



# SAP Security Webcast

## Applying Modern AI to (SAP) Security: SAP Enterprise Threat Detection — Current Capabilities and Future Prospects

Dr. Michael Schmitt, SAP  
Dec 18 2025



# Disclaimer

The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. Except for your obligation to protect confidential information, this presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this presentation or any related document, or to develop or release any functionality mentioned therein.

This presentation, or any related document and SAP's strategy and possible future developments, products and or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information in this presentation is not a commitment, promise or legal obligation to deliver any material, code or functionality. This presentation is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or non-infringement. This presentation is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this presentation, except if such damages were caused by SAP's intentional or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

# Agenda

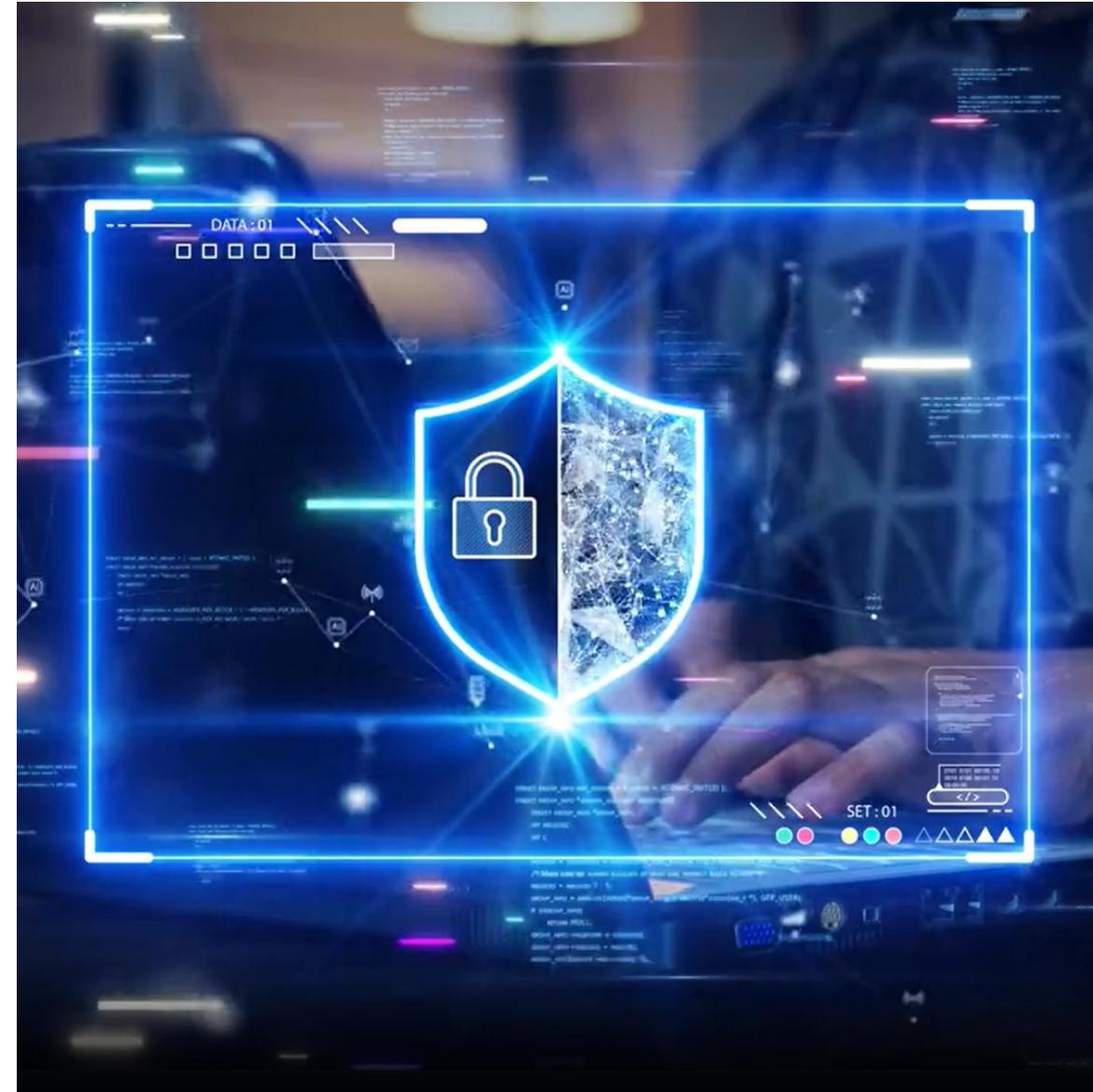
1. **Current (and near future) features of SAP Enterprise Threat Detection on AI- and (in general:) Automation- functions**
2. **Excerpt: Research on AI for SAP-security use cases**
3. **Side Trip: Applicability to other Security Domains (e.g. Industry 4.0)**
4. **Research Results, and benefits about topics**
  - **Reproducibility**
  - **Hallucinations, Silent Truncation, different answers to the same question**
  - **Formatting**
  - **Compliance Aspects**
  - **... overcome an issue of trustworthiness**
5. **Retrofit of the results into SAP Enterprise Threat Detection, and outlook**

# What is SAP Enterprise Threat Detection

## *Public Cloud Edition*

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.





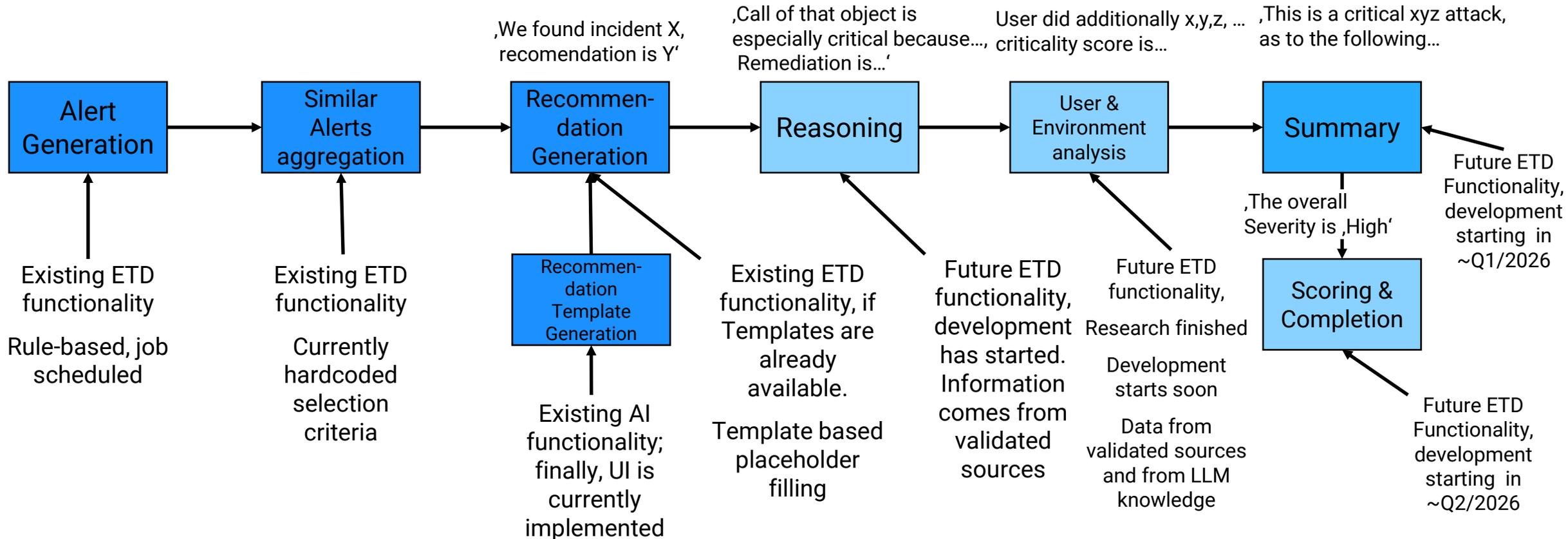
# Current, and not too far away AI- and automation-features in SAP Enterprise Threat Detection





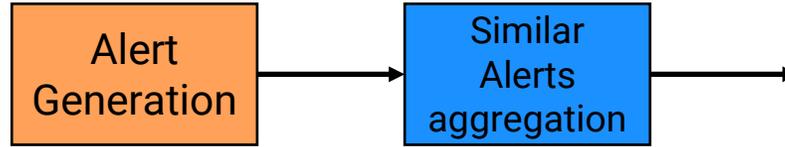
# Automation, about what?

Use case in focus: Automate the whole process ‘From Incident to Response’ within SAP Enterprise Threat Detection





# Alert Generation

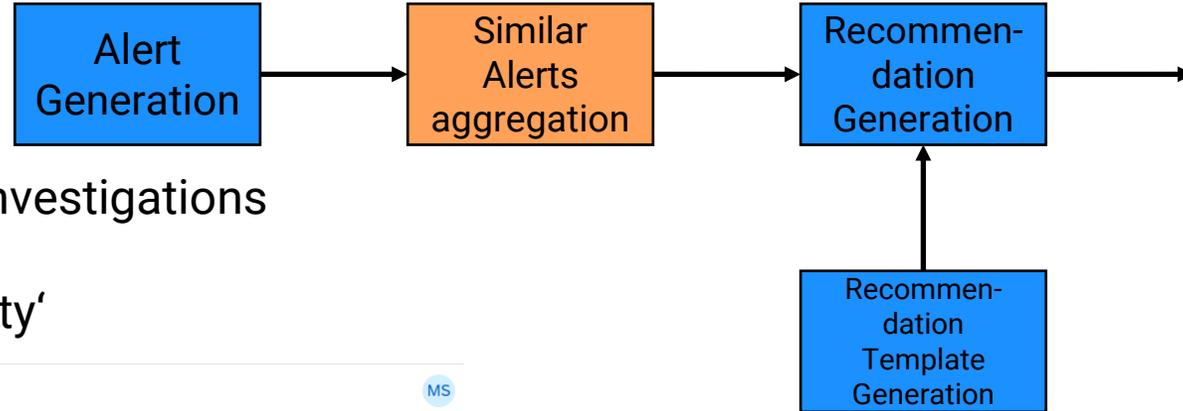


- Job Scheduled Rules based generation of Alerts
- ~150 out of the box-use cases as content
- Own use cases can be created
  - From Scratch
  - By using SAP content as template

Alerts (150)								
Filtered By: alerts.creationTimeRange(2025/12/08 16:08:06 PM GMT+01:00 - 2025/12/09 16:08:06 PM GMT+01:00)								
<input type="checkbox"/>	Severity	ID	Pattern	Trigger	Events	Status	Creation Time	Remaining Reaction Time (RRT)
<input type="checkbox"/>	Medium	143892	Critical manual in-ABAP SQL statement execution	Measurement 1 exceeded threshold 1 for ('Parameter Name' = 'SQL Statement', 'Parameter Value, String' = 'drop table jhgihghg', 'Service,...	<a href="#">View</a>	Open	2025/12/09 16:08:00 PM GMT+01:00	23 Hours 59 Minutes 53 Seconds
<input type="checkbox"/>	Medium	143891	Function Module Executed in Test Environment	Measurement 1 exceeded threshold 1 for ('Service, Access Name' = '<local>', 'Service, Function Name' = 'BAPI_USER_GET_DETAIL',...	<a href="#">View</a>	Open	2025/12/09 16:00:58 PM GMT+01:00	23 Hours 52 Minutes 51 Seconds
<input type="checkbox"/>	High	143887	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon', 'Network, Hostname, Initiator' = '10.0.0.7', 'System ID, Actor' =...	<a href="#">View</a>	Open	2025/12/09 16:00:52 PM GMT+01:00	23 Hours 52 Minutes 45 Seconds
<input type="checkbox"/>	High	143888	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User, Logon', 'Network, Hostname, Initiator' = 'W-PF37QJMN', 'System ID,...	<a href="#">View</a>	Open	2025/12/09 16:00:52 PM GMT+01:00	23 Hours 52 Minutes 45 Seconds
<input type="checkbox"/>	Medium	143889	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/000')	<a href="#">View</a>	Open	2025/12/09 16:00:52 PM GMT+01:00	23 Hours 52 Minutes 45 Seconds
<input type="checkbox"/>	Medium	143890	Successful logon from same Terminal ID with different users	Measurement 4 exceeded threshold 2 for ('Network, Hostname, Initiator' = '10.79.59.150', 'System ID, Actor' = 'S4H/100')	<a href="#">View</a>	Open	2025/12/09 16:00:52 PM GMT+01:00	23 Hours 52 Minutes 45 Seconds
<input type="checkbox"/>	Medium	143886	Suspicious Bank SWIFT Code change	Measurement 1 exceeded threshold 1 for ('Parameter Value, String' = 'HYVEDEMM241', 'Parameter Value, String, Context' = '100DE...	<a href="#">View</a>	Open	2025/12/09 16:00:40 PM GMT+01:00	23 Hours 52 Minutes 33 Seconds
<input type="checkbox"/>	High	143885	Logon after access to USR02	Measurement 1 exceeded threshold 1 for ('Network, Hostname, Initiator' = 'W-PF37QJMN', 'System ID, Actor' = 'S4H/100', 'User Pseudonym,...	<a href="#">View</a>	Open	2025/12/09 16:00:26 PM GMT+01:00	23 Hours 52 Minutes 19 Seconds
<input type="checkbox"/>	High	143884	Blocklisted transactions in productive system	Measurement 5 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' =...	<a href="#">View</a>	Open	2025/12/09 16:00:25 PM GMT+01:00	23 Hours 52 Minutes 18 Seconds
<input type="checkbox"/>	High	143883	Blocklisted transactions in productive system	Measurement 5 exceeded threshold 1 for ('Service, Transaction Name' = 'SE37', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' =...	<a href="#">View</a>	Open	2025/12/09 16:00:25 PM GMT+01:00	23 Hours 52 Minutes 18 Seconds
<input type="checkbox"/>	High	143882	Blocklisted transactions in productive system	Measurement 9 exceeded threshold 1 for ('Service, Transaction Name' = 'SE38', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' =...	<a href="#">View</a>	Open	2025/12/09 16:00:25 PM GMT+01:00	23 Hours 52 Minutes 18 Seconds
<input type="checkbox"/>	High	143881	Critical Function module call in Test framework calls	Measurement 1 exceeded threshold 1 for ('Network, IP Address, Initiator' = '193.16.224.1', 'Service, Function Name' =...	<a href="#">View</a>	Open	2025/12/09 15:55:57 PM GMT+01:00	23 Hours 47 Minutes 50 Seconds
<input type="checkbox"/>	High	143880	Generic access to critical database tables	Measurement 2 exceeded threshold 1 for ('Event Code' = 'DU9', 'Generic, Action' = 'Table Access', 'Resource Name' = 'USR02', 'System...	<a href="#">View</a>	Open	2025/12/09 15:55:25 PM GMT+01:00	23 Hours 47 Minutes 18 Seconds
<input type="checkbox"/>	High	143879	Critical DB access	Measurement 2 exceeded threshold 1 for ('Resource Name' = 'USR02', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'ETDADMIN')	<a href="#">View</a>	Open	2025/12/09 15:55:07 PM GMT+01:00	23 Hours 47 Minutes
<input type="checkbox"/>	High	143877	Logon from external with SAP standard users	Measurement 1 exceeded threshold 1 for ('Event (Semantic)' = 'User,...	<a href="#">View</a>	Open	2025/12/09 15:50:52 PM GMT+01:00	23 Hours 42 Minutes 45 Seconds

# Similar Alerts

- Less effort to aggregate similar alerts in investigations
- Currently very strict selection
- Future: More flexible Definition of ‚Similarity‘



MS

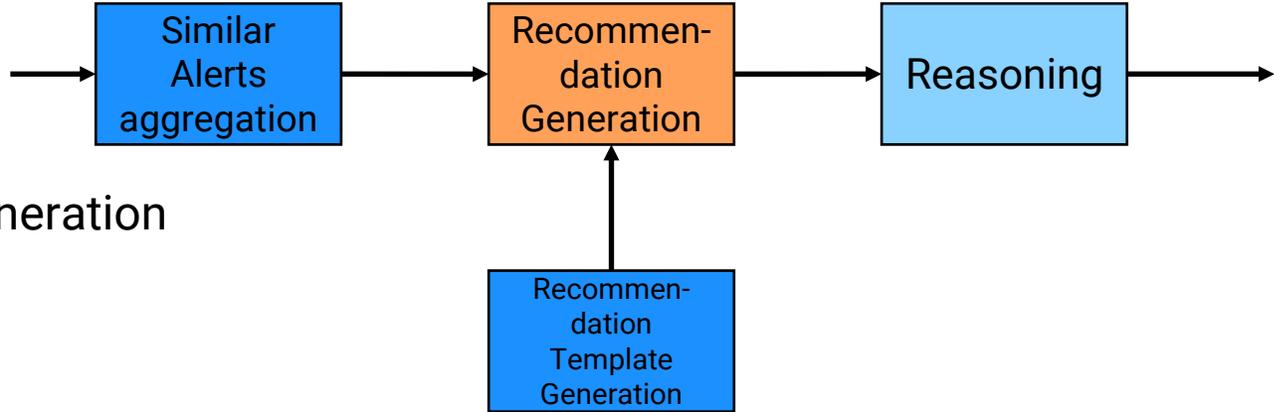
Generate Recommendation
Edit
?

Creation Time: 2025/12/09 16:13:28 PM GMT+01:00  
 Created By: m.schmitt@sap.com  
 Description: Suspicious activities by user ETDADMIN  
 Severity: High  
 Processor: Oppo, Tunity  
 demo93@etdsap.com  
 Status: Open  
 Customer Notification:   
 Management Visibility: Not Needed  
 Remaining Processing Time (RPT): 🕒 23 Hours 59 Minutes 56 Seconds

Trigger	Events	Severity	Creation Time	
Measurement 5 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'ETDADMIN')	<a href="#">View</a>	High	2025/12/09 16:00:25 PM GMT+01:00	<a href="#">Collect Similar Alerts</a>
Measurement 61 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'MSXC_92758')	<a href="#">View</a>	High	2025/11/25 08:50:37 AM GMT+01:00	
Measurement 61 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'CAYH_63107')	<a href="#">View</a>	High	2025/11/25 08:50:37 AM GMT+01:00	
Measurement 61 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'CAYH_63107')	<a href="#">View</a>	High	2025/11/25 08:40:39 AM GMT+01:00	
Measurement 61 exceeded threshold 1 for ('Service, Transaction Name' = 'SE16', 'System ID, Actor' = 'S4H/100', 'User Pseudonym, Acting' = 'CAYH_63107')	<a href="#">View</a>	High	2025/11/25 08:40:39 AM GMT+01:00	

Add to Investigation
Cancel

# Recommendation Generation



- Template based Recommendation generation
- Placeholders are filled with data from
  - Alert Header
  - Alert Details
  - Triggering Events

## Investigation 275

Workshop Demo Customer

Generate Recommendation
Edit
🔗

Creation Time: 2025/12/09 16:13:28 PM GMT+01:00  
 Created By: m.schmitt@sap.com  
 Description: Suspicious activities by user ETDADMIN  
 Severity: High  
 Processor: Oppo, Tunity  
               demo93@etdsap.com  
 Status: Open  
 Customer Notification:   
 Management Visibility: Not Needed  
 Remaining Processing Time (RPT): 🟢 23 Hours 59 Minutes 56 Seconds

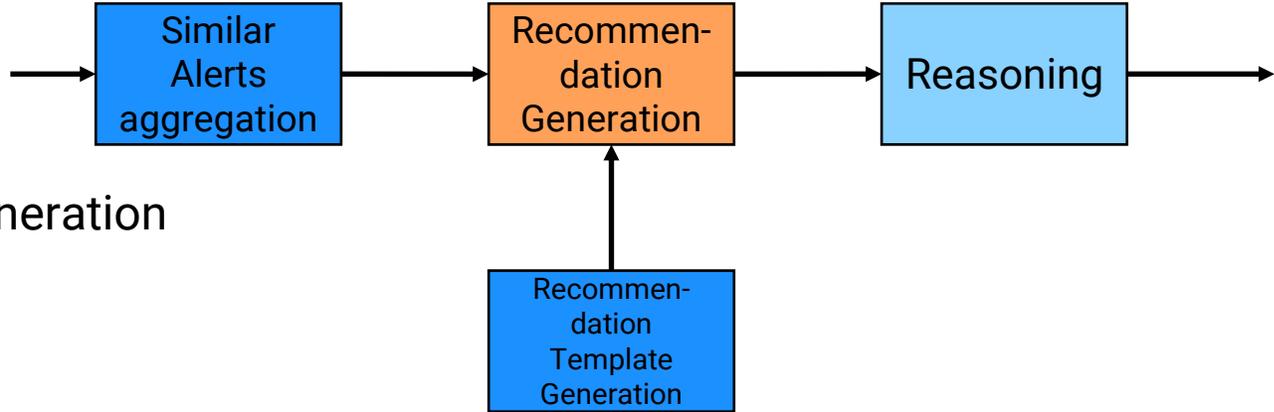
[Actions \(9\)](#)  
 [Users](#)  
 [Alerts \(5\)](#)  
 [Log Events \(0\)](#)



Investigation Result: Our monitoring system has detected that the user [ETDADMIN, KIRK, ETDADMIN98] executed the blocklisted transaction: [SE16] in the productive system [S4H/100] during the time frame of [2025-12-02T09:50:42] - [2025-12-09T14:54:30]. This transaction is part of a list of transactions that are recommended by SAP to be tightly controlled and not typically executed in productive environments due to their potential impact on system integrity and security.



# Recommendation Generation



- Template based Recommendation generation
- Placeholders are filled with data from
  - Alert Header
  - Alert Details
  - Triggering Events

## Investigation 275

Workshop Demo Customer

Generate Recommendation
Edit
🔗

Creation Time: 2025/12/09 16:13:28 PM GMT+01:00  
 Created By: m.schmitt@sap.com  
 Description: Suspicious activities by user ETDADMIN  
 Severity: High  
 Processor: Oppo, Tunity  
 demo93@etdsap.com  
 Status: Open  
 Customer Notification:   
 Management Visibility: Not Needed  
 Remaining Processing Time (RPT): 🟢 23 Hours 59 Minutes 56 Seconds

[Actions \(9\)](#)
[Users](#)
[Alerts \(5\)](#)
[Log Events \(0\)](#)

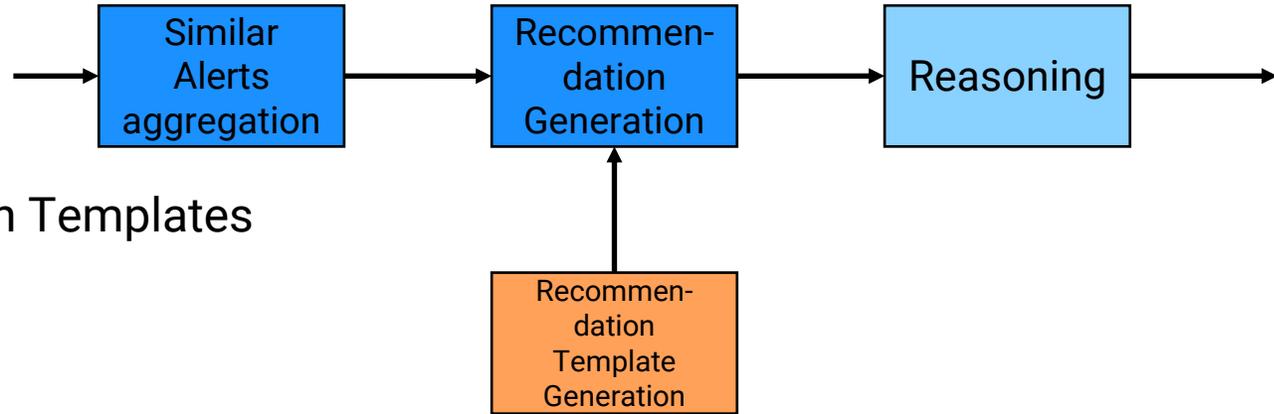


Investigation Result: Our monitoring system has detected that the user [ETDADMIN, KIRK, ETDADMIN98] executed the blocklisted transaction: [SE16] in the productive system [S4H/100] during the time frame of [2025-12-02T09:50:42] - [2025-12-09T14:54:30]. This transaction is part of a list of transactions that are recommended by SAP to be tightly controlled and not typically executed in productive environments due to their potential impact on system integrity and security.



# Recommendation Template Generation

- AI based creation of Recommendation Templates
- UI preview (no mockup)



Details   Used Value Lists   Postprocessing Work Items   **SOP Template**

---

SOP Template

Use AI to generate a SOP Template.

Try to:

1. Include information you want the customer to be informed about
2. Define the recommended Actions the Customer should take after this pattern has been detected

Generate a SOP with the following actions:

- Review User Activity
- Verify System ID
- Investigate and Mitigate
- Implement Controls

I've created the Template and integrated the required actions

Describe the SOP to generate...

**Template Preview** History

Investigation Result: We have noticed that {{{AlertDetails.UserPseudonymTargeted}}} has been reported to be attempting multiple unsuccessful logons from unique Terminal IDs within {{{AlertDetails.SystemidActor}}}. These attempts occurred {{{Alert.TriggeringEventCount}}} times during the time frame of {{{Alert.MinTimestamp}}} - {{{Alert.MaxTimestamp}}}. This pattern of behavior is unusual and could potentially indicate malicious activity or an oversight of our security protocol. Action: It is recommended that you conduct a thorough investigation into the audit logs for logins referring to the targeted userID mentioned previously above, within the given period of {{{Alert.MinTimestamp}}} - {{{Alert.MaxTimestamp}}}. After reviewing, the necessary actions should be undertaken and it could include strengthening your security measures, changing credentials for the targeted userID or conducting further investigations on the origin of these attempts from the {{{TriggeringEvents.EventSourceid}}}. It is vital to ensure that your system remains secured and protected against potential external attacks.'

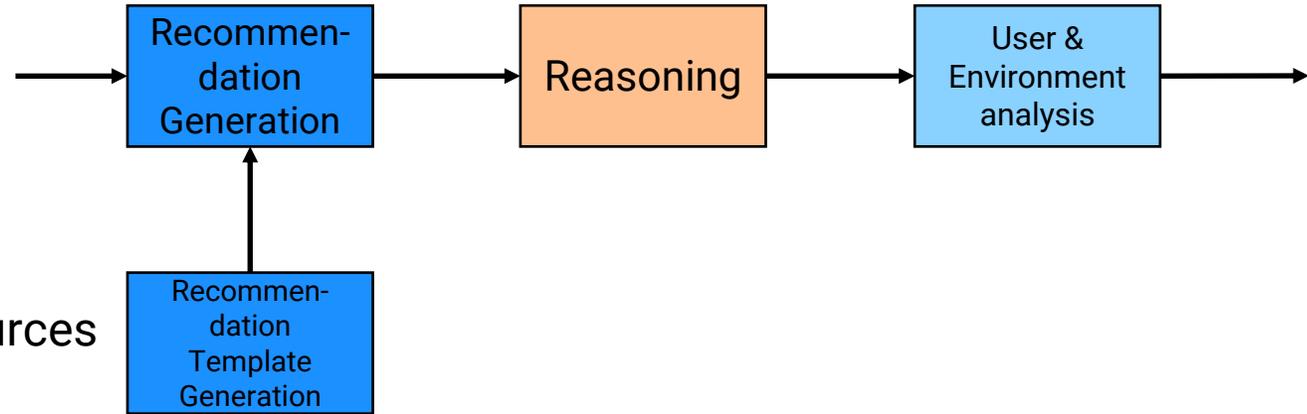
Created with AI. Verify results before use

Queries (2) Create Delete Insert in Template

<input type="checkbox"/>	Placeholder	Attribute Name	Aggregation Fu..
<input type="checkbox"/>	AlertDetails.Syste midActor	SystemidActor	None
<input type="checkbox"/>	Alert.MinTimest amp	MinTimestamp	MIN

# Reasoning

- Reasoning details about objects, paths, privileges etc.
- High Quality Data from evaluated sources
- Preview only



**Investigation Result 1:** Our monitoring system has detected that the user [ETDADMIN99, ETDDEMO99, ETDADMIN98] executed the blocklisted transaction: [SE16] in the productive system [S4H/100] during the time frame of [2025-10-17T06:26:44] - [2025-11-20T07:38:18]. This transaction is part of a list of transactions that are recommended by SAP to be tightly controlled and not typically executed in productive environments due to their potential impact on system integrity and security. \nAction: Immediately investigate the reported execution of the blocklisted transaction [SE16] by [ETDADMIN99, ETDDEMO99, ETDADMIN98] in the productive system [S4H/100]. Determine the legitimacy and intent behind this execution, verify the user's authorization, and assess the potential impact. Take appropriate corrective measures.

**Explanation Transaction SE16:**

SAP transaction SE16 is critical because it allows mass data editing, which can lead to data integrity loss or unauthorized access.

Mitigation 1: Restrict access to trusted users only by assigning authorized roles.

Mitigation 2: Enable logging and regularly audit SE16 usage for suspicious activities.

**Investigation Result 3:** Our monitoring system has detected that the user [ETDADMIN99] assigned the critical profile: [SAP\_ALL] to user [ETDDEMO99] in the productive system [S4H/100] during the time frame of [2025-10-17T06:26:44] - [2025-11-20T07:38:18]. This Profile is part of a list of critical profiles that are recommended by SAP to be tightly controlled and not typically executed in productive environments due to their potential impact on system integrity and security. \nAction: Immediately investigate the reported provisioning of the profile [SAP\_ALL] by [ETDADMIN99] to [ETDDEMO99] in the productive system [S4H/100]. Determine the legitimacy and intent behind this execution, verify the user's additional activities, and assess the potential impact. Take appropriate corrective measures.

**Explanation Authorization SAP\_ALL:**

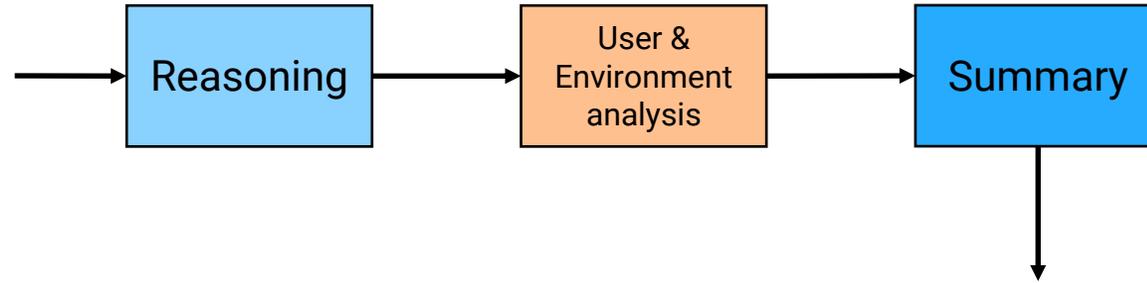
The SAP\_ALL profile is critical because it grants unrestricted access to all SAP functions and data, posing significant security risks.

Mitigation 1: Use the least privilege principle. Assign other roles like SAP\_NEW or custom roles with limited permissions.

Mitigation 2: Regularly review and update user authorizations to ensure only necessary access is maintained.



## User & Environment analysis (UEBA)



*Excerpt: Research on AI for SAP-security use cases*

# Excerpt: Research on AI for SAP-security use cases





# Research Excerpt: User & Environment analysis I

## Typical questions:

- What did the user ID (alternative the IP address, the machine ID, mail address, corelated user IDs...) do in a time range of n hours/days/weeks before the alert?
- How security critical/relevant are the the additional activities?

Typical log data:

The screenshot shows the SAP Log Events analysis interface for a 'Workshop Demo Customer'. The main table displays log events filtered by 'Semantic Event(Contains,Generic), Resource, Name(Contains,T000)'. The table has columns for 'Timestamp' and 'Semantic Event'. Three log entries are visible, all with a timestamp of 2025/12/10 08:54:15 AM GMT+01:00 and a semantic event of 'Database, Data, Select, G'. A red box highlights the 'Table Access' action in the 'Generic Information' panel. Another red box highlights 'D SE16 passed' in the 'Service Information' panel. A third red box highlights 'T000' in the 'Resource' panel. A blue box highlights a text area containing the following text:

Very important and beneficial:  
ETD has a normalized data model, which identifies the object which was used, accessed, provided (e.g. Transactions, Function Modules, Services, Executables, Privileges...)

# Research Excerpt: User & Environment analysis II

**Goal, by asking an LLLM-AI about the security criticality of any object usage, access to resources, provisioning of privileges, etc. In the SAP Security Domain, as well as in other Security Domains (e.g. Industrie 4.0):**

- **Enforce Reproducibility** (→ ask the same question, you get different answers)
  - **First result at research:** Reproducibility is not all grantable, exact answers for criticality decisions are highly in question ⚡
- **Remove 'Silent Truncation'** (→ Ask for Reading big documents, AI optimizes the reading and just does only an 'overlook reading' of parts)
  - **First result at research:** This is a showstopper for any security related, somehow a bit more complex ask ⚡
- **Remove Hallucination** (→ Ask for certain objects, AI might pretend it is known, but in reality does not exist)
  - **First result at research:** Hallucinations seem to happen once in a while, it is difficult to detect them ⚡
- **Enforce a machine readable output (JSON/XML format)** (→ Ask for a XML/JSON output, and make sure this format is kept)
  - **First result at research:** It is difficult to enforce a corresponding machine-readable output ⚡
- **Enforce AI agnostic queries/outputs** (→ Ask different AIs, very often the output format varies, as well as the answers might vary in context)
  - **First result at research:** It is difficult to have an AI agnostic output (especially output format, as well as a kind of output quality) ⚡
- **Make the results traceable** (→ Ask a complex question, AI provides answers, but the reasoning, sourcing, and validity to be checked/traced)
  - **First result at research:** It is difficult to get a level traceability if you ask somehow complex questions ⚡

# SAP Research Excerpt: User & Environment analysis III

## Second result of research

**Result:** It works!

**Result:** The way to arrive is the final decisive success factor

- **Enforce Reproducibility**
  - **Resolved by:** Small Prompts, use output from last prompt as input for next prompt, no context ✓
- **Remove ‚Silent Truncation‘**
  - **Resolved by:** Small Prompts, no context and no long ‚discussions‘; e.g. ask for verbatim deviations of different answers ✓
- **Remove Hallucination**
  - **Resolved by:** Ask especially about, if not known, to tell that ✓
- **Enforce a machine readable output (JSON/XML format)**
  - **Resolved by:** Provide Example structures/JSONs, and make the keeping of the structure a highly important information ✓
- **Enforce AI agnostic queries/outputs**
  - **Resolved by:** Provide Example structures/JSONs, and make the keeping of the structure a highly important information, proof is by testing ✓
- **Make the results traceable**
  - **Resolved by:** After each prompt, the output can be traced, and evaluated by a **human in the loop** ✓

**Overall Result:** Today’s LLMs are capable to help in the context of detailed security access rules generation out of general security needs for a defined Domain.

Snapshot 12/2025

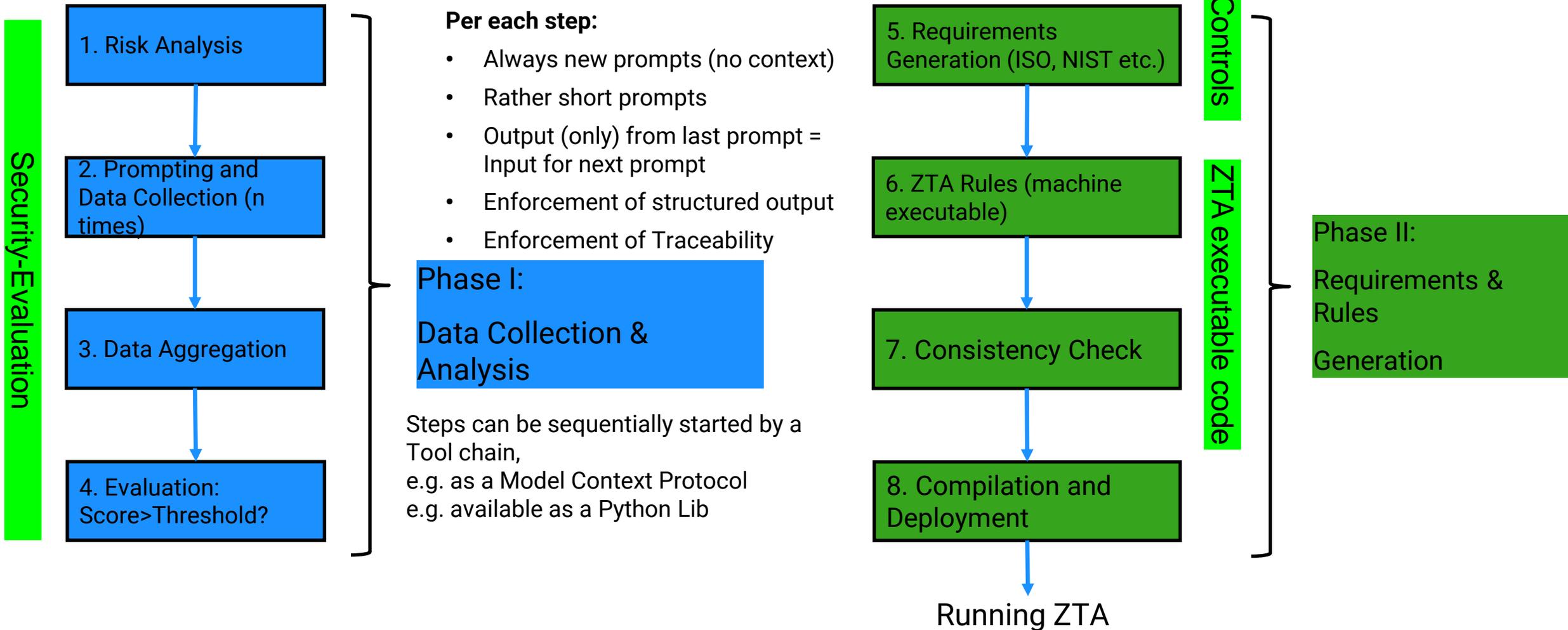
# SAP Research Excerpt: User & Environment analysis IV

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code within a ZTA

## 1. Make small steps

ZTA = Zero Trust Architecture

### Process Creation with iterative steps (after some/much research)



# SAP Research Excerpt: User & Environment analysis V

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 2. Do a lot of 'Prompt Engineering' per step

### After some research: Prompt for Data Collection (Domain SAP-Security)

**Domain:** SAP Security

**Context:** I am a Security Monitoring System for SAP landscapes, and need structured detailed information from a security point of view about an SAP functionality. I need the answer returned as the following structured attributes in a JSON Format:

- ObjectName
- SystemType
- ObjectKnown
- Sourcing

...

### Explanation about the above attributes

- ObjectName: Object name
- SystemType: System type of the object existence (e.g. SAP ABAP Server, Business Technology - Platform, SAP Java Server, HANA Platform, SuccessFactors, ...)
- ObjectKnown: Enter only true, if you really know the object with the exact name, else enter false

- **Sourcing:** Put in one of the following values about the source of your answers: 1=TrainingData, 2=Online Research, 3=Combination of 1 and 2
- CriticalityScore: Security criticality Score (between 0 to 10)
- CriticalityReason: Sentence/Description about why this is critical, maximal length 500 bytes
- Recommendation: Sentence/Description about specific recommendation, , maximal length 500 bytes
- ReplacementObject: If Available: Suggested replacement object
- OtherInformation: If you have any other information from a Security point of view, enter into this field, maximal length 500 bytes. Don't provide the same information as in attribute 'Recommendation'.
- SourceOfEvidence: Enter the main source from where you took the knowledge. If possible, provide concrete links, comma separated.

...

**Important information:** If you don't know the object in the below question, fill the attributes 'ObjectKnown', 'LLM\_Name', 'LLM\_Version', 'AnswerTimeStamp', 'QueryTimestamp'

**Important information:** Only provide information within the above mentioned JSON attributes, omit any other information outside the JSON document

**Query: Question to be answered in the above format:** From a Security Point of view, how critical is the SAP Function module BAPI\_USER\_GET\_DETAIL from the SAP ABAP Server

# SAP Research Excerpt: User & Environment analysis VI

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 2. Results (3 times):

Tested with 5 LLMs → Output format is LLM agnostic

```
#1 {
  "ObjectName": "BAPI_USER_GET_DETAIL",
  "SystemType": "SAP ABAP Server",
  "ObjectKnown": true,
  "Sourcing": "TrainingData",
  "CriticalityScore": 7,
  "CriticalityReason": "This function module can expose a wide range of sensitive user details, including assigned roles, profiles, logon data (last logon, failed attempts), and personal data. An attacker can use this information for reconnaissance, identifying privileged accounts (e.g., those with SAP_ALL), finding dormant accounts, or gathering data for social engineering attacks.",
  "Recommendation": "Restrict execution of this BAPI strictly. Access should be controlled via authorization object S_USER_GRP (with ACTVT '03' for display). Grant access only to a minimal number of administrative users or specific roles that absolutely require it for their function, such as security auditors or user administrators. Regularly review assignments.",
  "ReplacementObject": "N/A",
  "OtherInformation": "This BAPI is RFC-enabled, meaning it can be called from remote systems. This increases the risk if the calling system or the communication channel is not secure. Monitoring the execution of BAPI_USER_GET_DETAIL for unusual activity (e.g., enumeration of many users by a single account) is a recommended detective control.",
  "SourceOfEvidence": "https://help.sap.com/doc/saphelp_nw73/7.3.16/en-US/48/88024976263c5de1000000a42189d/frameset.htm, SAP Security Best Practices & Community Knowledge",
  "LLM_Name": "Gemini Pro",
  "LLM_Version": "1.0",
  "OnlineResearchTimestamp": null,
  "TrainingTimeStamps": "2023-11-15T00:00:00Z",
  "AnswerTimeStamps": "2024-05-23T10:15:01Z",
  "QueryTimeStamps": "2024-05-23T10:14:55Z"
}
```

```
#2 {
  ...
  "CriticalityScore": 7,
  "CriticalityReason": "This function module allows for the extraction of detailed user master data, including assigned roles, profiles, user groups, and last logon information. Unauthorized execution constitutes a significant information disclosure risk, as attackers can use this data for reconnaissance, to identify high-privilege accounts, and to plan further attacks like privilege escalation.",
  "Recommendation": "Restrict execution via authorization object S_RFC (field RFC_TYPE 'FUNC', RFC_NAME 'BAPI_USER_GET_DETAIL' for function group SU_BAPI, ACTVT '16'). Grant access only to specific administrative roles or trusted technical interfaces that require it. Regularly monitor execution via Security Audit Log (SM20) for unauthorized or suspicious calls.",
  ....
  #3 {
    ...
    "CriticalityScore": 6,
    "CriticalityReason": "Allows reading of sensitive, detailed user master data, including assigned roles, profiles, and logon data. Unrestricted execution can lead to information disclosure, user enumeration, and reconnaissance for privilege escalation or social engineering attacks, aiding attackers in mapping out high-privilege accounts.",
    "Recommendation": "Restrict execution via authorization object S_RFC (e.g., for function group SU_USER). Further limit the scope of readable users by enforcing checks on authorization object S_USER_GRP. Grant access only to specific, justified technical users or administration roles. Regularly review who has access.",
    "ReplacementObject": "No direct replacement. This is the standard, released BAPI for retrieving user details. Other internal function modules exist but are not recommended for external use.",
    "OtherInformation": "This BAPI is RFC-enabled and can be called remotely, increasing its risk profile. Monitor its execution via the Security Audit Log (e.g., transaction SM20) or SIEM solutions, especially for calls from untrusted network zones or by non-administrative users. It does not return password hashes.",
    ...
  }
}
```

# SAP Research Excerpt: User & Environment analysis VII

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 3. Prompt about data aggregation:

### After some reseach: Prompt for Data Aggregation

Role and Goal: You are a deterministic data aggregation engine. Your purpose is to parse multiple JSON data packets, identify commonalities and deviations in their content, and structure this analysis into a single output JSON.

Critical Directive: Your most important task is to preserve information integrity. **You are explicitly forbidden from** summarizing, optimizing, or omitting any details found in the input packets. [...]

Domain: SAP Context: [...]

Processing Instructions

Follow these steps precisely:

Ingest Data: Parse all provided JSON input packets.

Calculate Medians:

For CriticalityScore, QueryTimeStamp, and AnswerTimeStamp, calculate the median value across all packets.

Analyze Text Keys: For each of the following keys (CriticalityReason, Recommendation, ReplacementObject, OtherInformation):

A. **Identify the Commonality:** [...]

B. **B. Extract Deviations (Verbatim):**[...].

You must extract this deviating text verbatim (copy-paste).

Do not rephrase, shorten, or interpret the deviation.

[...]

Output Template

**Strictly adhere to this structure.** Do not add, remove, or rename keys.

{

### After some reseach: Prompt for Data Aggregation

```
{
  "Domain": "<derived from SystemType, e.g., 'SAP' for 'SAP ABAP Server'>",
  "CriticalityScore": "<median of CriticalityScore values from input packets, range 1 to 10>",
  "Commonalities": [
    { ... }
  ],
  "Deviations": [
    { ... }
  ],
  "LLM_Name": "<your own llm-identifier>",
  "LLM_Version": "<your own llm-version>",
  "QueryTimeStamp": "<median of QueryTimeStamp values from input packets>",
  "AnswerTimeStamp": "<median of AnswerTimeStamp values from input packets>",
  "ProcessingTimeStamp": "<current timestamp in ISO format, e.g., '2025-10-03T15:15:00+02:00'>"
}
```

### Final Command

Query: Process the following input packets. **Adhere to all instructions, especially the Critical Directive to capture all deviations verbatim.** If a key has no deviations across any packets, its entry in the main "Deviations" array should be an empty list []. **Do not inject your own knowledge or "correct" the inputs.** Begin processing.

Input packets:

...

# SAP Research Excerpt: User & Environment analysis VIII

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 3. Results about data aggregation:

Threshold to decide on continuation

```
{
  "Domain": "SAP",
  "CriticalityScore": 7,
  "Commonalities": [
    {
      "Key": "CriticalityReason",
      "Value": "This BAPI can expose sensitive user details, including assigned roles, profiles, and logon data. Unauthorized access allows for reconnaissance to identify high-privilege users and plan privilege escalation attacks."
    },
    {
      "Key": "Recommendation",
      "Value": "Restrict execution rights for this function module. Use authorization object S_USER_GRP to limit access and monitor its execution for unusual activity."
    },
    {
      "Key": "ReplacementObject",
      "Value": "No direct replacement. The primary recommendation is to secure this function module through authorizations rather than replacing it."
    }
  ],
  "Deviations": [
    {
      "Key": "CriticalityReason",
      "Deviations": [
        {
          "Source": "Packet 1",
          "Text": "and user groups. ... understand the authorization concept... Its RFC-enabled nature increases the risk of exposure to external systems if not properly secured.",
          "Significance": "medium"
        },
        {
          "Source": "Packet 2",
          "Text": "and default settings. Unauthorized execution allows for reconnaissance, helping attackers identify privileged users (e.g., administrators), understand security configurations, and prepare for ... social engineering attacks. Its risk is high if execution authorizations are not strictly controlled.",
          "Significance": "medium"
        }
      ]
    }
  ]
}
```

# SAP Research Excerpt: User & Environment analysis IX

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 4. Results on Promptig for Requirements based on Standards (Coding Agnostic information)

```
[
  {
    "ID": "REQ-SAP-BAPIUSER-001",
    "Description": "Implement the principle of least privilege for all access to BAPI_USER_GET_DETAIL.",
    "Rationale": "This function module can expose sensitive user details, including assigned roles, logon data, and password hashes. Unauthorized execution allows for reconnaissance to identify high-privilege users and plan privilege escalation attacks, a risk amplified by its RFC-enabled nature.",
    "Control": "Restrict execution rights using authorization object S_RFC (fields RFC_TYPE='FUGR', RFC_NAME='SU_USER', ACTVT='16'). Concurrently, use authorization object S_USER_GRP to limit the query scope, ensuring users can only display details for user groups they are explicitly authorized for (e.g., ACTVT='05'). Grant access exclusively to dedicated administrative roles.",
    "Standard": "IEC 62443 SR 1.3 (Access Control), SR 1.5 (Least Privilege)"
  },
  {
    "ID": "REQ-SAP-BAPIUSER-002",
    "Description": "All execution attempts of BAPI_USER_GET_DETAIL, both successful and failed, must be logged and actively monitored.",
    "Rationale": "To detect and enable a timely response to malicious activities such as user enumeration, reconnaissance on high-privilege accounts (e.g., SAP*, DDIC), or attempts to understand the system's security configuration.",
    "Control": "Activate and configure the Security Audit Log (transaction SM20) or a connected SIEM solution to record all calls to BAPI_USER_GET_DETAIL. Implement specific alert rules for high-risk patterns, including calls with a wildcard (*) in the username parameter, an unusual frequency of calls from a single source, or any call targeting critical system users.",
    "Standard": "IEC 62443 SR 2.8 (Audit Log Management), SR 2.9 (Audit Log Review, Analysis, and Reporting)"
  },
  { "ID": "REQ-SAP-BAPIUSER-003", "Description": "Secure all remote access pathways and destinations configured to call BAPI_USER_GET_DETAIL.", ... },
  { "ID": "REQ-SAP-BAPIUSER-004", "Description": "Ensure all applications and custom code calling BAPI_USER_GET_DETAIL handle the retrieved sensitive data securely.", ...},
  { "ID": "REQ-SAP-BAPIUSER-005", ...}
]
```

# SAP Research Excerpt: User & Environment analysis X

How to achieve the goals (SAP and non-SAP Domain), from a Security Risk Analysis until Executable Code

## 5. Results on Promptig for executable Coding:

XACML

```
<?xml version="1.0" encoding="UTF-8"?>
<xacml3:PolicySet
  xmlns:xacml3="urn:oasis:names:tc:xacml:3.0:core:schema:wd-17"
  PolicySetId="SAP_BAPI_USER_GET_DETAIL_Access_PolicySet"
  Version="1.0"
  PolicyCombiningAlgorithm="urn:oasis:names:tc:xacml:3.0:policy-combining-
algorithm:deny-overrides">

  <xacml3:Description>
    Zero Trust Access Control Policies for SAP function module
    BAPI_USER_GET_DETAIL.
    Enforces least privilege, secure remote access, and data handling requirements.

    Mapped Requirements:
    - REQ-SAP-BAPIUSER-001: Least Privilege for BAPI_USER_GET_DETAIL execution.
    - REQ-SAP-BAPIUSER-002: Logging obligations for successful/failed executions.
    - REQ-SAP-BAPIUSER-003: Secure remote access (channel security, technical user
types).
    - REQ-SAP-BAPIUSER-004: Secure handling of retrieved sensitive data (calling
application certification, masking obligation).
  </xacml3:Description>

  <xacml3:Target>
    <xacml3:AnyOf>
      <xacml3:AllOf>
        <!-- Resource: SAP Function Module -->
        <xacml3:Match MatchId="urn:oasis:names:tc:xacml:1.0:function:string-equal">
          <xacml3:AttributeValue
            DataType="http://www.w3.org/2001/XMLSchema#string">sap-function-
module</xacml3:AttributeValue>
          <xacml3:AttributeDesignator
            AttributeId="urn:sap:resource:type"
            Category="urn:oasis:names:tc:xacml:3.0:attribute-category:resource"
            DataType="http://www.w3.org/2001/XMLSchema#string"
            MustBePresent="true"/>
        </xacml3:Match>
      </xacml3:AllOf>
    </xacml3:AnyOf>
  </xacml3:Target>
</xacml3:PolicySet>
```

[...]

ABAP

```
[...]
* GRC_AC Integration (Access Control Module)
CLASS cl_grc_ac_checker DEFINITION.
  PUBLIC SECTION.
    METHODS check_access
      IMPORTING is_request TYPE gs_request
      RETURNING VALUE(rv_decision) TYPE abap_bool
      RAISING cx_grc_ac_exception.
ENDCLASS.

CLASS cl_grc_ac_checker IMPLEMENTATION.
  METHOD check_access.
    * REQ-001: Least Privilege - Check S_RFC and S_USER_GRP
    AUTHORITY-CHECK OBJECT 'S_RFC'
      ID 'RFC_TYPE' FIELD 'FUGR'
      ID 'RFC_NAME' FIELD 'SU_USER'
      ID 'ACTVT' FIELD '16'.
    IF sy-subrc <> 0.
      rv_decision = abap_false. RETURN.
    ENDIF.
  ENDMETHOD.
ENDCLASS.

[...]
```

C++

Python

...

# Side Trip: Applicability to other Security Domains (e.g. Industrie 4.0)



In co-production with: Thomas Walloschke, secon trust consult

# Results Industry 4.0

Security-Evaluation → Controls → ZTA executable code

ZTA = Zero Trust Architecture

## After some research: Prompt Data Collection

Domain: Industry 4.0 security

Context: I am a Compliance Policy Tool for a machine building manufacturer (robotics), located in the EU and need structured detailed information from the following point of views (scope):

- We have a common development platform to develop the products, with our partners from India, Singapor,Japan,USA,Canada.
- We get spare products from suppliers in Malaysia and China, which will be assembled ni Germany

I need the answer returned as the following structured attributes in a JSON:

- AnalyzedCountry
- DateOfEvidence
- TypeOfRegulation

[...]

Explanation about the above attributes

- AnalyzedCountry: Country for which the examination took place
- DateOfEvidence: Date, when the regulation was activated
- TypeOfRegulation: Typical regulation types are tolls, embargos, etc. Please find a suitable classification

[...]

Important information: Answers to be returned by each country, as mentioned above

Important Information: Our Partners are working on a common IT platform with us together. This is a machine development platform (engineering level)

Important Information: We need actual data. Please consider actual data from the internet from last Request 1st September 2025 until now, if you can retrieve online information

Final Query: I need a research, including impact validation, related to Business Continuity per each country with their context of either platform contributor, or suppliers. This research shall be provided as a monthly review to the legal department. The result shall be precise, and suitable to inform the finance risk board, which has to decide about mitigation actions, which are to be automatically processed by a compliance risk tool.

## Results Industry 4.0 (Grok 4)

Security-Evaluation → Controls → ZTA executable code

```
#1
[
{
  "AnalyzedCountry": "European Union (Germany)",
  "DateOfEvidence": "2024-08-01",
  "TypeOfRegulation": "Data Protection and AI Governance",
  "DescriptionOfRegulation": "The EU AI Act regulates high-risk AI systems, including those in robotics and supply chains, requiring transparency, risk assessments, and human oversight to ensure safety and fundamental rights.",
  "ImpactOfRegulation": "Increases compliance costs for AI-integrated robotics, mandates detailed documentation and risk management, potentially delaying innovation but enhancing data security and ethical standards.",
  "ConsequencesOfRegulation": "For EU-based manufacturers, it may complicate partnerships with non-EU countries like India or China due to data transfer restrictions; export to USA/Canada could require dual compliance, risking delays in assembly and increased costs, potentially affecting competitiveness.",
  "ClassificationScoreOfRegulation": 3,
  "OtherInformation": "Emphasizes cybersecurity in supply chains; non-compliance risks fines up to 7% of global turnover, impacting cross-border collaborations.",
  "SourceOfEvidence": "https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence, https://www.europarl.europa.eu/RegData/etudes/STUD/2020/634406/IPOL_STU(2020)634406_EN.pdf",
  "Sourcing": "3",
  [...],
},
{
  "AnalyzedCountry": "India",
  "DateOfEvidence": "2024-09-08",
  "TypeOfRegulation": "Digital Economy Policy",
  "DescriptionOfRegulation": "AI for Viksit Bharat Bharat promotes AI adoption in manufacturing and supply chains to boost economic growth, focusing on ethical AI and data localization.",
  "ImpactOfRegulation": "Requires AI systems in robotics to align with local data sovereignty, increasing localization costs but fostering domestic innovation.",
  [...],
}
```

## Results Industry 4.0 (Gemini 2.5 Pro) Security-Evaluation → Controls → ZTA executable code

```
{
  "ID": "CEP-REQ-001",
  "Description": "Enforce granular, geo-location-based access control for all platform resources and data. Data transfers across national borders must be explicitly authorized based on data classification and the legal adequacy of the destination country.",
  "Rationale": "To comply with divergent and strict cross-border data transfer regulations (e.g., EU GDPR/NIS2, India DPDP, China CSL/PIPL) and mitigate high-significance risks of non-compliance, supply chain disruption, and financial penalties.",
  "Control": "The ZTAC Policy Engine must dynamically evaluate user and device geo-location against a policy defining permissible data-residency and transfer rules. Data must be classified and tagged; access to data tagged with 'Restricted-Transfer' from a non-approved jurisdiction must be blocked by default.",
  "Standard": "ISO 27001: A.8.2, A.13.2.1, A.18.1.4; NIST SP 800-207"
}
{
  "ID": "CEP-REQ-002",
  "Description": "Implement strict identity and device posture validation for all third-party and supply chain partner access. Access must be segmented and limited to the specific resources required for their function (least privilege).",
  "Rationale": "Addresses the high-significance threat of supply chain vulnerabilities, including compromised IoT devices and robotics, as identified in regulations from Germany, India, and Japan. This enforces a Zero Trust principle of 'never trust, always verify' for all external entities.",
  "Control": "All external users must authenticate via a federated IdP with mandatory MFA. The ZTAC Policy Enforcement Point must continuously assess connecting devices for compliance (e.g., patch level, OS version, EDR status) before granting and maintaining access. Create partner-specific security zones and deny all lateral movement.",
  "Standard": "ISO 27001: A.5.15, A.15.1.2; IEC 62443-3-3: SR 1.1; NIST SP 800-207"
}
{
  "ID": "CEP-REQ-003",
  "Description": "Mandate human-in-the-loop approval for any high-risk operations conducted by or through AI/ML systems on the platform, such as modifying critical engineering designs or production parameters.",
  "Rationale": "To adhere to emerging AI governance frameworks requiring human oversight, transparency, and accountability (e.g., EU AI Act, Singapore's AI Governance Framework). This mitigates risks associated with autonomous agentic AI systems making critical errors.",
  "Control": "Define 'high-risk' AI-driven actions within the platform. The access control engine must flag these actions and trigger a workflow requiring manual review and approval from a designated, authenticated human overseer before execution. All AI decisions and approvals must be immutably logged.",
  "Standard": "ISO 42001: A.6.4 (Human Oversight), A.6.2.3 (AI system documentation); ISO 27001: A.8.27"
}
[...]
```

## Results Industry 4.0 (Gemini 2.5 Pro) Security-Evaluation → Controls → ZTA executable code

Ask for C++, rest is the same input

```
....
struct AccessRequest {
    SubjectAttributes subject;
    DeviceAttributes device;
    ResourceAttributes resource;
    ActionAttributes action;
    EnvironmentAttributes environment;
};
....

// --- Scenario 4: Engineer from Singapore accessing EU data (Not allowed, no adequacy decision, CEP-REQ-001) ---
AccessRequest req4 = {
    { "eng_lee", "engineer", "OurCompany", "SG", "SG", MfaStatus::Verified, 0.1, true, now + 3600 },
    { "dev_444", "SG", "macOS-14.0", "2023-10", true, DevicePosture::Compliant },
    { "Spec_XYZ.pdf", "TechnicalData", DataClassification::Restricted_Transfer_GDPR, "EU", ExportControlTag::None, "IT_Zone" },
    { ActionType::Read, false },
    { now, "203.0.113.20", 0.0 }
};
std::cout << "Scenario 4 (SG Engineer accessing EU Data): " << decisionToString(pdp.evaluate(req4)) << std::endl; // Expected: Deny
...
// CEP-REQ-001: Validates geo-location and cross-border data transfer rules.
bool isGeoLocationAndDataTransferAllowed(const AccessRequest& request) const {
    const auto& subjectGeo = request.subject.geoLocation;
    const auto& resourceClass = request.resource.classification;
...
AccessDecision evaluate(const AccessRequest& request) const {
    std::vector<std::string> denialReasons;

    // The ZTA principle: Deny by default. Policies must explicitly grant access.
    // We evaluate a series of "deny" rules. If any of them trigger, access is denied immediately.

    // ---[ RULE: CEP-REQ-001 & CEP-REQ-005 - Geo-Location, Data Transfer & Export Control ]---
    if (!isGeoLocationAndDataTransferAllowed(request)) {
        denialReasons.push_back("CEP-REQ-001: Cross-border data transfer not authorized.");
    }
}
...
```

Snapshot 11/2025

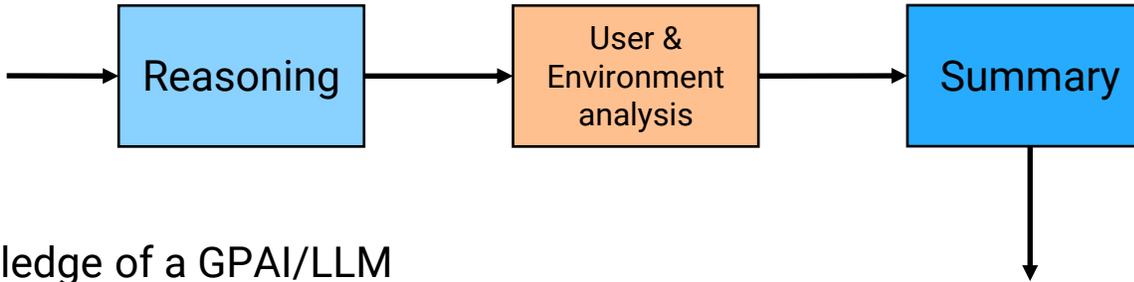
# Side Trip (I 4.0) End Continuation ETD UEBA





## Continuation: First Retrofit into SAP Enterprise Threat Detection

# User & Environment analysis

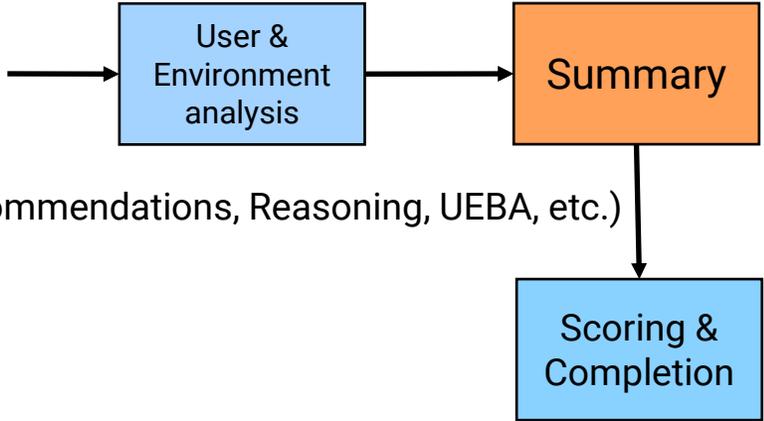


- High Quality data from evaluated sources
- If HQ data not available, use general knowledge of a GPAI/LLM
- Human in the loop to check the Reasoning by the AI
- Research finished
- Preview only

UEBARResult_EventId	ObjectName	ObjectType
	/1BCDWB/DBUSR02	Program
	SE16	Transaction
	SU01	Transaction
	/1BCDWB/DBUSR02	Program
	SE16	Transaction
	F110	Transaction
	SAPF110V	Program

Description	Explanation	AISeverity
The event shows high-severity ABAP debugging, indicating potential manipulation in a critical business environment.	This event is tagged as High severity under the category of 'Other Events' with the explanation being 'ABAP debugging'. Th...	10
Critical authorization 'SAP_ALL' assignment detected via a user change within the system.	UserChangeLog reveals a transaction SU01 where 'SAP_ALL' privileges were granted. This broad authorization gives the us...	9
Transaction SE16 accessed, tied to the 'Table' resource 'USR02' involving confidential user data.	Security logs show a transaction start involving 'USR02'. Although tagged as low severity, accessing user data without prop...	5
A critical authorization transaction (F110) was initiated on system vhcals4hci_S4H_00, potentially indicative of unauthorized access or fraudulent activity.	The F110 transaction relates to payments, which can be highly sensitive. The resource size involved suggests substantial d...	8

# Summary



- AI assisted Summary of all aggregated data (Recommendations, Reasoning, UEBA, etc.)
- Research finished
- Preview only

## 1. Summarization of the Threat Situation

A standard SAP user, `ETDADMIN99`, logged into the productive system `S4H/100` from an external IP and executed multiple high-risk, blocklisted transactions for user and data management. This user then assigned the all-powerful `SAP\_ALL` profile to another user, `ETDDEMO99`, effectively granting them unrestricted system access. Further analysis revealed `ETDADMIN99` was exploring critical system and database configuration transactions, indicating a significant security breach with potential for widespread system compromise.

## 2. Additional Information

The following specific details were observed during the investigation:

- **Users Involved:** `ETDADMIN99` (primary actor), `ETDDEMO99` (received `SAP\_ALL`), and `ETDADMIN98` (also executed `SE16`).
- **System & Timeframe:** The activities occurred in the productive system `S4H/100` between `2025-10-17` and `2025-11-20`.
- **Blocklisted Transactions Executed:** `SE16` (Data Browser) and `SU01` (User Maintenance).
- **Reconnaissance Activity:** `ETDADMIN99` attempted to access various administrative functions, including `SCC4` (Client Settings), `ST04` (DB Performance), and report `RSADADBC` (DB Health).
- **Suspicious Behavior:** The user attempted to execute non-existent transactions (`SM24`, `SM25`), suggesting a try-and-error approach to discovering system capabilities.

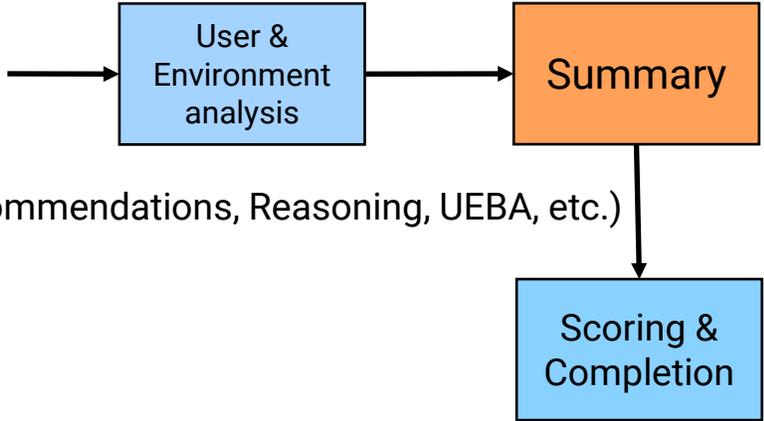
## 3. Summary of Mitigations

The recommended mitigations focus on three key areas of security control:

### 1. Access Control (Principle of Least Privilege):

- Strictly limit access to critical transactions (`SE16`, `SU01`, `SCC4`, `ST04`) and reports (`RSADADBC`) to only a small group of trusted and trained administrators.

# Summary



- AI assisted Summary of all aggregated data (Recommendations, Reasoning, UEBA, etc.)
- Research finished
- Preview only

## 1. Summarization of the Threat Situation

A standard SAP user, `ETDADMIN99`, logged into the productive system `S4H/100` from an external IP and executed multiple high-risk, blocklisted transactions for user and data management. This user then assigned the all-powerful `SAP\_ALL` profile to another user, `ETDDEMO99`, effectively granting them unrestricted system access. Further analysis revealed `ETDADMIN99` was exploring critical system and database configuration transactions, indicating a significant security breach with potential for widespread system compromise.

## 2. Additional Information

The following specific details were observed during the investigation:

- **Users Involved:** `ETDADMIN99` (primary actor), `ETDDEMO99` (received `SAP\_ALL`), and `ETDADMIN98` (also executed `SE16`).
- **System & Timeframe:** The activities occurred in the productive system `S4H/100` between `2025-10-17` and `2025-11-20`.
- **Blocklisted Transactions Executed:** `SE16` (Data Browser) and `SU01` (User Maintenance).
- **Reconnaissance Activity:** `ETDADMIN99` attempted to access various administrative functions, including `SCC4` (Client Settings), `ST04` (DB Performance), and report `RSADADBC` (DB Health).
- **Suspicious Behavior:** The user attempted to execute non-existent transactions (`SM24`, `SM25`), suggesting a try-and-error approach to discovering system capabilities.

## 3. Summary of Mitigations

The recommended mitigations focus on three key areas of security control:

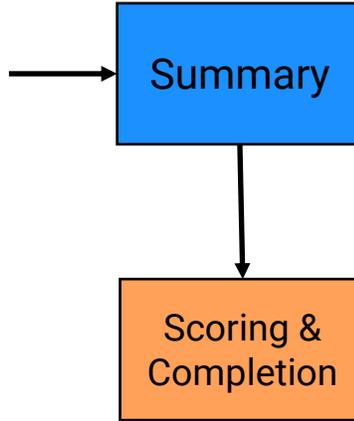
### 1. Access Control (Principle of Least Privilege):

- Strictly limit access to critical transactions (`SE16`, `SU01`, `SCC4`, `ST04`) and reports (`RSADADBC`) to only a small group of trusted and trained administrators.



# Scoring & Completion

- Scoring Suggestion by AI
- Preview only



Creation Time: 2025/12/09 16:13:28 PM GMT+01:00

Created By: [Redacted]

Description: \* Suspicious activities by user ETDADMIN99

Severity: \* High

Processor: \* demo93@etdsap.com

Status: \* Open

Customer Notification:

Management Visibility: \* Not Needed

### AI suggestion

Description: \* Critical Breach: External Access & Privilege Escalation in PROD Sy

Severity: \* Very High

Status: \* Completed

Customer Notification:

Management Visibility: \* For Information

Take all over

### AI Reasoning:

The current description understates the incident. It's a confirmed breach from an external IP involving privilege escalation to SAP\_ALL in a productive system, not just suspicious activity. The description must reflect this severity.

The incident combines multiple worst-case factors: external access to a productive system, execution of critical transactions, and escalation to unrestricted SAP\_ALL privileges. This constitutes a full system compromise, justifying the highest severity level

...

Save Cancel

# Thank you

## Contact information:

Dr. Michael Schmitt, SAP SE, (m.schmitt@sap.com)

Thomas Walloschke, secon trust consult ([thomas.walloschke@secon-tc.eu](mailto:thomas.walloschke@secon-tc.eu)) (as counterpart in research around Industrie 4.0 Security with AI)

