

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
1.2 UI Round trip	7
2. First Log Events from SAP S/4HANA	7
2.1 Logon & Preparation Steps.....	7
2.2 Creating a User With High Privileges.....	Error! Bookmark not defined.
3. Checking Alerts and Creating Investigations.....	7
3.1 Check for Log Events.....	7
3.2 Search for Alerts	7
3.3 Interpreting the Investigation Entries	7
4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table.....	7
5. User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab	7
5.1 Build up a Workspace	8
5.1.1 Assigning a Chart.....	16
6. From Workspace to Pattern to Alerts.....	18
6.1 Understanding Patterns	18
7. Finalize the Investigation	21
7.1 Information: Maintain your email ID to receive investigation reports	21
7.2 Finalize the investigation.....	22
8. Consumer/Processor role: Work with Investigation reports.....	24

Overview & Touring SAP Enterprise Threat Detection, public cloud

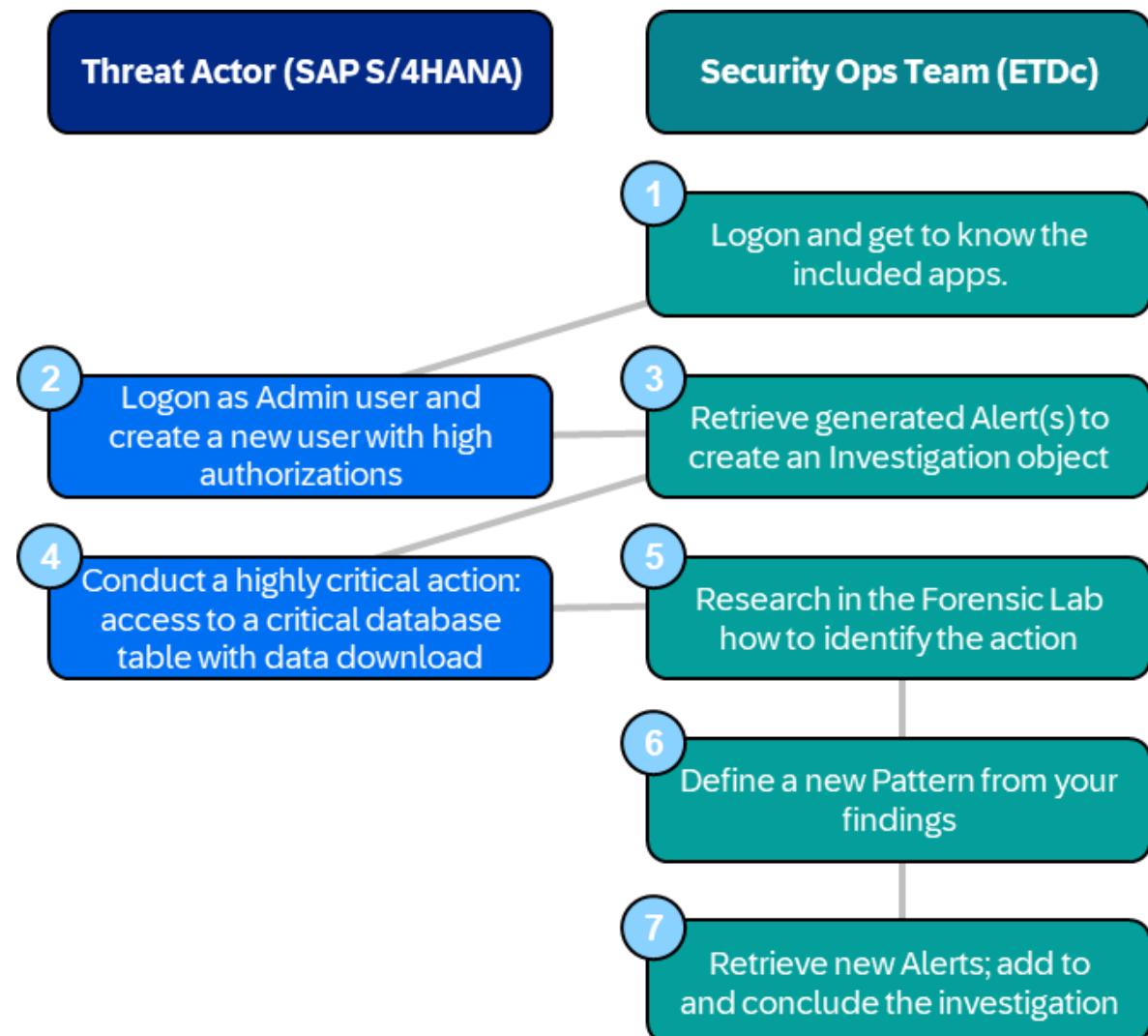
In this hands-on session and workshop of about 1.5 – 2h, you will get to know the basic functioning of *SAP Enterprise Threat Detection, public cloud*, including the terminology employed.

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 two 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.

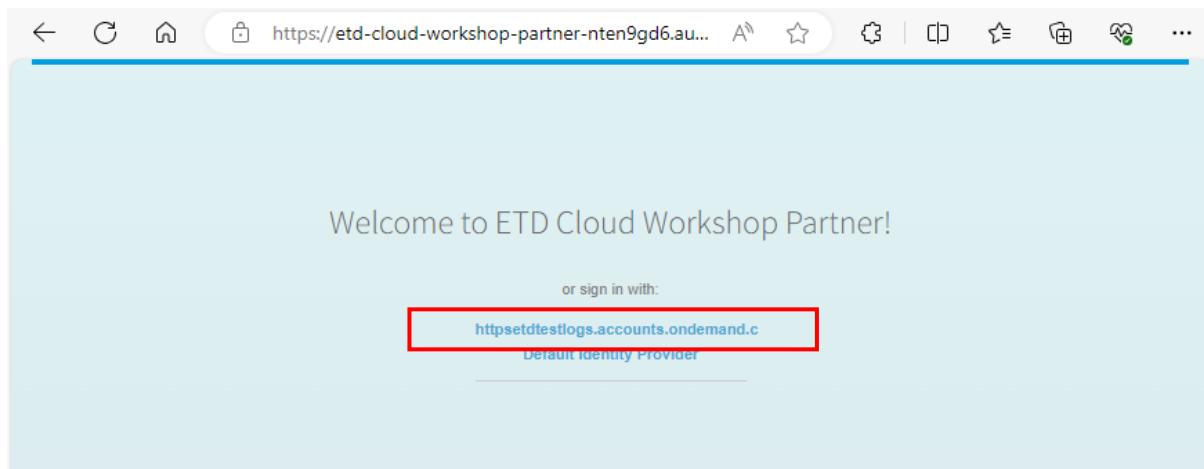
Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

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 ("https://etd-testlogs.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 a 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".

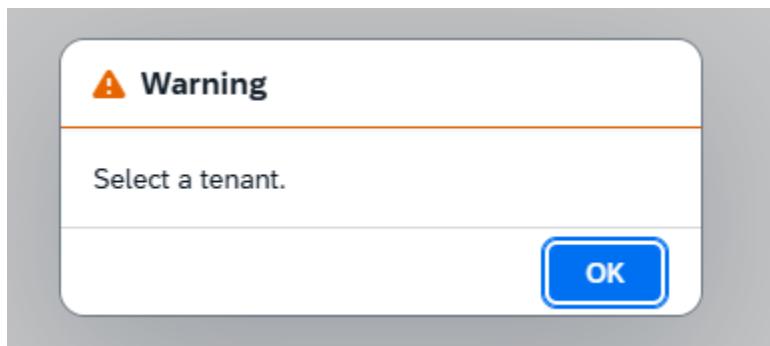
The screenshot shows a SAP web application interface titled "Select Tenant". At the top, there are input fields for "Customer Name" and "Status" (set to "Inactive"), and dropdowns for "Subdomain" and "Tenant ID". Below these are filter buttons and a "Go" button. A table below lists a single tenant entry: "Workshop Demo Customer" with status "Inactive", subdomain "etd-cloud-workshop-customer-6p3zpomw", and tenant ID "9189d8d0-c3ea-4f11-a145-1a7d13e32c3d".

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.

The screenshot shows the SAP Enterprise Threat Detection monitoring console. The top navigation bar includes "Home", "Enterprise Threat Detection: Cross-Tenant Applications", and "Enterprise Threat Detection: Tenant Applications". The main area features several cards: "Select Tenant" (with a cursor icon), "Manage Alerts for All Tenants" (with a warning icon), "Manage Investigations for All Tenants" (with a magnifying glass icon). Below these are two rows of six cards each under "Enterprise Threat Detection: Tenant Applications": Row 1 includes "Manage Settings" (camera icon), "Manage Value Lists" (grid icon), "Analyze Log Events" (magnifying glass icon), "Manage Alerts" (warning icon), "Monitor Pattern Executions" (right arrow icon), and "Manage Patterns" (puzzle piece icon). Row 2 includes "Manage Investigations" (document icon), "Record of Actions" (document icon), "Download Investigation Reports" (document icon), "Forensic Lab" (binoculars icon), "Monitor Incoming Logs" (log icon), and "Resolve User Identity" (person icon).

1.1 Got a Warning ‘Select a Tenant’

If you encounter a the warning popup

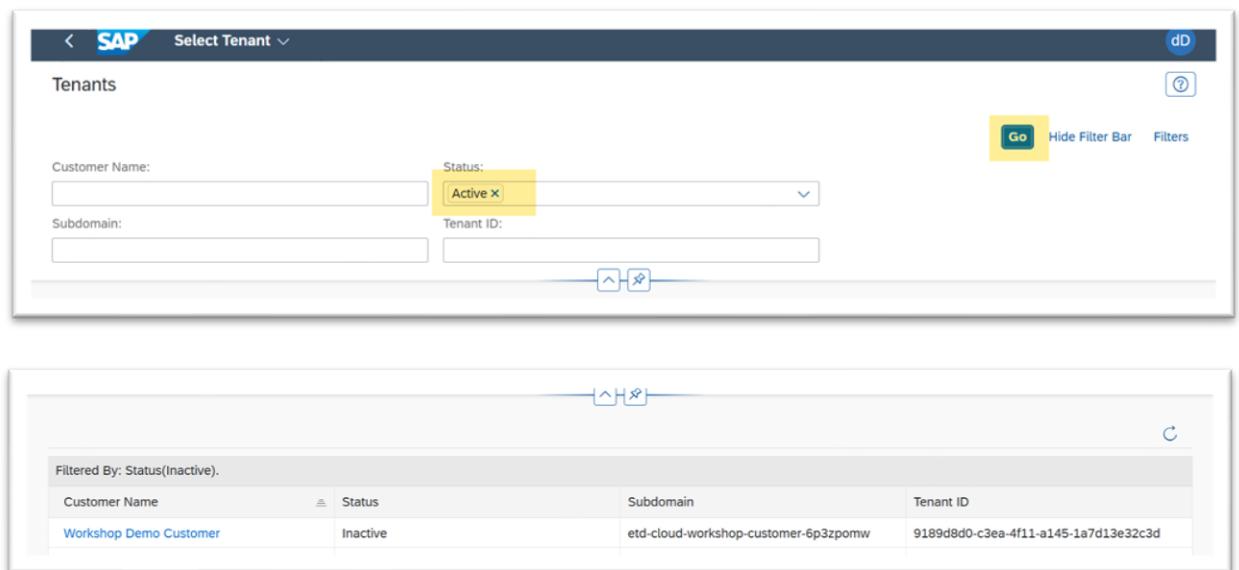


the system has lost the information which Tenant you've been working on (most likely you had been logged out).

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)



Customer Name	Status	Subdomain	Tenant ID
Workshop Demo Customer	Inactive	etd-cloud-workshop-customer-6p3zpmow	9189d8d0-c3ea-4f11-a145-1a7d13e32c3d

1.2 UI Round trip

2. First Log Events from SAP S/4HANA

2.1 Logon & Preparation Steps

3. Checking Alerts and Creating Investigations

3.1 Check for Log Events

3.2 Search for Alerts

3.3 Interpreting the Investigation Entries

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

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

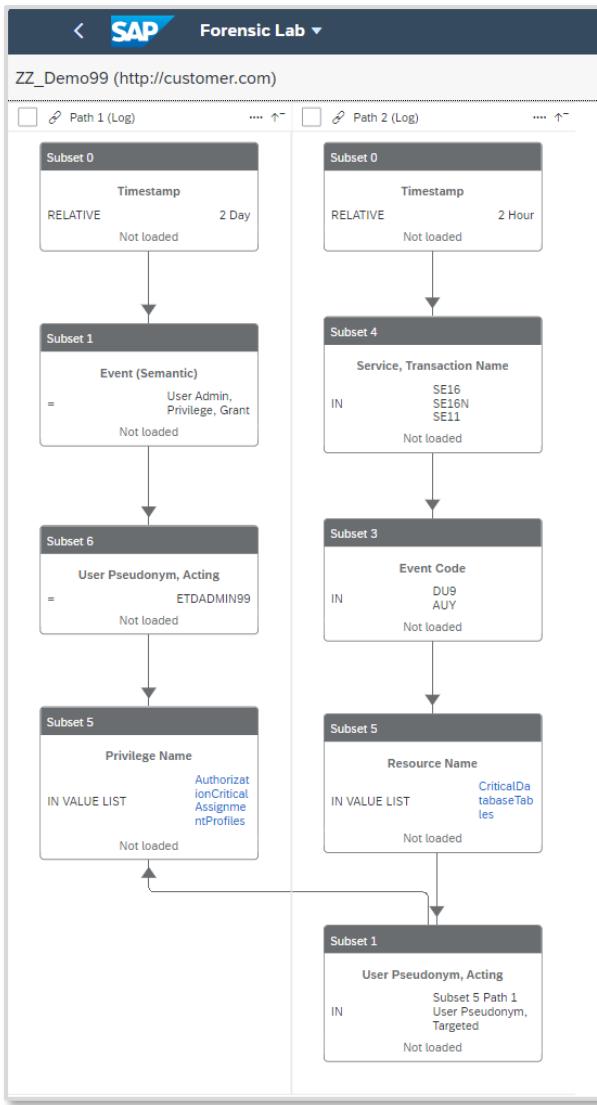
The Forensic Lab is the area where you work on ways to identify new potential threat vectors by filtering your way through the large volume of log entries until you arrive at a definition yielding few and specific logs that should point at a real threat.

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”.



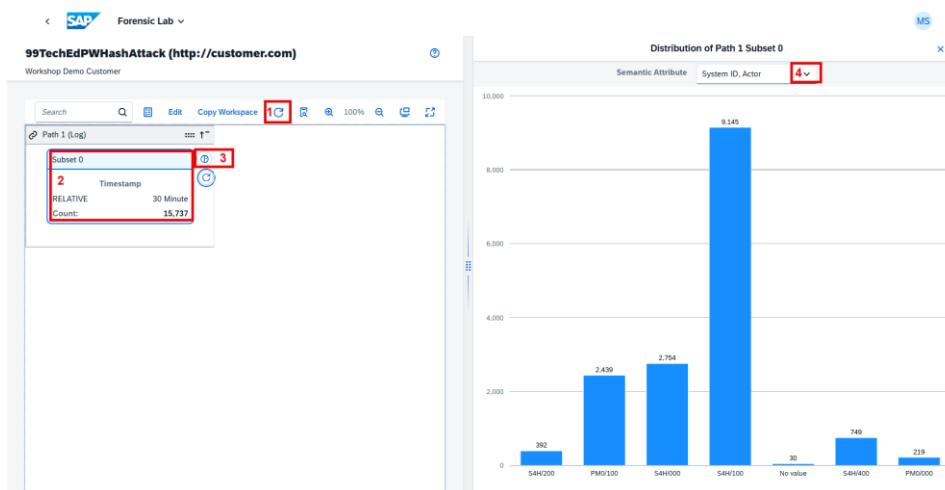
- In the area “Custom Workspaces”, you see a list of existing workspaces.
- Create a new Workspace with Name ##TechEdPWHAttack, by replacing the ## with your participant number. Enter some additional information (Use case, Severity, Description), and then click on ‘Create’

The screenshot shows the SAP Workspaces interface. On the left, there's a list of 'Workspaces (21)'. In the center, a modal window titled 'Create Workspace' is open. The 'Name' field contains '<YourNumber>TechEdPWHashAttack' (highlighted with a red box). The 'Namespace' field is set to 'http://customer.com'. The 'Use Case' field contains 'Admin creates a new user with which they attack passwords hashes.' The 'Risk Classification' dropdown is set to 'High'. The 'Description' field is empty. At the bottom right of the modal, there are 'Create' and 'Close' buttons, with 'Create' highlighted with a blue box. To the right of the modal, there's a table for 'Process Status' and 'Editing Status' with several rows. A red box highlights the 'Create Workspace' button in the top right corner of the main interface.

- You then see your new Workspace in the Workspace list. To open it, click on the arrow on the right for your Workspace.

The screenshot shows the SAP Workspaces interface after creating a new workspace. The 'Workspaces (22)' list now includes a new entry: '99TechEdPWHashAttack' with 'http://customer.com' as the namespace. The 'Use Case' column shows 'Admin creates a new user with which they attack passwords hashes.' To the right of the workspace name, there's a blue arrow symbol (highlighted with a red box) indicating it can be expanded.

- Your new workspace contains already a first Filter Path (Path 1) with a subset (Subset 0) to filter on the time range.
- Click on the 'Refresh' Button to see incoming log data.
- Click into the Subset 0, to get some Symbols at the right
- Click into the Pi-Chart Symbol to view the data in a chart preview. You see as a default the distribution of log events, related to their systems
- By clicking on the Drop-Down-Symbol, you can select other attributes of the ETD normalized Data Model



By e.g. selecting 'Event (Semantic)' you get a distribution of all log events, related to the Semantic Events.



- By clicking the 'Edit' Button , you start modelling your workspace. You see now some additional Symbols at the right of your Subset 0.
- Change the relative Timestamp of Subset 0 to 2 hours by clicking on the symbol 'Edit Subset'



Change Subset 0 Path 1

Semantic Attribute: * 

Value: * 

Select Time Range

Last Hours 

From  Local Time

To  Local Time

Change Subset 0 Path 1

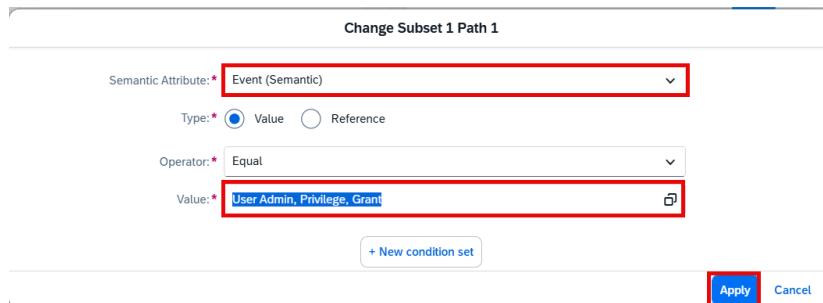
Semantic Attribute: * 

Value: * 

Subset 0	
Timestamp	
RELATIVE	2 Hour
Not loaded	

Information: To be able to see some data in the following filter steps, directly before the session started, all ETDADMIN## users in the S4/H system got a mass change by adding a high privilege.

- By clicking on the ‘Create Subset’  Symbol, a Popup appears to enter the filter criteria for the next subset. Please enter:
 - Semantic Attribute: Event (Semantic)
 - Type: Value
 - Operator: Equal
 - Value: User Admin, Privilege, Grant
- Then click ‘Apply’.

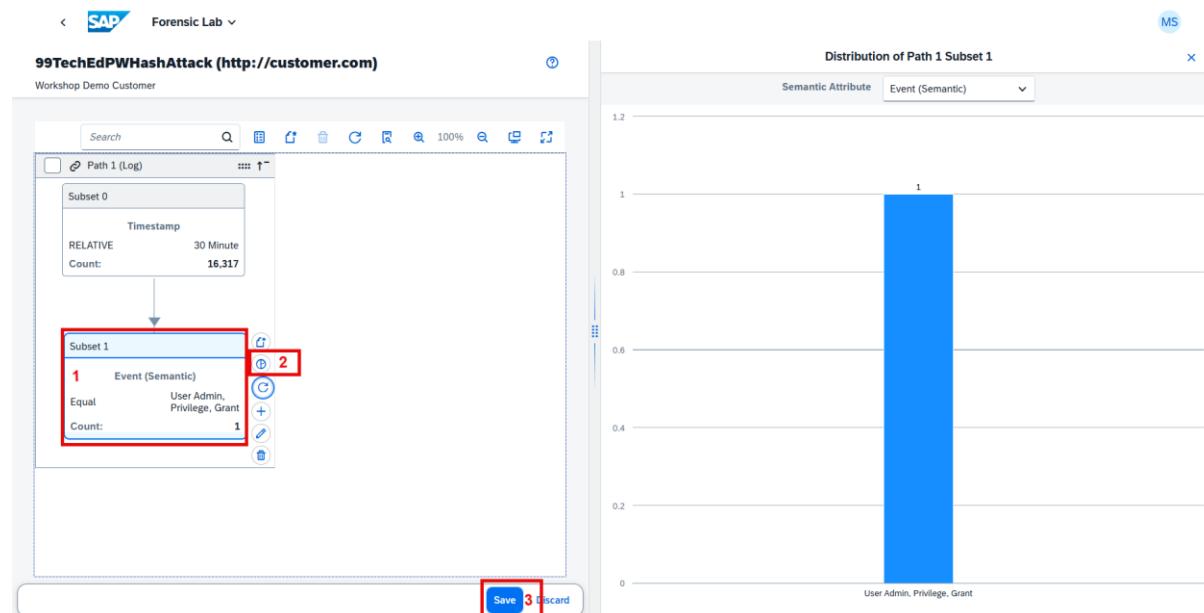


The screenshot shows the 'Change Subset 1 Path 1' dialog box. It contains the following fields:

- Semantic Attribute: * **Event (Semantic)**
- Type: * Value Reference
- Operator: * Equal
- Value: * **User Admin, Privilege, Grant**

 At the bottom right are 'Apply' and 'Cancel' buttons, with 'Apply' being highlighted with a red box.

- Your new Filter Subset ‘Subset 1’ appears. By clicking into the Subset 1, you can use the small symbols at the side (especially the Pie-Chart Symbol) to do a preview on the data filtered in Subset 1 in the Preview area.
- Sometimes click on the ‘Save’ Button



- Create a new Subset  to filter (for Demo Purposes) on your own ABAP User ETDADMIN<YourNumber>. In the Popup enter:
 - Semantic Attribute: User Pseudonym, Target
 - Type: Value

- Operator: Equal
- Value: ETDADMIN<YourNumber>
- Then click on 'Create'

Change Subset 2 Path 1

Semantic Attribute: * User Pseudonym, Target

Type: * Value Reference

Operator: * Equal

Value: * ETDADMIN<YourNumber>

+ New condition set Apply Cancel

- You new Subset is showing as 'Subset 2'. By refreshing and selecting the Pie Chart you can see some data in Subset 2.

Information: ETD provides a role concept about users, systems, IP addresses, etc. An 'Acting User' is a user, who does something. A 'Target User' is e.g. a user, to whom something is done.

- Create a new Subset with the following values:
 - Semantic Attribute: Privilege Name
 - Type: Value
 - Operator: In value list
 - Value: AuthorizationCriticalAssignmentProfiles
- Then click on 'Create'

Create Subset

Semantic Attribute: * Privilege Name

Type: * Value Reference

Operator: * In value list

Value List Name: * AuthorizationCriticalAssignmentProfiles

+ New condition set Create Cancel

- You new Subset is showing as 'Subset 3'. By refreshing and selecting the Pie Chart you can see some data in Subset 3.

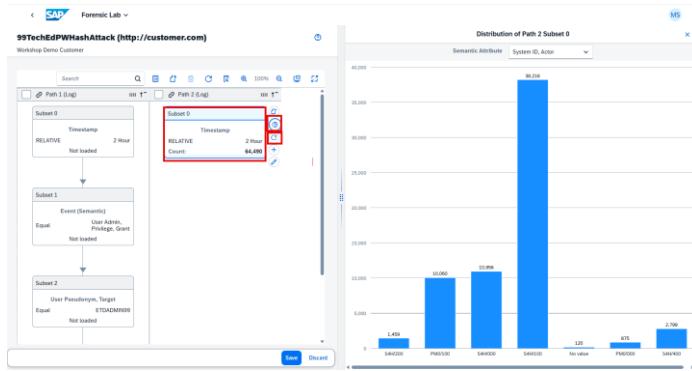
Information: The value list AuthorizationCriticalAssignmentProfiles contains typical predelivered values for Profiles (e.g. SAP_ALL, SAP_NEW, ...). The filter is then set as an 'IN'-filter about all values.

To be able to corelate the provisioning of a high privilege with the miss-use of the privilege (in the example: look up Password hashes), a second filter path needs to filter on that activity, and then corelate to the high privilege provisioning (via reference filter).

- Click the 'Create Path' Symbol

The screenshot shows the SAP Forensic Lab interface with a path configuration window. The path is named 'Path 1 (Log)' and contains a single subset named 'Subset 0'. The subset has a timestamp filter set to 'RELATIVE' with a value of '2 Hour' and 'Not loaded'. The toolbar at the top includes a 'Save' icon, which is highlighted with a red box.

- Select the Context 'Log' and 'save'. Your second filter path 'Path 2' is created and already contains a timestamp filter in Subset 0.
- Again, change the timestamp filter to Last 2 hours (to be able to see some data). Then you can click the 'Refresh' symbol and the 'Pie-Chart' symbol to see the data of Path2, Subset 0.



- Create a new Subset with the following values:
 - Semantic Attribute: Service, Transaction Name
 - Type: Value
 - Operator: In
 - Value: SE16, SE16N, SE11
 - i. **Hint:** To enter the In-Value List, enter the 1st value, then press 'Enter', then enter the 2nd/next value and always press 'Enter' in between. The single values are shown separately.
- Then click on 'Create'

The screenshot shows the 'Create Subset' dialog box. The fields are filled as follows:

- Semantic Attribute: Service, Transaction Name
- Type: Value
- Operator: In
- Value: SE16, SE16N, SE11

 The 'Create' button at the bottom is highlighted with a blue box.

- Your new Subset is showing as 'Subset 1' in Path 2. By refreshing and selecting the Pie Chart you can see some data in Subset 1.
- Create a new Subset with the following values:
 - Semantic Attribute: Event (Semantic)
 - Type: Value
 - Operator: In
 - Value: Data, Download ; Database, Data, Select, Generic

- i. **Hint:** To enter the In-Value List, enter the 1st value, then press ‘Enter’, then enter the 2nd/next value and always press ‘Enter’ in between. The single values are shown separately. You can as well check if the Semantic events are visible in the selection box, then you can select them via checkboxes

- Then click on ‘Create’

Semantic Attribute: * Event (Semantic)

Type: * Value Reference

Operator: * In

Value: * Data, Download Database, Data, Select, Generic

+ New condition set

Create Cancel

- Your new Subset is showing as ‘Subset 2’ in Path 2. By refreshing and selecting the Pie Chart you can see some data in Subset 2.
- Create a new Subset with the following values:
 - Semantic Attribute: Resource Name
 - Type: Value
 - Operator: In value list
 - Value: CriticalDatabaseTables
 - i. Hint: The Attribute ‘Resource Name’ contains objects (like DB tables, files) from where/to which data is read/written
- Then click on ‘Create’

Semantic Attribute: * Resource Name

Type: * Value Reference

Operator: * In value list

Value List Name: * CriticalDatabaseTables

+ New condition set

Create Cancel

- Your new Subset is showing as ‘Subset 3’ in Path 2. By refreshing and selecting the Pie Chart you can see some data in Subset 3.
- Finally, create a Subset, which correlates between Path 1 filter results for provisioning of high privileges to a **target** user, and path 2 results for the same **acting** user accessing a critical DB table with Password hashes. Use the following values:
 - Semantic Attribute: User Pseudonym, Acting
 - Type: Reference
 - Operator: In
 - Reference To: Subset 3, Path 1
 - Value: User Pseudonym, Target
- Then click on ‘Create’

Create Subset

Semantic Attribute: * User Pseudonym, Acting

Type: Value Reference

Operator: * In

Reference To: * Subset 3 Path 1

Semantic Attribute: * User Pseudonym, Target

+ New condition set

Create Cancel

The screenshot shows a 'Create Subset' dialog box. It has several input fields:

- Semantic Attribute: * User Pseudonym, Acting
- Type: Value Reference
- Operator: * In
- Reference To: * Subset 3 Path 1
- Semantic Attribute: * User Pseudonym, Target

At the bottom right are 'Create' and 'Cancel' buttons.

- Your new Subset is showing as 'Subset 4' in Path 2. By refreshing and selecting the Pie Chart you can see some data in Subset 4. Data can be seen if within last 2 hours the user got a high privilege, and in the same timeframe accessed a critical DB table.

The final result should look like this:



5.1.1 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 4, Path 2. Then press “Create Chart”:



In the pop-up, assign a name among the lines of “<YourNumber>PWHashAttack”, and a description. Mark down the name.

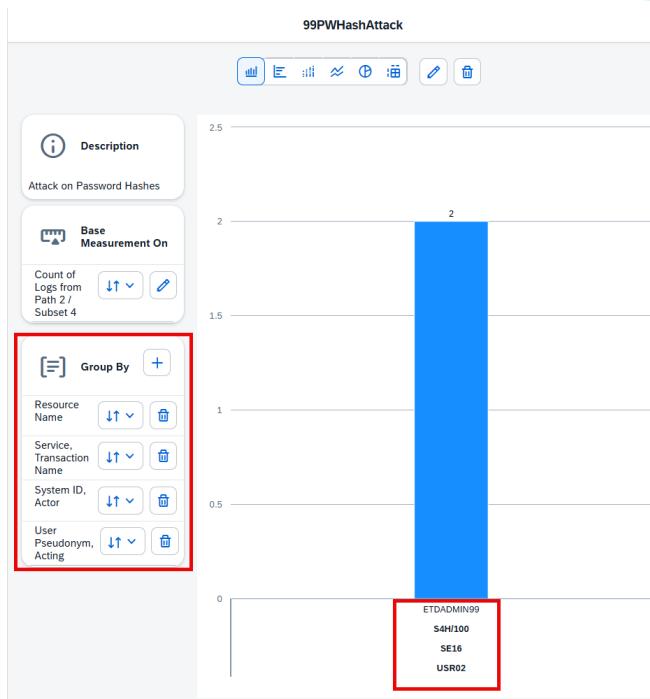
For measurement, choose the “count” * and a fitting Display Name if you like:

The screenshot shows the "Create Chart" dialog box. It has sections for "Chart" and "Measurement". In the "Chart" section, the "Name" field contains "<YourNumber>PWHashAttack" and the "Description" field contains "Attack on Password Hashes". In the "Measurement" section, the "Definition" dropdown is set to "Count" and the "Display Name" field contains "Count of Logs from Path 2 / Subset 4". At the bottom right are "Create" and "Cancel" buttons.

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

- Resource Name
- Service, Transaction Name
- System ID, Actor
- User Pseudonym, Acting

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):



- Finally, click the 'Save' Button

Note: Per each deviating combination of the (in this example) 4 grouped attributes, there would arrive another bar in the bar chart.

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 screenshot shows the SAP Manage Patterns interface with the following details:

- General** section:
 - Name: * 99_PWHashAttack
 - Namespace: * http://customer.com
 - Description: * Fake user accessing PW Hashes
- Chart and Execution** section:
 - Chart: * 99_PWHashAttack
 - Execution Type: * Scheduled
 - Execution Output: Alert
- Configuration** section:
 - Status: Active
 - Frequency: * 5 Minutes
 - Threshold Operator: >=
 - Threshold: * 1
 - Severity: Very High
 - Test Mode:
- Credibility of Attack Detection** section:
 - Likelihood Confidentiality: N/A
 - Likelihood Integrity System: * N/A
 - Likelihood Integrity Data: * N/A
 - Likelihood Availability: * N/A
- Success of Attack** section:
 - Success Confidentiality: * N/A
 - Success Integrity System: N/A
 - Success Integrity Data: * N/A
 - Success Availability: * N/A

At the bottom right are the **Save** and **Cancel** buttons.

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.

Information: If you mark the checkbox ‘Test Mode’, then alerts will as well be created, and be visible in the alert list, but they will be in status ‘Test Mode’ and can be deleted later-on. Reasoning is, that in ‘Test Mode’, the Pattern is still reworked, until it functions properly, and does not create too many false positives. Later, the marker can be removed, and from that time on, the alerts cannot be deleted any more, as they are now seen as real alerts, and deletion might cause compliance issues.

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.

The screenshot shows the SAP Manage Patterns interface. At the top, it says "Manage Patterns" and "Pattern Generic access to critical database tables". Below that, it says "Customer: Workshop Demo Customer". There are buttons for "Execute", "Edit", and a help icon. The main area has tabs for "Details", "Used Value Lists", and "Postprocessing Work Items". Under "Details", there are sections for "General" and "Administration". The "General" section includes fields for Name (Generic access to critical database tables), Namespace (http://sap.com/secmon/basis), and Description (Issue an alert when client gets access to critical database tables). The "Administration" section shows Created By: SAP, Created At: 2018/12/31 16:00:00 PM GMT-08:00, and other details like Changed By and Changed At. Below these are sections for "Chart and Execution" and "Configuration". The "Chart and Execution" section shows details like Namespace of Chart Workspace (http://sap.com/secmon/basis), Name of Chart (Data Manipulation), and various execution parameters. The "Configuration" section shows Status: Active, Frequency: 5 Minutes, and threshold settings. A yellow box highlights the "Chart and Execution" section.

- 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).

Your Alert looks like this:

The screenshot shows the SAP Manage Alerts interface. At the top, it says "Alerts (Workshop Demo Customer)". Below that, there are filters for Creation Time Range (Last 1 day), Pattern (Enter the name of a pattern (at least 2 characters)), Status, Severity, Trigger Value 1, and Trigger Value 2. The main area shows a table of alerts with columns for Severity, ID, Pattern, and Trigger. One alert is selected, and its trigger details are expanded in a red box. The trigger details show Measurement 2 exceeded threshold 1 for (Resource Name = 'USR02', Service, Transaction Name = 'SE16', System ID, Actor = 'S4H100...'). Measurement 1 exceeded threshold 1 for (Event (Semantic) = 'User, Logon', Network, Hostname, Initiator = '10.0.0.7', System ID, Actor = '...', Measurement 1 exceeded threshold 1 for (Event (Semantic) = 'User, Logon Failure', Network, Hostname, Initiator = '1n 70 RG 1n', System ID, Actor = '...', and Measurement 2 exceeded threshold 1 for (Resource Name = 'USR02', Service, Transaction Name = 'SE16', System ID, Actor = 'S4H100...', User Pseudonym, Acting = 'UNKN_18727'). The time for this trigger is listed as 10/20 13:44.

- 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 Information: 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. It is possible to maintain a mail address to receive information about a newly created report, if the checkbox ‘Customer notification’ is marked within the Investigation during processing. The mail address can be maintained within the ‘Manage Settings’ Tile.

Please note:

- Please don't exchange the mail address, neither to an own one, nor to another one, although you might have the authorization. It results in receiving multiple reports also from other workshop participants to the maintained mail address.

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.

Actions (4) Users Alerts (3)						
ID	Pattern	Trigger	Events	Severity	Creation Time	
424	Logon from internal with SAP standard users...	Measurement 3 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User...)			High	2024/03/12 21:13:30 PM GMT+01:00
254	Logon from internal with SAP standard users...	Measurement 3 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User...)			0 PM GMT+01:00	
240	Critical authorization assignment	Measurement 1 exceeded threshold 1 for ('Network, Hostname, Initiator' = ..., 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'ETDADMIN99', 'User Pseudonym, Targeted' = 'UTNK_18727', 'User Type, Targeted' = '')			8 PM GMT+01:00	

- 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.

The screenshot shows the SAP Manage Alerts interface. At the top, there's a search bar with 'Pattern:' and 'Status:' fields, and a dropdown for 'Severity'. Below the search bar, there's a table header with columns: Severity, ID, Pattern, Trigger, Events, and Status. The 'Severity' column is highlighted with a yellow box. The main table body contains 22 rows of alert data, each with a checkbox in the first column. The 'Trigger' column for the first row shows a complex measurement threshold. At the bottom right of the table area, there are buttons for 'Create Investigation' and 'Add to 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:

The screenshot shows the SAP Users interface. At the top, there are tabs for 'Actions (80)', 'Users' (which is selected), and 'Alerts (76)'. Below the tabs is a table with columns: Pseudonym, Roles, and Alerts. The first two rows are highlighted with yellow boxes. The 'Alerts' column for the second row lists several alert IDs. To the right of the table is an 'Action' column with two buttons: 'Depseudonymize' for each row.

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

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

The screenshot shows the SAP Manage Investigations interface. At the top, it says "Investigation 38" and "Customer: Workshop Demo Customer". Below that, there are several input fields:

- Description:** Test99BETA
- Severity:** High
- Processor:** tobias.keller@sap.com
- Status:** Completed
- Customer Notification:**
- Management Visibility:** Not Needed

 At the bottom right of the form are "Save" and "Cancel" buttons.

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.

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 investigations report processor(s) (see next chapter), who may involve their security team to take action on the system users and physical persons behind them.

8. Consumer/Processor role: Work with Investigation reports

This exercise is Demo only!

You are now switching to your 3rd role as consumer/processor of the final product, the investigation report.

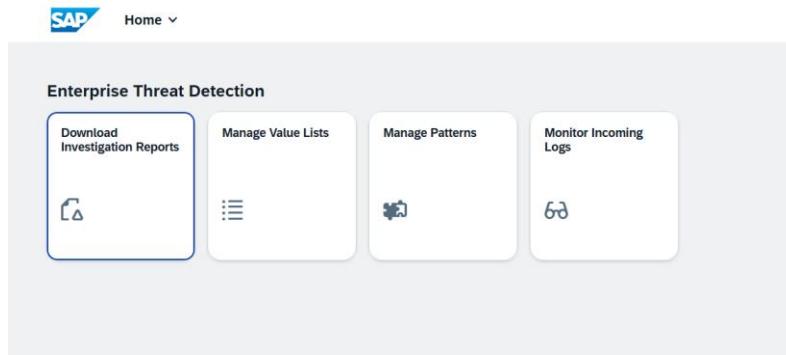
Logon to the consumer view of SAP Enterprise Threat Detection, cloud edition .

Use the ID indicated to you (01-35; afterwards referred to as “##”)

User: teched##@etdsap.com

Password: will be provided in the session

You see the starting page for the consumer/processor role. It contains some view-only tiles, provided for corresponding transparency, if the analysis is provided by a service. The processor role does hence not see the analysis tiles.

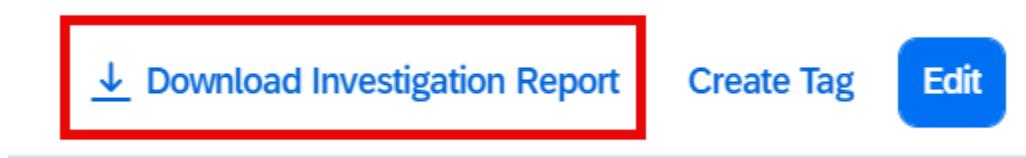


Click on Tile 'Download Investigation Reports'

In the opening list UI, find your investigation (i.e. with your description), provided by you in your role as a security analyst.

Severity	ID	Report Creation Date	Description	Customer Notification	Completion Timestamp	Investigator	Report Status	Report Severity	Closing Remarks	Tags	
<input type="checkbox"/> High	142	2025/09/29 11:23:00 AM GMT+02:00	teched99B	No	2025/09/29 11:23:58 AM GMT+02:00	teched99	Open	High		>	
<input type="checkbox"/> High	141	2025/09/26 14:11:51 PM GMT+02:00	Sensitive Data download	No	2025/09/26 14:20:01 PM GMT+02:00	teched99	In Process	Medium	LOBA	>	
<input type="checkbox"/> High	140	2025/09/26 10:18:28 AM GMT+02:00	Critical Data Download	No	2025/09/26 10:27:05 AM GMT+02:00	teched99	Open	Medium		>	
<input type="checkbox"/> High	138	2025/09/25 21:57:56 PM GMT+02:00	Critical Data download	No	2025/09/25 22:12:46 PM GMT+02:00	(Unassigned User)	Open			>	
<input type="checkbox"/> High	133	2025/09/22 17:13:32 PM GMT+02:00	USER is doing critical business manipulation	No	2025/09/22 17:15:04 PM GMT+02:00	(Unassigned User)	Open			>	
<input type="checkbox"/> High	132	2025/09/15 16:22:38 PM GMT+02:00	Standard User Manual Logon from different systems	No	2025/09/15 16:23:32 PM GMT+02:00	teched99	In Process	Medium	remark 1	LOB1	>
<input type="checkbox"/> Medium	131	2025/09/11 17:36:59 PM GMT+02:00	Critical access abc Test	No	2025/09/11 17:37:58 PM GMT+02:00	teched99	No Reaction Needed		False positive, see ticket 423		>

By clicking on the small arrow, the Details-UI opens. By using the 'Download Investigation Report', a PDF document is downloaded. It contains all evidences (recommendations, comments, Alerts, triggering events)



An example report looks like:

SAP Enterprise Threat Detection, Cloud Edition

Report for Investigation 38

Investigation Overview

Creation Time	6/18/2024 13:43:23 PM UTC
Created By	teched99
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.

The Download activity can be seen in the 'Download History' Section

Comments (0)	Download History				
	<table border="1"><thead><tr><th>Downloaded By</th><th>Downloaded At</th></tr></thead><tbody><tr><td>teched99</td><td>2025-10-15T13:55:51.485Z</td></tr></tbody></table>	Downloaded By	Downloaded At	teched99	2025-10-15T13:55:51.485Z
Downloaded By	Downloaded At				
teched99	2025-10-15T13:55:51.485Z				

By clicking on the 'Edit' Button, the entry fields can be changed. The processor of the Investigation Report can here enter his own status about mitigation of the incidents, which are analyzed by the security specialist.

[!\[\]\(32649322933639c398e75a484b1b1ad0_img.jpg\) Download Investigation Report](#) [Create Tag](#) 

Completion Timestamp: 2025/09/29 11:35:05 AM GMT+02:00

Closing Remarks:

Investigator: [Edit](#)

Report Severity: [Edit](#)

Report Status: [Edit](#)

Timestamp of Download: The report has not been downloaded yet.

Downloaded By: The report has not been downloaded yet.

[Save](#) [Cancel](#)

You can play around with filling the different fields, and save it.

Information: After selecting the Report to the status 'Closed', it cannot be re-edited again, as to compliance reasons.

Additionally, you can add tags with search keywords, on which you can easily search in the Report list.

[Download Investigation Report](#) Create Tag [Edit](#)

Enter a tag value, and enter the 'Create' Button.

Create Tag

Tag Name: *

[Create](#) [Cancel](#)

Afterwards, you find the tag value in the 'Details'-UI.

[SAP](#) Download Investigation Reports [Back](#)

Investigation Report 142

teched99

And, going back to the list, you find the tag in the list entry, and you can search for it

The screenshot shows the SAP Enterprise Threat Detection interface. At the top, there is a search bar with fields for Severity, Description, ID, Customer Notification, Investigator, Report Status, Report Severity, Closing Remarks, and Tags. The 'Tags' field contains 'teched99'. Below the search bar is a table titled 'Filtered By: Tags(teched99)'. The table has columns: Severity, ID, Report Creation Date, Description, Customer Notification, Completion Timestamp, Investigator, Report Status, Report Severity, Closing Remarks, and Tags. One row is visible, showing: Severity (High), ID (142), Report Creation Date (2025/09/29 11:23:00 AM GMT+02:00), Description (teched99), Customer Notification (No), Completion Timestamp (2025/09/29 11:23:58 AM GMT+02:00), Investigator (teched99), Report Status (Open), Report Severity (High), Closing Remarks (empty), and Tags (teched99). A red box highlights the 'Tags' column header and the value 'teched99' in the table row.

Severity: Description: ID: Customer Notification: Investigator: Report Status: Report Severity: Closing Remarks: Tags:

Report Status: Report Severity: Closing Remarks: Tags: teched99 x

Filtered By: Tags(teched99).

Severity	ID	Report Creation Date	Description	Customer Notification	Completion Timestamp	Investigator	Report Status	Report Severity	Closing Remarks	Tags
<input type="checkbox"/> High	142	2025/09/29 11:23:00 AM GMT+02:00	teched99	No	2025/09/29 11:23:58 AM GMT+02:00	teched99	Open	High		teched99 >

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