

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	13
2.1 Logon & Preparation Steps.....	13
2.2 Creating a User With High Privileges.....	14
3. Checking Alerts and Creating Investigations.....	16
3.1 Check for Log Events.....	16
3.2 Search for Alerts	17
3.3 Interpreting the Investigation Entries	18
4. Trigger a Critical Action from SAP S/4HANA: Download of a Critical Database Table.....	19
5. User & Environment Behavioral Analysis – Identify the Critical Action in the Forensic Lab	21
5.1 Build up a Workspace	22
5.1.1 Assigning a Chart.....	30
6. From Workspace to Pattern to Alerts.....	32
6.1 Understanding Patterns	32
7. Finalize the Investigation	35
7.1 Information: Maintain your email ID to receive investigation reports	35
7.2 Finalize the investigation.....	36
8. Consumer/Processor role: Work with Investigation reports.....	38

Overview & Touring SAP Enterprise Threat Detection, public cloud

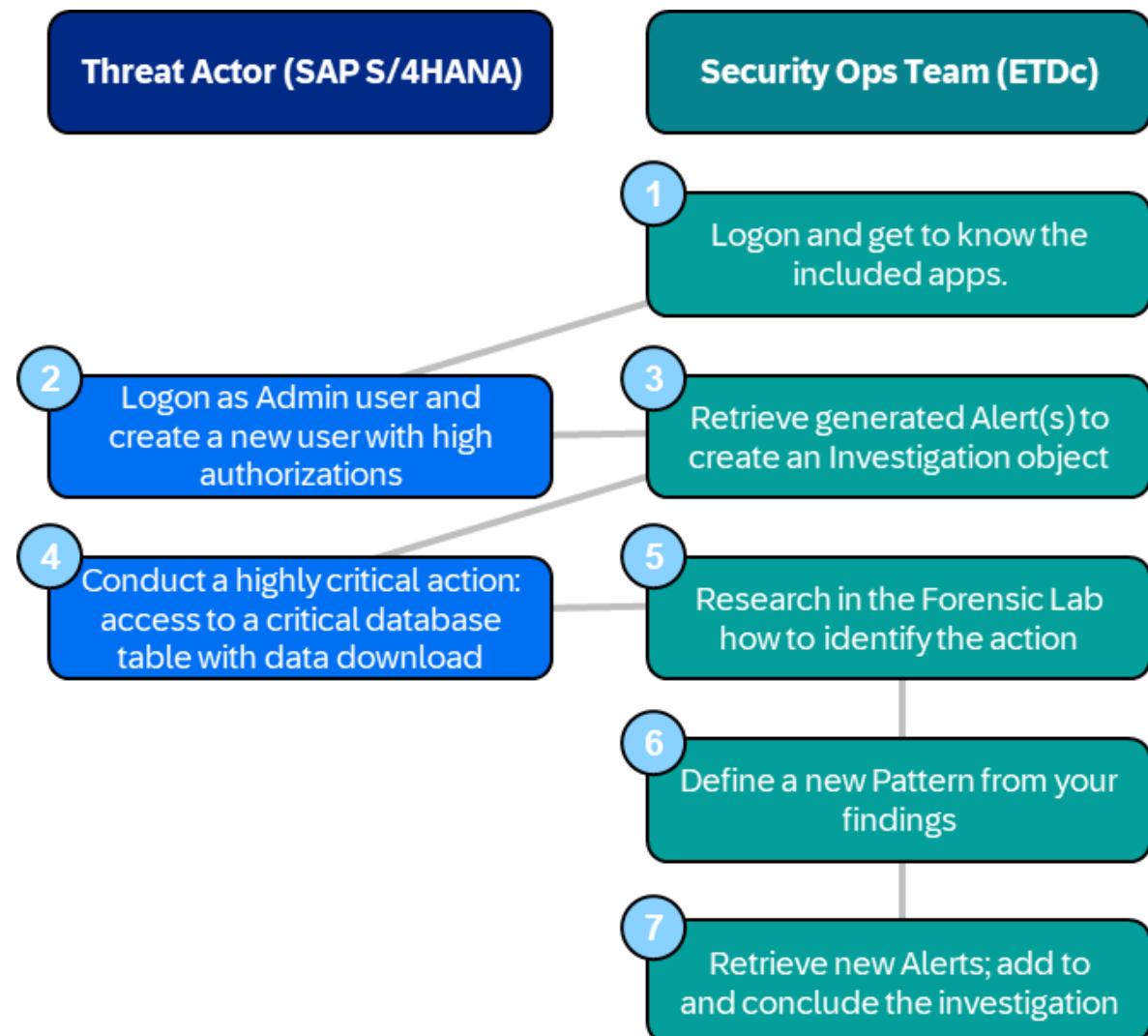
In this hands-on session and workshop of about 1.5 – 2h, you will get to know the basic functioning of *SAP Enterprise Threat Detection, public cloud*, including the terminology employed.

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.

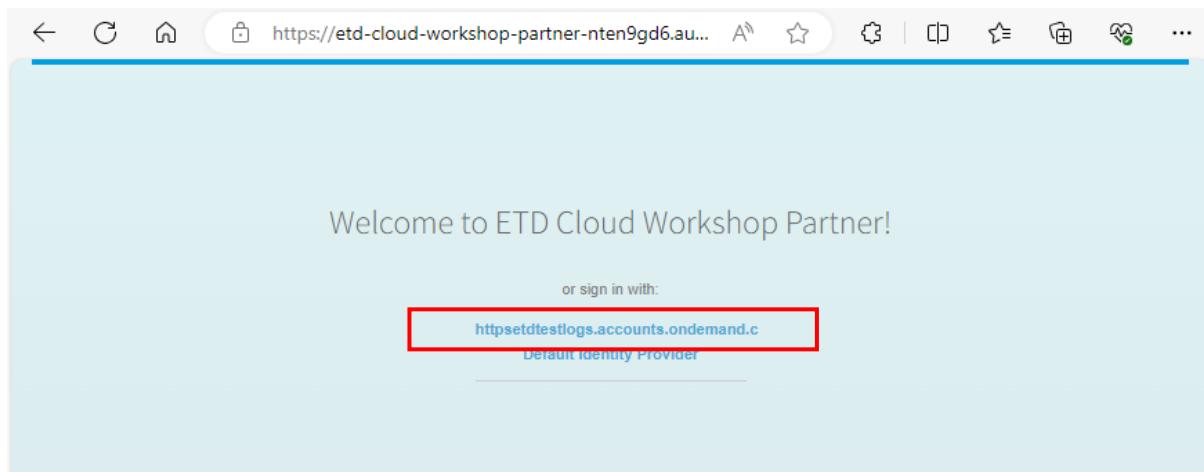
Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

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".

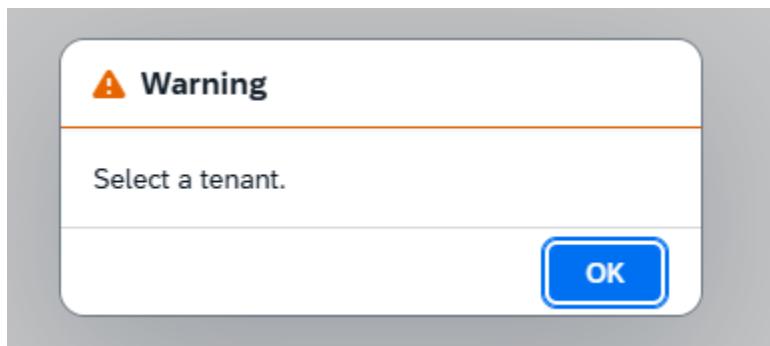
The screenshot shows a SAP web application interface titled 'Select Tenant'. At the top, there are input fields for 'Customer Name' (with placeholder 'etd-cloud-workshop-partner-nten9gd6-monitoringapprouter'), 'Status' (set to 'Inactive'), 'Subdomain' (placeholder 'etd-cloud-workshop-customer-6p3zpomw'), and 'Tenant ID' (placeholder '9189d8d0-c3ea-4f11-a145-1a7d13e32c3d'). Below these fields is a 'Go' button and a 'Hide Filter Bar' link. A 'Filters' button is also present. The main area displays a table with one row, filtered by 'Status: Inactive'. The table columns are 'Customer Name', 'Status', 'Subdomain', and 'Tenant ID'. The single row contains 'Workshop Demo Customer', 'Inactive', 'etd-cloud-workshop-customer-6p3zpomw', and '9189d8d0-c3ea-4f11-a145-1a7d13e32c3d' respectively.

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'. Below this, there are two main sections: 'Enterprise Threat Detection: Cross-Tenant Applications' and 'Enterprise Threat Detection: Tenant Applications'. The 'Cross-Tenant Applications' section contains three cards: 'Select Tenant' (with a cursor icon), 'Manage Alerts for All Tenants' (with a warning icon), and 'Manage Investigations for All Tenants' (with a magnifying glass icon). The 'Tenant Applications' section is divided into a grid of twelve smaller cards arranged in three rows and four columns. The cards are: 'Manage Settings' (camera icon), 'Manage Value Lists' (grid icon), 'Analyze Log Events' (magnifying glass icon), 'Manage Alerts' (warning icon), 'Monitor Pattern Executions' (right-pointing arrow icon), 'Manage Patterns' (puzzle piece icon); 'Manage Investigations' (magnifying glass icon), 'Record of Actions' (document icon), 'Download Investigation Reports' (warning 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)

The image contains two screenshots of the SAP Select Tenant interface. The top screenshot shows the filter bar with fields for Customer Name, Status (set to 'Active'), Subdomain, and Tenant ID. There are also buttons for 'Go', 'Hide Filter Bar', and 'Filters'. The bottom screenshot shows the results table with a single row for 'Workshop Demo Customer' with status 'Inactive'. The table has columns for Customer Name, Status, Subdomain, and Tenant ID.

1.2 UI Round trip

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

The screenshot shows the SAP Manage Settings interface. On the left, there is a sidebar with the following options:

- Manage Event Storage
- Manage Customer Information
- Time Zone
- Manage Reaction and Processing Times
- Manage Data Retention

The main content area is titled "Manage Event Storage". It contains two sections:

- Event Information:** Shows "Log Events: 4.4 M".
- Automatic Deletion:** Shows "Retention Period for Log Events: 14 Days".

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

The screenshot shows the SAP Manage Value Lists interface. The left sidebar lists several value lists:

- ABAP Critical manual SQL Executions
- ABAPBlocklistedFunctionModules
- ABAPBlocklistedGenericTransactionsForDownload
- ABAPBlocklistedHTTPUrlPaths
- ABAPBlocklistedReports
- ABAPBlocklistedReportsSensitiveDataDownloads
- ABAPBlocklistedSOAPRFCFMs

The main content area is titled "Value Lists (Workshop Demo Customer)". It includes a search bar and a "Create" button. Below the search bar, there is a note: "Executions of direct SQL statements from SAP standard programs or transactions".

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

The screenshot shows the SAP Analyze Log Events interface. At the top, there are filter fields for Creation Time Range (Last 10 days), User, System, Service, and Semantic Event. Below these are fields for Event, Log Type, Service, Instance Name, Service, Program Name, and Service, Transaction Name. A search bar and a Go button are also present. The main area displays a table of log events from October 10, 2025, to October 20, 2025. The columns include Timestamp, Semantic Event, Event, Log Type, and User. The table shows various log entries, such as Indicator From Pattern and Executable, RFC-enabled Function Module, Run, along with their corresponding users like ETDADMIN (Target) and NODK_35740 (Acting).

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

The screenshot shows the SAP Manage Alerts interface. At the top, there are filter fields for Creation Time Range (Last 10 days), Pattern (text input field), Status, Severity, Trigger Value 1, and Trigger Value 2. Below these are buttons for Create Investigation, Add to Investigation, Set to Open, Set to No Reaction Needed, Mass Status Change, and Direct Access to Alert. The main area displays a table of alerts with 1,289 entries. The columns include Severity, ID, Pattern, Trigger, Events, and St. The table lists various alert patterns, such as Logon from internal with SAP standard users and Successful logon from same Terminal ID with different users, along with their triggers and associated details.



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

The screenshot shows the SAP Monitor Pattern Executions interface. At the top, there are filter options for Execution Time Range (Last 1 day), Pattern (text input field), Pattern Namespace (dropdown), Status (dropdown), and Execution Mode (dropdown). Below the filters is a table titled "Pattern Executions (23,762) 2025/10/18 18:47:59 PM UTC - 2025/10/19 18:47:59 PM UTC". The table columns include Pattern, Namespace, Execution Time, Ru..., St..., and E... (with icons for sorting and filtering). The data rows list various security-related events such as "DoS attack against different RFC destinations", "Security relevant Policy Changes", and "Calls from non-productive to productive systems via RFC".

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

The screenshot shows the SAP Manage Patterns interface. At the top, there are filter options for Name (text input field), Namespace (dropdown), Status (dropdown), Execution Output (dropdown), and Test Mode (dropdown). Below the filters is a table titled "Patterns (176)". The table has columns for Name, Namespace, and Description. The data rows list patterns like "04_PWHashAttack", "99_PWHashAttack", and "ABAP critical Function Module Calls per SOAP RFC". At the bottom of the table, there are buttons for Create Pattern, Activate, Deactivate, Execute, Delete Pattern, Test Mode On, and Test Mode Off.

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

The screenshot shows the SAP Manage Investigations interface. At the top, there are filter fields for Status, Severity, Management Visibility, Created By, Processor, and Description. Below the filters is a table titled "Investigations (63)". The table columns include Severity, Management Visibility, ID, Description, Status, and Remaining Processing Time (RPT). Each row in the table contains a checkbox, the investigation details, and its status and RPT. Some RPT values are highlighted in red.

Investigations (63)						
	Severity	Management Visibility	ID	Description	Status	Remaining Processing Time (RPT)
<input type="checkbox"/>	Medium	Not Needed	148	test	Open	✖ 38 Hours 31 Minutes 15 Seconds
<input type="checkbox"/>	Medium	Not Needed	147	jh	Open	✖ 38 Hours 34 Minutes 14 Seconds
<input type="checkbox"/>	Medium	Not Needed	146	yii	Open	✖ 38 Hours 35 Minutes 10 Seconds
<input type="checkbox"/>	Medium	Not Needed	145	test33	Open	✖ 38 Hours 39 Minutes 39 Seconds
<input type="checkbox"/>	Medium	Not Needed	144	test	Open	✖ 50 Hours 1 Minutes 24 Seconds
<input type="checkbox"/>	Medium	Not Needed	143	Std User Access	Open	✖ 293 Hours 54 Minutes 21 Seco...
<input type="checkbox"/>	High	Not Needed	142	Critical user activities	Completed	✖ 465 Hours 50 Minutes 15 Seco...
<input type="checkbox"/>	High	Not Needed	141	Sensitive Data download	Completed	✖ 535 Hours 1 Minutes 24 Seconds
<input type="checkbox"/>	High	Not Needed	140	Critical Data Download	Completed	✖ 538 Hours 54 Minutes 46 Seco...

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

The screenshot shows the SAP Record of Actions interface. At the top, there are filter fields for Time Range, User, Entity Type, Entity Namespace, Entity Operation, and Entity Name. Below the filters is a table titled "Records (2,899) 2025/10/19 00:19:15 AM GMT+05:30 - 2025/10/20 00:19:15 AM GMT+05:30". The table columns include Timestamp, User, Entity Type, Entity Namesp..., Entity Name, Entity Operation, and Text. Each row in the table contains the log entry details and a long URL in the Text column.

Timestamp	User	Entity Type	Entity Namesp...	Entity Name	Entity Operation	Text
2025/10/20 00:18:58 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:18:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:17:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:17:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:16:58 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:16:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:15:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:15:58 AM	system	Alert			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More
2025/10/20 00:14:59 AM	system	Investigation			Read	Request URL = https://etdcloudprod-004-prod-etd-cloud-data-retrieval-service.cfapps.eu10-004.hana.on... Show More

In Investigations Report tab, system analyst and view investigations



Investigation Reports (Workshop Demo Customer)

Investigation Reports Monthly Reports

Severity: Description: ID: Go Hide Filter Bar Filters

Customer Notification: Investigator: Report Status:

Report Severity: Closing Remarks: Tags:

Severity	ID	Report Created	Description	Customer Notified	Completion Status	Investigator	Report Status	Report Severity	Closing Remarks	Tags
<input type="checkbox"/> High	142	2025/09/29 14:53:00 PM GMT+05:30	Critical user activities	No	2025/09/29 14:53:58 PM GMT+05:30	m.schmitt@sap.com	Open	High		<input type="checkbox"/> teche...
<input type="checkbox"/> High	141	2025/09/26 17:41:51 PM GMT+05:30	Sensitive Data download	No	2025/09/26 17:50:01 PM GMT+05:30	m.schmitt@sap.com	In Process	Medium		<input type="checkbox"/> LOB A
<input type="checkbox"/> High	140	2025/09/26 13:48:28 PM GMT+05:30	Critical Data Download	No	2025/09/26 13:57:05 PM GMT+05:30	m.schmitt@sap.com	Open	Medium		
		2025/09/26	Critical Data		2025/09/26	(Unassigned)				

In Workspace tab, system analyst and view and create Workspaces

Forensic Lab

Workspaces (Workshop Demo Customer)

Name: Namespace: Use Case: Charts: Patterns: Go

Process Status:

Custom Workspaces SAP Workspaces

Workspaces (61) Create Workspace Delete Workspaces

Name	Namespace	Use Case	Charts	Patterns	Process Status	Editing Status
<input type="checkbox"/> 02_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.			Finished	
<input type="checkbox"/> 04_Demo_noch_ein_Test	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		07_PWHashAtt...	New	
<input type="checkbox"/> 04_Golden_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		05_Golden_PW...	Finished	
<input type="checkbox"/> 04_2_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		04_PWHashAtt...	Finished	
<input type="checkbox"/> 07_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		04.2_PWHashA...	Finished	
<input type="checkbox"/> 10_PWHash_Attack	http://customer.r.com	Useful for the analysis of singular events of user behavior based on an incident alert.		DataTheftWithF...	Finished	
<input type="checkbox"/> 1001_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		10_PWHashAtt...	Finished	
<input type="checkbox"/> 1005_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.			Finished	
<input type="checkbox"/> 95_PWHash_Attack_2	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.	95_PWHashAtt...		Finished	

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



The screenshot shows the SAP Monitor Incoming Logs interface. At the top, there are search fields for 'System Name' and 'Log Status', and a 'Go' button with a dropdown for 'Adapt Filters'. Below this is a table titled 'Systems (7)' with columns for System Name, Last Log Received, and Log Status. The data is as follows:

System Name	Last Log Received	Log Status
S4H	3 days ago	Not Received Last Day
PM0/000	2 days ago	Not Received Last Day
S4H/000	2 days ago	Not Received Last Day
S4H/200	2 days ago	Not Received Last Day
S4H/400	2 days ago	Not Received Last Day
S4H/100	2 days ago	Not Received Last Day
PM0/100	2 days ago	Not Received Last Day

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

The screenshot shows the SAP Resolve User Identity interface. At the top, there are tabs for 'Resolve' (selected) and 'Reverse'. Below this is a search bar with a placeholder 'Enter pseudonym' and a 'Resolve' button. A note below the search bar says 'Account Name Result will appear here...'. The rest of the page is blank.



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.

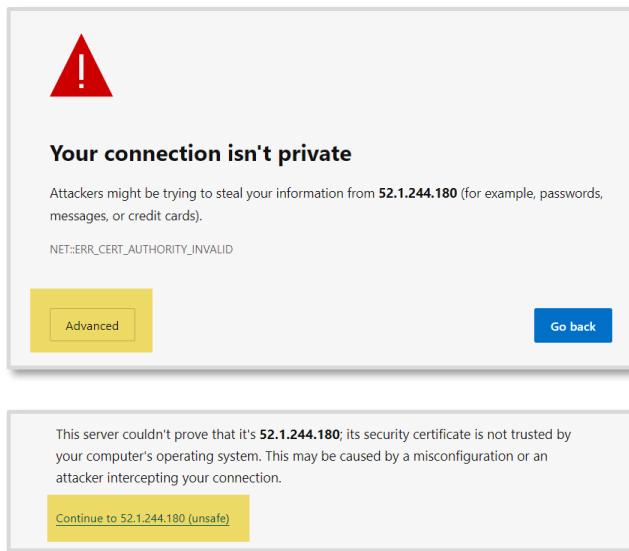
This system & credentials are available during the planned workshop hours only.

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:

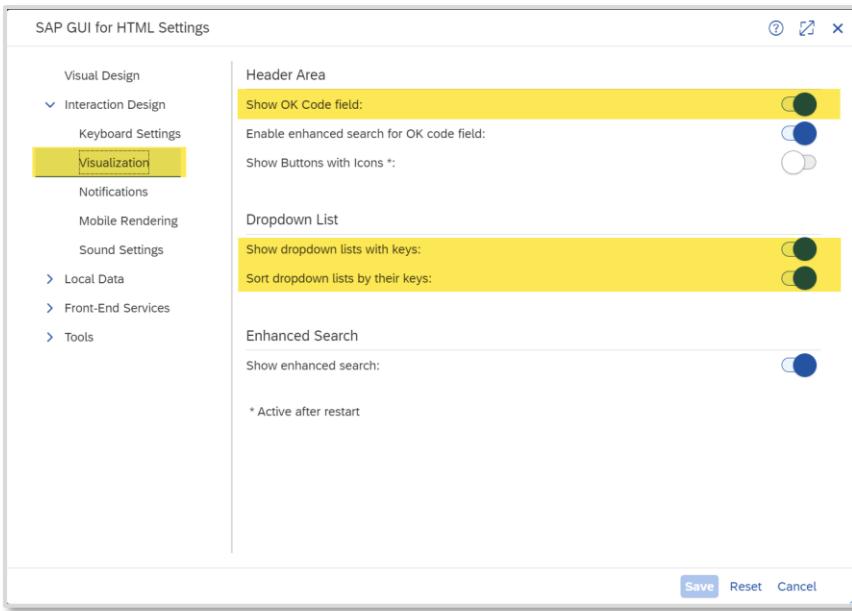


Log on credentials: **User: ETDADMIN##**

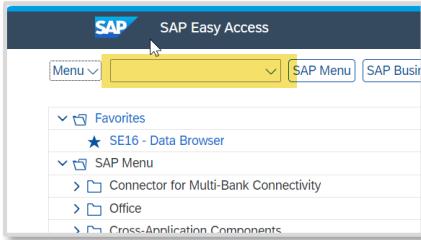
Password: Will be provided in the session

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.



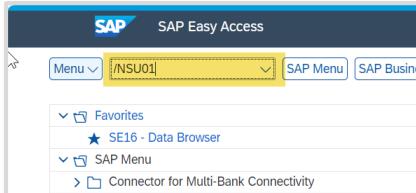
- Leave the menu. Your start screen should now show the transaction code entry field:



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”.

User Maintenance: Initial Screen

Menu: User, Technical User, Change, Display, Delete, **Copy**, Lock/Unlock, Change Password

User: ETDADMIN99

Alias:

- 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”:

Copy Users

From: ETDADMIN99

To: ETDDEMO99

Choose Parts

Address Data
 Defaults
 User Parameters
 Reference User
 Roles
 Authorization Profiles
 User Groups
 Personalization
 License Data
 SAP Easy Access Settings
 Documentation

Copy Cancel

- 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.

Maintain Users

User: ETDDEMO99

Changed By: 00:00:00

Status: Not s

Documentation Address **Logon Data** SNC Defaults Parameters Roles Profiles Groups

Alias: ETDDEMO99

* User Type: A Dialog

Security Policy:

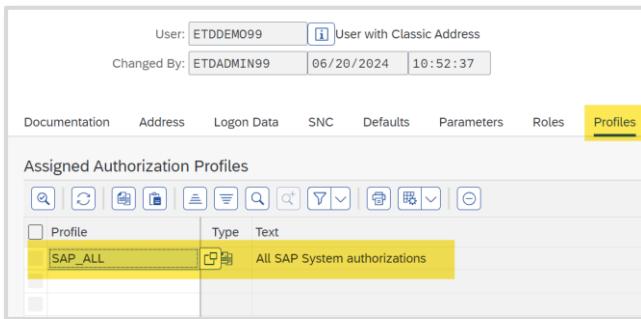
Password

New Password Rules (Case-Sensitive)

New Password: Repeat Password:

Password Status:

- 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.

The screenshot shows the SAP Analyze Log Events interface. The top navigation bar includes the SAP logo and a dropdown menu "Analyze Log Events". On the right, there are buttons for "Go", "Hide Filter Bar", and "Filters". The main area is titled "Log Events (Workshop Demo Customer)". The filter bar at the top has fields for "Creation Time Range" (set to "Last 10 days"), "User" (*etdadmin*), "System", "Service", "Semantic Event" (*user admin*), and several dropdowns for "Event, Log Type", "Service, Instance Name", "Service, Program Name", and "Service, Transaction Name". Below the filter bar, a timestamp range "2025/10/07 11:20:22 AM GMT+05:30 - 2025/10/17 11:20:22 AM GMT+05:30" is displayed. A legend indicates filters for "User", "System", "Service", and "Transaction". The results table shows log entries from 2025/10/16 15:34:51 PM GMT+05:30 to 2025/10/16 15:34:51 PM GMT+05:30. The columns include "Timestamp", "Semantic Event", "Event, Log Type", "User", and "System". The log entries show various system activities like User Admin, Privilege, Alter, Create, Attribute, and Grant.

- 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”.

The screenshot shows the SAP Manage Alerts interface. The top navigation bar includes the SAP logo and a dropdown menu "Manage Alerts". On the right, there are buttons for "Go", "Hide Filter Bar", and "Filters". The main area is titled "Alerts (Workshop Demo Customer)". The filter bar at the top has fields for "Creation Time Range" (set to "Last 1 day"), "Pattern" (text input field "Enter the name of a pattern (at least 2 characters)"), "Status", "Severity", and "Trigger Value 1" (*ETDADMIN*). Below the filter bar, a timestamp range "2025/10/15 22:27:21 PM GMT+05:30 - 2025/10/16 22:27:21 PM GMT+05:30" is displayed. The results table shows alerts with 28 entries. The columns include "Severity", "ID", "Pattern", "Trigger", "Events", and "St". The alerts listed are mostly High severity and involve logons from external and internal users, as well as blocklisted transactions.

- 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”.

The screenshot shows the 'Create Investigation' dialog box. The 'Description' field contains '99 Test Investigation'. The 'Severity' dropdown is set to 'Medium'. The 'Processor' dropdown shows '(Unassigned User)' with a search icon. The 'Status' dropdown is set to 'In Process'. The 'Management Visibility' dropdown is set to 'Not Needed', which is highlighted in blue. The 'Comment' section contains three items: 'Not Needed' (selected), 'For Information', and 'For Action'. At the bottom, there are three buttons: 'Add and Show Investigation' (highlighted in blue), 'Add and Return', and 'Cancel'.

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

The screenshot shows the SAP Manage Investigations interface for 'Investigation 5'. The investigation was created on 2024/03/19 at 05:54:51 AM GMT-07:00 by user P000048. The description is 'Demo99 test' and the severity is 'Medium'. The processor is listed as 'Tobias, Keller' with the email 'tobias.keller@sap.com'. The status is 'In Process'. There is an unchecked checkbox for 'Customer Notification'. The 'Management Visibility' is set to 'Not Needed'. The 'Remaining Processing Time (RPT)' is 23 Hours 59 Minutes 52 Seconds. At the bottom, there is a comment input field with a placeholder 'Enter your comment here' and a character limit of 5000. Navigation tabs at the bottom include 'Actions (14)', 'Users', and 'Alerts (12)'.

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.

Actions (9)	Users	Alerts (8)				
ID	Pattern	Trigger	Events	Severity	Creation Time	
132632	Logon from external with SAP stan...	Measurement 1 exceeded threshold 1 for ('Event...			High	2025/10/16 22:20:52 PM GMT+05:30
132624	Logon from internal with SAP stan...	Measurement 48 exceeded threshold 1 for ('System ID....			High	2025/10/16 21:43:31 PM GMT+05:30
132570	Logon from internal with SAP stan...	Measurement 39 exceeded threshold 1 for ('System ID....			Information	10 PM GMT+05:30
132563	Blocklisted transactions in producti...	Measurement 9 exceeded threshold 1 for ('Service,...			Information	4 PM GMT+05:30

- 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

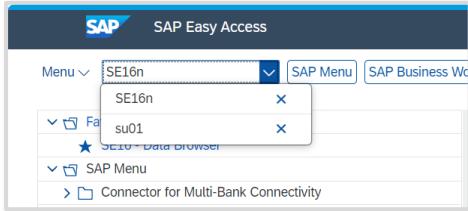
In this section, you will return into the role as a rogue actor and conduct several more actions resulting in Log Events flowing into *SAP Enterprise Threat Detection, public cloud*.

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”:

A screenshot of the 'General Table Display' dialog box. The title bar says 'General Table Display'. The 'Data base:' field contains 'USR02'. The 'Selection Criteria' section shows various fields like Client, User, Initial PW, Valid from, Valid to, User Type, User Group, Failed Logons, User Lock, Account no., Creator, Created On, and Last Logon Date. Each field has an 'O...' column, a 'Frm-Val.' column, a 'To-Value' column, and a 'More' column with checkboxes. The 'Output' column has checkboxes next to 'MANDT', 'BNAME', 'BCODE', 'GLTGV', 'GLTGB', 'USTYP', 'CLASS', 'LOCNT', 'UFLAG', 'ACCNT', 'ANAME', 'ERDAT', and 'TRDAT'. The 'Technical Name' column lists the corresponding database columns. At the bottom right are 'Save' and 'Cancel' buttons.

- 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.

The screenshot shows the SAP ERP interface with the title "USR02: Display of Entries Found". The search bar indicates "Search in Table: USR02 Logon Data (Kernel-Side Use)" with "Number of Hits: 115". The runtime is listed as 0. The table displays user activity logs with columns: User Name, Initial Password, Valid from, Type, User Group, Failed, Lock, Account number, and Creator. Several rows are highlighted in yellow, including "Local File Service", "Send Service", "SAPoffice Folders Dialog", "ABC Analys. Service", and multiple entries for "HTML download Dialog".

User Name	Initial Password	Valid from	Type	User Group	Failed	Lock	Account number	Creator
BGRFCUSER	0000000000000000	10/04/2017	Local File	Service	0	0		BPINST
BGRFC_SUPER3	0000000000000000	11/03/2021	Send	Service	0	0		BPINST
BPINST	0000000000000000		SAPoffice Folders	Dialog	0	0		DDIC
DDIC	0000000000000000		ABC Analys.	Dialog	0	0		BPINST
DELAY_LOGON	0000000000000000		HTML download	Service	0	0		ETDADMIN
DEMO01	0000000000000000			A Dialog	0	0		BPINST
DEMO1	0000000000000000			A Dialog	0	0		BPINST
DEMO2	0000000000000000			A Dialog	0	0		BPINST
DEVELOPER_5	0000000000000000			A Dialog	0	0		SAP*
ETDADMIN	0000000000000000			A Dialog	0	0		ETDADMIN
ETDADMIN01	0000000000000000			A Dialog	0	0		ETDADMIN
ETDADMIN02	0000000000000000			A Dialog	0	0		ETDADMIN
ETDADMIN03	0000000000000000			A Dialog	0	0		ETDADMIN

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

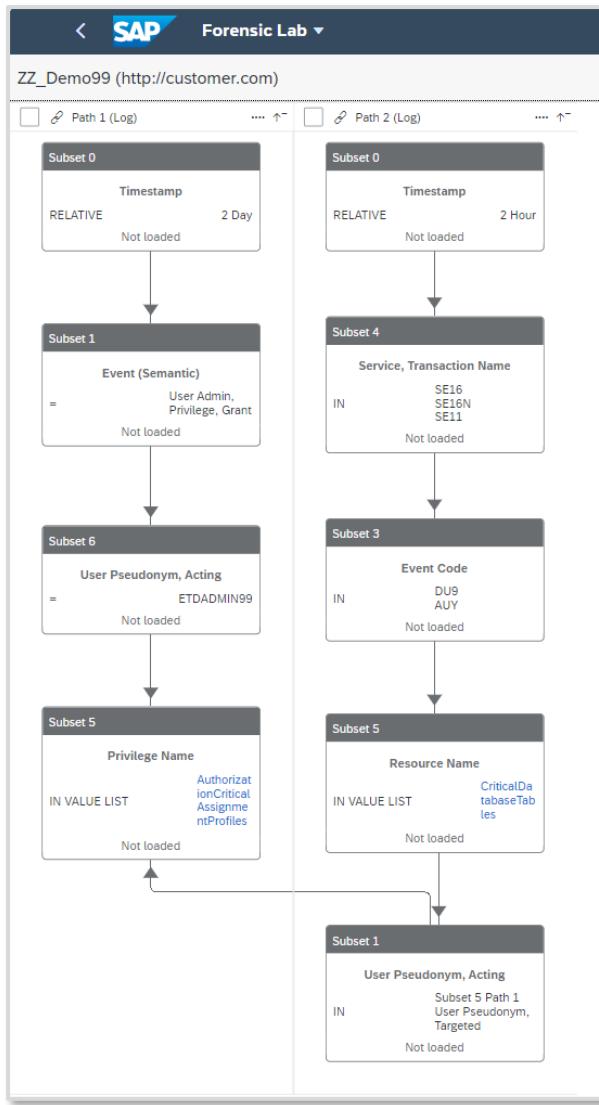
The Forensic Lab is the area where you work on ways to identify new potential threat vectors by filtering your way through the large volume of log entries until you arrive at a definition yielding few and specific logs that should point at a real threat.

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:

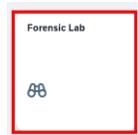
- “Path 1” should be capable of establishing a list of users who have been granted critical authorizations in the past 2 days.
- “Path 2” to the right shall be able to establish a list of all users who have accessed a critical resource recently.
- The “Reference” allows to single out users which are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



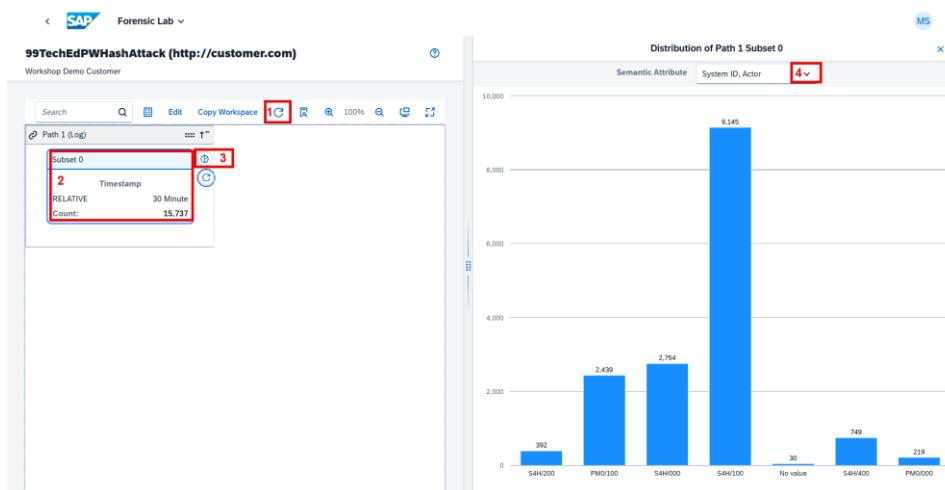
- In the area “Custom Workspaces”, you see a list of existing workspaces.
- Create a new Workspace with Name ##TechEdPWHAttack, by replacing the ## with your participant number. Enter some additional information (Use case, Severity, Description), and then click on ‘Create’

The screenshot shows the SAP Workspaces interface. On the left, there's a sidebar titled 'Custom Workspaces' and 'SAP Workspaces'. Below it, a table lists various workspaces with columns for Name, Namespace, and Use Case. In the center, a modal window titled 'Create Workspace' is open. It has fields for 'Name' (containing '<YourNumber>TechEdPWHashAttack'), 'Namespace' (set to 'http://customer.com'), 'Use Case' (described as 'Admin creates a new user with which they attack passwords hashes.'), 'Risk Classification' (set to 'High'), and a 'Description' field. At the bottom right of the modal are 'Create' and 'Close' buttons, with the 'Create' button highlighted by a red box. To the right of the modal, there's a table showing process status and editing status. A red box highlights the 'Create Workspace' and 'Delete Workspaces' buttons at the top right of the workspace list area.

- 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 with the newly created workspace '99TechEdPWHashAttack' selected. The workspace list table now includes a column for 'Editing Status' with a red box highlighting the 'Edit' icon for this workspace. A red box also highlights the arrow icon to the right of the workspace name in the list.

- 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

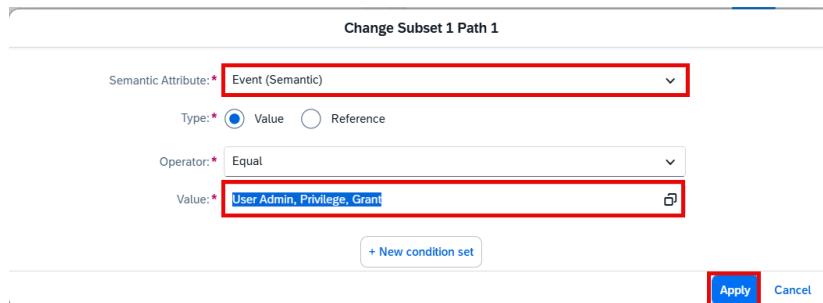
Semantic Attribute: * 

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’.

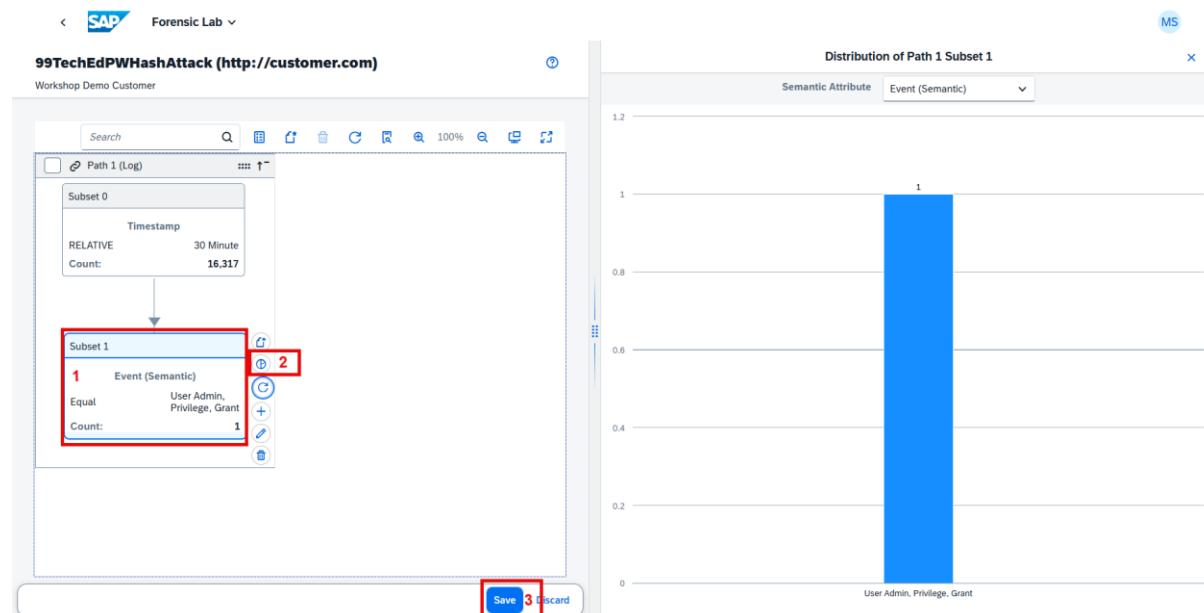


The screenshot shows the 'Change Subset 1 Path 1' dialog box. It contains the following fields:

- 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'

The screenshot shows the 'Change Subset 2 Path 1' dialog. At the top, it says 'Change Subset 2 Path 1'. Below that, there's a dropdown for 'Semantic Attribute' set to 'User Pseudonym, Target', which is also highlighted with a red box. Underneath is a 'Type' section with 'Value' selected (radio button is checked). The 'Operator' dropdown is set to 'Equal'. The 'Value' input field contains 'ETDADMIN<YourNumber>', which is also highlighted with a red box. There are 'Apply' and 'Cancel' buttons at the bottom right.

- 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'

The screenshot shows the 'Create Subset' dialog. At the top, it says 'Create Subset'. Below that, there's a dropdown for 'Semantic Attribute' set to 'Privilege Name', which is also highlighted with a red box. Underneath is a 'Type' section with 'Value' selected (radio button is checked). The 'Operator' dropdown is set to 'In value list'. The 'Value List Name' input field contains 'AuthorizationCriticalAssignmentProfiles', which is also highlighted with a red box. There are '+ New condition set', 'Create', and 'Cancel' buttons at the bottom right.

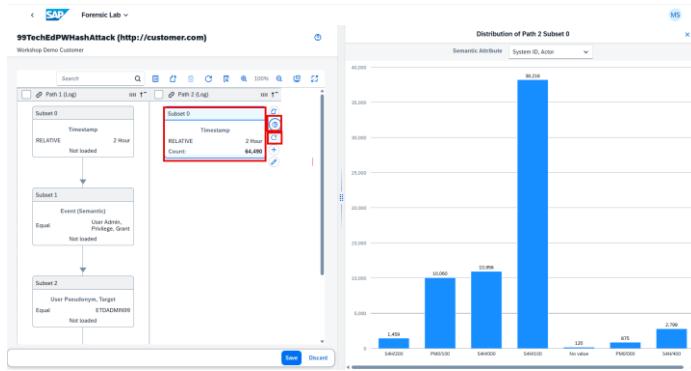
- You new Subset is showing as 'Subset 3'. By refreshing and selecting the Pie Chart you can see some data in Subset 3.

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

- 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'

- 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

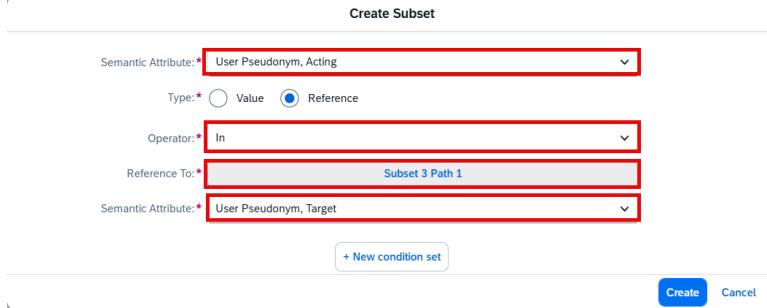
Operator: * In

Reference To: * Subset 3 Path 1

Semantic Attribute: * User Pseudonym, Target

+ New condition set

Create Cancel



- 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.

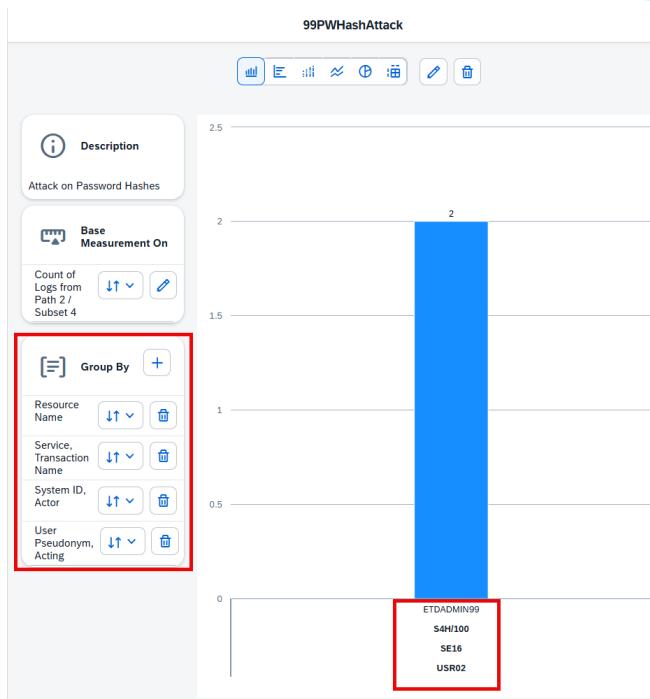
For measurement, choose the “count” * and a fitting Display Name if you like:

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, there 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.

SAP Manage Patterns < dD

Pattern Generic access to critical database tables

Customer: Workshop Demo Customer

Execute Edit ?

Details Used Value Lists Postprocessing Work Items

General		Administration	
Name:	Generic access to critical database tables	Created By:	SAP
Namespace:	http://sap.com/secomon/basis	Created At:	2018/12/31 16:00:00 PM GMT-08:00
Description:	Issue an alert when client gets access to critical database tables.	Changed By:	
		Changed At:	

Chart and Execution Configuration

Chart and Execution		Configuration	
Namespace of Chart Workspace:		Status: Active	
Name of Chart Workspace:		Frequency: 5 Minutes	
Name of Chart:		Threshold Operator: >=	
Execution Type:		Threshold: 1	
Execution Output:		Severity: High	
Time Range:		Test Mode: No	
Grouping Attributes:		View Details	

- 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:

Alerts (Workshop Demo Customer)

Creation Time Range: Pattern: Status:

Last 1 day Enter the name of a pattern (at least 2 characters) ▾

Severity: Trigger Value 1: Trigger Value 2:

Go Hide Filter Bar Filters

Alerts (181) Create Investigation Add to Investigation Set to Open Set to No Reaction Needed Mass Status Change Direct Access to Alert: Enter ID Open

Filtered By: alerts.creationTimeRange(2025/10/19 13:52:33 PM GMT+02:00 - 2025/10/20 13:52:33 PM GMT+02:00)

Severity	ID	Pattern	Trigger
High	133133	99PWHashAttack	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' = '10.79.50.150', 'System ID, Actor' = 'S4H100', 'User Pseudonym, Acting' = 'UTNK_18727')
High	133132	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for (Event (Semantic) = 'User Logon', 'Network Hostname, Initiator' = '10.79.50.150', 'System ID, Actor' = 'S4H100', 'User Pseudonym, Acting' = 'UTNK_18727')
High	133131	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for (Event (Semantic) = 'User Logon', 'Network Hostname, Initiator' = '10.79.50.150', 'System ID, Actor' = 'S4H100', 'User Pseudonym, Acting' = 'UTNK_18727')

- 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...)			Information	2024/03/12 21:13:30 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' = '')			Information	2024/03/12 21:13:30 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 are filters for 'Creation Time Range' (Last 3 days), 'Pattern' (Enter the name of a pattern (at least 2 characters) ...), 'Status' (dropdown), 'Severity' (dropdown), 'Trigger Value 1' (dropdown), and 'Trigger Value 2' (UTNK_18727). Below the filters, it says 'Customer: Workshop Demo Customer'. The main area displays a table of alerts with columns: Severity, ID, Pattern, Trigger, Events, and Status. The 'Trigger' column contains detailed log entries for each alert. At the bottom right of the table, 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 tab. It has tabs for 'Actions (80)', 'Users' (selected), and 'Alerts (76)'. Under the 'Users' tab, there is a section titled 'Depseudonymize All'. A table lists users with their pseudonyms, roles, and a list of alerts. For each user, there is a 'Depseudonymize' button. The users listed are ETDADMIN99 and UVED_14557.

Pseudonym	Roles	Alerts	Action
ETDADMIN99	Acting	3636,3646,3665,3680,3688	<button>Depseudonymize</button>
UVED_14557	Acting,Initiating,Targeted	3636,3643,3644,3645,3646,3649,3651,3652,3655,3657,3658,3660,3661,3663,3664,3665,3668,3669,3670,3671,3673,3675,3676,3677,3679,3680,3682,3684,3685,3686,3688,3690,3692,369	<button>Depseudonymize</button>

- 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.

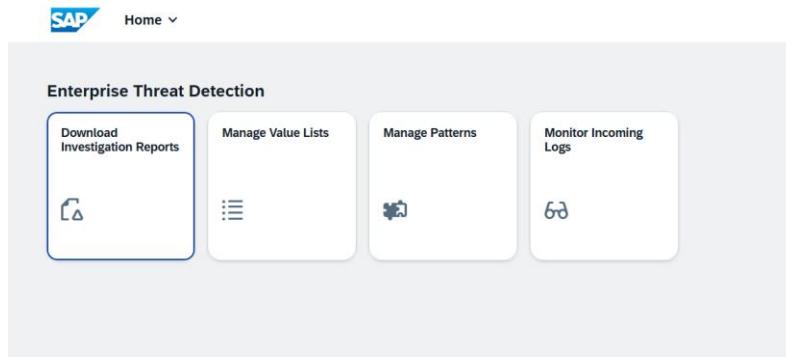
Logon to the consumer view of SAP Enterprise Threat Detection, cloud edition .

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.



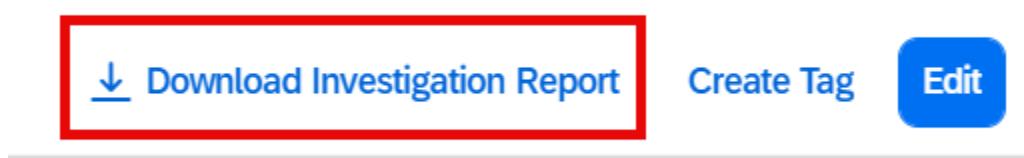
Click on Tile 'Download Investigation Reports'

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

The screenshot shows the 'Investigation Reports' list UI. At the top, there are filters for Severity, Description, ID, Customer Notification, Report Status, Report Severity, Closing Remarks, and Investigator. Below the filters is a table with columns: Severity, ID, Report Creation Date, Description, Customer Notification, Completion Timestamp, Investigator, Report Status, Report Severity, Closing Remarks, and Tags. Each row represents an investigation record. A red box highlights the 'Description' column for the first row, which contains the value 'teched99B'. To the right of the table are buttons for 'Investigation Reports', 'Create Tag', and 'Edit'.

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			
<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		
<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.

[!\[\]\(59e4e94ef536f221d5c47f9cdea485d8_img.jpg\) Download Investigation Report](#) [Create Tag](#) 

Completion Timestamp: 2025/09/29 11:35:05 AM GMT+02:00
Closing Remarks:
Investigator: teched99
Report Severity: High
Report Status: Open
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

Create Tag

Tag Name: * teched99

Create Cancel

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

Create Tag

Tag Name: * teched99

Create Cancel

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

← SAP Download Investigation Reports ▾

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 a user interface for an SAP application. 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' with a red box around it. Below the search bar is a toolbar with icons for 'Investigation Reports', 'C', and 'G'. A message bar indicates 'Filtered By: Tags(teched99)'. The main area displays a table of investigation reports. The columns are: Severity, ID, Report Creation Date, Description, Customer Notification, Completion Timestamp, Investigator, Report Status, Report Severity, Closing Remarks, and Tags. One row is shown in the table, corresponding to the filter applied in the search bar.

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		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