SAP TechEd

CA163

Hands-on experience with SAP Enterprise Threat Detection

Kirti Singh, Arpita Deshpande, Shivaprasad Naik, Ankit Sharma

November 2025

SAP TechEd

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

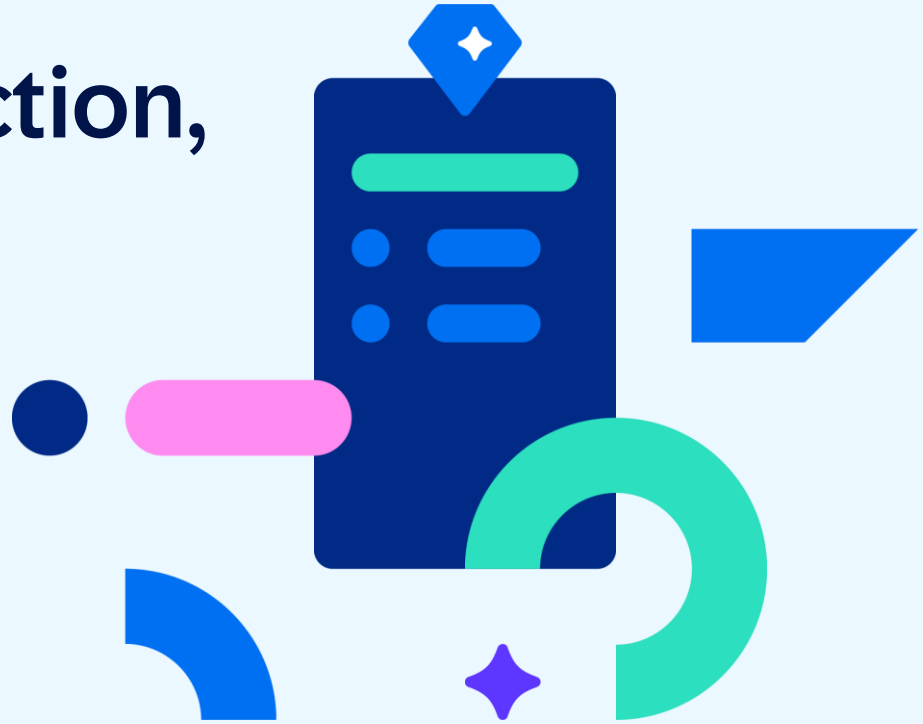
System Access

- 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

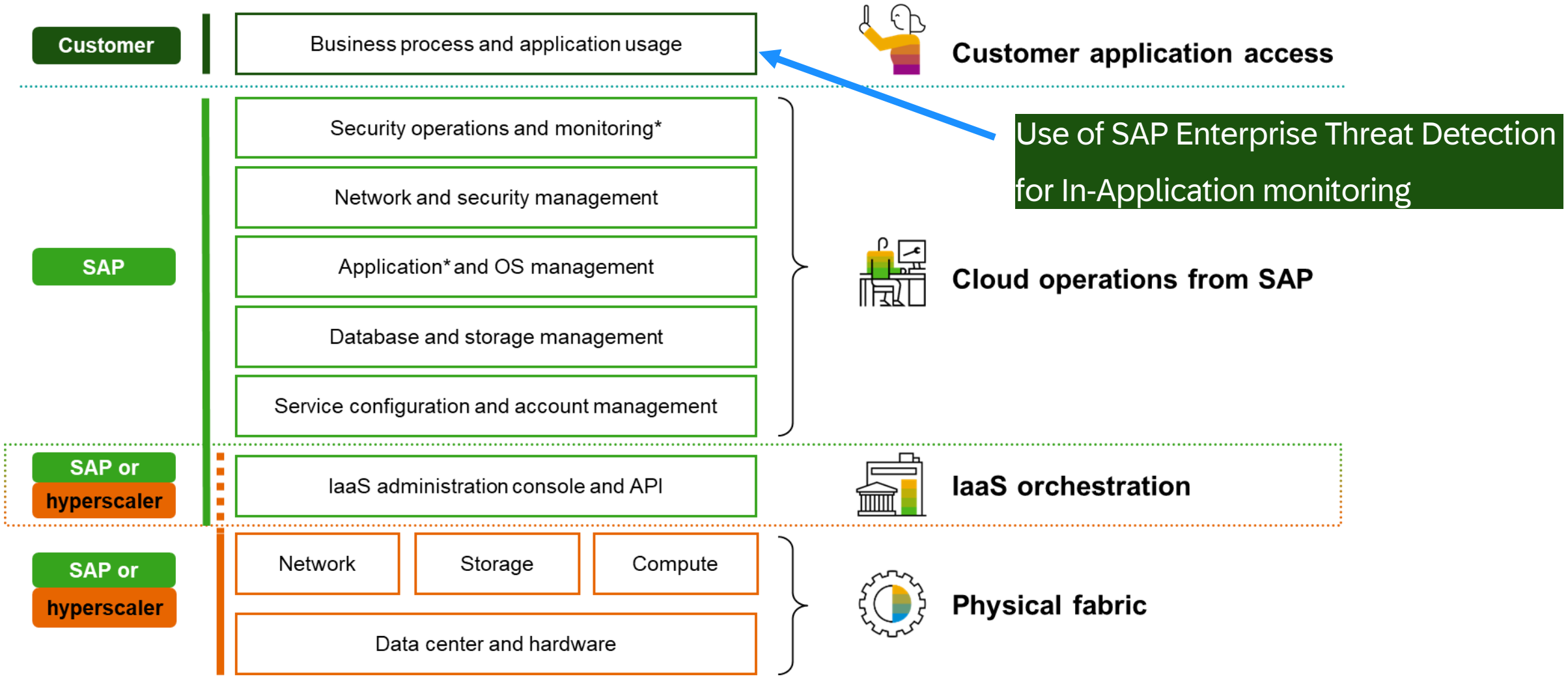
SAP Enterprise Threat Detection, (public) cloud edition for Private/Public Cloud SAP Landscapes



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

Run securely

Transparent



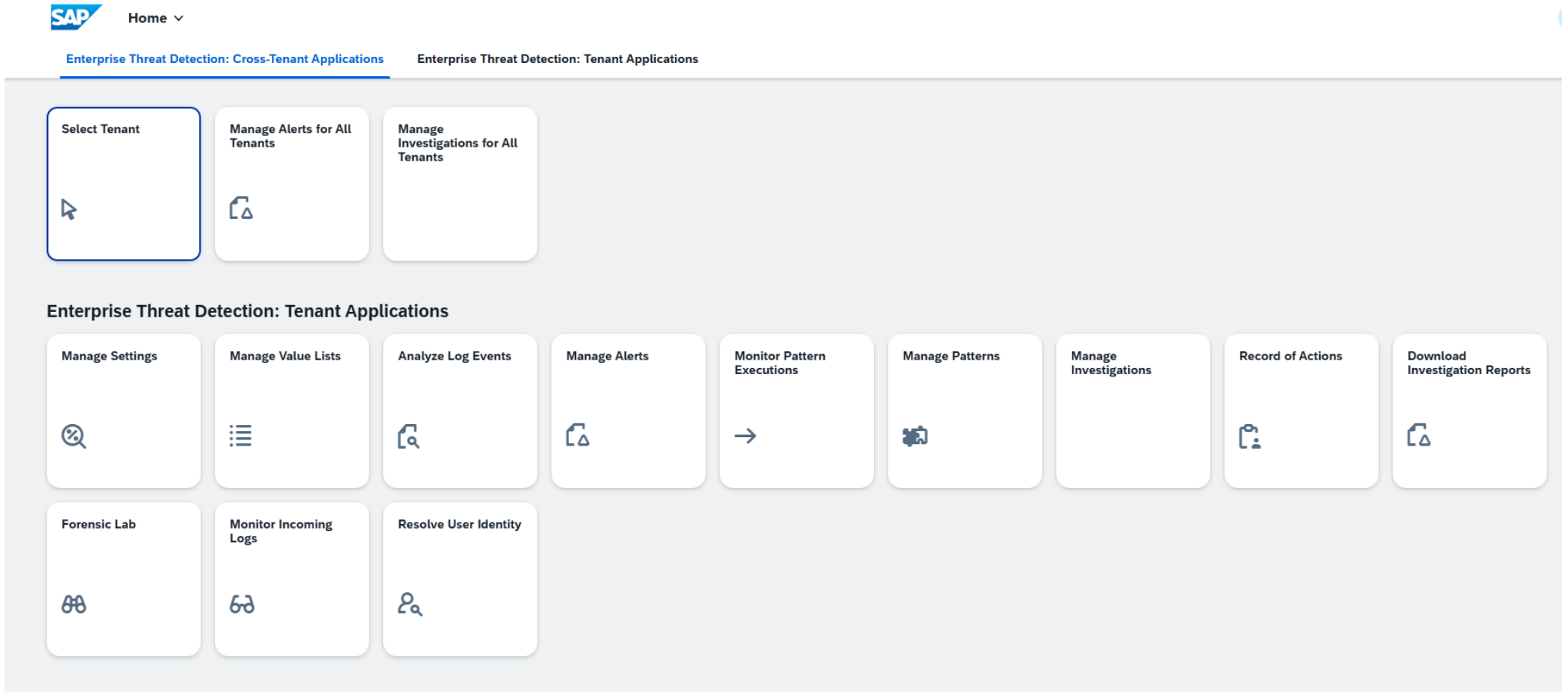
*Roles and responsibilities will vary depending on deployment (private, public).

Short Demo/Preview

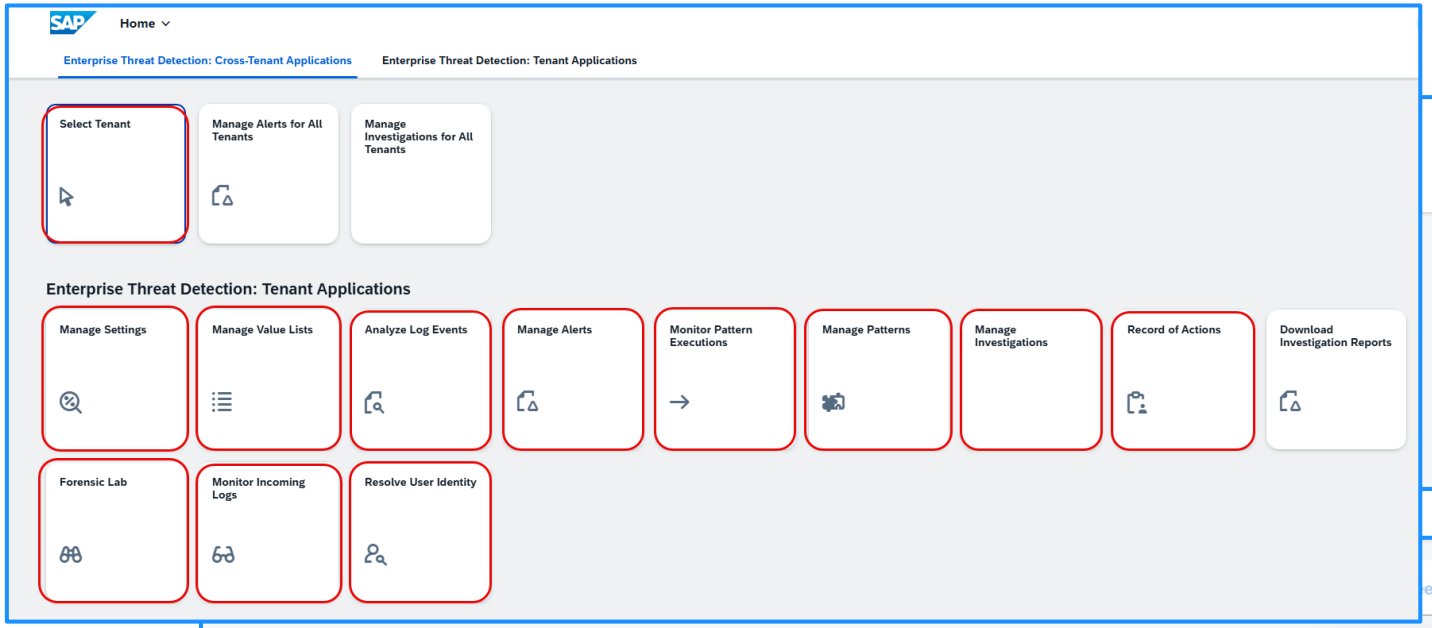
Security Analyst View/Partner View

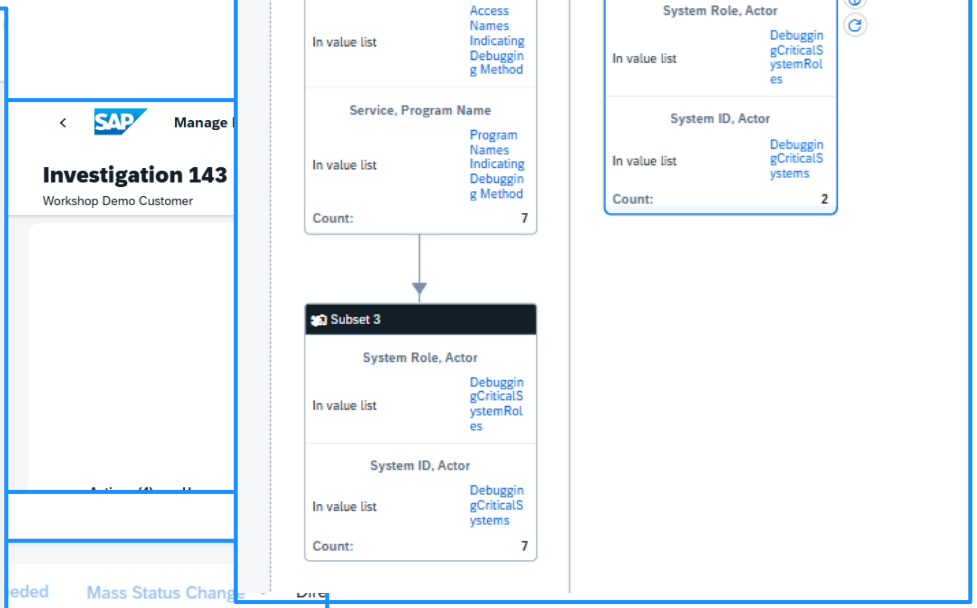
The Security Analyst

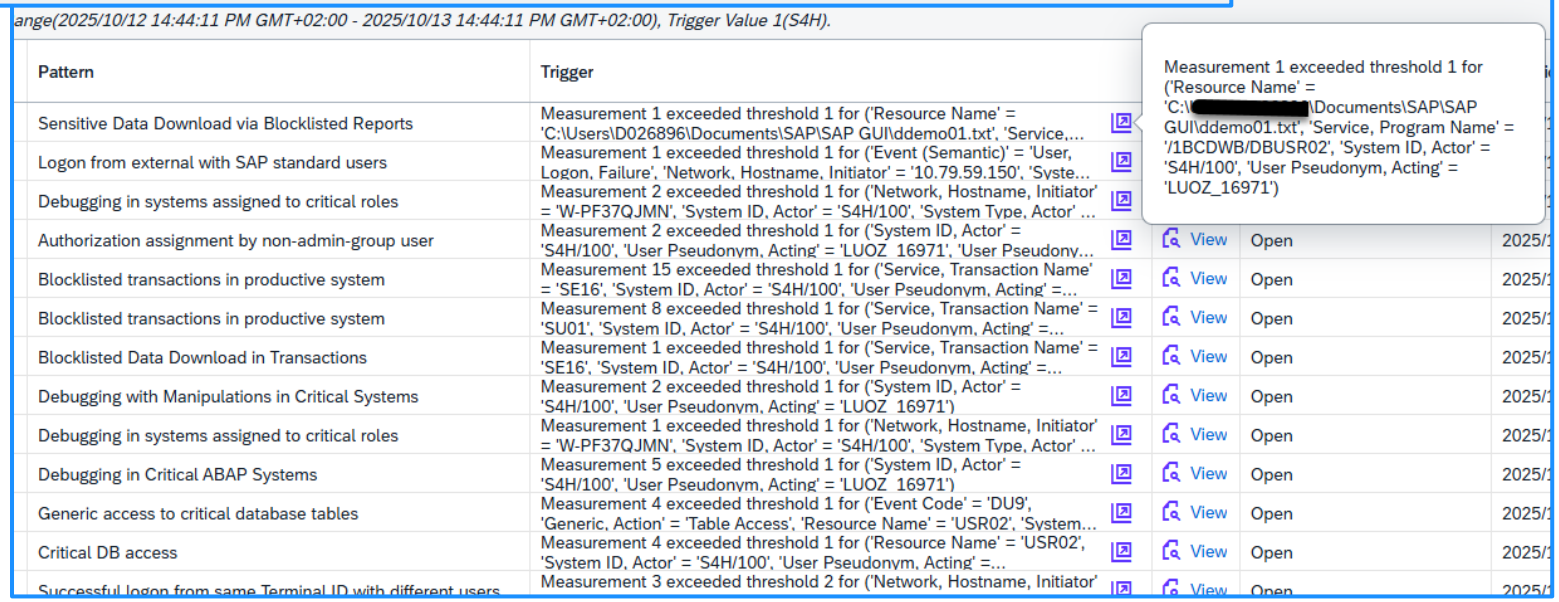
- does alert processing, deep dive analysis, new use case creation, ...
- has a lot of tools at hand to do his job



Hands-on goes through



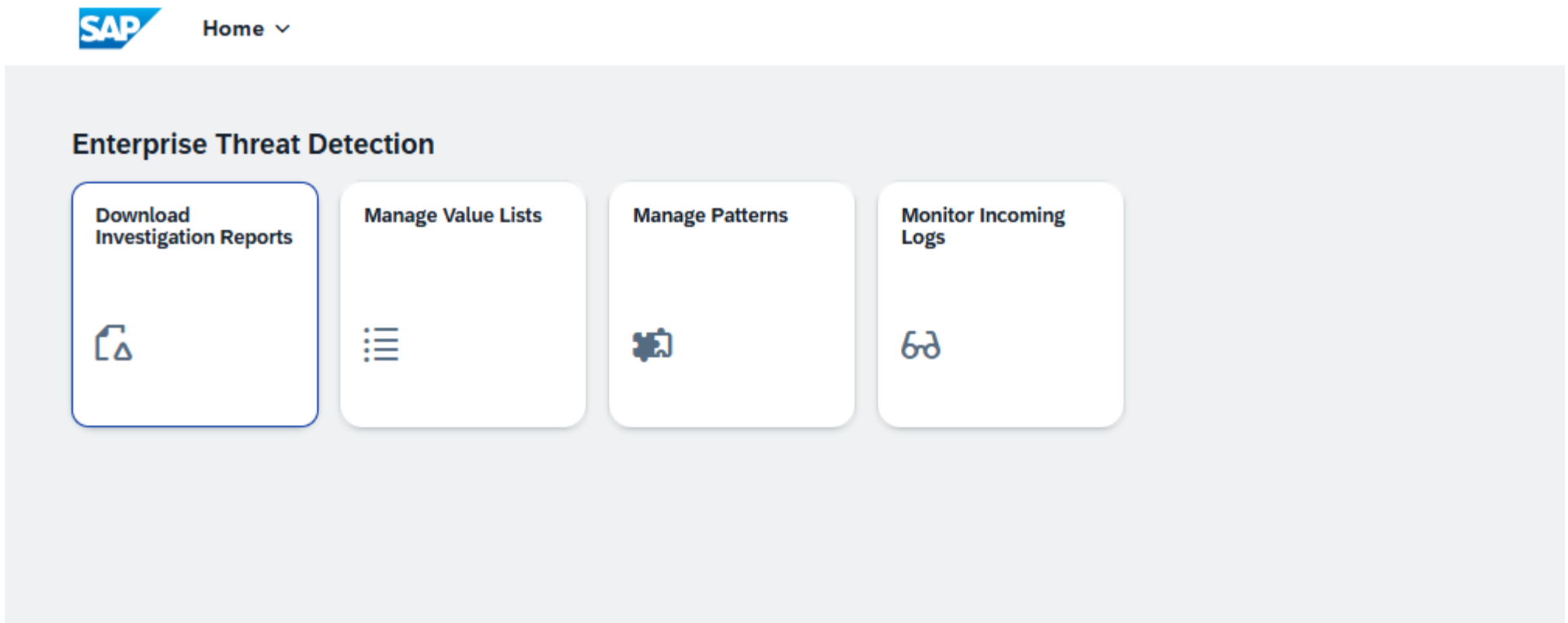




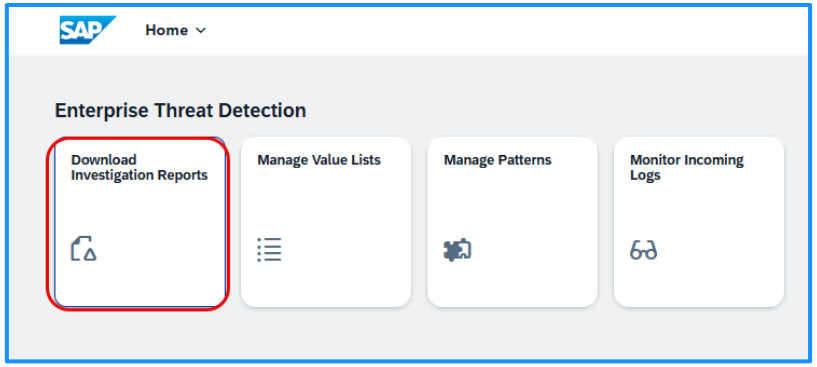
Processor View

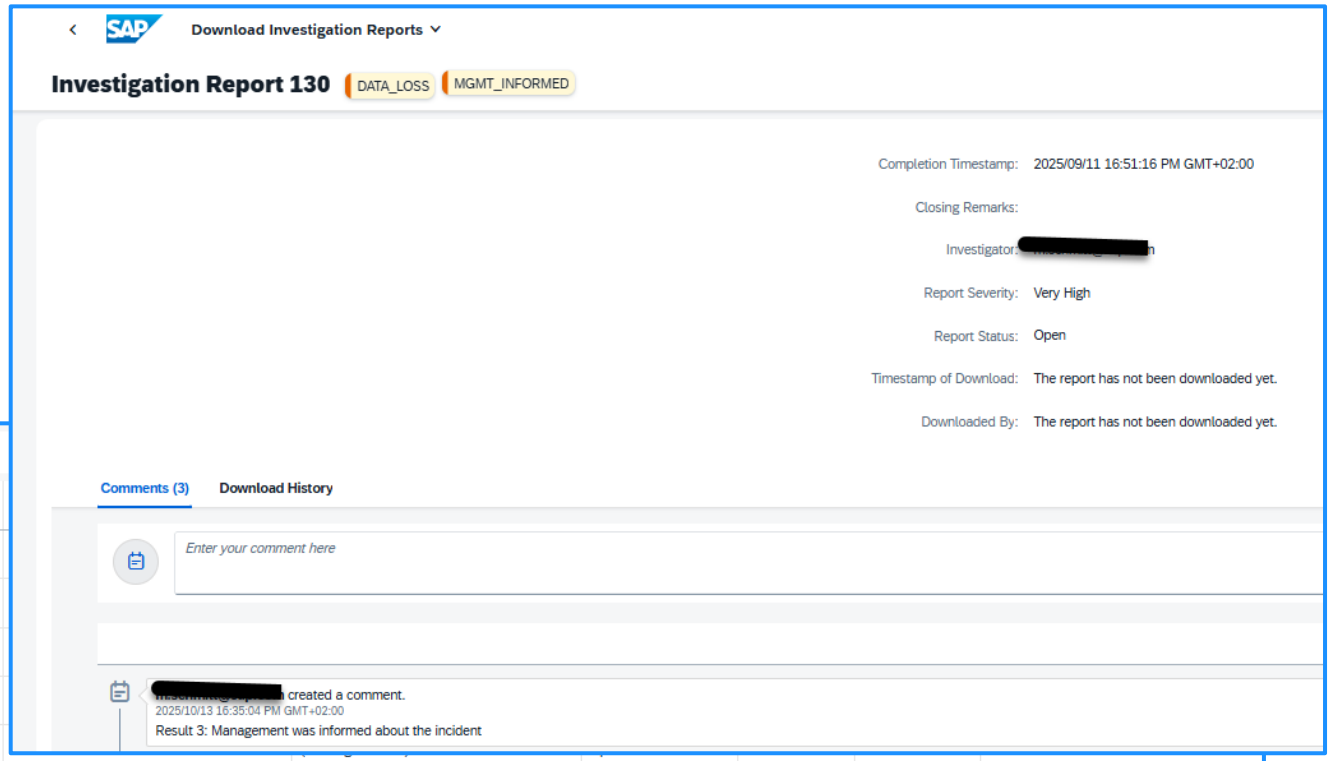
The Processor

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



Hands-on goes through





	Severity	ID	Report Creation Date	Description	Customer Notification						
☐	High	142	2025/09/29 11:23:00 AM GMT+02:00	Critical user cativities	No						
☐	High	141	2025/09/26 14:11:51 PM GMT+02:00	Sensitive Data download	No						
☐	High	140	2025/09/26 10:18:28 AM GMT+02:00	Critical Data Download	No						
☐	High	138	2025/09/25 21:57:56 PM GMT+02:00	Critical Data download	No						
☐	High	133	2025/09/22 17:13:32 PM GMT+02:00	USER is doing critical business manipulation	No						
☐	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	[redacted]	In Process	Medium	remark 1	LOB1
☐	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	[redacted]	No Reaction Needed		False positive, see ticket 423	
☐	High	130	2025/09/11 16:48:16 PM GMT+02:00	Useer Miss-Use on same terminal ID	No	2025/09/11 16:51:16 PM GMT+02:00	[redacted]	Open	Very High		MGMT_INFORMED DATA_LOSS
☐	Medium	127	2025/09/10 16:43:55 PM GMT+02:00	Test9	Yes	2025/09/10 16:45:18 PM GMT+02:00	[redacted]	No Reaction Needed	Low	Was acknowledged by ticket 158	
☐	Medium	121	2025/09/10 15:12:22 PM GMT+02:00	huubui	No	2025/09/10 15:48:13 PM GMT+02:00	[redacted]	Closed			
☐	Medium	117	2025/09/03 09:53:52 AM GMT+02:00	User TMSADM failed with logons	No	2025/09/03 09:57:15 AM GMT+02:00	[redacted]	In Process	Medium	checking	TMSADM SystemADMIN
☐	Medium	113	2025/08/05 08:55:13 AM GMT+02:00	TestReportWorkflows	No	2025/08/05 08:55:46 AM GMT+02:00	(Unassigned User)	Closed	High	Remediated by HCM department	LOB HCM BOARD
☐	Very High	93	2025/07/16 09:59:17 AM GMT+02:00	User KOJG_68809 highly suspicious activities	No	2025/07/16 10:23:24 AM GMT+02:00	(Unassigned User)				

SAP TechEd

Contact Information:

Kirti Singh
Product Manager
kirti.singh01@sap.com

Michael Schmitt
Product Manager
m.schmitt@sap.com

Thank you!

Bring out your best.