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 3

1. Logon to the Monitoring Console of SAP Enterprise Threat Detection, public cloud 4

1.1 Got a Warning 'Select a Tenant' 6

2. First Log Events from SAP S/4HANA 7

2.1 Logon & Preparation Steps 7

2.2 Creating a User With High Privileges 8

3. Checking Alerts and Creating Investigations 10

3.1 Check for Log Events 10

3.2 Search for Alerts 11

3.3 Interpreting the Investigation Entries 13

4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table 14

5. User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab 16

5.1 Build Up a Workspace 17

5.1.1 Path 1: identify users having received critical authorizations 18

5.1.1.1 Limiting to actions performed for your ID 21

5.1.2 Path 2: identify users accessing critical resources 22

5.1.3 Assigning a Chart 24

6. From Workspace to Pattern to Alerts 25

6.1 Understanding Patterns 25

7. Finalize the Investigation 27

7.1 Optional: maintain your email ID to receive investigation reports 27

7.2 Finalize the investigation 29

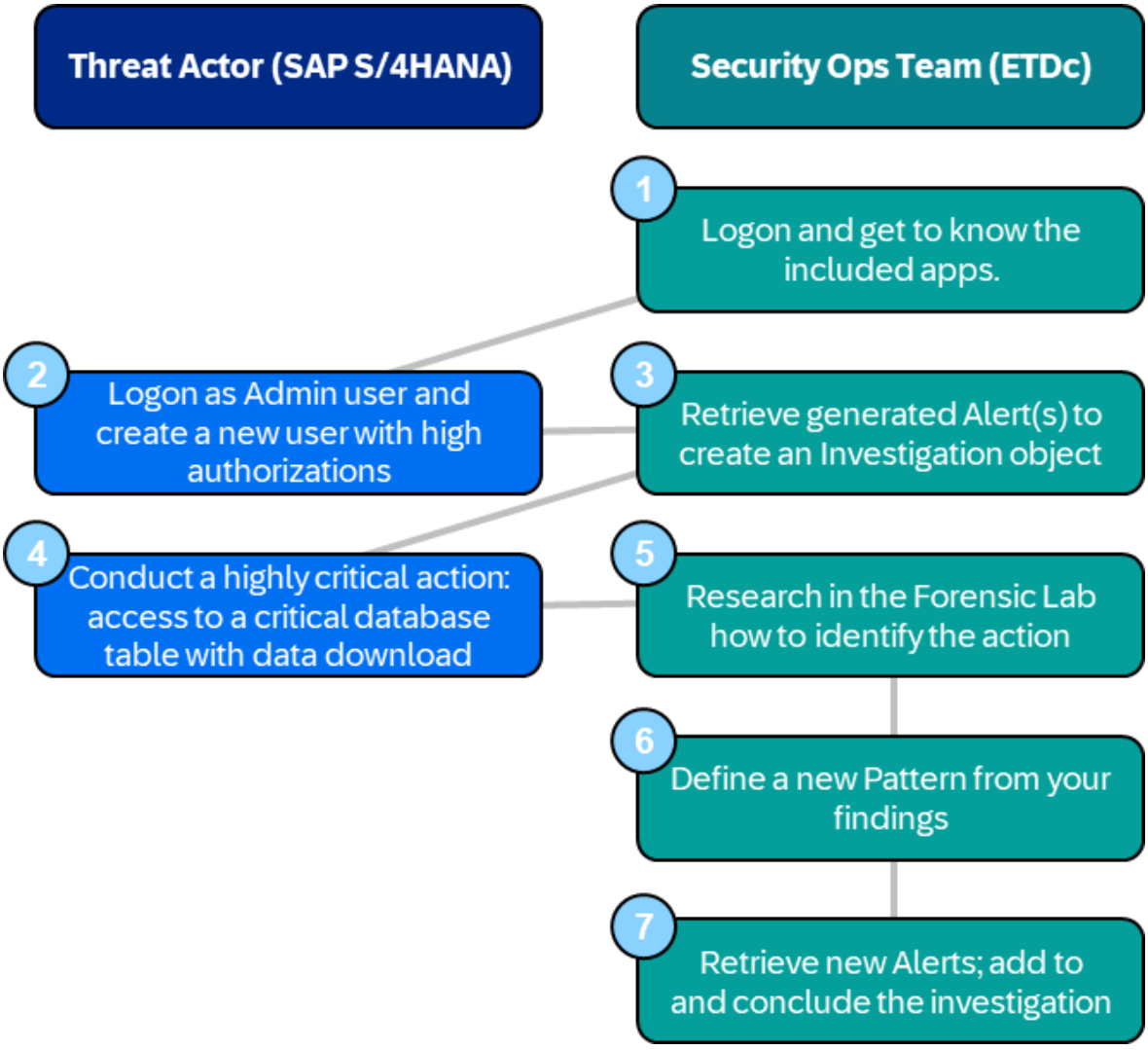
Overview & Touring SAP Enterprise Threat Detection, public cloud

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 two 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.

Here's the flow of the following exercises (the numbers relate to the chapters in this document:



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

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

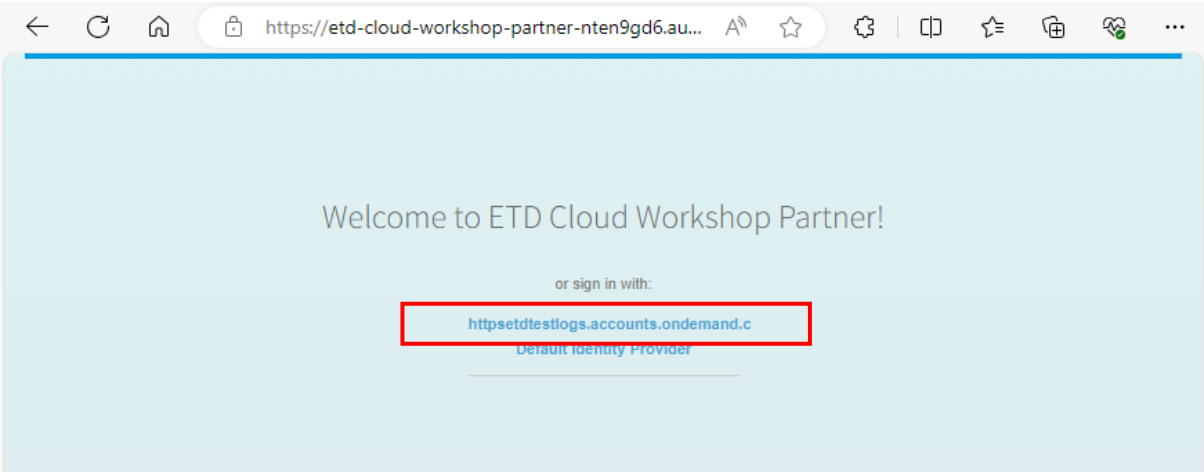
Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

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

[https://etd-cloud-workshop-partner-nten9gd6-monitoringapprouter.prod.monitoring.etd-cloud.cfapps.eu10-004.hana.ondemand.com/cp.portal/site#]

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 (01-25; afterwards referred to as "##").

User: demo##@etdsap.com

Password: will be provided in the session

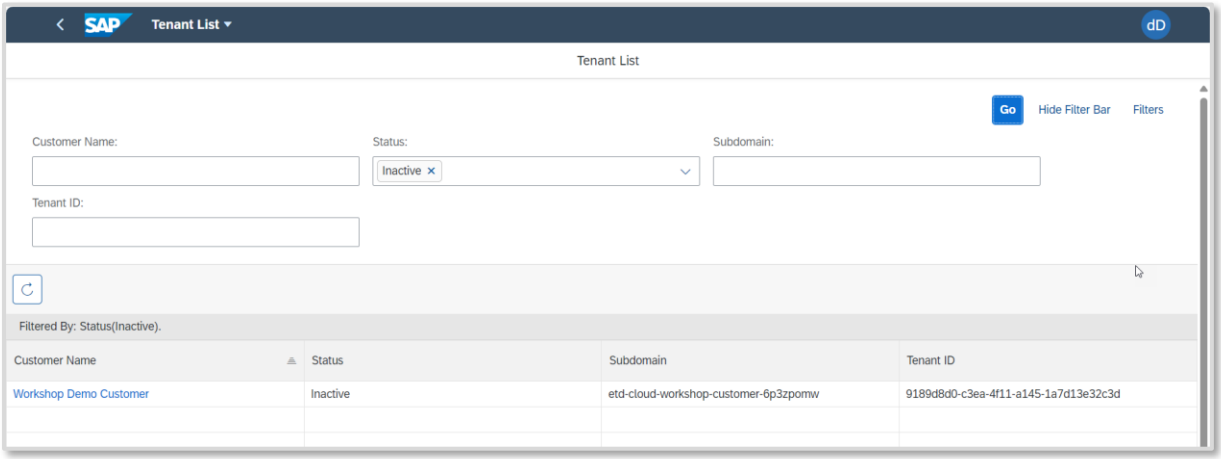
If you inadvertently lock the password, please notify the instructor.

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

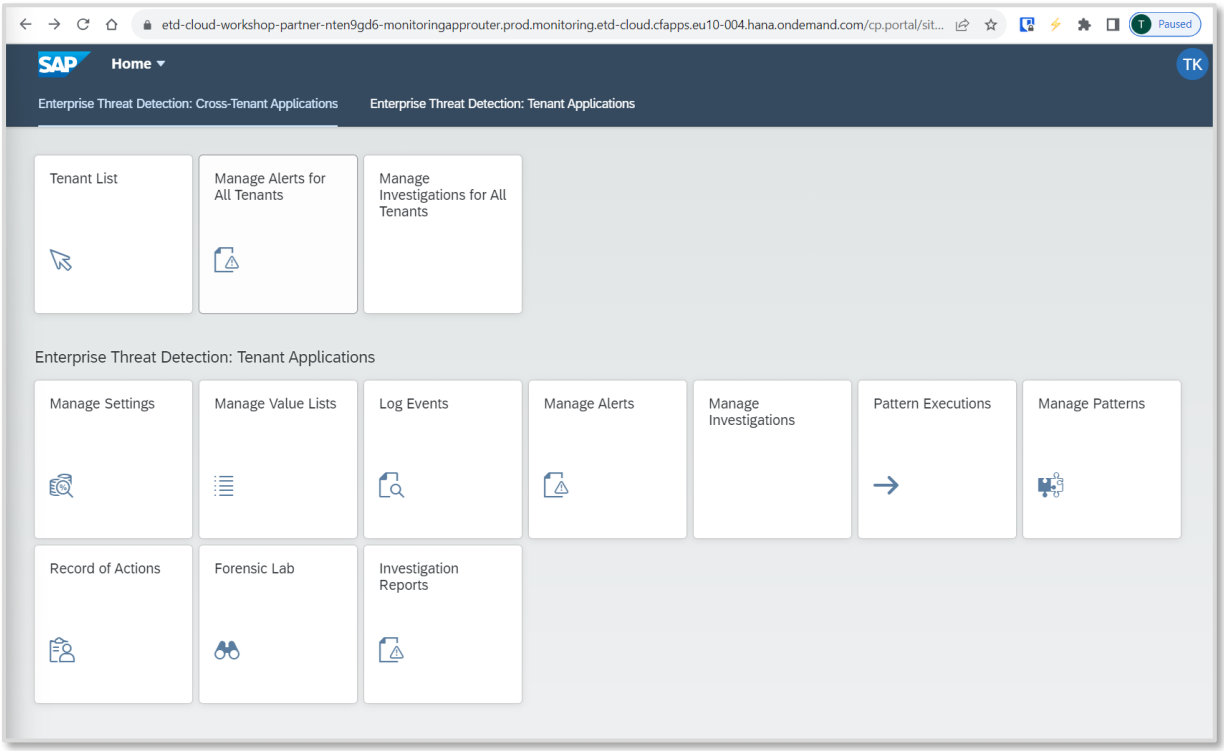
Upon initial logon, you will see the Tenant List screen for selecting a specific Tenant:

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".

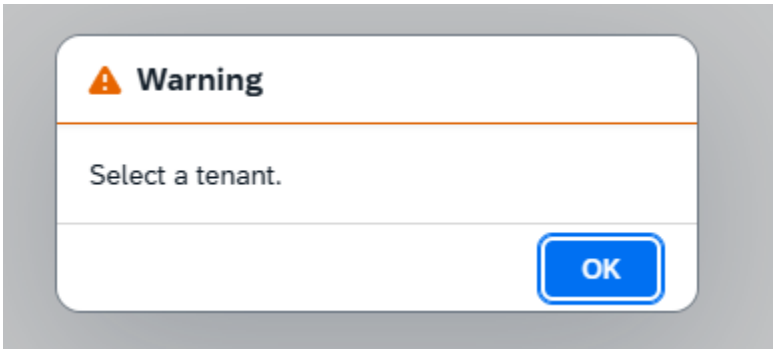


You will then see the *SAP Enterprise Threat Detection, public cloud* monitoring console. Take a bit of time to check by a few apps and how they behave.



1.1 Got a Warning ‘Select a Tenant’

If you encounter a the warning popup

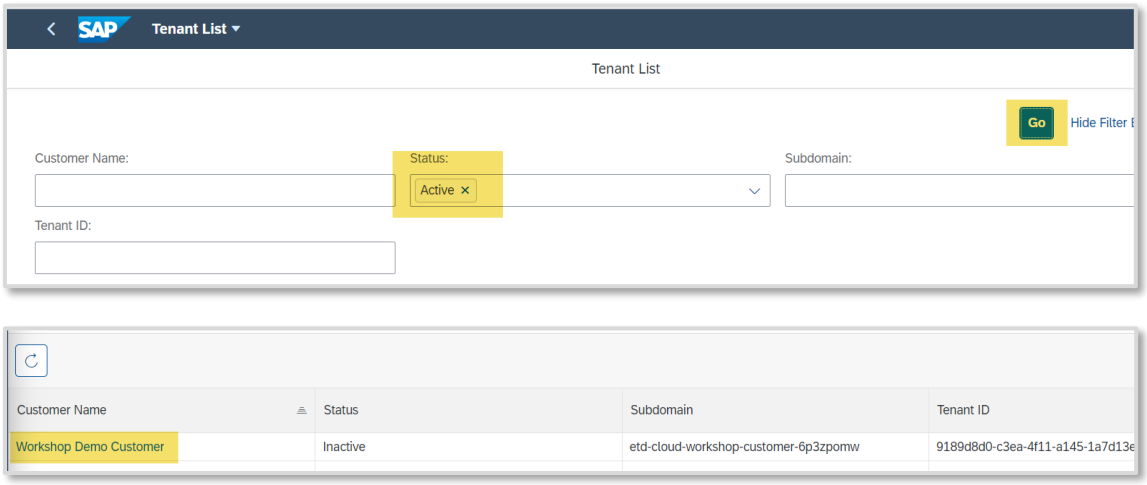


the system has lost the information which Tenant you’ve been working on (most likely you had been logged out).

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 “Tenant list”.
- 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)



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.

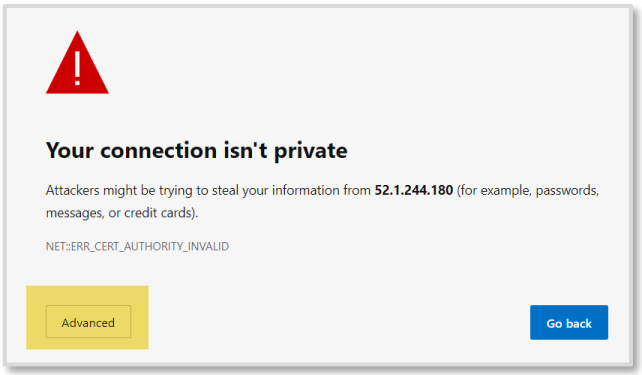
This system & credentials are available during the planned workshop hours only.

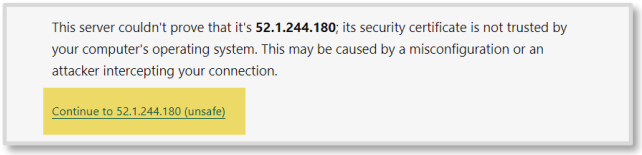
Please let the instructor know in case you'd like to have access afterwards; we're happy to check how long we can extend your access.

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:





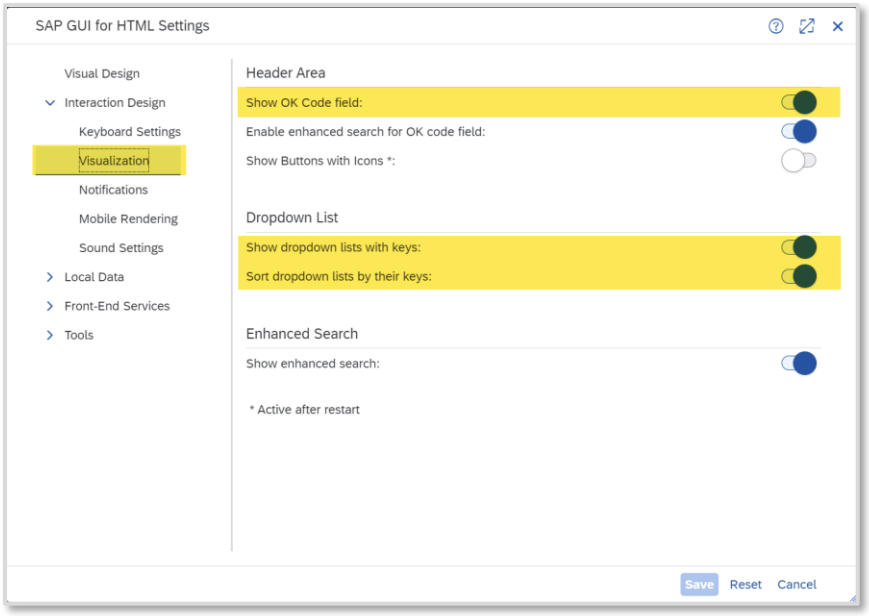
Log on credentials:

User: ETDADMIN##

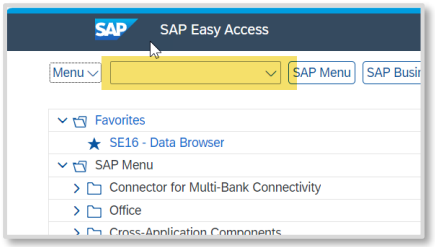
Password: Admin123

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.



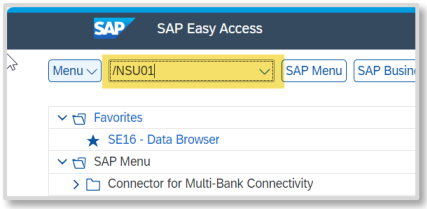
- Leave the menu. Your start screen should now show the transaction code entry field:



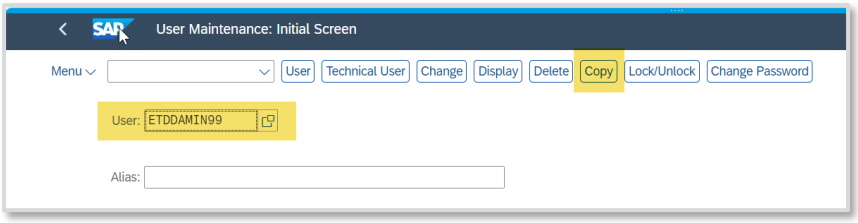
2.2 Creating a User With High Privileges

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

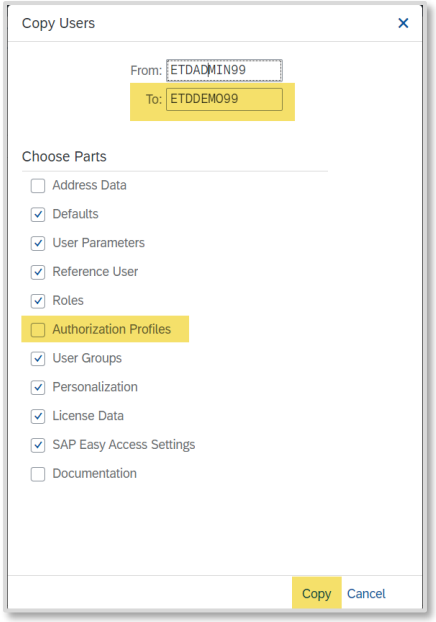
- In the transaction code entry, enter “SU01” (User Maintenance), and hit enter.



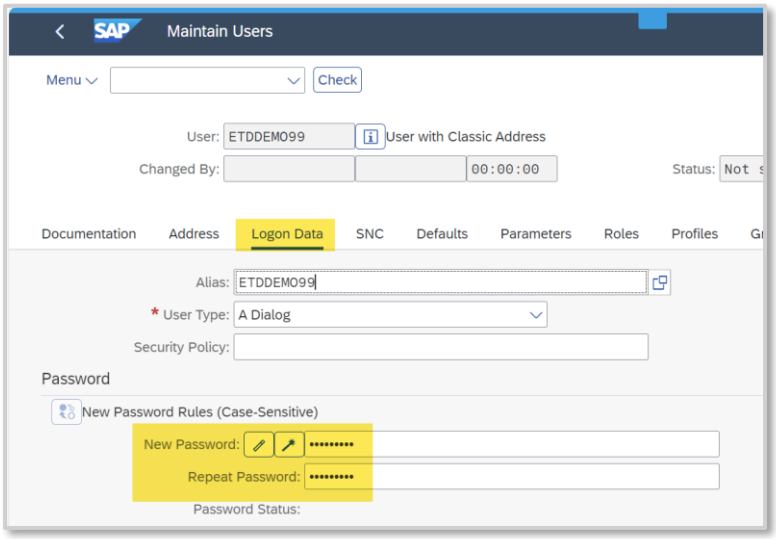
- In the User Maintenance transaction start screen, enter your user ETDADMIN## in the User field, and select “copy”.



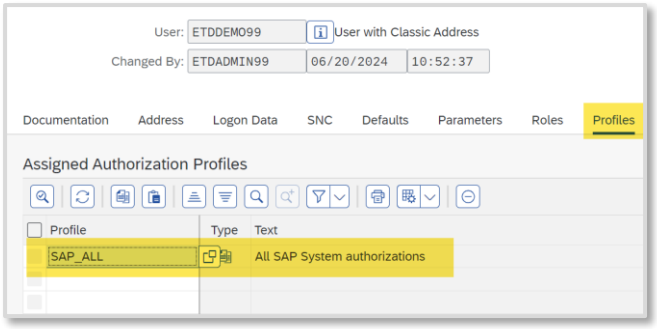
- In the pop up screen, maintain the new user name “ETDDEMO##” in the “To:” field; deselect the option to copy authorization profiles, and press “copy”:



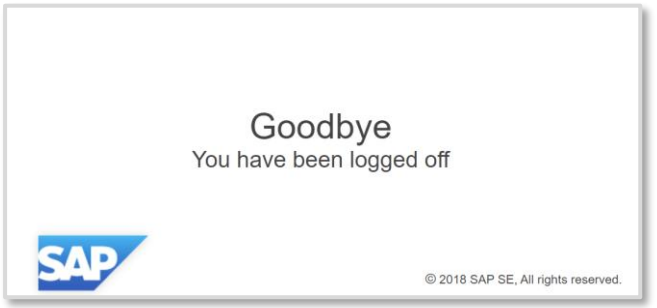
- In the resulting screen set, on tab “Logon Data”, assign an initial (temporary) password (it is suggested to note down this password as you will need this to log on with ETDDEMO##). Then save the user.



- 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

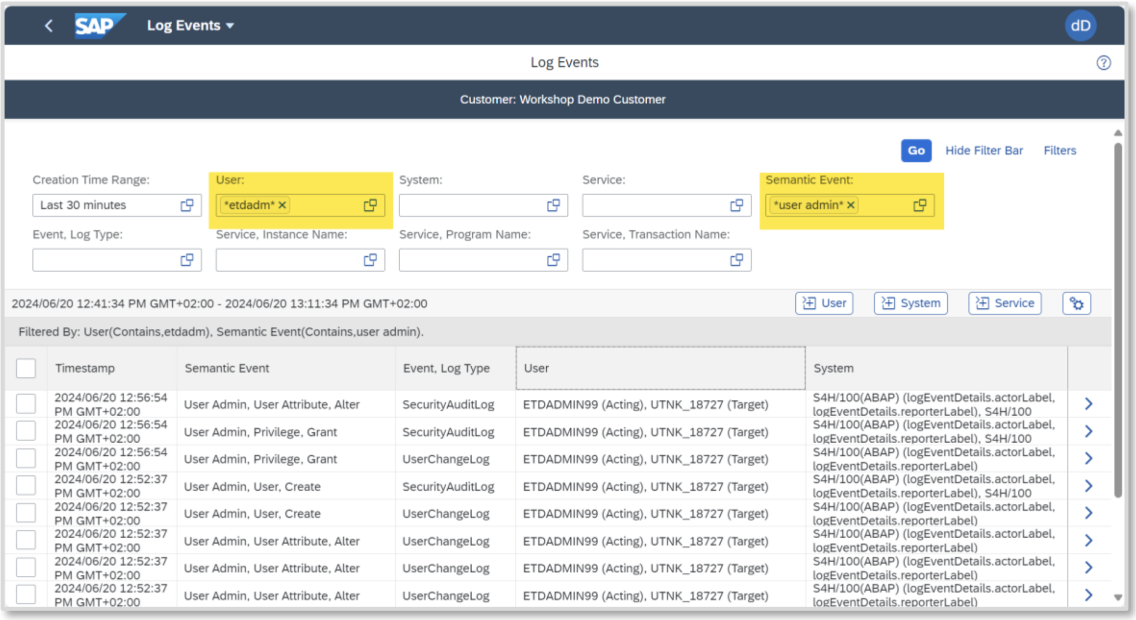
You will now look at alerts in *SAP Enterprise Threat Detection, public cloud* and create an Investigation object out of it.

Return to the *SAP Enterprise Threat Detection, public cloud* Monitoring Console. If necessary, log on again with your user demo**xx**@etdsap.com, password <ETDSAP_Demo> (cf. section 1) and in the Tenant List app, select the tenant “Workshop Demo Customer”.

If you receive the “404” error, refer to section 1.1 how to resolve.

3.1 Check for Log Events

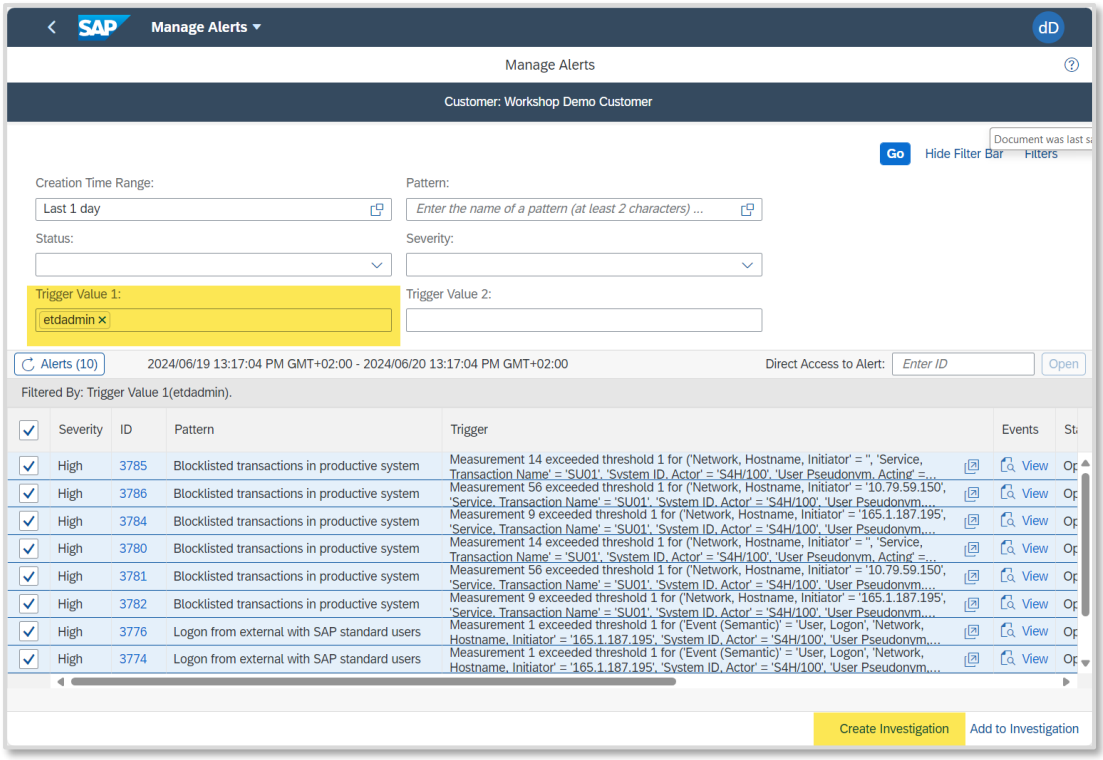
- Choose the app “Log Events” to check that your activities have generated log entries. Filter for your Admin user ETDADMIN##. If there are too many entries, additionally filter for semantic Events about “user” or user “admin” and you should see a shorter list.



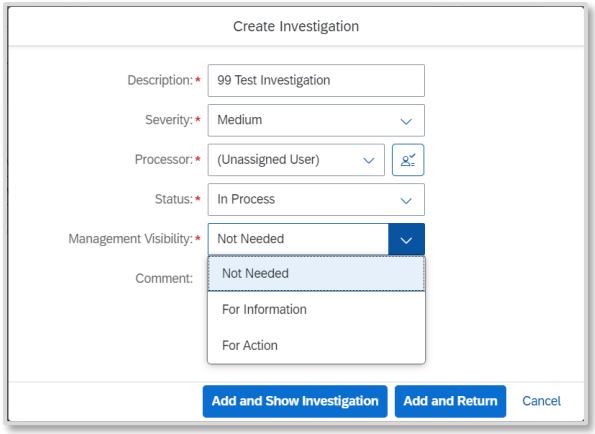
- Note how the "user" column refers to the ETDADMIN## user as "acting", but there is also an entry for "Target": this is a pseudonym for your newly generated ETDDEMO## user. Note down this pseudonym for later use.

3.2 Search for Alerts

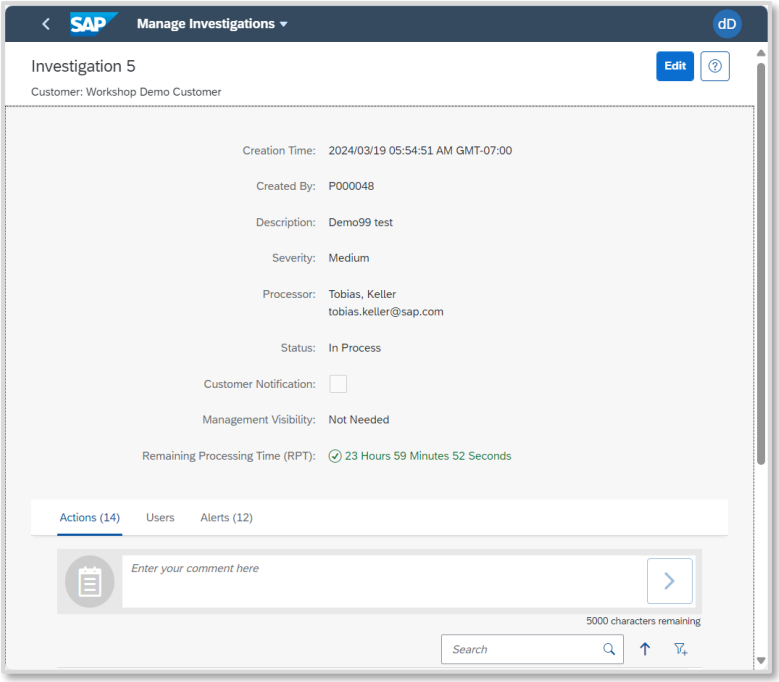
- Choose the app "Manage Alerts". The list should be populated with several recent entries. If yours is not in the system yet, give a little time – generation for these Alerts is triggered by a job every few minutes.
- Then, filter for your user ETDADMIN## in the Trigger Value 1 or 2 fields, and press "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”.



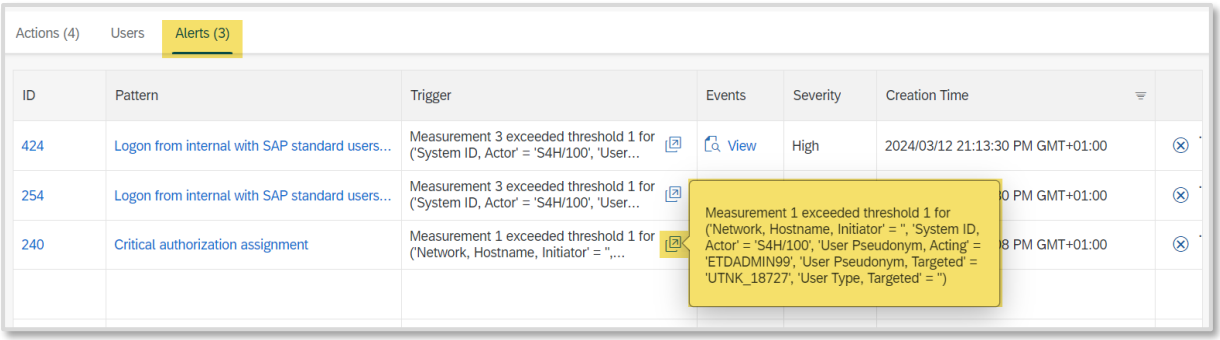
You will then proceed to the main screen of the Investigation you have just created, resembling this example:



3.3 Interpreting the Investigation Entries

What is the meaning of the different parts of the Inv estigation 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, Targeted”. 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

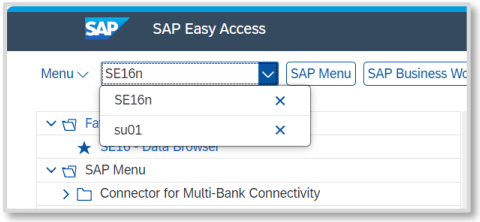
In this section, you will return into the role as a rogue actor and conduct several more actions resulting in Log Events flowing into *SAP Enterprise Threat Detection, public cloud*.

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

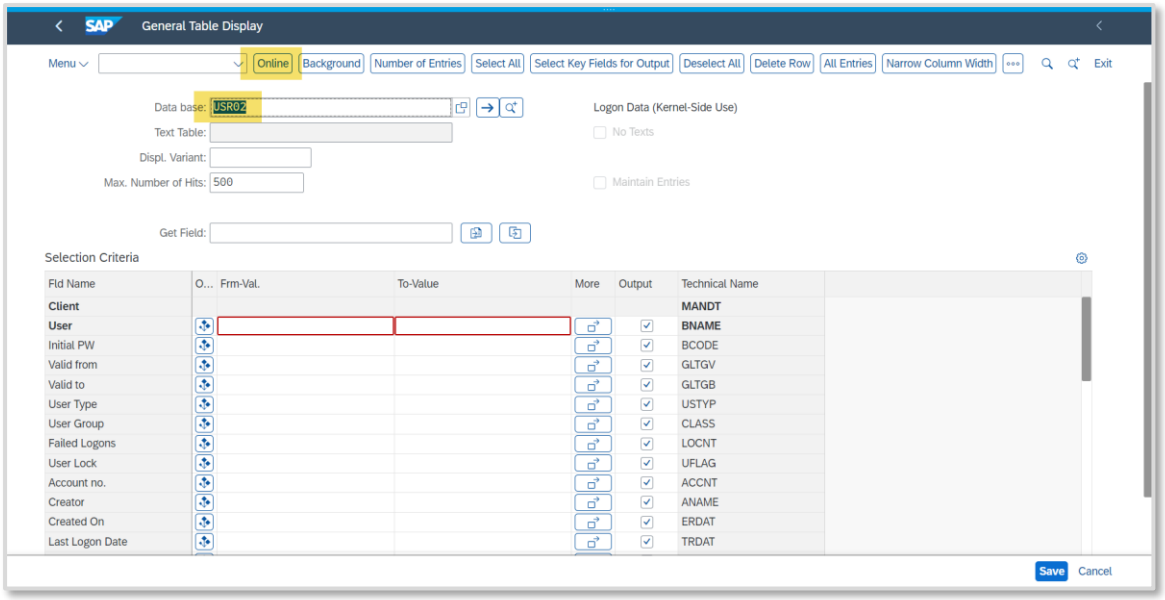
- In order to log on with your new user ETDDEMO##, you need to either open a new "incognito"/"private" session in your browser.
  Alternatively, you may also switch to another browser.
  Emptying the browser cache is also an option (in Chrome, use command CTRL + Shift + DEL → "Advanced". Here, mark at 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:

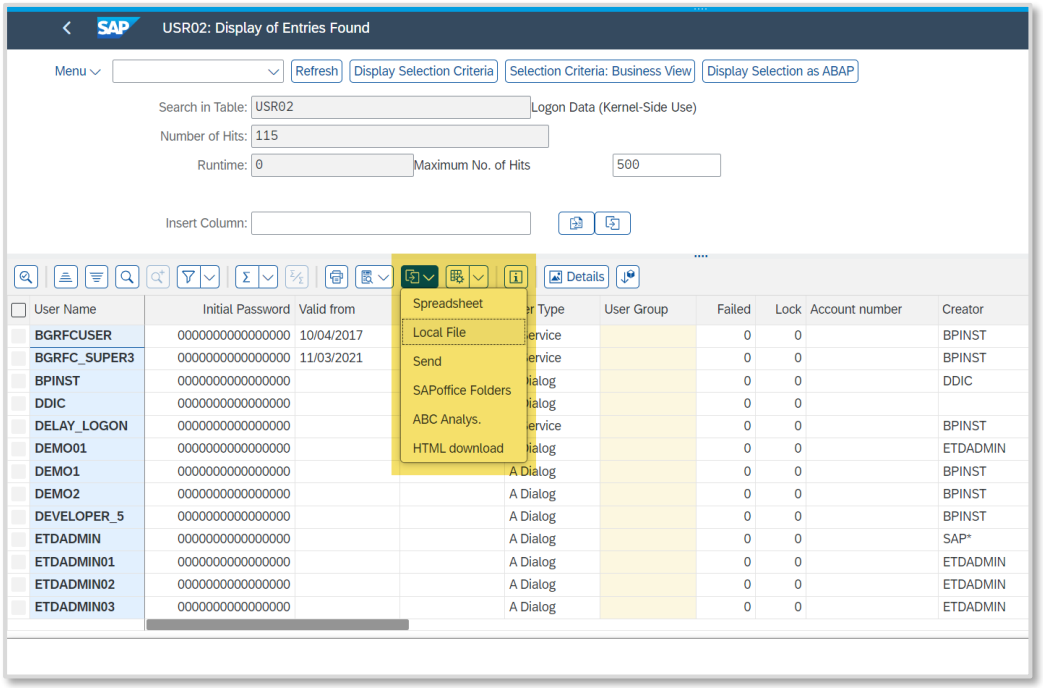
- With the transaction code entry, navigate to transaction SE16N. This is a table display/download transaction (and a tool so powerful that it should generally not be made available in a productive system…).



- 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 the “salted” hash, 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

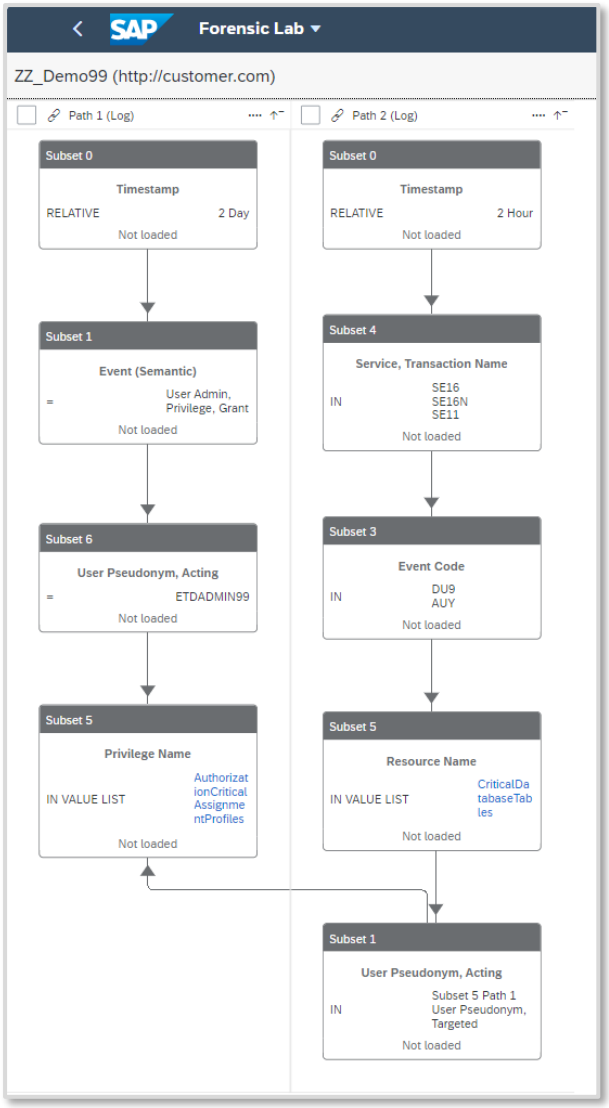
The Forensic Lab is the area where you work on ways to identify new potential threat vectors by filtering your way through the large volume of log entries until you arrive at a definition yielding few and specific logs that should point at a real threat.

Here, we will build a workspace with filters capable of identifying the case where a user is granted high authorizations, and then accesses a critical resource.

To this end, we will be building two filtering Paths linked by a Reference:

- “Path 1” should be capable of establishing a list of users who have been granted critical authorizations in the past 2 days.
- “Path 2” to the right shall be able to establish a list of all users who have accessed a critical resource recently.
- The “Reference” allows to single out users which are in the result lists of both paths.

The Workspace will look similar like this one:



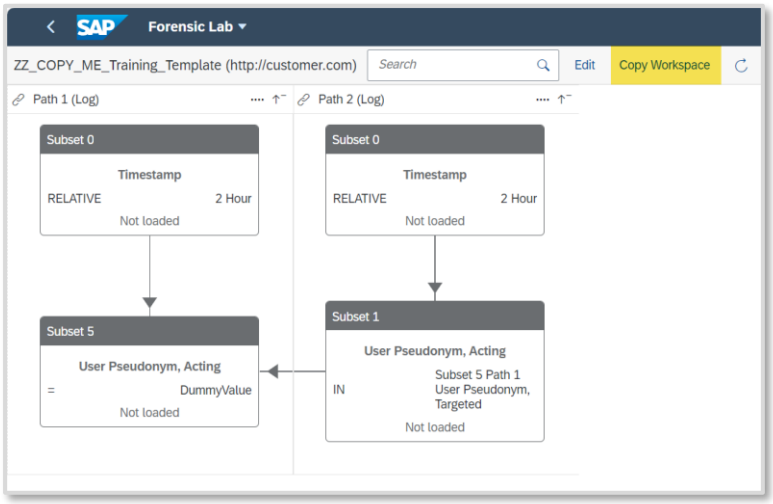
5.1 Build Up a Workspace

- Return to the monitoring console of SAP Enterprise Threat Detection, cloud edition.
- Go to the app “Forensic Lab”. In the area “Custom Workspaces”, you see a list of existing workspaces.

If you are progressing well on the workshop scenario and/or have a keen interest on the threat hunting/forensic lab functionality, just continue with the next paragraph. In case you feel you’re behind time on the workshop scenario, you may abbreviate the exercise. In this case, access the workspace “ZZ_GoldenWorkspace_DONOTCHANGE”. Here, choose “Copy Workspace” and in the resulting pop-up maintain a name for your new Workspace, like “##_PWHash_Attack”. Leave the Namespace value unchanged. The system will automatically open the new workspace for you to continue working. In this script, please jump to chapter 2.1.5.3, “Assigning a Chart”.

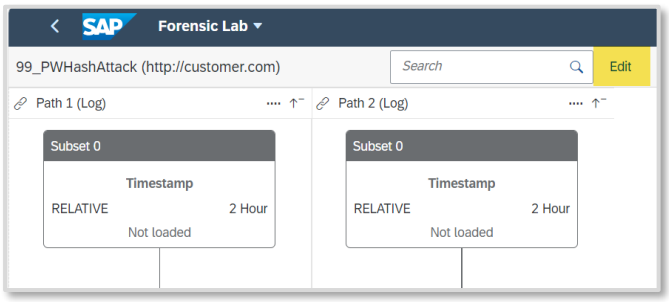
- In the normal progress, select the Workspace “ZZ_COPY_ME_Training_Template” (this Workspace is not yet usable, but links two filtering Paths with a “reference”, a feature which

in the future will be configurable but now is hard coded). Here as well, copy the Workspace, maintain a name for your new Workspace like “##_PWHash_Attack” without changing the Namespace. Your template (and resulting new Workspace will look like this:

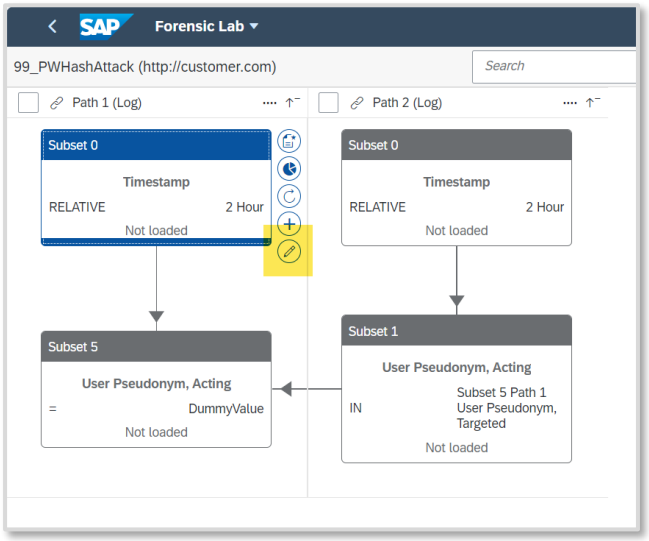


5.1.1 Path 1: identify users having received critical authorizations

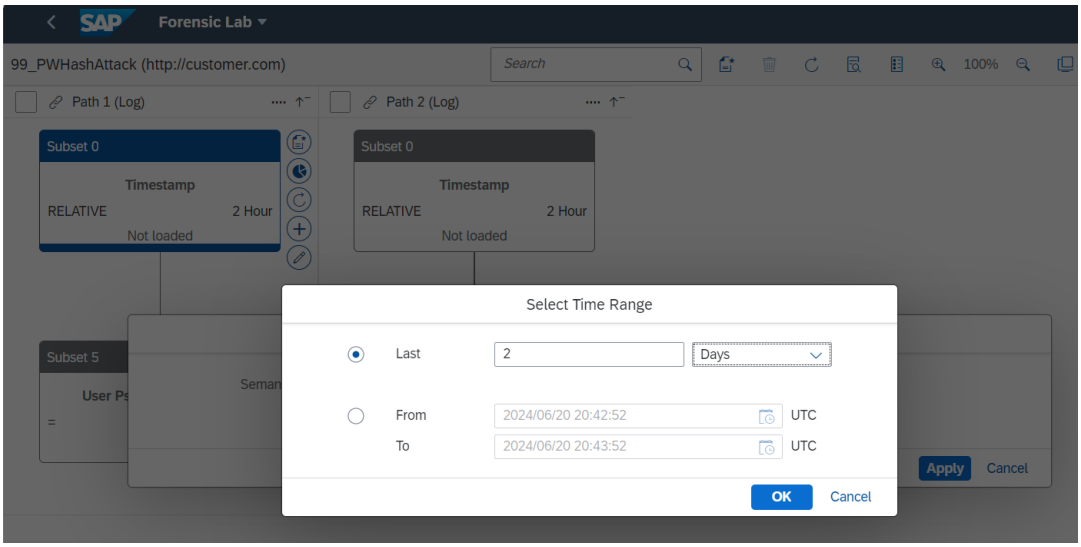
- In the next screen, press “edit” to be able to change and add subsets.



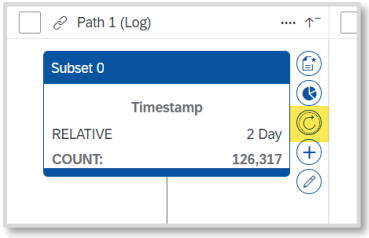
- Click on the “Subset 0” tile in Path 1. When activated, it shows a few icons next to it. Check the “pen” symbol to edit this Subset, e.g. to extend or reduce the time frame being considered:



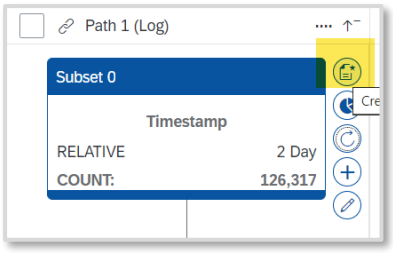
- In the resulting pop-up, set the time to 2 days, indicating that only logs newer than the last 2 days will be considered, and confirm with OK.



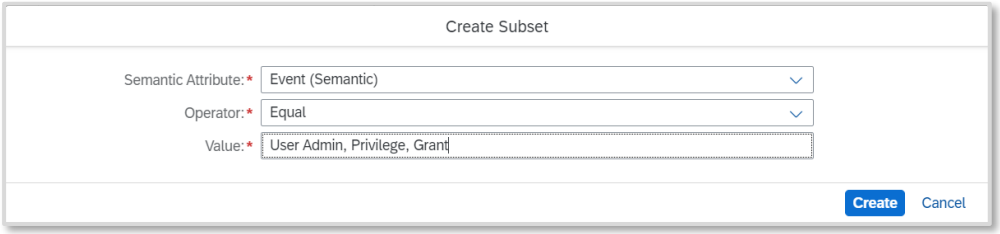
- Then click on the function “Refresh Subset Count” to get an indication of the number of matching log entries.



- In a next step, you expand the filter rules by expanding the structure with an additional Subset. Click on the Subset 0 tile again; now click on “create new Subset”

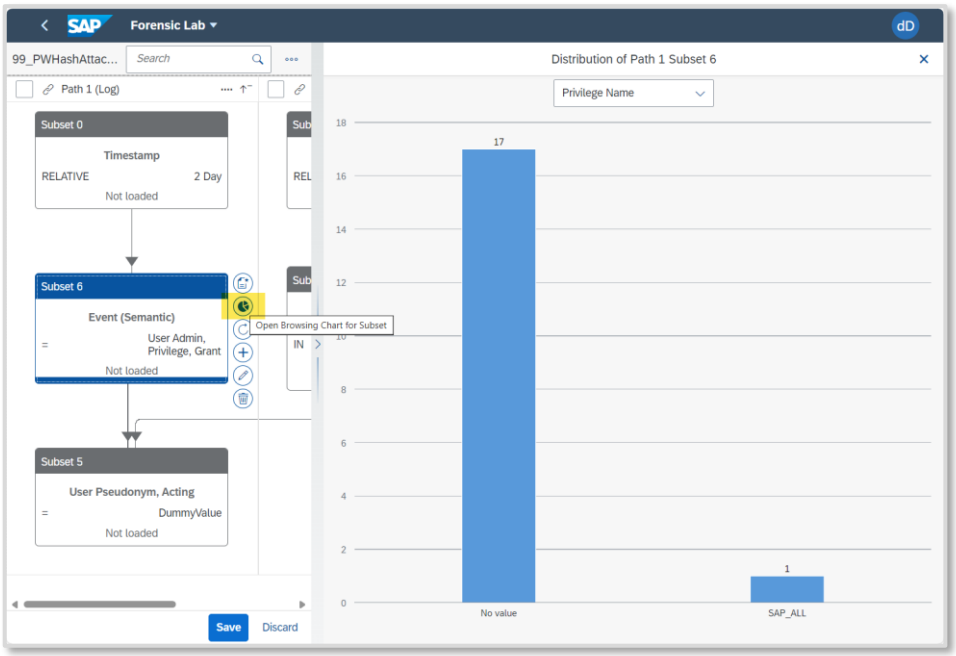


- In in the ensuing screen fill the following information:
  - Semantic attribute: Event (Semantic)
  - Operator: Equal
  - Value: User Admin, Privilege, Grant [be careful to use this exact capitalization]

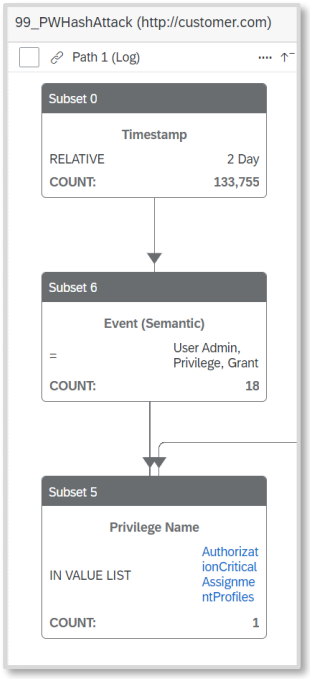


Then select “Create”, and in the ensuing screen refresh the Subset count as well – which should result in a substantially lower number of resulting log events because in this way, you are only considering log events that are mapped to the semantic event for admins granting users privileges.

- At this stage, it makes sense to break down the values in a visual way. At the right of the Subset 5, press the button “Open Browsing Chart for Subset”. In the resulting graph, you choose for which Semantic Attributes you want to see the distribution. It may make sense to look at distribution of “User Pseudonym, Acting” (giving privileges), “User Pseudonym, Targeted” (given privileges), or at “Privilege Name”:



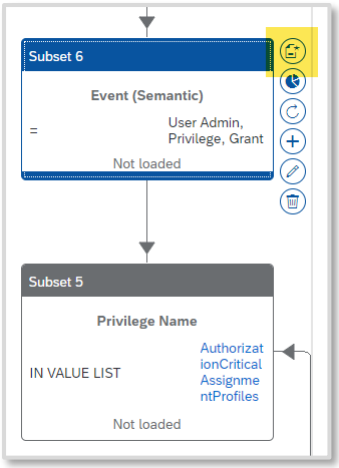
- After looking at the distribution of privilege names, we see that SAP_ALL has been granted. Instead of filtering for this one profile though, we may consider more privileges which are also critical and haven been summarized in a Value List.
  To do so, in the existing Subset 5, replace the definitions with the following filter for which privileges exactly you want to consider:
  - Semantic attribute: Privilege Name
  - Operator: In value list
  - Value: AuthorizationCriticalAssignmentProfiles (where the system will suggest this value list when you enter the first few letters).
- After refreshing the Subset Count, your Path 1 should be looking similar to this:



5.1.1.1 Limiting to actions performed for your ID

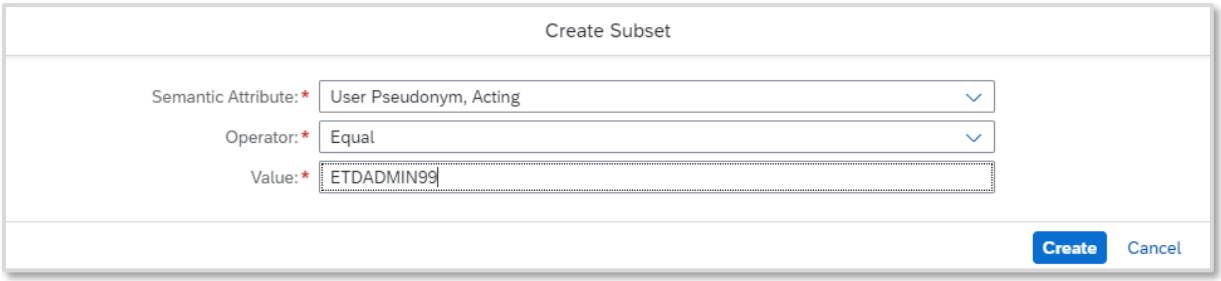
To make sure your Workspace will only react to your specific users and not to other participants, a last additional Subset is needed. Make sure you are in Edit more.

Under the Subset on “Event (Semantic)”, add another Subset:

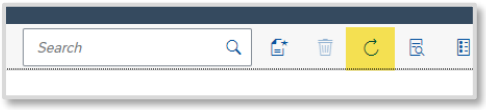


In the ensuing pop-up, maintain the following settings and hit “Create”:

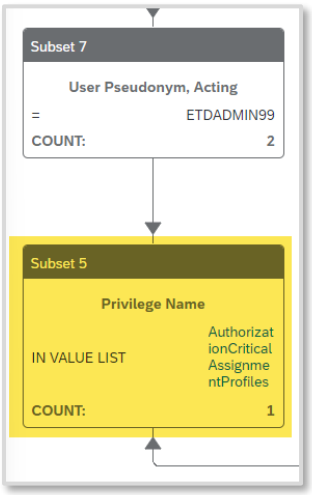
- Semantic attribute: User Pseudonym, acting.
- Operator: equal
- Value: [the pseudonym of your user ETDADMIN##]



Press the “refresh” button once more to see how many Log Events are relevant after each of the Subsets are applied.



Ideally, you should be seeing one log which your Workspace path 1 highlights (the case where YOUR admin user granted SAP_ALL access to your newly created DEMO user):



IMPORTANT: Save your Workspace before moving further!

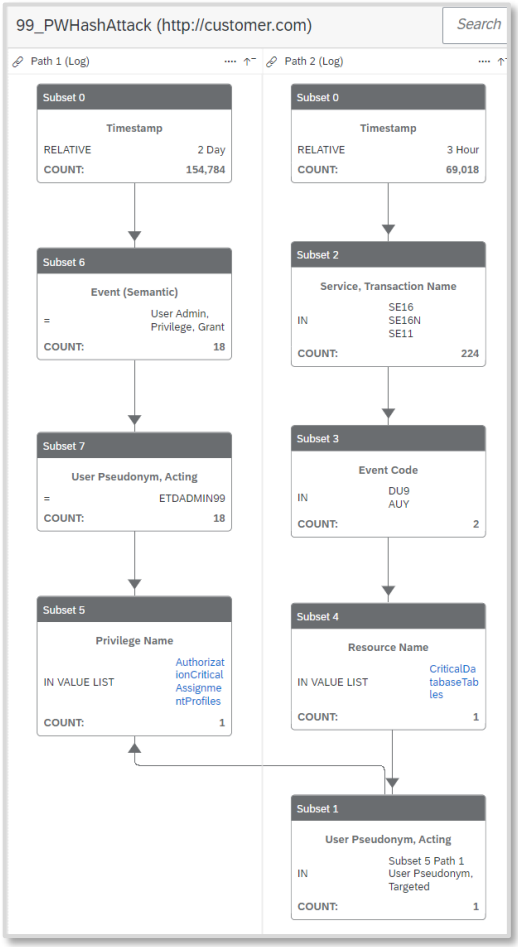
If you’re on the short track working with the already defined Workspace, you may move directly on to chapter 5.1.3 Assigning a Chart. Else, continue working on path 2 in the next paragraph.

5.1.2 Path 2: identify users accessing critical resources

In the right hand Path 2, we will be looking for users who recently accessed critical resources (database tables).

- In the Subset 0, limit to 1hour.
- Under this Subset, add a new Subset filtering for specific transaction names from which db tables can be accessed. Settings:
  - Semantic attribute: Service, Transaction Name
  - Operator: In

    - Value: SE16; SE16N; SE11 [be sure to use this exact capitalization. After each of the transaction names, hit enter.]
- Next, in an additional Subset, we want to restrict to relevant events, like accessing in read mode and downloading.
    - Semantic attribute: Event Code
    - Operator: In
    - Value: DU9; AUY
- In a final Subset, we want to limit to critical db tables only:
    - Semantic attribute: Resource Name
    - Operator: In value list
    - Value: CriticalDatabaseTables
- As a last step, let's look at the predefined Subset "User Pseudonym, Acting" setting up the comparison to "User Pseudonym, Targeted" from Path 1, i.e. the list of users who have been granted critical authorizations. [This subset is currently not editable; references will be possible to maintain in future releases of the functionality.
- If this worked well, your final subset should be resulting in a positive count, and look similar to this depiction:



- When done, please **SAVE YOUR WORKSPACE**

5.1.3 Assigning a Chart

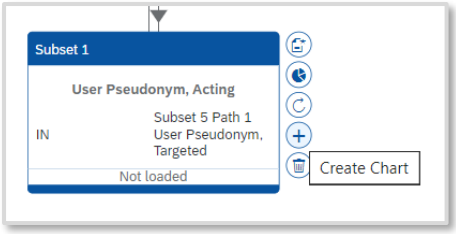
The Workspace and filters you have built defines a way to identify events pointing at a new threat. In real life, if you suspect this is an attack and that it might repeat, you want to re-use these definitions and actually automate them to throw an Alert whenever the same occurrence happens again.

To this end, the logical next step in *SAP Enterprise Threat Detection, cloud edition* is to define (name and save) the Browsing Chart pertaining to one of your Subsets.

Such a named Chart can then be used to build a new Pattern – which generates Alerts whenever Log Entries pertaining to the Subset/Chart reach a predefined threshold (e.g. “more than 5 processed bank account numbers per day”, or “every single access to a critical database table”).

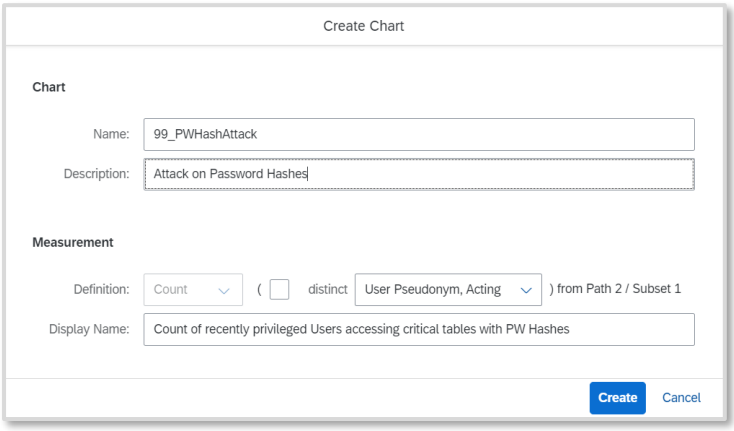
This is the primary way of building new content in *SAP Enterprise Threat Detection, public cloud*.

In this demo case, we look to the final Subset on “User Pseudonym, Acting” in Path 2. Switch to edit mode again, and mark Subset 1, Path 2. Then press “Create Chart”:



In the pop-up, assign a name among the lines of “##_PWHashAttack”, and a description. Mark down the name.

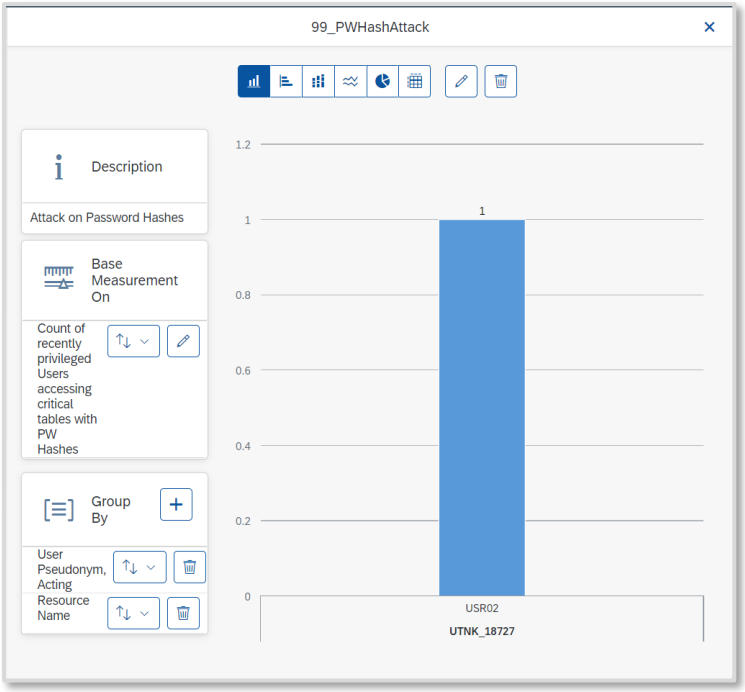
For measurement, choose the “count” of “User Pseudonym, Acting” and a fitting Display Name if you like:



Clock on “Create”. In the ensuing screen, choose to “Group By” the semantic events

- “User Pseudonym, Acting”
- “Resource Name”

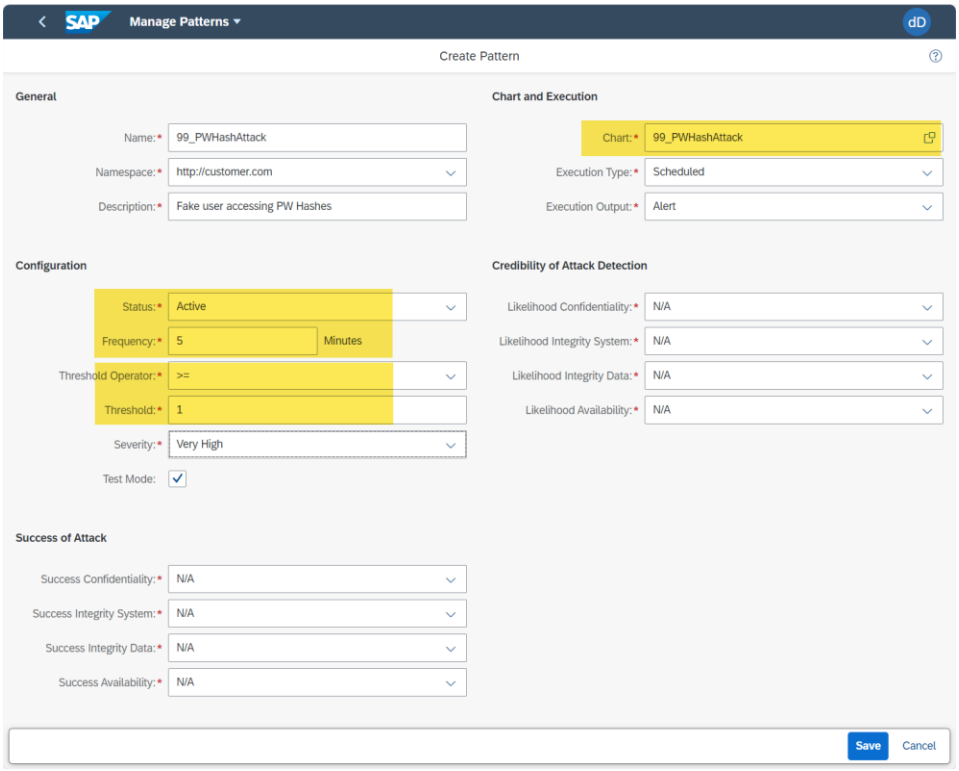
The resulting Chart should be looking something like this. Note how the grouping results in the resource USR02 and a user pseudonym being displayed (which should be the pseudonym assigned to your ETDDEMO## user):



6. From Workspace to Pattern to Alerts

6.1 Understanding Patterns

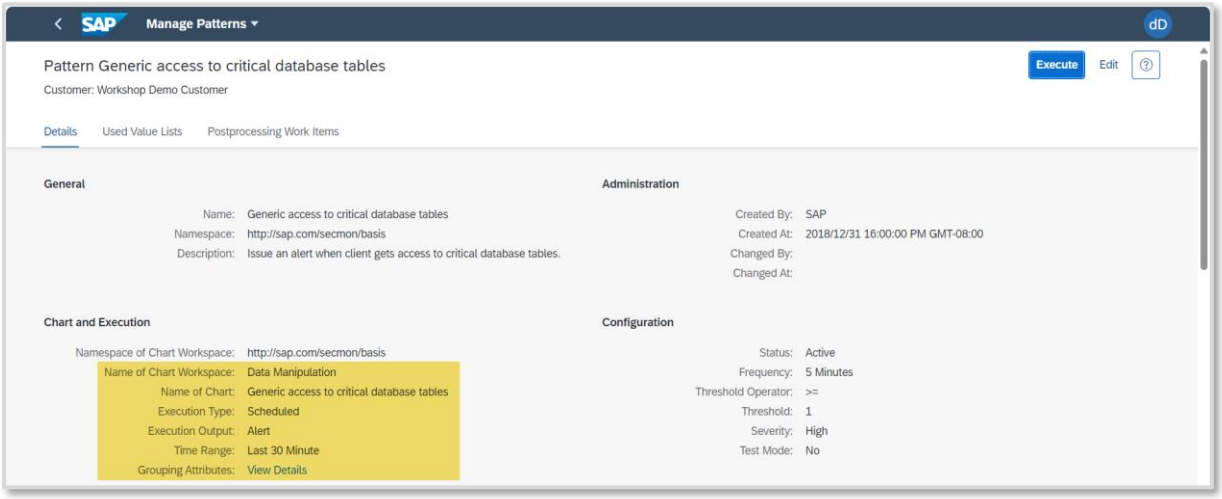
- Return to the Console Home Screen and Enter the “Manage Patterns” app.
- Choose to “Create Pattern” and in the pop-up maintain the relevant information. Importantly, set the status to “Active”, frequency to the lower limit of 5 minutes; and Threshold to >=1. In the “Chart” field, retrieve and assign the Chart you have created.



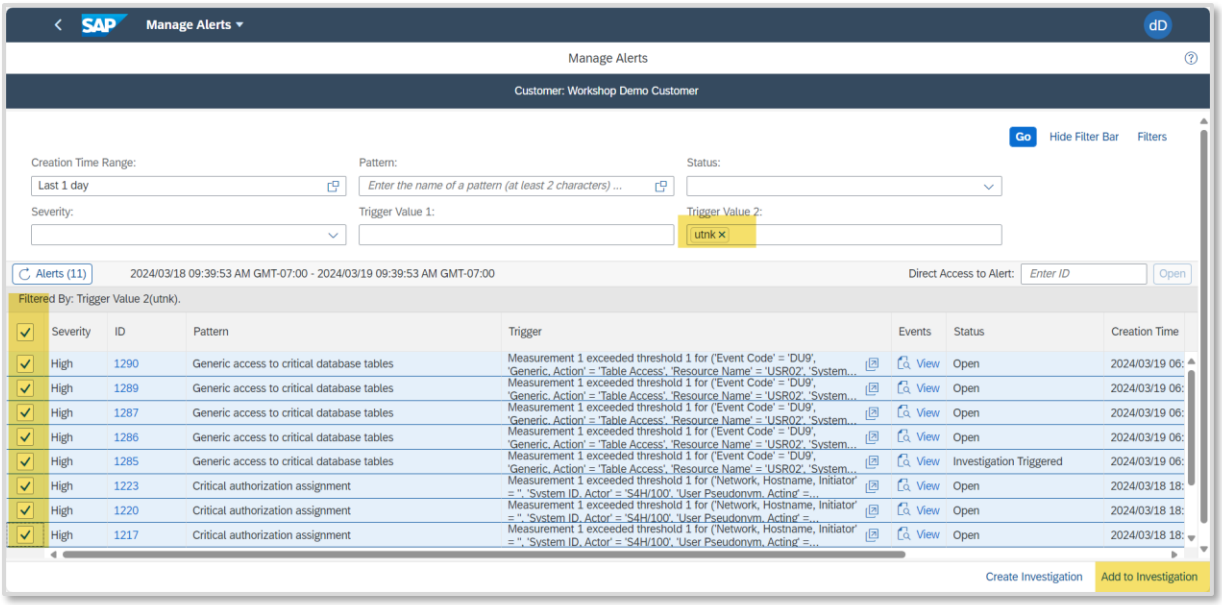
The fields for Success of Attack and Credibility of Attack Detection can help to gauge the severity of a breach, but does not have a direct influence in the context of this hands-on session.

Save your work.

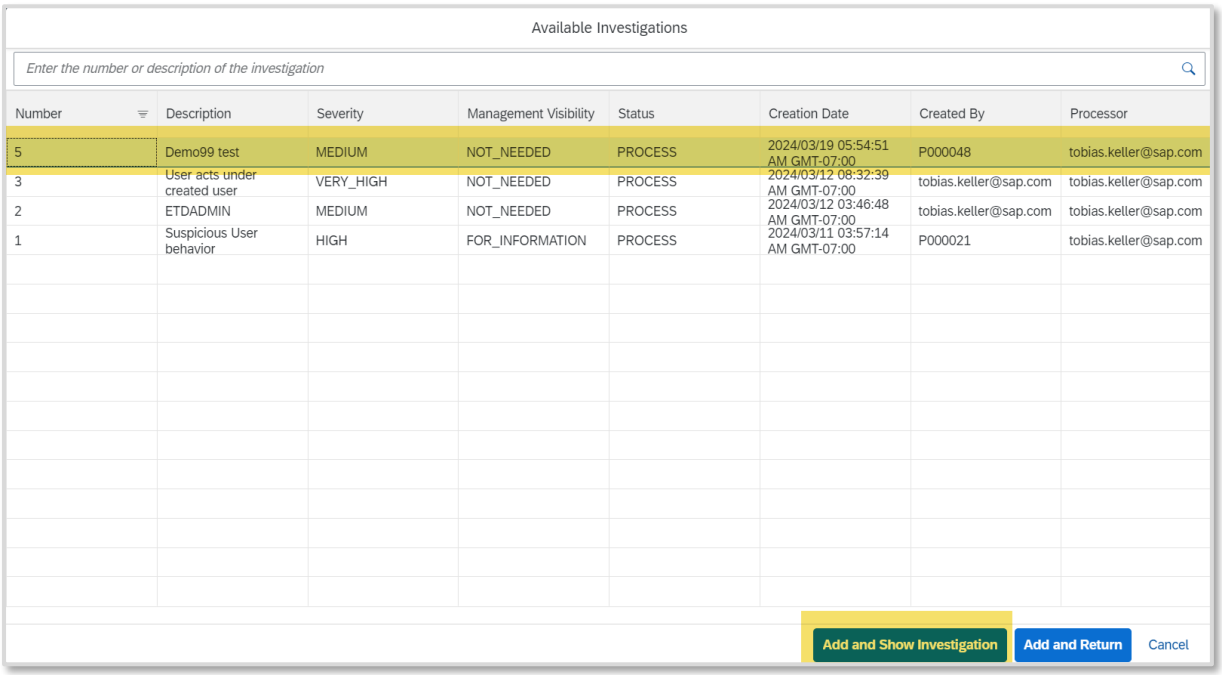
In the resulting screen, trigger the button “Execute” to run the pattern on the logs in the hot storage (evaluating past logs for the event happening), and generate Alerts.



- Finally, return to the Manage Alerts app. Filter for Alert(s) pertaining to your pattern xx_PWHashAttack. Have a look at the “trigger” field, detailing the resource and the user (pseudonym) responsible for creating the alert (if necessary, expand the text/field).
- Mark the alert(s), and add them to your Investigation:



In the following screen, press “Add and Show Investigation”:



7. Finalize the Investigation

You can now conclude the Investigation.

7.1 Optional: maintain your email ID to receive investigation reports

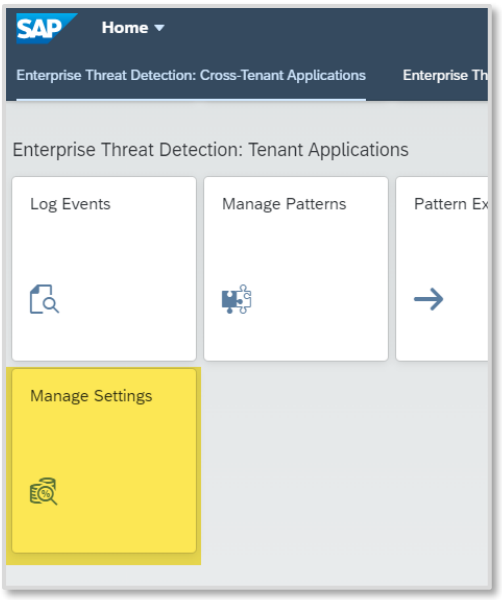
In SAP Enterprise Threat Detection, cloud edition, finalized and relevant investigations will result in reports generated and sent to the appropriate/responsible persons on customer/client side. You may maintain (and later delete) your mail address in order to receive such a notification including a link to the report.

Please note:

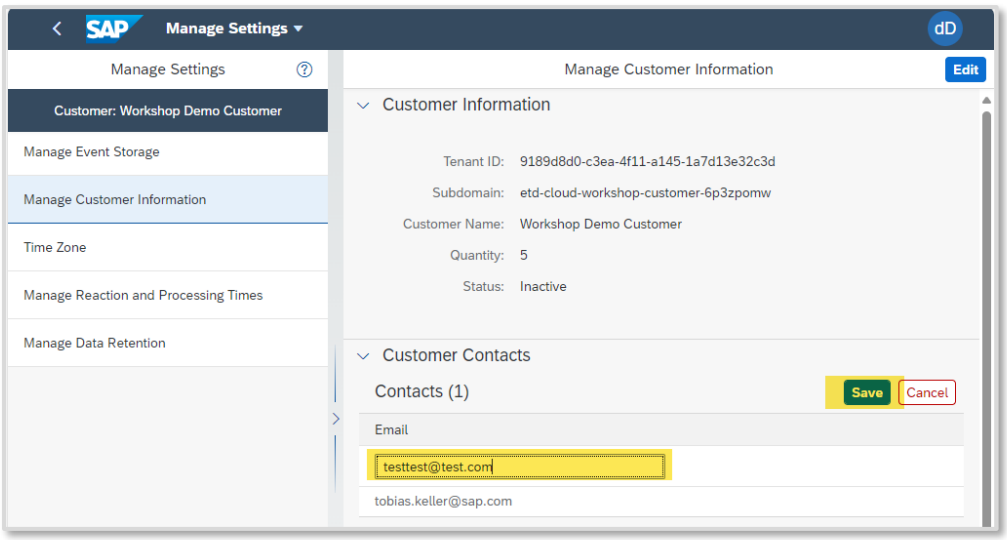
- You will not be able to access the link as your mail address is not linked to an account.
- If you choose to maintain your mail address, this will be visible to other workshop participants as well as the instructor
- You may receive multiple reports also from other workshop participants.

If you're not OK with this, please proceed to the next chapter.

In order to maintain your mail address, enter the app to "manage settings".

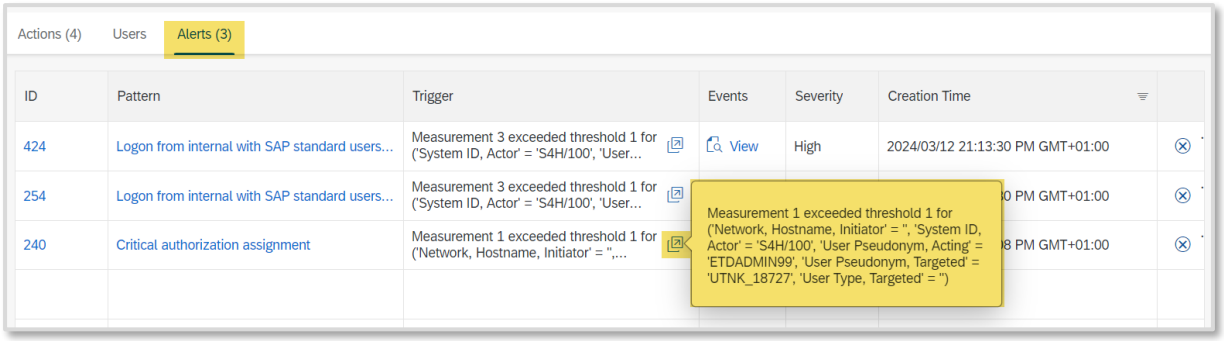


Here, navigate to "Manage Customer Notification", and in the "Customer Contacts" are, click "Add". Type your mail address and click on "Save":

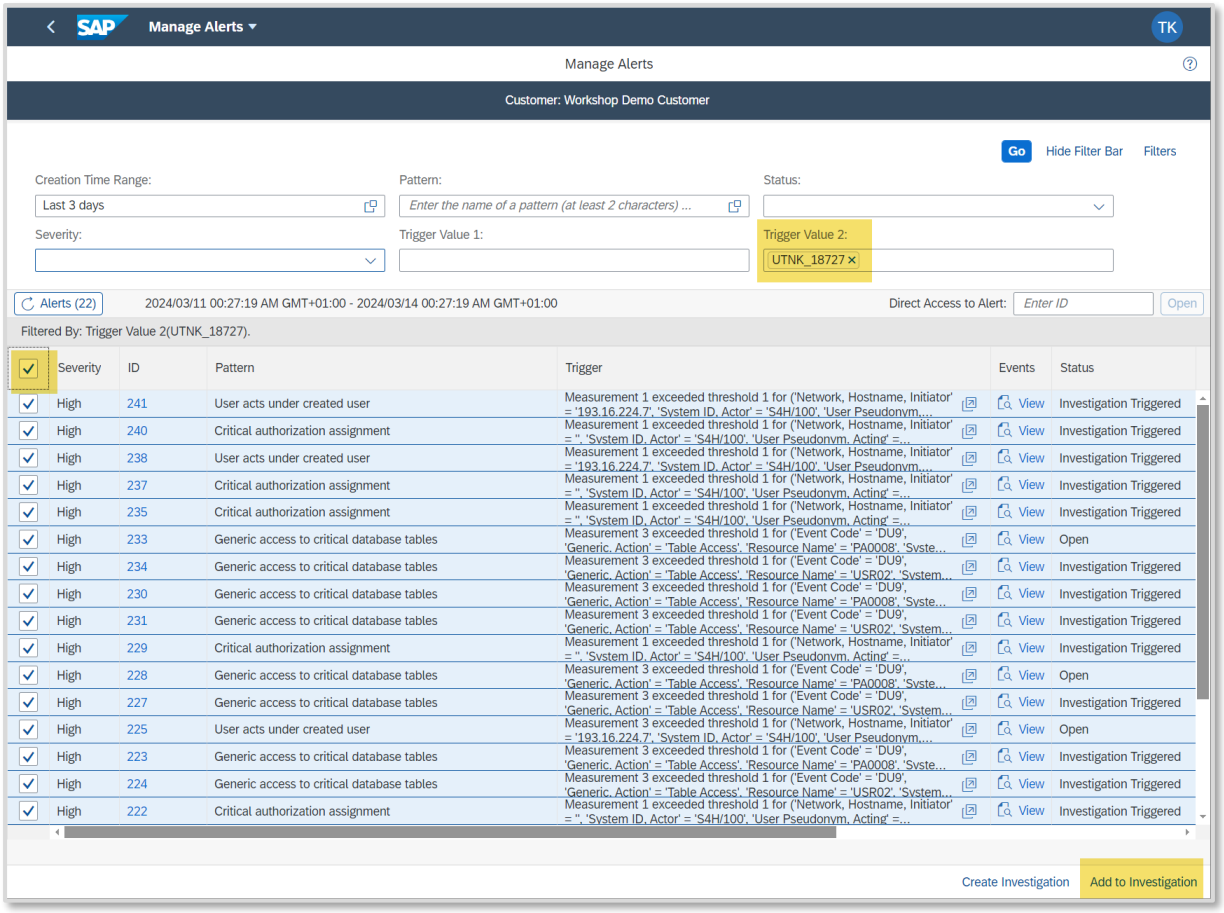


7.2 Finalize the investigation

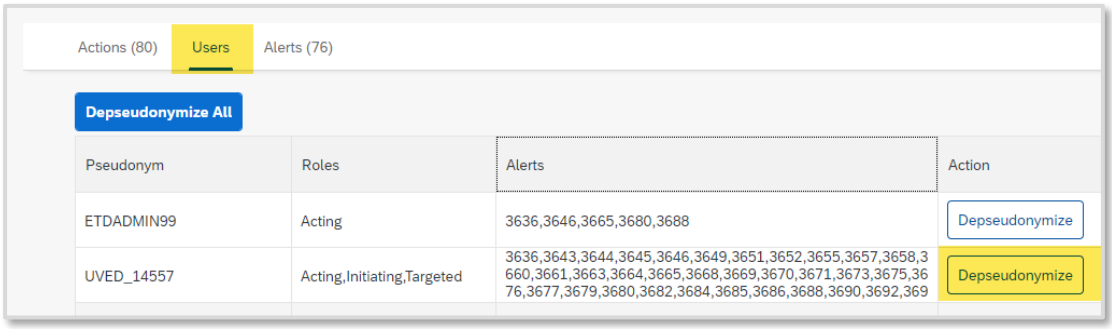
- In the app for “Manage Investigations”, you will find the header information you have maintained before and can edit. You may choose “edit” in case you desire to change the information.
- In the middle section, click on “Alerts”. Here, you can research the Alerts, have a look at some of the complete 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 may also come across additional user pseudonyms or references to IP addresses from where the triggering actions were initiated. These can be valuable leads to follow up on – If you have time left, you may note down the pseudonyms (or also users in clear) and IP addresses, return to the Manage Alerts app, search for more Alerts involving these pseudonyms, and add the results to your Investigation.

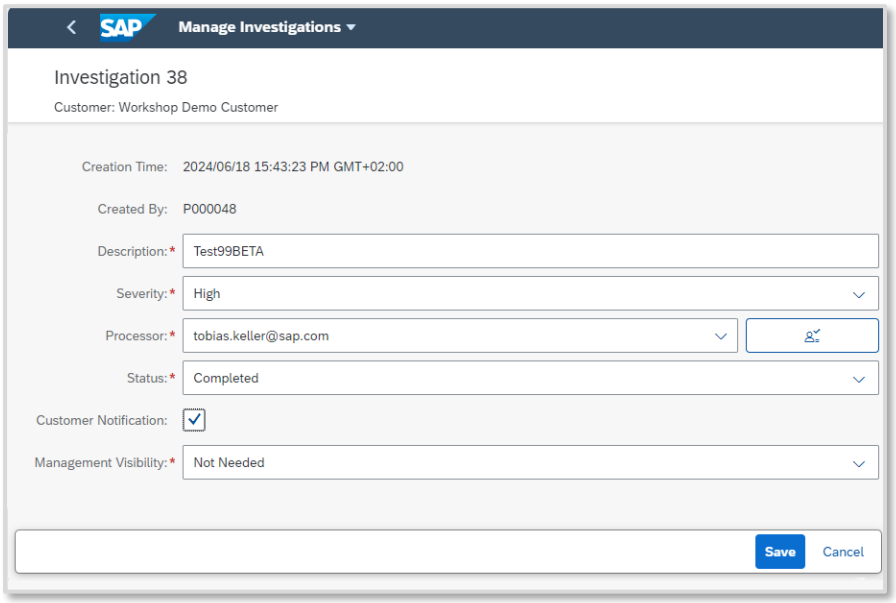


- Finally, return to your Investigation. You may comment/document what actions you have been performing, and what deductions these allow.
- Then return to the tab for “Users”. For each pseudonym, trigger the de-pseudonymization:



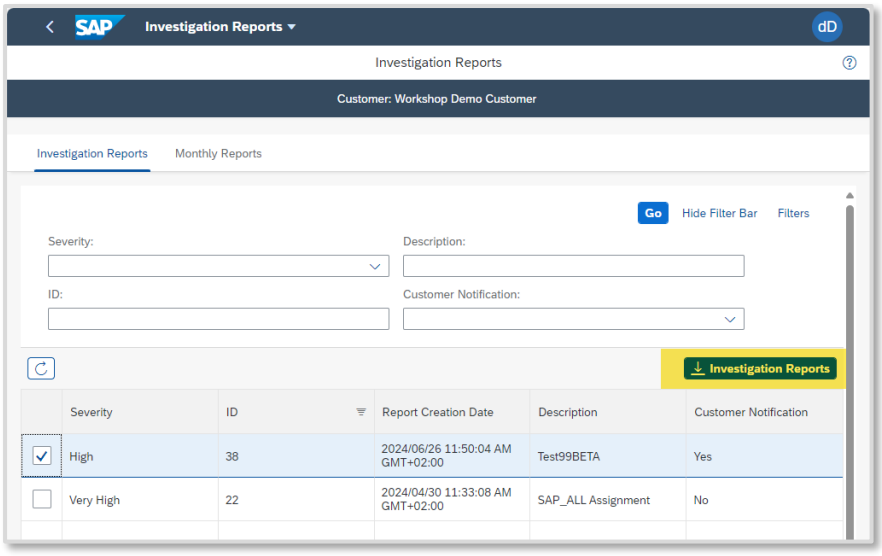
- This will reflect in the “Actions” tab – have a look at the clear user names. You should be spotting your ETDDEMO## somewhere!

- Lastly, finalize the Investigation. Click “Edit”, update the header information as needed, set status to “completed”, activate “Customer Notification”, and save.

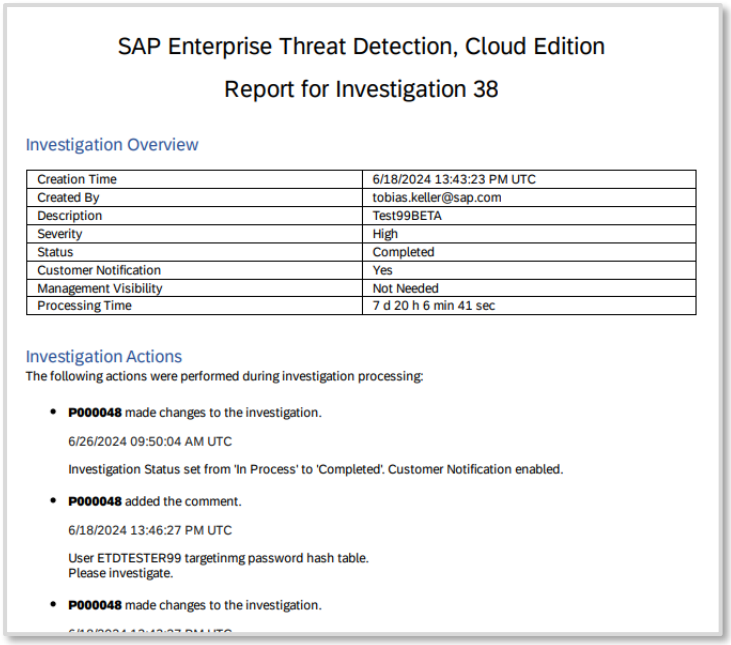


This closes the investigation, and no more changes are possible.

- At the same time, an Investigation Record is created (and a link sent via mail to the addresses maintained in chapter 7.1). This may take a couple of minutes.
- To retrieve and check the record, return to the Home screen and enter the app “Investigation Reports”. Retrieve and you’re your investigation, and download the report.



- After downloading to the local machine, have a look at your first Investigation Record with SAP Enterprise Threat Detection, cloud edition!



SAP Enterprise Threat Detection, Cloud Edition

Report for Investigation 38

Investigation Overview

Creation Time	6/18/2024 13:43:23 PM UTC
Created By	tobias.keller@sap.com
Description	Test99BETA
Severity	High
Status	Completed
Customer Notification	Yes
Management Visibility	Not Needed
Processing Time	7 d 20 h 6 min 41 sec

Investigation Actions

The following actions were performed during investigation processing:

- **P000048** made changes to the investigation.

  6/26/2024 09:50:04 AM UTC

  Investigation Status set from 'In Process' to 'Completed'. Customer Notification enabled.

- **P000048** added the comment.

  6/18/2024 13:46:27 PM UTC

  User ETDTESTER99 targetinmg password hash table.
  Please investigate.

- **P000048** made changes to the investigation.

This concludes the *SAP Enterprise Threat Detection, public cloud* part of the threat countering process. The further proceedings would now be in the hands of the customer proper, who may involve their security team to take action on the system users and physical persons behind them.

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