Secure the Intelligent Enterprise with SAP Enterprise Threat Detection

Exercise: Working with SAP Enterprise Threat Detection

Version TechEd 2023

Based on SAP Enterprise Threat Detection Version 2, Support Package 5

Run Simple

TABLE OF CONTENTS

ETD Demo Users

- Usernames: Demo01, …, Demo29: → You get your User ID in the room
- Password: Welcome0

In this exercise replace **<YOUR_USERNR>** with your user number:

- DEMO**01** → DEMO**ONE**
- DEMO**02** → DEMO**TWO**
- ….
- DEMO**10** → DEMO**TWENTYNINE**

Make use of the following pattern name for your own created content (Charts, Patterns, Value-Lists, etc.) in this session:

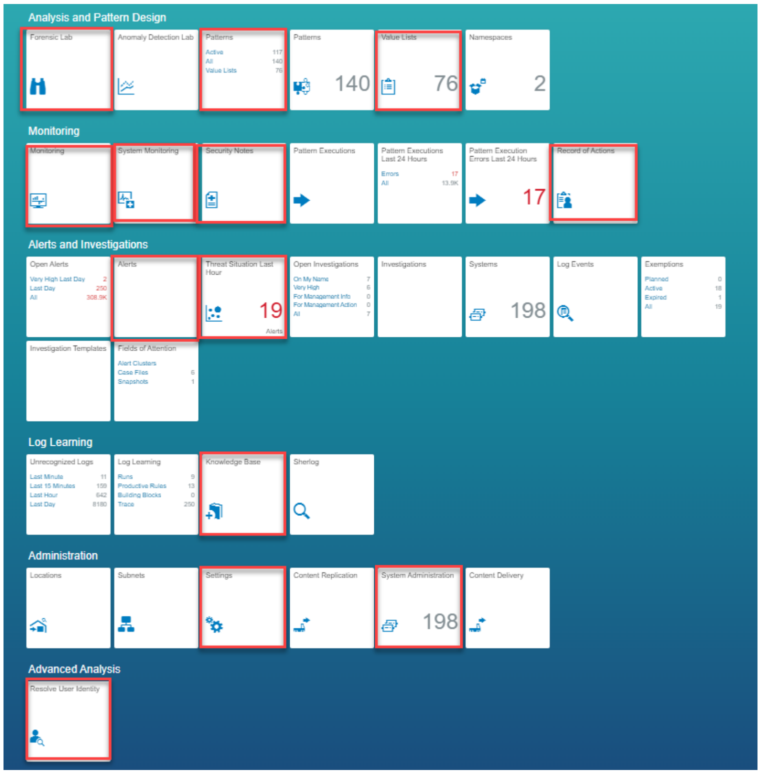
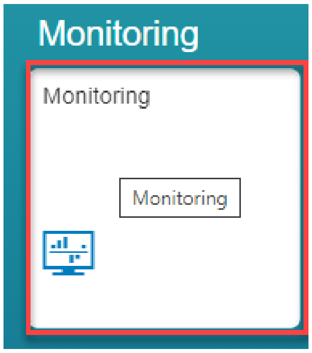
<Chart name> DEMO***<YOUR_USERNR>***

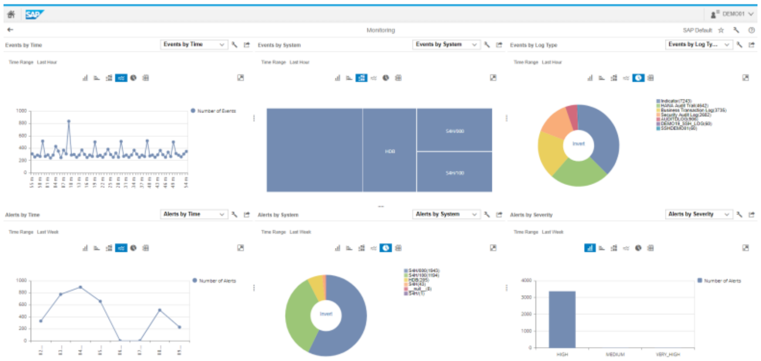
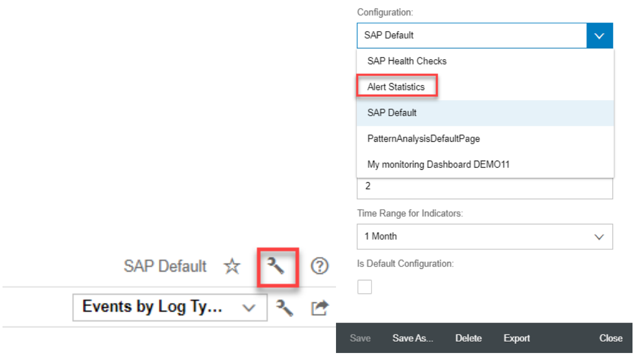
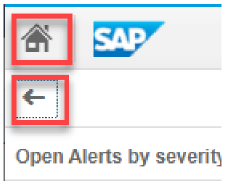
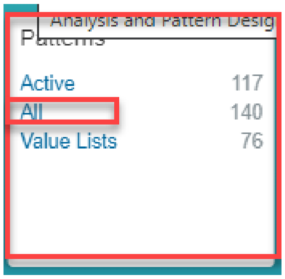
1. ETD USER – ETD ROUNDTRIP AND NAVIGATION

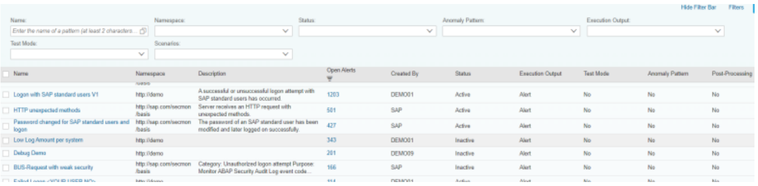
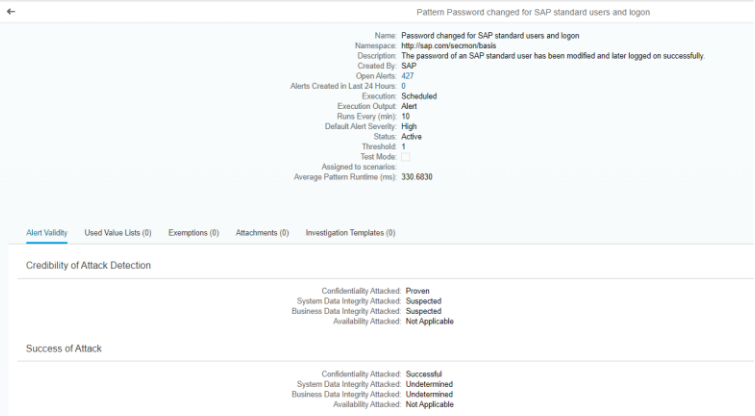
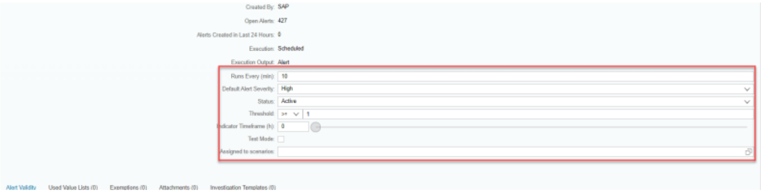
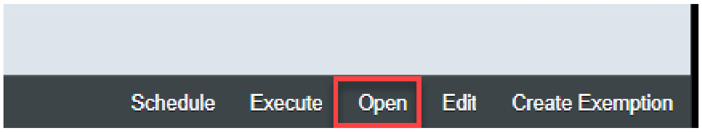
Tool Aspect: In this Exercise you as an ETD User will be able to navigate through the most important UIs of SAP Enterprise Threat Detection. You will get knowledge about different UIs like Monitoring, Alerts, Forensic Lab, Settings, (De-)Pseudonymization, Patterns, Value Lists, etc.

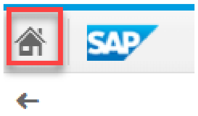
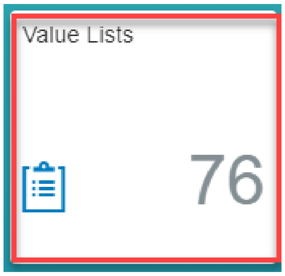
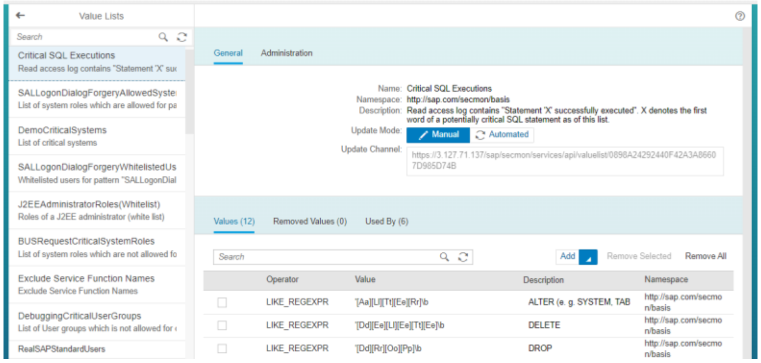
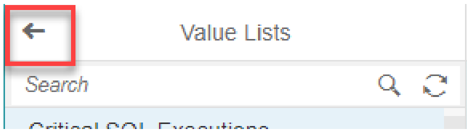
1.1. Start Page and Navigation to different tiles

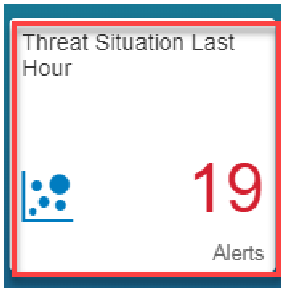
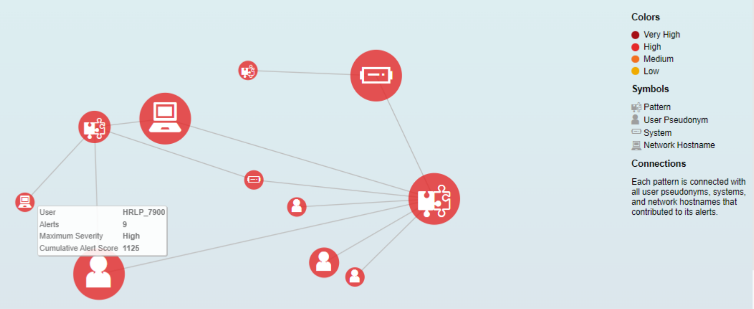
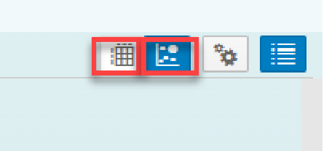
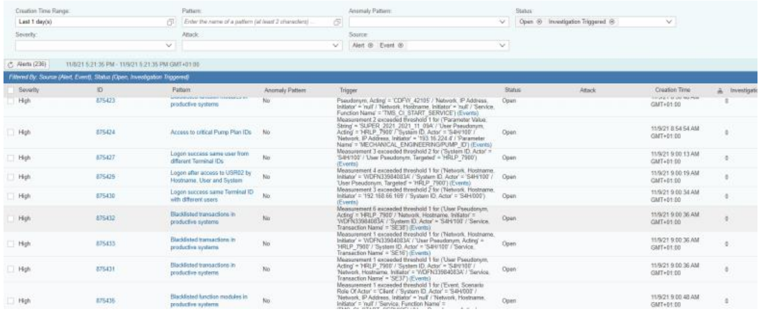
In this Exercise you will open the start page and click on several tiles to navigate forth and back

Explanation	Screenshot
1. After Logging on you are in the launch pad. In this exercise you will click on each of the red marked tiles to have a 1st look what's in there.	 Analysis and Pattern Design Forensic Lab Anomaly Detection Lab Patterns Active 117 All 140 Value Lists 76 Patterns 140 Value Lists 76 Namespaces 2 Monitoring Monitoring System Monitoring Security Notes Pattern Executions Pattern Executions Last 24 Hours Errors 17 All 13.9K Pattern Execution Errors Last 24 Hours 17 Record of Actions Alerts and Investigations Open Alerts Very High Last Day 2 Last Day 250 All 308.9K Alerts Threat Situation Last Hour 19 Alerts Open Investigations On My Name 7 Very High 6 For Management Info 0 For Management Action 0 All 7 Investigations Systems 198 Log Events Exemptions Planned 0 Active 18 Expired 1 All 19 Investigation Templates Fields of Attention Alert Clusters Case Files 6 Snapshots 1 Log Learning Unrecognized Logs Last Minute 11 Last 15 Minutes 159 Last Hour 642 Last Day 8180 Log Learning Runs 9 Productive Rules 13 Building Blocks 0 Trace 250 Knowledge Base Sherlog Administration Locations Subnets Settings Content Replication System Administration 198 Content Delivery Advanced Analysis Resolve User Identity
2. Click on Tile Monitoring	

Explanation	Screenshot
3. The Default Monitoring page will be shown	
4. Click on the small tool icon in the upper right corner and select another Monitoring page (e.g. Alert Statistics). Another Monitoring page will be shown. In a later exercise you will learn how to create own monitoring pages with own charts.	 Configuration: SAP Default SAP Health Checks Alert Statistics SAP Default PatternAnalysisDefaultPage My monitoring Dashboard DEMO11 2 Time Range for Indicators: 1 Month Is Default Configuration: SAP Default Events by Log Ty... Save Save As... Delete Export Close
5. Jump back to the launch pad via using upper left arrow or the home button.	
6. In Tile Patterns, Click on the link 'All' or 'Active'.	 Analysis and Pattern Desig Patterns Active 117 All 140 Value Lists 76

Explanation	Screenshot
7. You see the list of the patterns, with their current state, and how many alerts they raised.	 Hide Filter Bar Filters Name: Enter the name of a pattern (at least 2 characters... Namespace: Status: Anomaly Pattern: Execution Output: Test Mode: Scenarios: Name / Namespace / Description / Open Alerts / Created By / Status / Execution Output / Test Mode / Anomaly Pattern / Post-Processing Logon with SAP standard users V1 / http://demo / A successful or unsuccessful logon attempt with SAP standard users has occurred. / 1203 / DEMO01 / Active / Alert / No / No / No HTTP unexpected methods / http://sap.com/secmon/basis / Server receives an HTTP request with unexpected methods. / 501 / SAP / Active / Alert / No / No / No Password changed for SAP standard users and logon / http://sap.com/secmon/basis / The password of an SAP standard user has been modified and later logged on successfully. / 427 / SAP / Active / Alert / No / No / No Low Log Amount per system / http://demo / / 343 / DEMO01 / Inactive / Alert / No / No / No Debug Demo / http://demo / / 201 / DEMO09 / Inactive / Alert / No / No / No BUS-Request with weak security / http://sap.com/secmon/basis / Category: Unauthorized logon attempt Purpose: Monitor ABAP Security Audit Log event code... / 166 / SAP / Inactive / Alert / No / No / No Failed Logon <YOUR USER NO> / http://demo / / 114 / DEMO01 / Active / Alert / No / No / No
8. You can jump to the details of any pattern, by clicking on the pattern name in the list.	 Pattern Password changed for SAP standard users and logon Name: Password changed for SAP standard users and logon Namespace: http://sap.com/secmon/basis Description: The password of an SAP standard user has been modified and later logged on successfully. Created By: SAP Open Alerts: 427 Alerts Created in Last 24 Hours: 0 Execution: Scheduled Execution Output: Alert Runs Every (min): 10 Default Alert Severity: High Status: Active Threshold: 1 Test Mode: □ Assigned to scenarios: Average Pattern Runtime (ms): 330.6830 Alert Validity Used Value Lists (0) Exemptions (0) Attachments (0) Investigation Templates (0) Credibility of Attack Detection Confidentiality Attacked: Proven System Data Integrity Attacked: Suspected Business Data Integrity Attacked: Suspected Availability Attacked: Not Applicable Success of Attack Confidentiality Attacked: Successful System Data Integrity Attacked: Undetermined Business Data Integrity Attacked: Undetermined Availability Attacked: Not Applicable
9. When clicking on 'Edit', some parameter of the pattern can be changed, e.g.: a. Run frequency b. Severity c. Status (Active/Inactive) d. Threshold e. Test Mode Checkbox You can save via using the 'Save' button	 Created By: SAP Open Alerts: 427 Alerts Created in Last 24 Hours: 0 Execution: Scheduled Execution Output: Alert Runs Every (min): 10 Default Alert Severity: High Status: Active Threshold: >= 1 Indicator Timeframe (h): 0 Test Mode: □ Assigned to scenarios: Alert Validity Used Value Lists (0) Exemptions (0) Attachments (0) Investigation Templates (0)
10. When clicking on the 'Open' Button, the Forensic Lab opens and you can see the modeling of the patterns, as it is delivered by SAP. The Forensic Lab will be explained in a separate part of this exercise, and in other exercises about modeling own use cases.	

Explanation	Screenshot
11. Click the Home button to jump back to the launch pad.	
12. Klick on Tile 'Value Lists'	 Value Lists 76
13. You see the list containing all value lists. A value list can act as a block-list or as an allow list. They are used as filter elements in patterns, all list entries are used to filter based on these value list entries in an inclusive or exclusive way. Value lists can automatedly updated from outside via a rest endpoint, if Checkbox 'Automated' is switched on. Values can be added by customers ('Add'), or SAP delivered values can be removed ('Remove Selected'). The changes to standard value lists are not overwritten by updates.	 Value Lists Search Critical SQL Executions Read access log contains "Statement 'X' suc SALLogonDialogForgeryAllowedSyste List of system roles which are allowed for pa DemoCriticalSystems List of critical systems SALLogonDialogForgeryWhitelistedUs Whitelisted users for pattern "SALLogonDial J2EEAdministratorRoles(Whitelist) Roles of a J2EE administrator (white list) BUSRequestCriticalSystemRoles List of system roles which are not allowed fo Exclude Service Function Names Exclude Service Function Names DebuggingCriticalUserGroups List of User groups which is not allowed for RealSAPStandardUsers General Administration Name: Critical SQL Executions Namespace: http://sap.com/secmon/basis Description: Read access log contains "Statement 'X' successfully executed". X denotes the first word of a potentially critical SQL statement as of this list. Update Mode: Manual Automated Update Channel: https://3.127.71.137/sap/secmon/services/api/valuelist/0898A24292440F42A3A8660 7D985D74B Values (12) Removed Values (0) Used By (6) Search Add Remove Selected Remove All Operator / Value / Description / Namespace □ LIKE_REGEXPR / '[Aa][Ll][Tt][Ee][Rr]\b / ALTER (e. g. SYSTEM, TAB / http://sap.com/secmon/basis □ LIKE_REGEXPR / '[Dd][Ee][Ll][Ee][Tt][Ee]\b / DELETE / http://sap.com/secmon/basis □ LIKE_REGEXPR / '[Dd][Rr][Oo][Pp]\b / DROP / http://sap.com/secmon/basis
14. Go back to launch pad via the left arrow	 Value Lists Search Critical SQL Executions

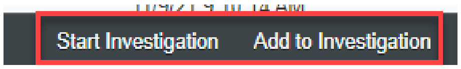
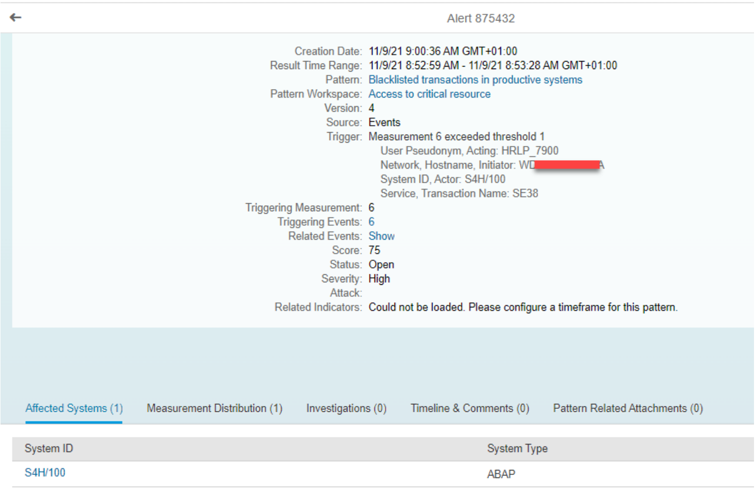
Explanation	Screenshot
15. Klick on Tile ‘Threat Situation Last Hour’.	
16. The UI shows the correlation between Users, Systems, Patterns, Alerts, End User Machine Hostnames. The bigger a circle, the more an entity is involved into the correlations. E.g. in the Screenshot the User Pseudonym HRLP_7900 is involved in 9 different Alerts, based on two patterns. By that it can be easily found out where there are hot spots of Alerts, Suspicious Activities or cyber Attacks correspondingly. By hovering over an Alert, you can as well jump to the detailed Alert list	User HRLP_7900 Alerts 9 Maximum Severity High Cumulative Alert Score 1125 Colors ● Very High ● High ● Medium ● Low Symbols Pattern User Pseudonym System Network Hostname Connections Each pattern is connected with all user pseudonyms, systems, and network hostnames that contributed to its alerts.
17. You can toggle between the Threat Situation graphical view and the detailed Alert list by clicking on the list button (and back from the list)	
18. In the alert list, you can see all single alerts with already some alert triggering information in the column ‘Trigger’. From here you can jump to: a. The Alert itself, with more detailed descriptions. b. The Pattern description, as you find it in the Tile ‘Patterns’ c. The triggering Events, when clicking on the Link ‘Events’ in the ‘Trigger’ Description. This is as well possible from the opened single alert	

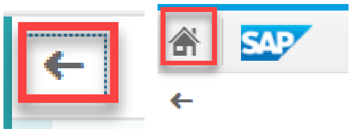
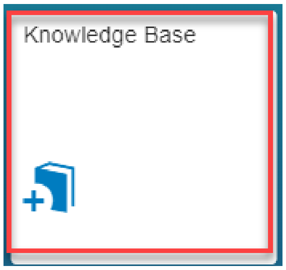
Creation Time Range: Last 1 day(s)
Pattern: Enter the name of a pattern (at least 2 characters) ...
Anomaly Pattern:
Status: Open ⊗ Investigation Triggered ⊗
Severity:
Attack:
Source: Alert ⊗ Event ⊗

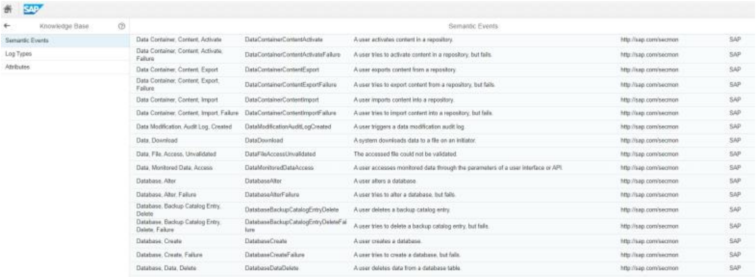
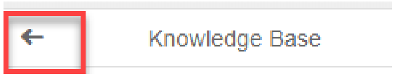
Alerts (236) 11/8/21 5:21:35 PM - 11/9/21 5:21:35 PM GMT+01:00

Filtered By: Source (Alert, Event), Status (Open, Investigation Triggered)

Severity	ID	Pattern	Anomaly Pattern	Trigger	Status	Attack	Creation Time	Investigati
High	875423	productive systems	No	Pseudonym, Acting' = 'CDFW_42105' / 'Network, IP Address, Initiator' = 'null' / 'Network, Hostname, Initiator' = 'null' / 'Service, Function Name' = 'TMS_CI_START_SERVICE') (Events)	Open		GMT+01:00	0
High	875424	Access to critical Pump Plan IDs	No	Measurement 2 exceeded threshold 1 for ('Parameter Value, String' = 'SUPER_2021_2021_11_09A' / 'User Pseudonym, Acting' = 'HRLP_7900' / 'System ID, Actor' = 'S4H/100' / 'Network, IP Address, Initiator' = '193.16.224.4' / 'Parameter Name' = 'MECHANICAL_ENGINEERING/PUMP_ID') (Events)	Open		11/9/21 8:54:54 AM GMT+01:00	0
High	875427	Logon success same user from different Terminal IDs	No	Measurement 3 exceeded threshold 2 for ('System ID, Actor' = 'S4H/100' / 'User Pseudonym, Targeted' = 'HRLP_7900') (Events)	Open		11/9/21 9:00:13 AM GMT+01:00	0
High	875429	Logon after access to USR02 by Hostname, User and System	No	Measurement 4 exceeded threshold 1 for ('Network, Hostname, Initiator' = 'WDFN33984083A' / 'System ID, Actor' = 'S4H/100' / 'User Pseudonym, Targeted' = 'HRLP_7900') (Events)	Open		11/9/21 9:00:19 AM GMT+01:00	0
High	875430	Logon success same Terminal ID with different users	No	Measurement 3 exceeded threshold 2 for ('Network, Hostname, Initiator' = '192.168.66.169' / 'System ID, Actor' = 'S4H/000') (Events)	Open		11/9/21 9:00:34 AM GMT+01:00	0
High	875432	Blacklisted transactions in productive systems	No	Measurement 6 exceeded threshold 1 for ('User Pseudonym, Acting' = 'HRLP_7900' / 'Network, Hostname, Initiator' = 'WDFN33984083A' / 'System ID, Actor' = 'S4H/100' / 'Service, Transaction Name' = 'SE38') (Events)	Open		11/9/21 9:00:36 AM GMT+01:00	0
High	875433	Blacklisted transactions in productive systems	No	Measurement 1 exceeded threshold 1 for ('Network, Hostname, Initiator' = 'WDFN33984083A' / 'User Pseudonym, Acting' = 'HRLP_7900' / 'System ID, Actor' = 'S4H/100' / 'Service, Transaction Name' = 'SE16') (Events)	Open		11/9/21 9:00:36 AM GMT+01:00	0
High	875431	Blacklisted transactions in productive systems	No	Measurement 1 exceeded threshold 1 for ('User Pseudonym, Acting' = 'HRLP_7900' / 'System ID, Actor' = 'S4H/100' / 'Network, Hostname, Initiator' = 'WDFN33984083A' / 'Service, Transaction Name' = 'SE37') (Events)	Open		11/9/21 9:00:36 AM GMT+01:00	0
High	875435	Blacklisted function modules in productive systems	No	Measurement 1 exceeded threshold 1 for ('Event, Scenario Role Of Actor' = 'Client' / 'System ID, Actor' = 'S4H/000' / 'Network, IP Address, Initiator' = 'null' / 'Network, Hostname, Initiator' = 'null' / 'Service, Function Name' =	Open		11/9/21 9:00:48 AM GMT+01:00	0

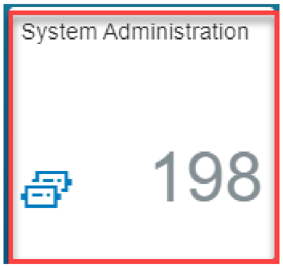
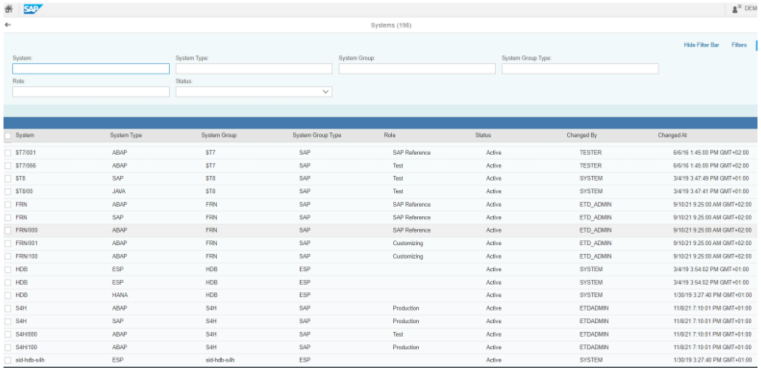
Explanation	Screenshot
19. In order to process alerts, you can mark several alerts belonging together (i.e. having the same root cause) and start an investigation (or add to an existing investigation). An investigation is the evidence collection object in ETD. It will be used for collecting all corelated alerts, screenshots, documents, single logs, snapshots, etc., and finally provide a state and potential resolvement. Alert and investigation handling is a separate exercise.	
20. Click on one of the Alert IDs to jump to the Alert details. From here you can jump to: a. the pattern definition b. the pattern workspace in the forensic lab. The time frame then filters automatically to the time when the alert was raised, so you can see the log events at time of the raising of the alert. Forensic Lab will be part of another exercise c. the triggering events, so you can see the detailed normalized and original log data that was analyzed to raise the alert. Alert handling is part of another excercise d. the related events, by filtering on the alert raising time frame, and different available correlating attributes (e.g. user, system ,…) Additionally you can see the Severity (Low, Medium, High, Very High) and a Score. The Pattern related default severity can be automatedly raised if the system is a critical system related to confidentiality, integrity and availability. The Score multiplies the pattern criticality (related to confidentiality, integrity and availability) with the system criticality related to attacks against confidentiality, integrity and availability. It can vary between 0 and 100.	Alert 875432 Creation Date: 11/9/21 9:00:36 AM GMT+01:00 Result Time Range: 11/9/21 8:52:59 AM - 11/9/21 8:53:28 AM GMT+01:00 Pattern: Blacklisted transactions in productive systems Pattern Workspace: Access to critical resource Version: 4 Source: Events Trigger: Measurement 6 exceeded threshold 1 User Pseudonym, Acting: HRLP_7900 Network, Hostname, Initiator: WD[redacted]A System ID, Actor: S4H/100 Service, Transaction Name: SE38 Triggering Measurement: 6 Triggering Events: 6 Related Events: Show Score: 75 Status: Open Severity: High Attack: Related Indicators: Could not be loaded. Please configure a timeframe for this pattern. Affected Systems (1) Measurement Distribution (1) Investigations (0) Timeline & Comments (0) Pattern Related Attachments (0) System ID — System Type S4H/100 — ABAP

Explanation	Screenshot
21. Go back to the Alert list by clicking on the ‘back’ arrow. Then go back to the launch pad by clicking again to the ‘back’ arrow or to the home-button	
22. Click on Tile ‘Knowledge Base’.	

Explanation	Screenshot
23. You can choose between 3 lists. The list of ‘Semantic Events’ shows all events in a human understandable wording and with a short explanation. The semantic events are very often translations from a technical event ID. E.g. the technical Event AU1 from a SAP Security Audit Log is translated to User, Logon. The semantic events are used in the forensic lab to be filtered on. Additional semantic events can be created by customers to be used when ingesting own log data, that needs to be normalized (learned) The list of ‘Attributes’ shows all normalized attributes in the Event Database table with Display Name, short description and data type. Via each of these attributes a correlation and filtering on events is possible within the forensic lab. Each of the attributes can be previewed in the forensic lab with the different scatterings/value distributions. **Information:** Very often the Attributes are shown in different roles. E.g, a user acting, and a user targeted. An acting user can e.g. provide additional roles to a targeted user. Both users are then part of the same log event, in their different roles. The list of ‘Log Types’ shows all supported log types with short names and descriptions. The log types are either the ones that are supported out of the box or that were created there for usage in the log learning tool, if ingesting own log data.	
24. Go back to the launch pad via the back arrow.	

Semantic Events

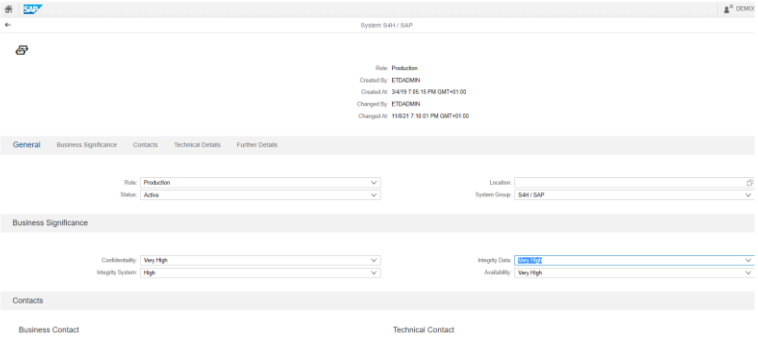
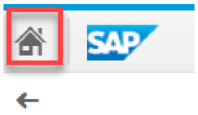
Data Container, Content, Activate	DataContainerContentActivate	A user activates content in a repository.	http://sap.com/secmon	SAP
Data Container, Content, Activate, Failure	DataContainerContentActivateFailure	A user tries to activate content in a repository, but fails.	http://sap.com/secmon	SAP
Data Container, Content, Export	DataContainerContentExport	A user exports content from a repository.	http://sap.com/secmon	SAP
Data Container, Content, Export, Failure	DataContainerContentExportFailure	A user tries to export content from a repository, but fails.	http://sap.com/secmon	SAP
Data Container, Content, Import	DataContainerContentImport	A user imports content into a repository.	http://sap.com/secmon	SAP
Data Container, Content, Import, Failure	DataContainerContentImportFailure	A user tries to import content into a repository, but fails.	http://sap.com/secmon	SAP
Data Modification, Audit Log, Created	DataModificationAuditLogCreated	A user triggers a data modification audit log.	http://sap.com/secmon	SAP
Data, Download	DataDownload	A system downloads data to a file on an initiator.	http://sap.com/secmon	SAP
Data, File, Access, Unvalidated	DataFileAccessUnvalidated	The accessed file could not be validated.	http://sap.com/secmon	SAP
Data, Monitored Data, Access	DataMonitoredDataAccess	A user accesses monitored data through the parameters of a user interface or API.	http://sap.com/secmon	SAP
Database, Alter	DatabaseAlter	A user alters a database.	http://sap.com/secmon	SAP
Database, Alter, Failure	DatabaseAlterFailure	A user tries to alter a database, but fails.	http://sap.com/secmon	SAP
Database, Backup Catalog Entry, Delete	DatabaseBackupCatalogEntryDelete	A user deletes a backup catalog entry.	http://sap.com/secmon	SAP
Database, Backup Catalog Entry, Delete, Failure	DatabaseBackupCatalogEntryDeleteFailure	A user tries to delete a backup catalog entry, but fails.	http://sap.com/secmon	SAP
Database, Create	DatabaseCreate	A user creates a database.	http://sap.com/secmon	SAP
Database, Create, Failure	DatabaseCreateFailure	A user tries to create a database, but fails.	http://sap.com/secmon	SAP
Database, Data, Delete	DatabaseDataDelete	A user deletes data from a database table.	http://sap.com/secmon	SAP

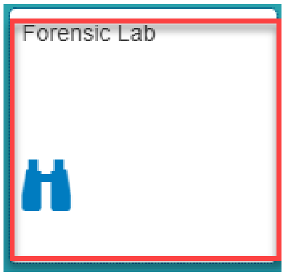
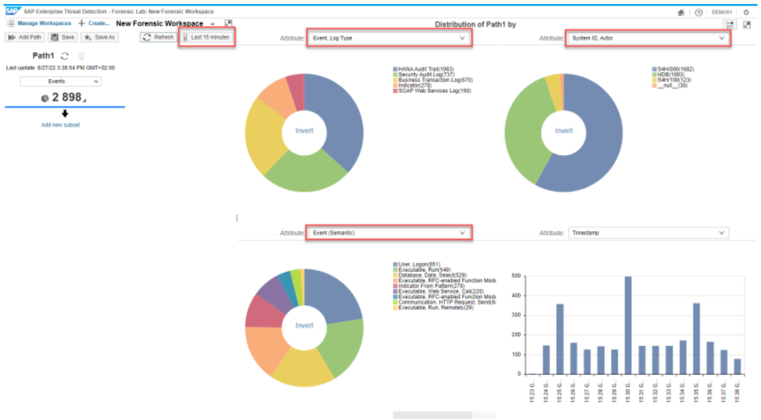
Explanation	Screenshot
25. Klick on Tile ‘System Administration’	
26. You see a list of systems with some major attributes.	

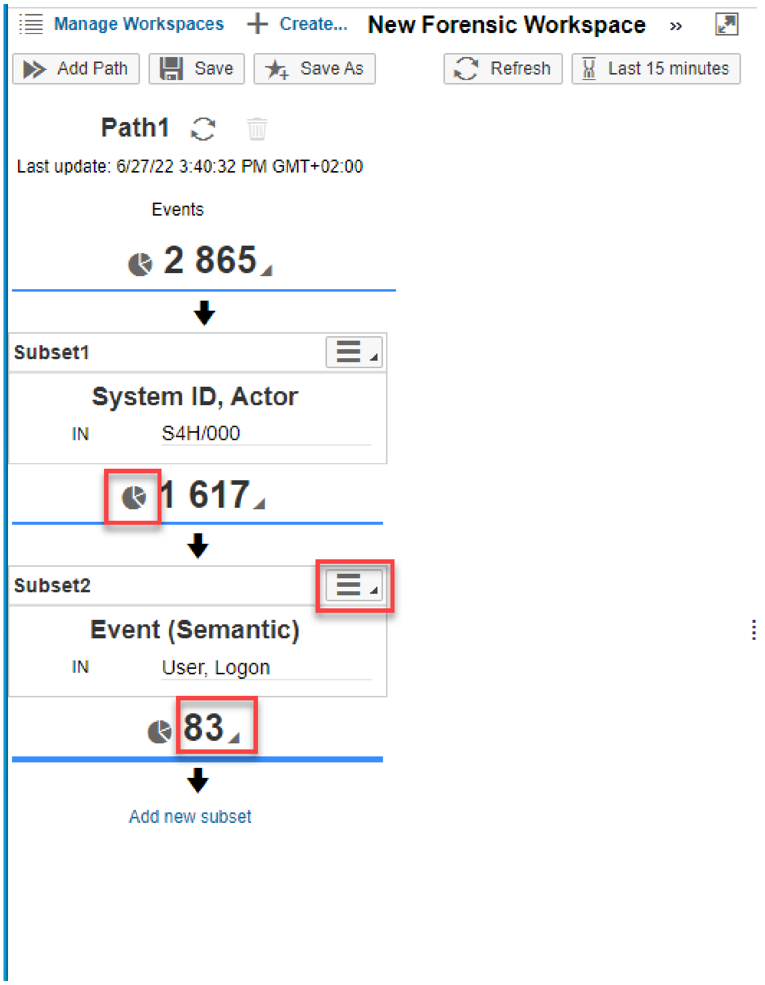
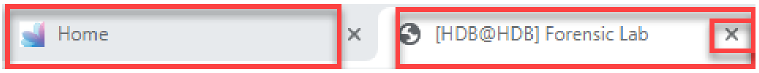
Systems (198)

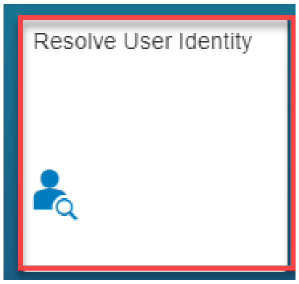
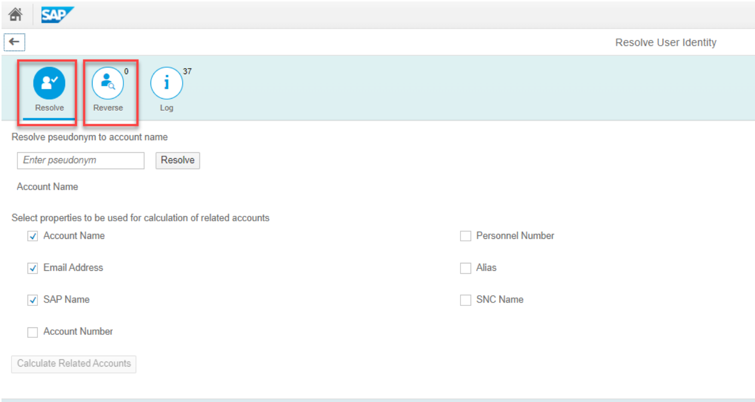
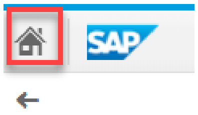
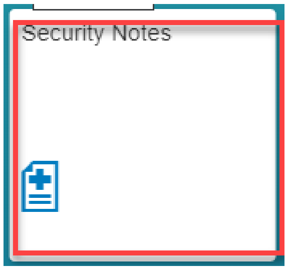
System:
System Type:
System Group:
System Group Type:
Role:
Status:

System	System Type	System Group	System Group Type	Role	Status	Changed By	Changed At
$T7/001	ABAP	$T7	SAP	SAP Reference	Active	TESTER	6/6/16 1:45:00 PM GMT+02:00
$T7/066	ABAP	$T7	SAP	Test	Active	TESTER	6/6/16 1:45:00 PM GMT+02:00
$T8	SAP	$T8	SAP	Test	Active	SYSTEM	3/4/19 3:47:49 PM GMT+01:00
$T8/00	JAVA	$T8	SAP	Test	Active	SYSTEM	3/4/19 3:47:41 PM GMT+01:00
FRN	ABAP	FRN	SAP	SAP Reference	Active	ETD_ADMIN	9/10/21 9:25:00 AM GMT+02:00
FRN	SAP	FRN	SAP	SAP Reference	Active	ETD_ADMIN	9/10/21 9:25:00 AM GMT+02:00
FRN/000	ABAP	FRN	SAP	SAP Reference	Active	ETD_ADMIN	9/10/21 9:25:00 AM GMT+02:00
FRN/001	ABAP	FRN	SAP	Customizing	Active	ETD_ADMIN	9/10/21 9:25:00 AM GMT+02:00
FRN/100	ABAP	FRN	SAP	Customizing	Active	ETD_ADMIN	9/10/21 9:25:00 AM GMT+02:00
HDB	ESP	HDB	ESP		Active	SYSTEM	3/4/19 3:54:02 PM GMT+01:00
HDB	ESP	HDB	ESP		Active	SYSTEM	3/4/19 3:54:02 PM GMT+01:00
HDB	HANA	HDB	ESP		Active	SYSTEM	1/30/19 3:27:40 PM GMT+01:00
S4H	ABAP	S4H	SAP	Production	Active	ETDADMIN	11/8/21 7:10:01 PM GMT+01:00
S4H	SAP	S4H	SAP	Production	Active	ETDADMIN	11/8/21 7:10:01 PM GMT+01:00
S4H/000	ABAP	S4H	SAP	Test	Active	ETDADMIN	11/8/21 7:10:01 PM GMT+01:00
S4H/100	ABAP	S4H	SAP	Production	Active	ETDADMIN	11/8/21 7:10:01 PM GMT+01:00
sid-hdb-s4h	ESP	sid-hdb-s4h	ESP		Active	SYSTEM	1/30/19 3:27:40 PM GMT+01:00

Explanation	Screenshot
27. Click on any of the lines to see the details. Some of the entries are filled from Meta data arriving from SAP Application Server ABAP Systems: • Role (e.g. Production, Test, …) • System Group • Database Host, Type, Version • Application Servers for the System Group Other entries can be maintained manually: • Business Significance with regards to Confidentiality, Integrity and Availability of the system. **These attributes are multiplied out with the corresponding pattern attributes for Confidentiality, Integrity and Availability** (see extra exercise) **and determine the raise of an Alert Severity as well as the Alert Score!** • Location • Contact Persons • Organizational information (Names, LOB, phone number, mail address) • Status (Active/Inactive) • Landscape Information **Information**: We distinguish between System Integrity and Data Integrity. System Integrity describes the integrity of SAP Basis (e.g. Use cases related to manipulation of system configurations, Security settings, debugging, etc.), Data integrity describes the integrity of Business Data (Manipulation of Business data, spy out of Data Privacy relevant data, etc.) **Information**: The system meta data attributes can be partly used in the forensic lab to model patterns (e.g. System Type, System Role, System Location, System ID, System Group ID)	 System S4H / SAP Role: Production Created By: ETDADMIN Created At: 3/4/19 7:05:15 PM GMT+01:00 Changed By: ETDADMIN Changed At: 11/8/21 7:10:01 PM GMT+01:00 General · Business Significance · Contacts · Technical Details · Further Details Role: Production Status: Active Location: System Group: S4H / SAP Business Significance Confidentiality: Very High Integrity System: High Integrity Data: Very High Availability: Very High Contacts Business Contact Technical Contact
28. Use the Home button to jump back to the launch pad	

Explanation	Screenshot
29. Click on Tile ‘Forensic Lab’	
30. In the UI you can see a filtering area on the left side and a preview area on the right side (Pie Charts). In the forensic lab you can do analysis, correlation over all the log data, semantic attributes, semantic events over shorter or longer time frames. It can be used e.g. for User and System Behavior Analysis and Threat Hunting. Here you can as well define own charts and patterns (as SAP does it) and save them in a ‘Forensic Workspace’. When starting up, it shows: • Log data having arrived the last 15 minutes (can be changed to any other time frame) • In the upper left pie chart: Log types having arrives in that time frame • In the lower left pie chart: Semantic events which were contained in the incoming log data • In the upper right pie chart: System IDs, from which data arrived (as far as the log provides the information) The creation of charts, patterns, workspaces is part of additional exercises.	

Explanation	Screenshot
31. The basic navigation in the forensic lab is described below. Click on the drop down box above any of the pie charts. You see all the ~180 semantic attributes which are available (→ see Knowledge Base) and might be filled with values. Select e.g. 'Service, Program Name'. Then you see in the preview all the programs (in general SAP system executable reports) which were called within the time frame, coming out from different logs. Click on any of the values in the list or within a pie chart (e.g. a certain System ID, Actor), and in the context menu, click 'Add to Path'. The filter path gets a new filter subset, and all information is now filtered according to this subset. Click on another Attribute value (e.g. a certain semantic Event and 'Add to Path'. Then you see two filter subsets, and all data is filtered according to these two subsets. You can jump between the different filter subset results by clicking on the small pie chart at each subset. You can edit the filter conditions by clicking on the small rectangle upper right in each subset You can create charts and patterns, look at normalized and original data, use the logs in a 'Case File' (separate exercise later), by clicking on the number under the subset, and opening a context menu.	 Manage Workspaces · Create... · New Forensic Workspace Add Path · Save · Save As · Refresh · Last 15 minutes Path1 Last update: 6/27/22 3:40:32 PM GMT+02:00 Events 2 865 Subset1 System ID, Actor IN S4H/000 1 617 Subset2 Event (Semantic) IN User, Logon 83 Add new subset
32. The forensic lab opens as an extra browser tab, you can close it in the browser, and jump back to the launch pad browser tab.	 Home × [HDB@HDB] Forensic Lab ×

Explanation	Screenshot
33. Click on Tile ‘Resolve User Identity’	
34. In the UI you can enter a user Pseudonym, as you saw it e.g. within Alert data, or in the forensic lab You can/should resolve a pseudonym, especially if a suspicious activity was finally determined or acknowledged by the security analyst. If there is the need to do e.g. an ad’hoc analysis for a user, a reverse resolution (UserID → Pseudonym) can be done, and then even a jump to the forensic lab can be done from within the reverse resolution, prefiltered to the different roles (Acting, Targeted, …) of the user id. Information: A special Authorization/Role is needed to do the resolution. A 4-eyes principle or special resolution policy can hence be established. (De-) Pseudonymization is part of another exercise.	Resolve User Identity Resolve · Reverse 0 · Log 37 Resolve pseudonym to account name *Enter pseudonym* Resolve Account Name Select properties to be used for calculation of related accounts ☑ Account Name ☐ Personnel Number ☑ Email Address ☐ Alias ☑ SAP Name ☐ SNC Name ☐ Account Number Calculate Related Accounts
35. Jump back to launch pad by using the home button.	
36. Click on Tile ‘Security Notes’	

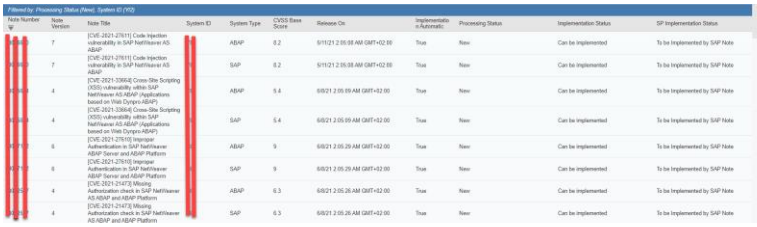
<table>
<tr><th>Explanation</th><th>Screenshot</th></tr>
<tr><td>

37. If the corresponding meta data transfer is set up in the Source SAP Application Server ABAP Systems, the UI provides an overview about available and relevant security notes and the patch state of the systems related to these notes.

It shows if a note is relevant for a certain system (or not), By Clicking on e.g. the CVSS Base Score Column, a sorting is possible, and an overview can be provided related to the most important Security notes. The filtering allows as well to find out if e.g. a certain note is relevant for a certain system, etc.

This functionality as such can be as well provided by other tools from SAP and partners, it is just a precondition for the 'Patch Risk Score' shown in 'System Monitoring', together with a 'Business Attack Score' and a 'Business Risk Score'.

</td><td>



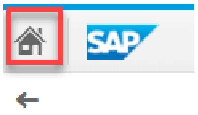
Filtered by: Processing Status (New), System ID (YI2)

<table>
<tr><th>Note Number</th><th>Note Version</th><th>Note Title</th><th>System ID</th><th>System Type</th><th>CVSS Base Score</th><th>Release On</th><th>Implementation Automatic</th><th>Processing Status</th><th>Implementation Status</th><th>SP Implementation Status</th></tr>
<tr><td>[redacted]</td><td>7</td><td>[CVE-2021-27611] Code Injection vulnerability in SAP NetWeaver AS ABAP</td><td>[redacted]</td><td>ABAP</td><td>8.2</td><td>5/11/21 2:05:08 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>7</td><td>[CVE-2021-27611] Code Injection vulnerability in SAP NetWeaver AS ABAP</td><td>[redacted]</td><td>SAP</td><td>8.2</td><td>5/11/21 2:05:08 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>4</td><td>[CVE-2021-33664] Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on Web Dynpro ABAP)</td><td>[redacted]</td><td>ABAP</td><td>5.4</td><td>6/8/21 2:05:09 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>4</td><td>[CVE-2021-33664] Cross-Site Scripting (XSS) vulnerability within SAP NetWeaver AS ABAP (Applications based on Web Dynpro ABAP)</td><td>[redacted]</td><td>SAP</td><td>5.4</td><td>6/8/21 2:05:09 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>6</td><td>[CVE-2021-27610] Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform</td><td>[redacted]</td><td>ABAP</td><td>9</td><td>6/8/21 2:05:29 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>6</td><td>[CVE-2021-27610] Improper Authentication in SAP NetWeaver ABAP Server and ABAP Platform</td><td>[redacted]</td><td>SAP</td><td>9</td><td>6/8/21 2:05:29 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>4</td><td>[CVE-2021-21473] Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform</td><td>[redacted]</td><td>ABAP</td><td>6.3</td><td>6/8/21 2:05:26 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
<tr><td>[redacted]</td><td>4</td><td>[CVE-2021-21473] Missing Authorization check in SAP NetWeaver AS ABAP and ABAP Platform</td><td>[redacted]</td><td>SAP</td><td>6.3</td><td>6/8/21 2:05:26 AM GMT+02:00</td><td>True</td><td>New</td><td>Can be implemented</td><td>To be Implemented by SAP Note</td></tr>
</table>

</td></tr>
<tr><td>

38. Jump back to launch pad by using the home button.

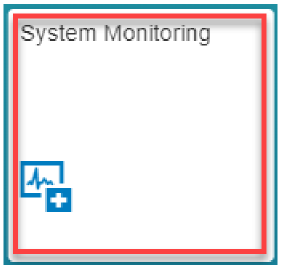
</td><td>



</td></tr>
<tr><td>

39. Click on Tile 'System Monitoring'.

</td><td>



</td></tr>
</table>

<table>
<tr><th>Explanation</th><th>Screenshot</th></tr>
<tr><td>

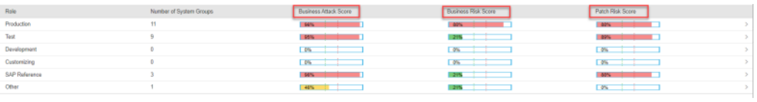
40. The UI shows per different system roles (Production, Test, …) the different scores:
    - Business Risk Score: System criticality as to the maintained criticality in ‘System Administration’ about Confidentiality, Integrity and Availability. It can be changed by changing/maintaining the values in ‘System Administration’.
    - Business Attack Score: Aggregated Alert Score from Alerts related to the system landscape, or to single systems, or to single systems and clients. If there exist non-processed Alerts related to the system, with a high Alert score, then the Business Attack Score is high.
    - Patch Risk Score: Based on the Patch State (See Tile ‘Security Notes’), the criticality of the system and the criticality of relevant notes which are not patched, a Patch Risk Score is calculated.

In the 1st UI the Scores are shown in an aggregated way, drill down is possible. The next level shows the same scores for a whole system. The next drilldown level shows the Scores for a system and its correlated clients. The next drilldown shows the detailed information, why the scores are high low:

- List of top 20 open Alerts
- List of top 20 missing security patches

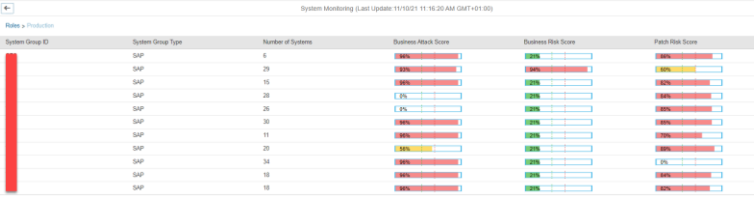
Navigation into each Alert is possible from there.

</td><td>



<table>
<tr><th>Role</th><th>Number of System Groups</th><th>Business Attack Score</th><th>Business Risk Score</th><th>Patch Risk Score</th></tr>
<tr><td>Production</td><td>11</td><td>96%</td><td>80%</td><td>80%</td></tr>
<tr><td>Test</td><td>9</td><td>95%</td><td>21%</td><td>89%</td></tr>
<tr><td>Development</td><td>0</td><td>0%</td><td>0%</td><td>0%</td></tr>
<tr><td>Customizing</td><td>0</td><td>0%</td><td>0%</td><td>0%</td></tr>
<tr><td>SAP Reference</td><td>3</td><td>96%</td><td>21%</td><td>80%</td></tr>
<tr><td>Other</td><td>1</td><td>40%</td><td>21%</td><td>0%</td></tr>
</table>

Aggregated Landscape View

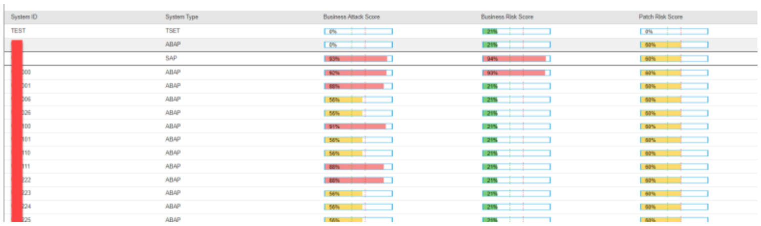


System Monitoring (Last Update:11/10/21 11:16:20 AM GMT+01:00)

Roles > Production

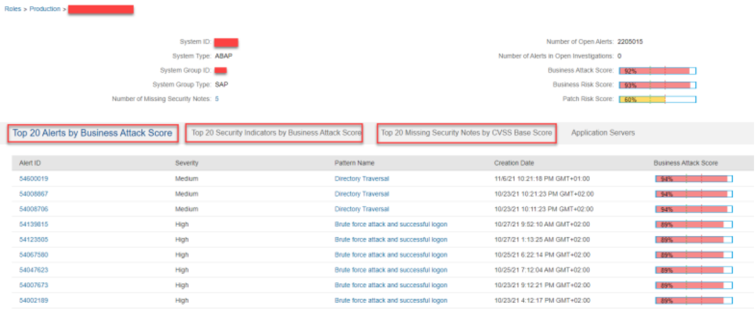
<table>
<tr><th>System Group ID</th><th>System Group Type</th><th>Number of Systems</th><th>Business Attack Score</th><th>Business Risk Score</th><th>Patch Risk Score</th></tr>
<tr><td>[redacted]</td><td>SAP</td><td>6</td><td>96%</td><td>21%</td><td>86%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>29</td><td>93%</td><td>94%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>15</td><td>96%</td><td>21%</td><td>82%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>28</td><td>0%</td><td>21%</td><td>84%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>26</td><td>0%</td><td>21%</td><td>85%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>30</td><td>96%</td><td>21%</td><td>85%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>11</td><td>96%</td><td>21%</td><td>70%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>20</td><td>56%</td><td>21%</td><td>89%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>34</td><td>96%</td><td>21%</td><td>0%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>18</td><td>96%</td><td>21%</td><td>84%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>18</td><td>96%</td><td>21%</td><td>82%</td></tr>
</table>

Aggregated System ID View



<table>
<tr><th>System ID</th><th>System Type</th><th>Business Attack Score</th><th>Business Risk Score</th><th>Patch Risk Score</th></tr>
<tr><td>TEST</td><td>TSET</td><td>0%</td><td>21%</td><td>0%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>0%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>SAP</td><td>93%</td><td>94%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>92%</td><td>93%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>88%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>91%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>88%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>88%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
<tr><td>[redacted]</td><td>ABAP</td><td>56%</td><td>21%</td><td>60%</td></tr>
</table>

Aggregated System/Client View



Roles > Production > [redacted]

System ID: [redacted]
System Type: ABAP
System Group ID: [redacted]
System Group Type: SAP
Number of Missing Security Notes: 5

Number of Open Alerts: 2205015
Number of Alerts in Open Investigations: 0
Business Attack Score: 92%
Business Risk Score: 93%
Patch Risk Score: 60%

Top 20 Alerts by Business Attack Score
Top 20 Security Indicators by Business Attack Score
Top 20 Missing Security Notes by CVSS Base Score
Application Servers

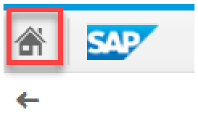
<table>
<tr><th>Alert ID</th><th>Severity</th><th>Pattern Name</th><th>Creation Date</th><th>Business Attack Score</th></tr>
<tr><td>54600019</td><td>Medium</td><td>Directory Traversal</td><td>11/6/21 10:21:18 PM GMT+01:00</td><td>94%</td></tr>
<tr><td>54008867</td><td>Medium</td><td>Directory Traversal</td><td>10/23/21 10:21:23 PM GMT+02:00</td><td>94%</td></tr>
<tr><td>54008706</td><td>Medium</td><td>Directory Traversal</td><td>10/23/21 10:11:23 PM GMT+02:00</td><td>94%</td></tr>
<tr><td>54139815</td><td>High</td><td>Brute force attack and successful logon</td><td>10/27/21 9:52:10 AM GMT+02:00</td><td>89%</td></tr>
<tr><td>54123505</td><td>High</td><td>Brute force attack and successful logon</td><td>10/27/21 1:13:25 AM GMT+02:00</td><td>89%</td></tr>
<tr><td>54067580</td><td>High</td><td>Brute force attack and successful logon</td><td>10/25/21 6:22:14 PM GMT+02:00</td><td>89%</td></tr>
<tr><td>54047623</td><td>High</td><td>Brute force attack and successful logon</td><td>10/25/21 7:12:04 AM GMT+02:00</td><td>89%</td></tr>
<tr><td>54007673</td><td>High</td><td>Brute force attack and successful logon</td><td>10/23/21 9:12:21 PM GMT+02:00</td><td>89%</td></tr>
<tr><td>54002189</td><td>High</td><td>Brute force attack and successful logon</td><td>10/23/21 4:12:17 PM GMT+02:00</td><td>89%</td></tr>
</table>

Detailed View for one System or System and client

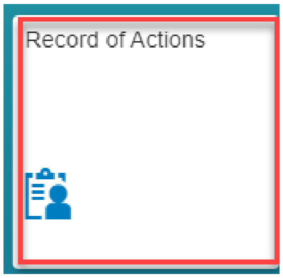
</td></tr>
<tr><td>

41. Jump back to launch pad by using the home button.

</td><td>



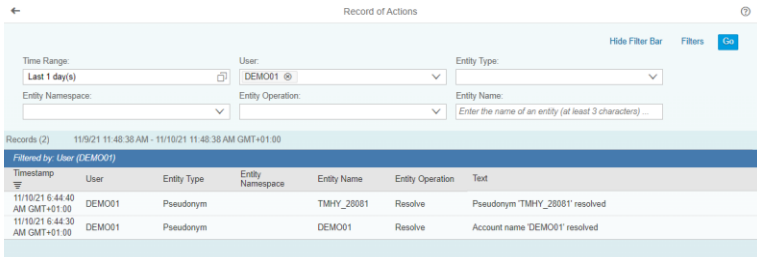
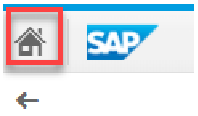
</td></tr>
</table>

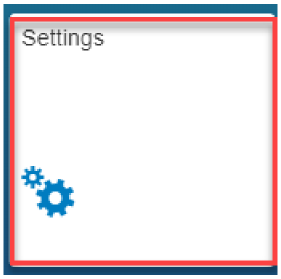
<table>
<tr><th>Explanation</th><th>Screenshot</th></tr>
<tr><td>42. Click on Tile ‘Record of Actions’</td><td> </td></tr>
<tr><td>43. In the UI you can see all actions either done automatically or by Users using ETD.

In the example a filtering took place about actions that happened last day and that were triggered by user DEMO01. User DEMO01 resolved a user pseudonym TMHY_28081 and looked up the user pseudonym for user DEMO01.

In the filter it can be selected via very different Entity Types about what happened in the ETD system.

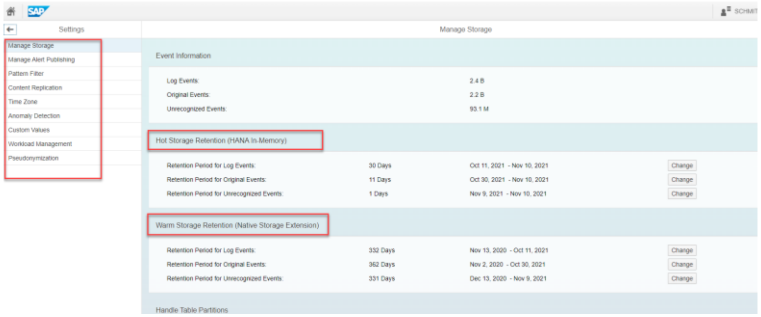
The functionality is built in for compliance reasons, to get exact information about who did what and to be able to find out this was compliant/incompliant.

Information: The Record of Action Log is additionally used for ETD self-monitoring. Patterns/Use cases that throw alerts are available, e.g. in the case of critical changed to a pattern (e.g. deactivate it)</td><td>
Time Range: Last 1 day(s)
User: DEMO01
Entity Type:
Entity Namespace:
Entity Operation:
Entity Name: Enter the name of an entity (at least 3 characters) ...
Records (2) 11/9/21 11:48:38 AM - 11/10/21 11:48:38 AM GMT+01:00
Filtered by: User (DEMO01)
<table>
<tr><th>Timestamp</th><th>User</th><th>Entity Type</th><th>Entity Namespace</th><th>Entity Name</th><th>Entity Operation</th><th>Text</th></tr>
<tr><td>11/10/21 6:44:40 AM GMT+01:00</td><td>DEMO01</td><td>Pseudonym</td><td></td><td>TMHY_28081</td><td>Resolve</td><td>Pseudonym 'TMHY_28081' resolved</td></tr>
<tr><td>11/10/21 6:44:30 AM GMT+01:00</td><td>DEMO01</td><td>Pseudonym</td><td></td><td>DEMO01</td><td>Resolve</td><td>Account name 'DEMO01' resolved</td></tr>
</table></td></tr>
<tr><td>44. Jump back to launch pad by using the home button.</td><td></td></tr>
</table>

Explanation	Screenshot
45. Click on Tile ‘Settings’	

46. In the UI you can see the different possibilities for ETD configuration.

- Manage Storage: Here you can define the retention periods for Hot Storage and Warm Storage. Information: To determine these values, SAP provides a sizing guide.
- Manage Alert Publishing: Here you can define an Alert Forwarding/Pushing from ETD to any Rest Endpoint. You can define the base URL to send to (credentials are created within the HANA platform), the Alert format, a filter maintained in Menu item ‘Pattern Filter’, whether the triggering events shall be added to the alert, and whether the Alert status shall be set to ‘Forwarded’. Additionally, you can define mail receivers to send the alerts via mail.
- Pattern Filter: Here you can define different filters you can use either to push out only certain alerts, or to hand over the filter ID via the Alert retrieval API to get only the alerts related to the patterns within the filter
- Content Replication: If you use a 2-tier ETD landscape (one pre-prod for Pattern creation and testing, one prod for running the patterns and processing alerts. Then the objects (like Workspaces, patterns, value lists, as well as e.g. maintained system meta data) can be transported from the pre-prod system to the prod system. In this UI you can define the transport directions for this data. The configuration of the transport directions are done in a configuration file (described in the SAP help documentation)
- Time Zone: Here you can define whether the ETD users work always in UTC timezone (makes sense if the ressourcces are distributed over the world. So that they can easily discuss critical topics and speak about the same time) or in local time zone (easier in case everyone works in the same time zone)
- Anomaly Detection: You can define whether you want to collect data as well for currently inactive anomaly detection patterns. Reason: If you set such a Pattern active at a later point in time´, it can directly create alerts, instead of needing to start now collecting data



Manage Storage

Event Information

Log Events:	2.4 B
Original Events:	2.2 B
Unrecognized Events:	93.1 M

Hot Storage Retention (HANA In-Memory)

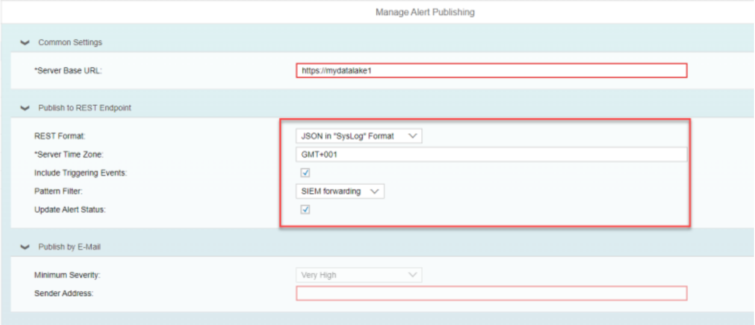
Retention Period for Log Events:	30 Days	Oct 11, 2021 - Nov 10, 2021	Change
Retention Period for Original Events:	11 Days	Oct 30, 2021 - Nov 10, 2021	Change
Retention Period for Unrecognized Events:	1 Days	Nov 9, 2021 - Nov 10, 2021	Change

Warm Storage Retention (Native Storage Extension)

Retention Period for Log Events:	332 Days	Nov 13, 2020 - Oct 11, 2021	Change
Retention Period for Original Events:	362 Days	Nov 2, 2020 - Oct 30, 2021	Change
Retention Period for Unrecognized Events:	331 Days	Dec 13, 2020 - Nov 9, 2021	Change

Handle Table Partitions

Retention Times



Manage Alert Publishing

Common Settings

*Server Base URL: https://mydatalake1

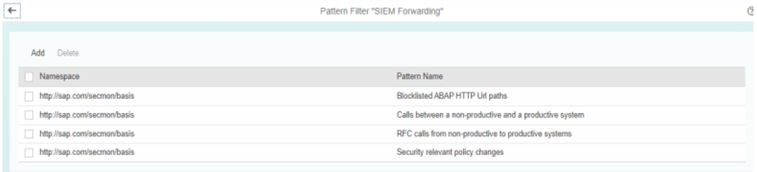
Publish to REST Endpoint

REST Format: JSON in "SysLog" Format
*Server Time Zone: GMT+001
Include Triggering Events: ☑
Pattern Filter: SIEM forwarding
Update Alert Status: ☑

Publish by E-Mail

Minimum Severity: Very High
Sender Address:

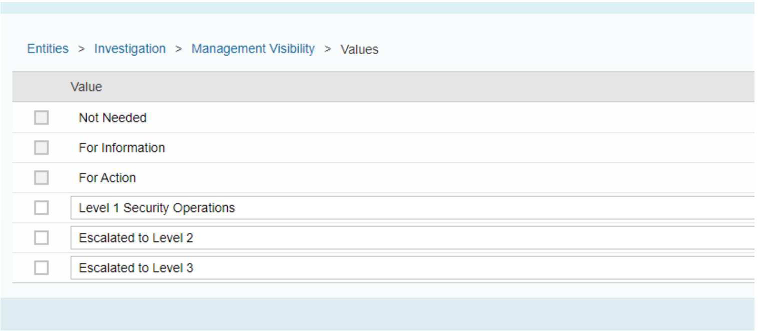
Alert forwarding



Pattern Filter "SIEM Forwarding"

Namespace	Pattern Name
http://sap.com/secmon/basis	Blocklisted ABAP HTTP Url paths
http://sap.com/secmon/basis	Calls between a non-productive and a productive system
http://sap.com/secmon/basis	RFC calls from non-productive to productive systems
http://sap.com/secmon/basis	Security relevant policy changes

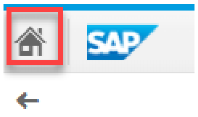
Pattern Filter



Entities > Investigation > Management Visibility > Values

Value
Not Needed
For Information
For Action
Level 1 Security Operations
Escalated to Level 2
Escalated to Level 3

Custom Values

Explanation	Screenshot
over e.g. 12 weeks with some waiting time if the 12 weeks more than the retention time. • Custom Values: You can create own custom values for investigations and workspaces. In the example screenshot further investigation values are created to define a kind of a current processing state by different security analyst levels • Workload Management: If queries start to be to memory exhausting, the HANA DB slows down for other users to fulfill the current request with all resources needed. In order to allow other to work, during such a 'heavy' query is running, the workload management restricts the resources to a maximum threshold for executing one query. • Pseudonymization: can be switched on and off, depending on the Country specific, industry specific, company specific regulations.	
47. Jump back to launch pad by using the home button.	

1.2. Summary

Tool Aspect: You learned how to navigate within SAP Enterprise Threat Detection, and by that you went through the most relevant UIs and functionalities, allowing you to understand, what it is made for, and how things are correlated (e.g., information from knowledge base, and what you see in alerts and in the forensic lab). Some of the tools are further explored in detail in the following exercises.

2. SECURITY EXPERT - WORKING WITH THE FORENSIC LAB

Security Aspect: The Security Expert sometimes needs to do an ad-hoc analysis about things that happen in the landscape, or he gets a hint about certain suspicious behavior of an IP Address, within an SAP System, of certain program calls etc.

He might need to create own charts to easier interpret the data and the suspicious behavior within, and even he might need to create an own detection patterns to get future alerts about the suspicious actions he found during his analysis.

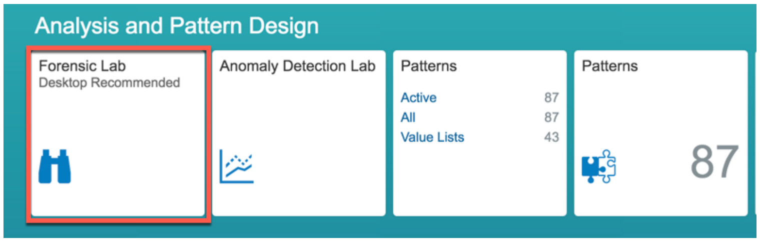
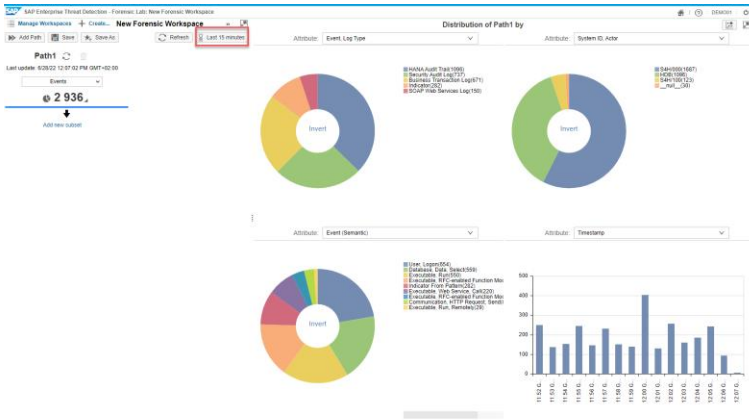
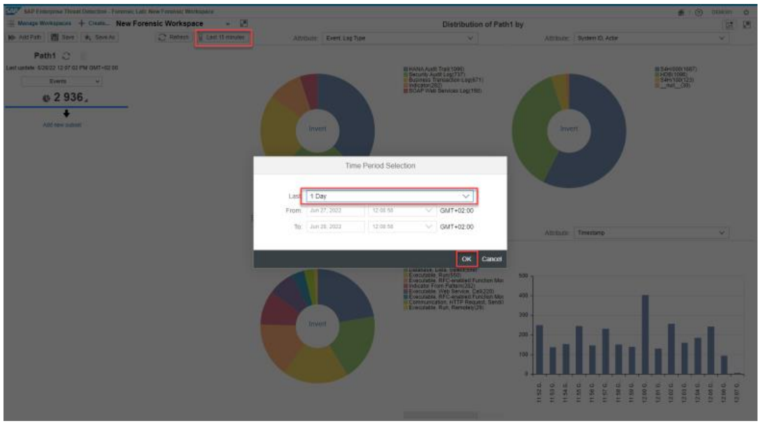
Tool Aspect: The forensic lab is one the most important application in SAP Enterprise Threat Detection and helps you to gain insight about what is going on at present in your system landscape.

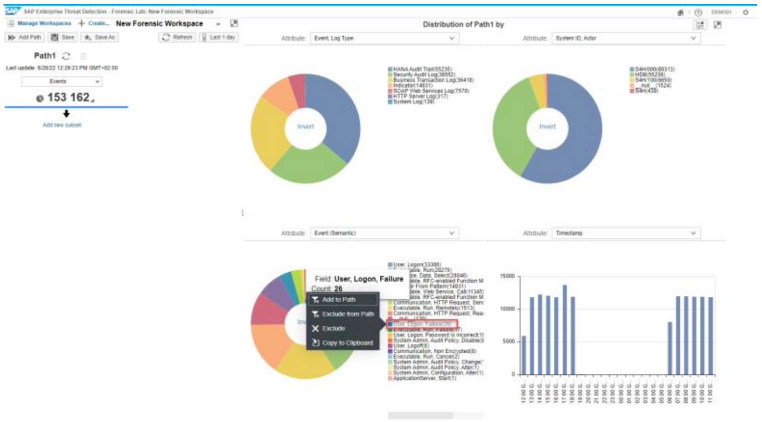
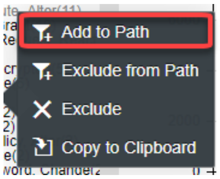
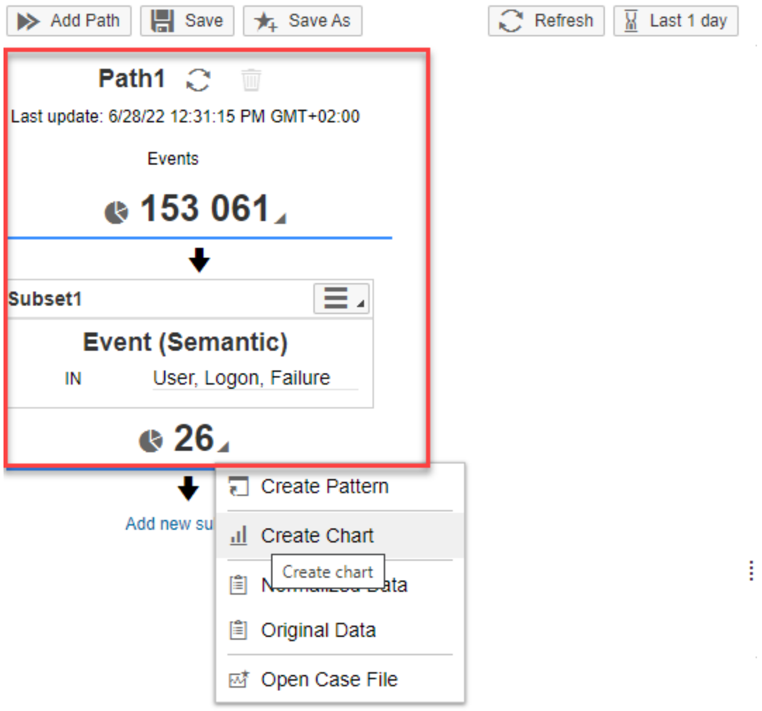
Forensic lab supports workspaces for identifying and analyzing weaknesses or attacks and supports the modelling of charts or attack detection patterns. For attack detection patterns, you create the configurations, which you want SAP Enterprise Threat Detection to use to scan for events that match the pattern. No coding or complex regex/SQL queries are needed, instead SAP Enterprise Threat Detection takes care of transforming your attack detection pattern model to SAP HANA optimized queries.

In this exercise you will learn how to work with the forensic lab, how to analyze log events and how to create charts and attack detection patterns.

2.1. Filtering Data

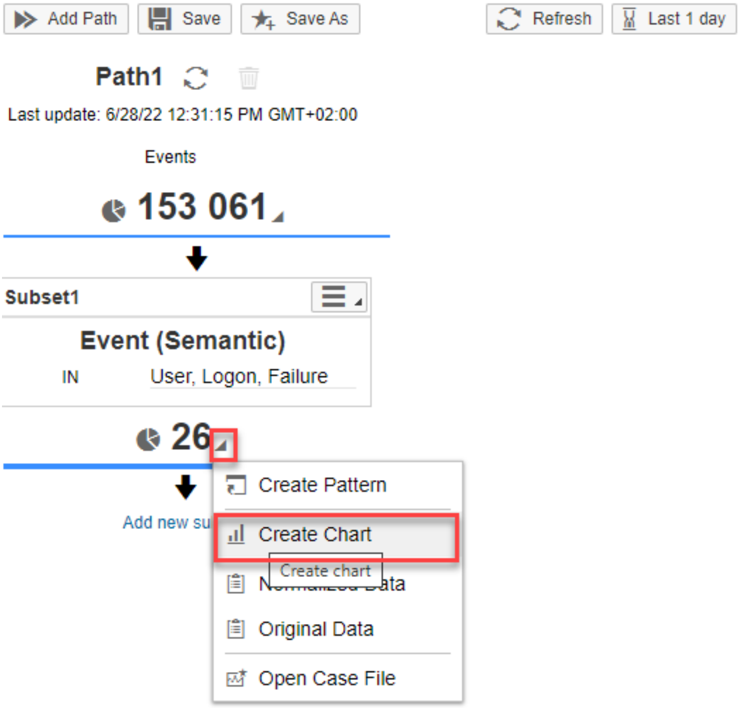
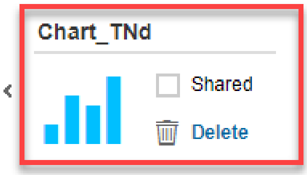
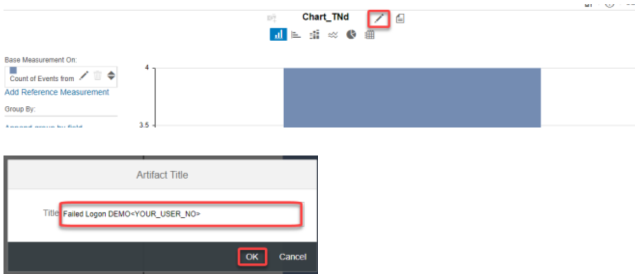
In this exercise, you will display failed log on attempts, and you will learn how filters can be created.

Explanation	Screenshot
48. Open tile **Forensic Lab** in the SAP Enterprise Threat Detection Launchpad.	 Analysis and Pattern Design Forensic Lab Desktop Recommended Anomaly Detection Lab Patterns Active 87 All 87 Value Lists 43 Patterns 87
49. The initial screen of the forensic lab shows the log events from last 15 minutes. The left part of the workspace contains the filter paths. The right part of the workspace is used to display the log events. They are called browsing charts. You can e.g. see which log types – *Event, Log Type* - are received, from which systems - *System ID, Actor* - or which actions - *Event (Semantic)* - have been performed. Change the drop-down value in one of the browsing charts to see information about other semantic attributes.	 SAP Enterprise Threat Detection - Forensic Lab: New Forensic Workspace Manage Workspaces + Create... New Forensic Workspace Add Path Save Save As Refresh Last 15 minutes Path1 Last update: 6/28/22 12:07:02 PM GMT+02:00 Events 2 936 Add new subset Distribution of Path1 by Attribute: Event, Log Type Attribute: System ID, Actor Attribute: Event (Semantic) Attribute: Timestamp
50. Push button *Change time period.* Change time period selection to ***1 hour*** and push button *OK* to analyze the log events from last day. Look at the path and the browsing charts that have been updated.	 Time Period Selection Last: 1 Day From: Jun 27, 2022 12:08:58 GMT+02:00 To: Jun 28, 2022 12:08:58 GMT+02:00 OK Cancel

Explanation	Screenshot
51. To add a filter for failed logon events, click on legend *User Logon, Failure.*	
52. Select menu item *Add to Path.* This will create a filter for failed logons that have been occurred in the last day. It is shown as *Subset* in the filter path.	Add to Path Exclude from Path Exclude Copy to Clipboard
53. Look at *Path1* and see the subset that has been added. Observe that the browsing charts have been updated as well.	Add Path · Save · Save As · Refresh · Last 1 day Path1 Last update: 6/28/22 12:31:15 PM GMT+02:00 Events 153 061 Subset1 Event (Semantic) IN User, Logon, Failure 26 Add new su Create Pattern Create Chart Create chart Normalized Data Original Data Open Case File

2.2. Modelling Charts

Based on the subset you have created in the filter path, you can further filter the log events, or you can create charts to see more details. In this exercise you will create a chart of failed logon events including information about systems and users.

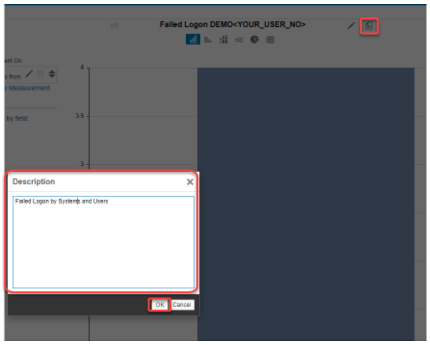
Explanation	Screenshot
54. Push button ◢ right to the subset number. This opens a drop-down menu with all available operations you can perform on the subset. Select menu item *Create Chart*	 Add Path Save Save As Refresh Last 1 day Path1 Last update: 6/28/22 12:31:15 PM GMT+02:00 Events 153 061 Subset1 Event (Semantic) IN User, Logon, Failure 26 Add new su Create Pattern Create Chart Create chart N ata Original Data Open Case File
55. Show the Chart: Click on the Chart Icon lower left. The Chart opens on the right part of the UI	
56. Change the chart name: *Click on the pencil symbol* *In the Popup enter:* *Failed Logon DEMO**<YOUR_USERNR>*** Press o.k.	 Chart_TNd Base Measurement On: Count of Events from Add Reference Measurement Group By: 4 3.5 Artifact Title OK CancelTitle: Failed Logon DEMO<YOUR_USER_NO>

<table>
<tr><th>Explanation</th><th>Screenshot</th></tr>
<tr><td>

57. Push button . Add the following description and push button *OK.*

    Description:
    Failed Logon Events by Systems and Users

</td><td>



Failed Logon DEMO<YOUR_USER_NO>

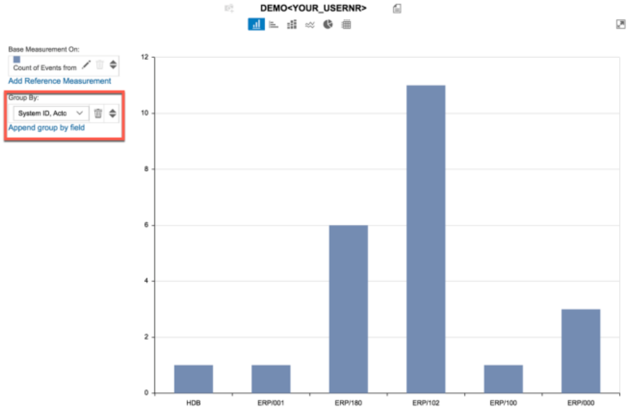
Description

Failed Logon by Systems and Users

</td></tr>
<tr><td>

58. Click on link *Append group by field* and add field *System ID, Actor.* The chart will be updated with the system information on which failed logon attempts have been observed.

</td><td>



DEMO<YOUR_USERNR>

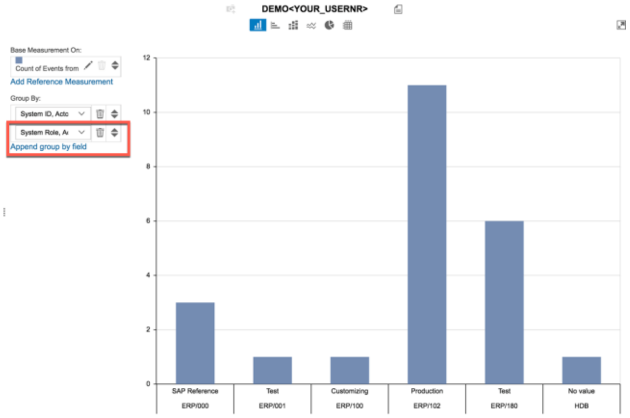
Base Measurement On: Count of Events from

Group By: System ID, Acto

</td></tr>
<tr><td>

59. Click on link *Append group by field* and add field *System Role, Actor.* The chart will be updated with additional system role information.

</td><td>



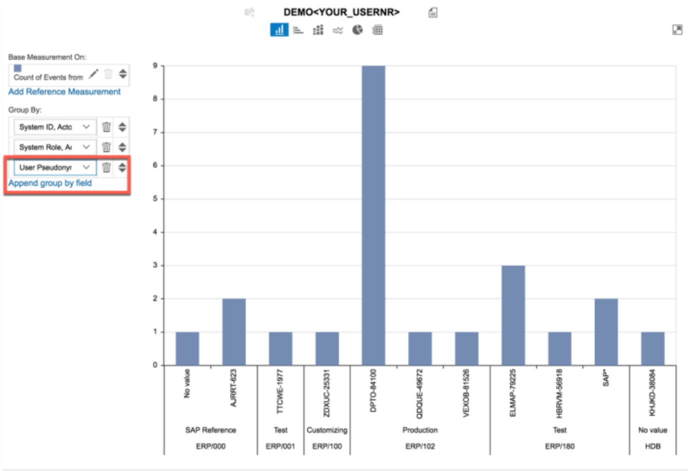
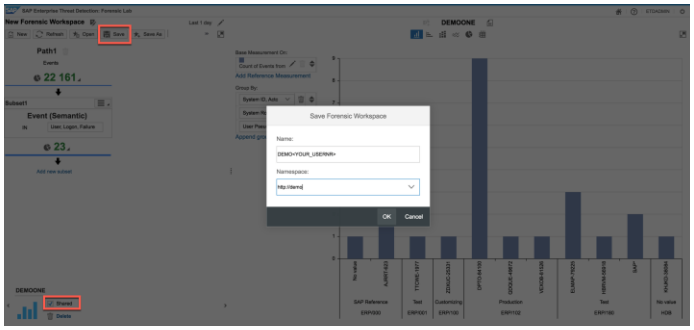
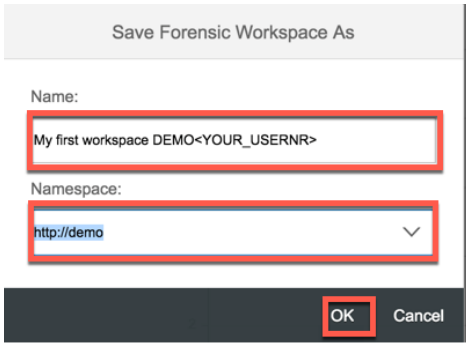
DEMO<YOUR_USERNR>

Base Measurement On: Count of Events from

Group By: System ID, Acto

System Role, A

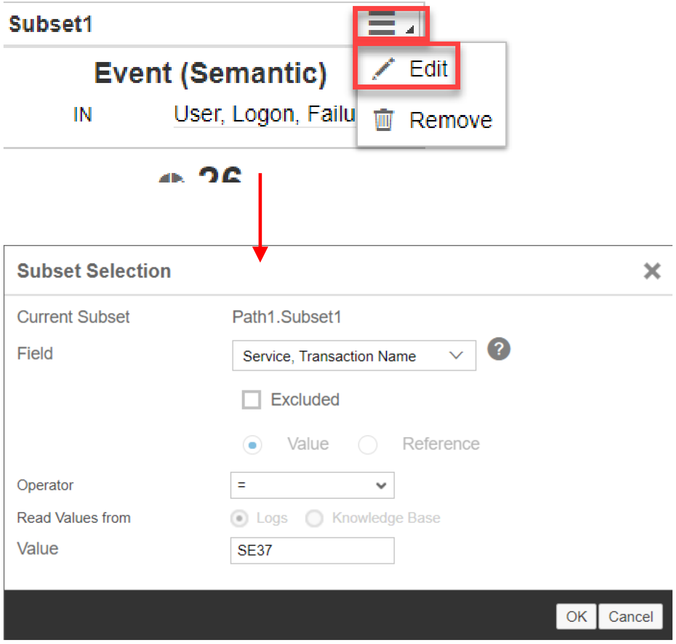
</td></tr>
</table>

Explanation	Screenshot
60. Click on link *Append group by field* and add field *User Account Name Pseudonym, Target.* The chart will be updated with additional user information.	 DEMO<YOUR_USERNR> Base Measurement On: Count of Events from Add Reference Measurement Group By: System ID, Acto System Role, A User Pseudonyr Append group by field 9 8 7 6 5 4 3 2 1 0 No value AJRRT-6823 TTCWE-1977 ZDXUC-25331 DPTO-84100 QDQUE-49672 VEXOB-81526 ELMAP-79225 HBRVM-56918 SAP* KHJKD-38084 SAP Reference ERP/000 Test ERP/001 Customizing ERP/100 Production ERP/102 Test ERP/180 No value HDB
61. You can now save your changes. On the left lower area enable checkbox *Shared*. This allows other users to access your charts. Push button *Save*.	 SAP Enterprise Threat Detection: Forensic Lab New Forensic Workspace Save Path1 22 161 Subset1 Event (Semantic) 23 Add new subset DEMOONE Save Forensic Workspace Name: DEMO<YOUR_USERNR> Namespace: http://demo OK Cancel Shared Delete
62. Provide name and namespace for your workspace and push button *OK.* Name: *My first workspace DEMO**<YOUR_USERNR>*** Namespace: *http://demo*	 Save Forensic Workspace As Name: My first workspace DEMO<YOUR_USERNR> Namespace: http://demo OK Cancel

2.3. Browse through the data and model your own individual charts

In your newly created workspace, *my first workspace DEMO<YOUR_USERNR>* you can add a new path by pushing the button ≫ Add Path . On the new path you can create new filters by adding new subsets either via the browsing charts or by clicking on the link Add new subset . AND operator ↓ between subsets can be toggled to an OR operator 🔗 .

Also have a close look on the *Subset Selection* options (Example):



Subset1

Event (Semantic)

IN User, Logon, Failu

Subset Selection

Current Subset: Path1.Subset1

Field: Service, Transaction Name

□ Excluded

● Value ○ Reference

Operator: =

Read Values from: ● Logs ○ Knowledge Base

Value: SE37

You can filter specific fields (= *Field*) from semantic attributes using a specific operator (=*Operators)* and providing corresponding filter values (= *Value*)

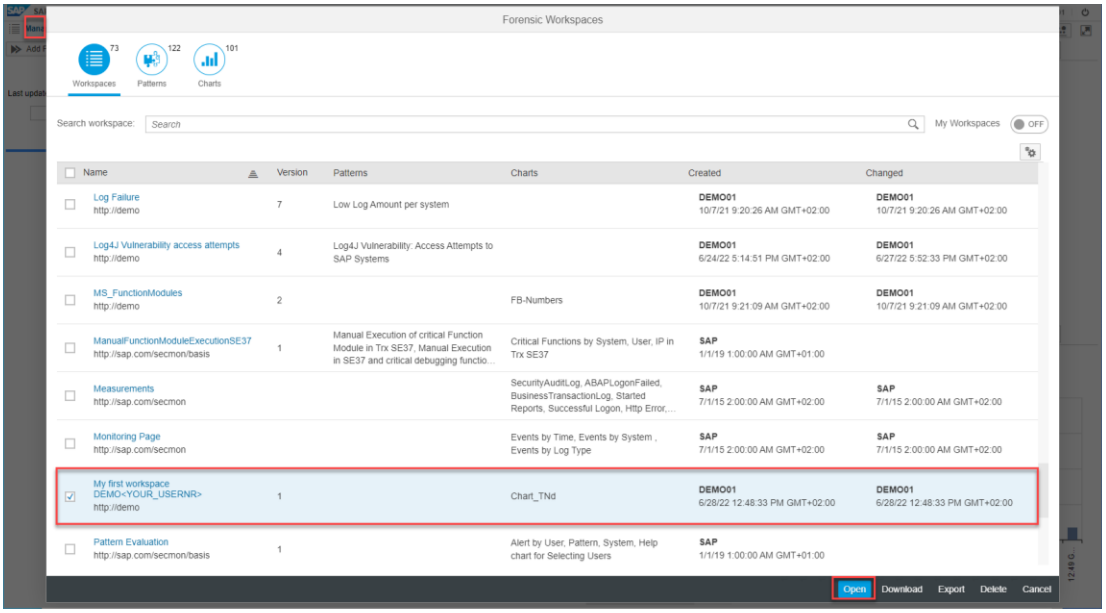
You can use the option *Reference* to correlate Events from one path to another path

You can use Value-List containing pre-defined values for filtering the data

Make use of the following chart name for your own created charts:

<Chart name> *DEMO***<*YOUR_USERNR*>**

Save your changes. To retrieve the Workspace when opening a new Forensic Lab UI, click on *'Manage Workspaces'* and select your own one.



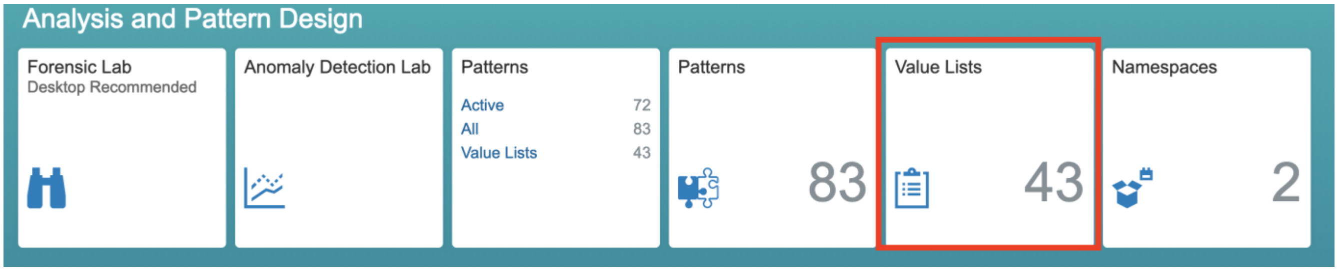
☐ Name	Version	Patterns	Charts	Created	Changed
☐ Log Failure http://demo	7	Low Log Amount per system		**DEMO01** 10/7/21 9:20:26 AM GMT+02:00	**DEMO01** 10/7/21 9:20:26 AM GMT+02:00
☐ Log4J Vulnerability access attempts http://demo	4	Log4J Vulnerability: Access Attempts to SAP Systems		**DEMO01** 6/24/22 5:14:51 PM GMT+02:00	**DEMO01** 6/27/22 5:52:33 PM GMT+02:00
☐ MS_FunctionModules http://demo	2		FB-Numbers	**DEMO01** 10/7/21 9:21:09 AM GMT+02:00	**DEMO01** 10/7/21 9:21:09 AM GMT+02:00
☐ ManualFunctionModuleExecutionSE37 http://sap.com/secmon/basis	1	Manual Execution of critical Function Module in Trx SE37, Manual Execution in SE37 and critical debugging functio...	Critical Functions by System, User, IP in Trx SE37	**SAP** 1/1/19 1:00:00 AM GMT+01:00	
☐ Measurements http://sap.com/secmon			SecurityAuditLog, ABAPLogonFailed, BusinessTransactionLog, Started Reports, Successful Logon, Http Error,...	**SAP** 7/1/15 2:00:00 AM GMT+02:00	**SAP** 7/1/15 2:00:00 AM GMT+02:00
☐ Monitoring Page http://sap.com/secmon			Events by Time, Events by System , Events by Log Type	**SAP** 7/1/15 2:00:00 AM GMT+02:00	**SAP** 7/1/15 2:00:00 AM GMT+02:00
☑ My first workspace DEMO<YOUR_USERNR> http://demo	1		Chart_TNd	**DEMO01** 6/28/22 12:48:33 PM GMT+02:00	**DEMO01** 6/28/22 12:48:33 PM GMT+02:00
☐ Pattern Evaluation http://sap.com/secmon/basis	1		Alert by User, Pattern, System, Help chart for Selecting Users	**SAP** 1/1/19 1:00:00 AM GMT+01:00	

2.4. Working with Value Lists

Value List allows to simplify the filtering of events. Instead of adding multiple values manually into the Subset Filter multiple times, you can filter the data for multiple values more easily by using a value-list.

Patterns delivered by SAP Enterprise Threat Detection makes as well use of value-lists. To tune the patterns in the way that the use case fits to the customers environment, the value lists can be adjusted and enhanced accordingly.

Open a new SAP ETD Launchpad tab in your browser and have a closer look on tile *Value Lists:*



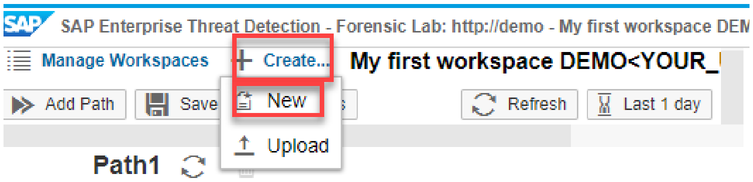
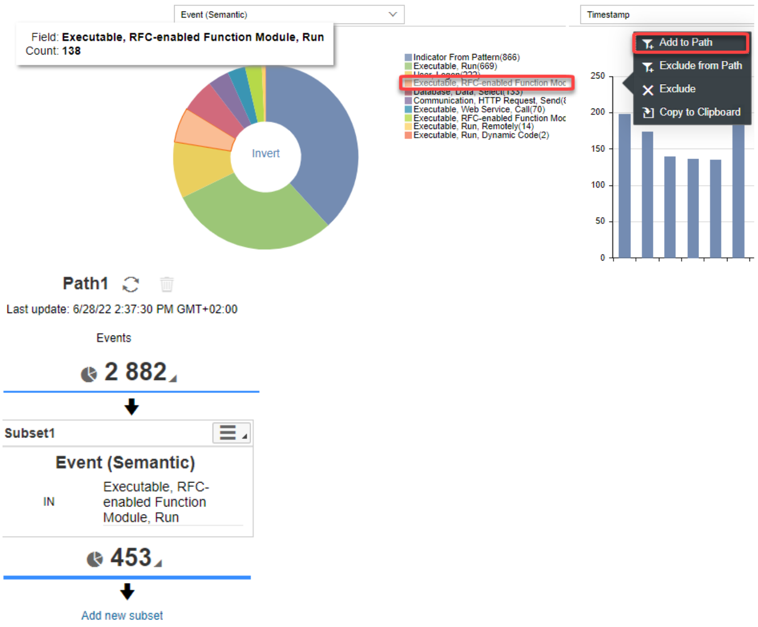
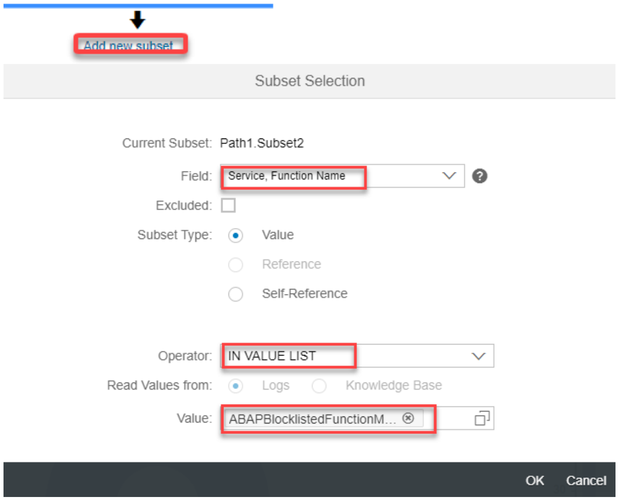
In the *Value List* application, you can view existing ones that are delivered with SAP Enterprise Threat Detection

The value lists delivered with SAP Enterprise Threat Detection have pre-defined values, that can be adjusted and enhanced

You can also create your own value lists

2.5. Modeling Attack Detection Patterns

The forensic lab supports the creation of attack detection patterns. The procedure is similar to the procedure of creating charts. Attack detection patterns are as well based on a particular subset of log events. Now you will create a pattern that will deliver an alert when SAP Standard users execute critical function modules in critical systems.

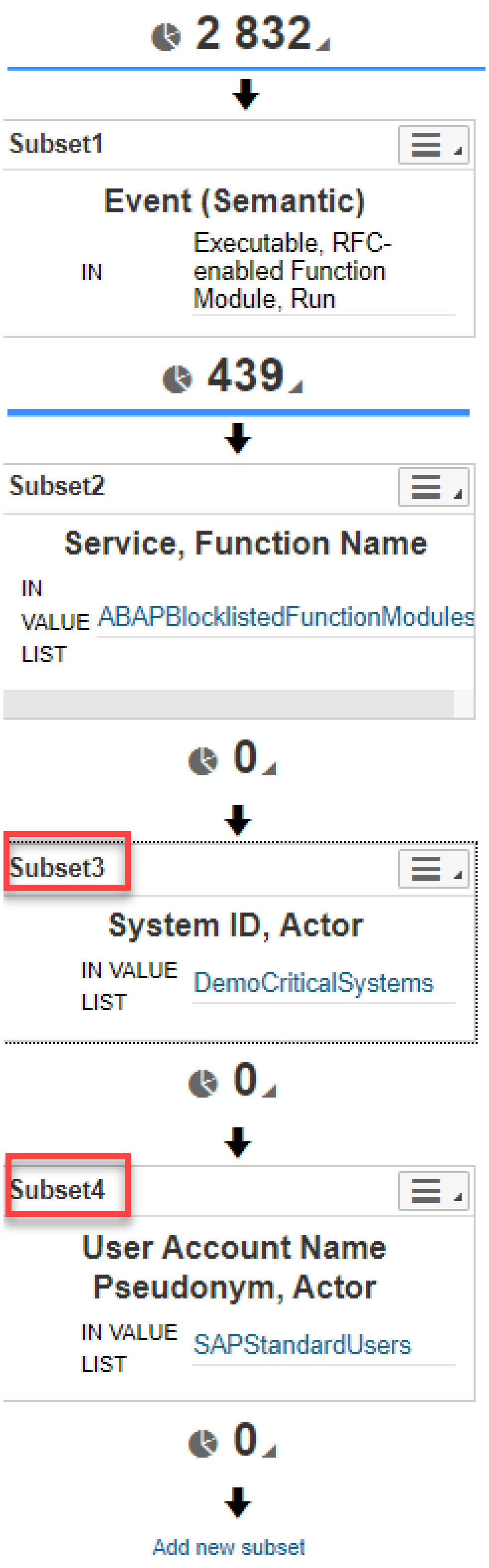
Explanation	Screenshot
63. Push button *Create* and then 'New' to create a new workspace.	 SAP Enterprise Threat Detection - Forensic Lab: http://demo - My first workspace DEM Manage Workspaces · Create... · My first workspace DEMO<YOUR_ Add Path · Save · New · Refresh · Last 1 day Upload Path1
64. In the Chart for 'Event (Semantic) Search for Event *Executable, RFC enabled Function Module, Run*, and by clicking on the Event, select *Add to Path*. As result, your filter path now has a filter on this event	 Event (Semantic) Timestamp Field: **Executable, RFC-enabled Function Module, Run** Count: **138** Invert Indicator From Pattern(866) Executable, Run(669) User, Logon(222) Executable, RFC-enabled Function Moc Database, Data, Select(133) Communication, HTTP Request, Send(Executable, Web Service, Call(70) Executable, RFC-enabled Function Moc Executable, Run, Remotely(14) Executable, Run, Dynamic Code(2) Add to Path Exclude from Path Exclude Copy to Clipboard 250 200 150 100 50 0 Path1 Last update: 6/28/22 2:37:30 PM GMT+02:00 Events 2 882 Subset1 Event (Semantic) IN Executable, RFC-enabled Function Module, Run 453 Add new subset
65. By clicking *Add new subset* in the path, you can add value lists to the path. To filter on the value list with critical function modules (pre-delivered by SAP), in the popup select: - Field: *Service, Function Name* - Operator: *IN VALUE LIST* - Value: *ABAPBlocklistedFunctionModules* Then press *OK* *As a result, another subset was added to the filter path.*	 Add new subset Subset Selection Current Subset: Path1.Subset2 Field: Service, Function Name Excluded: □ Subset Type: ● Value ○ Reference ○ Self-Reference Operator: IN VALUE LIST Read Values from: ● Logs ○ Knowledge Base Value: ABAPBlocklistedFunctionM... OK Cancel

66. Now, additionally add the following filter paths, as shown above, to further select on critical systems, and on SAP Standard Users:

Subset 3:
Field: *System ID, Actor*
Operator: *IN VALUE LIST*
Value: *DemoCriticalSystems*

Subset 4:
Field: *User Account Name Pseudonym, Actor*
Operator: *IN VALUE LIST*
Value: *SAPStandardUsers*

As a result, subsets 3 and 4 should have been added to the filter path.



2 832

Subset1

Event (Semantic)

IN Executable, RFC-enabled Function Module, Run

439

Subset2

Service, Function Name

IN VALUE LIST ABAPBlocklistedFunctionModules

0

Subset3

System ID, Actor

IN VALUE LIST DemoCriticalSystems

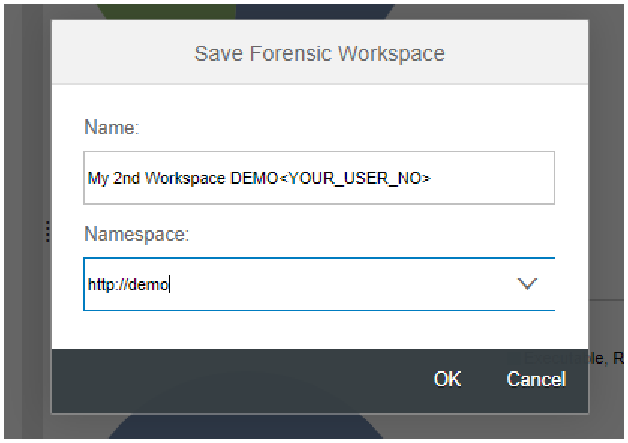
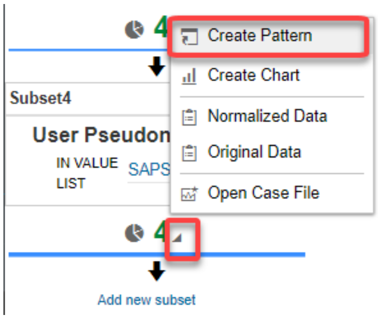
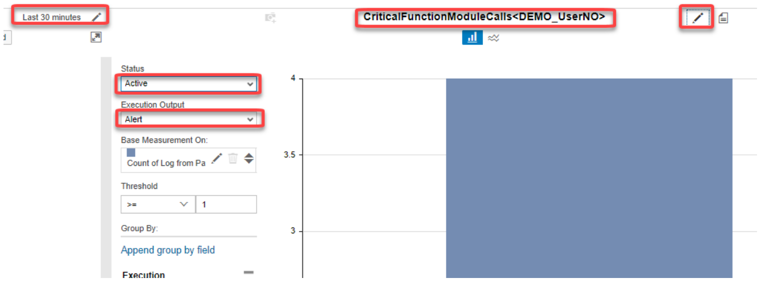
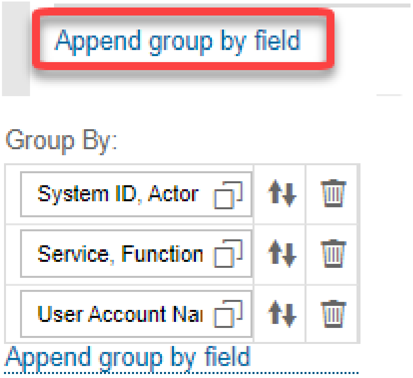
0

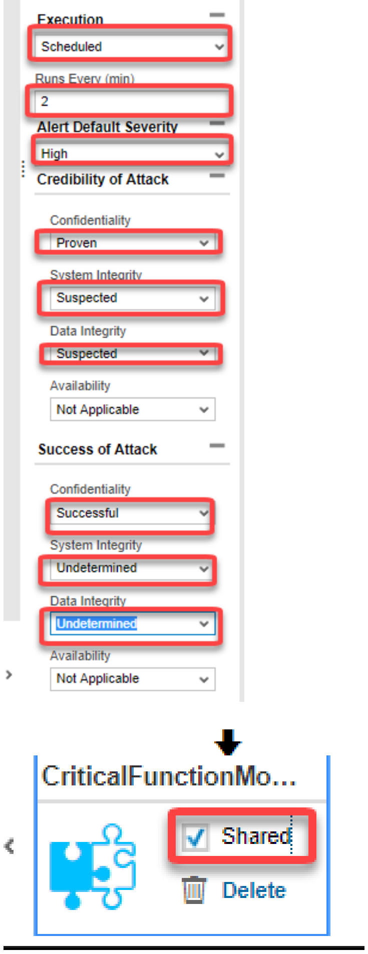
Subset4

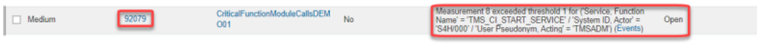
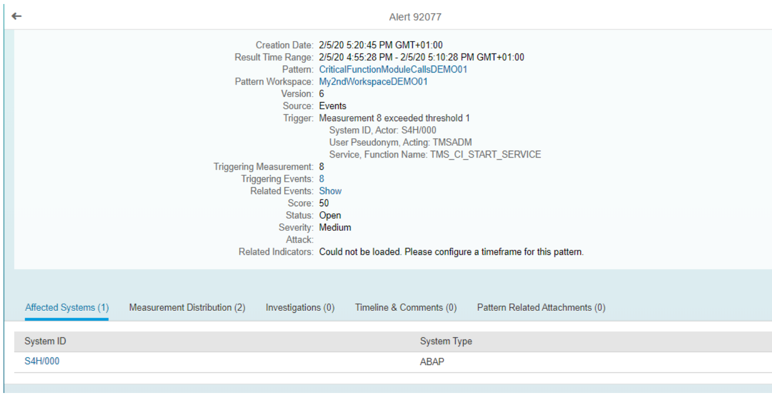
User Account Name Pseudonym, Actor

IN VALUE LIST SAPStandardUsers

0

Explanation	Screenshot
67. Save the Workspace	 Save Forensic Workspace Name: My 2nd Workspace DEMO<YOUR_USER_NO> Namespace: http://demo
68. Now create a Pattern that creates an Alert if the filter in subset 4 is not zero. Click on the small triangle within subset 4 and then in the popup click on *Create Pattern*	 Create Pattern Create Chart Normalized Data Original Data Open Case File Subset4 User Pseudon IN VALUE LIST SAPS Add new subset
69. On the right side of the screen you can now model the Pattern: Name: *CriticalFunctionModuleCalls<DEMO_UserNO>* Timeframe: *Last 30 Minutes* Status: *Active* Execution Output: *Alert*	 Last 30 minutes CriticalFunctionModuleCalls<DEMO_UserNO> Status: Active Execution Output: Alert Base Measurement On: Count of Log from Pa Threshold: >= 1 Group By:
70. To show data in the future Alerts, field grouping is needed. Exactly the grouped fields are each per grouping raising an Alert and exactly the grouped fields are shown in the upcoming Alerts. Press *Append group by field* and select the following fields to be grouped on: - *System ID, Actor* - *Service, Function Name* - *User Account Name Pseudonym, Actor*	 Group By: System ID, Actor Service, Function User Account Nai

Explanation	Screenshot
71. Do further settings within the Pattern: Execution: *Scheduled* Runs Every (min): *2* Alert Severity: *High* Credibility of the Attack: Confidentiality: *Proven* System Integrity: *Suspected* Data Integrity: *Suspected* Success of Attack Confidentiality: *Successful* System Integrity: *Undetermined* Data Integrity: *Undetermined* **Important**: Set the Pattern to value ***Shared*** **Finally Save again** **Notes**: the scheduled execution of each 2 minutes is for demo purposes only, so that alerts are raised when waiting. The scheduled execution times to select are dependent on: - Criticality of the Alert. The more critical the smaller the execution intervals - Numbers of aggregated log events to be considered in a certain time interval, to raise the Alert, if the threshold is bigger than one. **Example**: More than 3 failed logons per user and system within a timeframe of 5 Minutes or 30 Minutes or 2 hours or one week are considered to be alerted? - The Time frame selected for the whole workspace. **Example**: A selected time frame of last week aggregates the data of one week, but an execution of the pattern each 2 minutes might sometimes still make sense, but very often the selected values do not fit. Mostly the time frames of workspace time interval and Pattern-execution time interval should be similar, with some overlap. A typical value would be the execution of a Pattern each 10 minutes and the time interval of a Workspace of last 15 minutes.	Execution Scheduled Runs Every (min) 2 Alert Default Severity High Credibility of Attack Confidentiality Proven System Integrity Suspected Data Integrity Suspected Availability Not Applicable Success of Attack Confidentiality Successful System Integrity Undetermined Data Integrity Undetermined Availability Not Applicable CriticalFunctionMo... ☑ Shared Delete

Explanation	Screenshot
72. Check corresponding Alerts in he Alerts-Tile in the starting Page of ETD. After while (if the Filter Path in the workspace shows numbers bigger than zero). Find the Alerts for your Pattern in the Alert list and see the detail information that corresponds to the grouping in the modeled Pattern. Click on the Alert ID and see the details within the Alert. **Note**: Alert and Investigation handling will be handled in a later chapter	 Alerts  □ Medium 92079 CriticalFunctionModuleCallsDEMO01 No Measurement 8 exceeded threshold 1 for ('Service, Function Name' = 'TMS_CI_START_SERVICE' / 'System ID, Actor' = 'S4H/000' / 'User Pseudonym, Acting' = 'TMSADM') (Events) Open  Alert 92077 Creation Date: 2/5/20 5:20:45 PM GMT+01:00 Result Time Range: 2/5/20 4:55:28 PM - 2/5/20 5:10:28 PM GMT+01:00 Pattern: CriticalFunctionModuleCallsDEMO01 Pattern Workspace: My2ndWorkspaceDEMO01 Version: 6 Source: Events Trigger: Measurement 8 exceeded threshold 1 System ID, Actor: S4H/000 User Pseudonym, Acting: TMSADM Service, Function Name: TMS_CI_START_SERVICE Triggering Measurement: 8 Triggering Events: 8 Related Events: Show Score: 50 Status: Open Severity: Medium Attack: Related Indicators: Could not be loaded. Please configure a timeframe for this pattern. Affected Systems (1) Measurement Distribution (2) Investigations (0) Timeline & Comments (0) Pattern Related Attachments (0) System ID — System Type S4H/000 — ABAP

2.1. Summary

Security Aspect: As a Security Expert you are now able to do forensic analysis and find suspicious behaviors and evidences in big amounts of data. Now you can visualize this data as to your needs and create own Attack Detection Patterns in case you need to get Alerts on future occurrences of this situation.

Tool Aspect: You learned how to use the Forensic Lab to look into data, create Charts and Patterns and how to save them and to make them available to others.

Note: The example pattern you modelled is already part of the standard content delivery of ETD

3. PROCESSING ALERTS AND INVESTIGATIONS

Security Aspect: As a Security Analyst in Level 1, 2 or 3 one of your main tasks is to check for raised Alerts and to process them. You need to answer questions like

- Was this a real Alert or a false positive?
- What are evidences which need to be collected to proof the attack or misuse?
- Are there additional Alerts related to this Alert?

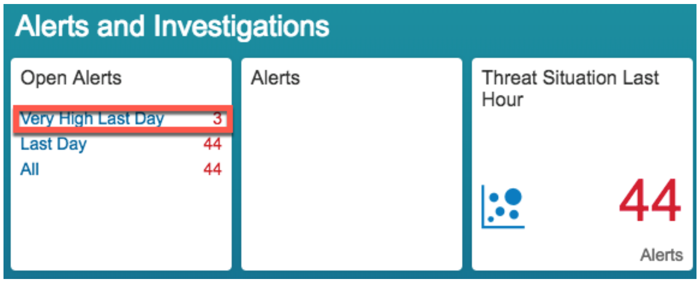
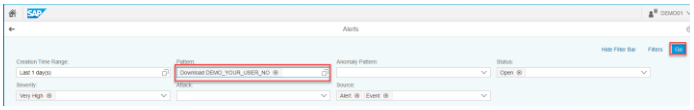
Then you may need to collect the evidences and to follow a Standard Operation Procedure for the further actions.

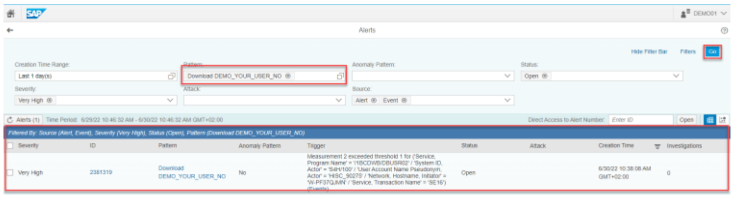
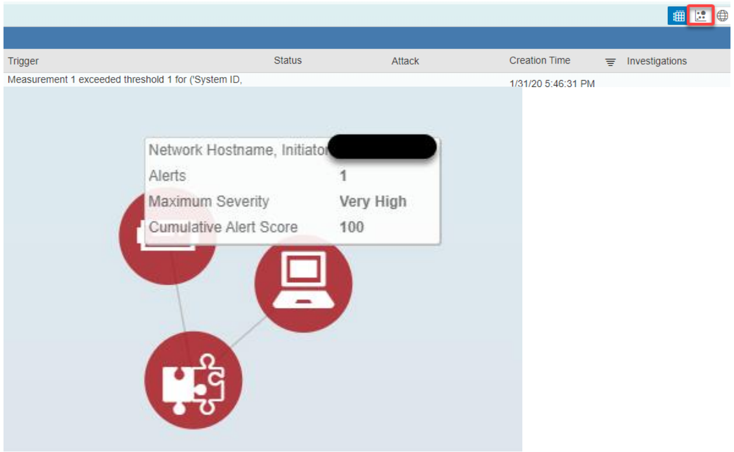
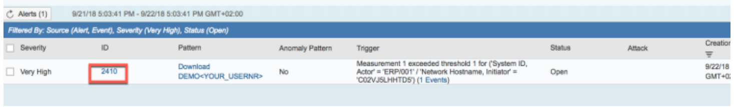
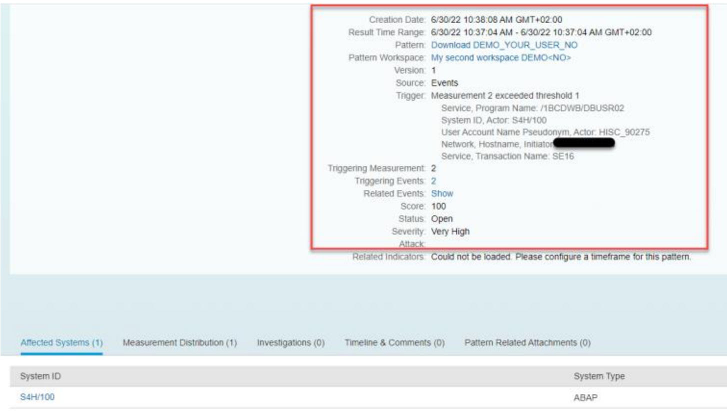
Tool Aspect: SAP Enterprise Threat Detection raises alerts as notification for potential attacks as they are happening. An alert includes references to the log events and the attack detection patterns or the anomaly detection patterns that led to its creation. Alerts are processed and analyzed by making use of various applications provided by SAP Enterprise Threat Detection. After your analysis of an alert, you can mark it as an attack, or a suspected attack and you can add it to an investigation. Investigations are collections of related material such as alerts, related events, case files, and snapshots. They are the central item with which more than one person might work with (e.g. monitoring agents and/or security experts).

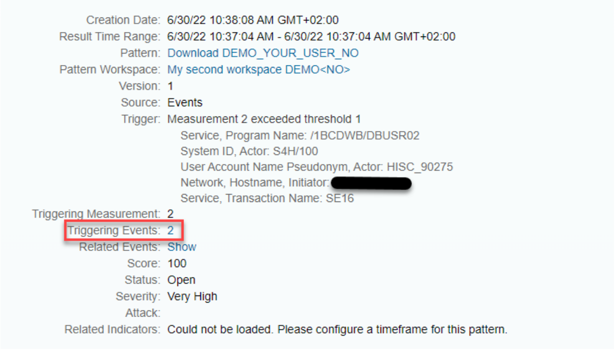
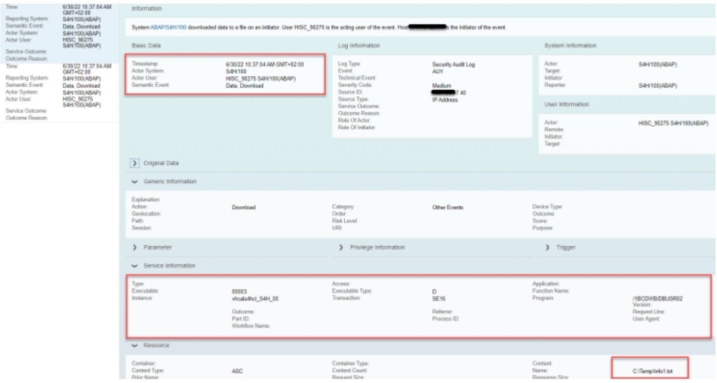
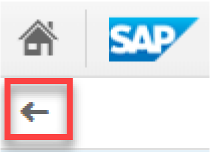
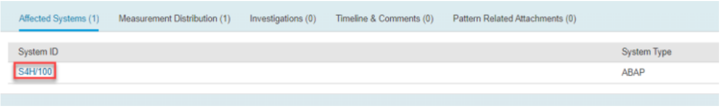
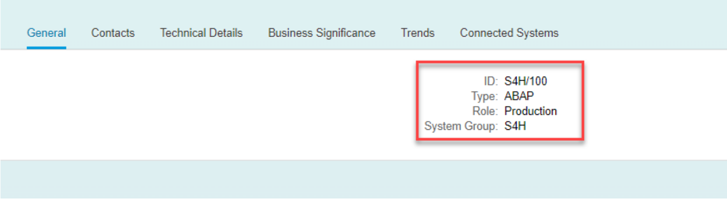
3.1. Viewing Alerts

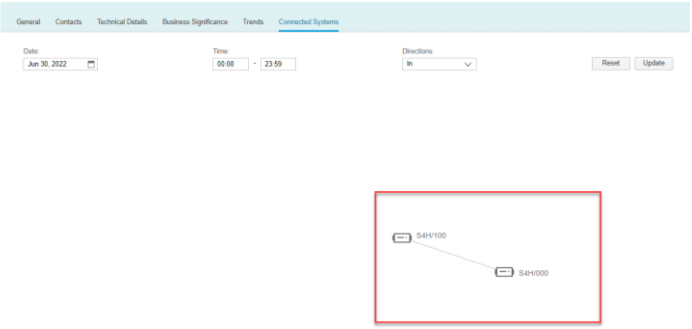
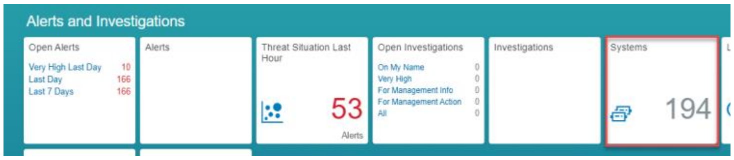
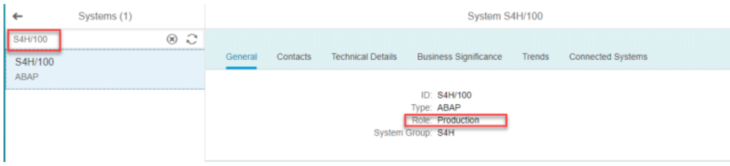
As the monitoring agent of a company, you need to monitor the alerts and react immediately. In the case of a suspected attack, it is usually the user or the hostname behind it or the system affected that you need to identify.

In this exercise you will learn how alerts are viewed and how an investigation is started in case of a suspected attack.

Explanation	Screenshot
73. Open tile *Open Alerts – Very High Last Day,* or as well click on the *Alerts* Tile, if no severity 'very high' alerts are available.	 Alerts and Investigations Open Alerts Very High Last Day 3 Last Day 44 All 44 Alerts Threat Situation Last Hour 44 Alerts
74. Open Filter Bar. Add the pattern you have created until step 71 as filter and push button *GO.* *CriticalFunctionModuleCalls<DEMO_UserNO>* *Comment:* *This is only needed for this exercise due to having multiple users working on the same exercise. In generals the Alerts List User Interface is used as a worklist for alerts by the monitoring agent.*	 Creation Time Range: Last 1 day(s) Pattern: Download DEMO_YOUR_USER_NO Anomaly Pattern: Status: Open Severity: Very High Attack: Source: Alert Event

Explanation	Screenshot
75. Look at the alert that has been raised. The severity of the alert provides the firsts indication how to prioritize the worklist of a monitoring agent. Under column ‘Trigger’ you can see the system on which a critical function module was executed.	 DEMO01 Alerts Hide Filter Bar Filters Go Creation Time Range: Last 1 day(s) Pattern: Download DEMO_YOUR_USER_NO Anomaly Pattern: Status: Open Severity: Very High Attack: Source: Alert Event Alerts (1) Time Period: 6/29/22 10:46:32 AM - 6/30/22 10:46:32 AM GMT+02:00 Direct Access to Alert Number: Enter ID Open *Filtered By: Source (Alert, Event), Severity (Very High), Status (Open), Pattern (Download DEMO_YOUR_USER_NO)* Severity | ID | Pattern | Anomaly Pattern | Trigger | Status | Attack | Creation Time | Investigations Very High | 2381319 | Download DEMO_YOUR_USER_NO | No | Measurement 2 exceeded threshold 1 for ('Service, Program Name' = '/1BCDWB/DBUSR02' / 'System ID, Actor' = 'S4H/100' / 'User Account Name Pseudonym, Actor' = 'HISC_90275' / 'Network, Hostname, Initiator' = 'W-PF37QJMN' / 'Service, Transaction Name' = 'SE16') (Events) | Open | | 6/30/22 10:38:08 AM GMT+02:00 | 0
76. Push button *View Threat Situation* and see e.g. the *Network Hostname Initiator* that has been used for downloading data.	 Trigger | Status | Attack | Creation Time | Investigations Measurement 1 exceeded threshold 1 for ('System ID, | | | 1/31/20 5:46:31 PM Network Hostname, Initiator [redacted] Alerts 1 Maximum Severity Very High Cumulative Alert Score 100
77. Switch back to the *Alerts List View* and click on alert *ID* to see more details about the alerts	 Alerts (1) 9/21/18 5:03:41 PM - 9/22/18 5:03:41 PM GMT+02:00 *Filtered By: Source (Alert, Event), Severity (Very High), Status (Open)* Severity | ID | Pattern | Anomaly Pattern | Trigger | Status | Attack | Creatio Very High | 2410 | Download DEMO<YOUR_USERNR> | No | Measurement 1 exceeded threshold 1 for ('System ID, Actor' = 'ERP/001' / 'Network Hostname, Initiator' = 'C02VJ5LHHTD5') (1 Events) | Open | | 9/22/18 GMT+0
78. Look at the header Information of the alerts. It shows basic data about the alert such as the pattern it was created by or by which metrics the alert has been triggered. Use the links to see the details of the alert.	 Creation Date: 6/30/22 10:38:08 AM GMT+02:00 Result Time Range: 6/30/22 10:37:04 AM - 6/30/22 10:37:04 AM GMT+02:00 Pattern: Download DEMO_YOUR_USER_NO Pattern Workspace: My second workspace DEMO<NO> Version: 1 Source: Events Trigger: Measurement 2 exceeded threshold 1 Service, Program Name: /1BCDWB/DBUSR02 System ID, Actor: S4H/100 User Account Name Pseudonym, Actor: HISC_90275 Network, Hostname, Initiator [redacted] Service, Transaction Name: SE16 Triggering Measurement: 2 Triggering Events: 2 Related Events: Show Score: 100 Status: Open Severity: Very High Attack: Related Indicators: Could not be loaded. Please configure a timeframe for this pattern. Affected Systems (1) Measurement Distribution (1) Investigations (0) Timeline & Comments (0) Pattern Related Attachments (0) System ID | System Type S4H/100 | ABAP

Explanation	Screenshot
79. Click on the *Triggering Events* to see more details.	 Creation Date: 6/30/22 10:38:08 AM GMT+02:00 Result Time Range: 6/30/22 10:37:04 AM - 6/30/22 10:37:04 AM GMT+02:00 Pattern: Download DEMO_YOUR_USER_NO Pattern Workspace: My second workspace DEMO<NO> Version: 1 Source: Events Trigger: Measurement 2 exceeded threshold 1 Service, Program Name: /1BCDWB/DBUSR02 System ID, Actor: S4H/100 User Account Name Pseudonym, Actor: HISC_90275 Network, Hostname, Initiator: [redacted] Service, Transaction Name: SE16 Triggering Measurement: 2 Triggering Events: 2 Related Events: Show Score: 100 Status: Open Severity: Very High Attack: Related Indicators: Could not be loaded. Please configure a timeframe for this pattern.
80. See the details of the events that has led to the alert creation e.g. the system where a suspicious activity has been detected or the transaction in which the download was executed.	 Time: 6/30/22 10:37:04 AM GMT+02:00 Reporting System: S4H/100(ABAP) Semantic Event: Data, Download Actor System: S4H/100(ABAP) Actor User: HISC_90275 S4H/100(ABAP) Service Outcome: Outcome Reason: Time: 6/30/22 10:37:04 AM GMT+02:00 Reporting System: S4H/100(ABAP) Semantic Event: Data, Download Actor System: S4H/100(ABAP) Actor User: HISC_90275 S4H/100(ABAP) Service Outcome: Outcome Reason: Information System ABAP/S4H/100 downloaded data to a file on an initiator. User HISC_90275 is the acting user of the event. Host[redacted]s the initiator of the event. Basic Data Timestamp: 6/30/22 10:37:04 AM GMT+02:00 Actor System: S4H/100 Actor User: HISC_90275 S4H/100(ABAP) Semantic Event: Data, Download Log Information Log Type: Security Audit Log Event: AUY Technical Event: Severity Code: Medium Source ID: [redacted]7.40 Source Type: IP Address Service Outcome: Outcome Reason: Role Of Actor: Role Of Initiator: System Information Actor: S4H/100(ABAP) Target: Initiator: Reporter: S4H/100(ABAP) User Information Actor: HISC_90275 S4H/100(ABAP) Remote: Initiator: Target: Original Data Generic Information Explanation: Action: Download Geolocation: Path: Session: Category: Other Events Order: Risk Level: URI: Device Type: Outcome: Score: Purpose: Parameter Privilege Information Trigger Service Information Type: Executable: 00003 Instance: vhcals4hci_S4H_00 Outcome: Part ID: Workflow Name: Access: Executable Type: D Transaction: SE16 Referrer: Process ID: Application: Function Name: Program: /1BCDWB/DBUSR02 Version: Request Line: User Agent: Resource Container: Content Type: ASC Prior Name: Container Type: Content Count: Request Size: Content: Name: C:\Temp\Info1.txt Response Size:
81. Click on button *Back* to return to the alert details view.	
82. Click on *System ID* to see the details of the affected system.	 Affected Systems (1) Measurement Distribution (1) Investigations (0) Timeline & Comments (0) Pattern Related Attachments (0) System ID: S4H/100 System Type: ABAP
83. Look at the details of the affected system.	 General Contacts Technical Details Business Significance Trends Connected Systems ID: S4H/100 Type: ABAP Role: Production System Group: S4H

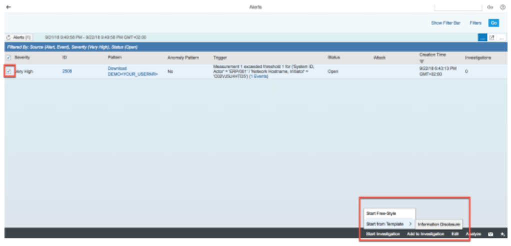
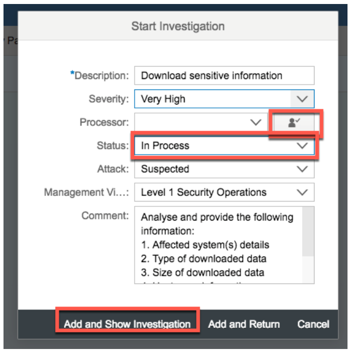
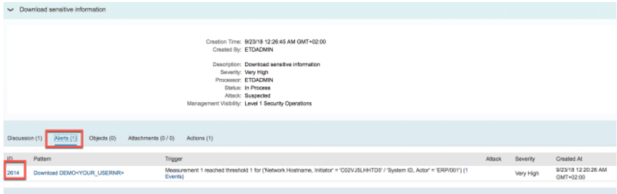
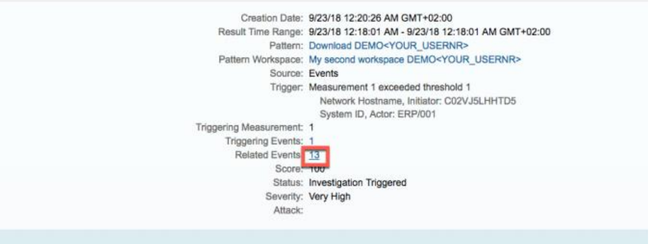
Explanation	Screenshot
84. Under tab *Connected Systems* you can see that the affected system has done a remote communication.	 General Contacts Technical Details Business Significance Trends Connected Systems Reset Update S4H/100 S4H/000 Date: Jun 30, 2022 Time: 00:00 - 23:59 Directions: In
85. Open a new browser tab and open SAP Enterprise Threat Detect Launchpad. Open tile *Systems* to see the details of the system to which a remote communication has taken place.	 Alerts and Investigations Open Alerts Very High Last Day 10 Last Day 166 Last 7 Days 166 Alerts Threat Situation Last Hour 53 Alerts Open Investigations On My Name 0 Very High 0 For Management Info 0 For Management Action 0 All 0 Investigations Systems 194
86. Enter the System ID in the search field an select the system to see the details. *(Hint: if there are too many systems in the ETD system, the filter only works for the shown Systems in the list. In case the system S4H/100 is not found, please page down until it is shown)*	 General Contacts Technical Details Business Significance Trends Connected Systems Systems (1) S4H/100 S4H/100 ABAP System S4H/100 ID: S4H/100 Type: ABAP Role: Production System Group: S4H

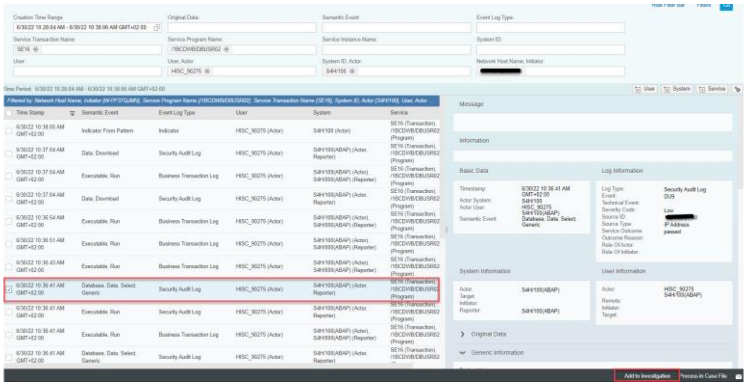
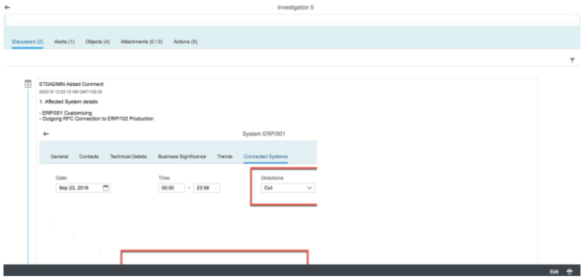
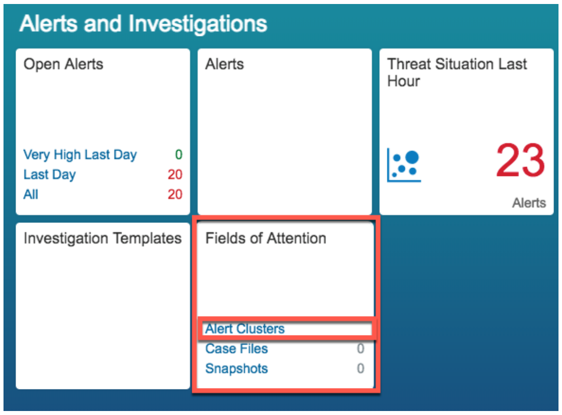
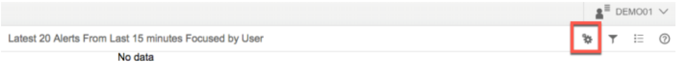
3.2. Investigating Alerts

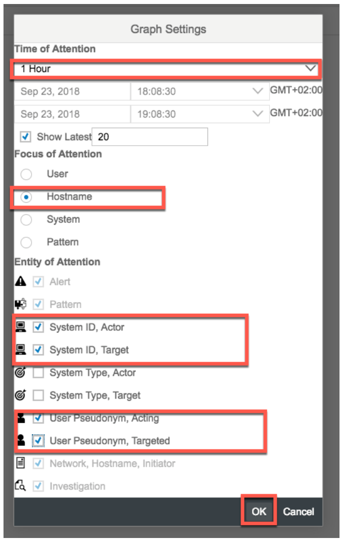
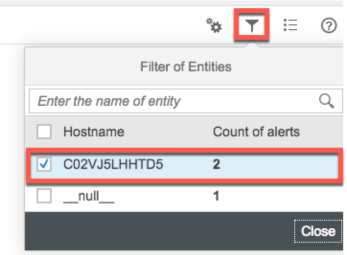
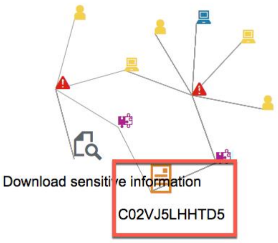
Investigations are collections of related material such as alerts, case files, and snapshots. They are the central item with which the monitoring agents and/or the security expert starts his forensic research, as they can lead to an incident.

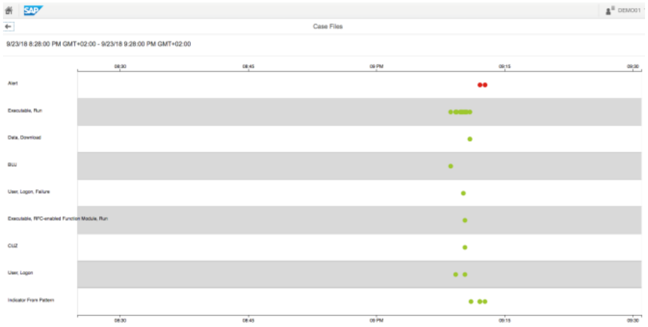
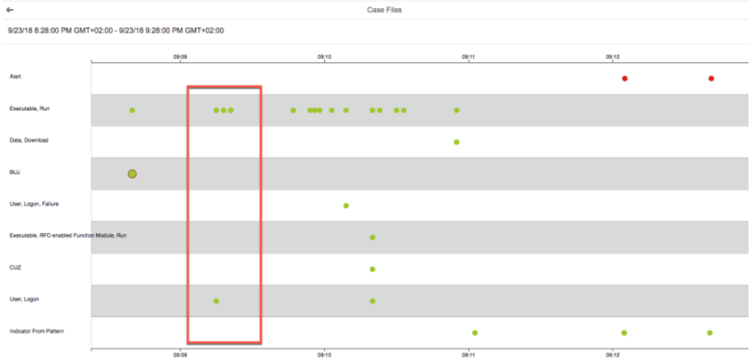
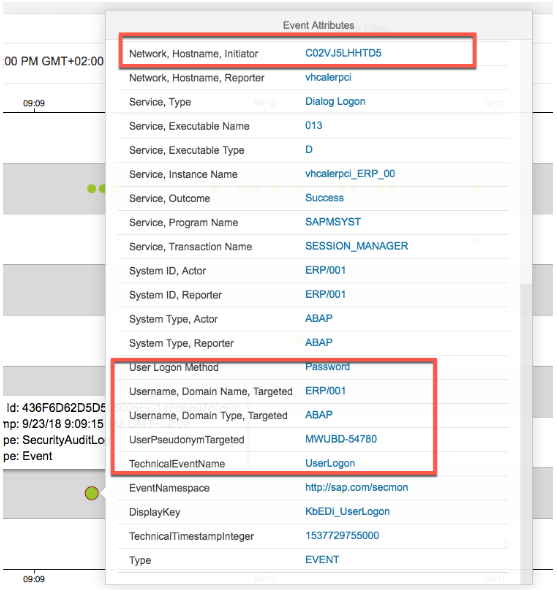
When the monitoring agent considers an alert suspicious, an investigation gets started. The investigation gets a description, a severity, a status and comments can be added. The investigation can be shared easily, either in emails or as tiles in the launchpad, or even as a PDF file. More alerts and other related material can be added later, and the status can be changed in order to make tracking of the investigation easy. It is also possible to create a CSV file with a list of all triggering or related events of the alerts in the investigation.

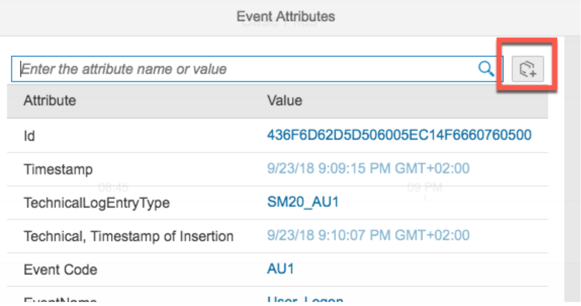
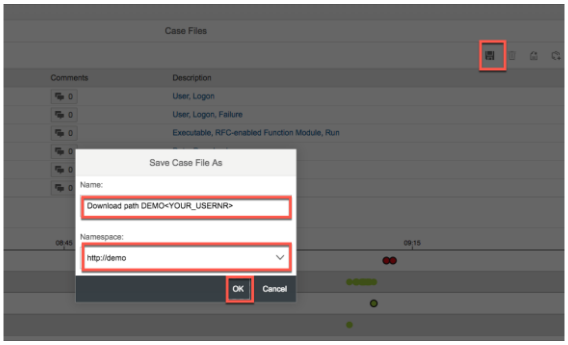
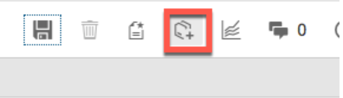
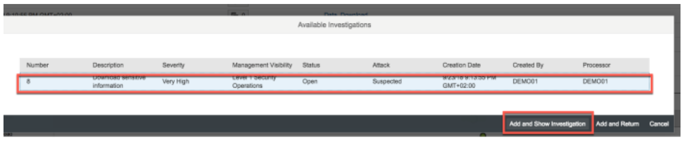
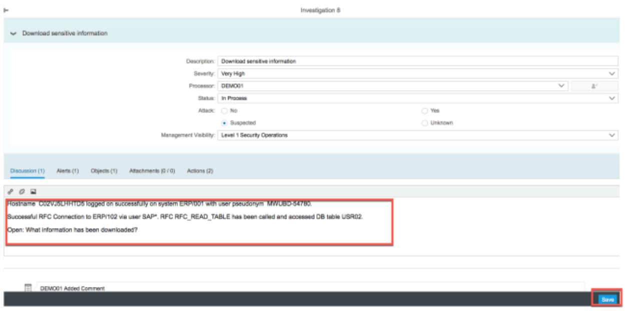
As the investigation is an item that more than one person might work with, there is a discussion and timeline tab in which manual comments as well as changes to the investigation are tracked.

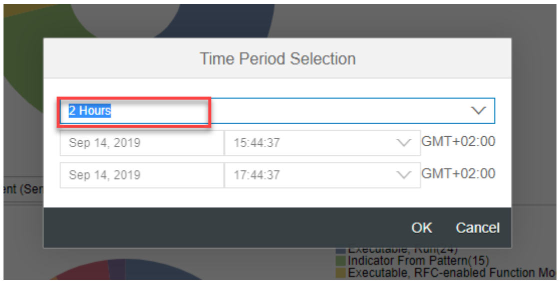
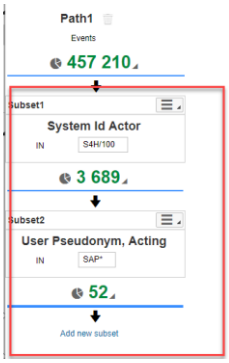
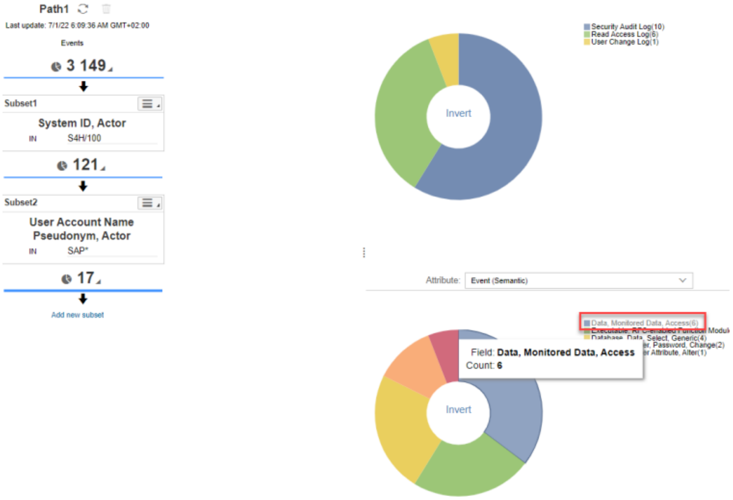
Explanation	Screenshot
87. In the Alerts worklist view, select the alert and push button *Start Investigation.* Choose *Start From Template → Information Disclosure* **INFORMATION:** The Investigation Popup should be prefilled from the template, but as to a software bug, this automated filling does not happen. By that please fill in: • Description: Download sensitive information • Severity: Very High • Status: In Process • Attack: Suspected • Management Visibility: Level 1 Security Operations • Comment: <Any comment you want>	 Alerts (1) 9/21/18 9:49:58 PM - 9/22/18 9:49:58 PM GMT+02:00 Filtered By: Source (Alert, Event), Severity (Very High), Status (Open) Severity ID Pattern Anomaly Pattern Trigger Status Attack Creation Time Investigations Very High 2508 Download DEMO<YOUR_USERNR> No Measurement 1 exceeded threshold 1 for ('System ID, Actor' = 'ERP/001' / 'Network Hostname, Initiator' = 'C02VJ5LHHTD5') (1 Events) Open 9/22/18 6:43:13 PM GMT+02:00 0 Alerts Go Show Filter Bar Filters Go Start Free-Style Start from Template Information Disclosure Start Investigation Add to Investigation Edit Analyze
88. Set yourself as processor of the investigation, set the Status to In Process and check the instructions how to handle this type of alert. Push button *Add and Show Investigation.*	 Start Investigation *Description: Download sensitive information Severity: Very High Processor: Status: In Process Attack: Suspected Management Vi...: Level 1 Security Operations Comment: Analyse and provide the following information: 1. Affected system(s) details 2. Type of downloaded data 3. Size of downloaded data
89. Click on tab *Alerts* and click on alert *ID* to further investigate details of the alert.	 Download sensitive information Creation Time: 9/23/18 12:26:45 AM GMT+02:00 Created By: ETDADMIN Description: Download sensitive information Severity: Very High Processor: ETDADMIN Status: In Process Attack: Suspected Management Visibility: Level 1 Security Operations ID Pattern Trigger Attack Severity Created At 2614 Download DEMO<YOUR_USERNR> Measurement 1 reached threshold 1 for ('Network Hostname, Initiator' = 'C02VJ5LHHTD5' / 'System ID, Actor' = 'ERP/001') (1 Events) Very High 9/23/18 12:20:26 AM GMT+02:00 Discussion (1) Alerts (1) Objects (0) Attachments (0 / 0) Actions (1)
90. Click on related events to gain more insight about the potential threat.	 Creation Date: 9/23/18 12:20:26 AM GMT+02:00 Result Time Range: 9/23/18 12:18:01 AM - 9/23/18 12:18:01 AM GMT+02:00 Pattern: Download DEMO<YOUR_USERNR> Pattern Workspace: My second workspace DEMO<YOUR_USERNR> Source: Events Trigger: Measurement 1 exceeded threshold 1 Network Hostname, Initiator: C02VJ5LHHTD5 System ID, Actor: ERP/001 Triggering Measurement: 1 Triggering Events: 1 Related Events: 13 Score: 100 Status: Investigation Triggered Severity: Very High Attack:

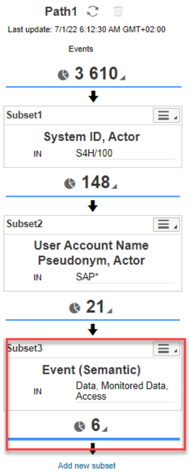
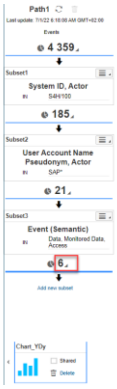
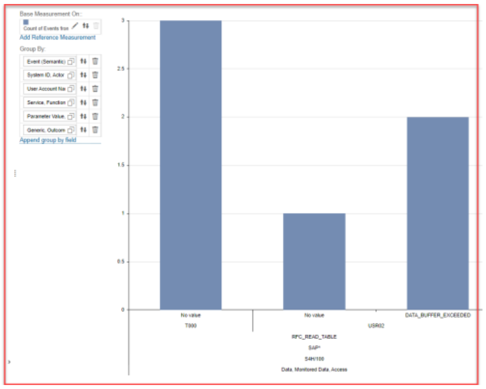
Explanation	Screenshot
91. Select the event row to see more details. Add to your investigation if relevant.	 Creation Time Range: 6/30/22 10:28:04 AM - 6/30/22 10:38:06 AM GMT+02:00 Original Data: Semantic Event: Event Log Type: Service Transaction Name: SE16 Service Program Name: /1BCDWB/DBUSR02 Service Instance Name: System ID: User: User, Actor: HISC_90275 System ID, Actor: S4H/100 Network Host Name, Initiator: [redacted] Time Period: 6/30/22 10:28:04 AM - 6/30/22 10:38:06 AM GMT+02:00 Filtered by: Network Host Name, Initiator (W-PF37QJMN), Service Program Name (/1BCDWB/DBUSR02), Service Transaction Name (SE16), System ID, Actor (S4H/100), User, Actor ... Time Stamp; Semantic Event; Event Log Type; User; System; Service 6/30/22 10:38:05 AM GMT+02:00; Indicator From Pattern; Indicator; HISC_90275 (Actor); S4H/100 (Actor); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:37:04 AM GMT+02:00; Data, Download; Security Audit Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor, Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:37:04 AM GMT+02:00; Executable, Run; Business Transaction Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor), S4H/000(ABAP) (Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:37:04 AM GMT+02:00; Data, Download; Security Audit Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor, Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:54 AM GMT+02:00; Executable, Run; Business Transaction Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor), S4H/000(ABAP) (Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:51 AM GMT+02:00; Executable, Run; Business Transaction Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor), S4H/000(ABAP) (Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:43 AM GMT+02:00; Executable, Run; Business Transaction Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor), S4H/000(ABAP) (Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) ☑ 6/30/22 10:36:41 AM GMT+02:00; Database, Data, Select, Generic; Security Audit Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor, Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:41 AM GMT+02:00; Executable, Run; Security Audit Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor, Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:41 AM GMT+02:00; Executable, Run; Business Transaction Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor), S4H/000(ABAP) (Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 (Program) 6/30/22 10:36:41 AM GMT+02:00; Database, Data, Select, Generic; Security Audit Log; HISC_90275 (Actor); S4H/100(ABAP) (Actor, Reporter); SE16 (Transaction), /1BCDWB/DBUSR02 Message Information Basic Data Timestamp: 6/30/22 10:36:41 AM GMT+02:00 Actor System: S4H/100 Actor User: HISC_90275 S4H/100(ABAP) Semantic Event: Database, Data, Select, Generic Log Information Log Type: Security Audit Log Event: DU9 Technical Event: Severity Code: Low Source ID: [redacted] Source Type: IP Address Service Outcome: passed Outcome Reason: Role Of Actor: Role Of Initiator: System Information Actor: S4H/100(ABAP) Target: Initiator: Reporter: S4H/100(ABAP) User Information Actor: HISC_90275 S4H/100(ABAP) Remote: Initiator: Target: Hide Filter Bar Filters Go User System Service Original Data Generic Information Add to Investigation Process in Case File
92. Update Investigations with your current investigation analysis results. E.g. use the tab discussions and add comments or screenshots to affected system details, size of downloaded data, hostname or user information. Screenshots can be added via Drag & Drop. *(In the picture on the right you see a screenshot which is pasted into the comment field)*	 Investigation 5 ETDADMIN Added Comment 9/23/18 12:52:15 AM GMT+02:00 1. Affected System details - ERP/001 Customizing - Outgoing RFC Connection to ERP/102 Production System ERP/001 Date: Sep 23, 2018 Time: 00:00 - 23:59 Directions: Out Discussion (2) Alerts (1) Objects (4) Attachments (0 / 0) Actions (5) General Contacts Technical Details Business Significance Trends Connected Systems Edit
93. Make use of Alert Clusters to visualize alerts based on the users, hostnames, systems or patterns involved. Open a new browser tab and start SAP Enterprise Threat Detection Launchpad. Open tile *Fields of Attention – Alert Clusters.*	 Alerts and Investigations Open Alerts Very High Last Day 0 Last Day 20 All 20 Alerts Threat Situation Last Hour 23 Alerts Investigation Templates Fields of Attention Alert Clusters Case Files 0 Snapshots 0
94. Choose button *Settings.*	 Latest 20 Alerts From Last 15 minutes Focused by User No data

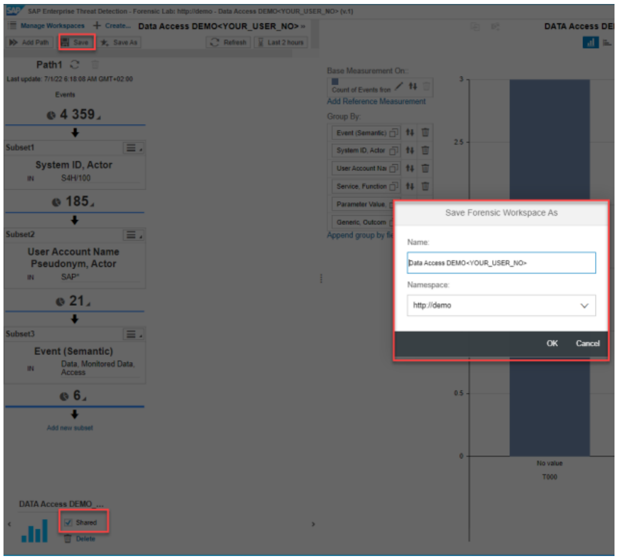
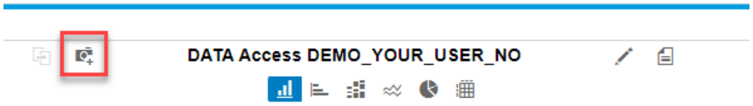
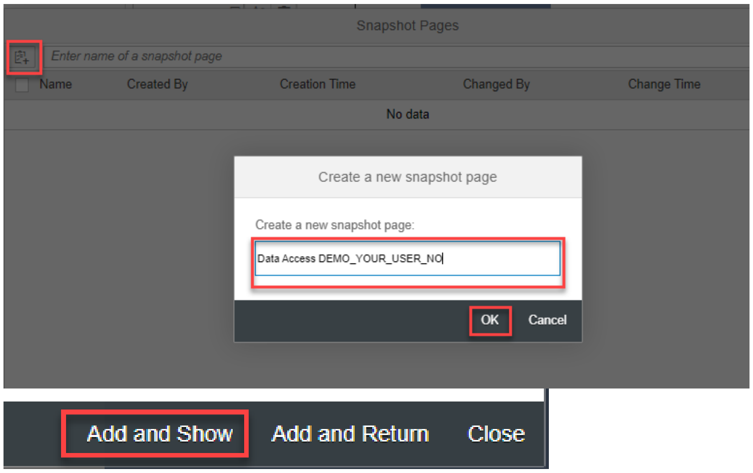
Explanation	Screenshot
95. Change Graph Settings as follows: Time range: *1 Hour* Focus of attention: *Hostname* Entity of attention: *System ID. Actor* *System ID, Target* *Account Name Pseudonym, Acting* *Account Name Pseudonym, Targeted* Push button *OK.*	 Graph Settings Time of Attention 1 Hour Sep 23, 2018 18:08:30 GMT+02:00 Sep 23, 2018 19:08:30 GMT+02:00 ☑ Show Latest 20 Focus of Attention ○ User ● Hostname ○ System ○ Pattern Entity of Attention ☑ Alert ☑ Pattern ☑ System ID, Actor ☑ System ID, Target □ System Type, Actor □ System Type, Target ☑ User Pseudonym, Acting ☑ User Pseudonym, Targeted ☑ Network, Hostname, Initiator ☑ Investigation OK Cancel
96. Push button *Filter* and only enable the hostname that has triggered the alerts.	 Filter of Entities Enter the name of entity □ Hostname Count of alerts ☑ C02VJ5LHHTD5 2 □ __null__ 1 Close
97. Look at the alert graph focusing on the selected hostname and see how it is connected to patterns, alerts and systems. Click on the hostname node to see further details.	

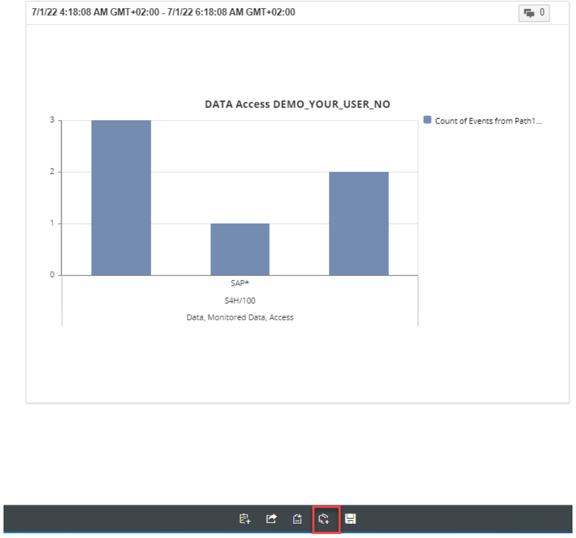
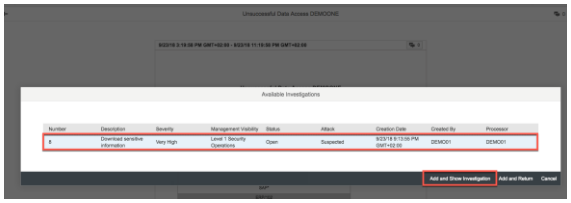
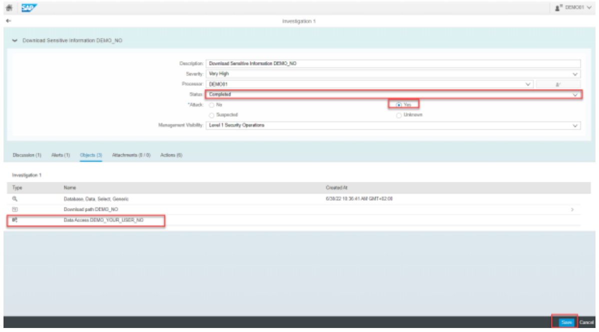
Explanation	Screenshot
98. Look at the alerts and events shown on the timeline where this hostname was involved.	 SAP DEMO01 Case Files 9/23/18 8:28:00 PM GMT+02:00 - 9/23/18 9:28:00 PM GMT+02:00 08:30 08:45 09 PM 09:15 09:30 Alert Executable, Run Data, Download BUJ User, Logon, Failure Executable, RFC-enabled Function Module, Run CUZ User, Logon Indicator From Pattern
99. You can slide and/or stretch the view to better visualize the events on the timeline. Start your analysis from left to right to get an understanding what has been done by the given hostname until the alerts have been raised.	 Case Files 9/23/18 8:28:00 PM GMT+02:00 - 9/23/18 9:28:00 PM GMT+02:00 09:09 09:10 09:11 09:12 Alert Executable, Run Data, Download BUJ User, Logon, Failure Executable, RFC-enabled Function Module, Run CUZ User, Logon Indicator From Pattern
100. Click on the circle to see the event details.	 Event Attributes Network, Hostname, Initiator: C02VJ5LHHTD5 Network, Hostname, Reporter: vhcalerpci Service, Type: Dialog Logon Service, Executable Name: 013 Service, Executable Type: D Service, Instance Name: vhcalerpci_ERP_00 Service, Outcome: Success Service, Program Name: SAPMSYST Service, Transaction Name: SESSION_MANAGER System ID, Actor: ERP/001 System ID, Reporter: ERP/001 System Type, Actor: ABAP System Type, Reporter: ABAP User Logon Method: Password Username, Domain Name, Targeted: ERP/001 Username, Domain Type, Targeted: ABAP UserPseudonymTargeted: MWUBD-54780 TechnicalEventName: UserLogon EventNamespace: http://sap.com/secmon DisplayKey: KbEDi_UserLogon TechnicalTimestampInteger: 1537729755000 Type: EVENT 00 PM GMT+02:00 09:09 Id: 436F6D62D5D5 np: 9/23/18 9:09:15 pe: SecurityAuditLo pe: Event

Explanation	Screenshot
101. Push button *Add to Case File* to add all relevant events that are related to the alert creation.	 Event Attributes *Enter the attribute name or value* Attribute — Value Id — 436F6D62D5D506005EC14F6660760500 Timestamp — 9/23/18 9:09:15 PM GMT+02:00 TechnicalLogEntryType — SM20_AU1 Technical, Timestamp of Insertion — 9/23/18 9:10:07 PM GMT+02:00 Event Code — AU1 EventName — User, Logon
102. Save your case file by pushing the button Save. Provide name and namespace as follows and push button *OK.* Name: Download path *DEMO<YOUR_USERNR>* Namespace: *http://demo*	 Case Files Comments — Description 0 — User, Logon 0 — User, Logon, Failure 0 — Executable, RFC-enabled Function Module, Run Save Case File As Name: Download path DEMO<YOUR_USERNR> Namespace: http://demo OK Cancel
103. Push button *Add to Investigation.*	
104. Select your investigation and push button *Add and Show Investigation.*	 Available Investigations Number: 8; Description: Download sensitive information; Severity: Very High; Management Visibility: Level 1 Security Operations; Status: Open; Attack: Suspected; Creation Date: 9/23/18 9:13:55 PM GMT+02:00; Created By: DEMO01; Processor: DEMO01 Add and Show Investigation · Add and Return · Cancel
105. Update the investigation Discussion with your analysis results.	 Investigation 8 Download sensitive information Description: Download sensitive information Severity: Very High Processor: DEMO01 Status: In Process Attack: ○ No ○ Yes ● Suspected ○ Unknown Management Visibility: Level 1 Security Operations Discussion (1) · Alerts (1) · Objects (1) · Attachments (0 / 0) · Actions (2) Hostname C02VJ5LHHTD5 logged on successfully on system ERP/001 with user pseudonym MWUBD-54780. Successful RFC Connection to ERP/102 via user SAP*. RFC RFC_READ_TABLE has been called and accessed DB table USR02. Open: What information has been downloaded? DEMO01 Added Comment Save

Explanation	Screenshot
106. Open forensic lab and change time range to last 2 hours. Analyze the log events and see if you can find further events related to the remote system and the SAP Standard user that has been mis-used.	 Time Period Selection 2 Hours Sep 14, 2019 15:44:37 GMT+02:00 Sep 14, 2019 17:44:37 GMT+02:00 OK Cancel Indicator From Pattern(15) Executable, RFC-enabled Function Mo
107. Create the following filters: System ID, Actor = *S4H/100* User Account Name Pseudonym, Acting = *SAP**	 Path1 Events 457 210 Subset1 System Id Actor IN S4H/100 3 689 Subset2 User Pseudonym, Acting IN SAP* 52 Add new subset
108. Look at the browsing chart for *Event (Semantic)* and see the event *Data, Monitored Data, Access.*	 Path1 Last update: 7/1/22 6:09:36 AM GMT+02:00 Events 3 149 Subset1 System ID, Actor IN S4H/100 121 Subset2 User Account Name Pseudonym, Actor IN SAP* 17 Add new subset Attribute: Event (Semantic) Field: **Data, Monitored Data, Access** Count: **6** Security Audit Log(10) Read Access Log(6) User Change Log(1) Invert Data, Monitored Data, Access(6) Executable, RFC-enabled Function Modul Database, Data, Select, Generic(4) er, Password, Change(2) er Attribute, Alter(1) Invert

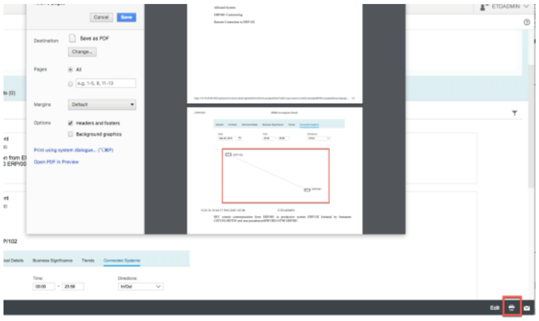
Explanation	Screenshot
109. Add a filter for this event.	 Path1 Last update: 7/1/22 6:12:30 AM GMT+02:00 Events 3 610 Subset1 System ID, Actor IN S4H/100 148 Subset2 User Account Name Pseudonym, Actor IN SAP* 21 Subset3 Event (Semantic) IN Data, Monitored Data, Access 6 Add new subset
110. Create a chart with the following *Group By* fields: *Event (Semantic)* *System ID, Actor* *User Account Pseudonym, Actor* *Service, Function Name* *Parameter Value, String* *Generic, Outcome*	 Path1 Last update: 7/1/22 6:18:08 AM GMT+02:00 Events 4 359 Subset1 System ID, Actor IN S4H/100 185 Subset2 User Account Name Pseudonym, Actor IN SAP* 21 Subset3 Event (Semantic) IN Data, Monitored Data, Access 6 Add new subset Chart_YDy □ Shared Delete  Base Measurement On:: Count of Events fron Add Reference Measurement Group By: Event (Semantic) System ID, Actor User Account Nai Service, Function Parameter Value, Generic, Outcom Append group by field 3 2.5 2 1.5 1 0.5 0 No value T000 No value DATA_BUFFER_EXCEEDED USR02 RFC_READ_TABLE SAP* S4H/100 Data, Monitored Data, Access

Explanation	Screenshot
111. Provide the following chart name. Chart name: *Data Access DEMO<YOUR_USERNR>* Enable checkbox *Shared* and push button *Save*. Provide the following workspace name. Name: *Unsuccessful Data Access DEMO<YOUR_USERNR>* Namespace: *http://demo*	 Save Forensic Workspace As Name: Data Access DEMO<YOUR_USER_NO> Namespace: http://demo
112. Push button *Add chart to snapshot page.*	 DATA Access DEMO_YOUR_USER_NO
113. Push button *Create a new snapshot page.* Provide the following snapshot page name and push button *Add and Show.* Snapshot page name: *Data Access DEMO<YOUR_USERNR>*	 Snapshot Pages Enter name of a snapshot page Name Created By Creation Time Changed By Change Time No data Create a new snapshot page Create a new snapshot page: Data Access DEMO_YOUR_USER_NO

Explanation	Screenshot
114. Push button *Add snapshot page to investigation.*	 7/1/22 4:18:08 AM GMT+02:00 - 7/1/22 6:18:08 AM GMT+02:00 0 DATA Access DEMO_YOUR_USER_NO Count of Events from Path1... 3 2 1 0 SAP* S4H/100 Data, Monitored Data, Access
115. Select your investigation and push button *Add and Show Investigation.*	 Unsuccessful Data Access DEMOONE 9/23/18 3:19:58 PM GMT+02:00 - 9/23/18 11:19:58 PM GMT+02:00 Available Investigations Number: 8; Description: Download sensitive information; Severity: Very High; Management Visibility: Level 1 Security Operations; Status: Open; Attack: Suspected; Creation Date: 9/23/18 9:13:56 PM GMT+02:00; Created By: DEMO01; Processor: DEMO01 Add and Show Investigation Add and Return Cancel
116. You find the Snapshot in the *Objects*-Tab of the Investigation Edit and update the investigation with your findings and close it.	 DEMO01 Investigation 1 Download Sensitive Information DEMO_NO Description: Download Sensitive Information DEMO_NO Severity: Very High Processor: DEMO01 Status: Completed *Attack: ○ No ● Yes ○ Suspected ○ Unknown Management Visibility: Level 1 Security Operations Discussion (1) Alerts (1) Objects (3) Attachments (0 / 0) Actions (6) Investigation 1 Type / Name / Created At Database, Data, Select, Generic — 6/30/22 10:36:41 AM GMT+02:00 Download path DEMO_NO Data Access DEMO_YOUR_USER_NO

3.3. Saving Evidence for Attacks

Print an investigation or save it to a PDF file. Such a PDF file can, for example, be used to attach an investigation to an external ticketing system.

Explanation	Screenshot
117. Within an investigation details push button *Print.* Push *Save* to save the content of an investigation as PDF file. This investigation can now be handed over to the Incident Management Team for further processing such as contacting the person behind the user pseudonym and contact system owner of production system to disable SAP Standard user SAP*.	 Destination □ Save as PDF Pages ● All ○ e.g. 1-5, 8, 11-13 Margins Default Options ☑ Headers and footers □ Background graphics Time: 00:00 - 23:59 Directions: In/Out ETDADMIN Cancel Save Change... Print using system dialogue... (⌥⌘P) Open PDF in Preview Business Significance Trends Connected Systems Edit

3.4. Summary

Security Aspect: As a Security Analyst you should be able to save the collected evidences to an investigation. You know now how to analyze the alert to avoid the false positives with several tools provided by ETD, and print the investigation in PFD format as a hard copy.

Tool Aspect: You learned how to view the Alerts, create an Investigation and assign alerts to it. You can find the User behind this alert using Threat Situation. You also know how to view the details of an Alert with its triggering Events, as well as add different objects to an investigation. You've got to know the advanced tools, such as Case Files.

4. PSEUDONYMIZATION OF USER DATA

Security Aspect: The users involved in a potential cyberattack are always the most interesting attributes for a Security Analyst. However, all the person-related data must be protected before the collected evidences indicating a real attack. SAP Enterprise Threat Detection replaces the real user ID with User Pseudonym so that no user can be identified during all phases of analysis. Only with very restrictive access right the User Pseudonym can be resolved to real user.

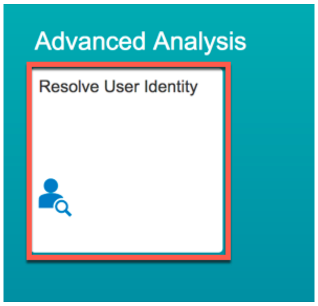
Tool Aspect: You will learn how to resolve the User Pseudonym.

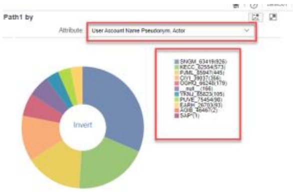
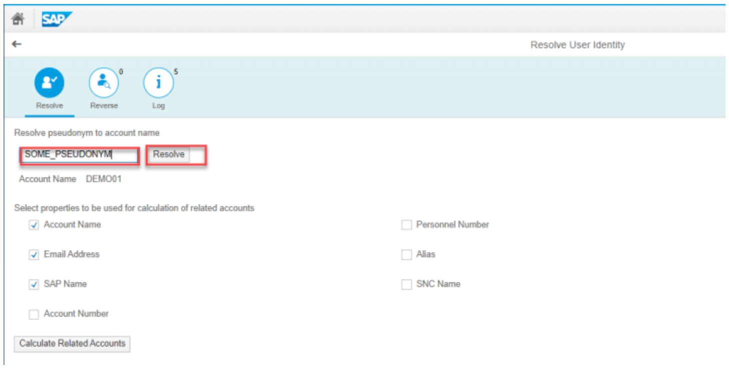
Pseudonymization is a procedure by which the user ID and other person-related data in a record is replaced by a pseudonym, so as to make it difficult or impossible to identify the person in question. In contrast to the anonymization procedure, pseudonymized data still references the original data.

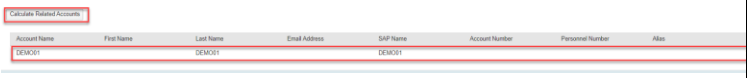
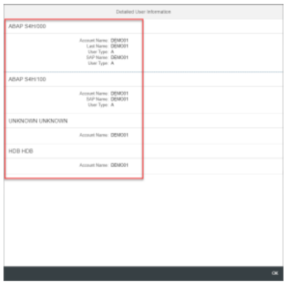
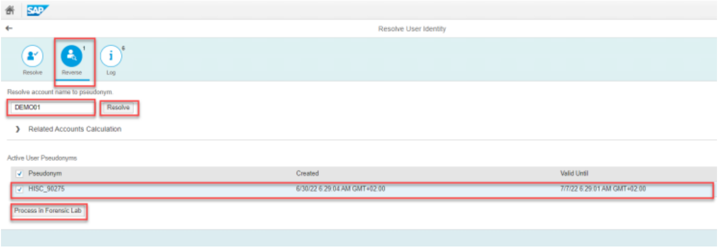
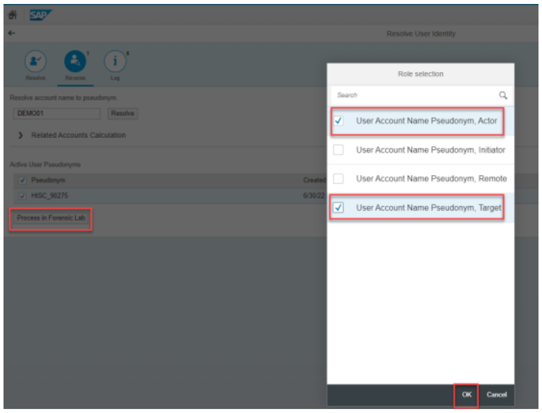
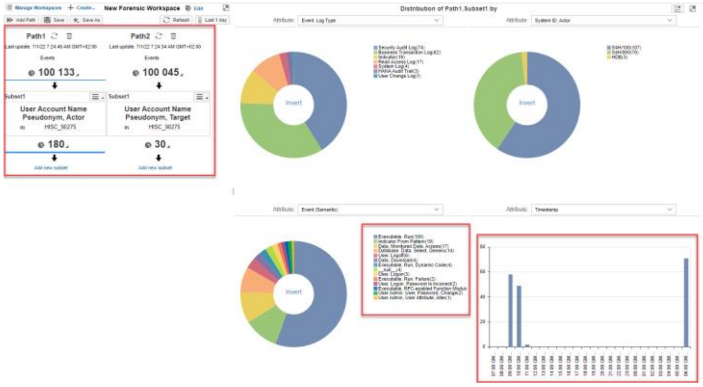
SAP Enterprise Threat Detection frequently changes the pseudonym associated with a user. The applications of SAP Enterprise Threat Detection, such as the forensic lab, can only access the current pseudonym of a user. You cannot use your past knowledge of user pseudonyms to pursue a user. SAP Enterprise Threat Detection protects this application with authorizations and records read-access to this data.

4.1. Determining the True Identity of Users

When suspicious events occur, you may be required to determine the true identity of the person behind the alias shown in the user interface. User Pseudonym can be resolved by authorized group of users only.

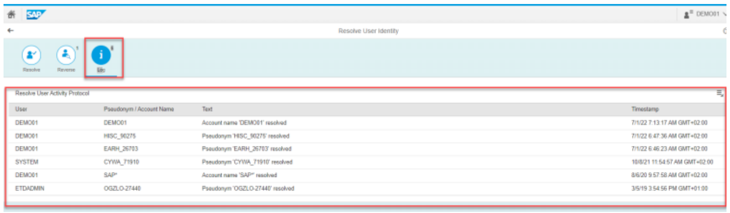
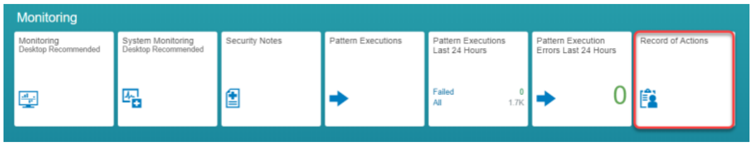
Explanation	**Screenshot**
118. Logon to SAP Enterprise Threat Detection Launchpad with the following user and open tile *Resolve User Identity* User: DEMO<*YOUR_USERNR*> Password: Welcome0	

119. Enter (a) user pseudonym and push button *OK. A* clear user name is then shown below
 	
Hint: You can e.g. find a user pseudonym in the alerts that were raised, or in Forensic Lab you can select one within a predefined visualization by e.g. viewing *User Account Name Pseudonym, Actor*

 Path1 by
Attribute: User Account Name Pseudonym, Actor
Invert
SNGM_63419(926)
KECC_82554(573)
PJML_35947(445)
OIYI_39037(356)
OGHQ_66248(179)
__null__(166)
TRNJ_85823(105)
PUVE_75454(98)
EARH_26703(93)
AGIB_46467(2)
SAP*(1)
	
	 SAP
	Resolve User Identity
	Resolve
	Reverse 0
	Log 5
	Resolve pseudonym to account name
	SOME_PSEUDONYM Resolve
	Account Name DEMO01
	Select properties to be used for calculation of related accounts
	☑ Account Name ☐ Personnel Number
	☑ Email Address ☐ Alias
	☑ SAP Name ☐ SNC Name
	☐ Account Number
	Calculate Related Accounts

Explanation	Screenshot
120. Additionally, you can calculate the corresponding, system dependent user accounts by clicking on the corresponding button *Calculate Related Amounts*.	 Calculate Related Accounts Account Name: DEMO01 · First Name: · Last Name: DEMO01 · Email Address: · SAP Name: DEMO01 · Account Number: · Personnel Number: · Alias:
121. When clicking onto the line(s) in the list, you can view the meta data coming from different systems.	 Detailed User Information ABAP S4H/000 Account Name: DEMO01 Last Name: DEMO01 User Type: A SAP Name: DEMO01 User Type: A ABAP S4H/100 Account Name: DEMO01 SAP Name: DEMO01 User Type: A UNKNOWN UNKNOWN Account Name: DEMO01 HDB HDB Account Name: DEMO01 OK
122. Additionally, there is the possibility to do a reverse resolution from a clear user name to the actual pseudonym.	 Resolve account name to pseudonym. DEMO01 Resolve Related Accounts Calculation Active User Pseudonyms ☑ Pseudonym · Created · Valid Until ☑ HISC_90275 · 6/30/22 6:29:04 AM GMT+02:00 · 7/7/22 6:29:01 AM GMT+02:00 Process in Forensic Lab
123. By clicking on Button *Process in Forensic Lab* you can directly filter on that user and check what the user did in different roles, e.g. as Actor, or as Target.	 Role selection Search ☑ User Account Name Pseudonym, Actor □ User Account Name Pseudonym, Initiator □ User Account Name Pseudonym, Remote ☑ User Account Name Pseudonym, Target OK Cancel
124. The result in the Forensic Lab looks like that.	 Manage Workspaces Create... New Forensic Workspace Edit Add Path Save Save As Refresh Last 1 day Distribution of Path1.Subset1 by Attribute: Event, Log Type Attribute: System ID, Actor Attribute: Event (Semantic) Attribute: Timestamp Invert Path1 · Last update: 7/1/22 7:24:46 AM GMT+02:00 · Events 100 133 Subset1: User Account Name Pseudonym, Actor IN HISC_90275 · 180 Add new subset Path2 · Last update: 7/1/22 7:24:34 AM GMT+02:00 · Events 100 045 Subset1: User Account Name Pseudonym, Target IN HISC_90275 · 30 Add new subset

4.2. Logging Access to User Identities

Personal user information is protected by local laws and regulations, SAP Enterprise Threat Detection logs when someone accesses this information.

Explanation	Screenshot
125. Click on tab *Log* and see the audit log for user resolutions Hint: The same information plus furthermore about who was doing what within ETD is found in Tile *Record of Actions*	 SAP DEMO01 Resolve User Identity Resolve Reverse Log  Monitoring Monitoring Desktop Recommended System Monitoring Desktop Recommended Security Notes Pattern Executions Pattern Executions Last 24 Hours Failed 0 All 1.7K Pattern Execution Errors Last 24 Hours 0 Record of Actions

Resolve User Activity Protocol

User	Pseudonym / Account Name	Text	Timestamp
DEMO01	DEMO01	Account name 'DEMO01' resolved	7/1/22 7:13:17 AM GMT+02:00
DEMO01	HISC_90275	Pseudonym 'HISC_90275' resolved	7/1/22 6:47:36 AM GMT+02:00
DEMO01	EARH_26703	Pseudonym 'EARH_26703' resolved	7/1/22 6:46:23 AM GMT+02:00
SYSTEM	CYWA_71910	Pseudonym 'CYWA_71910' resolved	10/8/21 11:54:57 AM GMT+02:00
DEMO01	SAP*	Account name 'SAP*' resolved	8/6/20 9:57:58 AM GMT+02:00
ETDADMIN	OGZLO-27440	Pseudonym 'OGZLO-27440' resolved	3/5/19 3:54:56 PM GMT+01:00

4.1. Summary

Security Aspect: As a User of a special authorized group you can find the real user behind a User Pseudonym.

Tool Aspect: You learned how to resolve a User with “Resolve User Identity”

5. MONITORING DASHBOARDS

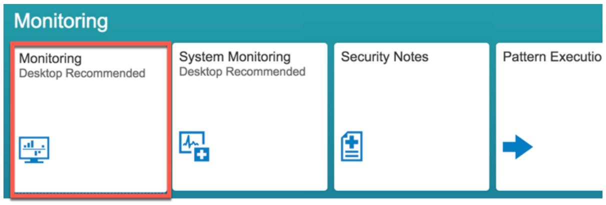
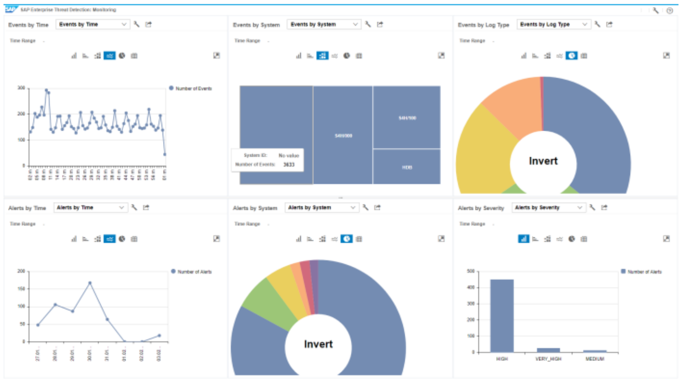
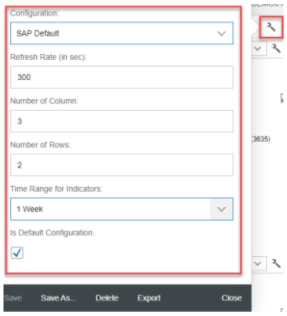
Security Aspect: During the daily operation of security monitoring a Security Agent needs to have an overview of the whole landscape. In ETD they include active alerts, the status of investigations and the log events. Since every agent has his own interested aspect, the content of the monitor must be able to be configured individually. In addition to the security related data he needs also an overview regarding the connected systems, to avoid unnecessary loss or delay of events.

Tool Aspect: Monitoring dashboards provide an overview of the events, alerts, and investigations in the system. The monitoring user interface is visualized for all users of SAP Enterprise Threat Detection. You can adjust the refresh rate, the number of charts and patterns displayed, and the time span monitored by the indicators of the Monitoring application. Monitoring dashboards can be customized the way you need.

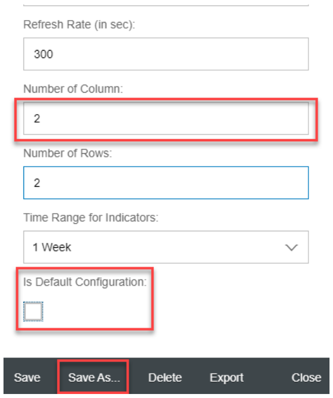
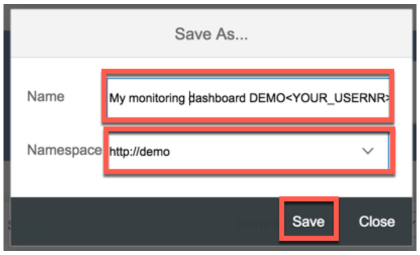
It is possible to define favorite monitoring dashboards by each individual user.

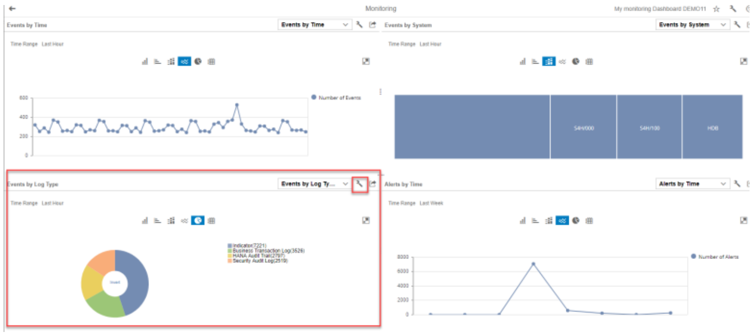
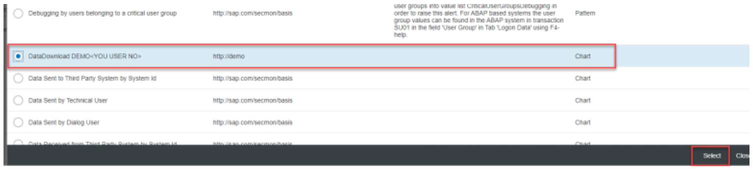
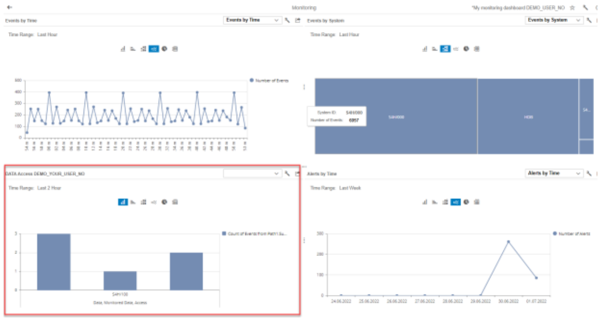
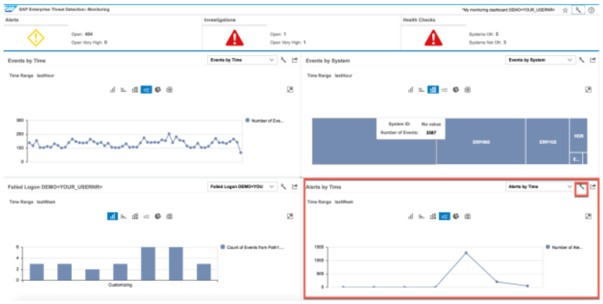
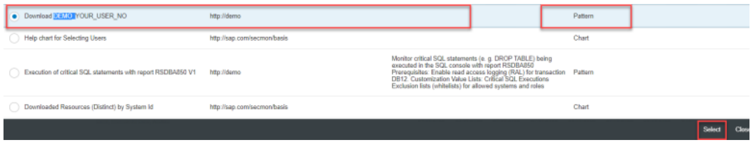
5.1. Viewing Default Monitoring Dashboard

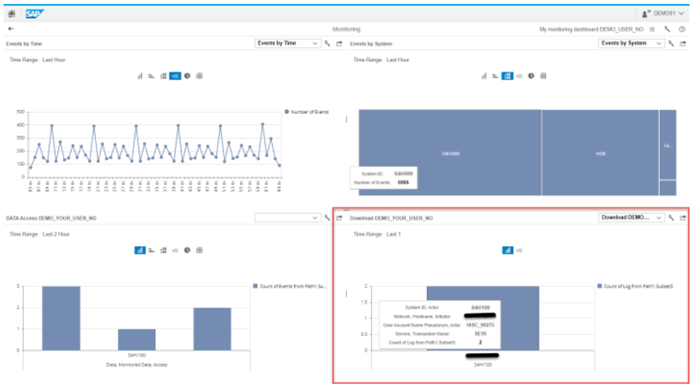
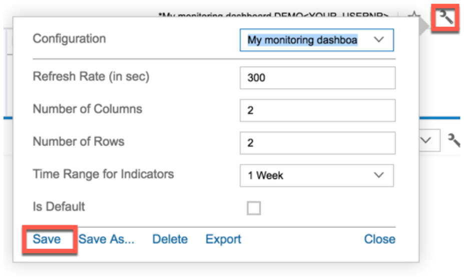
When opening the monitoring tile, a default monitoring dashboard is displayed. The default monitoring dashboard is typically used as a video wall.

Explanation	Screenshot
126. Open tile **Monitoring** in the SAP Enterprise Threat Detection Launchpad.	 Monitoring Monitoring Desktop Recommended System Monitoring Desktop Recommended Security Notes Pattern Executio
127. The initial screen shows the default monitoring dashboard with standard charts such as Events by Time, Events by System or Alerts by Severity. The default monitoring dashboard is typically used as a video wall.	 Events by Time Events by System Events by Log Type Invert Alerts by Time Alerts by System Alerts by Severity Invert HIGH VERY_HIGH MEDIUM
128. Click on the button *Setting* 🔧 to see configuration details of the default monitoring dashboard.	 Configuration: SAP Default Refresh Rate (in sec): 300 Number of Column: 3 Number of Rows: 2 Time Range for Indicators: 1 Week Is Default Configuration: ☑

5.2. Building your own Monitoring Dashboard

Explanation	Screenshot
129. Use the default monitoring dashboard to create your individual one. Change the values as follows and push button *Save As …* Number of Columns: *2* Number of Rows: *2* Is Default: *not checked*	 Refresh Rate (in sec): 300 Number of Column: 2 Number of Rows: 2 Time Range for Indicators: 1 Week Is Default Configuration: □
130. Enter the name and namespace and push button *Save.* Name: *My monitoring dashboard* DEMO***<YOUR_USERNR>*** Namespace: *http://demo*	 Save As... Name: My monitoring dashboard DEMO<YOUR_USERNR> Namespace: http://demo

Explanation	Screenshot
131. Push button *Settings* 🔧 to replace the left chart below.	 Monitoring My monitoring Dashboard DEMO11 Events by Time Events by System Time Range Last Hour Number of Events SAH000 SAN100 HDB Events by Log Type Events by Log Ty... Alerts by Time Time Range Last Week Indicator(7221) Business Transaction Log(3826) HANA Audit Trail(2797) Security Audit Log(2519) Number of Alerts
132. Search for your chart by scrolling through the list. Mark the chart you created and click on the Select Button	○ Debugging by users belonging to a critical user group — http://sap.com/secmon/basis — user groups into value list CriticalUserGroupsDebugging in order to raise this alert. For ABAP based systems the user group values can be found in the ABAP system in transaction SU01 in the field 'User Group' in Tab 'Logon Data' using F4-help. — Pattern ● DataDownload DEMO<YOU USER NO> — http://demo — Chart ○ Data Sent to Third Party System by System Id — http://sap.com/secmon/basis — Chart ○ Data Sent by Technical User — http://sap.com/secmon/basis — Chart ○ Data Sent by Dialog User — http://sap.com/secmon/basis — Chart ○ Data Received from Third Party System by System Id — http://sap.com/secmon/basis — Chart Select Clos
133. Look at left chart below that has been changed and updated	 Monitoring *My monitoring dashboard DEMO_USER_NO Events by Time Events by System Time Range Last Hour Number of Events SAH000 HDB DATA Access DEMO_YOUR_USER_NO Time Range Last 2 Hour Count of Events from Path1... Alerts by Time Time Range Last Week Number of Alerts
134. Push button *Settings* 🔧 to replace the right chart below.	 SAP Enterprise Threat Detection: Monitoring *My monitoring dashboard DEMO<YOUR_USERNR> Alerts Investigations Health Checks Events by Time Events by System Failed Logon DEMO<YOUR_USERNR> Count of Events from Path1... Customizing Alerts by Time Number of Ale...
135. Select one of your **patterns** and push button *Select.*	● Download DEMO YOUR_USER_NO — http://demo — Pattern ○ Help chart for Selecting Users — http://sap.com/secmon/basis — Chart ○ Execution of critical SQL statements with report RSDBA850 V1 — http://demo — Monitor critical SQL statements (e. g. DROP TABLE) being executed in the SQL console with report RSDBA850 Prerequisites: Enable read access logging (RAL) for transaction DB12. Customization Value Lists: Critical SQL Executions Exclusion lists (whitelists) for allowed systems and roles — Pattern ○ Downloaded Resources (Distinct) by System Id — http://sap.com/secmon/basis — Chart Select Clos

Explanation	Screenshot
136. Look at right chart below that has been changed and updated	 DEMO01 Monitoring My monitoring dashboard DEMO_USER_NO Events by Time Events by System Time Range: Last Hour Number of Events S4H/000 HDB System ID: S4H/000 Number of Events: 6966 DATA Access DEMO_YOUR_USER_NO Download DEMO_YOUR_USER_NO Download DEMO... Time Range: Last 2 Hour Time Range: Last 1 S4H/100
137. Click on the button Setting 🔧 and push button Save to save your monitoring dashboard.	 Configuration: My monitoring dashboa Refresh Rate (in sec): 300 Number of Columns: 2 Number of Rows: 2 Time Range for Indicators: 1 Week Is Default: □

5.1. Summary:

Security Aspect: As a Security Monitoring Agent you have learned that the Monitoring Dashboard is the most important tool for you to deal with your daily security monitoring task.

Tool Aspect: You learned how to open the default Monitoring Dashboard and customize it to fit your own need

www.sap.com/contactsap

© 2018 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. 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, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See https://www.sap.com/copyright for additional trademark information and notices.

THE BEST RUN SAP®