SAP Enterprise Threat Detection, Cloud Edition

Introduction
UI-Roundtrip
Compliance Features
Semantic data model

Public

What is SAP Enterprise Threat Detection?

Why SAP Enterprise Threat Detection?

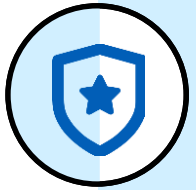
Key concerns

Critical security assets are located in SAP systems – and thus at constant danger to attacks

SAP systems are seen as “Black Box” concerning security aspects & suspicious behavior

Attacks are not detected in time, or go completely unnoticed

Constant & comprehensive monitoring of the SAP landscape turns into a big data problem



Leverage SAP knowledge & technology

How to protect our crown jewels?

How to detect attacks in time?

How to deliver insights fast enough?

How to correlate log data to gain insights into attack paths?

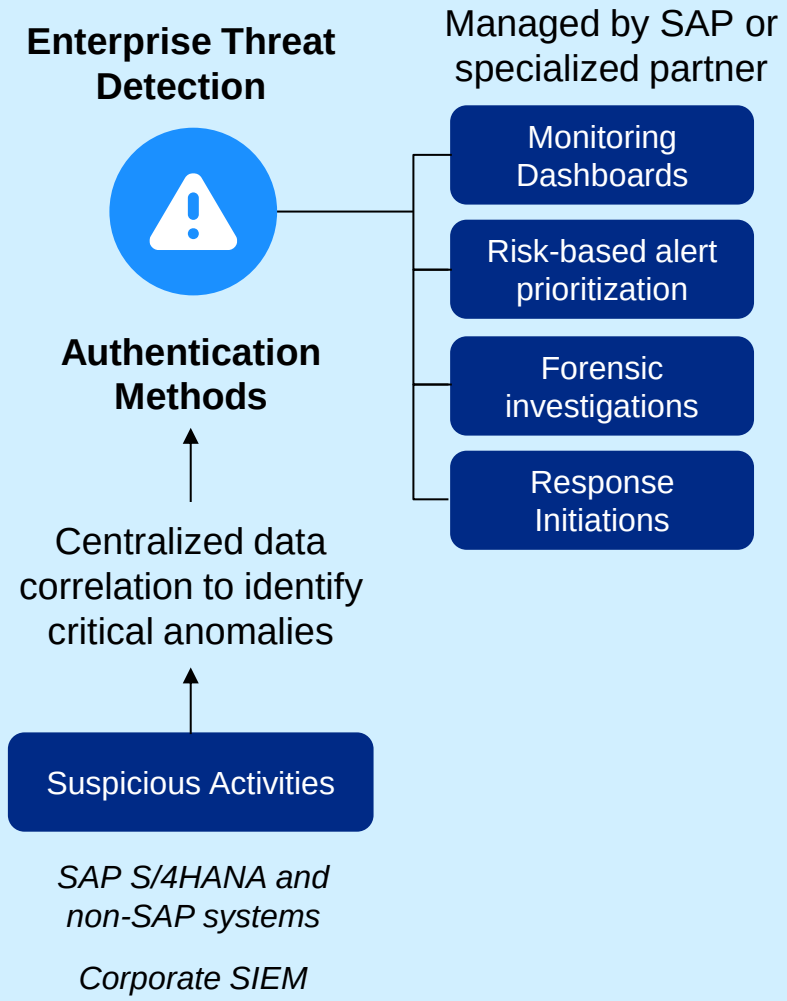
How to handle the big data problem?

How to neutralize threats effectively?

SAP Enterprise Threat Detection
Solution Capabilities

Managed service from either SAP or a specialized partner to help identify, analyse, and report malicious activities in your SAP applications before serious damage occurs.

- Analyze vast quantities of log data and correlate information to get a complete picture of landscape activities.
- Detect threats at the application server level and at the database level.
- Find SAP software-specific threats related to known attacks by using attack detection patterns.
- Perform forensic threat detection to discover previously unknown attack variants.
- Create attack detection patterns without the need to code.
- Customize the integration of third-party systems and infrastructure components.



SAP Enterprise Threat Detection

Application hacking by malicious actors is a never-ending process leading to black mail, ransom, loss of trust and penalties.

Brute force attacks, lost and stolen credentials with successful login leading to identity theft and loss of confidentiality, integrity, and availability.

Creation of new users and vial RFC, mpromise

Unsecure company secrets and books can

Continuous Threat Monitoring

Monitor Controls

Forensic Analysis

Manage Incident

Sourcing → Contracting + Forecasting → Requesting + Ordering → Receiving + Invoicing → Invoicing Receipt + Processing → Payment Processing

Detection Processes

ve information has been disclosed to unauthorized individuals.

Anomalies and Events

ta be

Loss of Availability: the information is not consistent and readily accessible to authorized persons.

User Behaviour Analysis

card, bank details, customer PII, pricing information, order **data** to hackers.

Financial reporting information has been e-mail rowth.

Vulnerable systems and in-house built apps leading to data breaches and ransomware leading to loss of trust and high penalties.

Threat Hunting

Response Planning

make purchases,

Financial or production

delayed therefor revenue is lost.

Integrate SIEM / SOAR

SAP S/4HANA Source-to-Pay Process

What could go wrong?

Application hacking by malicious actors is a never-ending process leading to black mail, ransom, loss of trust, revenue and penalties.

Brute force attacks, lost and stolen credentials with successful login leading to identity theft and loss of confidentiality, integrity, and availability.

Modification and changes of business documents.

Privileged user manipulated books, duplicated bills and changed bank details.

Unsecure company secrets and books can lead to a loss of competitive advantage or & misstatement of the financial books.

Breach of Confidentiality: sensitive information has been disclosed to unauthorized individuals.

Loss of Integrity: consistency, accuracy and trustworthiness of data over its lifecycle is lost. Data can be altered by unauthorized individuals.

Loss of Availability: the information is not consistent and readily accessible to authorized persons.

Exfiltration of sensitive credit card, bank details, customer PII, pricing information, order **data** to hackers.

Financial reporting information has been sent automatically to an external e-mail address, to help to predict stock growth.

Vulnerable systems and in-house built apps leading to data breaches and ransomware leading to loss of trust and high penalties.

Customers are unable to make purchases

Financial or production planning gets delayed

Decision making based on that information must be delayed therefor revenue is lost.

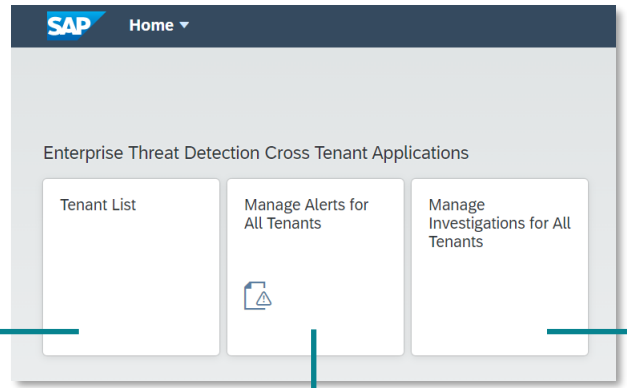
UI Roundtrip & Compliance Features

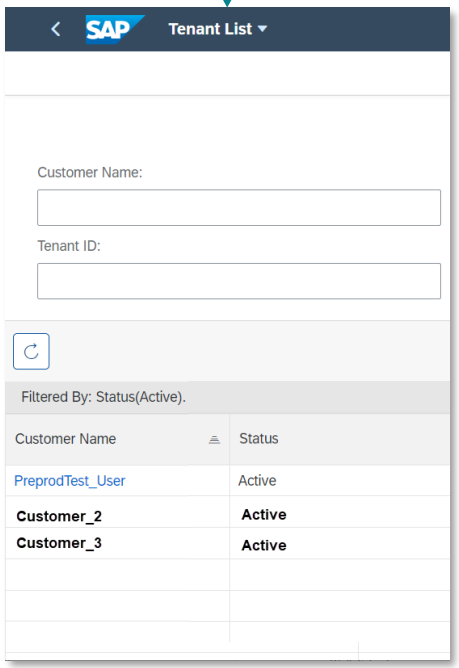
UI Roundtrip

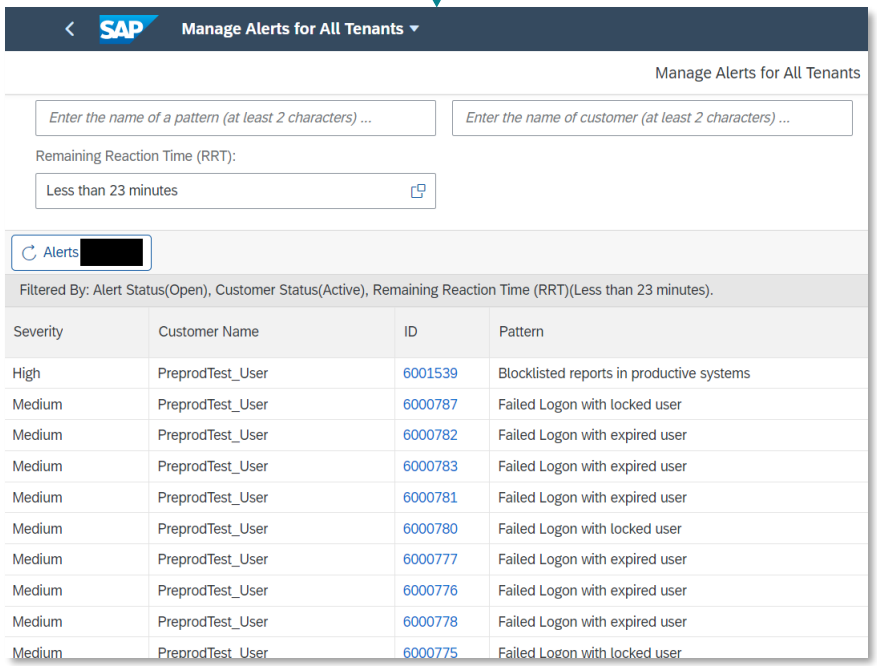
Central Partner UI

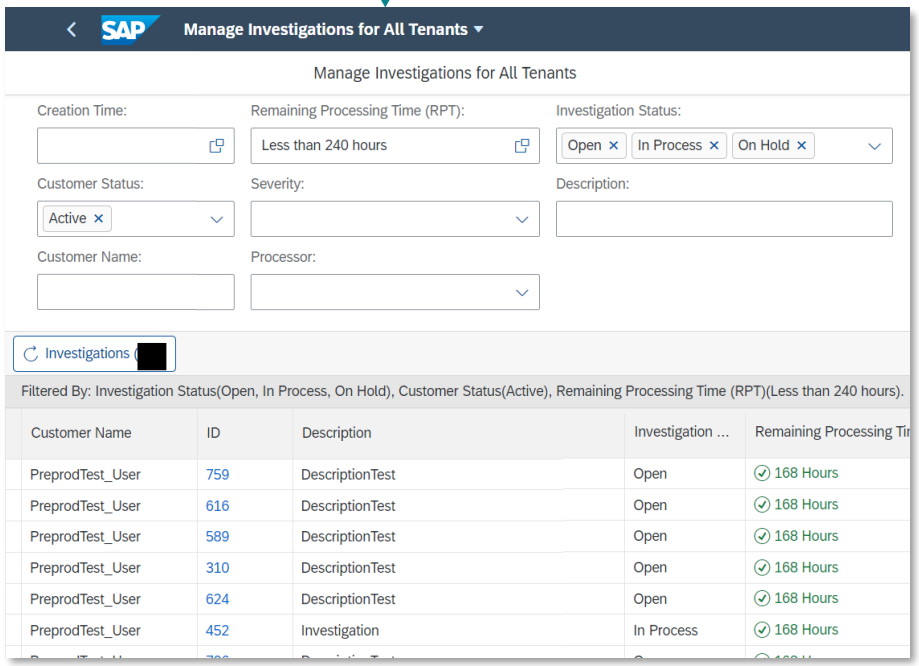
Applications for centrally handling multiple customers

1. List for selecting a specific (customer) Tenant
2. List of Alerts from all Tenants (customers)
3. List of Investigations from all Tenants (customers)



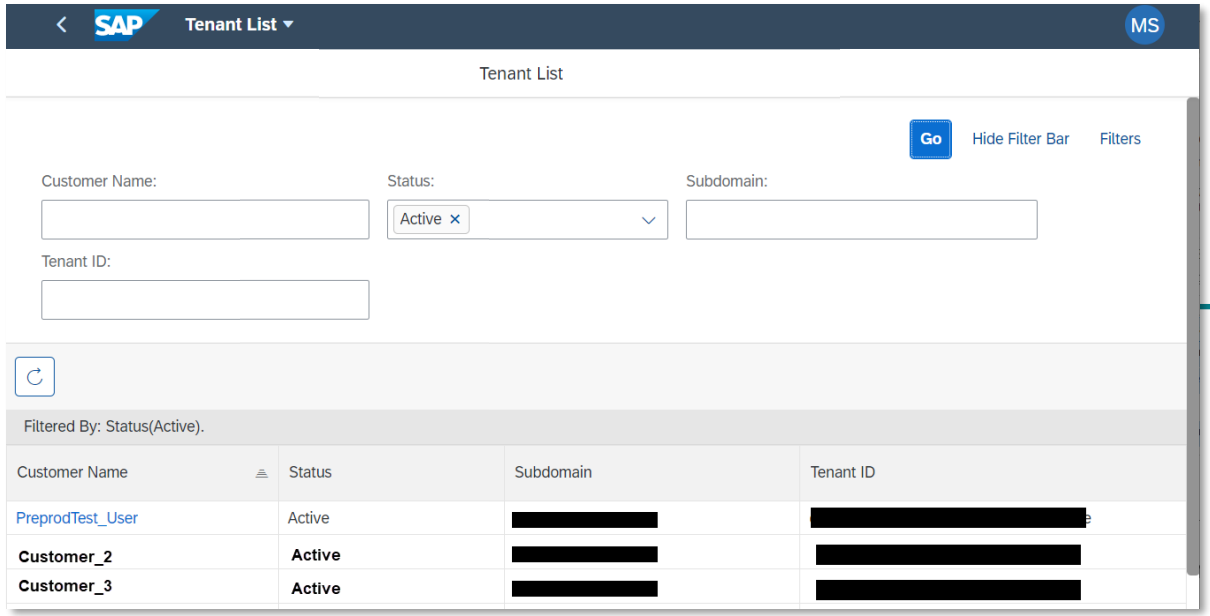


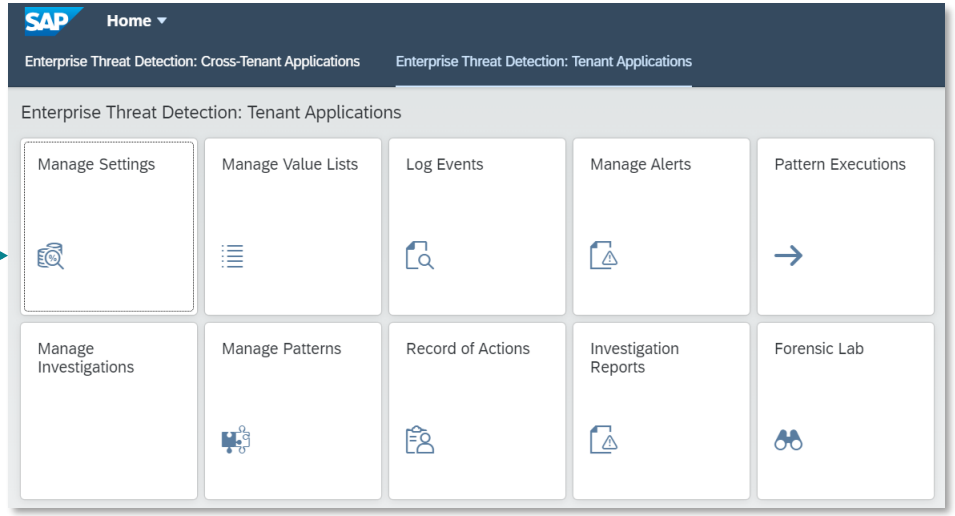




From Tenant List to Single Tenant

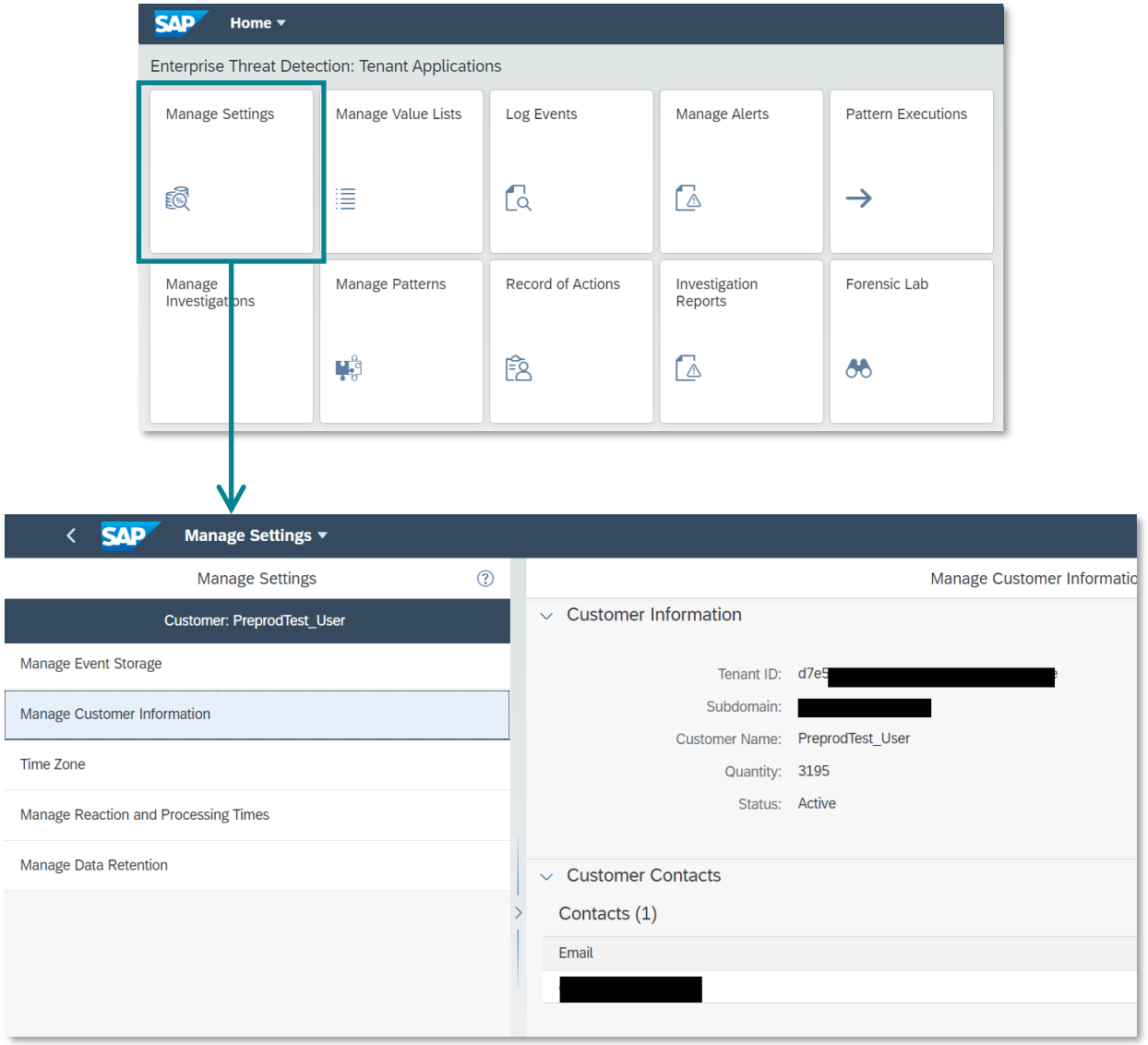
Selection of a specific customer (Tenant) makes additional applications available for managing the Tenant, and security monitoring activities in the Tenant.





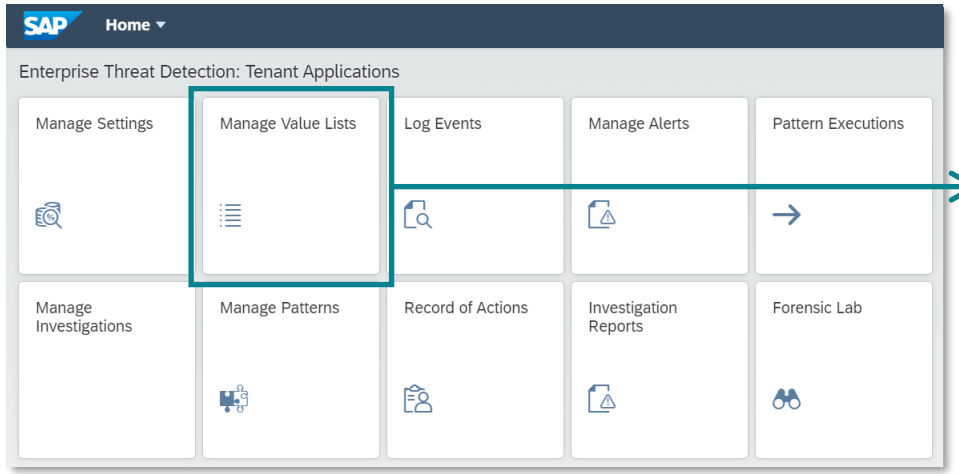
Manage Settings

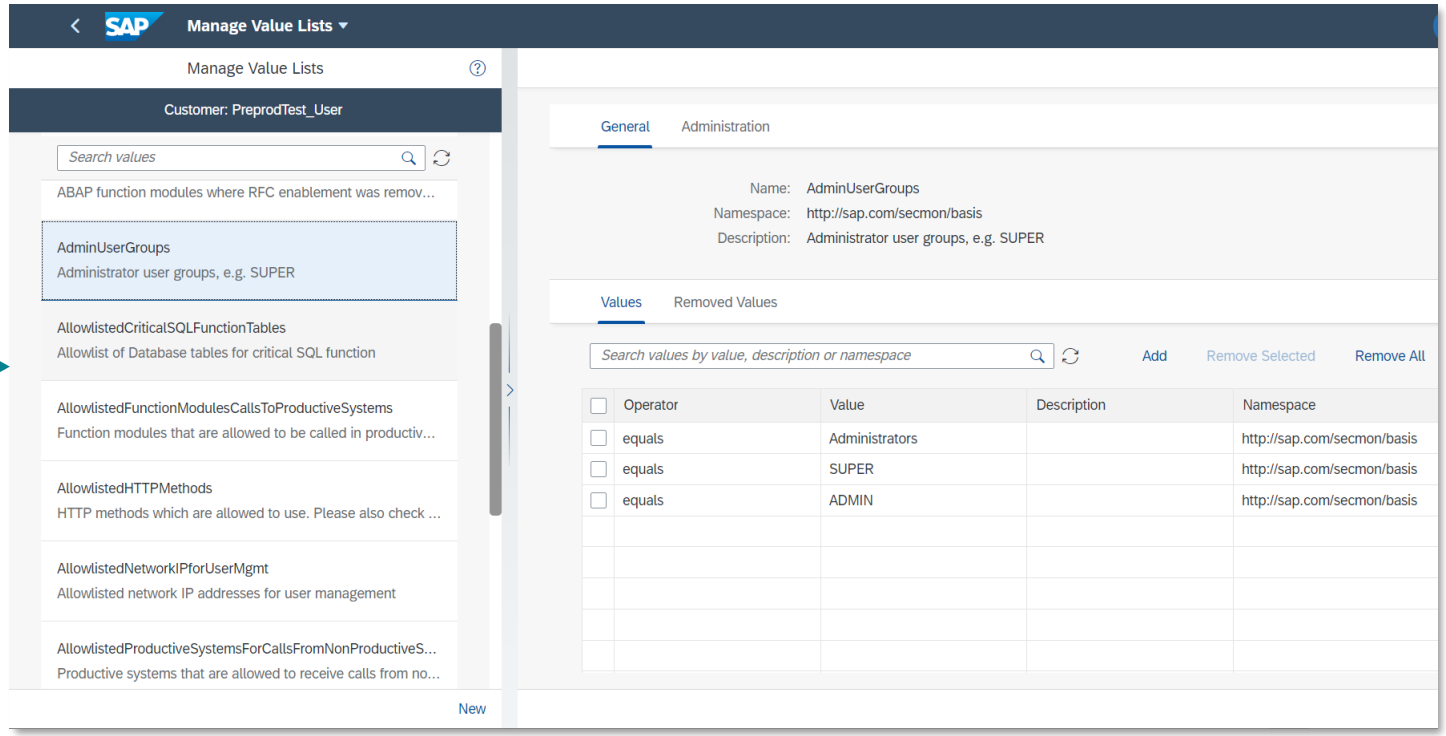
The Manage Settings app gives access to Tenant specific information and settings.



Manage Value Lists

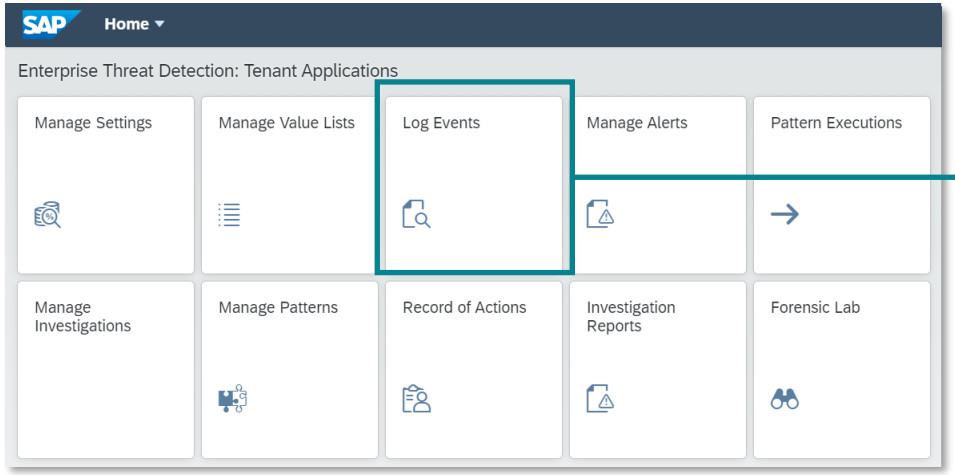
The Manage Value Lists app allows to create, view, change, and delete value lists and entries (Values).

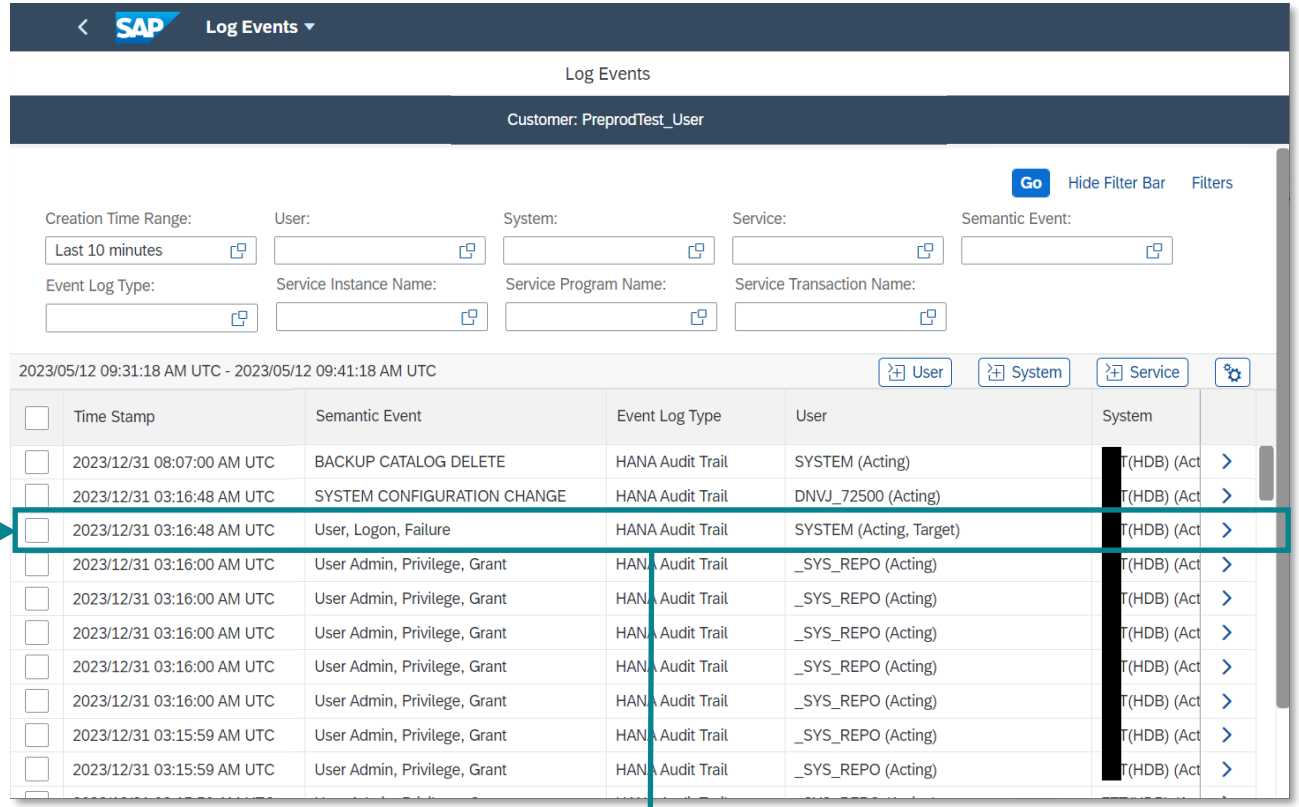


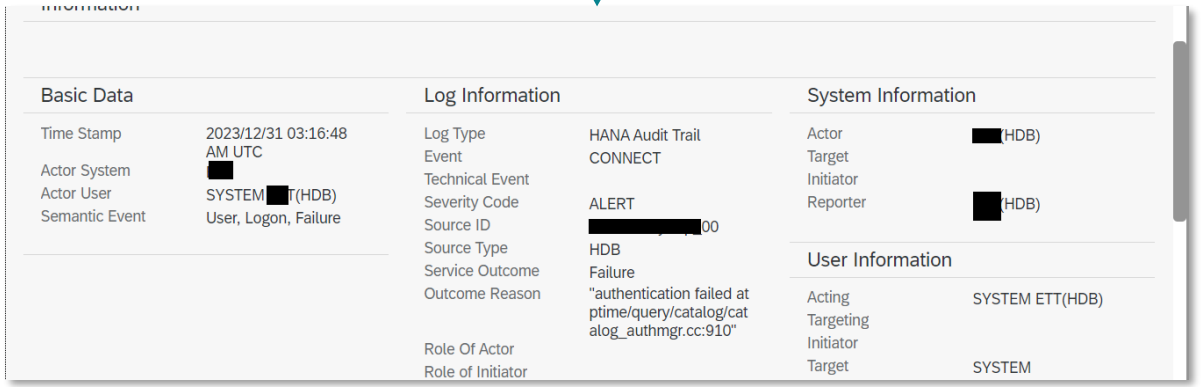


Log Events

The Log Events app allows to access the list and details of all client specific Log Entries.

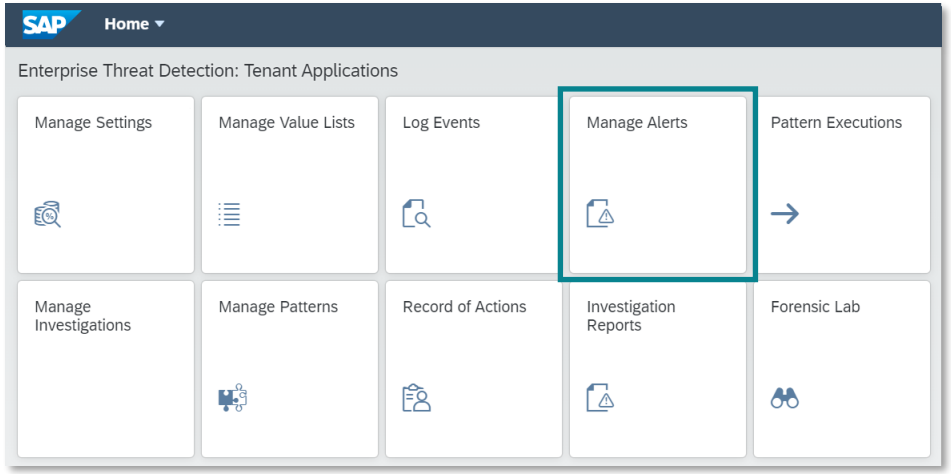


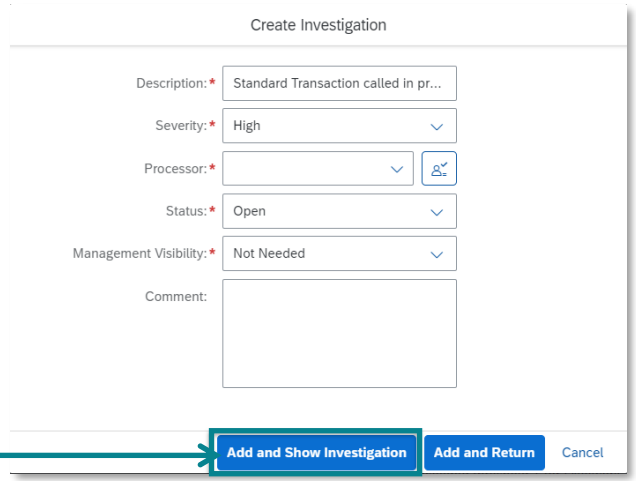


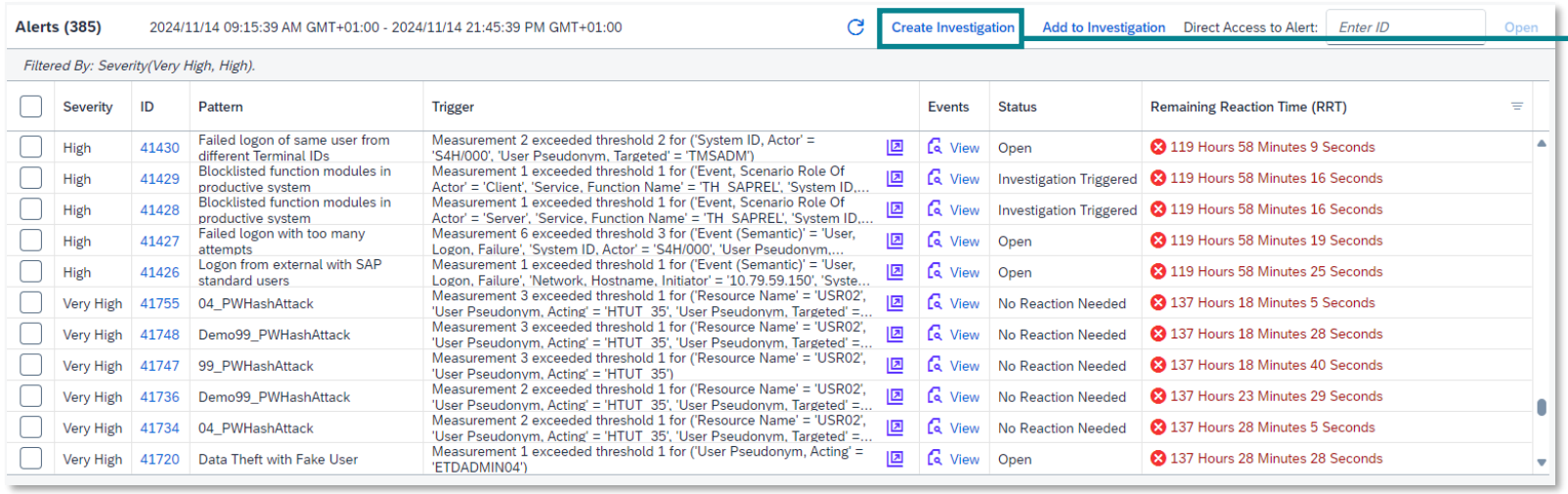


Manage Alerts

The Manage Alerts app allows to view and analyze each client specific Alert, and drill down into related Log Events and Patterns. It allows lends a functionality to create a new Investigation directly out of one or more Alerts.



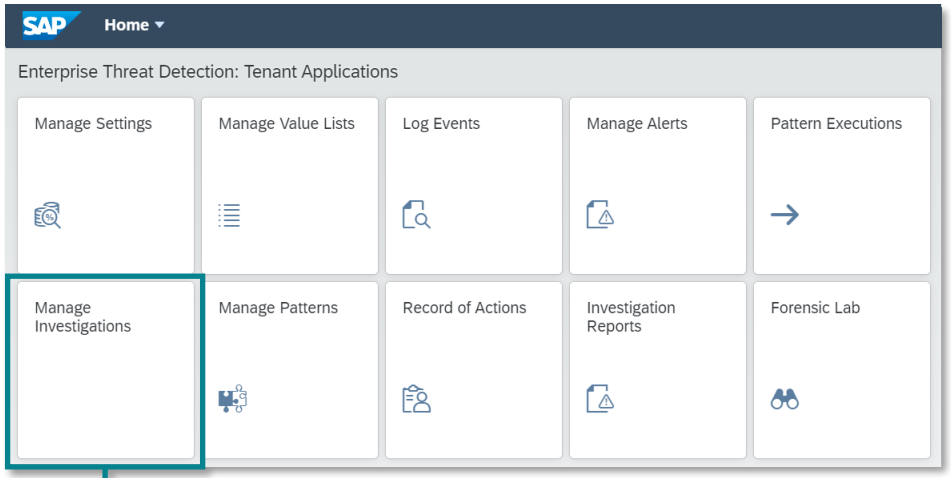


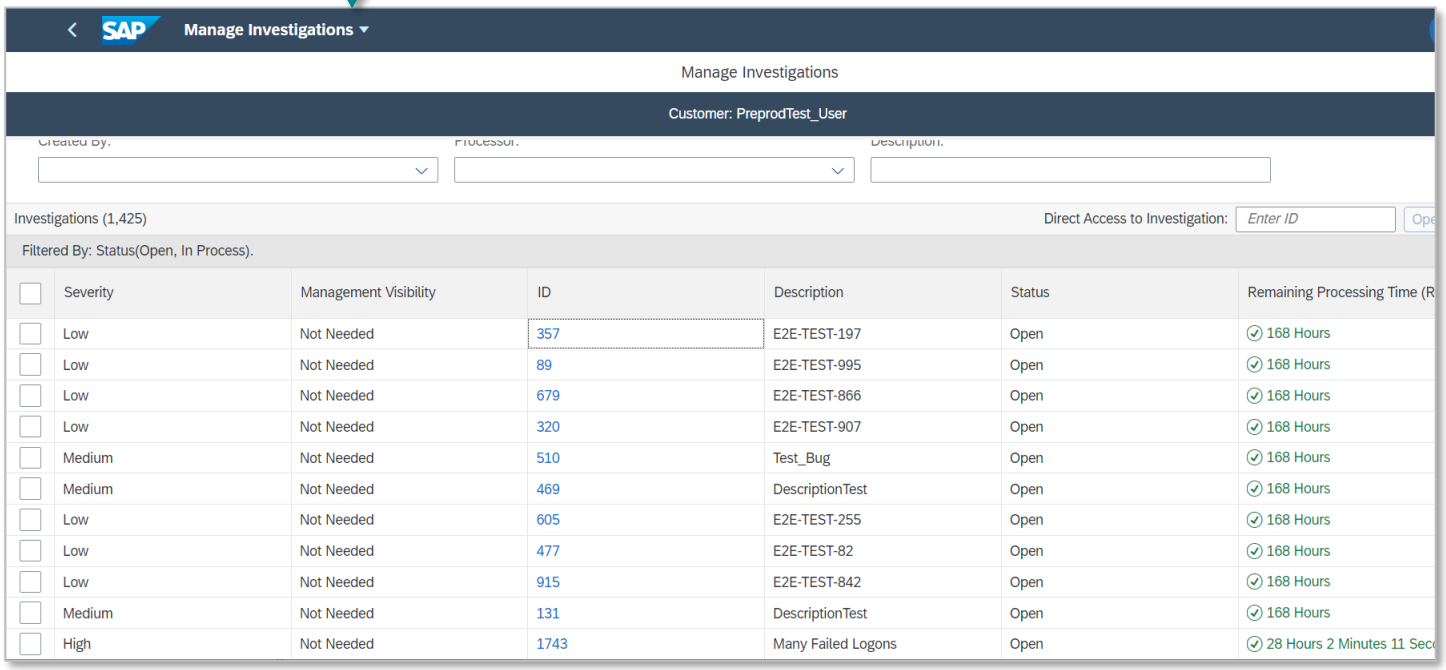


Severity	ID	Pattern	Trigger	Events	Status	Remaining Reaction Time (RRT)
High	41430	Failed logon of same user from different Terminal IDs	Measurement 2 exceeded threshold 2 for ('System ID, Actor' = 'S4H/000', 'User Pseudonym, Targeted' = 'TMSADM')	View	Open	119 Hours 58 Minutes 9 Seconds
High	41429	Blocklisted function modules in productive system	Measurement 1 exceeded threshold 1 for ('Event, Scenario Role Of Actor' = 'Client', 'Service, Function Name' = 'TH_SAPREL', 'System ID,...	View	Investigation Triggered	119 Hours 58 Minutes 16 Seconds
High	41428	Blocklisted function modules in productive system	Measurement 1 exceeded threshold 1 for ('Event, Scenario Role Of Actor' = 'Server', 'Service, Function Name' = 'TH_SAPREL', 'System ID,...	View	Investigation Triggered	119 Hours 58 Minutes 16 Seconds
High	41427	Failed logon with too many attempts	Measurement 6 exceeded threshold 3 for ('Event (Semantic)' = 'User, Logon, Failure', 'System ID, Actor' = 'S4H/000', 'User Pseudonym,...	View	Open	119 Hours 58 Minutes 19 Seconds
High	41426	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', 'Syste...	View	Open	119 Hours 58 Minutes 25 Seconds
Very High	41755	04_PWHashAttack	Measurement 3 exceeded threshold 1 for ('Resource Name' = 'USR02', 'User Pseudonym, Acting' = 'HTUT_35', 'User Pseudonym, Targeted' =...	View	No Reaction Needed	137 Hours 18 Minutes 5 Seconds
Very High	41748	Demo99_PWHashAttack	Measurement 3 exceeded threshold 1 for ('Resource Name' = 'USR02', 'User Pseudonym, Acting' = 'HTUT_35', 'User Pseudonym, Targeted' =...	View	No Reaction Needed	137 Hours 18 Minutes 28 Seconds
Very High	41747	99_PWHashAttack	Measurement 3 exceeded threshold 1 for ('Resource Name' = 'USR02', 'User Pseudonym, Acting' = 'HTUT_35')	View	No Reaction Needed	137 Hours 18 Minutes 40 Seconds
Very High	41736	Demo99_PWHashAttack	Measurement 2 exceeded threshold 1 for ('Resource Name' = 'USR02', 'User Pseudonym, Acting' = 'HTUT_35', 'User Pseudonym, Targeted' =...	View	No Reaction Needed	137 Hours 23 Minutes 29 Seconds
Very High	41734	04_PWHashAttack	Measurement 2 exceeded threshold 1 for ('Resource Name' = 'USR02', 'User Pseudonym, Acting' = 'HTUT_35', 'User Pseudonym, Targeted' =...	View	No Reaction Needed	137 Hours 28 Minutes 5 Seconds
Very High	41720	Data Theft with Fake User	Measurement 1 exceeded threshold 1 for ('User Pseudonym, Acting' = 'ETDADMIN04')	View	Open	137 Hours 28 Minutes 28 Seconds

Manage Investigations

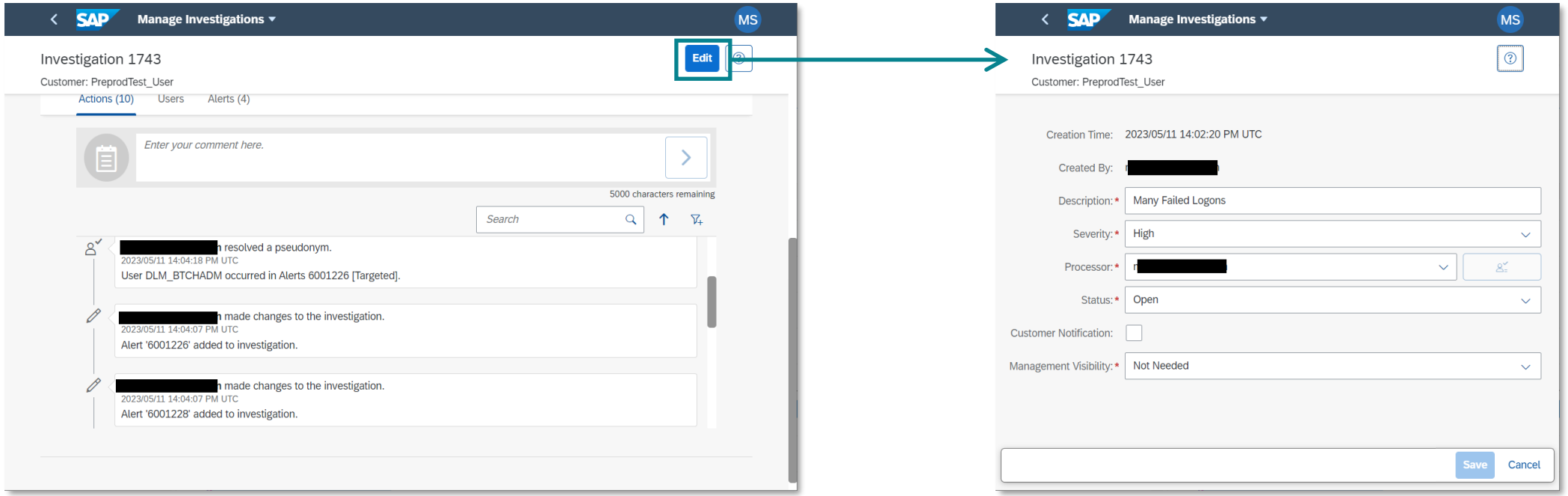
The Manage Investigations app can also be accessed from the Tenant Applications view. It allows viewing the list of Investigations, and drilling into details of each Investigation (cf. next slide).





Manage Investigations (2)

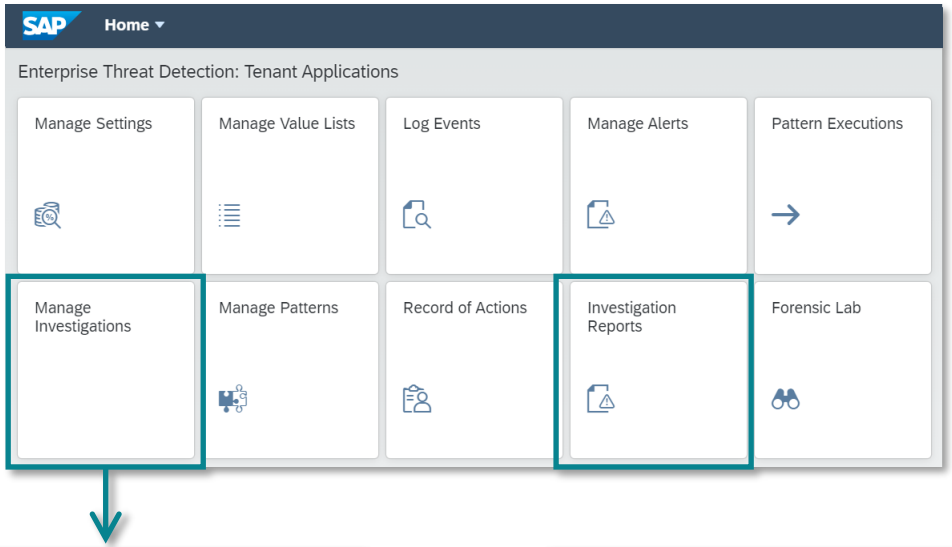
In the Manage Applications app, a monitoring agent can set details pertaining to the Investigation that will determine the visibility of the Investigation during and after processing.

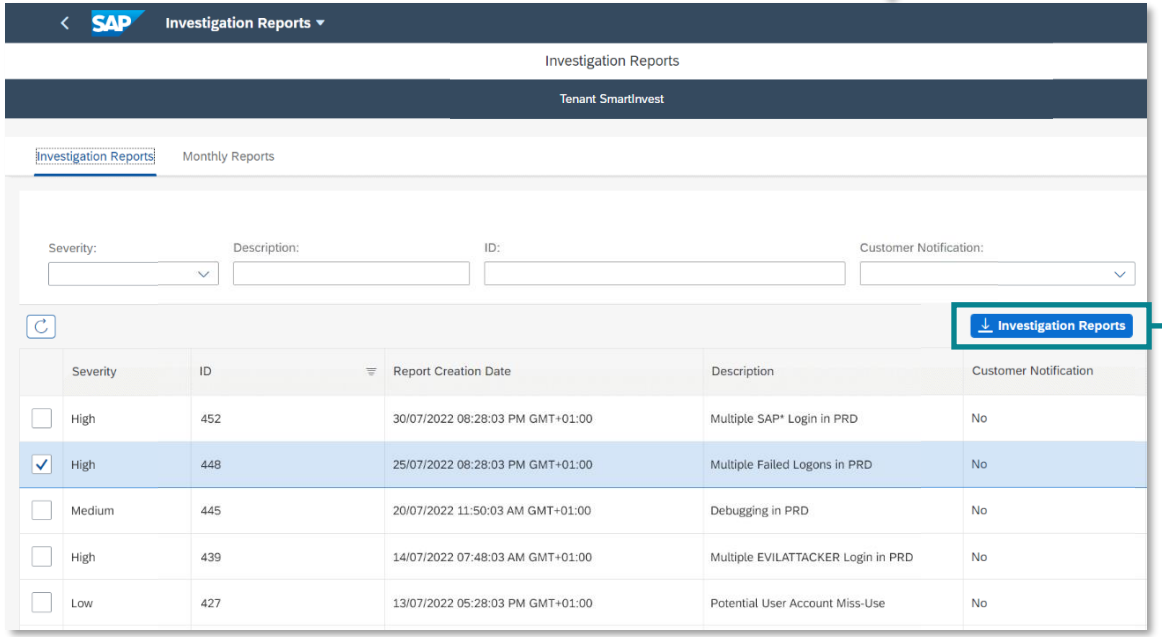


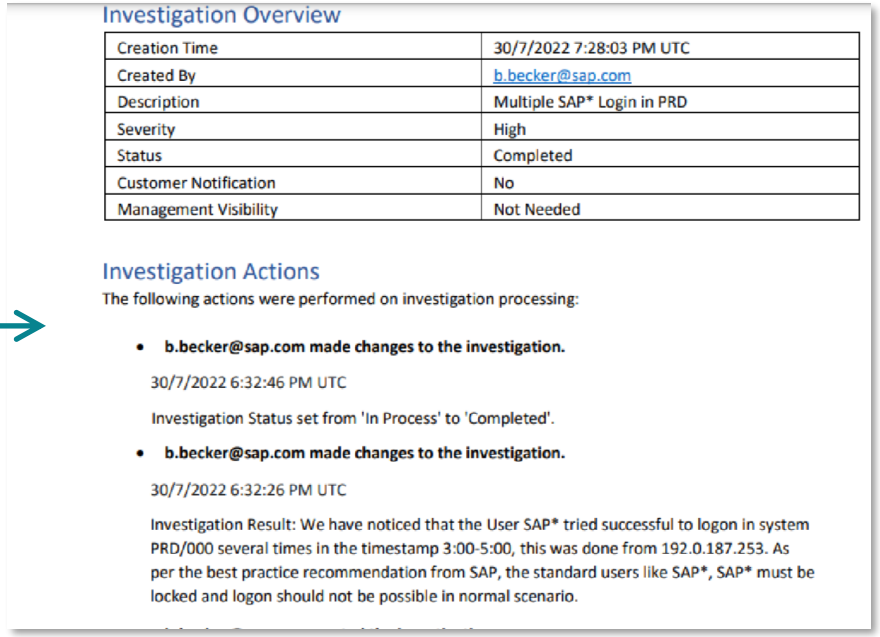
Investigation Reports

Upon concluding an Investigation, a report can be created and automatically distributed to relevant stakeholders.

The Investigation Reports app allows access to the repository of past Reports.







Investigation Overview

Creation Time	30/7/2022 7:28:03 PM UTC
Created By	b.becker@sap.com
Description	Multiple SAP* Login in PRD
Severity	High
Status	Completed
Customer Notification	No
Management Visibility	Not Needed

Investigation Actions

The following actions were performed on investigation processing:

- **b.becker@sap.com made changes to the investigation.**

  30/7/2022 6:32:46 PM UTC

  Investigation Status set from 'In Process' to 'Completed'.

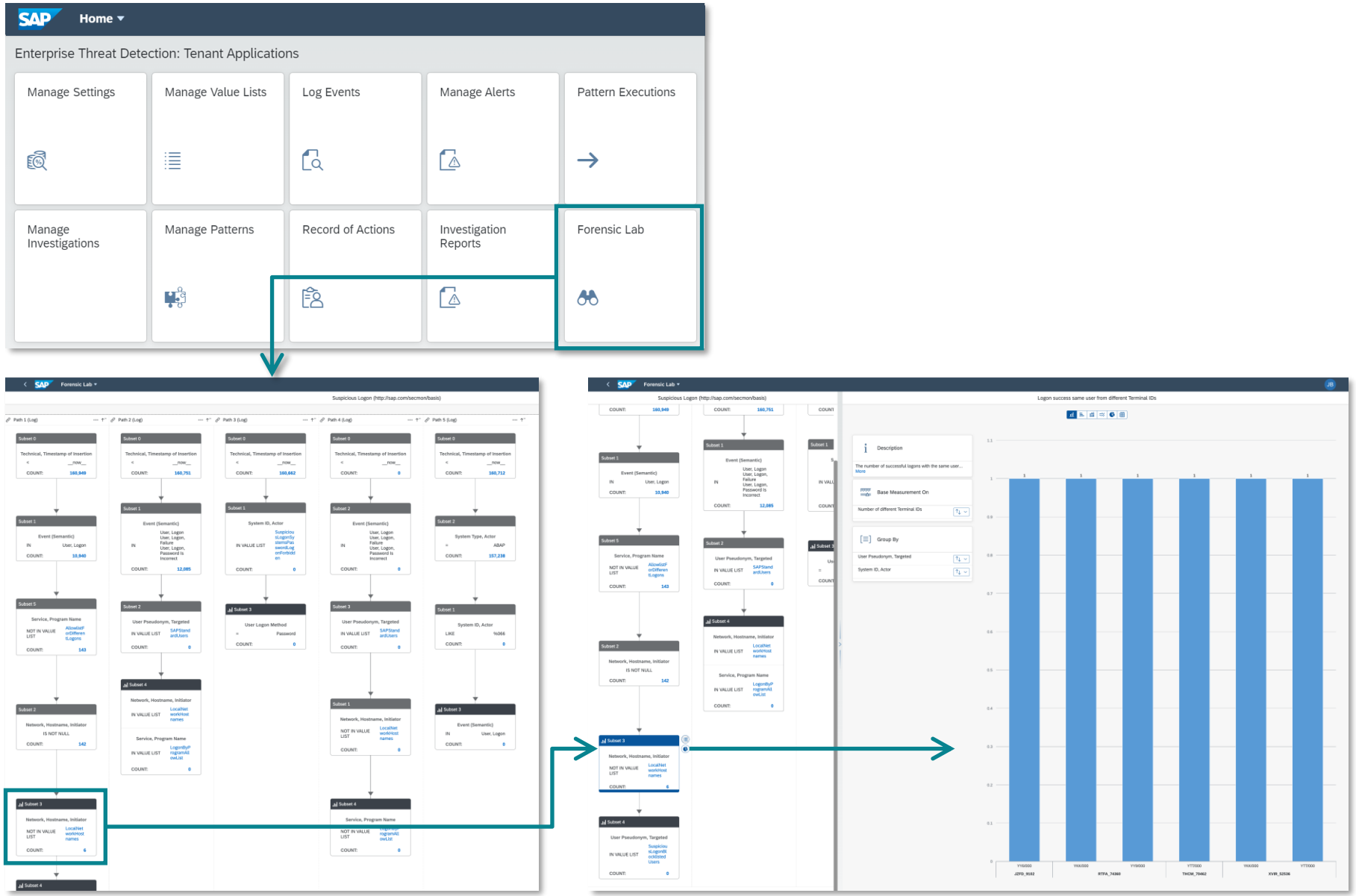
- **b.becker@sap.com made changes to the investigation.**

  30/7/2022 6:32:26 PM UTC

  Investigation Result: We have noticed that the User SAP* tried successful to logon in system PRD/000 several times in the timestamp 3:00-5:00, this was done from 192.0.187.253. As per the best practice recommendation from SAP, the standard users like SAP*, SAP* must be locked and logon should not be possible in normal scenario.

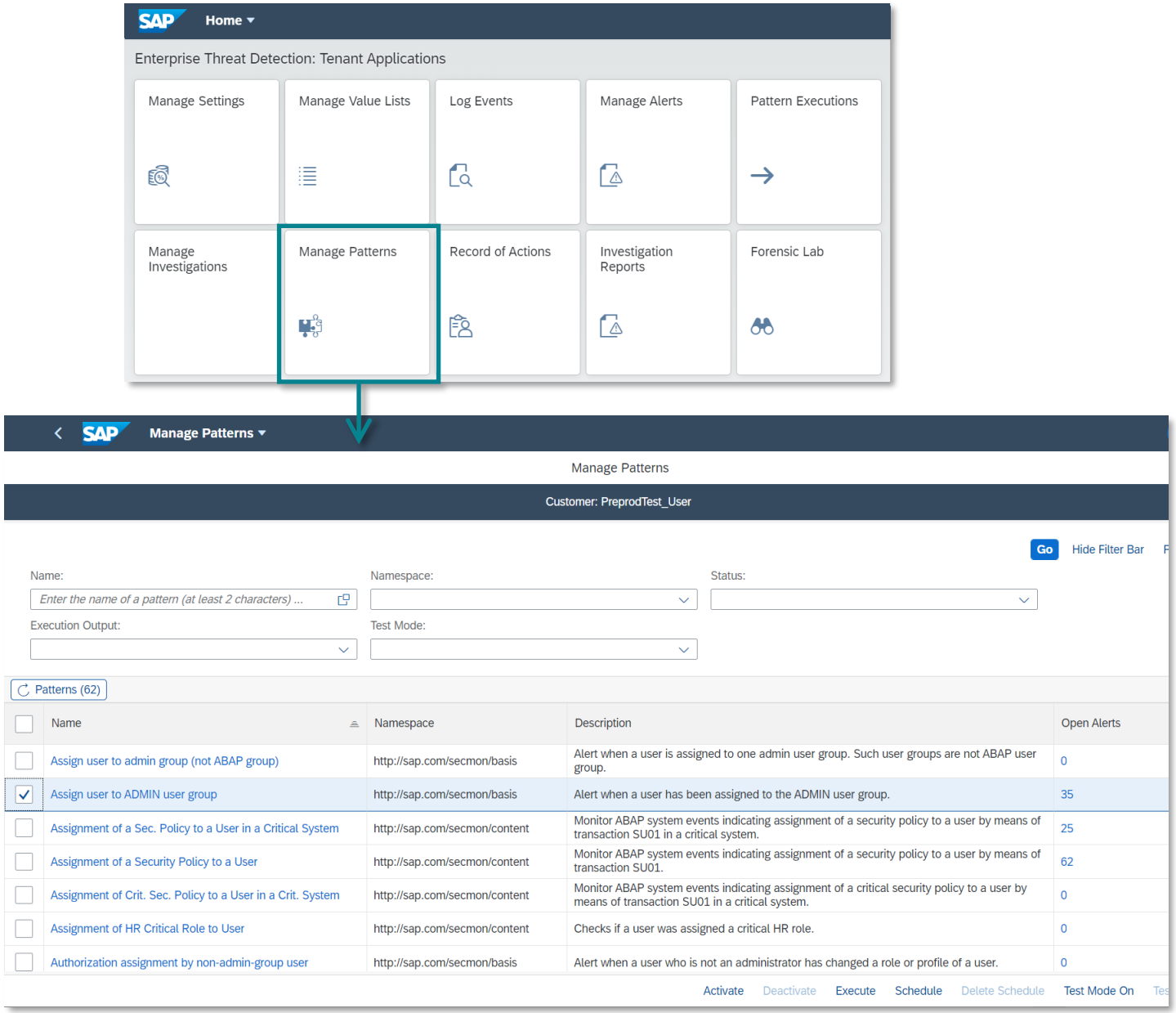
Forensic Lab

In the Forensic Lab, a monitoring agent can create new patterns and view and replay existing ones, and can obtain charts for better analysis.



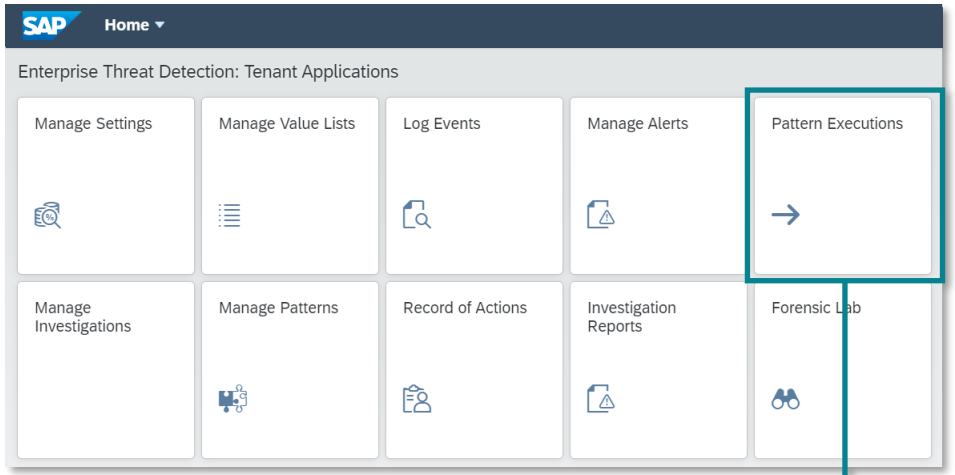
Manage Patterns

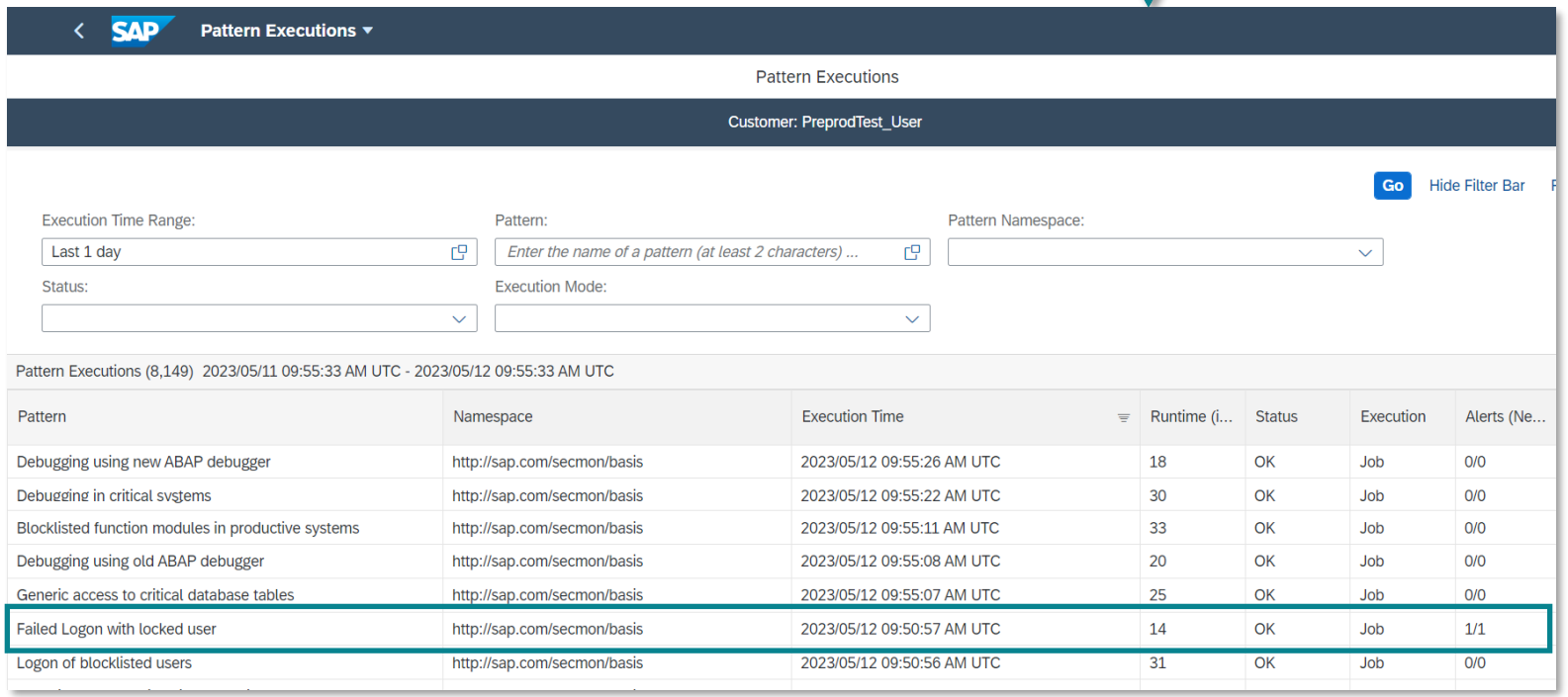
The Manage Patterns app renders a list of all Patterns, provides details of linked alerts, and constitutes a workbench for Patterns – creating, editing, activating Patterns; and scheduling or executing Patterns to throw additional Alerts if applicable.



Pattern Executions

The Pattern Execution app gives an overview which Patterns were executed, how many new Alerts the run generated, and allows for a detail view into the new Alerts.



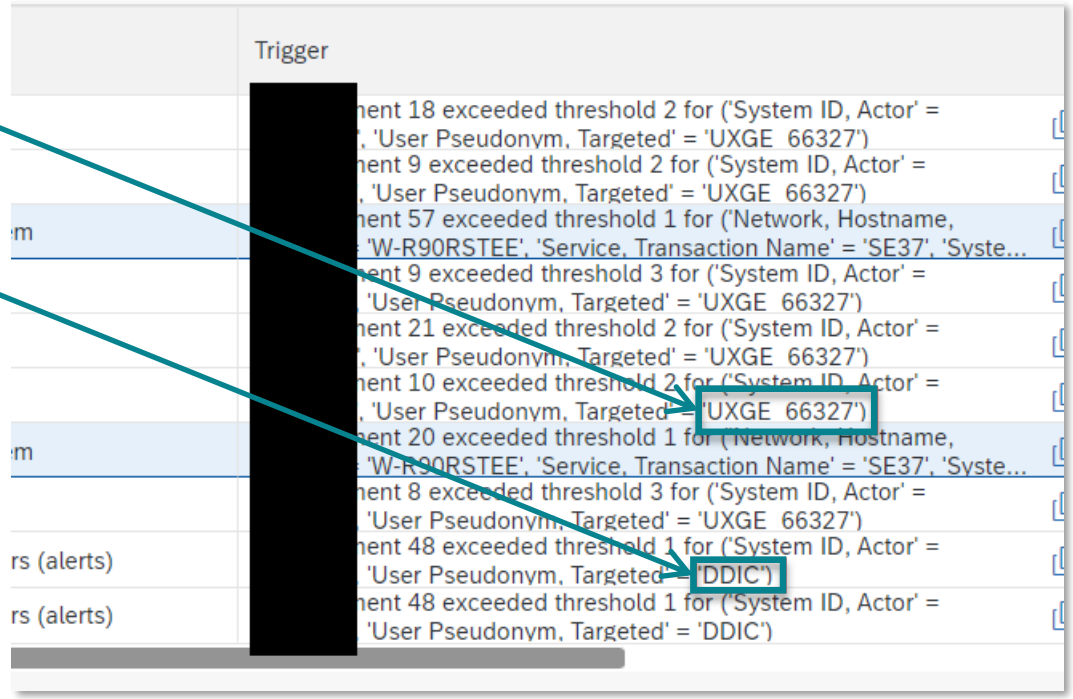


Compliance Features

Pseudonymization
Pseudonym Resolution
ETD Logs (who did what in ETD?)

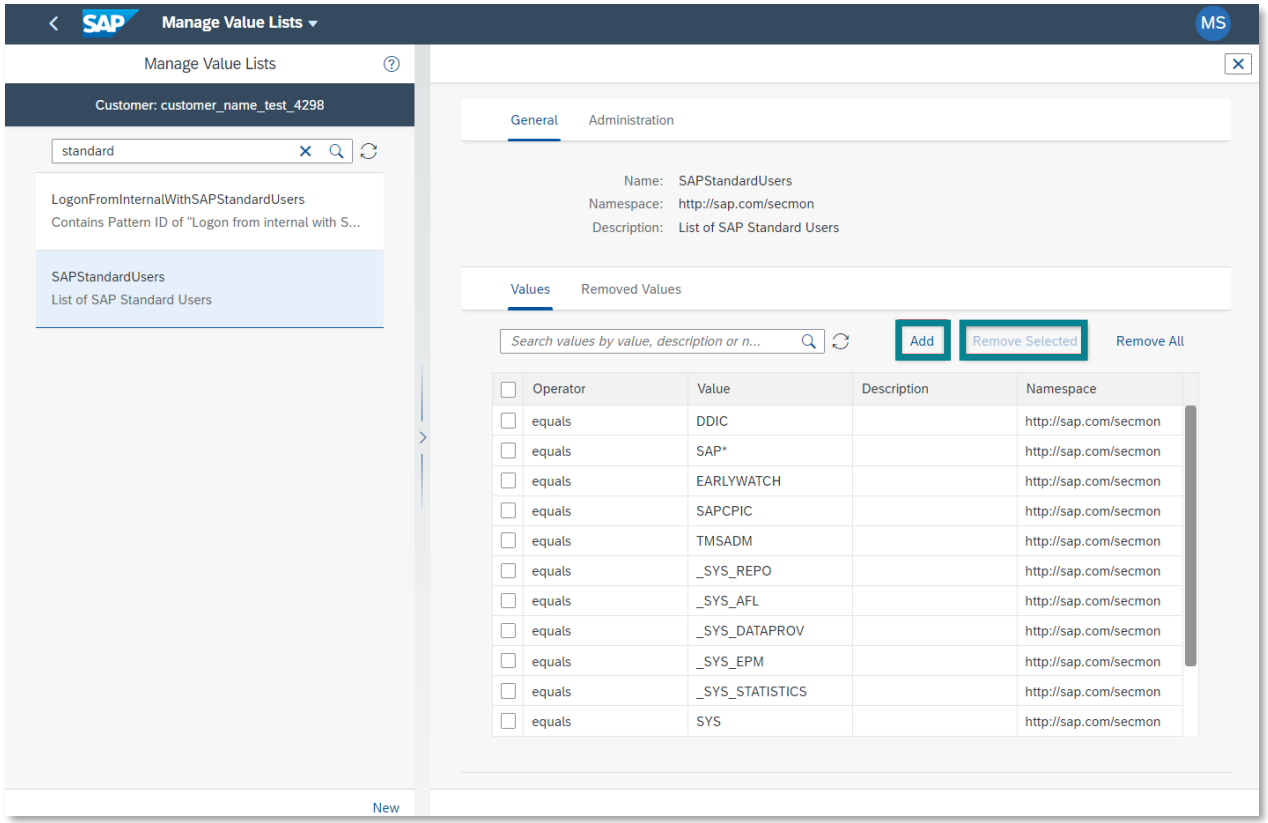
Pseudonymization by Default

- The system assigns each user ID a readable Pseudonym in a <Letters_Number> format
- SAP Standard users are not pseudonymized (if they are maintained in the value list “SAPStandardUsers” (cf. next slide)



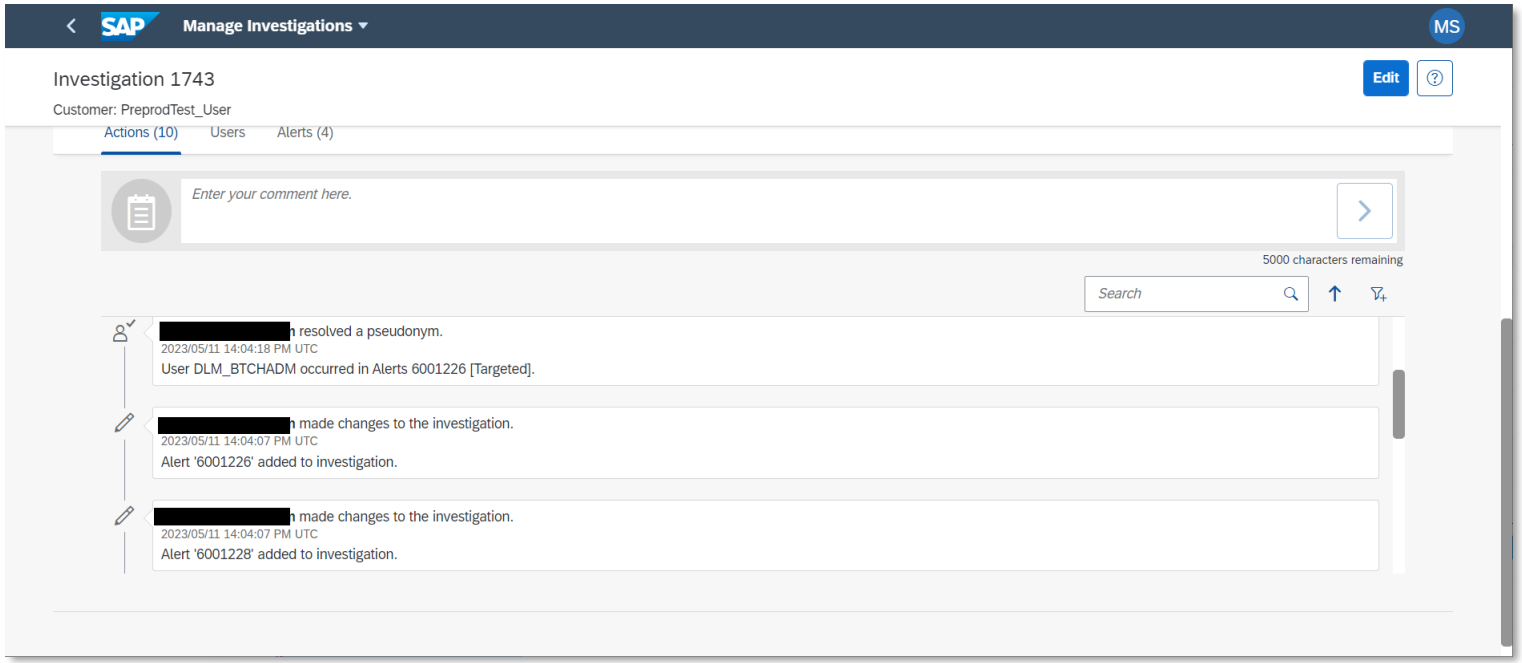
Value List SAPStandardUsers

- The list is prepopulated by SAP.
- SAP delivered values can be removed/excluded.
- More Values can be added, removed, or excluded.
- SAPStandardUsers Value Lists are never changed by solution updates.



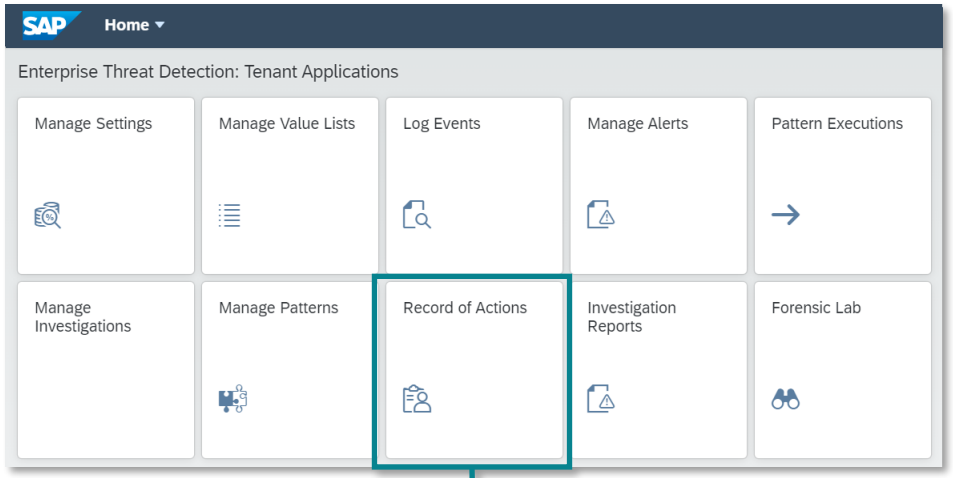
Pseudonym Resolution

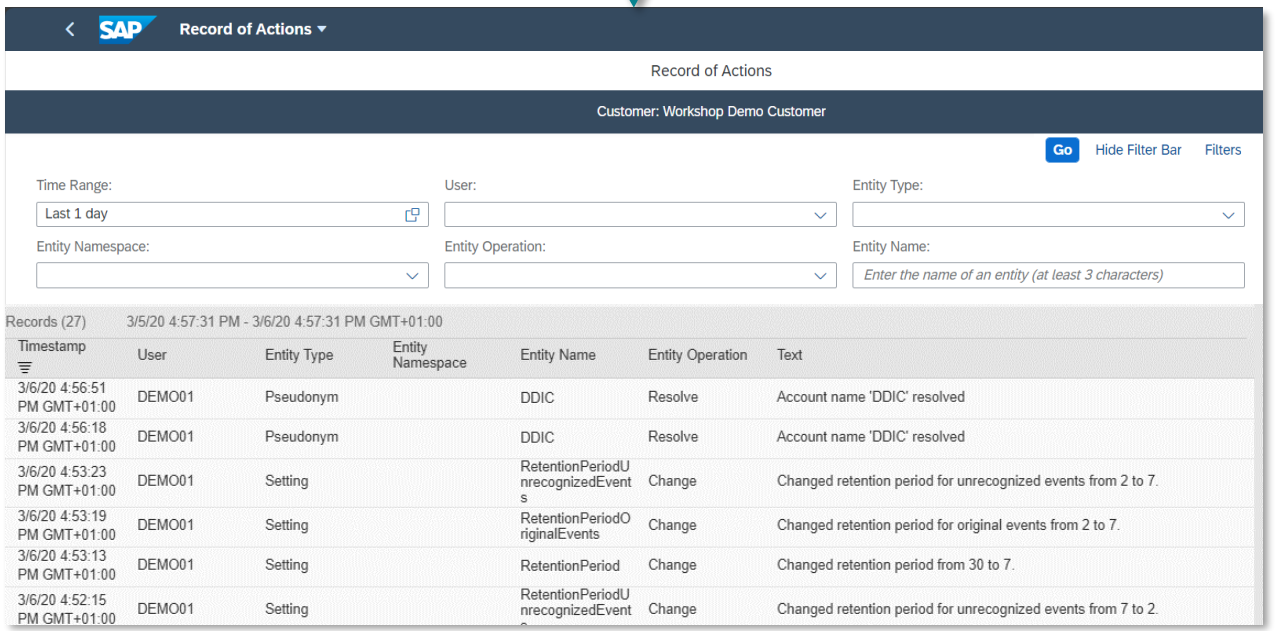
- Resolution of Pseudonyms (user accounts) can only be executed by users with special authorization.
- The resolution, triggering user, and the clear Name/ID are logged in the investigation action log.



ETD-own Action Logs: Record of Actions

All actions which are compliance relevant (e.g. changing the setup, or touching the identity of a user) are stored and can be viewed through the Record of Actions app.





Semantic Data Model

Log Sources and Log Types

Standard Log Types processed by ETD

Log Source ABAP: Any NetWeaver Application Server ABAP based System

- Security Audit Log
- System Log
- Business Transaction Log
- HTTP Server Log
- RFC Gateway Log
- User Change Log
- Change Document Log
- Read Access Log
- UI Logging Log
- SOAP based Web Services Log
- Message Server Log
- Database Table Change Log

Log Source Java: Any Netweaver Application Server Java based System

- Security Log
- Security Audit Log
- HTTP Access Log

Log Source HANA

- HANA Audit Trail

Log Source SAP Cloud Platform

- Audit Log SAP CP Neo
- Audit Log SAP CP CloudFoundry

Log Source SAP Cloud Products

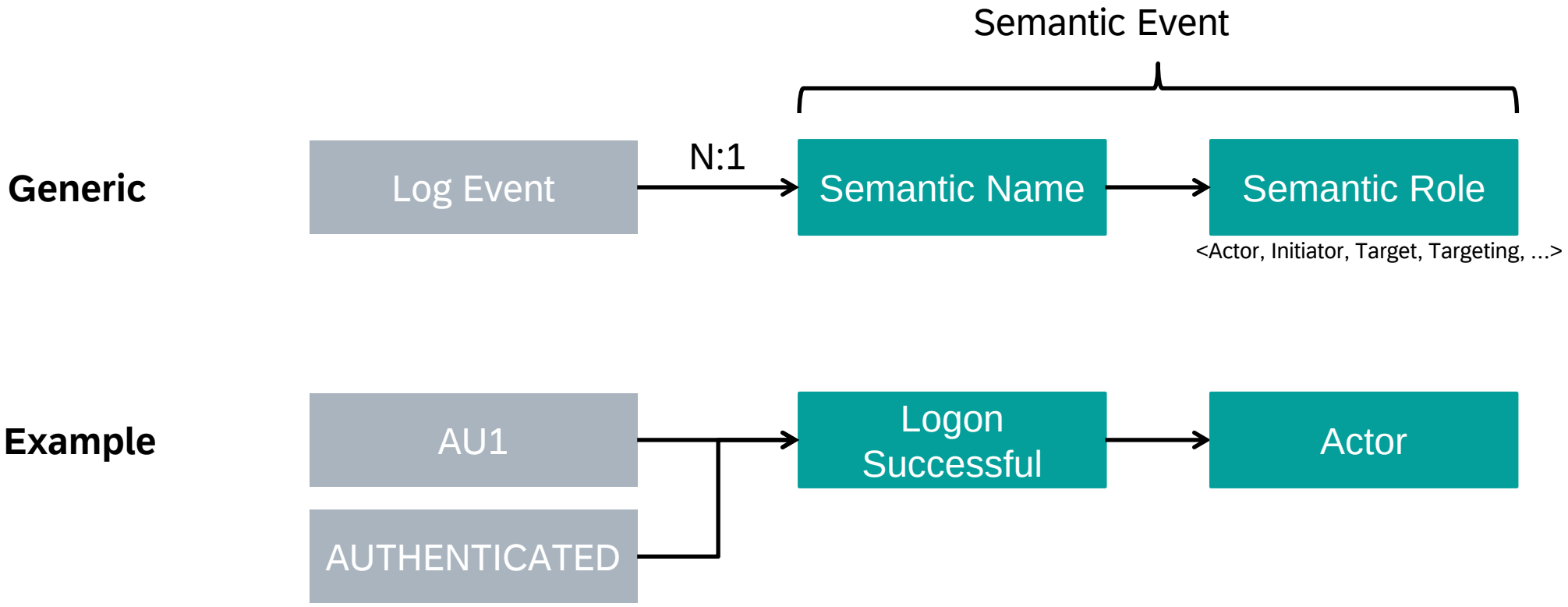
- SAP Analytics Cloud Audit Log
- SAP Cloud 4 Customer Log
- SAP Commerce Log

Other Log Sources

- Web Dispatcher Standalone HTTP Client and Server Log
- Cloud Connector Log
- SAPRouter Log

Semantic Attributes
Semantic Log Events

Semantic Data Model – Graphical View



SAP Enterprise Threat Detection – Semantic Data Model

- Vendor agnostic data model (~180 semantic attributes/160 semantic events)
- Supports logs from all layers
- Very fine granular and sophisticated analysis, via different roles
- Common procedures to do forensic analysis, independent of log data
- Log-independent, common tools to create Charts and Use Cases
- Reuse of defined Use Cases independent of new/unknown Log Data Sources
- Predelivered, re-usable Content
- Use Cases remain stable if logs change

Semantic Attributes : Roles of Attributes

System/Host Roles

System/Host Role	Description
Actor	The system that executes the software to perform the action that is logged. The software runs under the acting user account.
Initiator	The system that asks the actor to perform the action of the event. For example, an end device that asks an SAP system to run a transaction plays the initiator role.
Intermediary	In some events, the system that mediates between two other systems, usually between initiator and actor.
Reporter	The system that writes events to a log. Often the actor and reporter are the same system.
Target	The system that the actor asks to perform some function. For example, an actor requests a remote system, the target, to run a program.

e.g. within a Firewall Log: Contains IP Address Initiator/Reporter/Target

Semantic Attributes : Roles of Attributes

User Roles

User Role	Description
Acting	The user account under which the software on the actor system runs.
Initiating	The user account under which the software on the initiator system runs.
Targeted	In user administration, the account that is created, modified, or deleted.
Targeting	The user account under which the software on the target system runs.

e.g. within a User Change Log: Contains User Pseudonym Acting/Targeted

Semantic Log Events

Technical Log Events are translated to human readable Log Events

- Example: Technical Log Event “AU2” from Security Audit Log is translated to “User, Logon, Failure”

Semantic Log Events are shown in “Log Events”-Tile and in Forensic Lab

Examples of Semantic Log Events

[…]

User, Lock	UserLock	A system locks a targeted user.
User, Logoff	UserLogoff	A system logs off a targeted user.
User, Logon	UserLogon	A system logs on a targeted user. Usually the system authenticates the user and creates a session with GenericSessionId.
User, Logon, CSRF Attack	UserLogonCsrfAttack	A system detects a CSRF attack while trying to logon a targeted user.
User, Logon, Failure	UserLogonFailure	A system tries to log on a targeted user, but fails. Usually the system authenticates the user and creates a session with GenericSessionId.

[…]

Semantic Log Events

Complete list: help.sap.com → Application help → Basic Concepts

Display Name	Name	Description	Namespace	Created By
<Dynamic event assignment>	Dynamic	Dummy event for entry types with an event assignment that is based on extracted values	http://sap.com/secmon	SAP
<Ignore>	Ignore	Dummy event for entry types to be ignored	http://sap.com/secmon	SAP
<No event>	None	Dummy event for entry types with no semantic event assigned	http://sap.com/secmon	SAP
<OriginalDataOnly>	OriginalDataOnly	Dummy event to pass the original data to ETD, no event extraction	http://sap.com/secmon	SAP
Alert, Splunk	SplunkAlert	A Splunk alert has been received.	http://sap.com/secmon	SAP
ApplicationServer, Start	ApplicationServerStart	A user starts an application server.	http://sap.com/secmon	SAP
ApplicationServer, Stop	ApplicationServerStop	A user stops an application server.	http://sap.com/secmon	SAP
Attack, Call to Malicious Host, Detect	AttackCallToMaliciousHostDetect	A security system detects that an internal host calls a known malicious host or domain.	http://sap.com/secmon	SAP
Attack, Call to Malicious Host, Detect and Block	AttackCallToMaliciousHostDetectAndBlock	A security system detects that an internal host calls a known malicious host or domain. The security system blocks the call to a malicious host.	http://sap.com/secmon	SAP
Attack, Detect	AttackDetect	A system detects an attack.	http://sap.com/secmon	SAP
Attack, Detect and Block, By Means of Rules	AttackDetectAndBlockByMeansOfRules	A security system detects an attack by means of rules. The security system blocks the attack.	http://sap.com/secmon	SAP
Attack, Detect, By Means of Rules	AttackDetectByMeansOfRules	A security system detects an attack by means of rules.	http://sap.com/secmon	SAP
Attack, DNS Lookup Of Malicious Host, Detect	AttackDnsLookupOfMaliciousHostDetect	A security_system:actor detect#s #that an internal_host:initiator look#s #up a DNS_name_of_a_known_malicious_host_or_domain:target.	http://sap.com/secmon	SAP
Attack, Malware-object, Detect	AttackMalwareObjectDetect	A security system detects a malware-object.	http://sap.com/secmon	SAP
Attack, Zero-day Exploit, Detect, by Means of Dynamic Analysis	AttackZeroDayExploitDetectByMeansOfDynamicAnalysis	A security system detects a zero-day exploit by means of dynamic analysis. An internal host is the potential victim of the attack. A malicious host is the origin of the exploit.	http://sap.com/secmon	SAP
Attack, Zero-day Malware-object, Detect, by Means of Dynamic Analysis	AttackZeroDayMalwareObjectDetectByMeansOfDynamicAnalysis	A security system detects a zero-day malware-object by means of dynamic analysis. An internal host is the potential victim of the attack. A malicious host is the origin of the malware object.	http://sap.com/secmon	SAP
Communication, DNS Dynamic Zone Update, Deny	CommunicationDNSDynamicZoneUpdateDeny	A DNS server denies a dynamic zone update request from an initiator.	http://sap.com/secmon	SAP
Communication, DNS Forward Map, Add	CommunicationDNSForwardMapAdd	A DNS server adds a DNS forward map as requested by an initiator.	http://sap.com/secmon	SAP
Communication, DNS Forward Map, Add, Failure	CommunicationDNSForwardMapAddFailure	A DNS server tries to add a DNS forward map as requested by an initiator, but fails.	http://sap.com/secmon	SAP
Communication, DNS Reverse Map, Add	CommunicationDNSReverseMapAdd	A DNS server adds a DNS reverse map as requested by an initiator.	http://sap.com/secmon	SAP
Communication, DNS Reverse Map, Add, Failure	CommunicationDNSReverseMapAddFailure	A DNS server tries to add a DNS reverse map as requested by an initiator, but fails.	http://sap.com/secmon	SAP
Communication, HTTP Request or HTTP Response, Allow	CommunicationHttpRequestOrHttpResponseAllow	A web filter allows an HTTP request or HTTP response between an HTTP client and an HTTP server.	http://sap.com/secmon	SAP
Communication, HTTP Request or HTTP Response, Block	CommunicationHttpRequestOrHttpResponseBlock	A web filter blocks an HTTP request or HTTP response between an HTTP client and an HTTP server.	http://sap.com/secmon	SAP
Communication, HTTP Request, Allow	CommunicationHttpRequestAllow	A web filter allows an HTTP request from an HTTP client to an HTTP server.	http://sap.com/secmon	SAP
Communication, HTTP Request, Block	CommunicationHttpRequestBlock	A web filter blocks an HTTP request from an HTTP client to an HTTP server.	http://sap.com/secmon	SAP
Communication, HTTP Request, React To	CommunicationHttpRequestReactTo	An HTTP server reacts to an HTTP request.	http://sap.com/secmon	SAP
Communication, HTTP Request, Send	CommunicationHttpRequestSend	A client sends an HTTP request to an HTTP server.	http://sap.com/secmon	SAP
Communication, HTTP Response, Allow	CommunicationHttpResponseAllow	A web filter allows an HTTP response from a HTTP server to an HTTP client.	http://sap.com/secmon	SAP

All Log Data is normalized and inserted into a Log DB table with Semantic Attributes

Semantic Attribute Names : Examples

[...]

Network, IP Address, Actor	The IP address of the actor of the event.
Network, IP Address, Initiator	The IP address of the initiator of the event.
Network, IP Address, Intermediary	The IP address of the intermediary of the event.
Network, IP Address, Reporter	The IP address of the reporter of the event.
Network, IP Address, Target	The IP address of the target of the event.

[...]

User Pseudonym, Acting	The pseudonym of the acting user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off, etc.
User Pseudonym, Initiating	The pseudonym of the initiating user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off,…
User Pseudonym, Targeted	The pseudonym of the targeted user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off,…
User Pseudonym, Targeting	The pseudonym of the targeting user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off,…

[...]

Semantic Attributes in Detail

ETD Semantic Attributes – Events

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Attack Name	The attack name, for example, a malware name.	NVARCHAR
Attack Type	The attack type,for example, malware, spoof, or denial of service.	NVARCHAR
Correlation ID	Used to correlate log instances at the top level, for example, the root context ID of an SAP passport.	NVARCHAR
Correlation Sub ID	Used to correlate log instances at a lower level of a hierarchy of related instances, for example, the connection ID of an SAP passport.	NVARCHAR
Event (Semantic)	Choose this attribute if you want to select semantic events.	NVARCHAR
Event Code	Event name or event code. Either a code that identifies the log entry type, or a text that describes the event.	NVARCHAR
Event Source ID	The ID of the source of the event, for example, a hostname of a syslog server.	NVARCHAR
Event Source Type	The type of the source of the event, for example, a syslog server.	NVARCHAR
Event, Log Type	The type of log that the event comes from. This is set in the log learning process.	NVARCHAR
Event, Message	The text of the event instance, often called the event message.	NVARCHAR
Event, Original Message	Original log data	NVARCHAR
Event, Scenario Role Of Actor	The scenario role of the actor, for example, client, server, or proxy. An example of a scenario is a client-server scenario where one system plays the role of the client and the other the role of the server.	NVARCHAR
Event, Scenario Role Of Initiator	The scenario role of the initiator, for example, client, server, or proxy. An example of a scenario is a client-server scenario where one system plays the role of the client and the other the role of the server.	NVARCHAR
Event, Severity Code	The severity of the event.	NVARCHAR

Link to complete List of Semantic Attributes including documentation & categorization:
https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_CLOUD_EDITION/91cfc1d15c81413aaef9efee05069772/4826e1873fbd4df3863b06018b9be9a4.html?q=Semantic

ETD Semantic Attributes – generic, LoB

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Generic, Action	The action name or action code, usually the verb of the event, such as create.	NVARCHAR
Generic, Category	A general category for various purposes, for example, the category of a web site, such as sports or news.	NVARCHAR
Generic, Device Type	The type of a device, usually an end user device, for example, an android phone.	NVARCHAR
Generic, Explanation	An explanation of an action or attack, etc. Use 'Generic Outcome Reason' for the reason for an outcome. This is for more general explanatory text.	NVARCHAR
Generic, Geolocation Code, Initiator	A code for the geographic location of the initiator of the event. This code is found in some logs at network level.	NVARCHAR
Generic, Geolocation Code, Target	A code for the geographic location of the target of the event. This code is found in some logs at network level.	NVARCHAR
Generic, Order	The order of something. This can be used for the numbered step of a workflow, for example.	BIGINT
Generic, Outcome	The outcome of actions or processes. Use 'Service Outcome' for codes returned by services like HTTP servers.	NVARCHAR
Generic, Outcome, Reason	The reason for the outcome of an action, a service call, or other happening.	NVARCHAR
Generic, Path	A path, for example, a path of a URL or other hierarchical structure. Use 'Resource Name' for a filename. Include the directory path, if any, in 'Resource Name', rather than in this attribute.	NVARCHAR
Generic, Path, Prior	The prior path is used in case there are two paths in an event. If there are two, one is the prior, and the other is just the path.	NVARCHAR
Generic, Purpose	The purpose of the log instance. For example, an SAP Read Access Log instance might specify a purpose such as verification of conformance to a particular regulatory requirement.	NVARCHAR
Generic, Risk Level	The level of risk associated with an action or resource, etc.	NVARCHAR
Generic, Score	A number representing the importance of an event or other thing that can be assigned an importance. The larger the score, the more important the thing. Usually the score ranges from zero to one hundred.	BIGINT
Generic, Session ID	The ID of a session, usually a user session. This is an application level session ID. Use 'Network Session ID' for a network-level connection ID.	NVARCHAR
Generic, URI	Uniform Resource Identifier (URI), also referred to as a URL.	NVARCHAR
ID	Used to identify contret log entry.	NVARCHAR
Line of Business, Actor	The Line of Business of the actor system as defined in the System application.	NVARCHAR
Line of Business, Initiator	The Line of Business of the initiator system as defined in the System application.	NVARCHAR
Line of Business, Intermediary	The Line of Business of the intermediary system as defined in the System application.	NVARCHAR
Line of Business, Reporter	The Line of Business of the reporter system as defined in the System application.	NVARCHAR
Line of Business, Target	The Line of Business of the target system as defined in the System application.	NVARCHAR

ETD Semantic Attributes - Network

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

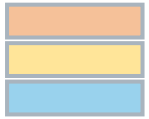
Network, Host Domain, Actor	The domain part of the hostname of the actor of the event.	NVARCHAR
Network, Host Domain, Initiator	The domain part of the hostname of the initiator of the event.	NVARCHAR
Network, Host Domain, Intermediary	The domain part of the hostname of the intermediary of the event.	NVARCHAR
Network, Host Domain, Reporter	The domain part of the hostname of the reporter of the event.	NVARCHAR
Network, Host Domain, Target	The domain part of the hostname of the target of the event.	NVARCHAR
Network, Hostname, Actor	The local part of the hostname of the actor of the event.	NVARCHAR
Network, Hostname, Initiator	The local part of the hostname of the initiator of the event.	NVARCHAR
Network, Hostname, Intermediary	The local part of the hostname of the intermediary of the event.	NVARCHAR
Network, Hostname, Reporter	The local part of the hostname of the reporter of the event.	NVARCHAR
Network, Hostname, Target	The local part of the hostname of the target of the event.	NVARCHAR
Network, Interface, Initiator	The name of a network interface that connects to the initiator. The network interface is part of the actor.	NVARCHAR
Network, Interface, Target	The name of a network interface that connects to the target. The network interface is part of the actor.	NVARCHAR
Network, IP Address, Actor	The IP address of the actor of the event.	NVARCHAR
Network, IP Address, Initiator	The IP address of the initiator of the event.	NVARCHAR
Network, IP Address, Intermediary	The IP address of the intermediary of the event.	NVARCHAR
Network, IP Address, Reporter	The IP address of the reporter of the event.	NVARCHAR
Network, IP Address, Target	The IP address of the target of the event.	NVARCHAR

ETD Semantic Attributes – Network (continued)

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Network, IP Before NAT, Initiator	The IP address of the initiator of the event before network address translation (NAT). The IP Address after NAT is in 'Network IP Address'.	NVARCHAR
Network, IP Before NAT, Target	The IP address of the target of the event before network address translation (NAT). The IP Address after NAT is in 'Network IP Address'.	NVARCHAR
Network, MAC Address, Actor	The MAC address of the actor of the event.	NVARCHAR
Network, MAC Address, Initiator	The MAC address of the initiator of the event.	NVARCHAR
Network, MAC Address, Intermediary	The MAC address of the intermediary of the event.	NVARCHAR
Network, MAC Address, Reporter	The MAC address of the reporter of the event.	NVARCHAR
Network, MAC Address, Target	The MAC address of the target of the event.	NVARCHAR
Network, Network Prefix, Initiator	The subnetwork for the initiator, for example, an IP prefix, reported in network level logs. It is represented as an IP address and number, where number is the length of the prefix in bits, for example, 24.	NVARCHAR
Network, Network Prefix, Target	The subnetwork for the target, for example, an IP prefix, reported in network level logs. It is represented as an IP address and number, where number is the length of the prefix in bits, for example, 24.	NVARCHAR
Network, Port Before NAT, Initiator	The initiator port number before Network Address Translation (NAT). The port number after NAT is in 'network, port'.	INTEGER
Network, Port Before NAT, Target	The target port number before Network Address Translation (NAT). The port number after NAT is in 'network, port'.	INTEGER
Network, Port, Actor	The port number of the actor of the event, for example, a UDP or TCP port number.	INTEGER
Network, Port, Initiator	The port number of the initiator of the event, for example, a UDP or TCP port number.	INTEGER
Network, Port, Intermediary	The port number of the intermediary of the event, for example, a UDP or TCP port number.	INTEGER
Network, Port, Reporter	The port number of the reporter of the event, for example, a UDP or TCP port number.	INTEGER
Network, Port, Target	The port number of the target of the event, for example, a UDP or TCP port number.	INTEGER
Network, Protocol	The protocol of the packet, for example, ICMP, TCP, or UDP. This is a code or name from IANA, or a vendor-specific protocol name.	NVARCHAR
Network, Session ID	Session or connection ID at network level. Use 'Generic session ID' for an application level session ID.	NVARCHAR

ETD Semantic Attributes – Network (continued)



Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Network, Subnet Description, Actor	Network Subnet Description Actor	NVARCHAR
Network, Subnet Description, Initiator	Network Subnet Description Initiator	NVARCHAR
Network, Subnet Description, Intermediary	Network Subnet Description Intermediary	NVARCHAR
Network, Subnet Description, Reporter	Network Subnet Description Reporter	NVARCHAR
Network, Subnet Description, Target	Network Subnet Description Target	NVARCHAR
Network, Subnet, Address, Actor	A network address that identifies the subnetwork that includes the actor of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Address, Initiator	A network address that identifies the subnetwork that includes the initiator of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Address, Intermediary	A network address that identifies the subnetwork that includes the intermediary of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Address, Reporter	A network address that identifies the subnetwork that includes the reporter of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Address, Target	A network address that identifies the subnetwork that includes the target of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Category, Actor	The category of the subnetwork that includes the actor of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Category, Initiator	The category of the subnetwork that includes the initiator of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Category, Intermediary	The category of the subnetwork that includes the intermediary of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Category, Reporter	The category of the subnetwork that includes the reporter of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Category, Target	The category of the subnetwork that includes the target of the event. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Location, Actor	The location of the subnetwork that includes the actor of the event, for example, the name of a city. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Location, Initiator	The location of the subnetwork that includes the initiator of the event, for example, the name of a city. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Location, Intermediary	The location of the subnetwork that includes the intermediary of the event, for example, the name of a city. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Location, Reporter	The location of the subnetwork that includes the reporter of the event, for example, the name of a city. Subnetworks are managed by administrators.	NVARCHAR
Network, Subnet, Location, Target	The location of the subnetwork that includes the target of the event, for example, the name of a city. Subnetworks are managed by administrators.	NVARCHAR
Network, Zone, Initiator	A name for an area of a network, for example, the user zone, the server zone, or the Internet zone. The named area is the area of the initiator of the event. Zones may occur in network level logs.	NVARCHAR
Network, Zone, Target	A name for an area of a network, for example, the user zone, the server zone, or the Internet zone. The named area is the area of the target of the event. Zones may occur in network level logs.	NVARCHAR

ETD Semantic Attributes – Parameter, Privilege

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Parameter Data Type	The datatype of the parameter, for example, numeric, string or timestamp.	NVARCHAR
Parameter Data Type, Context	The datatype of a context parameter, for example, string or numeric.	NVARCHAR
Parameter Direction	The direction of the parameter: input, output, or input and output.	NVARCHAR
Parameter Name	The name of a parameter. For Read Access Logging, this is the technical name of a field, that is, a service argument if the access channel is an API, or a screen element name, if the access channel is a User Interface (UI).	NVARCHAR
Parameter Name, Context	The name of a parameter that gives the context for other parameters, for example, an employee ID field in a Dynpro application could be the context for other fields containing data about this employee.	NVARCHAR
Parameter Type	The type of a parameter. Types of parameters include attributes, features, states, configuration settings, etc. For Read Access Logging, this is the log domain name, a name which provides some semantics for technical names.	NVARCHAR
Parameter Type, Context	The type of the context parameter. For Read Access Logging, this is the log domain.	NVARCHAR
Parameter Value, Double	The value of a floating point numeric parameter.	DOUBLE
Parameter Value, Double, Prio Rvalue	The value of a floating point numeric parameter prior to a modification.	DOUBLE
Parameter Value, Number	The value of a numeric parameter.	BIGINT
Parameter Value, Number, Context	The value of a numeric context parameter.	BIGINT
Parameter Value, Number, Prior Value	The value of a numeric parameter prior to a modification.	BIGINT
Parameter Value, String	The value of a string parameter.	NVARCHAR
Parameter Value, String, Context	The value of a string context parameter.	NVARCHAR
Parameter Value, String, Prior Value	The value of a string parameter prior to a modification.	NVARCHAR
Parameter Value, Timestamp	The value of a timestamp parameter.	TIMESTAMP
Parameter Value, Timestamp, Prior Value	The value of a timestamp parameter prior to a modification.	TIMESTAMP
Parameter, Direction, Context	The direction of a parameter that gives the context for other parameters, for example, an employee ID field in a Dynpro application could be the context for other fields containing data about this employee. The direction can be input, output, or inp...	NVARCHAR
Privilege Is Grantable	Indicates if the granted privileges can be granted to others by the grantee, the receiver of the privileges.	NVARCHAR
Privilege Name	The name of a privilege.	NVARCHAR
Privilege Type	The type of a privilege.	NVARCHAR
Privilege, Grantee Name	The name of a grantee, a receiver of privileges.	NVARCHAR
Privilege, Grantee Type	The type of a grantee, a receiver of privileges. If the type is user, then 'username, targeted' and 'privilege, grantee name' should both contain the username of the grantee.	NVARCHAR

ETD Semantic Attributes – Resource

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

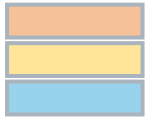
Resource Container Name	The name of a resource container.	NVARCHAR
Resource Container Type	The type of a resource container, for example, a database schema or a data repository.	NVARCHAR
Resource Content Or Hash	Either a hash of the content of a resource or simply the content of the resource. A hash is often used to check the integrity of the content. A mismatch between the computed hash and the given hash indicates that the content has been modified.	NVARCHAR
Resource Content Type	The type of content of a resource, for example, a MIME type.	NVARCHAR
Resource Count	The number of countable resources. Use 'resource type' for the type of the resource counted.	BIGINT
Resource Name	The name of a resource, for example, a filename, a database table name, etc. Not all resources are named, for example, a message has a type, but not usually a name. Use this attribute for a filename and include the directory path, if any.	NVARCHAR
Resource Name, Prior	The name of a prior resource, for example, if the event reports the execution of a command like 'copy /sys/x.exe to /com/y.exe', this is the name of the 'from file','/sys/x.exe'. The name of the 'to filename', '/com/y.exe' goes in 'resource name'.	NVARCHAR
Resource Request Size	The size of a request message, for example, an HTTP request. The units of measure for the size, for example, 'byte', are in 'resource, units of measure'.	BIGINT
Resource Response Size	The size of a response message, for example, an HTTP response. The units of measure for the size, for example, 'byte', are in 'resource, units of measure'.	BIGINT
Resource Size	The length or size of the resource, usually in bytes. Use 'resource type' for the type.	BIGINT
Resource Type	The type of a resource involved in an event. Examples of resources are files, messages, database tables, configurations, etc.	NVARCHAR
Resource, Sum Criteria	A phrase specifying what is summed over time, for example, 'matches of packets to denied list'. This sum is a count of how many packets matched a list of source IP addresses that are denied access to the network. In this case, 'resource type' would…	NVARCHAR
Resource, Sum Over Time	The sum over time of something related to a resource, 'resource, sum criteria' specifies what is summed.	DOUBLE
Resource, Units Of Measure	The units of measurement for a size or sum of a resource.	NVARCHAR

ETD Semantic Attributes – Service

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Service, Access Name	A name that can be used to access a service, used for RFC destination, for example.	NVARCHAR
Service, Application Component	A software building block within an application that enables a set of department-oriented business processes or cross-functional business processes. Application components can offer services to support these business processes. Application components…	NVARCHAR
Service, Application Name	The syslog application name or other application name. An application is, in general, at a higher level of hierarchy than a program.	NVARCHAR
Service, Executable Name	The name of an executable whose type is identified by 'executable type'. Only use these two fields if there is a special kind of executable that does not match an existing attribute such as transaction name or program name.	NVARCHAR
Service, Executable Type	The type of an executable whose name is identified by 'executable name'. Only use these two fields if there is a special kind of executable that does not match an existing attribute such as 'transaction name' or 'program name'.	NVARCHAR
Service, Function Name	The name of a function module, a procedure, an HTTP method, a web service operation, or similar type of relatively low level executable.	NVARCHAR
Service, Instance Name	The name of the service instance. For SAP Netweaver Application Server ABAP, the instance name identifies server, system and instance number.	NVARCHAR
Service, Outcome	The outcome of a service, for example, the code returned by an HTTP server.	NVARCHAR
Service, Part ID	An identifier for a part of some service, for example, a particular library that is used across services.	NVARCHAR
Service, Process ID	The identifier of a process, also called PID.	NVARCHAR
Service, Program Name	The name of a program or report.	NVARCHAR
Service, Referrer	The HTTP referrer or other type of referrer.	NVARCHAR
Service, Request Line	The request line for HTTP or the command line for a program, etc.	NVARCHAR
Service, Software Component	A set of SAP software objects that are grouped in development classes and can only be delivered together. For example, SAP CRM. The application component and the software component come from the object directory as part of ETD master data…	NVARCHAR
Service, Transaction Name	The name of a middle level of a hierarchy of execution. The hierarchy goes from workflow, to transaction, to program, to function.	NVARCHAR
Service, Type	The type of the service running on an actor, for example, 'HTTP Client', 'FTP Server', etc. This is often related to the network protocol, which would be 'HTTP'.	NVARCHAR
Service, User Agent	The HTTP user agent field or other field that gives information about the client's agent program.	NVARCHAR
Service, Version	The version of the type of service, for example, 1.1 for HTTP.	NVARCHAR
Service, Workflow Name	The name of a workflow, the highest level of a 4-level hierarchy of execution: workflow, transaction, program, function. Note that a report is a type of program.	NVARCHAR

ETD Semantic Attributes – System



Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

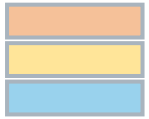
System Group, ID, Actor	The ID of the system group that the actor system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, ID, Initiator	The ID of the system group that the initiator system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, ID, Intermediary	The ID of the system group that the intermediary system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, ID, Reporter	The ID of the system group that the reporter system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, ID, Target	The ID of the system group that the target system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, Role, Actor	The role of the system group that the actor system belongs to. All systems that belong to the same system group have the same system group ID and type. Examples of roles are: test, production, and customizing.	NVARCHAR	>
System Group, Role, Initiator	The role of the system group that the initiator system belongs to. All systems that belong to the same system group have the same system group ID and type. Examples of roles are: test, production, and customizing.	NVARCHAR	>
System Group, Role, Intermediary	The role of the system group that the intermediary system belongs to. All systems that belong to the same system group have the same system group ID and type. Examples of roles are: test, production, and customizing.	NVARCHAR	>
System Group, Role, Reporter	The role of the system group that the reporter system belongs to. All systems that belong to the same system group have the same system group ID and type. Examples of roles are: test, production, and customizing.	NVARCHAR	>
System Group, Role, Target	The role of the system group that the target system belongs to. All systems that belong to the same system group have the same system group ID and type. Examples of roles are: test, production, and customizing.	NVARCHAR	>
System Group, Type, Actor	The type of the system group that the actor system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, Type, Initiator	The type of the system group that the initiator system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, Type, Intermediary	The type of the system group that the intermediary system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, Type, Reporter	The type of the system group that the reporter system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>
System Group, Type, Target	The type of the system group that the target system belongs to. All systems that belong to the same system group have the same system group ID and type.	NVARCHAR	>

ETD Semantic Attributes – System (ctd.)

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

System ID, Actor	The ID of the actor system of the event, for example, SID/client ID for an ABAP system.	NVARCHAR
System ID, Initiator	The ID of the initiator system of the event, for example, SID/client ID for an ABAP system.	NVARCHAR
System ID, Intermediary	The ID of the intermediary system of the event, for example, SID/client ID for an ABAP system.	NVARCHAR
System ID, Reporter	The ID of the reporter system of the event, for example, SID/client ID for an ABAP system.	NVARCHAR
System ID, Target	The ID of the target system of the event, for example, SID/client ID for an ABAP system.	NVARCHAR
System Location, Actor	The location of the actor system as defined in the Locations application.	NVARCHAR
System Location, Initiator	The location of the initiator system as defined in the Locations application.	NVARCHAR
System Location, Intermediary	The location of the intermediary system as defined in the Locations application.	NVARCHAR
System Location, Reporter	The location of the reporter system as defined in the Locations application.	NVARCHAR
System Location, Target	The location of the target system as defined in the Locations application.	NVARCHAR
System Role, Actor	Role of the actor system, for example, test, production, customizing.	NVARCHAR
System Role, Initiator	Role of the initiator system, for example, test, production, customizing.	NVARCHAR
System Role, Intermediary	Role of the intermediary system, for example, test, production, customizing.	NVARCHAR
System Role, Reporter	Role of the reporter system, for example, test, production, customizing.	NVARCHAR
System Role, Target	Role of the target system, for example, test, production, customizing.	NVARCHAR
System Type, Actor	The type of the actor system, for example, ABAP.	NVARCHAR
System Type, Initiator	The type of the initiator system, for example, ABAP.	NVARCHAR
System Type, Intermediary	The type of the intermediary system, for example, ABAP.	NVARCHAR
System Type, Reporter	The type of the reporter system, for example, ABAP.	NVARCHAR
System Type, Target	The type of the target system, for example, ABAP.	NVARCHAR

ETD Semantic Attributes – Technical, Time



Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Technical Timestamp	The time at which the event was observed or reported as Unix time.	BIGINT
Technical, Group ID	Used to group events from the same log instance.	NVARCHAR
Technical, Log Collector, IP Address	The IP address of the streaming server that received the log instance.	NVARCHAR
Technical, Log Collector, Name	The name of the streaming server that received the log instance.	NVARCHAR
Technical, Log Collector, Port	The port on the streaming server that received the log instance.	NVARCHAR
Technical, Log Entry Type	The type of the log instance.	NVARCHAR
Technical, Number	A number used to check the consistency of the data in the system.	BIGINT
Technical, Number Range	A number range used to check the consistency of the data in the system.	NVARCHAR
Technical, Timestamp of Insertion	The time at which the event was inserted in the database.	TIMESTAMP
Time Duration	An extent of time, often of an action, or of time to perform all actions leading up to the event report. For example, time to process the HTTP request, including the processing of the response.	BIGINT
Timestamp	The time at which the event was observed or reported.	TIMESTAMP
Timestamp Of End	The time at which something ends, for example, an action.	TIMESTAMP
Timestamp Of Start	The time at which something starts, for example, an action.	TIMESTAMP

ETD Semantic Attributes – Trigger, User

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

Trigger Name, Acting	The name of the thing that triggered the event, and/or caused it to be logged, for example, things like timers, audit policies, security configurations, or attack signatures.	NVARCHAR
Trigger Name, Targeted	The name of the trigger that is the target of some action, for example, creation, modification, enablement, disablement, deletion, etc.	NVARCHAR
Trigger Type, Acting	The type of thing that triggered the event, and/or caused it to be logged, for example, things like timers, audit policies, security configurations, or attack signatures.	NVARCHAR
Trigger Type, Targeted	The type of a trigger that is the target of some action, for example, creation, modification, enablement, disablement, deletion, etc.	NVARCHAR
User Account Name, Acting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. A real user often has accounts in different domains (systems), for example, one real user may have two accounts:...	NVARCHAR
User Account Name, Initiating	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. A real user often has accounts in different domains (systems), for example, one real user may have two accounts:...	NVARCHAR
User Account Name, Targeted	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. A real user often has accounts in different domains (systems), for example, one real user may have two accounts:...	NVARCHAR
User Account Name, Targeting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. A real user often has accounts in different domains (systems), for example, one real user may have two accounts:...	NVARCHAR
User Group, Acting	For an ABAP system, this is the user group in user master maintenance. The acting user belongs to this group.	NVARCHAR
User Group, Targeted	For an ABAP system, this is the user group in user master maintenance. The targeted user belongs to this group.	NVARCHAR
User ID, Acting	The ID of the acting user involved in the event.	NVARCHAR
User ID, Initiating	The ID of the initiating user involved in the event.	NVARCHAR
User ID, Targeted	The ID of the targeted user involved in the event.	NVARCHAR
User ID, Targeting	The ID of the targeting user involved in the event.	NVARCHAR
User Logon Method	The method of the logon, that is how the user is authenticated.	NVARCHAR
User Pseudonym, Acting	The pseudonym of the acting user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off, etc.	NVARCHAR
User Pseudonym, Initiating	The pseudonym of the initiating user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off, etc.	NVARCHAR
User Pseudonym, Targeted	The pseudonym of the targeted user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off, etc.	NVARCHAR
User Pseudonym, Targeting	The pseudonym of the targeting user involved in the event. In many events an acting user and/or actor system performs an action on a targeted user. A targeted user may be the target of actions such as create, alter, delete, log on, log off, etc.	NVARCHAR
User Type, Acting	For an ABAP system, this is the user type in user master maintenance. The acting user is of this type. Type can take one of five values: dialog, system, communication, service, or reference. They are represented by the letters A(Dialog), B(System),...	NVARCHAR
User Type, Initiating	For an ABAP system, this is the user type in user master maintenance. The initiating user is of this type. Type can take one of five values: dialog, system, communication, service, or reference. They are represented by the letters A(Dialog), B(System),...	NVARCHAR
User Type, Targeted	For an ABAP system, this is the user type in user master maintenance. The targeted user is of this type. Type can take one of five values: dialog, system, communication, service, or reference. They are represented by the letters A(Dialog), B(System),...	NVARCHAR
User Type, Targeting	For an ABAP system, this is the user type in user master maintenance. The targeting user is of this type. Type can take one of five values: dialog, system, communication, service, or reference. They are represented by the letters A(Dialog), B(System),...	NVARCHAR

ETD Semantic Attributes – User (ctd.)

Standard Attribute, rather always filled
Attribute filled in special cases
Generic Attribute, often worth while looking

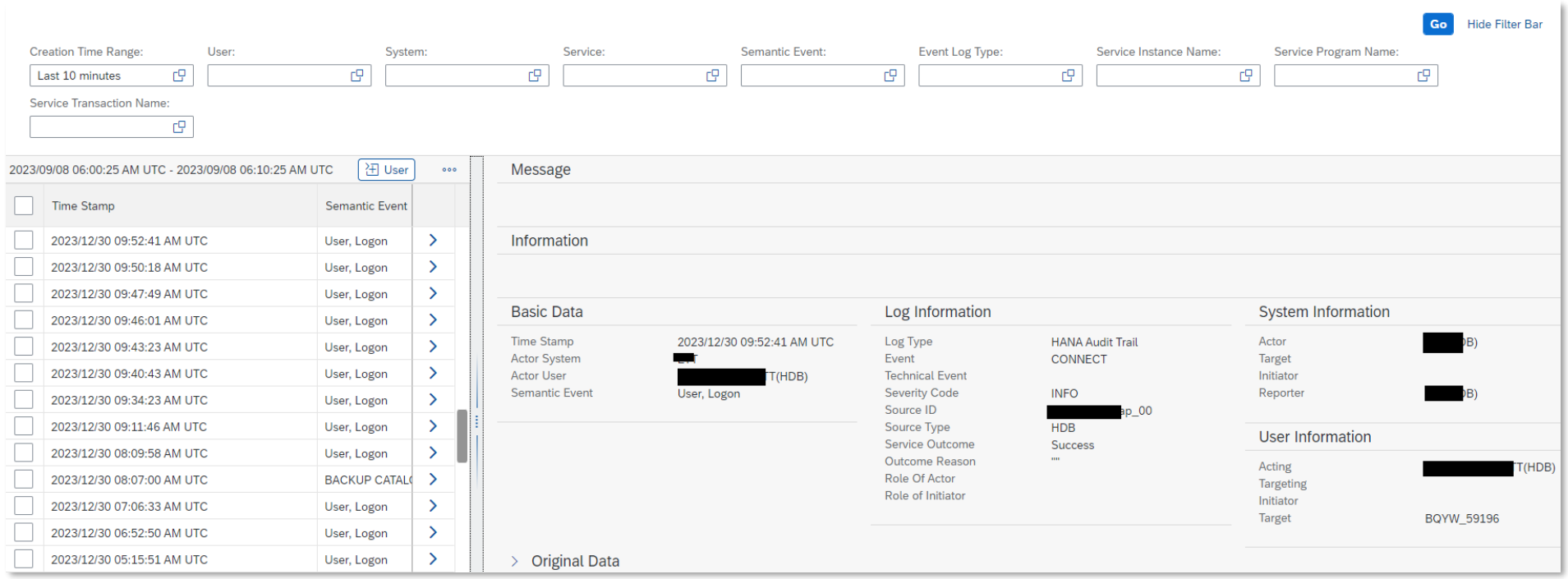
User, Floor, Acting	Floor of the building as more exact specification of the address of the acting user.	NVARCHAR
User, Function, Acting	Function of the acting user, for example, as contact person in a company. This is often part of the formatted address.	NVARCHAR
User, Room Number, Acting	Room number in the acting user's address.	NVARCHAR
Username, Acting	The Name of the acting user involved in the event.	NVARCHAR
Username, Domain Name, Acting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Name, Initiating	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Name, Targeted	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Name, Targeting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Type, Acting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Type, Initiating	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Type, Targeted	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Domain Type, Targeting	A user account is identified by a triple: 'User Account Name', 'Username Domain Type', and 'Username Domain Name'. The domain is the domain of validity of the user account name. It identifies the system that can resolve the user account name to a…	NVARCHAR
Username, Initiating	The Name of the initiating user involved in the event.	NVARCHAR
Username, Targeted	The Name of the targeted user involved in the event.	NVARCHAR
Username, Targeting	The Name of the targeting user involved in the event.	NVARCHAR

Examples: How to Use the Semantic Data Model

ETD Semantic Event Examples

Example 1: “User, Logon”

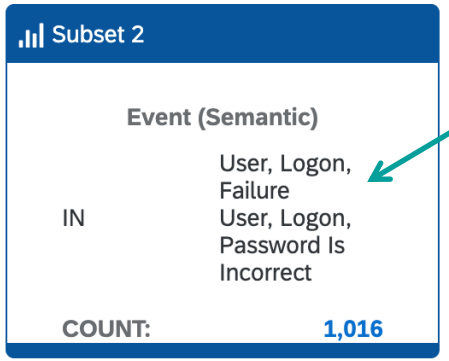
- Logon of a User in any System (e.g. S4/H system, HANA DB, BTP Application etc.)
- Coming out of different log types and systems (e.g. S4/H Security Audit Log, or HANA DB Audit Trail)
- Having different technical events (e.g. AU1 for S4/H, or CONNECT for HANA DB)

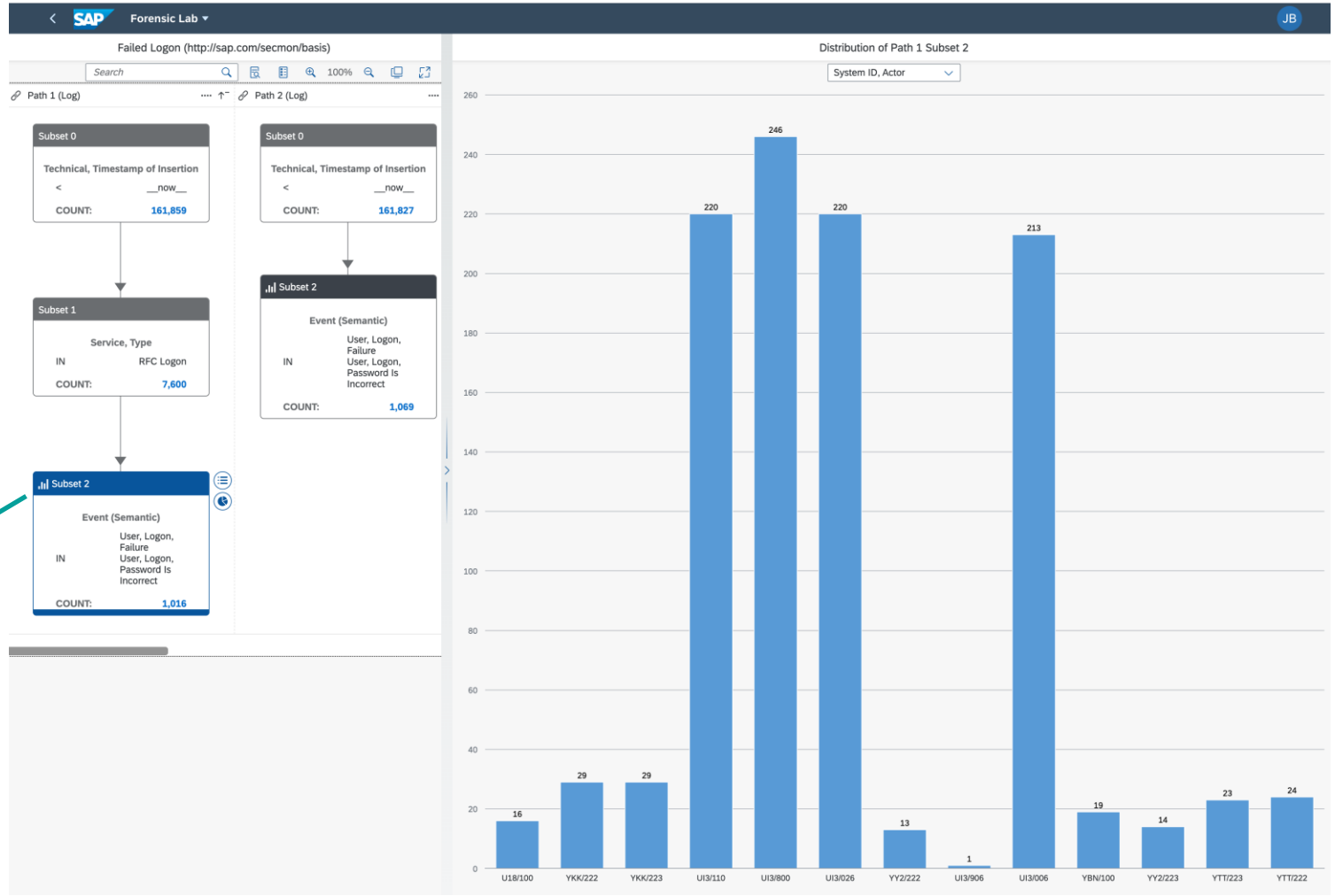


ETD Semantic Event Examples

Example: “User, Logon Failure – User, Logon, Password is incorrect”

- Failed Logon of a User in any System (e.g. S4/H system, HANA DB, BTP Application etc.)
- Coming out of different log types and systems (e.g. S4/H Security Audit Log, or HANA DB Audit Trail)

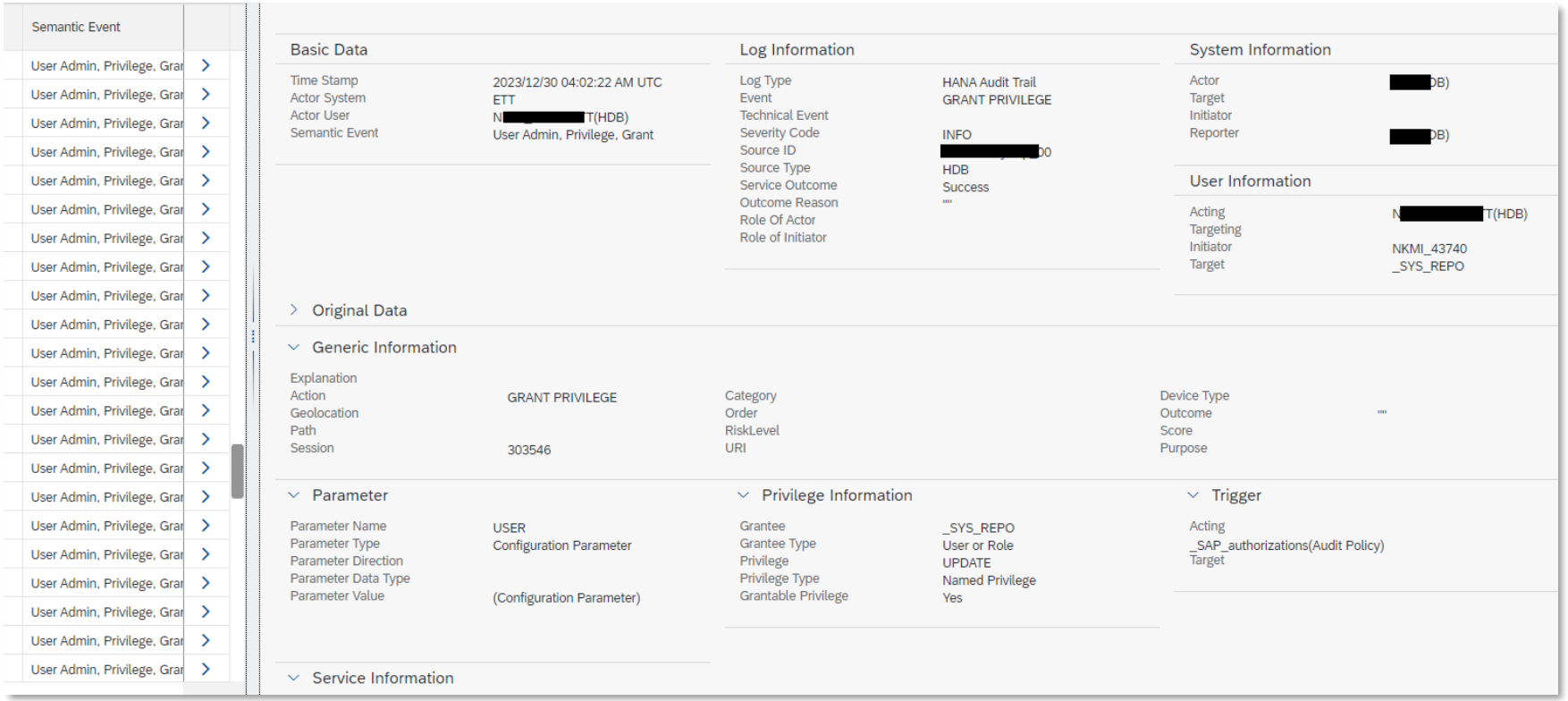




ETD Semantic Event Examples

Example 2: User Admin, Privilege, Grant

- Providing Roles/Authorizations to Users



Meta Data

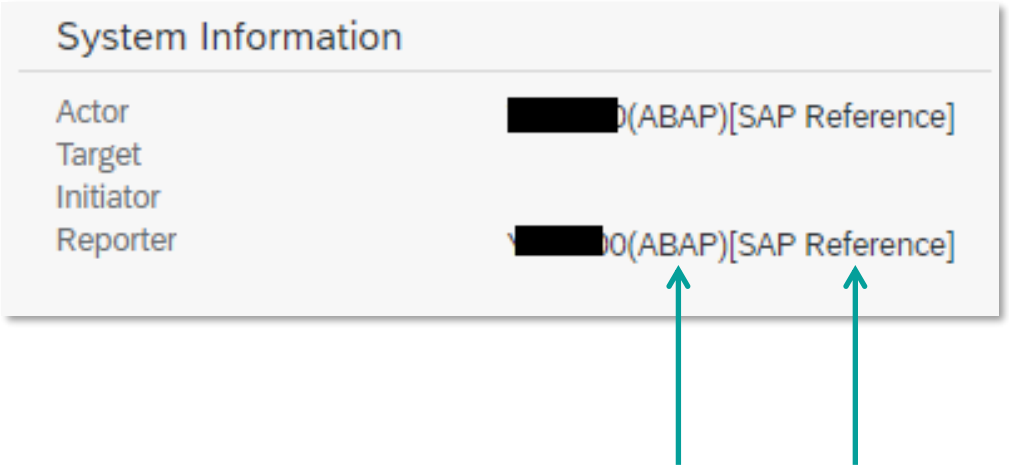
System Context Information
User Context Information
Pseudonymization

Context Information of Systems and Users

Example: Attributes System Type / System Role, Actor

- **Enriched System Context in Log Data via Meta Data Download**
  - System Role (Customizing, Training, Reference…)
  - System Type (ABAP, others, …)
  - System Group, Role (Test, Production, etc.)
  - System Group, Type (SAP, others)

- **Enriched User Context in Log Data via Meta Data Download**
  - User Name (pseudonymized)
  - User Group (ADMIN, DEVELOPER, etc.)
  - User Type (Technical, Dialog, etc.)
  - User Function (e.g. Batch Job User)
  - User Department



Thank you!

Contact information: SAP-ETD@sap.com

Michael Schmitt
m.schmitt@sap.com

Product Manager:
SAP Enterprise Threat Detection

Tobias Keller
tobias.keller@sap.com

Product / Partner Manager:
SAP Enterprise Threat Detection

Appendix: Additional Resources

- SAP CAS (Cloud Application Services) service description(s): https://www.sap.com/about/agreements/policies/cloud-service-specifications.html?sort=latest_desc&search=threat
- SAP Enterprise Threat Detection community pages: https://pages.community.sap.com/topics/enterprise-threat-detection
- SAP Enterprise Threat Detection, cloud edition partner portal pages: https://partneredge.sap.com/en/products/etd/about.html
- SAP Enterprise Threat Detection, Cloud Edition help pages: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_CLOUD_EDITION
- Documentation on the Log Collector: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_LOG_COLLECTOR
- Trouble shooting guide for Log Collector: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_LOG_COLLECTOR/db3fa475380b45d79813b390bf03deda/defa772dee3d4946814adf411bf8aa2c.html
- Link to complete List of Semantic Attributes including documentation & categorization: https://help.sap.com/docs/SAP_ENTERPRISE_THREAT_DETECTION_CLOUD_EDITION/91cfc1d15c81413aaef9efee05069772/4826e1873fbd4df3863b06018b9be9a4.html?q=Semantic
- Trouble shooting note: https://me.sap.com/notes/2790497