Hands-on experience with SAP Enterprise Threat Detection, cloud edition

Exercise: Working with SAP Enterprise Threat Detection Version

Based on SAP Enterprise Threat Detection, cloud edition, Version November 2025

Get Hands-On with the New *SAP Enterprise Threat Detection, cloud edition*

Contents

Overview & Touring SAP Enterprise Threat Detection, public cloud

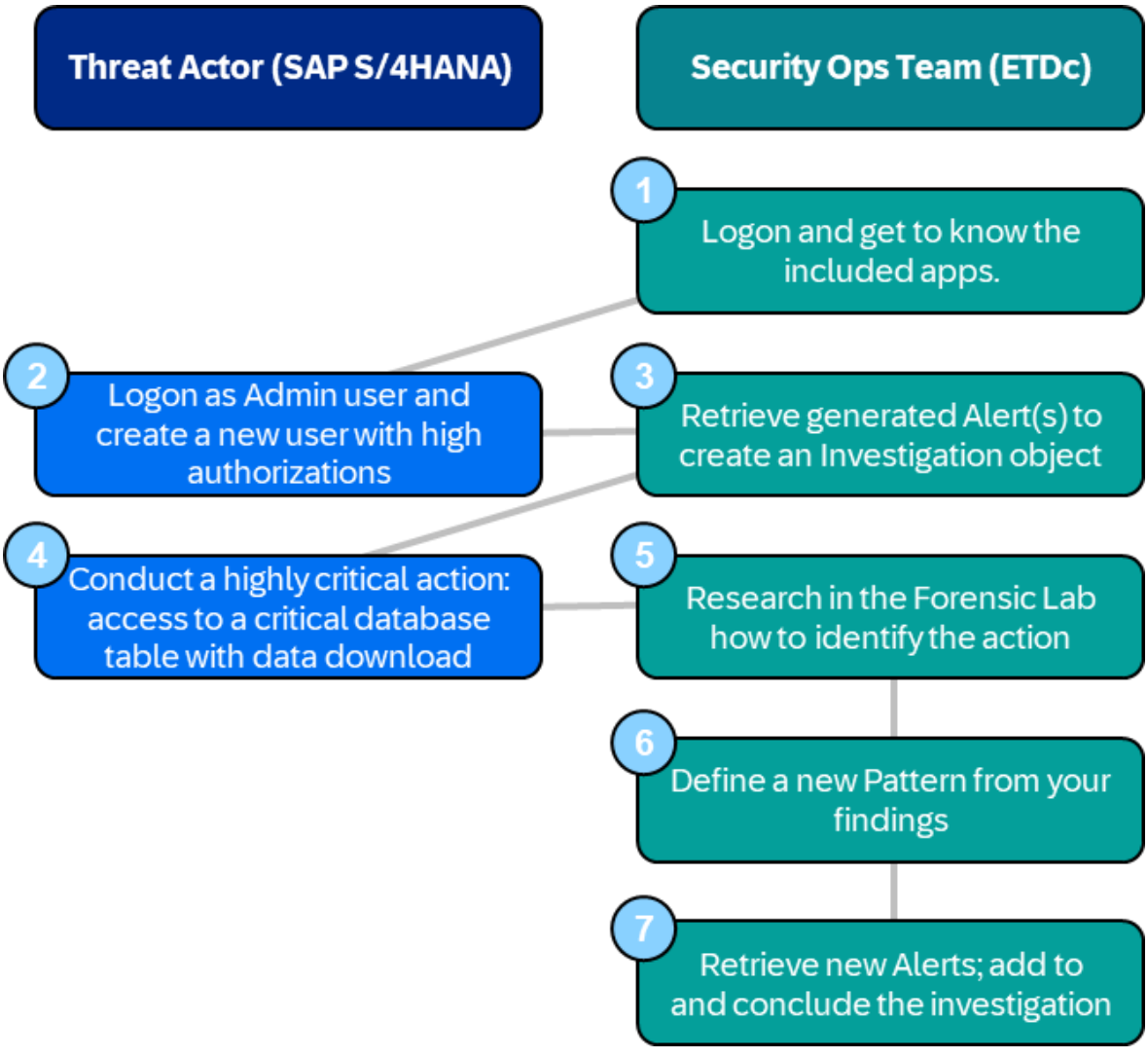
In this hands-on session and workshop of about 1.5 – 2h, you will get to know the basic functioning of *SAP Enterprise Threat Detection, public cloud*, including the terminology employed.

You will switch back and forth between 3 roles. In a first role, you will be a (potential) threat actor in an SAP S/4HANA system and conduct actions resulting in system responses in *SAP Enterprise Threat Detection, public cloud*.

In a second role, you will act as a security specialist in charge to identify potential threats, pin down what has happened and determine the relevance, as well as ensure that the knowledge about the attack vector is added to the repository on which *SAP Enterprise Threat Detection, public cloud* will automatically alert going forward.

In a 3rd role, you will act as a consumer/processor of the results (Investigation Report), that was created by you in your second role as a security specialist.

Here's the flow of the following exercises in your roles as threat actor and security specialist (the numbers relate to the chapters in this document:



Chapters 1 to 7 are related to these to roles. Chapter 8 is related to the consumer/processor role

1. Logon to the Monitoring Console of SAP Enterprise Threat Detection, public cloud

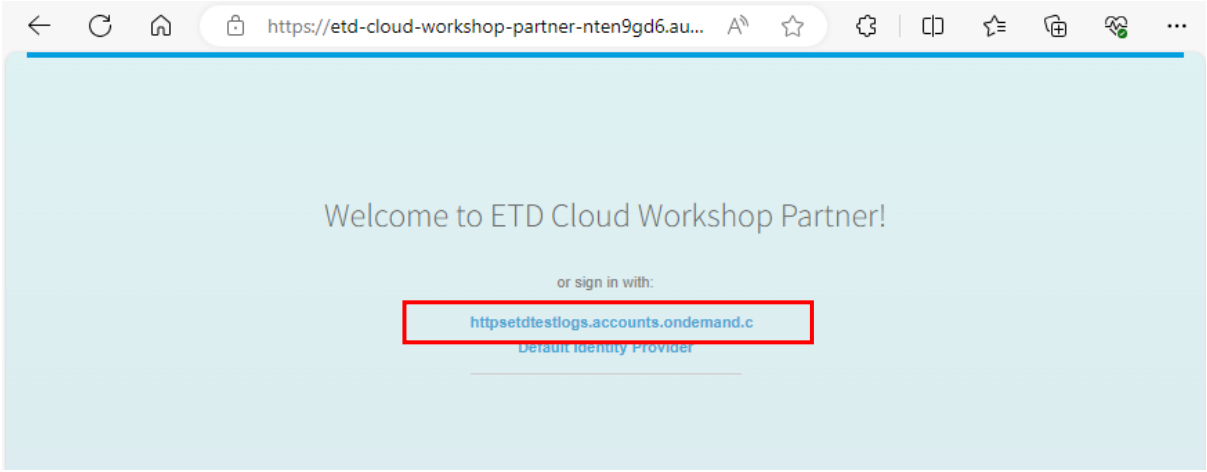
This system & credentials are available during the planned workshop hours only.

Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

Access the *SAP Enterprise Threat Detection, public cloud* monitoring console

IMPORTANT:

- You should get the below start page (if not, please empty your browser cache and try again).
- Here, select the first entry ("httpsetdtestlogs.accounts.ondemand") to log on with the generic workshop users below (not any personal credentials – they won't be recognized in this cloud application).
  Do **NOT** choose the "Default Identity Provider" (here, the generic users won't work).



In the ensuing (logon) screen, use the ID indicated to you (01-35; afterwards referred to as "##").

User: teched##@etdsap.com

Password: will be provided in the session

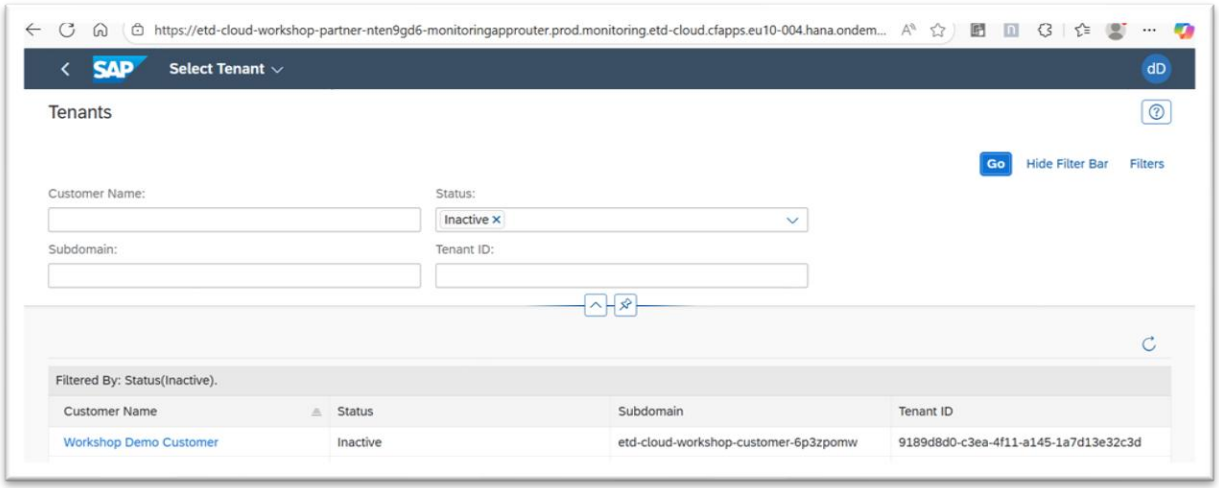
If you inadvertently lock the password, please notify the instructor.

If you receive a blank screen saying "Where to", please clear the cache, then close and restart the browser. If you may also open an private browsing window (often "incognito" or "InPrivate"). Log on again.

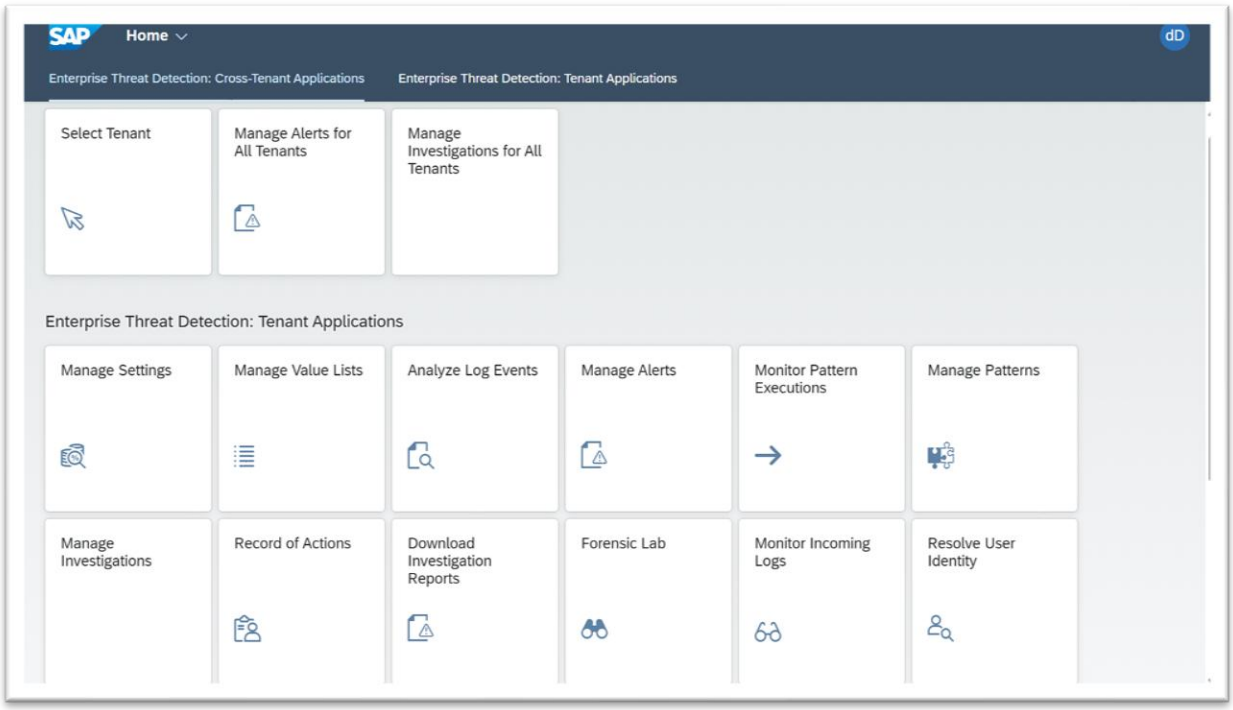
Upon initial logon, In case you get pop-up message to select a Tenant, than click the Select Tenant screen for selecting a specific Tenant:

As a monitoring agent providing services to multiple clients, you will log on to your organization's own productive Tenant; however from here commonly access and work in the specific Tenant of a client, which you can select from this list reflecting all clients/Tenants linked to your organization.

For this hands-on there is only one customer system linked. Click on the blue hyperlink and select "Workshop Demo Customer".

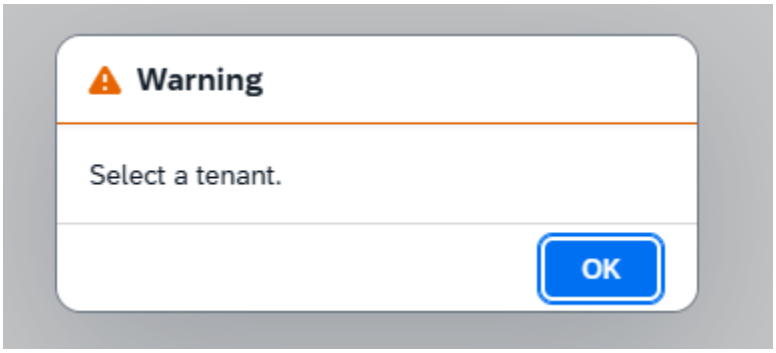


You will then see the *SAP Enterprise Threat Detection, public cloud* monitoring console. Take a bit of time to check by a few apps and how they behave.



1.1 Got a Warning ‘Select a Tenant’

If you encounter a the warning popup

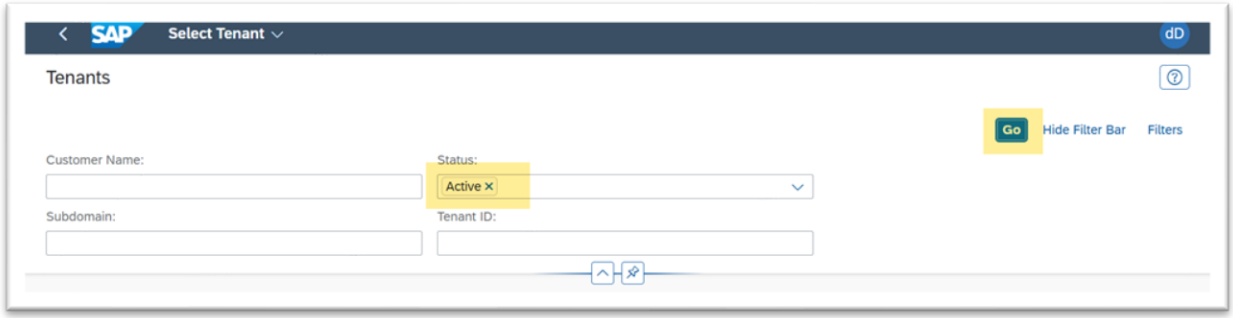


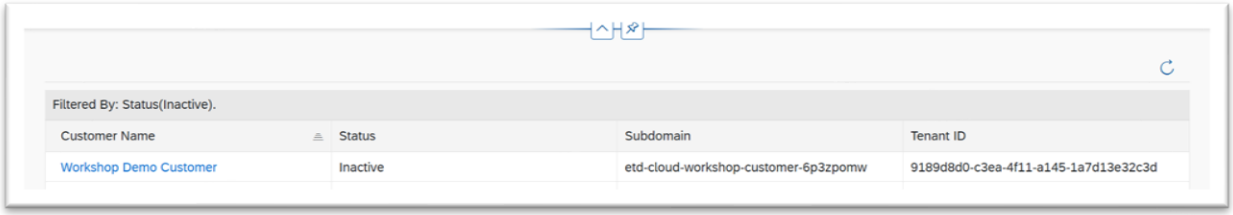
the system has lost the information which Tenant you’ve been working on (most likely you had been logged out).

In this case, either start the *SAP Enterprise Threat Detection, public cloud* console again via the above link.

Alternatively, you can manually set the correct tenant:

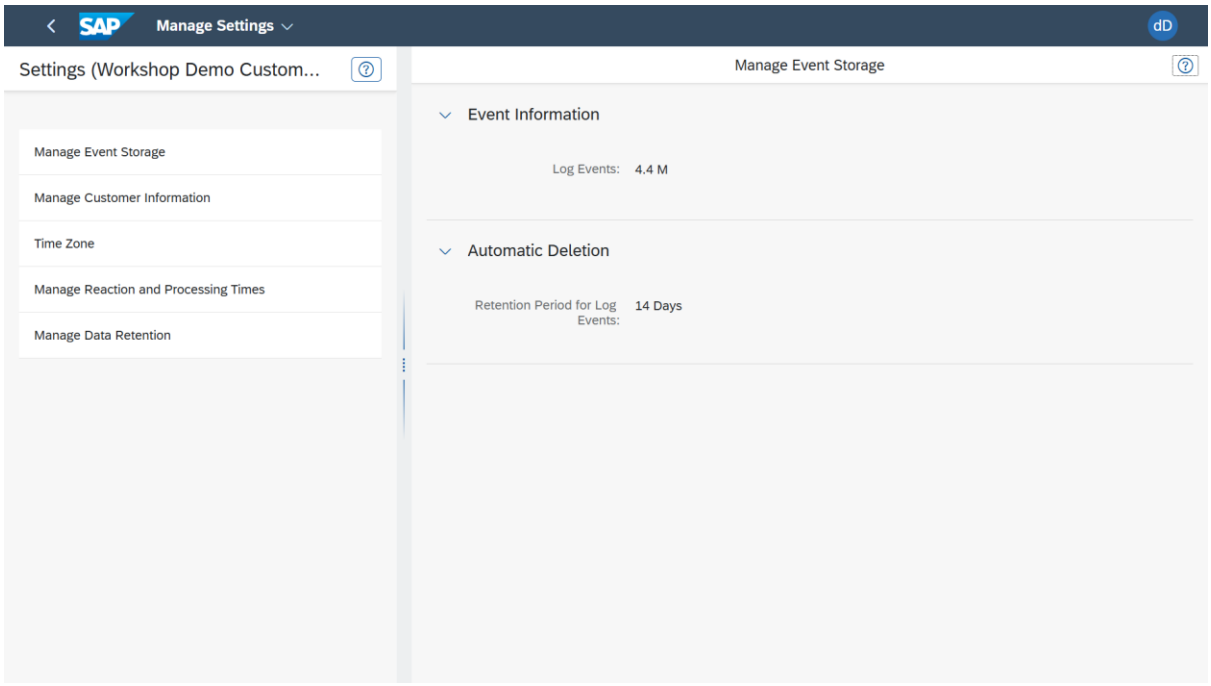
- In the section for “Cross-Tenant Applications”, open the app “Select Tenant”.
- Remove filters “active” and press “go”.
- The entry “Workshop Demo Customer” will show; select this so the system is aware which Tenant you are working on – which is relevant in case you’re a partner providing monitoring services to multiple clients)



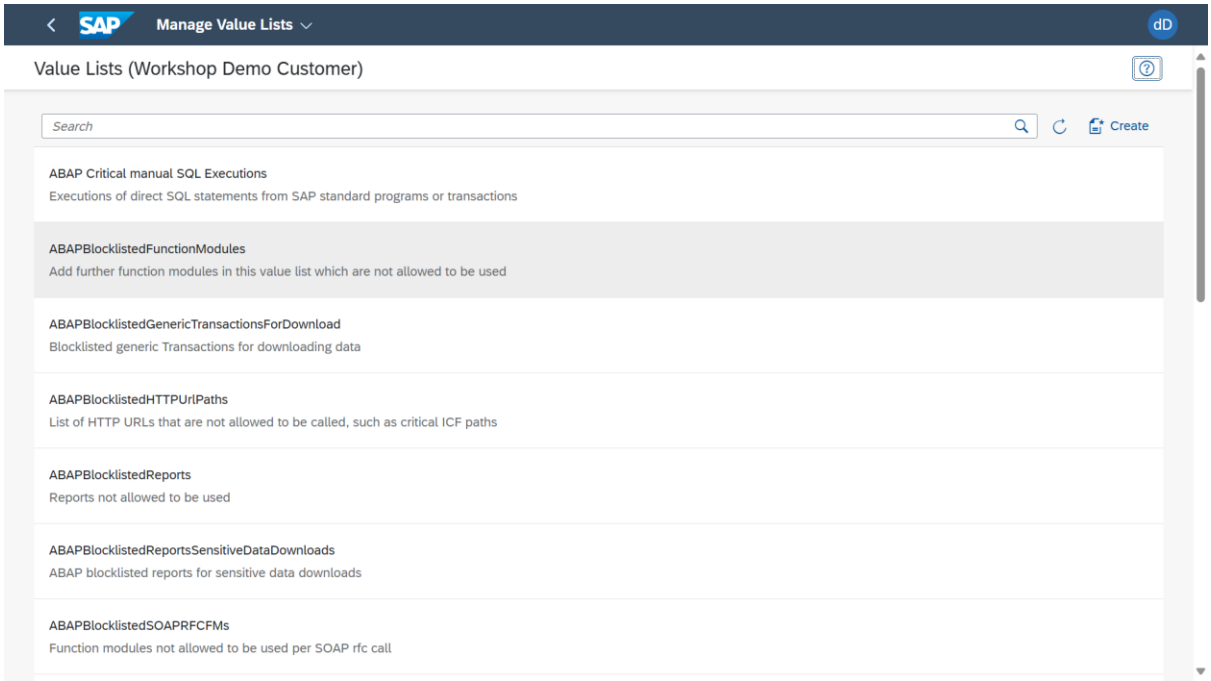


1.2 UI Round trip

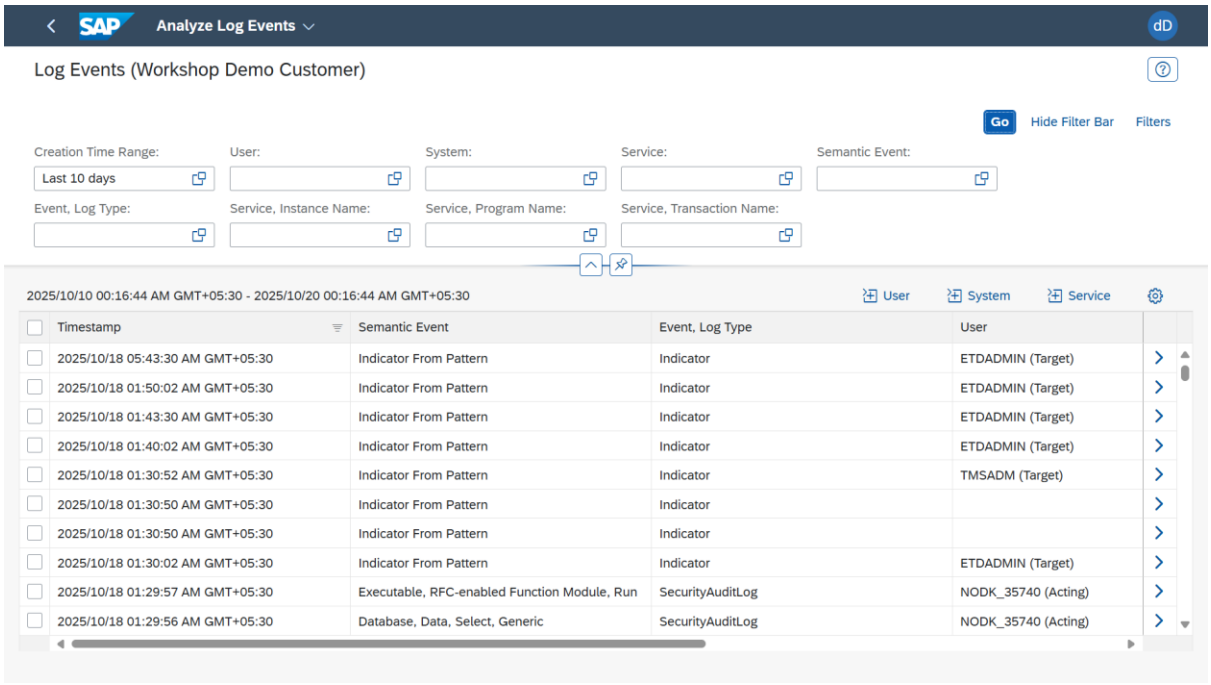
In Manage Setting tab, users can manage system setting like retention times and time zone etc.



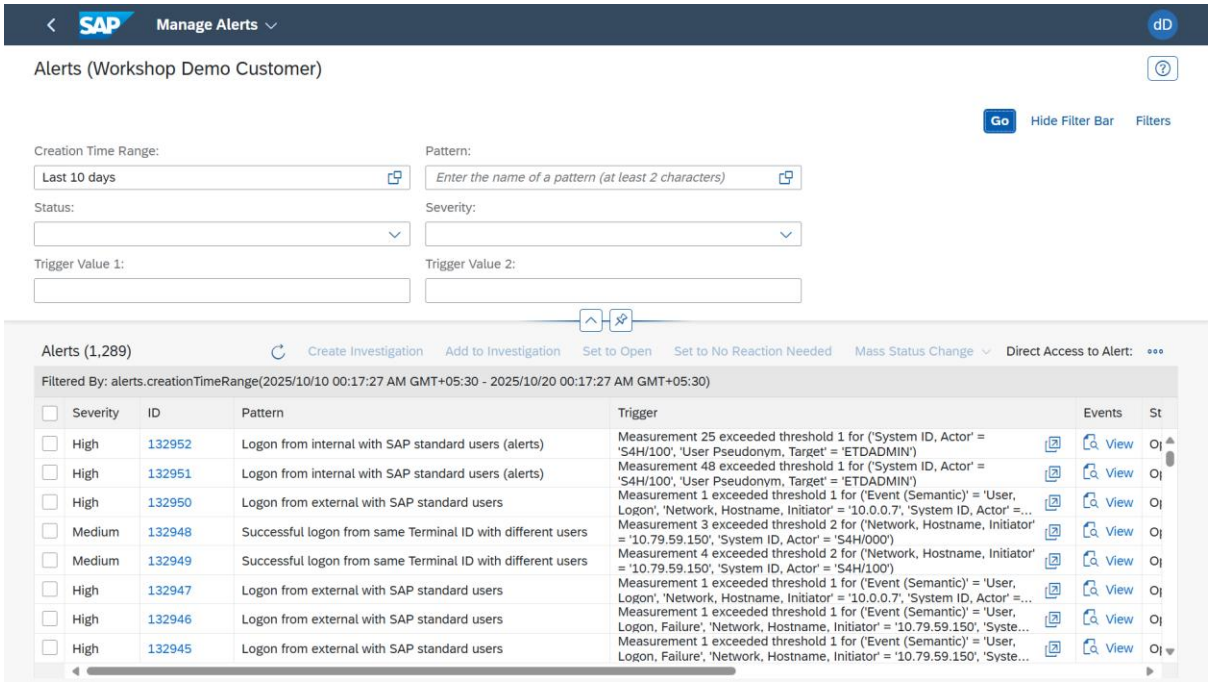
In Value list tab, users can manage value lists which are allow or disallow list where system analyst and put custom values and even can create custom value lists



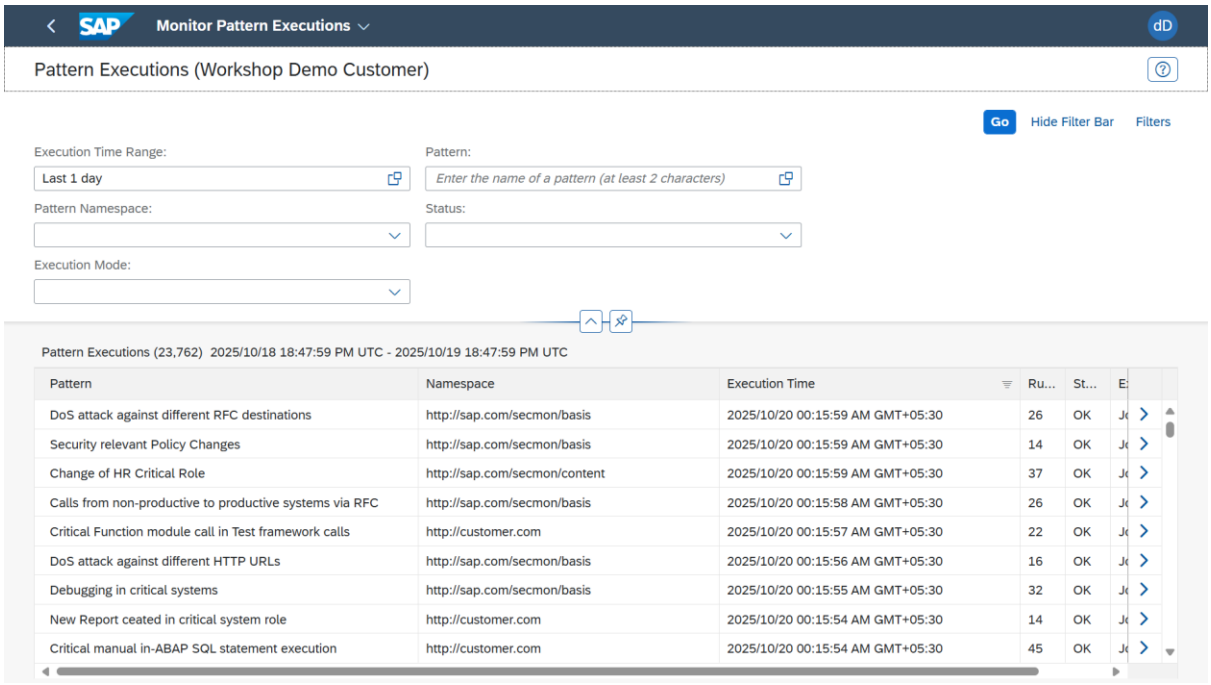
In Analyze Log Events tab, system analyst and view and analyze customers normalized log data.



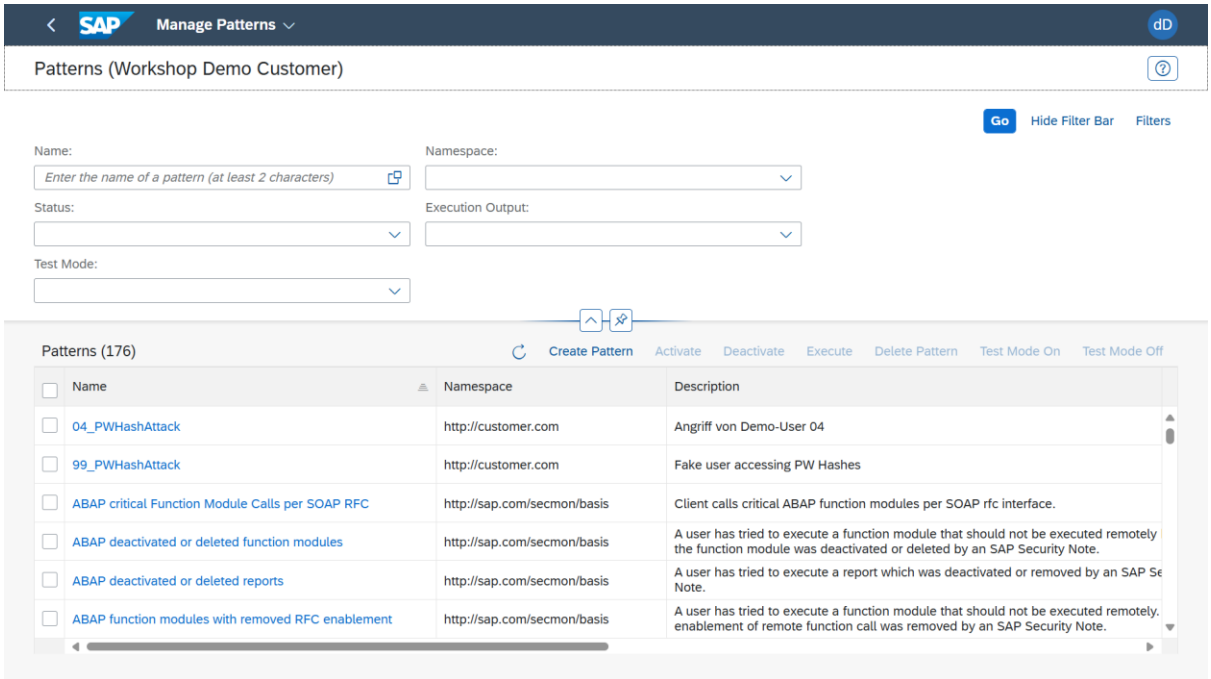
In Manage Alerts tab, system analyst and view and analyze generated alerts.



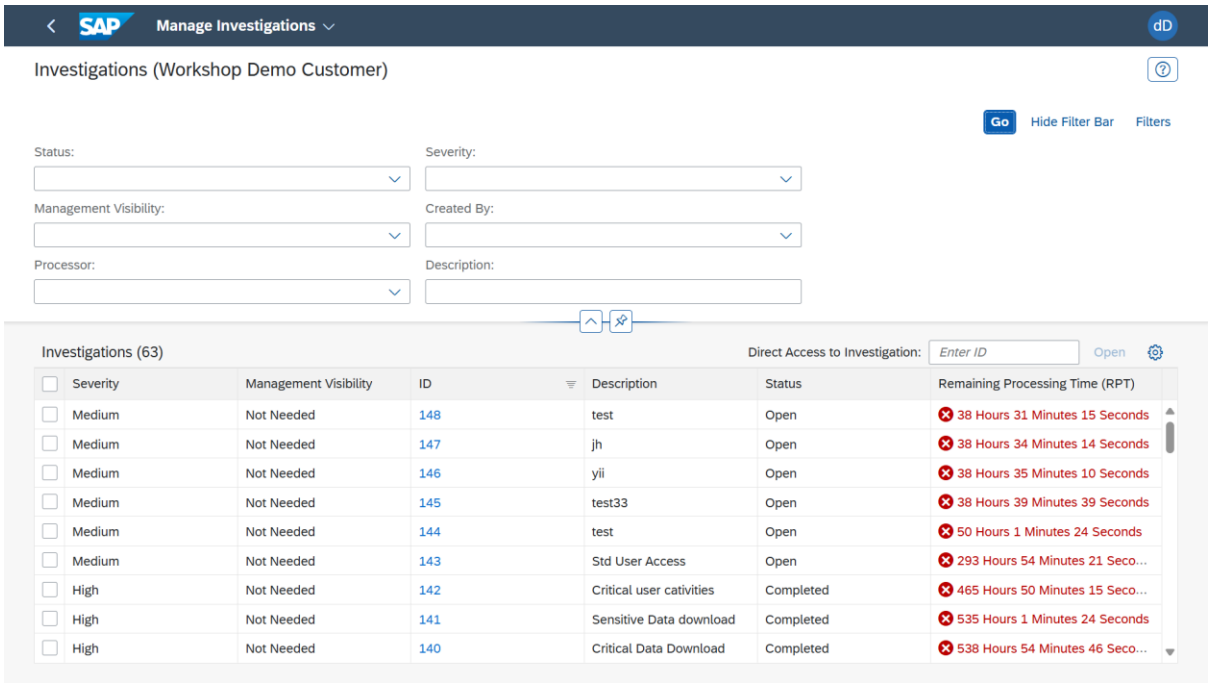
In Pattern Executions tab, system analyst and view and check status of pattern executions



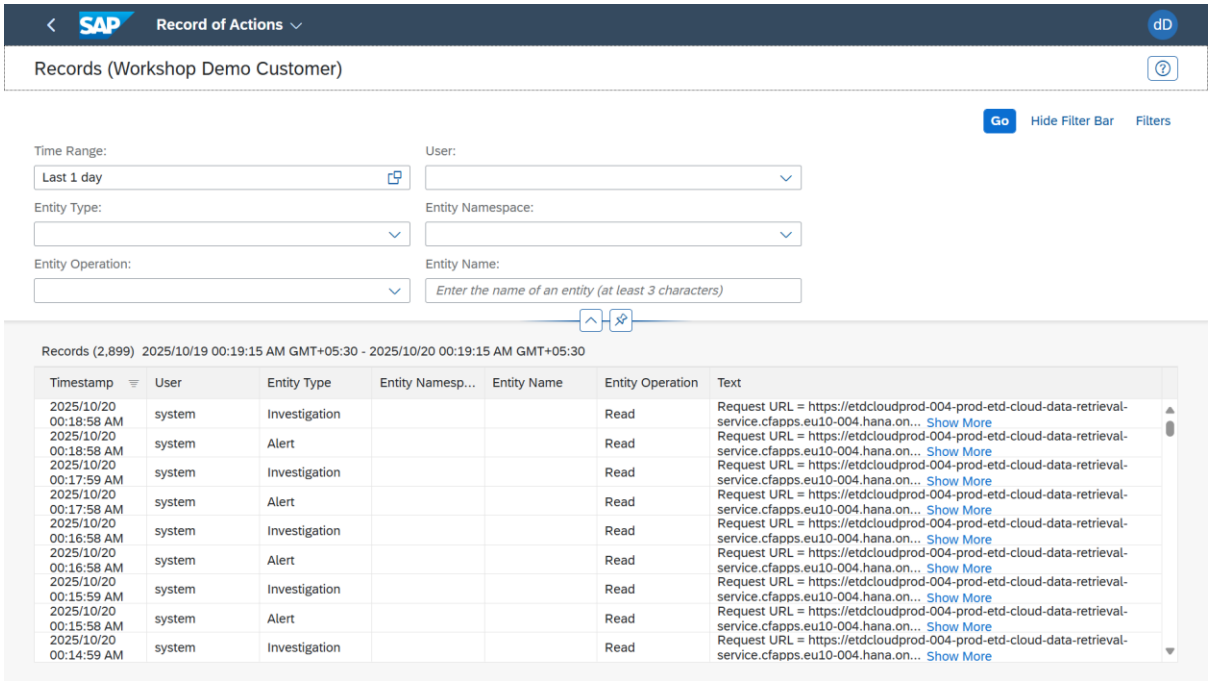
In Pattern tab, system analyst and view and create patterns(i.e. use cases)



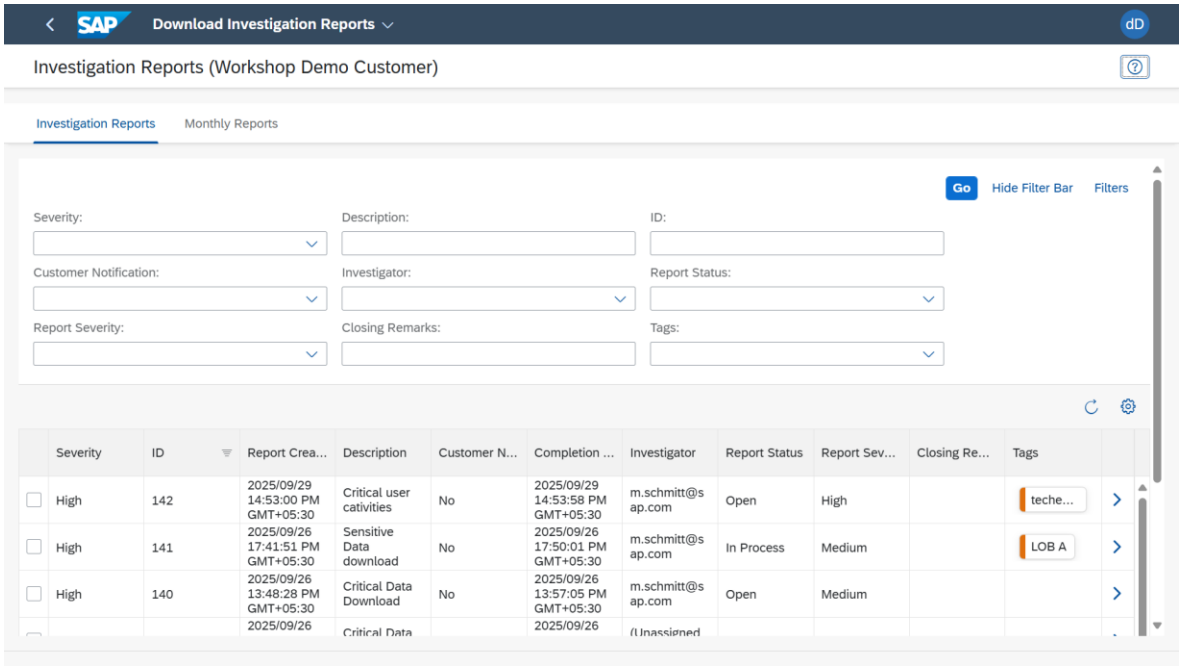
In Investigations tab, system analyst and view and manage investigations.



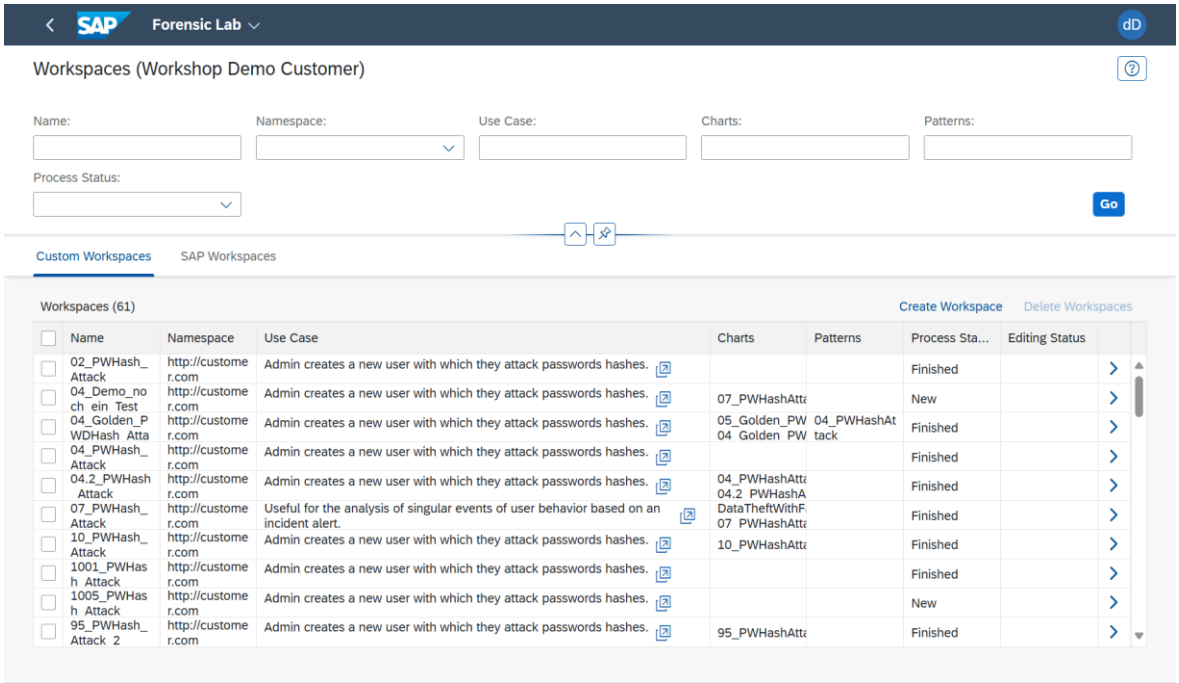
In Records tab, system analyst and view use activity logs of ETD system



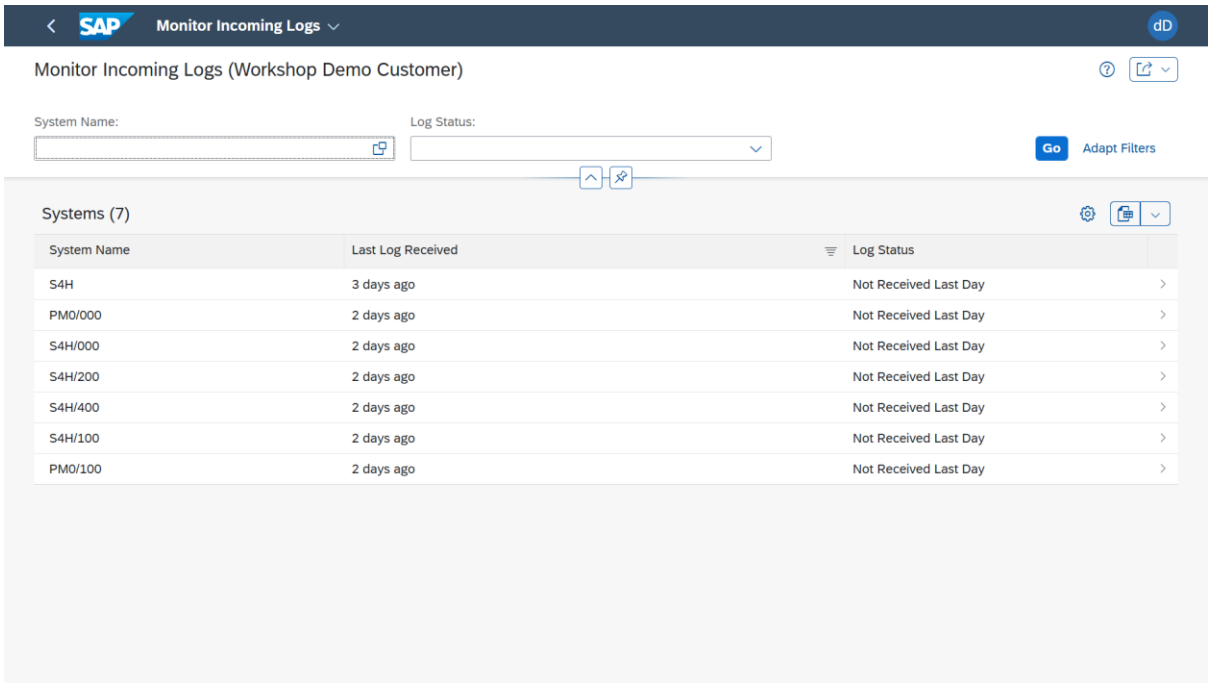
In Investigations Report tab, system analyst and view investigations



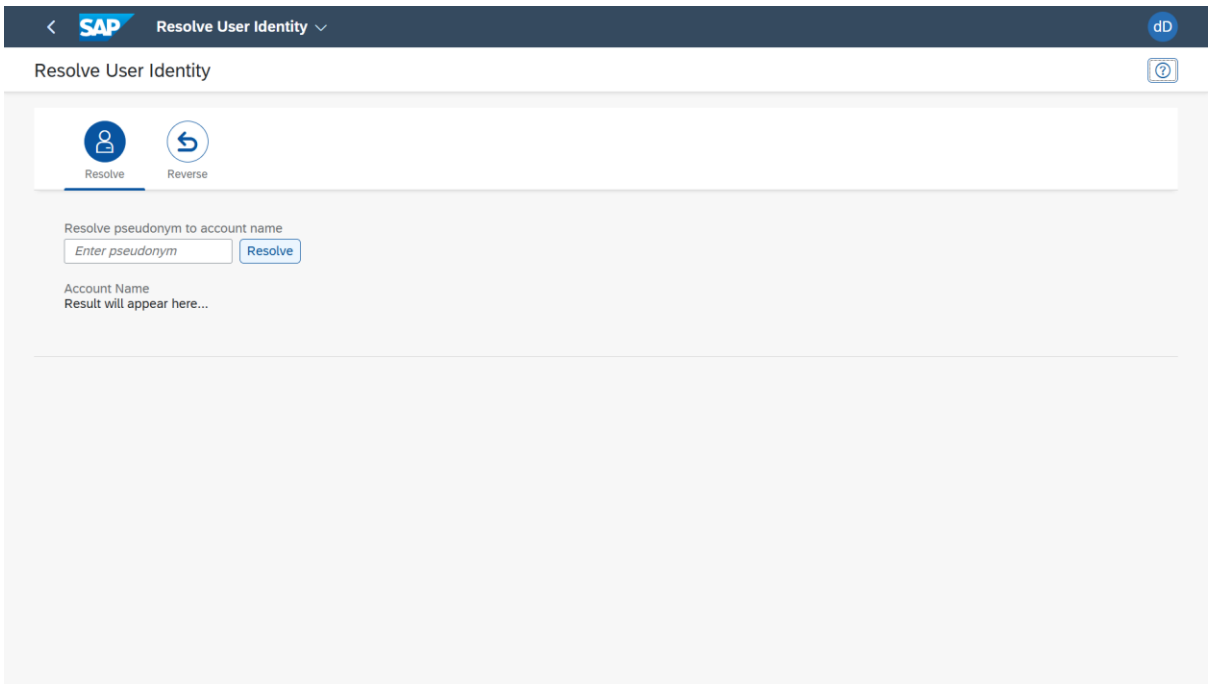
In Workspace tab, system analyst and view and create Workspace



In Manage Incoming logs tab, system analyst and view incoming logs



In Resolve user identity tab, system analyst and view and pseudonymize and pseudonymize user name



2. First Log Events from SAP S/4HANA

Please note: in this exercise, every workshop station/computer has a designated set of users already existing; throughout the description, "##" is the number of your workshop computer ID.

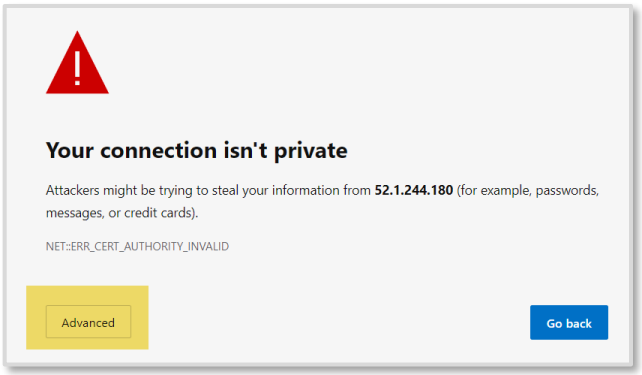
This system & credentials are available during the planned workshop hours only.

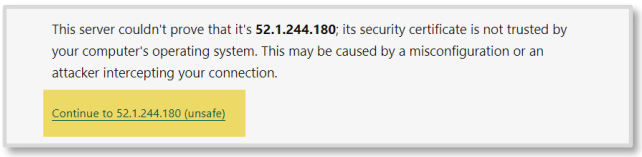
Please let the instructor know in case you'd like to have access afterwards; we're happy to check how long we can extend your access.

In this section, you will conduct actions in SAP GUI to generate Log Events which in return will result in Alerts in *SAP Enterprise Threat Detection, public cloud*.

2.1 Logon & Preparation Steps

- access the WebGUI interface: https://52.1.244.180:44301/sap/bc/gui/sap/its/webgui
- Proceed through the "advanced" mode in case you get a warning of unsafe/non-private connection – which might look like this:





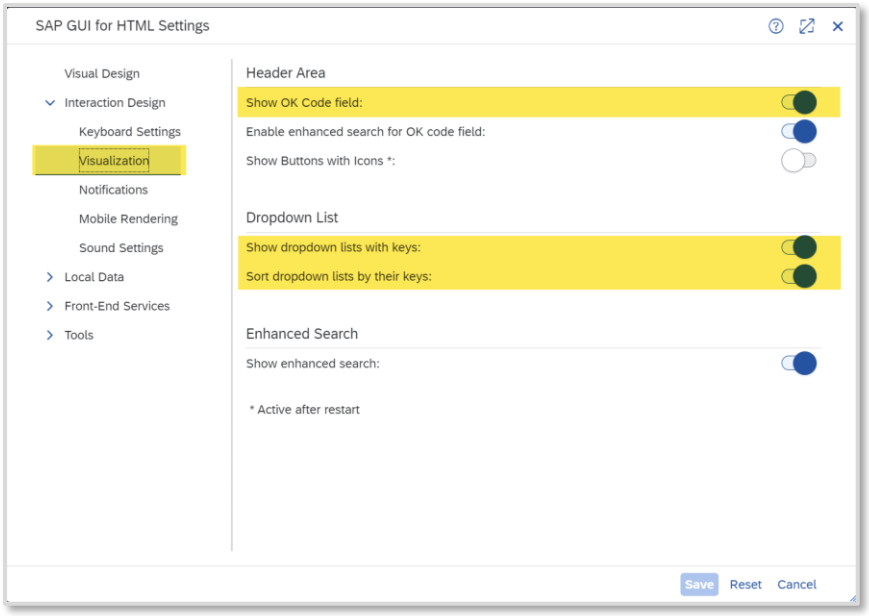
Log on credentials:

User: ETDADMIN##

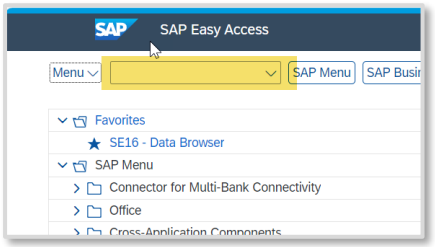
Password: Will be provided in the session

If you inadvertently lock the password, please notify the instructor.

- Activate the display of the "transaction code entry" field for easier navigation:
  Go to Menu → Settings → Visualization.
  Activate "Show OK Code field" as well as "Show dropdown lists with keys" and "Sort dropdown lists by their keys" and save.



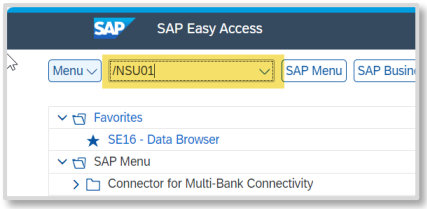
- Leave the menu. Your start screen should now show the transaction code entry field:



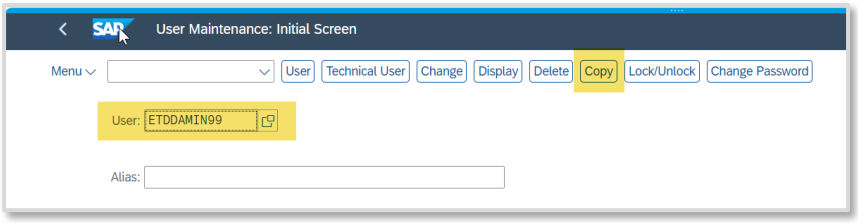
2.2 Creating a User With High Privileges

You will now conduct an action which triggers your first logs into *SAP Enterprise Threat Detection, public cloud:* creating a highly privileged user.

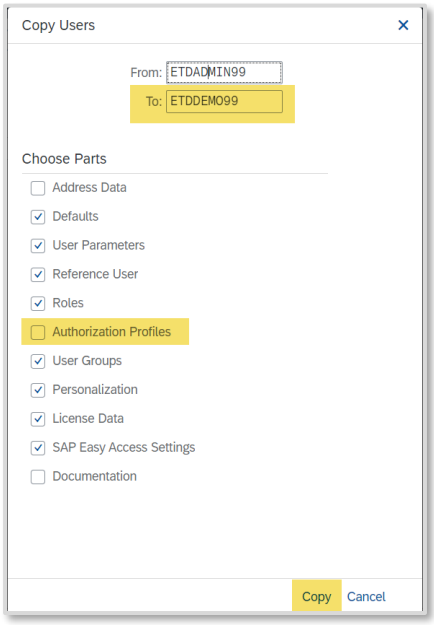
- In the transaction code entry, enter “SU01” (User Maintenance), and hit enter.



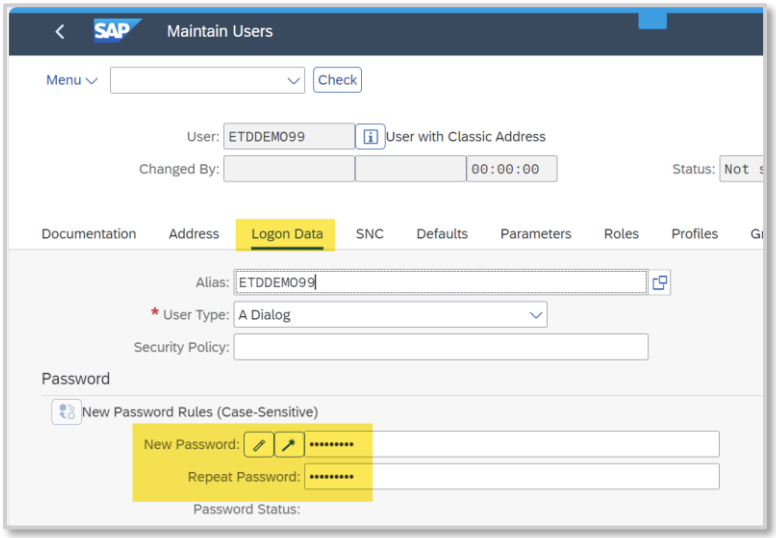
- In the User Maintenance transaction start screen, enter your user ETDADMIN## in the User field, and select “copy”.



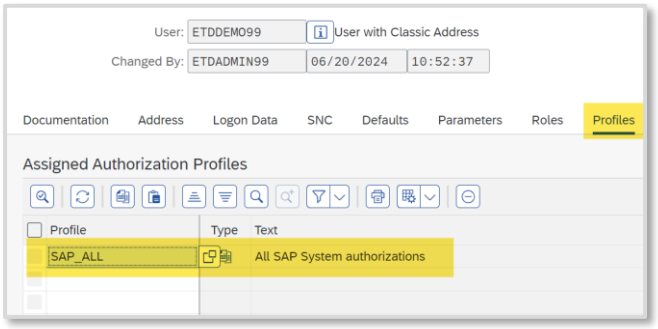
- In the pop up screen, maintain the new user name “ETDDEMO##” in the “To:” field; deselect the option to copy authorization profiles, and press “copy”:



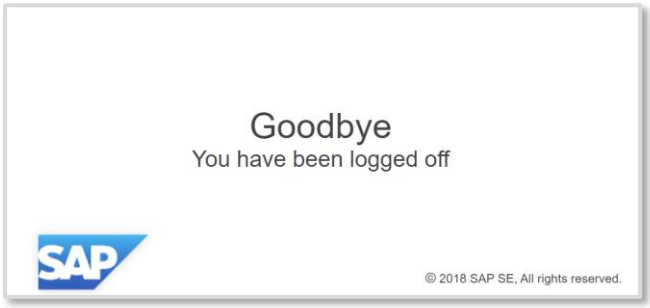
- In the resulting screen set, on tab “Logon Data”, assign an initial (temporary) password (it is suggested to note down this password as you will need this to log on with ETDDEMO##). Then save the user.



- Back in the SU01 initial screen, put in your user ETDDEMOxx and select the button “Change”. Move to the tab “Profiles”, add the profile “SAP_ALL” (making this user a super user basically without restrictions), and hit enter. Then press “Save”.



- This has been the first set of noteworthy actions. Exit the SAP Web GUI (button “Exit” in the top right; or hit Shift+F3; or in the transaction code entry field, type “/nex”).



3. Checking Alerts and Creating Investigations

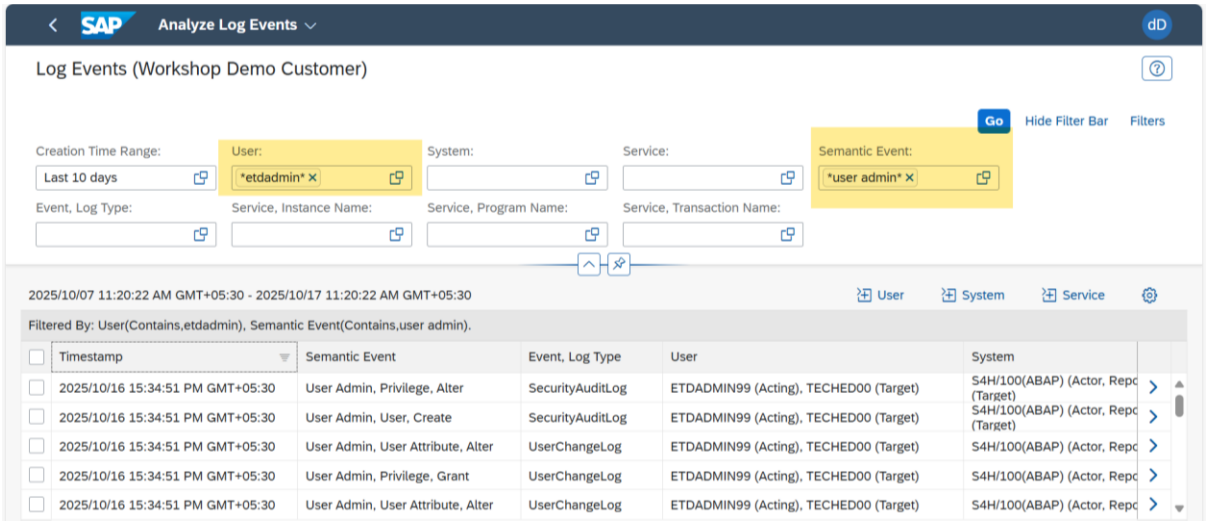
You will now look at alerts in *SAP Enterprise Threat Detection, public cloud* and create an Investigation object out of it.

Return to the *SAP Enterprise Threat Detection, public cloud* Monitoring Console. If necessary, log on again with your user techedxx@etdsap.com, and in the Select Tenant app, select the tenant “Workshop Demo Customer”.

If you receive the ‘Select a Tenant’ popup, refer to section 1.1 how to resolve.

3.1 Check for Log Events

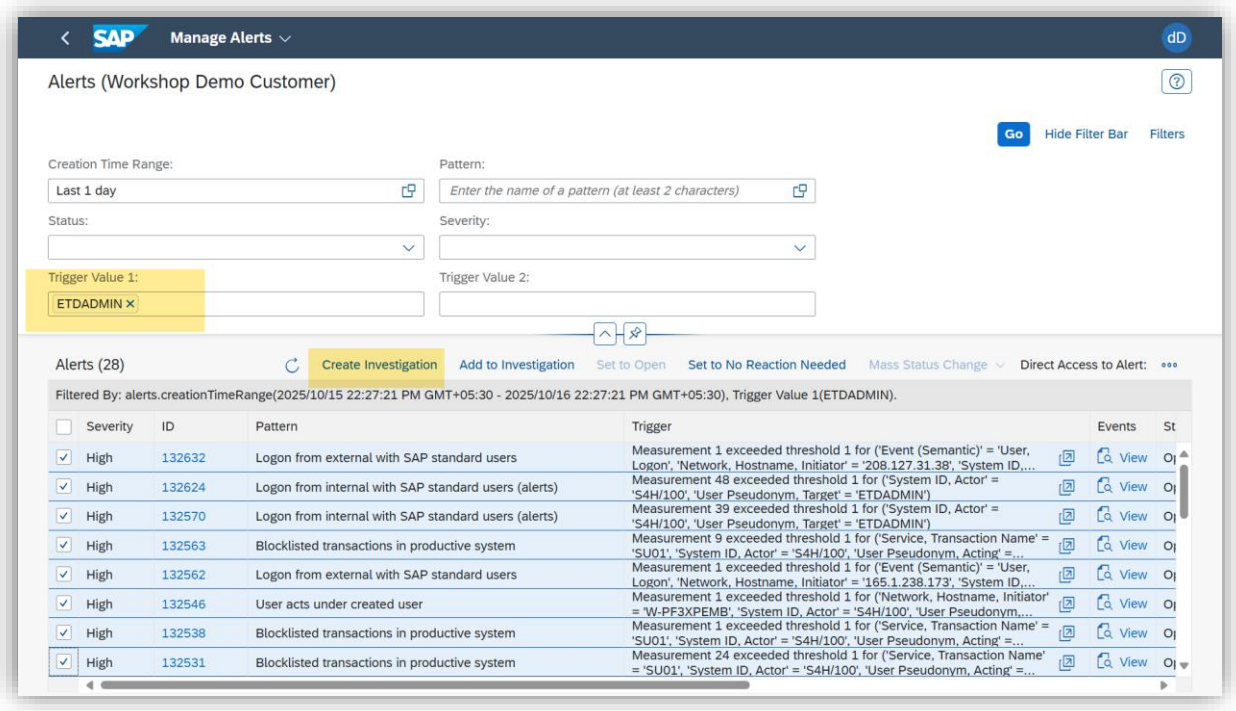
- Choose the app “Analyze Log Events” to check that your activities have generated log entries. Filter for your Admin user ETDADMIN##. If there are too many entries, additionally filter for semantic Events about “user” or “user admin” and you should see a shorter list.



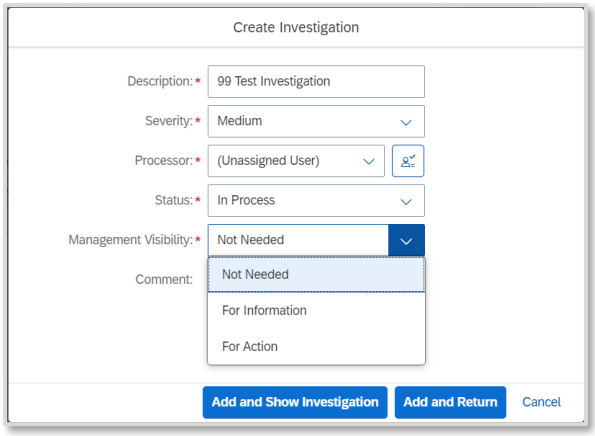
- Note how the “user” column refers to the ETDADMIN## user as “acting”, but there is also an entry for “Target”: this is a pseudonym for your newly generated ETDDEMO## user. Note down this pseudonym for later use.

3.2 Search for Alerts

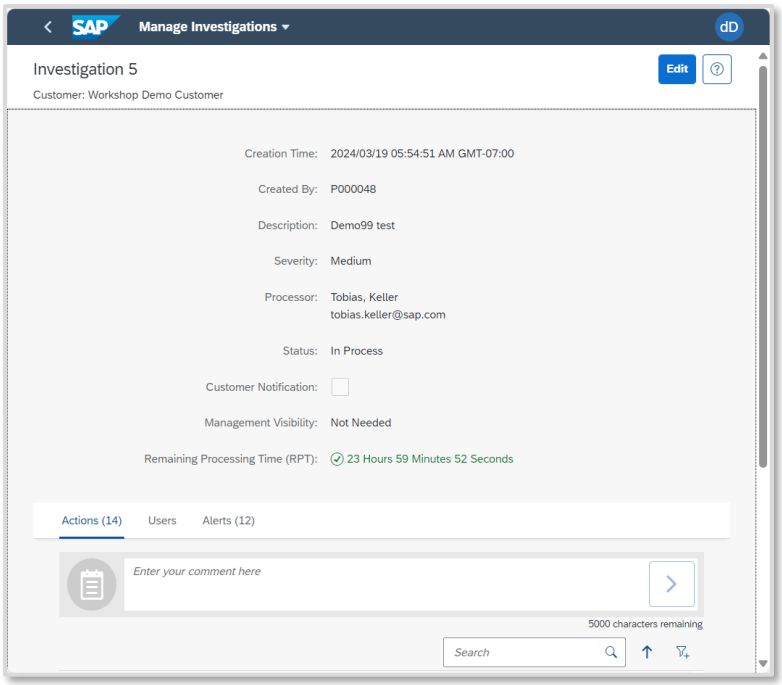
- Choose the app “Manage Alerts”. The list should be populated with several recent entries. If yours is not in the system yet, give a little time – generation for these Alerts is triggered by a job every few minutes.
- Then, filter for your user ETDADMIN## in the Trigger Value 1 or 2 fields, and press “go”. Mark some Alerts you find relevant (or all), and in the bottom right corner, click on “Create Investigation”.



- In the ensuing “Create Investigation” screen, maintain a description referring to your demo ID so you can identify the object later. For “processor”, there are only few options available; just assign any email address.
- What else you enter is not of relevance in the demo flow. Of course, in a productive system these settings determine how the Investigation, if confirming a problem, will be made visible and which follow-on actions it triggers.
- Next, click on “Add and Show Investigation”.



You will then proceed to the main screen of the Investigation you have just created, resembling this example:

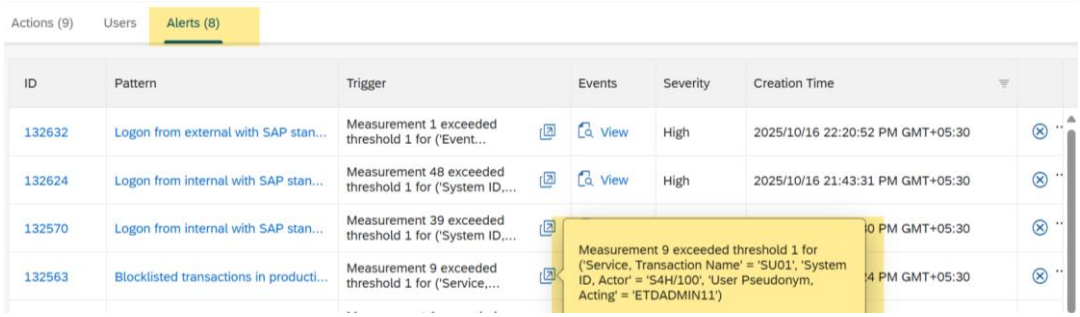


3.3 Interpreting the Investigation Entries

What is the meaning of the different parts of the Investigation object?

- In the Investigation screen, you will find the header information you have maintained before. You can choose to “edit” in case you wish to change the information.

- In the middle section, click on “Alerts”. Here, you can research the Alerts, have a look at some of the complete triggers explanation texts and how they codify the core findings in this text. You may also review some of the triggering Events.



- In the Trigger text, you should also come across at least one additional user – in the form of a “User Pseudonym, Target”. Note down the pseudonym of this user (which you will later see refers to your ETDDEMO## user that was granted high level authorizations).
- In a real life scenario (but beyond the scope of a demo like this), user pseudonyms or other specific pointers like IP addresses, terminal ID/computer name etc. would be used to extend the search for alerts which are relevant for an investigation.
- Return to the tab “Actions”. Here, you may document anything - actions you have been performing, preliminary findings etc. and deductions these allow. These insights will be rendered in the investigation report later and can strongly increase the value and actionability of an investigation.

4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table

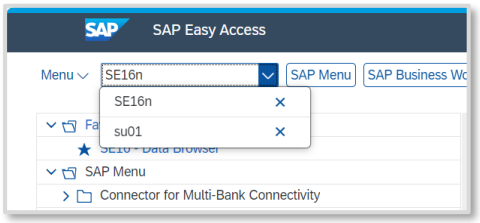
In this section, you will return into the role as a rogue actor and conduct several more actions resulting in Log Events flowing into *SAP Enterprise Threat Detection, public cloud*.

First, you need to log on to the SAP S/4HANA with the newly generated user ETDDEMO##.

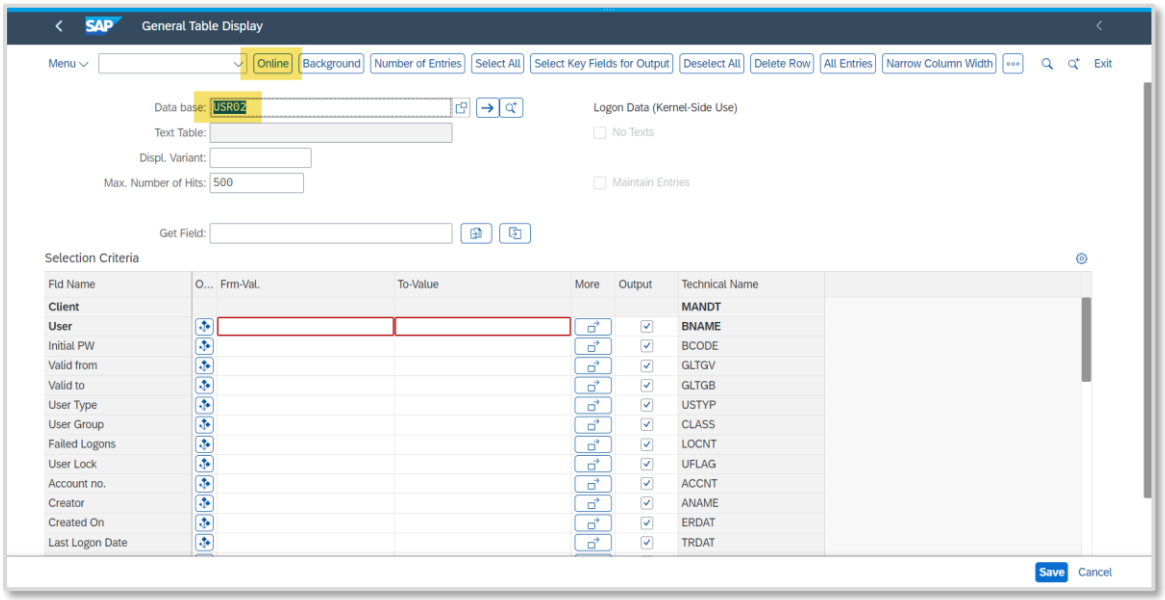
- In order to log on with your new user ETDDEMO##, you need to either open a new “incognito”/”private” session in your browser.
  Alternatively, you may also switch to another browser.
  Emptying the browser cache is also an option. Here, mark at least history, cookies, and password sections, then confirm).
- Now, call the Web Gui console https://52.1.244.180:44301/sap/bc/gui/sap/its/webgui, logon with your new user ETDDEMO## and the password you have chosen. At start, you need to set a new password (suggestion to take a note).

Executing a critical action:

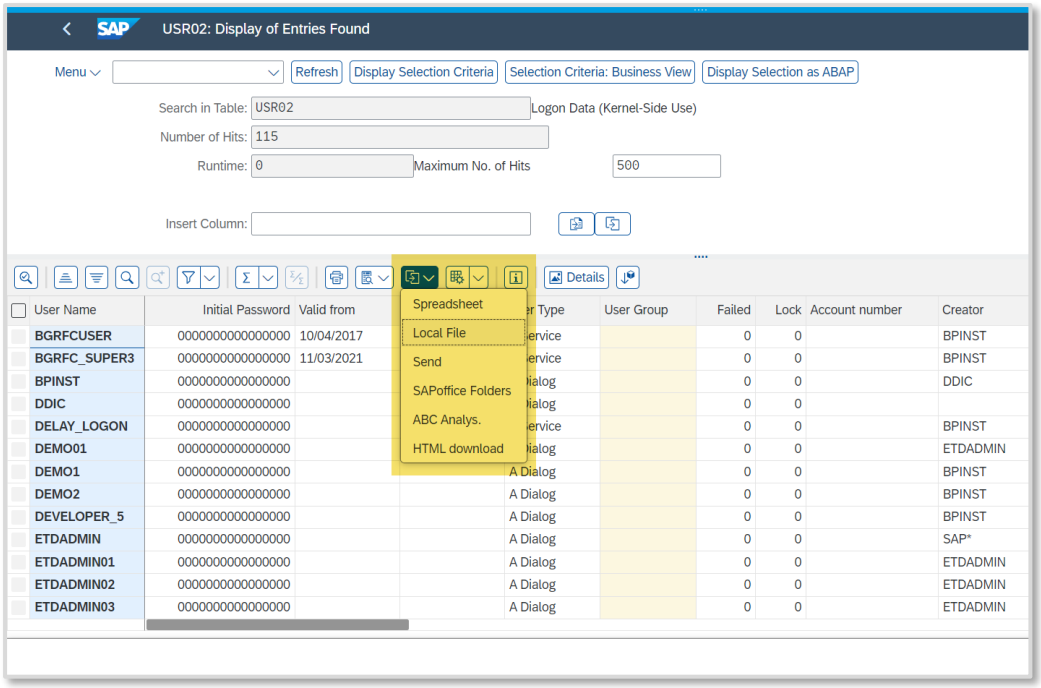
- With the transaction code entry, navigate to transaction SE16N. This is a table display/download transaction (and a tool so powerful that it should generally not be made available in a productive system…).



- In the transaction, call table USR02. USR02 is a table which holds personal information (bad enough) and stores user password hashes (very critical: Although the passwords are hashed out, this would not stop a determined attacker. They may either crack simple passwords and, if they have identified out one single password from any user, they can take the respective hash value to overwrite the hashed password of any other user, allowing them to log on as that user i.e. impersonate the other user. Theoretically the password hashes should be “salted” however, in practice, this attack vector has been working quite reliably. (That said, think about the value of MFA and other tools independent from passwords).
- Access with the function “Online”:



- Search for your user ETDDEMO## and display details. Check out Password Hash Value (real table attribute name PWDSALTEDHASH), towards the end of the table.
- Return to the table display and trigger a download with the icon “Export”, then choose “local file” and confirm the following two interactions. The file can be stored anywhere – in case you need to indicate a directory, pick any that you like.



You have conducted a seemingly simple but dangerous activity which should be resulting in at least one Alert in *SAP Enterprise Threat Detection, public cloud*.
Let's continue to retrieve and process them!

5. User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab

5.1 Build up a Workspace

5.1.1 Assigning a Chart

6. From Workspace to Pattern to Alerts

6.1 Understanding Patterns

7. Finalize the Investigation

7.1 Information: Maintain your email ID to receive investigation reports

7.2 Finalize the investigation

8. Consumer/Processor role: Work with Investigation reports

Thank you for your patience and hard work on this demo. We hope you liked this session and exercise!

For any feedback, please address your trainer, or product management:
SAP-ETD@sap.com