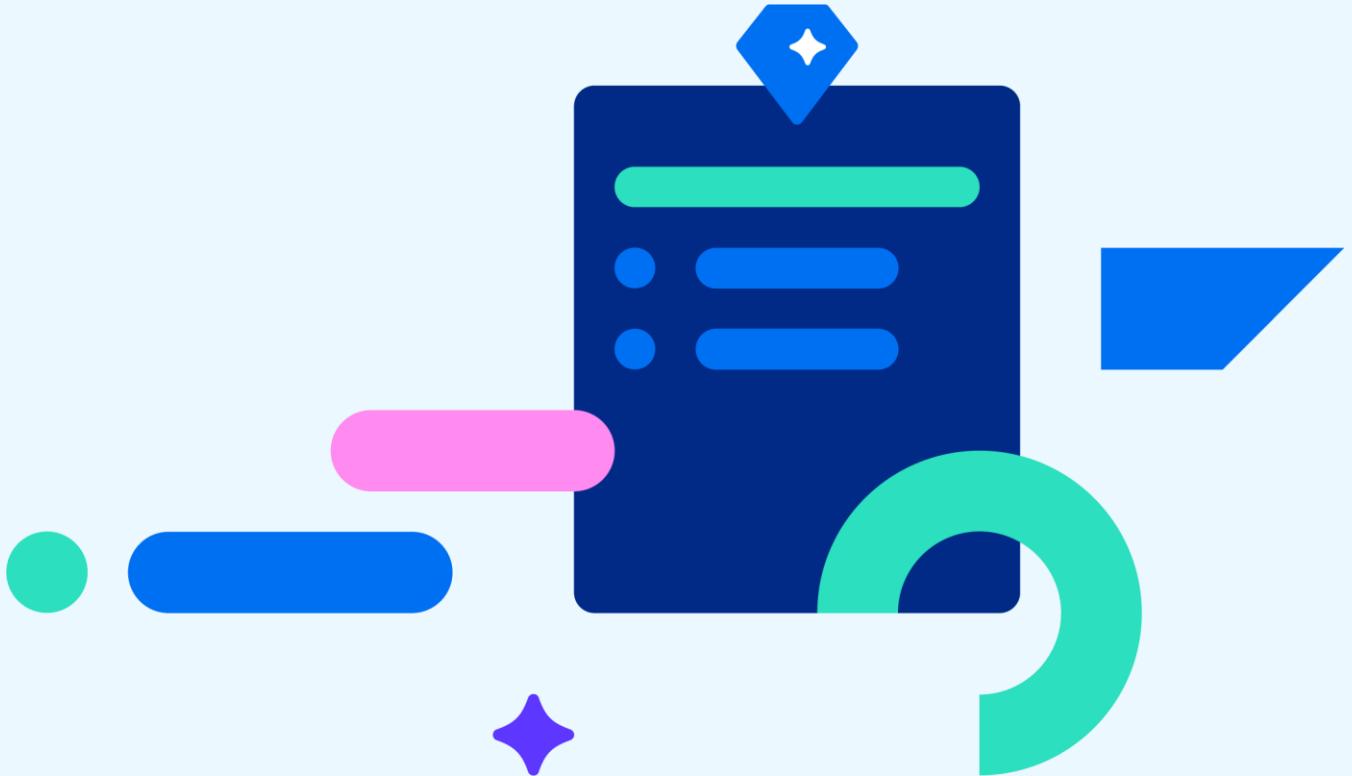


CA163
**Hands-on experience
with SAP Enterprise
Threat Detection**

Kirti Singh, Arpita Deshpande, Shivaprasad
Naik, Ankit Sharma

November 2025



Agenda

1. Introduction SAP Enterprise Threat Detection,
cloud edition
2. SAP Enterprise Threat Detection, (public) cloud
edition for Private/Public Cloud SAP Landscapes
3. Short Preview
 - Starting UI
 - Dashboards (preview)



Introduction SAP Enterprise Threat Detection Cloud Edition



What is SAP Enterprise Threat Detection

SAP Enterprise Threat Detection raises alerts in (near-) real-time, if security/compliance relevant suspicious activities happen in the application layer of your SAP landscape.

SAP Enterprise Threat Detection uses HANA technology to digest mass data log volumes, and run highly efficient automated processes to track hacker activity using SAP's predefined and easy customizable use cases.



Use case categories



Use of critical resource

- Execution of critical functions, reports and transactions
- Change, manipulation or spy out of business data
- Change or manipulation of critical configuration



User Manipulation

- Critical authorization assignment
- User role create, drop or manipulation
- Reference user assignment
- User morphing by changing type or probable identity theft



Debugging

- Debugging with change of control flow while debugging
- Debugging with change of variable values during debugging
- Debugging in critical systems
- Debugging in systems assigned to critical roles



System Access

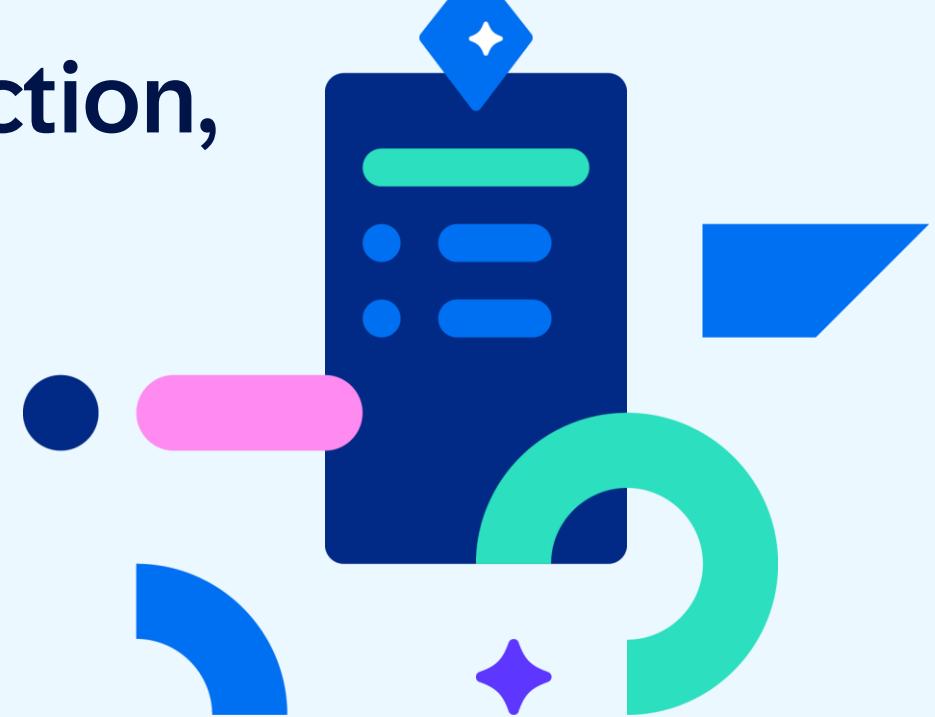
- Failed logon with too many attempts
- Failed Logon with too many password logon attempts
- Logon with SAP standard users, or high privileged users



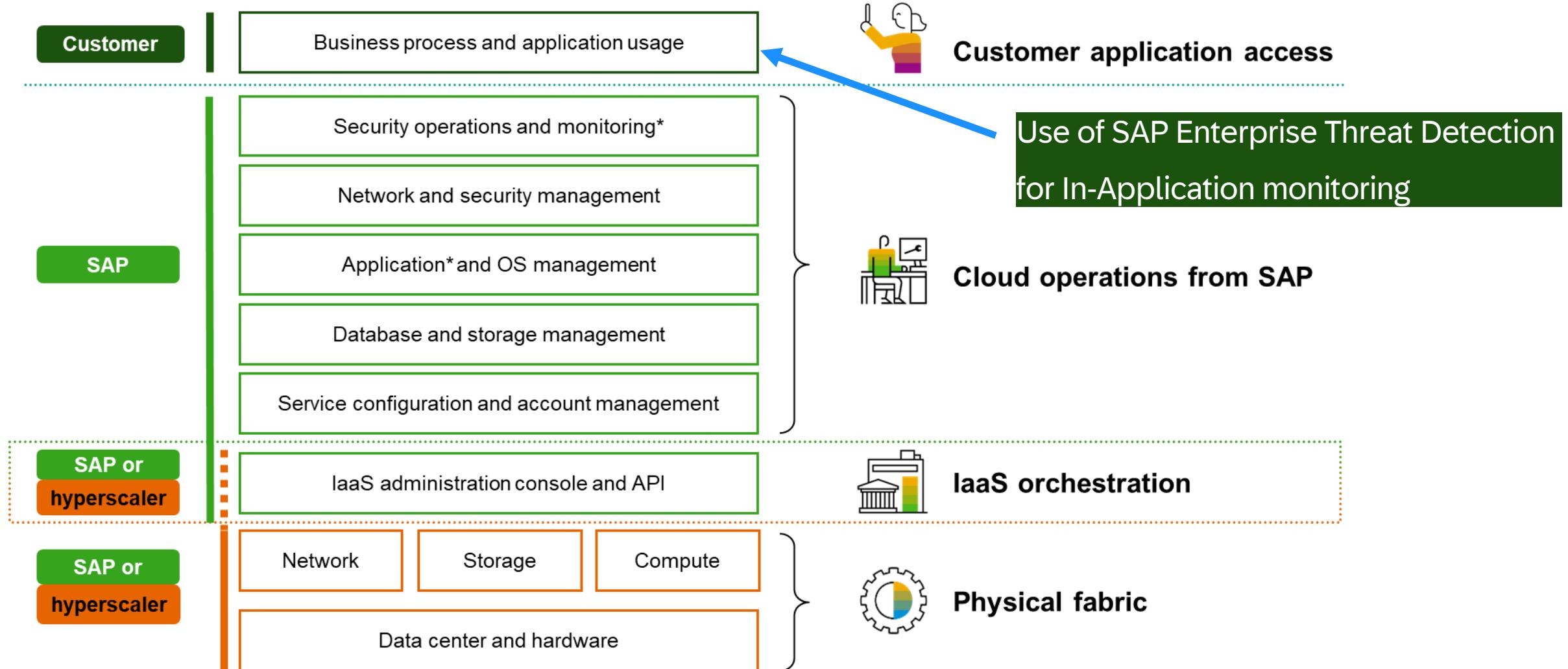
Suspicious Actions

- Dynamic program execution, download
- Dynamic code and system changes

SAP Enterprise Threat Detection, (public) cloud edition for Private/Public Cloud SAP Landscapes



SAP S/4HANA Private/Public Cloud: Shared responsibility



Short Demo/Preview



Security Analyst View/Partner View

The Security Analyst

- does alert processing, deep dive analysis, new use case creation, ...
- has a lot of tools at hand to do his job

The screenshot displays the SAP Security Analyst View interface. At the top, there is a navigation bar with the SAP logo, a 'Home' dropdown, and a search bar. Below the navigation bar, there are two tabs: 'Enterprise Threat Detection: Cross-Tenant Applications' (selected) and 'Enterprise Threat Detection: Tenant Applications'. The main area contains several cards representing different security functions:

- Enterprise Threat Detection: Cross-Tenant Applications**:
 - Select Tenant (with a cursor icon pointing to it)
 - Manage Alerts for All Tenants
 - Manage Investigations for All Tenants
- Enterprise Threat Detection: Tenant Applications**:
 - Manage Settings
 - Manage Value Lists
 - Analyze Log Events
 - Manage Alerts
 - Monitor Pattern Executions
 - Manage Patterns
 - Manage Investigations
 - Record of Actions
 - Download Investigation Reports
- Forensic Lab**
- Monitor Incoming Logs**
- Resolve User Identity**

Hands-on goes through

SAP Home ▾

Enterprise Threat Detection: Cross-Tenant Applications Enterprise Threat Detection: Tenant Applications

Select Tenant Manage Alerts for All Tenants Manage Investigations for All Tenants

Enterprise Threat Detection: Tenant Applications

Manage Settings Manage Value Lists Analyze Log Events Manage Alerts Monitor Pattern Executions Manage Patterns Manage Investigations Record of Actions Download Investigation Reports

Forensic Lab Monitor Incoming Logs Resolve User Identity

Investigation 143
Workshop Demo Customer

Subset 2

Service, Access Name	Access Names Indicating Debugging Method
In value list	

Count: 7

Subset 3

System Role, Actor	DebuggingCriticalSystems
In value list	DebuggingCriticalSystems

System ID, Actor

Program Names Indicating Debugging Method	DebuggingCriticalSystems
In value list	DebuggingCriticalSystems

Count: 2

Subset 2

System Role, Actor	DebuggingCriticalSystems
In value list	DebuggingCriticalSystems

System ID, Actor

Program Names Indicating Debugging Method	DebuggingCriticalSystems
In value list	DebuggingCriticalSystems

Count: 7

Range(2025/10/12 14:44:11 PM GMT+02:00 - 2025/10/13 14:44:11 PM GMT+02:00), Trigger Value 1(S4H).

Pattern	Trigger
Sensitive Data Download via Blocklisted Reports	Measurement 1 exceeded threshold 1 for ('Resource Name' = 'C:\Users\026896\Documents\SAP\SAP GUI\ddemo01.txt', 'Service,...'
Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon, Failure', 'Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'W-PF37QJMN', 'System ID, Actor' = 'S4H/100', 'System Type, Actor' = 'SAP Standard User')
Debugging in systems assigned to critical roles	Measurement 2 exceeded threshold 1 for ('Network, Hostname, Initiator' = 'W-PF37QJMN', 'System ID, Actor' = 'S4H/100', 'System Type, Actor' = 'SAP Standard User')
Authorization assignment by non-admin-group user	Measurement 2 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'LUOZ_16971', 'User Pseudonym,...')
Blocklisted transactions in productive system	Measurement 15 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')
Blocklisted transactions in productive system	Measurement 8 exceeded threshold 1 for ('Service, Transaction Name' = 'SU01', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')
Blocklisted Data Download in Transactions	Measurement 1 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')
Debugging with Manipulations in Critical Systems	Measurement 2 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'LUOZ_16971')
Debugging in systems assigned to critical roles	Measurement 1 exceeded threshold 1 for ('Network, Hostname, Initiator' = 'W-PF37QJMN', 'System ID, Actor' = 'S4H/100', 'System Type, Actor' = 'SAP Standard User')
Debugging in Critical ABAP Systems	Measurement 5 exceeded threshold 1 for ('System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'LUOZ_16971')
Generic access to critical database tables	Measurement 4 exceeded threshold 1 for ('Event Code' = 'DU9', 'Generic, Action' = 'Table Access', 'Resource Name' = 'USR02', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')
Critical DB access	Measurement 4 exceeded threshold 1 for ('Resource Name' = 'USR02', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')
Successful logon from same Terminal ID with different users	Measurement 3 exceeded threshold 2 for ('Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = '...')

Measurement 1 exceeded threshold 1 for ('Resource Name' = 'C:\Users\026896\Documents\SAP\SAP GUI\ddemo01.txt', 'Service, Program Name' = '/1BCDWB/DBUSR02', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'LUOZ_16971')

Description: A successful or unsuccessful logon external attempt... Show More

Base Measurement On: COUNT(DISTINCT All)

Group By: User Pseudonym, Target, System ID, Actor, Event (Semantic), Network, Hostname, Initiator

Logon from external with SAP standard users

10.0.0.7 User, Logon
10.79.59.150 User, Logon, Failure

Processor View

The Processor

- is another persona than the Security Analyst
- mainly consumes the results of the analysis

The screenshot shows a SAP interface titled "Enterprise Threat Detection". It features four main functional buttons:

- Download Investigation Reports**: Represented by a document icon.
- Manage Value Lists**: Represented by a list icon.
- Manage Patterns**: Represented by a puzzle piece icon.
- Monitor Incoming Logs**: Represented by a log file icon.

Hands-on goes through

SAP Home ▾

Enterprise Threat Detection

Download Investigation Reports	Manage Value Lists	Manage Patterns	Monitor Incoming Logs
--	------------------------------------	---------------------------------	---------------------------------------

Completion Timestamp: 2025/09/11 16:51:16 PM GMT+02:00

Closing Remarks: [REDACTED]

Investigator: [REDACTED]

Report Severity: Very High

Report Status: Open

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

Downloaded By: The report has not been downloaded yet.

Severity	ID	Report Creation Date	Description	Customer Notification
<input type="checkbox"/> High	142	2025/09/29 11:23:00 AM GMT+02:00	Critical user activities	No
<input type="checkbox"/> High	141	2025/09/26 14:11:51 PM GMT+02:00	Sensitive Data download	No
<input type="checkbox"/> High	140	2025/09/26 10:18:28 AM GMT+02:00	Critical Data Download	No
<input type="checkbox"/> High	138	2025/09/25 21:57:56 PM GMT+02:00	Critical Data download	No
<input type="checkbox"/> High	133	2025/09/22 17:13:32 PM GMT+02:00	USER is doing critical business manipulation	No
<input type="checkbox"/> High	132	2025/09/15 16:22:38 PM GMT+02:00	Standard User Manual Logon from different systems	No
<input type="checkbox"/> Medium	131	2025/09/11 17:36:59 PM GMT+02:00	Critical access abc Test	No
<input type="checkbox"/> High	130	2025/09/11 16:48:16 PM GMT+02:00	User Miss-Use on same terminal ID	No
<input type="checkbox"/> Medium	127	2025/09/10 16:43:55 PM GMT+02:00	Test9	Yes
<input type="checkbox"/> Medium	121	2025/09/10 15:12:22 PM GMT+02:00	huubui	No
<input type="checkbox"/> Medium	117	2025/09/03 09:53:52 AM GMT+02:00	User TMSADM failed with logons	No
<input type="checkbox"/> Medium	113	2025/08/05 08:55:13 AM GMT+02:00	TestReportWorkflows	No
<input type="checkbox"/> Very High	93	2025/07/16 09:59:17 AM GMT+02:00	User KOJG_68809 highly suspicious activities	No

SAP Download Investigation Reports ▾

Investigation Report 130 DATA LOSS MGMT_INFORMED

Completion Timestamp: 2025/09/11 16:51:16 PM GMT+02:00

Closing Remarks: [REDACTED]

Investigator: [REDACTED]

Report Severity: Very High

Report Status: Open

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

Downloaded By: The report has not been downloaded yet.

Comments (3) Download History

Enter your comment here

[REDACTED] created a comment.
2025/10/13 16:35:04 PM GMT+02:00
Result 3: Management was informed about the incident

2025/09/15 16:23:32 PM GMT+02:00	[REDACTED]	In Process	Medium	remark 1	LOB1
2025/09/11 17:37:58 PM GMT+02:00	[REDACTED]	No Reaction Needed		False positive, see ticket 423	
2025/09/11 16:51:16 PM GMT+02:00	[REDACTED]	Open	Very High		MGMT_INFORMED DATA LOSS
2025/09/10 16:45:18 PM GMT+02:00	[REDACTED]	No Reaction Needed	Low	Was acknowledged by ticket 158	
2025/09/10 15:48:13 PM GMT+02:00	[REDACTED]	Closed			
2025/09/03 09:57:15 AM GMT+02:00	[REDACTED]	In Process	Medium	checking	TMSADM SystemADMIN
2025/08/05 08:55:46 AM GMT+02:00	(Unassigned User)	Closed	High	Remediated by HCM department	LOB HCM BOARD
2025/07/16 10:23:24 AM GMT+02:00	(Unassigned User)				

Contact Information:

Kirti Singh
Product Manager
kirti.singh01@sap.com

Michael Schmitt
Product Manager
m.schmitt@sap.com

Thank you!



SAP Bring out your best.