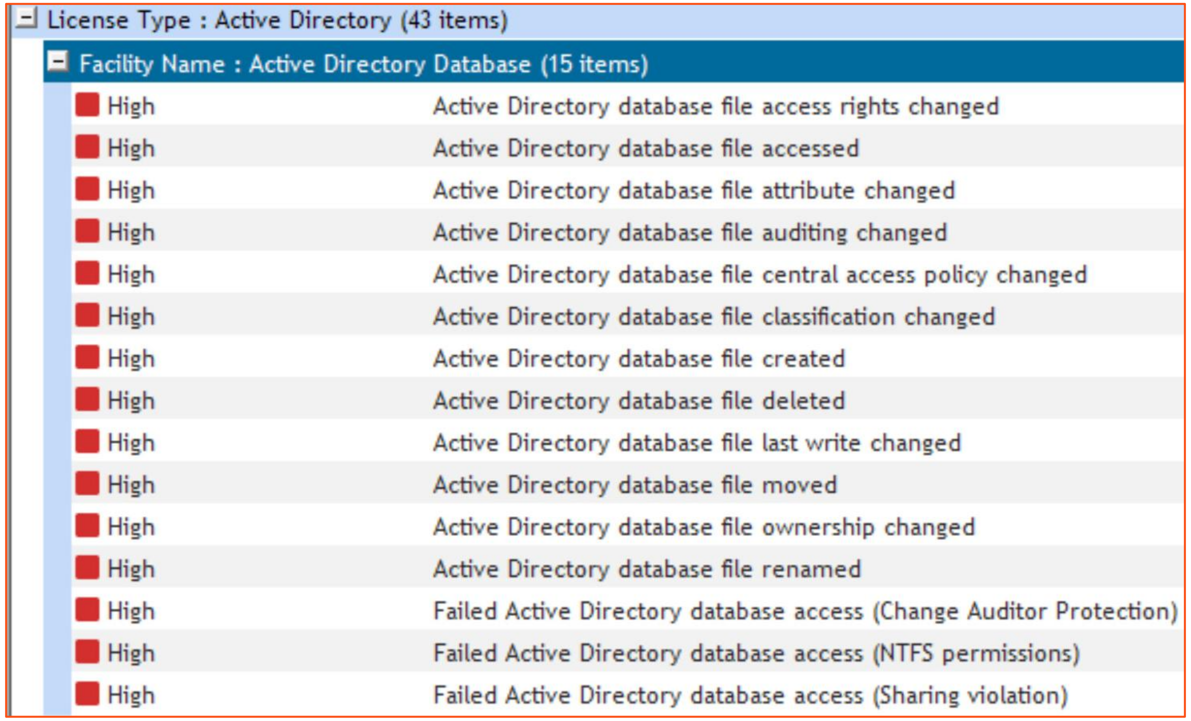
Polling Interval: 900 seconds
Retry Interval: 300 seconds
Forwarding Interval: 5 seconds
Max events per connection: 500
Kerberos Ticket Lifetime: 10 hours
Agent Load Threshold: 10000

Allowed time for connection
☑ Sun ☑ Mon ☑ Tue ☑ Wed ☑ Thu ☑ Fri ☑ Sat From: 12:00:00 AM To: 11:59:00 PM

Assigned	Type	Name	Status
🟥 No	SQL Auditing	Best Practice SQL Auditing Template - hymer mods	● Enabled
🟥 No	SQL Auditing	Brian Demo Test Template	● Enabled
🟥 No	SQL Auditing	DBCC ShrinkDatabase Audit test	● Enabled
🟥 No	SQL Auditing	Best Practice SQL Auditing Template	● Enabled
● Yes	Active Directory Database Auditing	Dit File auditing ALL	● Enabled
🟥 No	Active Directory Database Auditing	Dit File Access Auditing	🟥 Disabled
● Yes	Active Directory Database Protection	DIT protection	● Enabled

NTDS.DIT File (Events & Built-In Searches)

The ability to audit changes to this file reduces the risk of the user account information from being accessed and tampered with by unwanted processes or users.



⊟ License Type : Active Directory (43 items)

⊟ Facility Name : Active Directory Database (15 items)

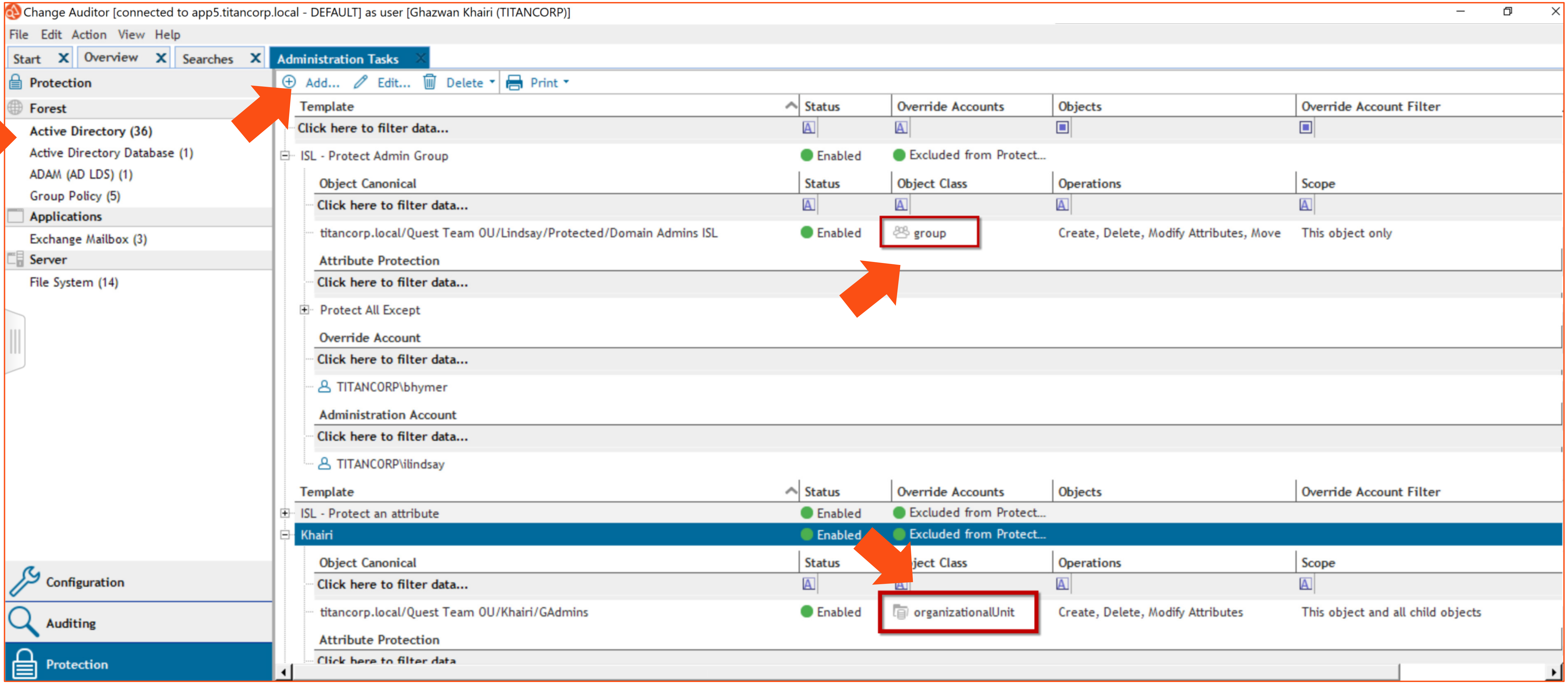
🟥 High	Active Directory database file access rights changed
🟥 High	Active Directory database file accessed
🟥 High	Active Directory database file attribute changed
🟥 High	Active Directory database file auditing changed
🟥 High	Active Directory database file central access policy changed
🟥 High	Active Directory database file classification changed
🟥 High	Active Directory database file created
🟥 High	Active Directory database file deleted
🟥 High	Active Directory database file last write changed
🟥 High	Active Directory database file moved
🟥 High	Active Directory database file ownership changed
🟥 High	Active Directory database file renamed
🟥 High	Failed Active Directory database access (Change Auditor Protection)
🟥 High	Failed Active Directory database access (NTFS permissions)
🟥 High	Failed Active Directory database access (Sharing violation)

The following built-in searches have been added:

- All Active Directory Database Events under Shared | Built-in | All Events
- Active Directory Database Events in last 30 days under Shared | Built-in | Security | Domain Controller Security
- GDPR - Active Directory Database Events in last 30 days under Shared | Built-in | Regulatory Compliance |GDPR |Audit and Accountability | Active Directory
- GDPR 32 - Active Directory Database Events in last 30 days under Shared | Built-in | Regulatory Compliance |GDPR |Security of Processing (32) | Active Directory

Protect Privileged Groups

Protection of privileged groups or OUs prevents unwanted tampering and unapproved membership changes



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Ghazwan Khairi (TITANCORP)]

Template	Status	Override Accounts	Objects	Override Account Filter
Click here to filter data...				
ISL - Protect Admin Group	● Enabled	● Excluded from Protect...		

Object Canonical	Status	Object Class	Operations	Scope
Click here to filter data...				
titancorp.local/Quest Team OU/Lindsay/Protected/Domain Admins ISL	● Enabled	group	Create, Delete, Modify Attributes, Move	This object only

Attribute Protection

Click here to filter data...

Protect All Except

Override Account

Click here to filter data...

TITANCORP\bhymer

Administration Account

Click here to filter data...

TITANCORP\ilindsay

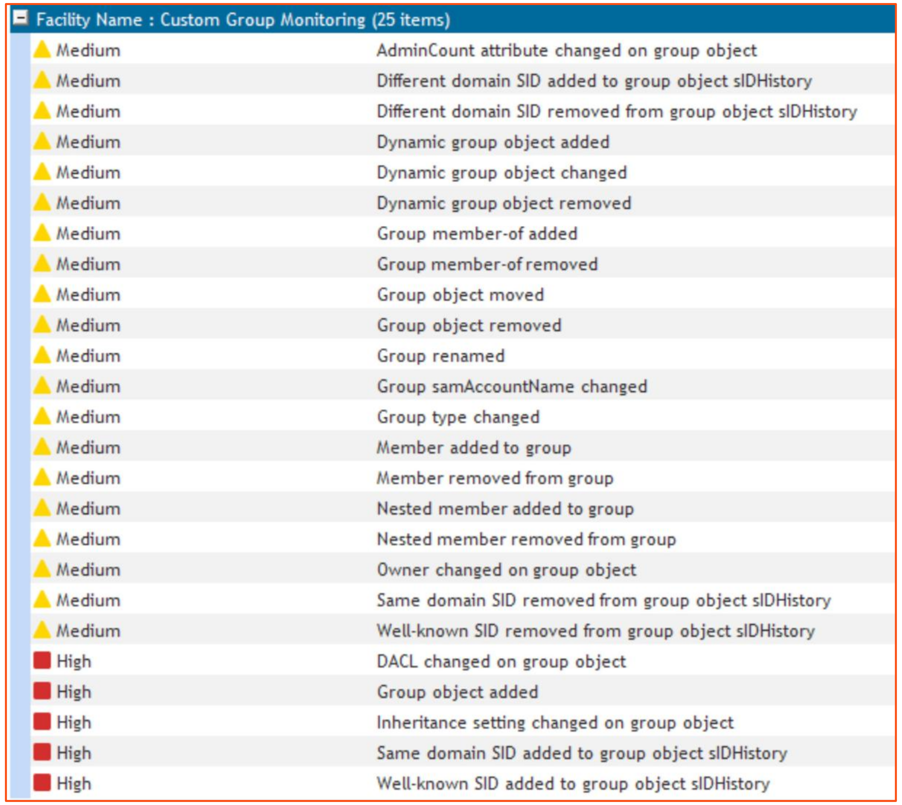
Template	Status	Override Accounts	Objects	Override Account Filter
ISL - Protect an attribute	● Enabled	● Excluded from Protect...		
Khairi	● Enabled	● Excluded from Protect...		

Object Canonical	Status	Object Class	Operations	Scope
Click here to filter data...				
titancorp.local/Quest Team OU/Khairi/GAdmins	● Enabled	organizationalUnit	Create, Delete, Modify Attributes	This object and all child objects

Attribute Protection

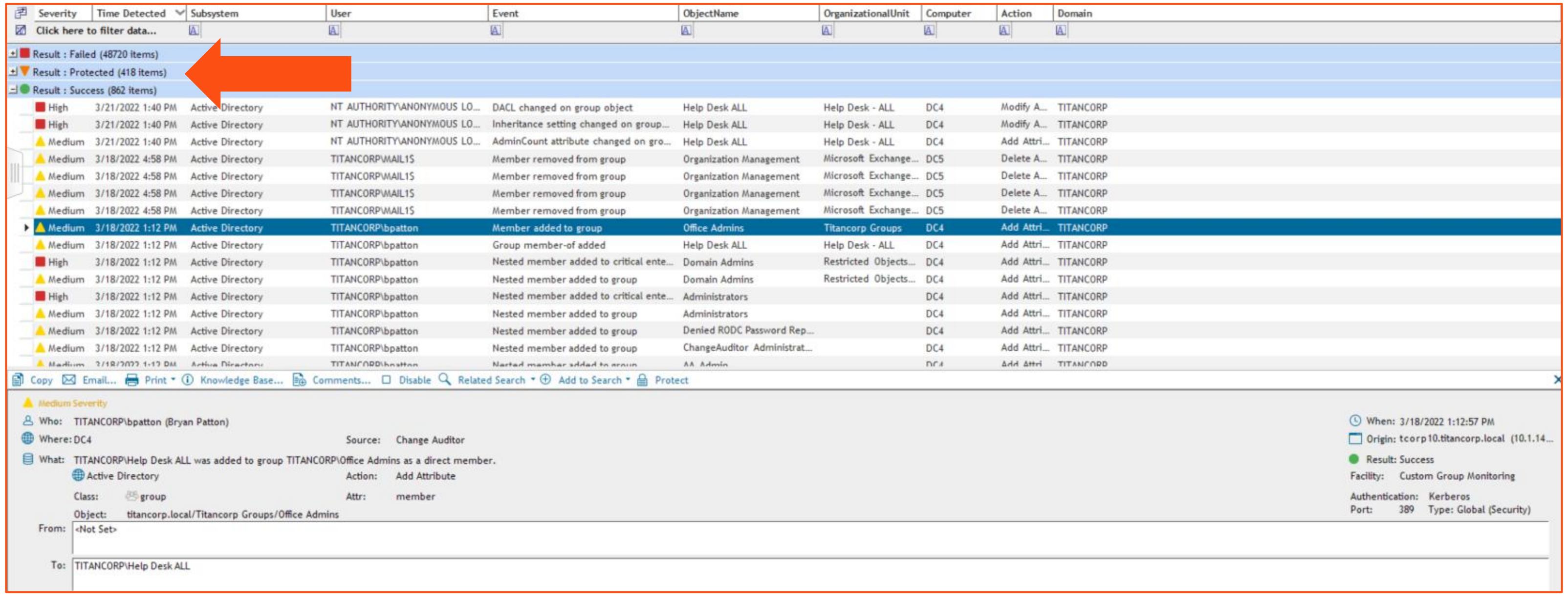
Click here to filter data

Privileged Groups (Events & Built-In searches)



Facility Name : Custom Group Monitoring (25 items)

⚠ Medium	AdminCount attribute changed on group object
⚠ Medium	Different domain SID added to group object sIDHistory
⚠ Medium	Different domain SID removed from group object sIDHistory
⚠ Medium	Dynamic group object added
⚠ Medium	Dynamic group object changed
⚠ Medium	Dynamic group object removed
⚠ Medium	Group member-of added
⚠ Medium	Group member-of removed
⚠ Medium	Group object moved
⚠ Medium	Group object removed
⚠ Medium	Group renamed
⚠ Medium	Group samAccountName changed
⚠ Medium	Group type changed
⚠ Medium	Member added to group
⚠ Medium	Member removed from group
⚠ Medium	Nested member added to group
⚠ Medium	Nested member removed from group
⚠ Medium	Owner changed on group object
⚠ Medium	Same domain SID removed from group object sIDHistory
⚠ Medium	Well-known SID removed from group object sIDHistory
🟥 High	DACL changed on group object
🟥 High	Group object added
🟥 High	Inheritance setting changed on group object
🟥 High	Same domain SID added to group object sIDHistory
🟥 High	Well-known SID added to group object sIDHistory



Result : Failed (48720 items)

Result : Protected (418 items)

Result : Success (862 items)

Severity	Time Detected	Subsystem	User	Event	ObjectName	OrganizationalUnit	Computer	Action	Domain
🟥 High	3/21/2022 1:40 PM	Active Directory	NT AUTHORITY\ANONYMOUS LO...	DACL changed on group object	Help Desk ALL	Help Desk - ALL	DC4	Modify A...	TITANCORP
🟥 High	3/21/2022 1:40 PM	Active Directory	NT AUTHORITY\ANONYMOUS LO...	Inheritance setting changed on group...	Help Desk ALL	Help Desk - ALL	DC4	Modify A...	TITANCORP
⚠ Medium	3/21/2022 1:40 PM	Active Directory	NT AUTHORITY\ANONYMOUS LO...	AdminCount attribute changed on gro...	Help Desk ALL	Help Desk - ALL	DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 4:58 PM	Active Directory	TITANCORP\MAIL1$	Member removed from group	Organization Management	Microsoft Exchange...	DC5	Delete A...	TITANCORP
⚠ Medium	3/18/2022 4:58 PM	Active Directory	TITANCORP\MAIL1$	Member removed from group	Organization Management	Microsoft Exchange...	DC5	Delete A...	TITANCORP
⚠ Medium	3/18/2022 4:58 PM	Active Directory	TITANCORP\MAIL1$	Member removed from group	Organization Management	Microsoft Exchange...	DC5	Delete A...	TITANCORP
⚠ Medium	3/18/2022 4:58 PM	Active Directory	TITANCORP\MAIL1$	Member removed from group	Organization Management	Microsoft Exchange...	DC5	Delete A...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Member added to group	Office Admins	Titancorp Groups	DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Group member-of added	Help Desk ALL	Help Desk - ALL	DC4	Add Attri...	TITANCORP
🟥 High	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to critical ente...	Domain Admins	Restricted Objects...	DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to group	Domain Admins	Restricted Objects...	DC4	Add Attri...	TITANCORP
🟥 High	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to critical ente...	Administrators		DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to group	Administrators		DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to group	Denied RODC Password Rep...		DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to group	ChangeAuditor Administrat...		DC4	Add Attri...	TITANCORP
⚠ Medium	3/18/2022 1:12 PM	Active Directory	TITANCORP\bpatton	Nested member added to group	AA Admin		DC4	Add Attri	TITANCORP

⚠ Medium Severity

Who: TITANCORP\bpatton (Bryan Patton)

Where: DC4

Source: Change Auditor

What: TITANCORP\Help Desk ALL was added to group TITANCORP\Office Admins as a direct member.

Active Directory

Action: Add Attribute

Class: group

Attr: member

Object: titancorp.local/Titancorp Groups/Office Admins

From: <Not Set>

To: TITANCORP\Help Desk ALL

When: 3/18/2022 1:12:57 PM

Origin: tcorp10.titancorp.local (10.1.14...

● Result: Success

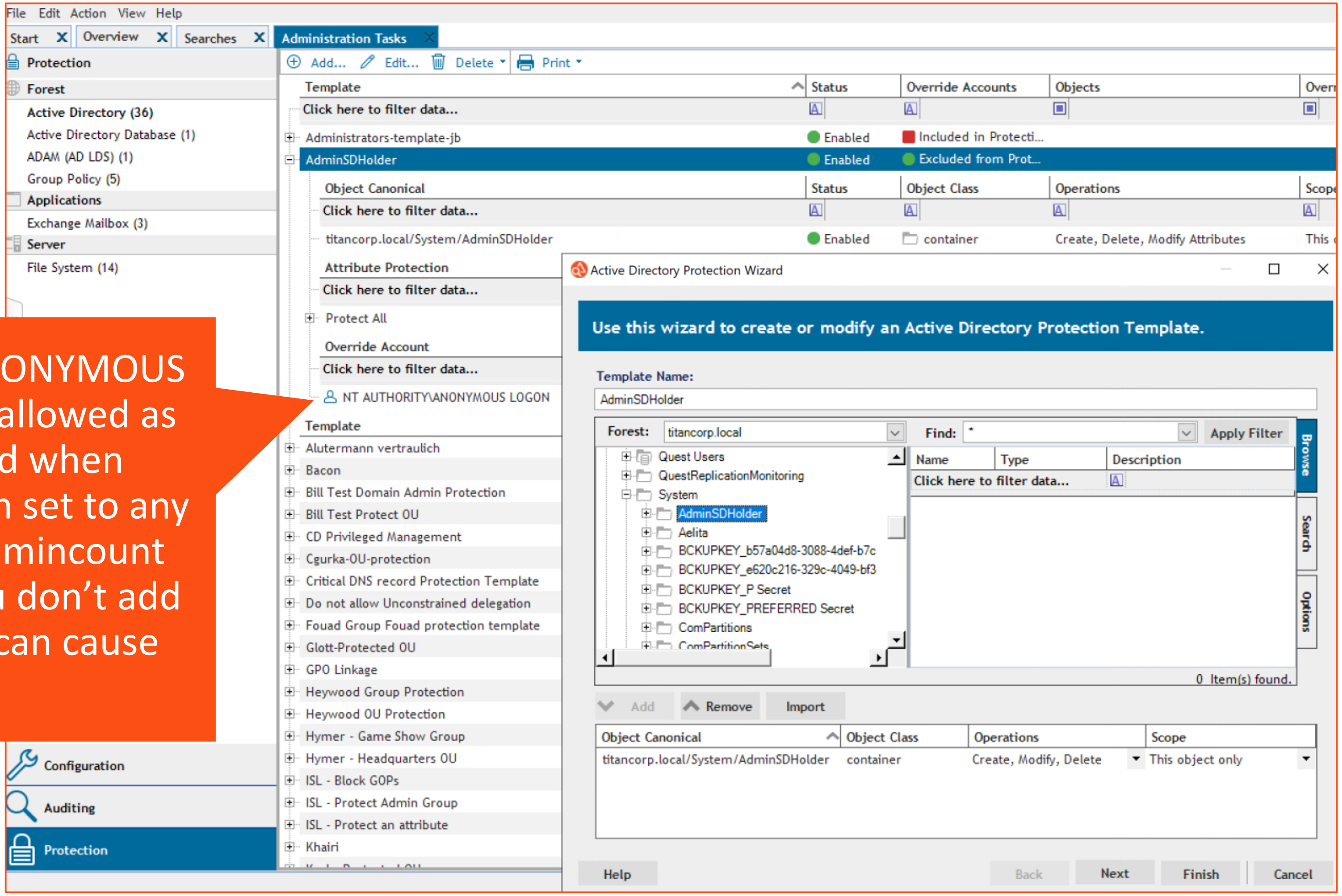
Facility: Custom Group Monitoring

Authentication: Kerberos

Port: 389 Type: Global (Security)

Protect AdminSDHolder

The ACL of the AdminSDHolder object is used as a template to copy permissions to all “protected groups” in Active Directory and their members. If an attacker can manipulate the ACL for AdminSDHolder, then those permissions will automatically be applied to all protected objects. This will give an attacker a way to create **persistent access to privileged accounts within the domain**.



Template	Status	Override Accounts	Objects	Overr
Click here to filter data...				
Administrators-template-jb	● Enabled	🟥 Included in Protecti...		
AdminSDHolder	● Enabled	● Excluded from Prot...		

Object Canonical	Status	Object Class	Operations	Scope
Click here to filter data...				
titancorp.local/System/AdminSDHolder	● Enabled	container	Create, Delete, Modify Attributes	This

Attribute Protection

Click here to filter data...

Protect All

Override Account

Click here to filter data...

NT AUTHORITY\ANONYMOUS LOGON

Template
- Alutermann vertraulich
- Bacon
- Bill Test Domain Admin Protection
- Bill Test Protect OU
- CD Privileged Management
- Cgurka-OU-protection
- Critical DNS record Protection Template
- Do not allow Unconstrained delegation
- Fouad Group Fouad protection template
- Glott-Protected OU
- GPO Linkage
- Heywood Group Protection
- Heywood OU Protection
- Hymer - Game Show Group
- Hymer - Headquarters OU
- ISL - Block GOPs
- ISL - Protect Admin Group
- ISL - Protect an attribute
- Khairi

Active Directory Protection Wizard

Use this wizard to create or modify an Active Directory Protection Template.

Template Name: AdminSDHolder

Forest: titancorp.local

Find: *

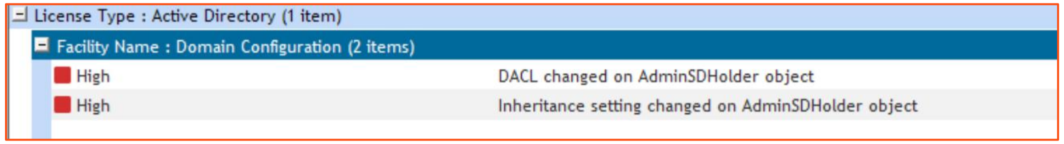
0 Item(s) found.

Object Canonical	Object Class	Operations	Scope
titancorp.local/System/AdminSDHolder	container	Create, Modify, Delete	This object only

NT AUTHORITY\ANONYMOUS LOGON should be allowed as that will be used when applying permission set to any object that has admincount attribute =1. If you don't add this exception, it can cause errors

Where Next Meets Now.

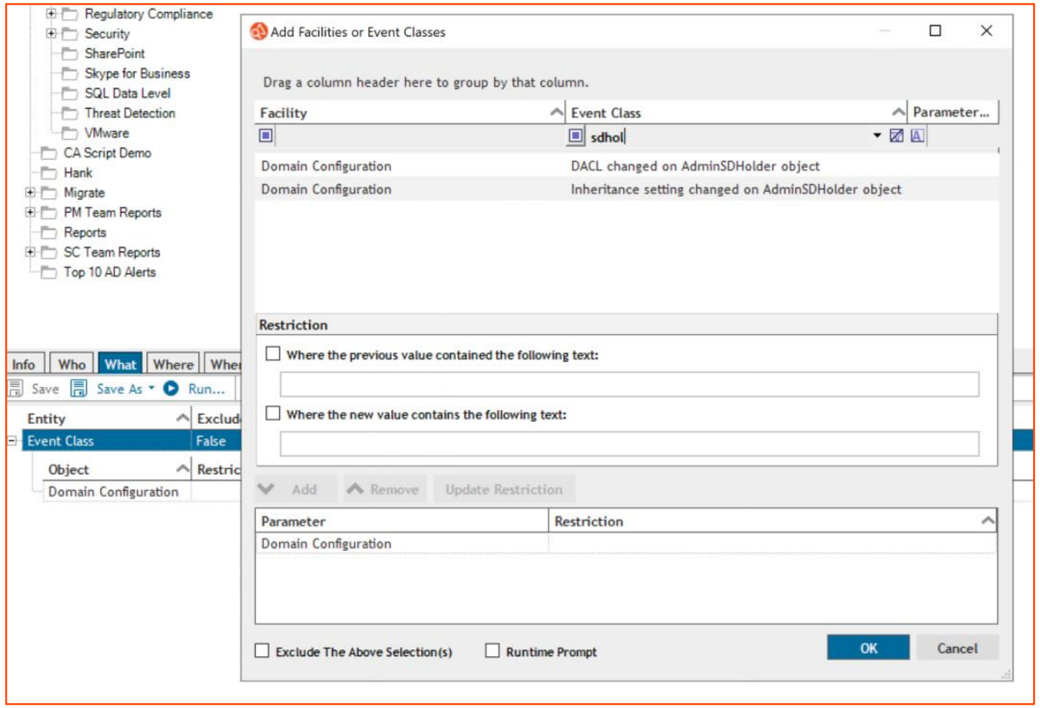
AdminSDHolder (Events / Searches)



License Type : Active Directory (1 item)

Facility Name : Domain Configuration (2 items)

🟥 High	DACL changed on AdminSDHolder object
🟥 High	Inheritance setting changed on AdminSDHolder object



Entity	Exclude
Event Class	False

Object	Restriction
Domain Configuration	

Facility	Event Class	Parameter...
	sdhol	
Domain Configuration	DACL changed on AdminSDHolder object	
Domain Configuration	Inheritance setting changed on AdminSDHolder object	

☐ Where the previous value contained the following text:

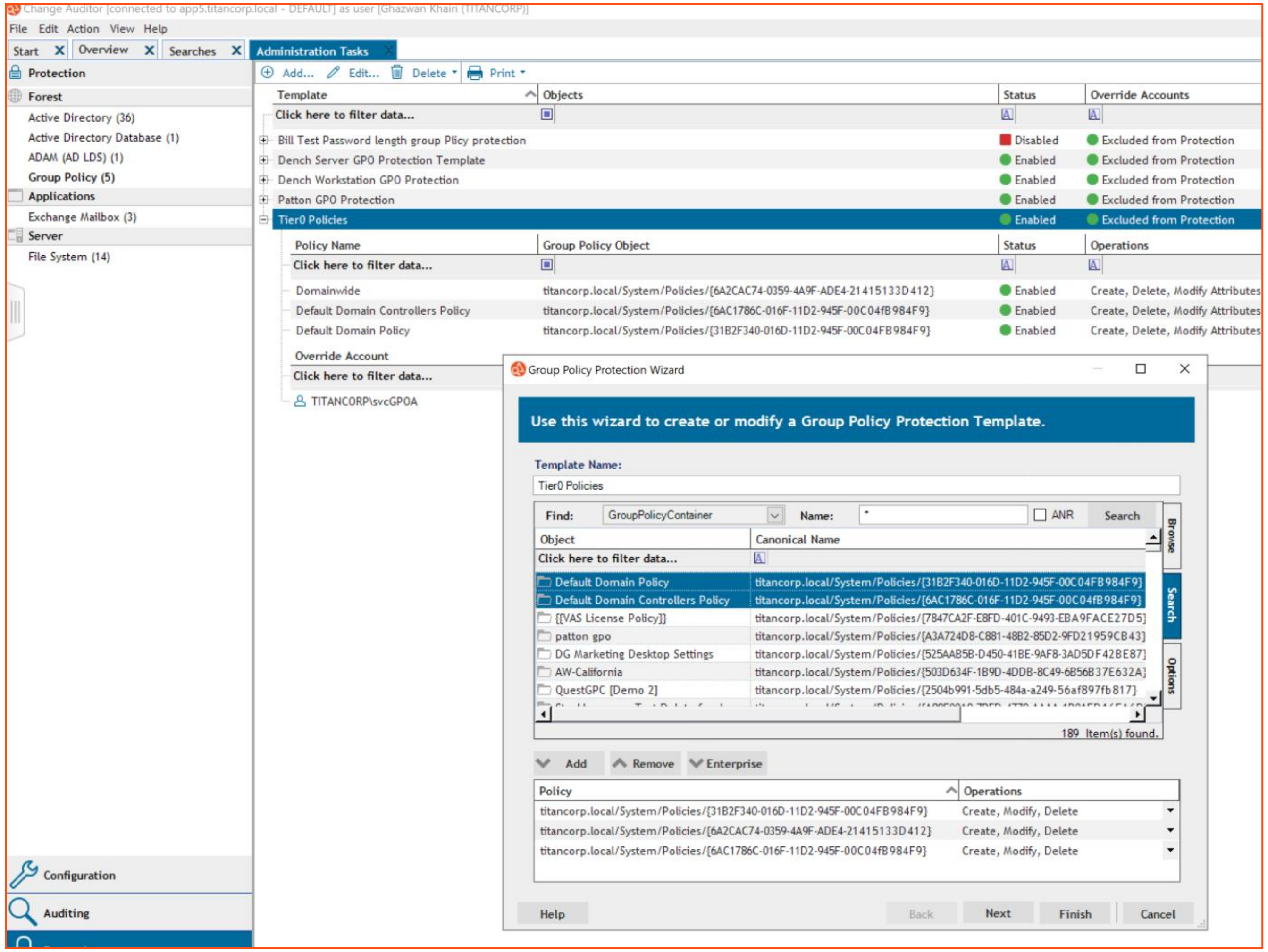
☐ Where the new value contains the following text:

Parameter	Restriction
Domain Configuration	

☐ Exclude The Above Selection(s) ☐ Runtime Prompt

Protect GPOs

A change to the default domain policy or default domain controllers’ policy can affect every person in an organization and should be protected. Ideally, a workflow would be configured using a product like GPOADmin and its service account can be excluded from the protection. If no GPO version control system in place, these policies should be protected to prevent company wide changes.



Change Auditor [connected to app5.titancorp.local - DEFAULT] as user [Ghazwan Khairi (TITANCORP)]

Template	Objects	Status	Override Accounts
Click here to filter data...			
Bill Test Password length group Plicy protection		🟥 Disabled	● Excluded from Protection
Dench Server GPO Protection Template		● Enabled	● Excluded from Protection
Dench Workstation GPO Protection		● Enabled	● Excluded from Protection
Patton GPO Protection		● Enabled	● Excluded from Protection
Tier0 Policies		● Enabled	● Excluded from Protection

Policy Name	Group Policy Object	Status	Operations
Click here to filter data...			
Domainwide	titancorp.local/System/Policies/{6A2CAC74-0359-4A9F-ADE4-21415133D412}	● Enabled	Create, Delete, Modify Attributes
Default Domain Controllers Policy	titancorp.local/System/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}	● Enabled	Create, Delete, Modify Attributes
Default Domain Policy	titancorp.local/System/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}	● Enabled	Create, Delete, Modify Attributes

Override Account
Click here to filter data...
TITANCORP\svcGPOA

Group Policy Protection Wizard

Use this wizard to create or modify a Group Policy Protection Template.

Template Name: Tier0 Policies

Find: GroupPolicyContainer Name: * □ ANR Search

Object	Canonical Name
Click here to filter data...	
Default Domain Policy	titancorp.local/System/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}
Default Domain Controllers Policy	titancorp.local/System/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}
{[VAS License Policy]}	titancorp.local/System/Policies/{7847CA2F-E8FD-401C-9493-EBA9FACE27D5}
patton gpo	titancorp.local/System/Policies/{A3A724D8-C881-48B2-85D2-9FD21959CB43}
DG Marketing Desktop Settings	titancorp.local/System/Policies/{525AAB5B-D450-41BE-9AF8-3AD5DF42BE87}
AW-California	titancorp.local/System/Policies/{503D634F-1B9D-4DDB-8C49-6B56B37E632A}
QuestGPC [Demo 2]	titancorp.local/System/Policies/{2504b991-5db5-484a-a249-56af897fb817}

189 Item(s) found.

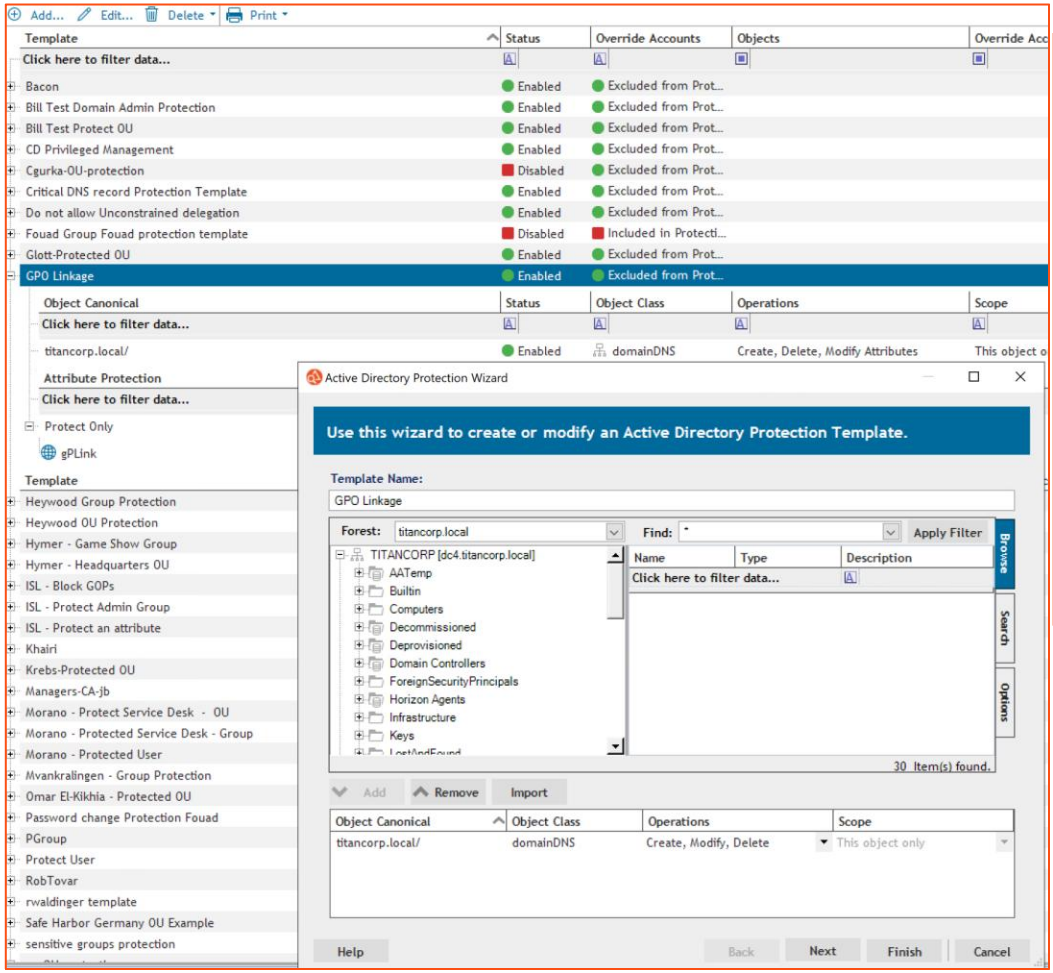
Policy	Operations
titancorp.local/System/Policies/{31B2F340-016D-11D2-945F-00C04FB984F9}	Create, Modify, Delete
titancorp.local/System/Policies/{6A2CAC74-0359-4A9F-ADE4-21415133D412}	Create, Modify, Delete
titancorp.local/System/Policies/{6AC1786C-016F-11D2-945F-00C04fB984F9}	Create, Modify, Delete

Quest

Where Next Meets Now.

Protect GPO Linkage

A GPO linked at the Domain level can potentially harm your organization! It is recommended to restrict the linkage of any GPO at the Domain level and if required should be done with multiple levels of approvals. If using GPOAdmin and/or AGPM it is recommended to add their service accounts to the access for the protection template



Template	Status	Override Accounts	Objects	Override Acc
Click here to filter data...				
Bacon	● Enabled	● Excluded from Prot...		
Bill Test Domain Admin Protection	● Enabled	● Excluded from Prot...		
Bill Test Protect OU	● Enabled	● Excluded from Prot...		
CD Privileged Management	● Enabled	● Excluded from Prot...		
Cgurka-OU-protection	■ Disabled	● Excluded from Prot...		
Critical DNS record Protection Template	● Enabled	● Excluded from Prot...		
Do not allow Unconstrained delegation	● Enabled	● Excluded from Prot...		
Fouad Group Fouad protection template	■ Disabled	■ Included in Protecti...		
Glott-Protected OU	● Enabled	● Excluded from Prot...		
GPO Linkage	● Enabled	● Excluded from Prot...		

Object Canonical	Status	Object Class	Operations	Scope
Click here to filter data...				
titancorp.local/	● Enabled	domainDNS	Create, Delete, Modify Attributes	This object o

Attribute Protection

Click here to filter data...

Protect Only

gPLink

Template

- Heywood Group Protection
- Heywood OU Protection
- Hymer - Game Show Group
- Hymer - Headquarters OU
- ISL - Block GOPs
- ISL - Protect Admin Group
- ISL - Protect an attribute
- Khairi
- Krebs-Protected OU
- Managers-CA-jb
- Morano - Protect Service Desk - OU
- Morano - Protected Service Desk - Group
- Morano - Protected User
- Mvankralingen - Group Protection
- Omar El-Kikhia - Protected OU
- Password change Protection Fouad
- PGroup
- Protect User
- RobTovar
- rwaldinger template
- Safe Harbor Germany OU Example
- sensitive groups protection

Active Directory Protection Wizard

Use this wizard to create or modify an Active Directory Protection Template.

Template Name: GPO Linkage

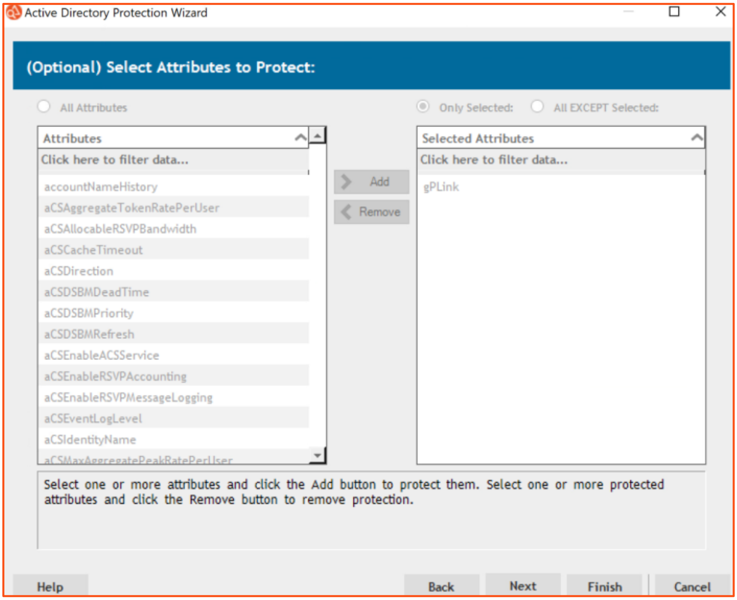
Forest: titancorp.local Find: * Apply Filter

- TITANCORP [dc4.titancorp.local]
  - AATemp
  - Builtin
  - Computers
  - Decommissioned
  - Deprovisioned
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Horizon Agents
  - Infrastructure
  - Keys
  - LostAndFound

Name	Type	Description
Click here to filter data...		

30 Item(s) found.

Object Canonical	Object Class	Operations	Scope
titancorp.local/	domainDNS	Create, Modify, Delete	This object only


Active Directory Protection Wizard

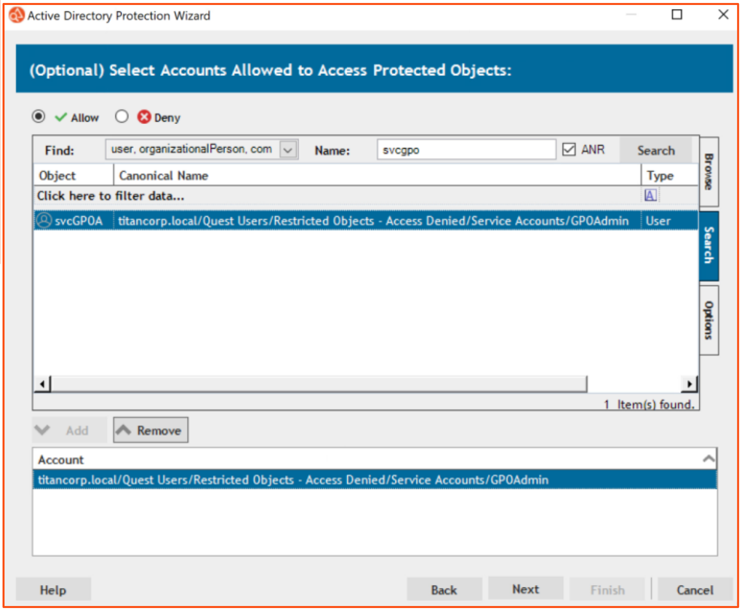
(Optional) Select Attributes to Protect:

○ All Attributes ● Only Selected: ○ All EXCEPT Selected:

Attributes
Click here to filter data...
accountNameHistory
aCSAggregateTokenRatePerUser
aCSAllocableRSVPBandwidth
aCSCacheTimeout
aCSDirection
aCSDSBMDeadTime
aCSDSBMPriority
aCSDSBMRefresh
aCSEnableACSService
aCSEnableRSVPAccounting
aCSEnableRSVPMessageLogging
aCSEventLogLevel
aCSIdentityName
aCSMaxAggregatePeakRatePerUser

Selected Attributes
Click here to filter data...
gPLink

Select one or more attributes and click the Add button to protect them. Select one or more protected attributes and click the Remove button to remove protection.


Active Directory Protection Wizard

(Optional) Select Accounts Allowed to Access Protected Objects:

● ✓ Allow ○ ✕ Deny

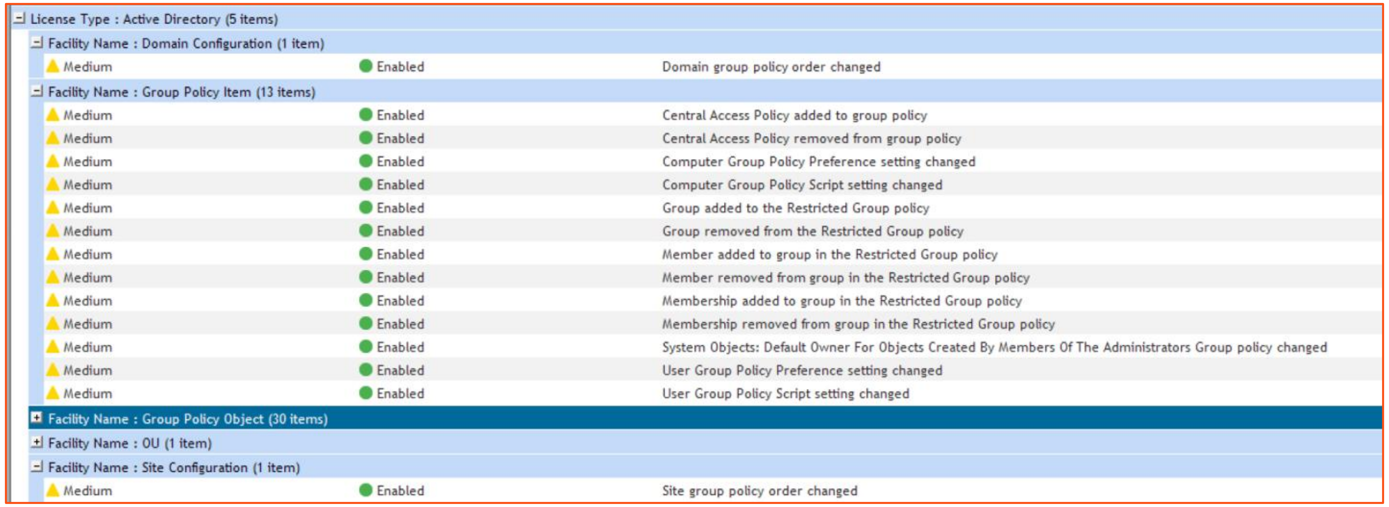
Find: user, organizationalPerson, com Name: svcgpo ☑ ANR Search

Object	Canonical Name	Type
Click here to filter data...		
svcGPOA	titancorp.local/Quest Users/Restricted Objects - Access Denied/Service Accounts/GPOAdmin	User

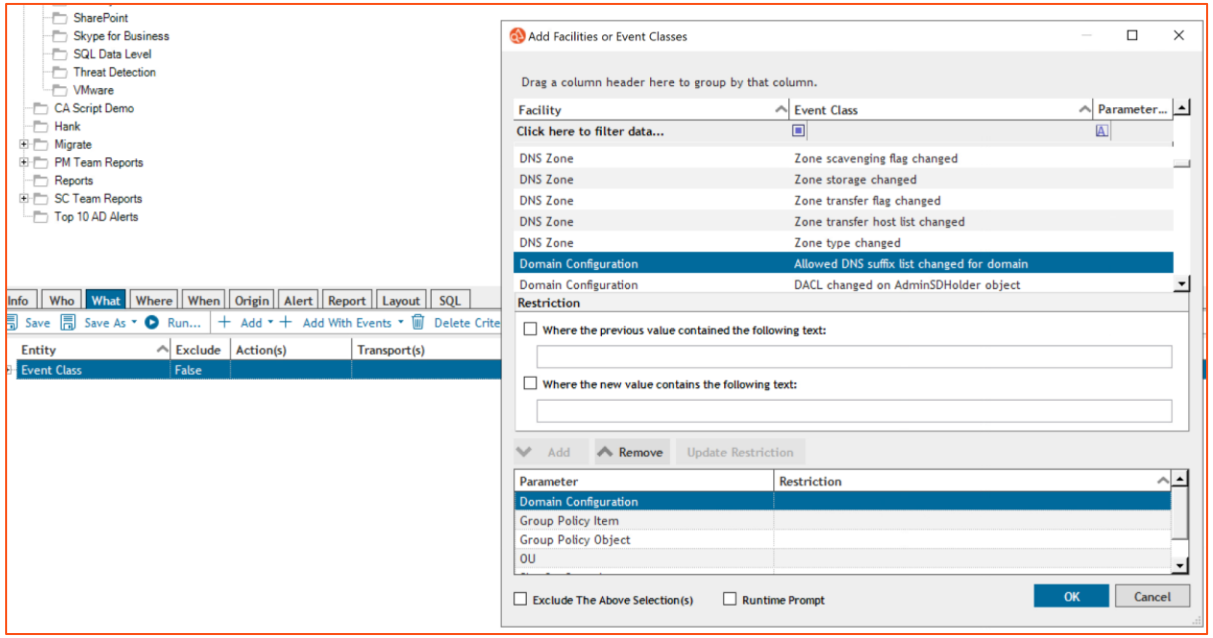
1 Item(s) found.

Account
titancorp.local/Quest Users/Restricted Objects - Access Denied/Service Accounts/GPOAdmin

GPOs (Events / Searches)



License Type : Active Directory (5 items)		
Facility Name : Domain Configuration (1 item)		
Medium	Enabled	Domain group policy order changed
Facility Name : Group Policy Item (13 items)		
Medium	Enabled	Central Access Policy added to group policy
Medium	Enabled	Central Access Policy removed from group policy
Medium	Enabled	Computer Group Policy Preference setting changed
Medium	Enabled	Computer Group Policy Script setting changed
Medium	Enabled	Group added to the Restricted Group policy
Medium	Enabled	Group removed from the Restricted Group policy
Medium	Enabled	Member added to group in the Restricted Group policy
Medium	Enabled	Member removed from group in the Restricted Group policy
Medium	Enabled	Membership added to group in the Restricted Group policy
Medium	Enabled	Membership removed from group in the Restricted Group policy
Medium	Enabled	System Objects: Default Owner For Objects Created By Members Of The Administrators Group policy changed
Medium	Enabled	User Group Policy Preference setting changed
Medium	Enabled	User Group Policy Script setting changed
Facility Name : Group Policy Object (30 items)		
Facility Name : OU (1 item)		
Facility Name : Site Configuration (1 item)		
Medium	Enabled	Site group policy order changed



Entity	Exclude	Action(s)	Transport(s)
Event Class	False		

Add Facilities or Event Classes

Drag a column header here to group by that column.

Facility	Event Class	Parameter...
Click here to filter data...		
DNS Zone	Zone scavenging flag changed	
DNS Zone	Zone storage changed	
DNS Zone	Zone transfer flag changed	
DNS Zone	Zone transfer host list changed	
DNS Zone	Zone type changed	
Domain Configuration	Allowed DNS suffix list changed for domain	
Domain Configuration	DACL changed on AdminSDHolder object	

Restriction

☐ Where the previous value contained the following text:

☐ Where the new value contains the following text:

Parameter	Restriction
Domain Configuration	
Group Policy Item	
Group Policy Object	
OU	

☐ Exclude The Above Selection(s)   ☐ Runtime Prompt