

## **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 .....	21
5.1.1 Assigning a Chart.....	21
6. From Workspace to Pattern to Alerts.....	21
6.1 Understanding Patterns .....	21
7. Finalize the Investigation .....	21
7.1 Information: Maintain your email ID to receive investigation reports .....	21
7.2 Finalize the investigation.....	21
8. Consumer/Processor role: Work with Investigation reports.....	21

## Overview & Touring SAP Enterprise Threat Detection, public cloud

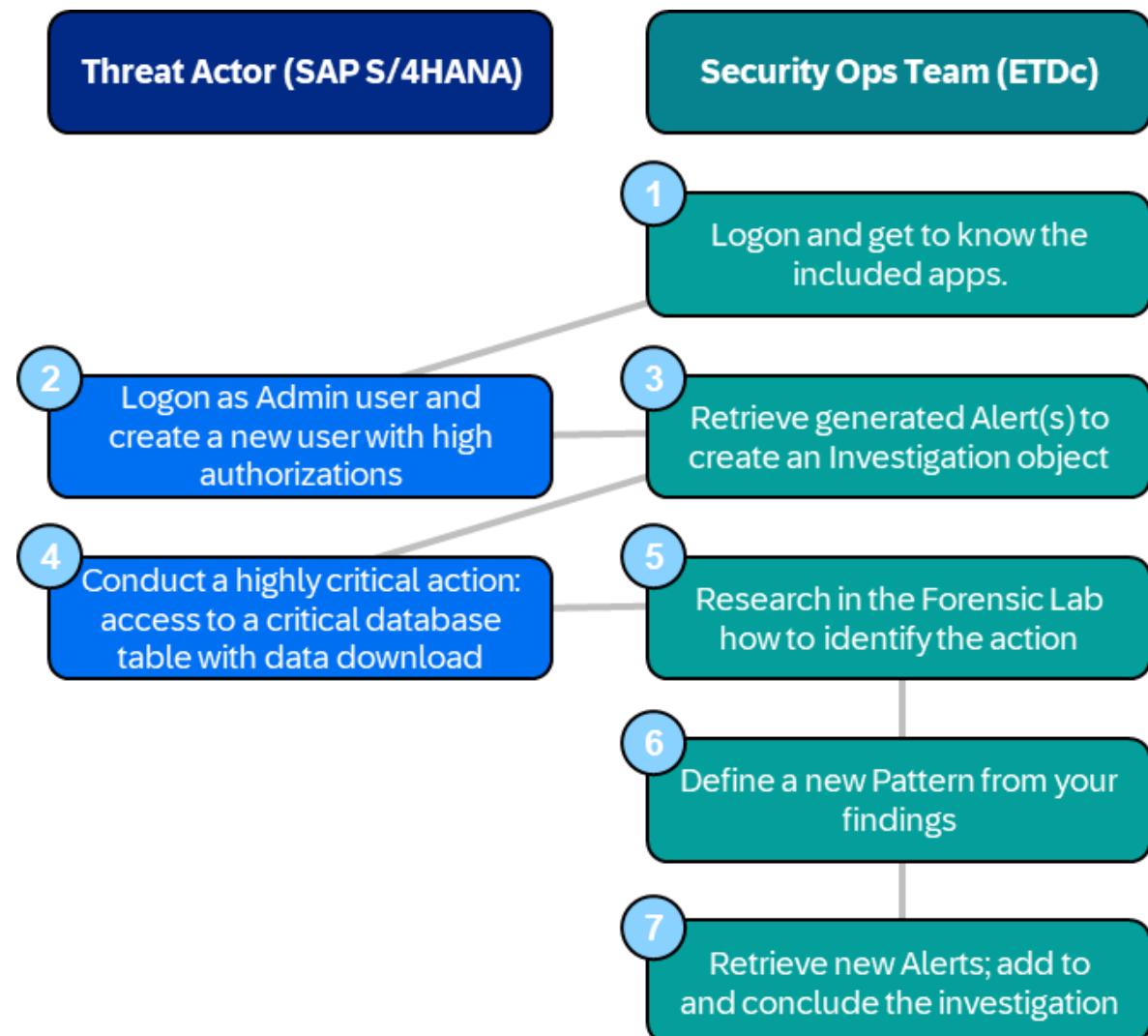
In this hands-on session and workshop of about 1.5 – 2h, you will get to know the basic functioning of *SAP Enterprise Threat Detection, public cloud*, including the terminology employed.

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 3<sup>rd</sup> 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.

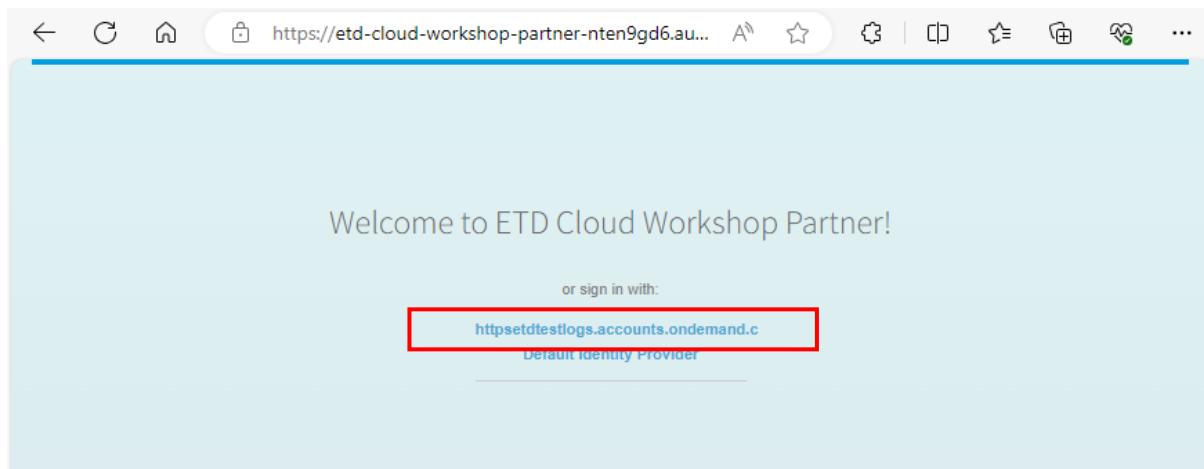
Please let us know if you'd like to have access afterwards; we're happy to check how long we can extend your access.

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".

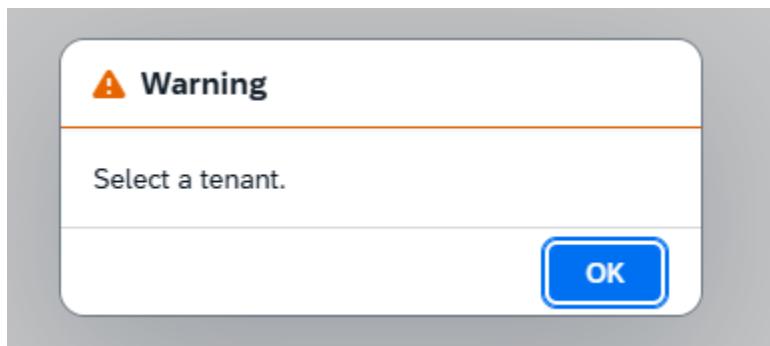
The screenshot shows a SAP web application interface titled "Select Tenant". At the top, there are input fields for "Customer Name" and "Status" (set to "Inactive"), and dropdowns for "Subdomain" and "Tenant ID". Below these are filter buttons and a "Go" button. A table below lists a single tenant entry: "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 links for "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 the heading "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)

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. The table has columns for Customer Name, Status, Subdomain, and Tenant ID. The row shows 'Workshop Demo Customer' in the Customer Name column, 'Inactive' in the Status column, 'etd-cloud-workshop-customer-6p3zpmow' in the Subdomain column, and '9189d8d0-c3ea-4f11-a145-1a7d13e32c3d' in the Tenant ID column. A note at the top of the table says 'Filtered By: Status(Inactive)'.

## 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 sidebar lists several value lists:

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

Each item has a brief description below it. At the top right, there is a "Create" button.

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 with a magnifying glass icon is positioned between the filters and the table. 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 contains several entries, such as Indicator From Pattern and Executable, RFC-enabled Function Module, Run.

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 titled 'Alerts (1,289)'. The columns include Severity, ID, Pattern, Trigger, Events, and St. The table lists various alert entries, such as 'Logon from internal with SAP standard users (alerts)' and 'Successful logon from same Terminal ID with different users'.



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 section titled "Pattern Executions (23,762) 2025/10/18 18:47:59 PM UTC - 2025/10/19 18:47:59 PM UTC". The main area displays a table of executed patterns:

Pattern	Namespace	Execution Time	Ru...	St...	E...
DoS attack against different RFC destinations	http://sap.com/secmon/basis	2025/10/20 00:15:59 AM GMT+05:30	26	OK	Ja
Security relevant Policy Changes	http://sap.com/secmon/basis	2025/10/20 00:15:59 AM GMT+05:30	14	OK	Ja
Change of HR Critical Role	http://sap.com/secmon/content	2025/10/20 00:15:59 AM GMT+05:30	37	OK	Ja
Calls from non-productive to productive systems via RFC	http://sap.com/secmon/basis	2025/10/20 00:15:58 AM GMT+05:30	26	OK	Ja
Critical Function module call in Test framework calls	http://customer.com	2025/10/20 00:15:57 AM GMT+05:30	22	OK	Ja
DoS attack against different HTTP URLs	http://sap.com/secmon/basis	2025/10/20 00:15:56 AM GMT+05:30	16	OK	Ja
Debugging in critical systems	http://sap.com/secmon/basis	2025/10/20 00:15:55 AM GMT+05:30	32	OK	Ja
New Report created in critical system role	http://customer.com	2025/10/20 00:15:54 AM GMT+05:30	14	OK	Ja
Critical manual in-ABAP SQL statement execution	http://customer.com	2025/10/20 00:15:54 AM GMT+05:30	45	OK	Ja

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 section titled "Patterns (176)". The main area displays a table of defined patterns:

Name	Namespace	Description
04_PWHashAttack	http://customer.com	Angriff von Demo-User 04
99_PWHashAttack	http://customer.com	Fake user accessing PW Hashes
ABAP critical Function Module Calls per SOAP RFC	http://sap.com/secmon/basis	Client calls critical ABAP function modules per SOAP rfc interface.
ABAP deactivated or deleted function modules	http://sap.com/secmon/basis	A user has tried to execute a function module that should not be executed remotely. The function module was deactivated or deleted by an SAP Security Note.
ABAP deactivated or deleted reports	http://sap.com/secmon/basis	A user has tried to execute a report which was deactivated or removed by an SAP Security Note.
ABAP function modules with removed RFC enablement	http://sap.com/secmon/basis	A user has tried to execute a function module that should not be executed remotely. enablement of remote function call was removed by an SAP Security Note.

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 are: Severity, Management Visibility, ID, Description, Status, and Remaining Processing Time (RPT). Each row in the table contains a checkbox, the investigation details, its status, and a red RPT value. The RPT values range from 38 hours to 538 hours and 15 seconds.

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 (Last 1 day), 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 are: Timestamp, User, Entity Type, Entity Namesp..., Entity Name, Entity Operation, and Text. Each row in the table contains the timestamp, user, entity type, namespace, name, operation, and a detailed text log entry.

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

**SAP** Download Investigation Reports dD

### 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		<span>tech...</span> >
<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	<span>LOB A</span> >	
<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

**SAP** Forensic Lab dD

### 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
02_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.			Finished	>
04_Demo_noch_ein_Test	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		07_PWHashAtt	New	>
04_Golden_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		05_Golden_PW	04_Golden PW	Attack
04_2_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		04_PWHashAtt	Finished	>
07_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		04.2_PWHashA	Finished	>
10_PWHash_Attack	http://customer.r.com	Useful for the analysis of singular events of user behavior based on an incident alert.		DataTheftWithF	Finished	>
1001_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.		07_PWHashAtt	10_PWHashAtt	Finished
1005_PWHash_Attack	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.			Finished	>
95_PWHash_Attack_2	http://customer.r.com	Admin creates a new user with which they attack passwords hashes.	95_PWHashAtt		New	>

### 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' and 'Reverse', with 'Resolve' being the active tab. Below this is a search bar with placeholder text 'Enter pseudonym' and a 'Resolve' button. The main area displays the message 'Account Name' and 'Result will appear here...'.

## 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.

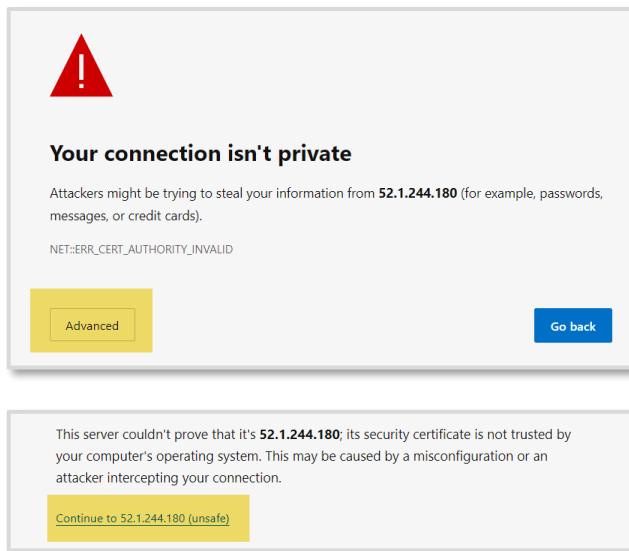
This system & credentials are available during the planned workshop hours only.

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:

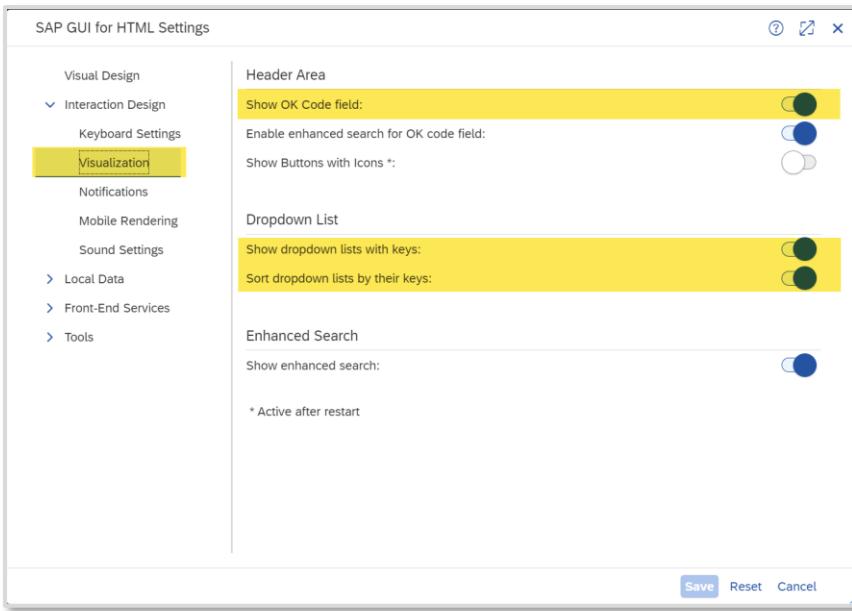


Log on credentials: **User: ETDADMIN##**

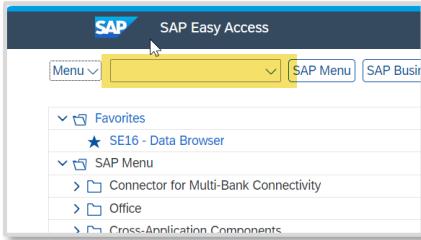
**Password: Will be provided in the session**

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.



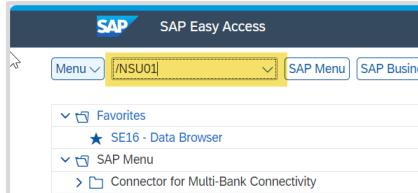
- Leave the menu. Your start screen should now show the transaction code entry field:



## 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

Logon Data

Alias: ETDDEMO99

\* User Type: A Dialog

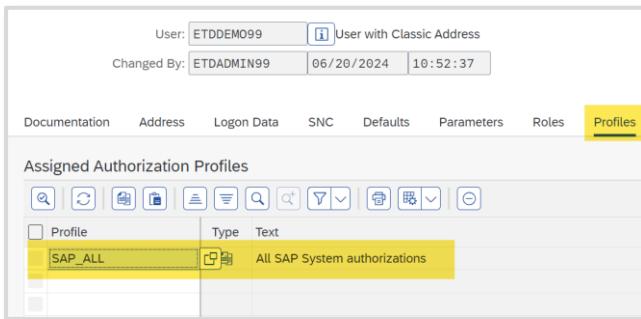
Security Policy:

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 [techedx@etdsap.com](mailto:techedx@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 sources, 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)'. There are also buttons for 'Edit' and 'Help'.

### 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

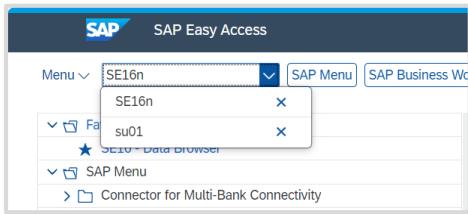
In this section, you will return into the role as a rogue actor and conduct several more actions resulting in Log Events flowing into *SAP Enterprise Threat Detection, public cloud*.

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. To the right of these fields are 'From-Val.' and 'To-Value' columns, and checkboxes for 'More', 'Output', and 'Technical Name'. A grid below lists these names with corresponding checkboxes. At the bottom right are 'Save' and 'Cancel' buttons.

Fld Name	From-Val.	To-Value	More	Output	Technical Name
Client			<input type="checkbox"/>	<input checked="" type="checkbox"/>	MANDT
User	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	BNAME
Initial PW	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	BCODE
Valid from	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	GLTGV
Valid to	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	GLTGB
User Type	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	USTYP
User Group	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	CLASS
Failed Logons	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	LOCNT
User Lock	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	UFLAG
Account no.	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	ACCNT
Creator	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	ANAME
Created On	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	ERDAT
Last Logon Date	<input type="checkbox"/>		<input type="checkbox"/>	<input checked="" type="checkbox"/>	TRDAT

- 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.

USR02: Display of Entries Found							
Menu		Search in Table:	Refresh	Display Selection Criteria	Selection Criteria: Business View	Display Selection as ABAP	
Logon Data (Kernel-Side Use)		USR02					
Number of Hits:		115					
Runtime:		0	Maximum No. of Hits	500			
Insert Column:							
<input type="checkbox"/> User Name      Initial Password      Valid from      Type      User Group      Failed      Lock      Account number      Creator <input checked="" type="checkbox"/> BGRFCUSER      0000000000000000      10/04/2017      Local File      Service      0      0      BPINST <input checked="" type="checkbox"/> BGRFC_SUPER3      0000000000000000      11/03/2021      Send      Service      0      0      BPINST <input checked="" type="checkbox"/> BPINST      0000000000000000           SAPoffice Folders      Dialog      0      0      DDIC <input checked="" type="checkbox"/> DDIC      0000000000000000           ABC Analys.      Dialog      0      0      BPINST <input checked="" type="checkbox"/> DELAY_LOGON      0000000000000000           HTML download      Dialog      0      0      ETDADMIN <input checked="" type="checkbox"/> DEMO01      0000000000000000                A Dialog      0      0      BPINST <input checked="" type="checkbox"/> DEMO1      0000000000000000                A Dialog      0      0      BPINST <input checked="" type="checkbox"/> DEMO2      0000000000000000                A Dialog      0      0      BPINST <input checked="" type="checkbox"/> DEVELOPER_5      0000000000000000                A Dialog      0      0      SAP* <input checked="" type="checkbox"/> ETDADMIN      0000000000000000                A Dialog      0      0      ETDADMIN <input checked="" type="checkbox"/> ETDADMIN01      0000000000000000                A Dialog      0      0      ETDADMIN01 <input checked="" type="checkbox"/> ETDADMIN02      0000000000000000                A Dialog      0      0      ETDADMIN02 <input checked="" type="checkbox"/> ETDADMIN03      0000000000000000                A Dialog      0      0      ETDADMIN03							

You have conducted a seemingly simple but dangerous activity which should be resulting in at least one Alert in *SAP Enterprise Threat Detection, public cloud*.

Let's continue to retrieve and process them!

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

### 5.1 Build up a Workspace

#### 5.1.1 Assigning a Chart

## 6. From Workspace to Pattern to Alerts

### 6.1 Understanding Patterns

## 7. Finalize the Investigation

### 7.1 Information: Maintain your email ID to receive investigation reports

### 7.2 Finalize the investigation

## 8. Consumer/Processor role: Work with Investigation reports

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

For any feedback, please address your trainer, or product management:

[SAP-ETD@sap.com](mailto:SAP-ETD@sap.com)

