Secure the Intelligent Enterprise with SAP Enterprise Threat Detection

Exercise: Working with SAP Enterprise Threat Detection

TechEd Version 2021

Run Simple

TABLE OF CONTENTS

ETD Demo Users

- Usernames: Demo01, …, Demo29
- 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:

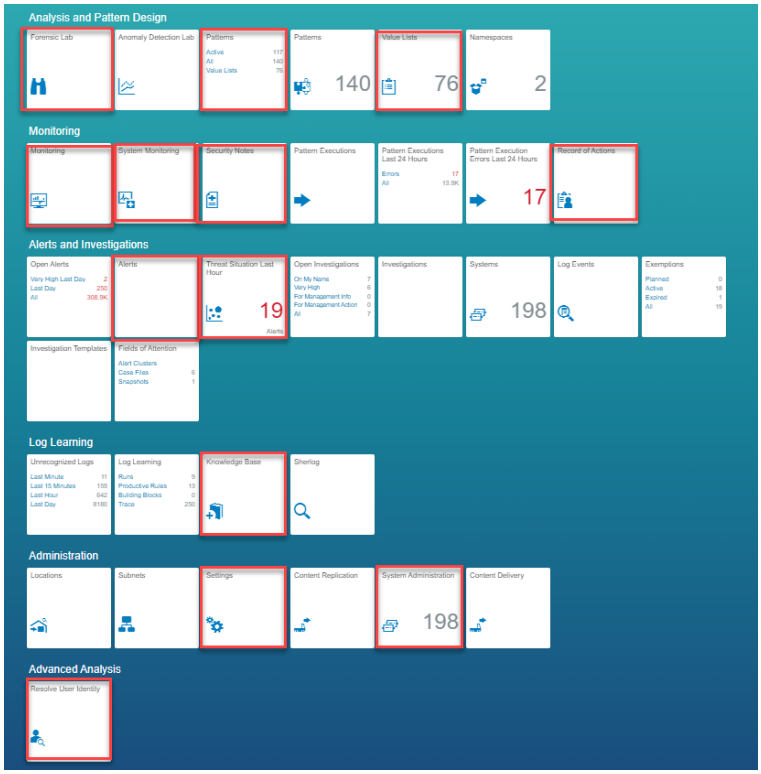
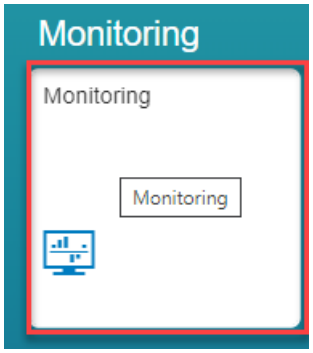
<Chart name> DEMO***<YOUR_USERNR>***

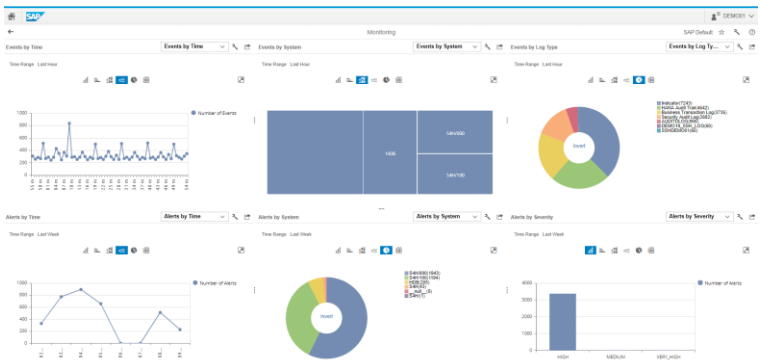
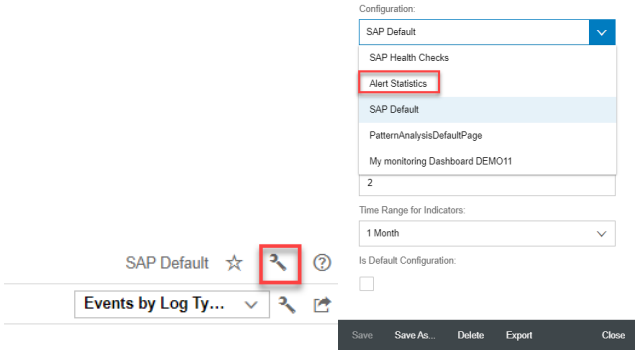
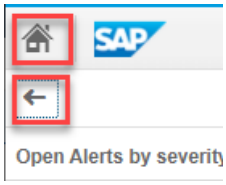
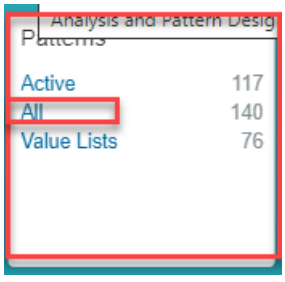
1. ETD USER – ETD ROUNDTRIP AND NAVIGATION

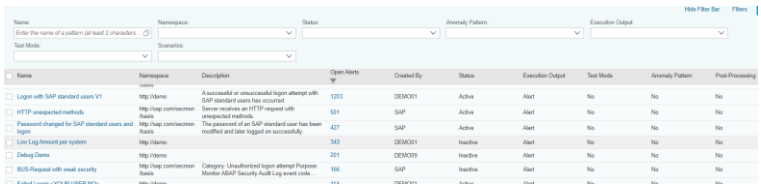
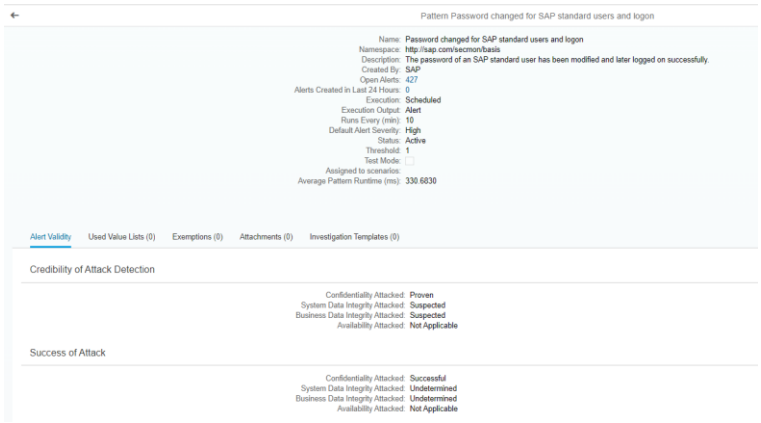
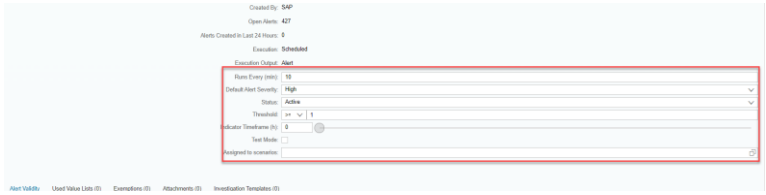
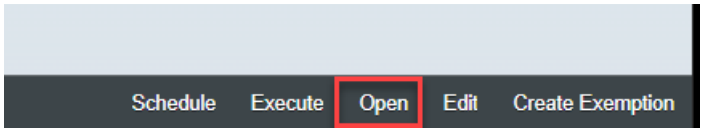
Tool Aspect: In this Exercise you as an ETD User will be able to navigate through the most important UIs of SAP Enterprise Threat Detection. You will get knowledge about different UIs like Monitoring, Alerts, Forensic Lab, Settings, (De-)Pseudonymization, Patterns, Value Lists, etc.

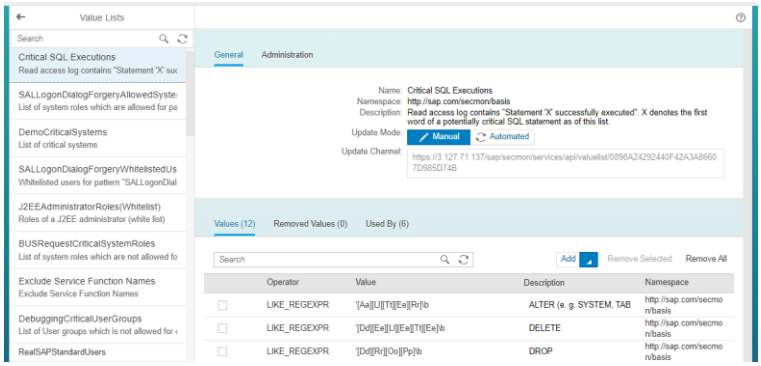
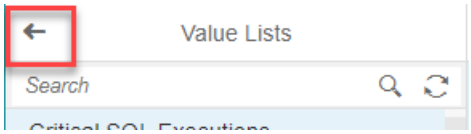
1.1. Start Page and Navigation to different tiles

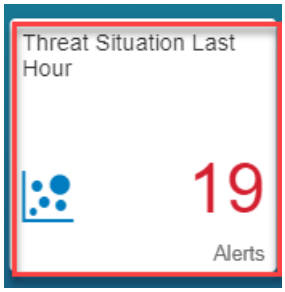
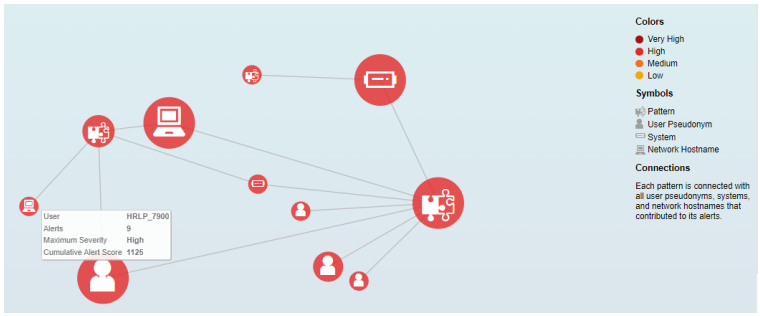
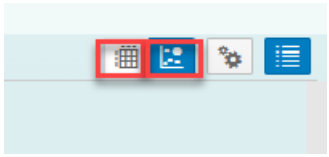
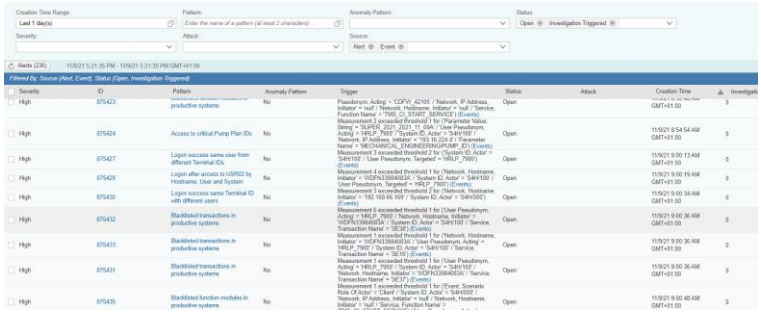
In this Exercise you will open the start page and click on several tiles to navigate forth and back

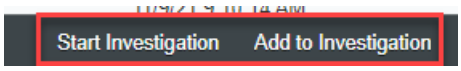
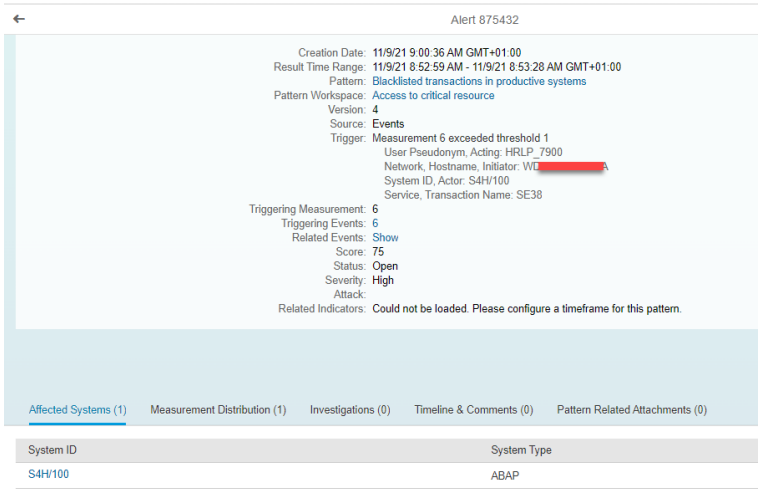
Explanation	Screenshot
1. After Logging on you are in the launch pad. In this exercise you will click on each of the red marked tiles to have a 1st look what's in there.	
2. Click on Tile Monitoring	

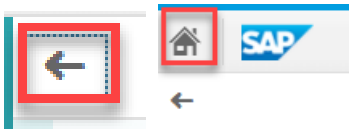
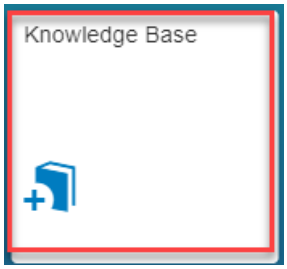
Explanation	Screenshot
3. The Default Monitoring page will be shown	
4. Click on the small tool icon in the upper right corner and select another Monitoring page (e.g. Alert Statistics). Another Monitoring page will be shown. In a later exercise you will learn how to create own monitoring pages with own charts.	
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’.	

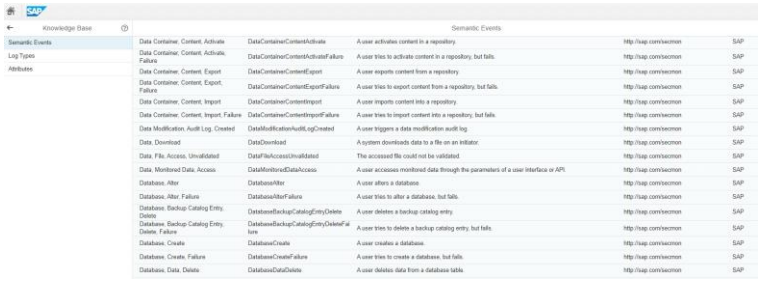
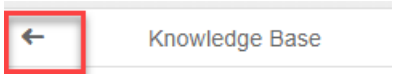
Explanation	Screenshot
7. You see the list of the patterns, with their current state, and how many alerts they raised.	
8. You can jump to the details of any pattern, by clicking on the pattern name in the list.	
9. When clicking on 'Edit', some parameter of the pattern can be changed, e.g.: a. Run frequency b. Severity c. Status (Active/Inactive) d. Threshold e. Test Mode Checkbox You can save via using the 'Save' button	
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.	

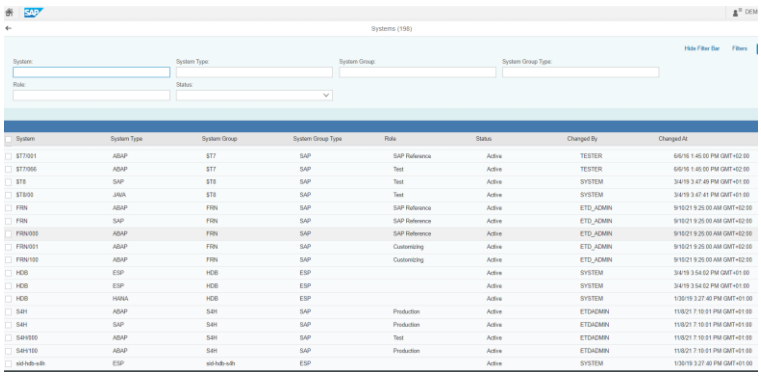
Explanation	Screenshot
11. Click the Home button to jump back to the launch pad.	
12. Klick on Tile ‘Value Lists’	
13. You see the list containing all value lists. A value list can act as a block-list or as an allow list. They are used as filter elements in patterns, all list entries are used to filter 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.	
14. Go back to launch pad via the left arrow	

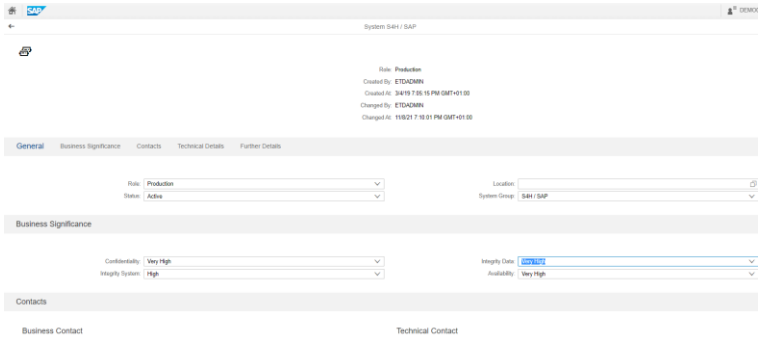
Explanation	Screenshot
15. Klick on Tile ‘Threat Situation Last Hour’.	
16. The UI shows the correlation between Users, Systems, Patterns, Alerts, End User Machine Hostnames. The bigger a circle, the more an entity is involved into the correlations. E.g. in the Screenshot the User Pseudonym HRLP_7900 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	
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	

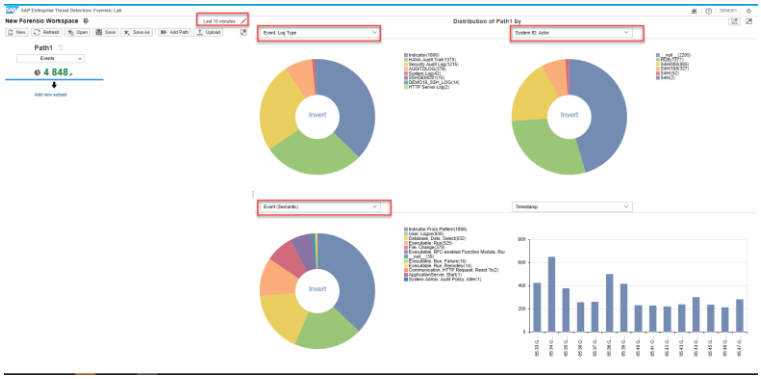
Explanation	Screenshot
19. In order to process alerts, you can mark several alerts belonging together (i.e. having the same root cause) and start an investigation (or add to an existing investigation). An investigation is the evidence collection object in ETD. It will be used for collecting all corelated 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.	

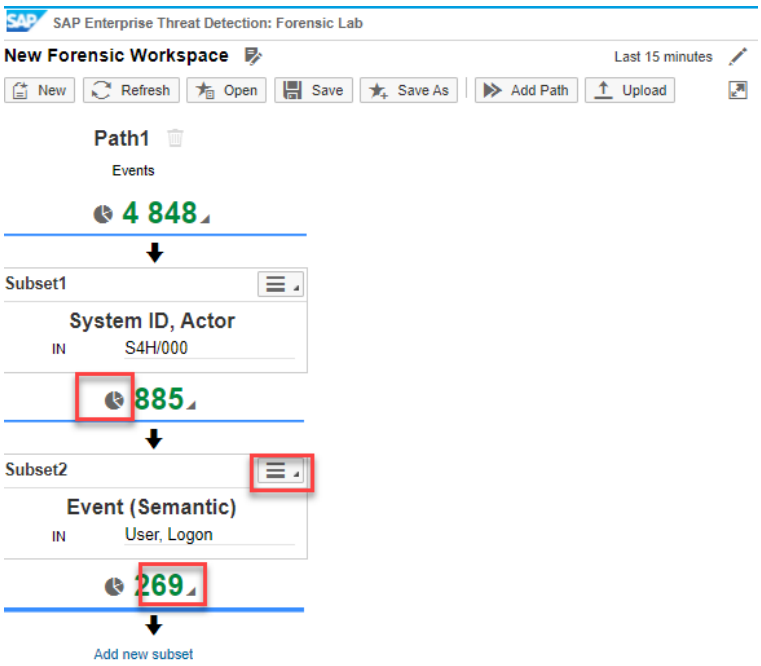
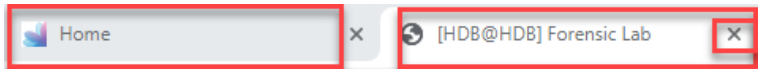
Explanation	Screenshot
21. Go back to the Alert list by clicking on the ‘back’ arrow. Then go back to the launch pad by clicking again to the ‘back’ arrow or to the home-button	
22. Click on Tile ‘Knowledge Base’.	

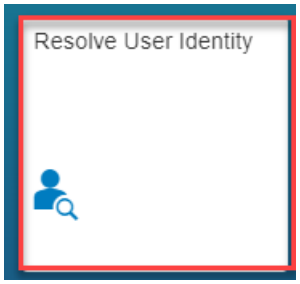
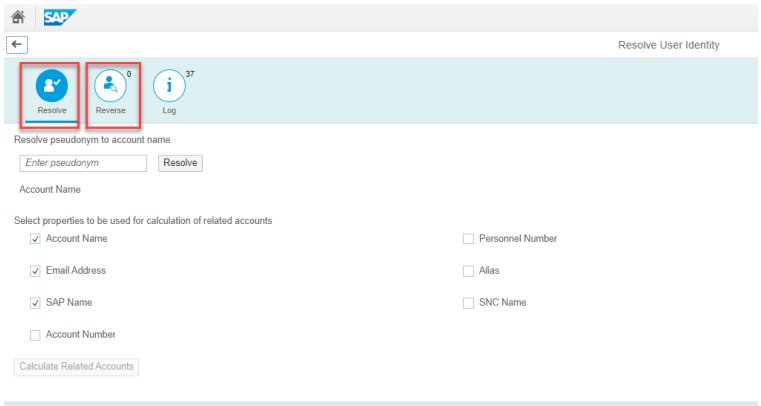
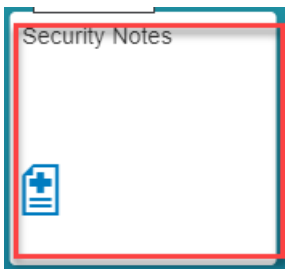
Explanation	Screenshot
23. You can choose between 3 lists. The list of ‘Semantic Events’ shows all events in a human understandable wording and with a short explanation. The semantic events are very often translations from a technical event ID. E.g. the technical Event AU1 from a SAP Security Audit Log 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.	

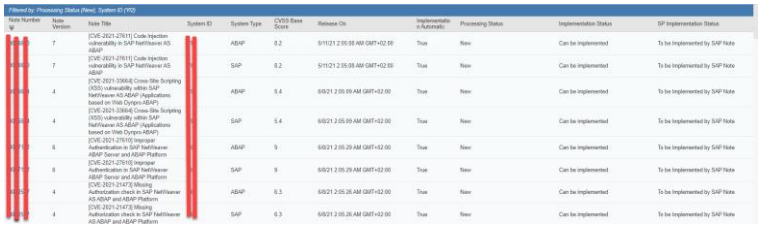
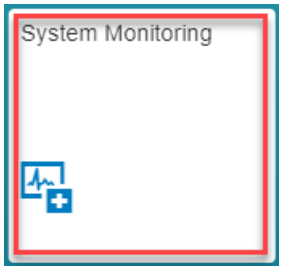
Explanation	Screenshot
25. Klick on Tile ‘System Administration’	
26. You see a list of systems with some major attributes.	

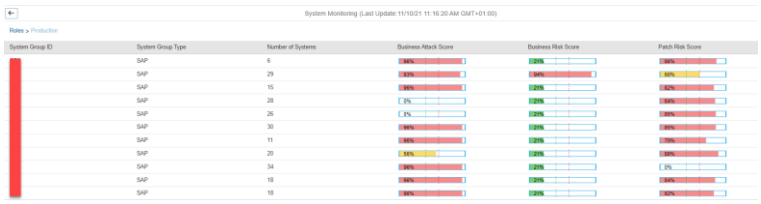
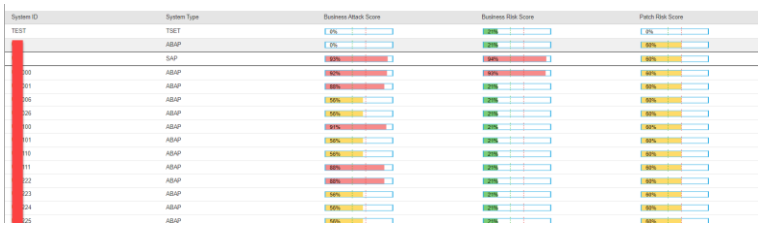
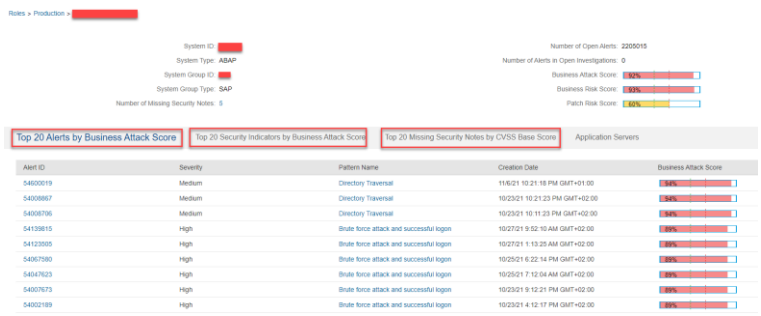
Explanation	Screenshot
27. Click on any of the lines to see the details. Some of the entries are filled from Meta data arriving from SAP Application Server ABAP Systems: • Role (e.g. Production, Test, …) • System Group • Database Host, Type, Version • Application Servers for the System Group Other entries 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)	
28. Use the Home button to jump back to the launch pad	

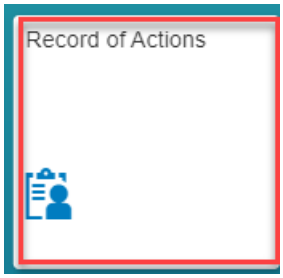
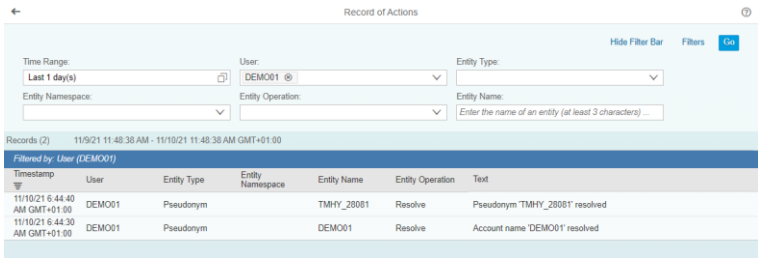
Explanation	Screenshot
29. Click on Tile ‘Forensic Lab’	
30. In the UI you can see a filtering area on the left side and a preview area on the right side (Pie Charts). In the forensic lab you can do analysis, correlation over all the log data, semantic attributes, semantic events over shorter or longer 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.	

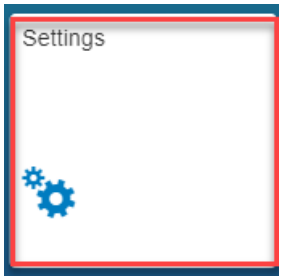
Explanation	Screenshot
31. The basic navigation in the forensic lab is described below. Click on the drop down box above any of the pie charts. You see all the ~180 semantic attributes which are available (→ see Knowledge Base) and might be filled with values. Select e.g. 'Service, Program Name'. Then 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.	
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.	

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.	
35. Jump back to launch pad by using the home button.	
36. Click on Tile ‘Security Notes’	

Explanation	Screenshot
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'.	
38. Jump back to launch pad by using the home button.	
39. Click on Tile 'System Monitoring'.	

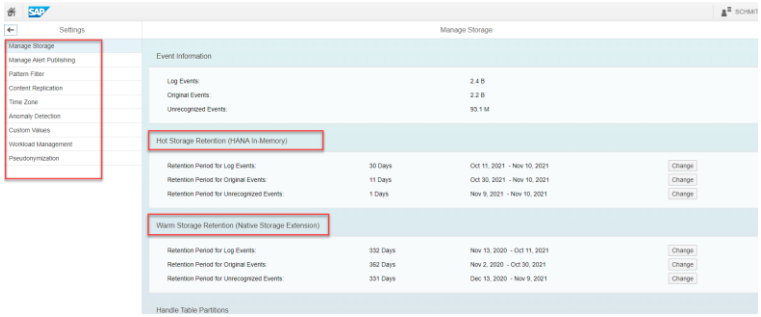
Explanation	Screenshot
40. The UI shows per different system roles (Production, Test, …) the different scores: • Business Risk Score: System criticality as to the maintained criticality in 'System Administration' about Confidentiality, Integrity and Availability. It can be changed by changing/maintaining 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.	 Aggregated Landscape View  Aggregated System ID View  Aggregated System/Client View  Detailed View for one System or System and client
41. Jump back to launch pad by using the home button.	

Explanation	Screenshot
42. Click on Tile ‘Record of Actions’	
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)	
44. Jump back to launch pad by using the home button.	

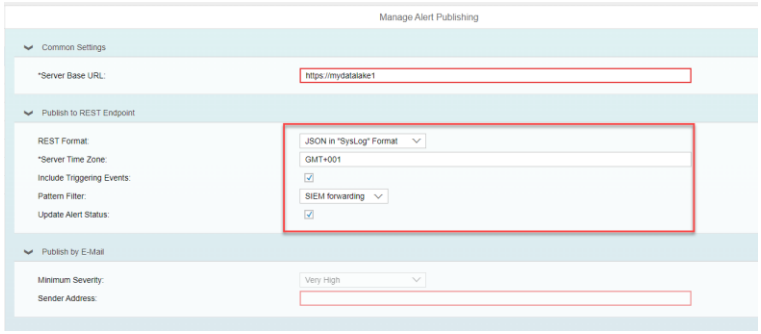
Explanation	Screenshot
45. Click on Tile ‘Settings’	

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

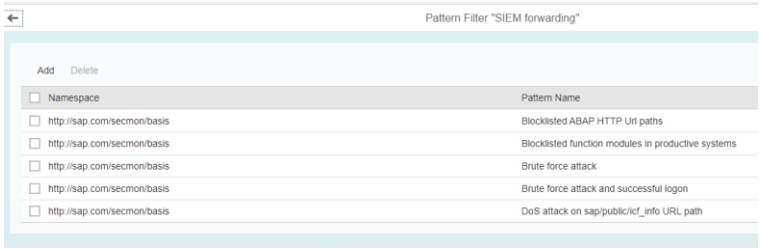
- Manage Storage: Here you can define the retention periods for Hot Storage and Warm Storage. Information: To determine these values, SAP provides a sizing guide.
- Manage Alert Publishing: Here you can define an Alert Forwarding/Pushing from ETD to any Rest Endpoint. You can define the base URL to send 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



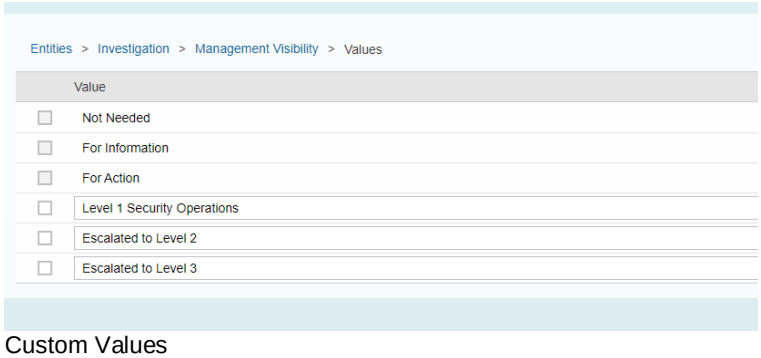
Retention Times



Alert forwarding



Pattern Filter



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.

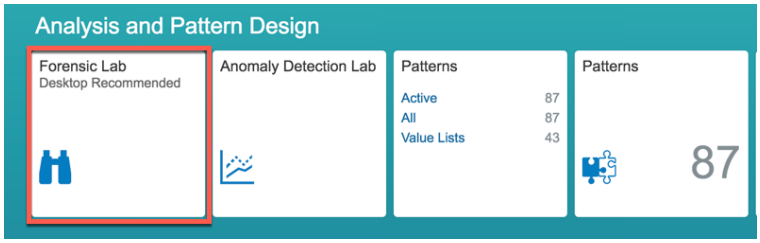
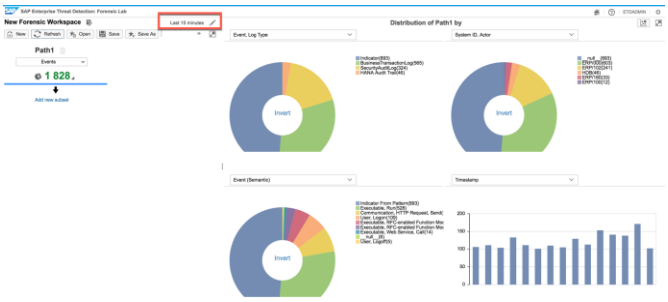
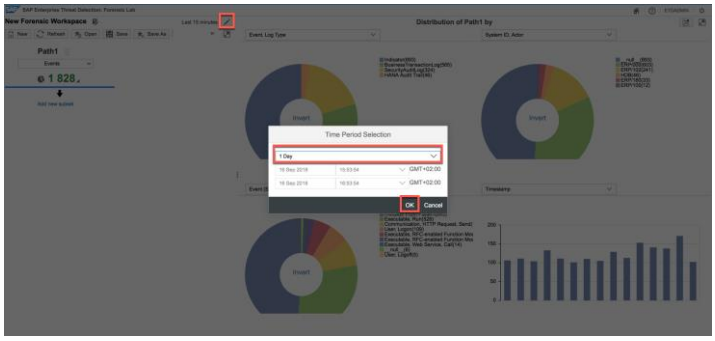
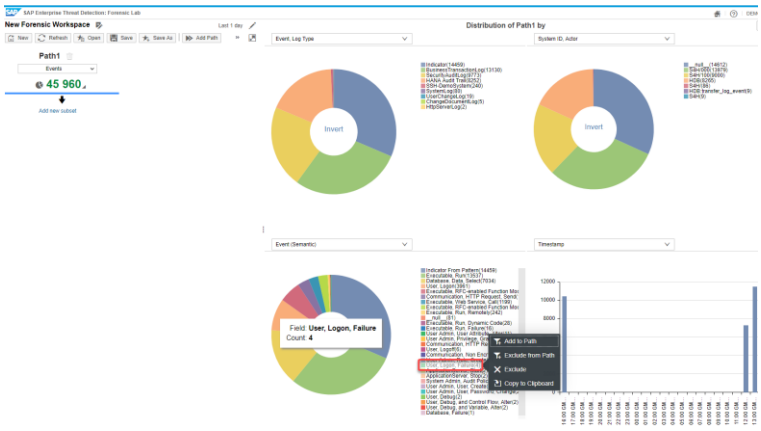
Tool Aspect: The forensic lab is one the most important application in SAP Enterprise Threat Detection and helps you to gain insight about what is going on at present in your system landscape.

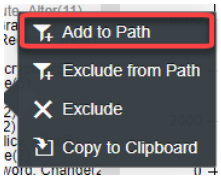
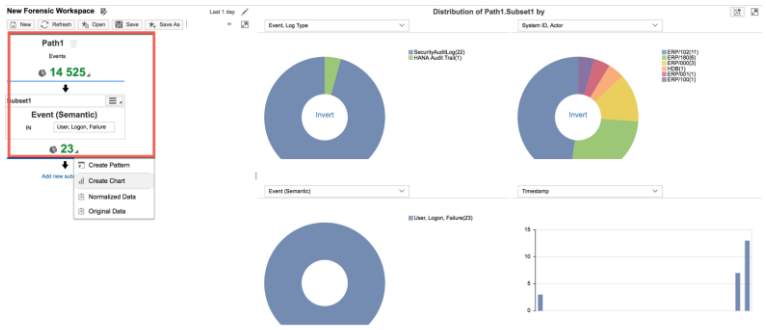
Forensic lab supports workspaces for identifying and analyzing weaknesses or attacks and supports the modelling of charts or attack detection patterns. For attack detection patterns, you create the configurations, which you want SAP Enterprise Threat Detection to use to scan for events that match the 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

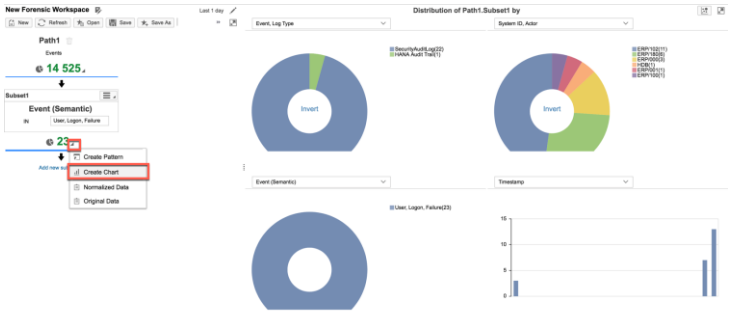
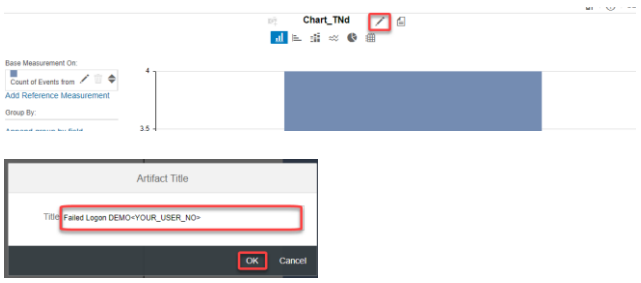
In this exercise, you will display failed log on attempts, and you will learn how filters can be created.

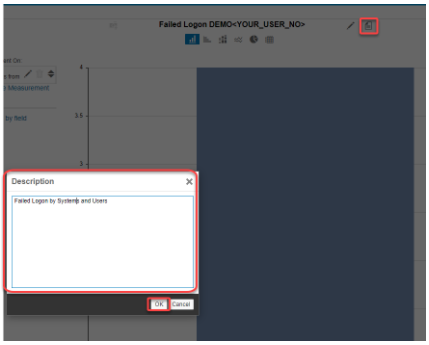
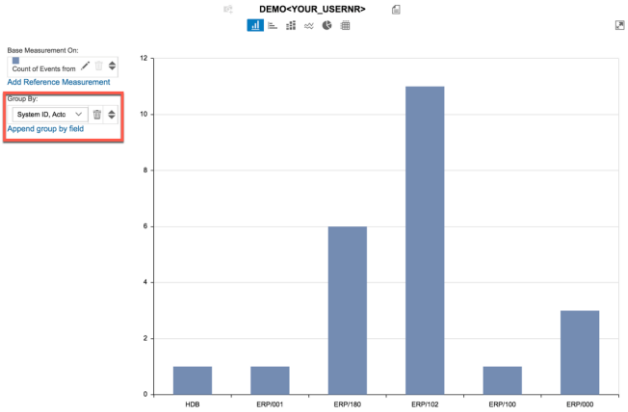
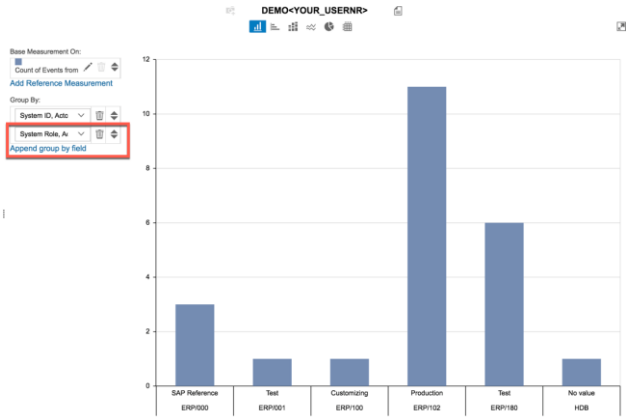
Explanation	Screenshot
48. Open tile **Forensic Lab** in the SAP Enterprise Threat Detection Launchpad.	
49. The initial screen of the forensic lab shows the log events from last 15 minutes. The left part of the workspace contains the filter paths. The right part of the workspace is used to display the 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.	
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.	
51. To add a filter for failed logon events, click on legend *User Logon, Failure.*	

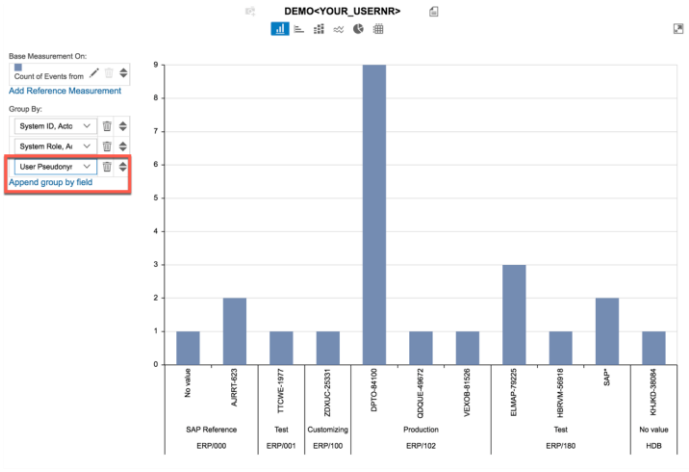
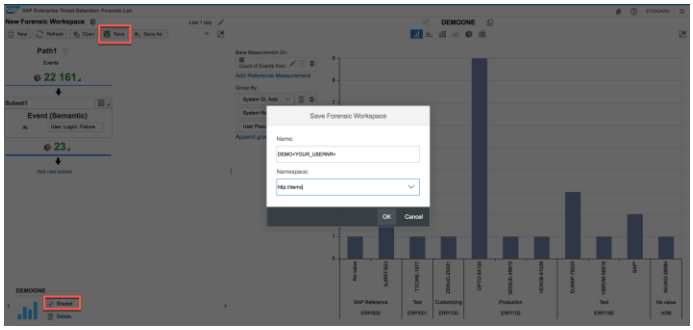
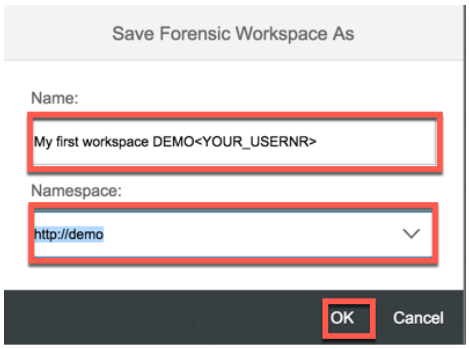
Explanation	Screenshot
52. Select menu item *Add to Path.* This will create a filter for failed logons that have been occurred in the last day. It is shown as *Subset* in the filter path.	
53. Look at *Path1* and see the subset that has been added. Observe that the browsing charts have been updated as well.	

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*	
55. Change the chart name: *Click on the pencil symbol* *In the Popup enter:* *Failed Logon DEMO**<YOUR_USERNR>*** Press o.k.	

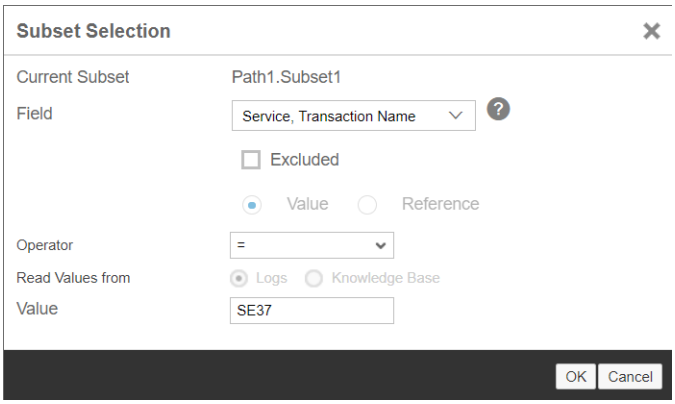
Explanation	Screenshot
56. Push button  . Add the following description and push button *OK.* Description: *Failed Logon Events by Systems and Users*	
57. Click on link *Append group by field* and add field *System ID, Actor.* The chart will be updated with the system information on which failed logon attempts have been observed.	
58. Click on link *Append group by field* and add field *System Role, Actor.* The chart will be updated with additional system role information.	

Explanation	Screenshot
59. Click on link *Append group by field* and add field *Account Name Pseudonym, Targeted.* The chart will be updated with additional user information.	
60. 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*.	
61. Provide name and namespace for your workspace and push button *OK.* Name: *My first workspace DEMO<YOUR_USERNR>* Namespace: *http://demo*	

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):



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>***

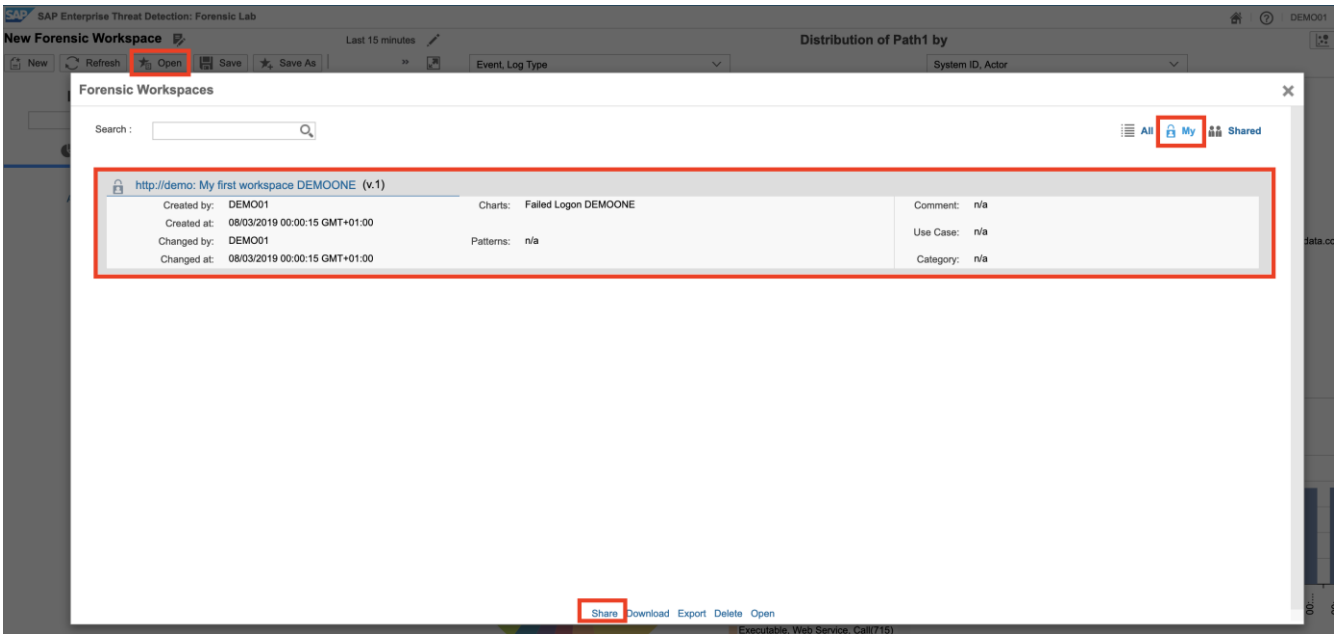
Save your changes and share your workspace. Sharing your workspace allows other users to view the content of your workspace. To share the workspace:

Push *Open* button 

Push *My* button 

Select the workspace you want to share

Push the link *Share*



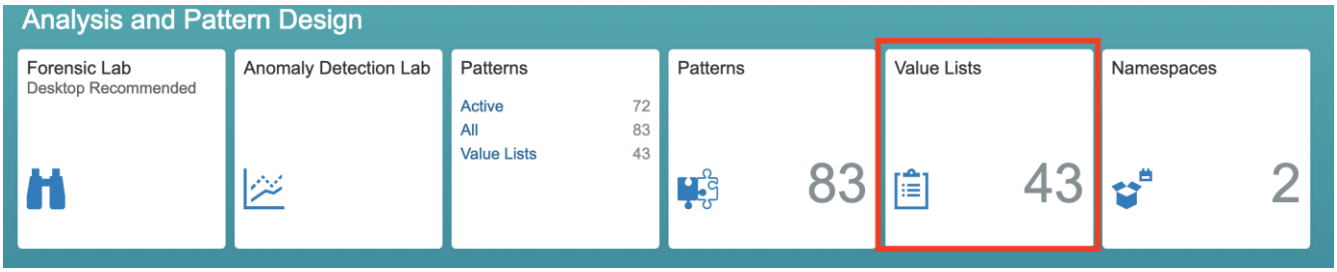
Your workspace is now visible to other users.

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:*



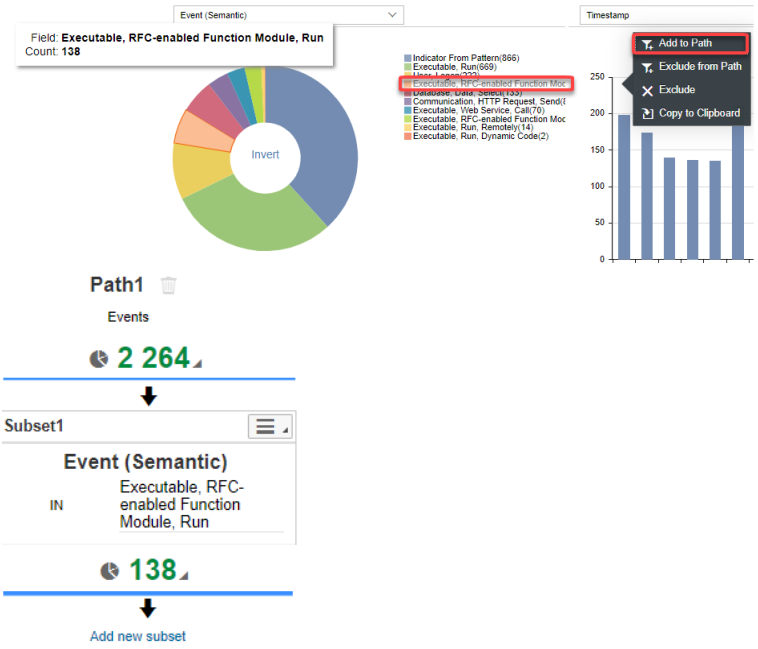
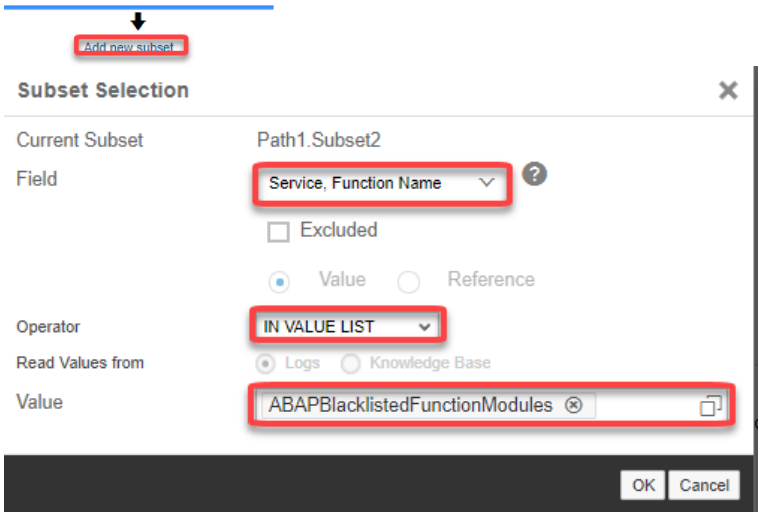
In the *Value List* application, you can view existing ones that are delivered with SAP Enterprise Threat Detection

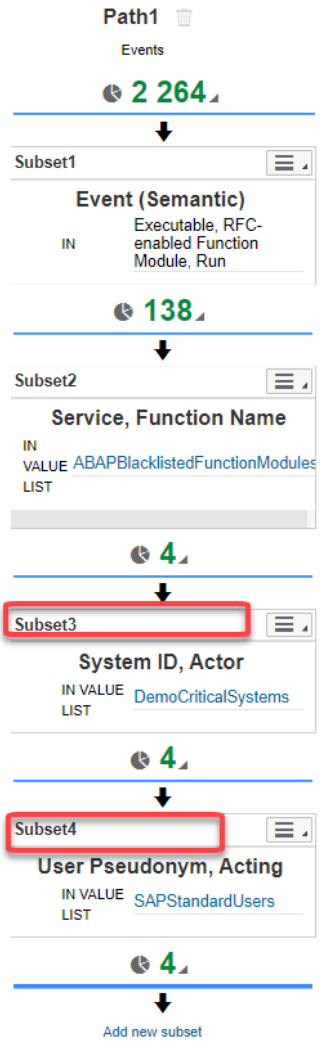
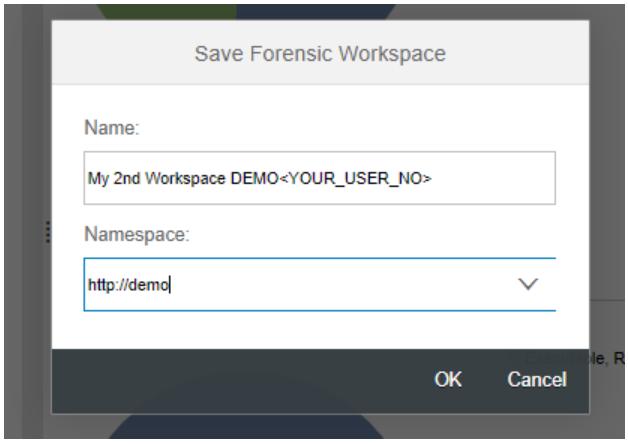
The value lists delivered with SAP Enterprise Threat Detection have pre-defined values, that can be adjusted and enhanced

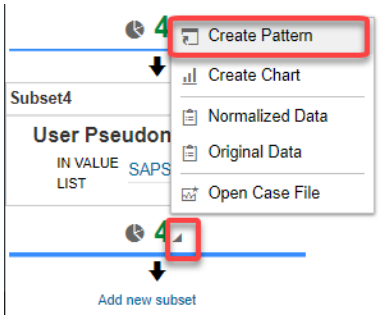
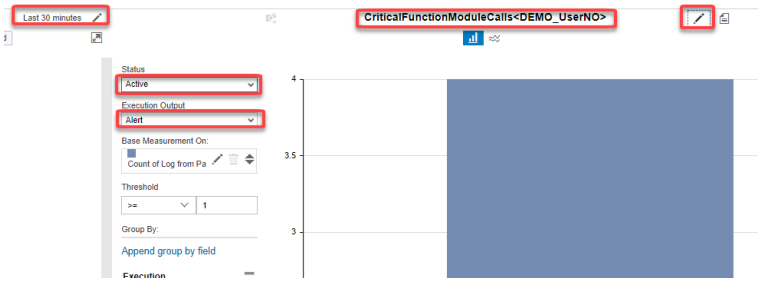
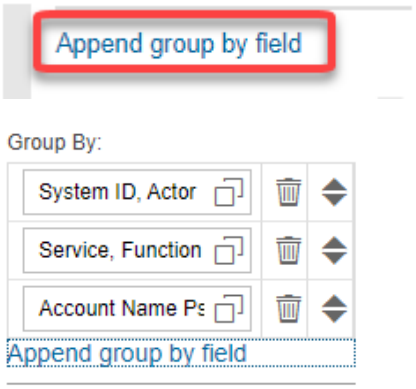
You can also create your own value lists

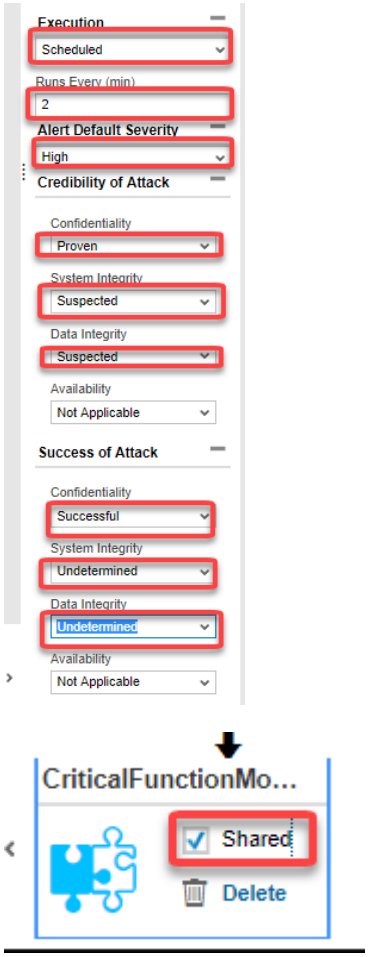
2.5. Modeling Attack Detection Patterns

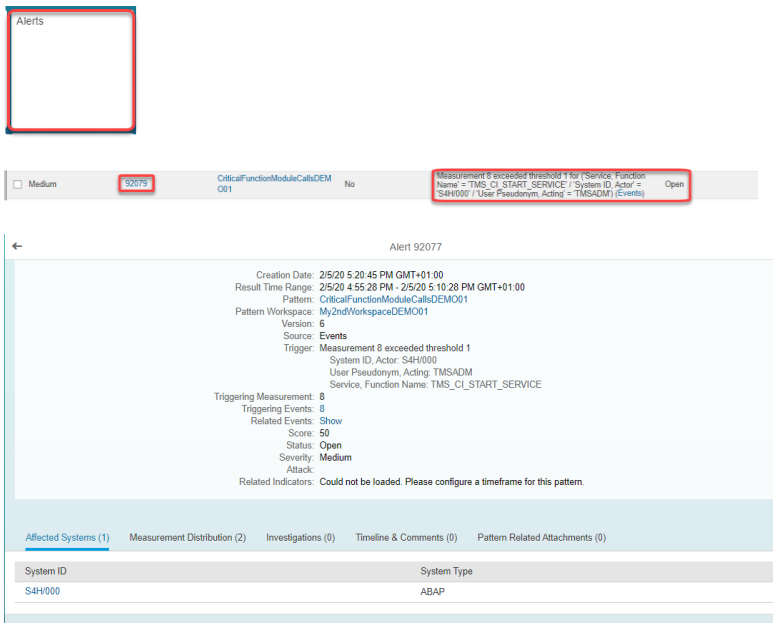
The forensic lab supports the creation of attack detection patterns. The procedure is similar to the procedure of creating charts. Attack detection patterns are as well based on a particular subset of log events. Now you will create a pattern that will deliver an alert when SAP Standard users execute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

Explanation	Screenshot
62. Push button *New* to create a new workspace.	
63. 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	
64. 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: *ABAPBlacklistedFunctionModules* Then press *OK* *As a result, another subset was added to the filter path.*	

Explanation	Screenshot
65. 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: *Account Name Pseudonym, Acting* Operator: *IN VALUE LIST* Value: *SAPStandardUsers* As a result, subsets 3 and 4 should have been added to the filter path.	
66. Save the Workspace	

Explanation	Screenshot
67. 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*	
68. 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*	
69. 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* • *Account Name Pseudonym, Acting*	

Explanation	Screenshot
70. 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.	

Explanation	Screenshot
71. 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	

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. BROWSE, MODEL, AND ATTACK

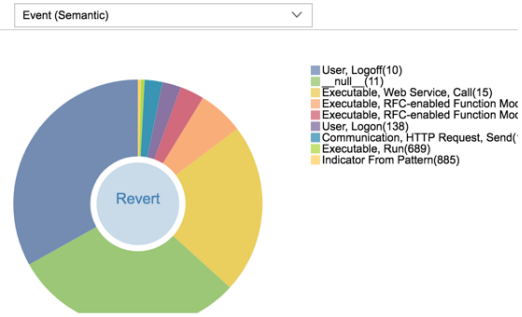
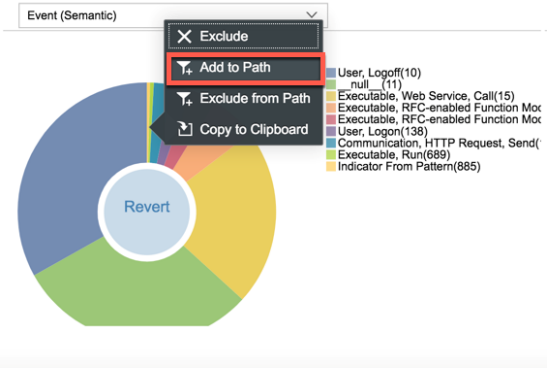
Security Aspect: As a Security Expert you very much have a feeling about anomalies and suspicious behavior within your systems and landscapes, by that if just looking at the data you would already find some presumably critical aspects that you want to explore. The invention of new Patterns based on this knowledge and these findings is the next important step to put your knowledge into automated action. In order to see if your pattern runs in the defined way, you may need to simulate the attack on a Test application, and presumably do a penetration test with Alert Checks.

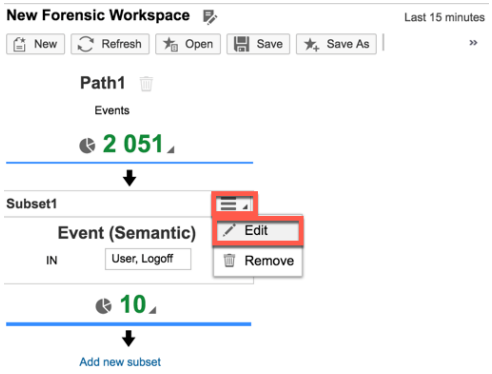
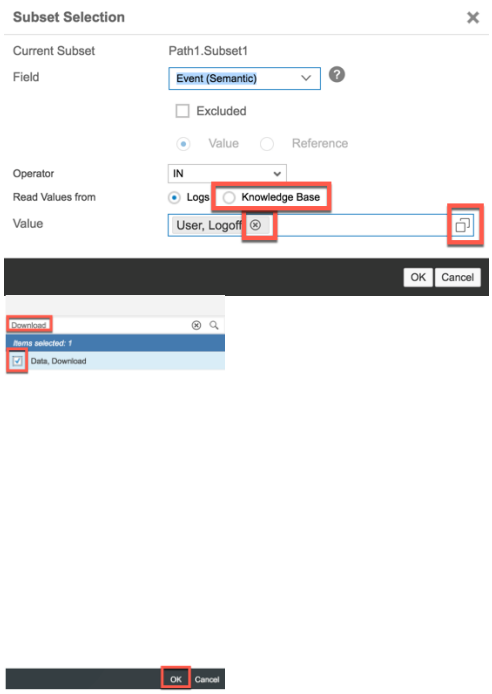
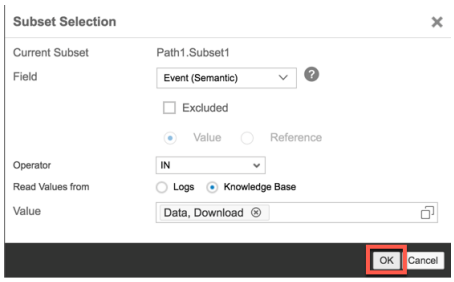
Tool Aspect: You will use the Forensic Lab to model a Pattern for Data Download-Alerts and then simulate the attack within an SAP S/4H system to verify that your Pattern works.

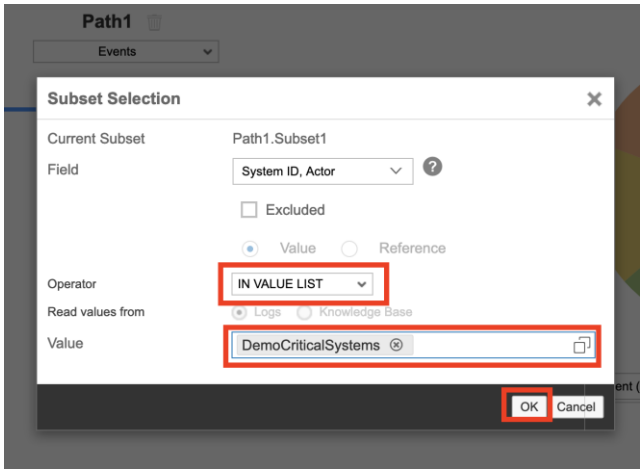
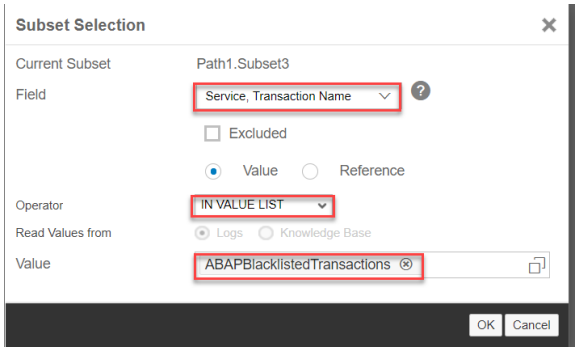
Further you can create a Free-Style Pattern to check your knowledge.

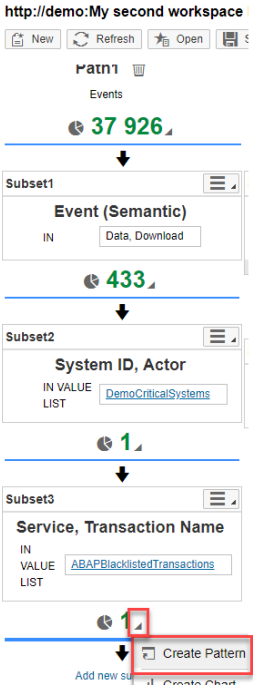
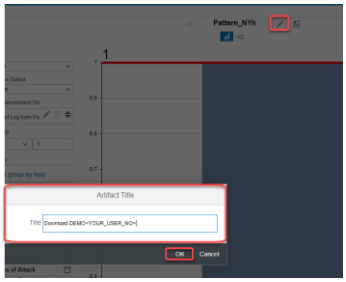
3.1. Create a Data Download Pattern and simulate the Attack

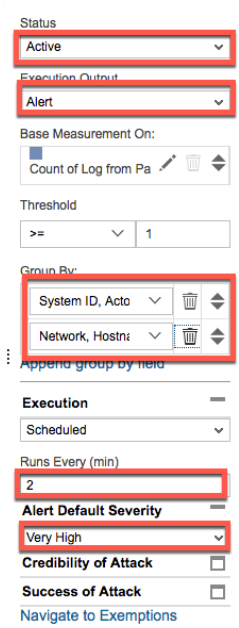
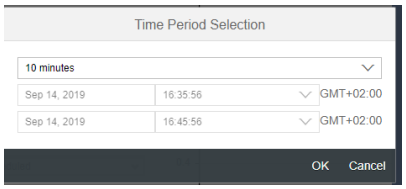
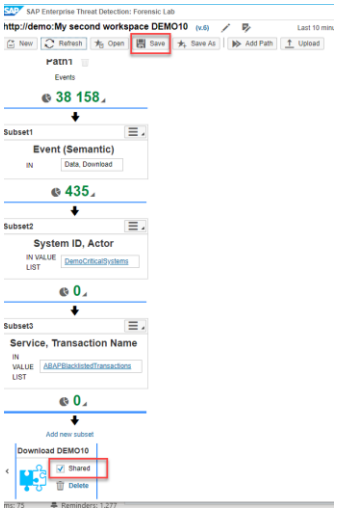
In this chapter you will create a Pattern if Data Download happens in critical transactions within critical systems.

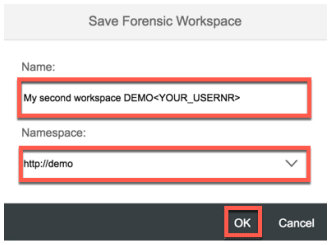
Explanation	Screenshot
72. Push button *New* to create a new workspace.	
73. Look at the left lower bottom chart. If the *_null_* value dominates the chart, click *Invert* in the middle of the chart.	
74. Click on a section of the chart and select menu item *Add to Path.*	
75. Look at *Path1* and see that the subset has been added. Observe that the browsing charts have been updated as well.	

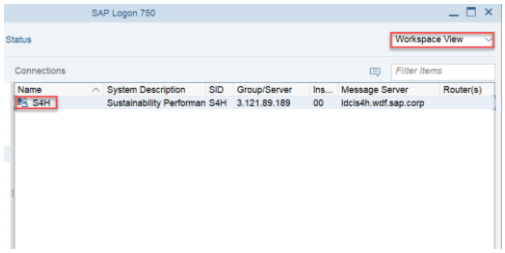
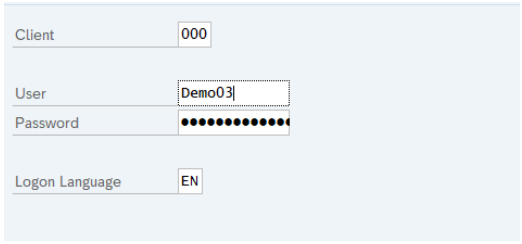
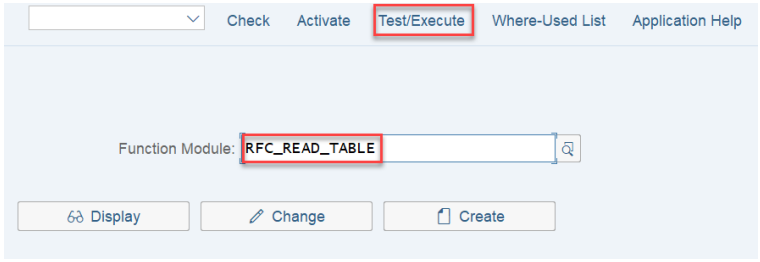
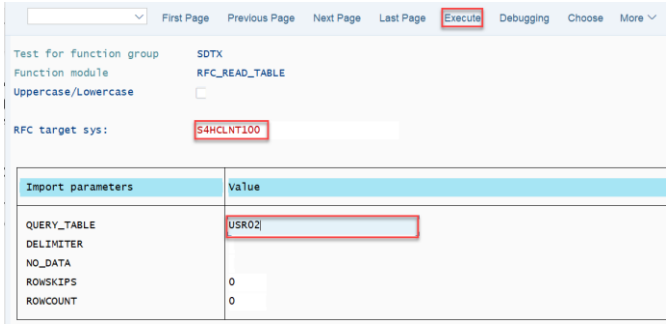
Explanation	Screenshot
76. Change the subset to filter for download events. Click on the top right button of the subset  and select menu item *Edit.*	
77. Change selection of *Read Values From* from *Logs* to *Knowledge Base.* This is needed in case no download events can be found in the forensic lab. In *Value* remove the entry by clicking on button  and push button for *F4-Help.* Enter search term *Download* and click on button  . Enable selection for *Data, Download* and push button *OK.*	
78. Push button *OK* to apply filter for download events.	

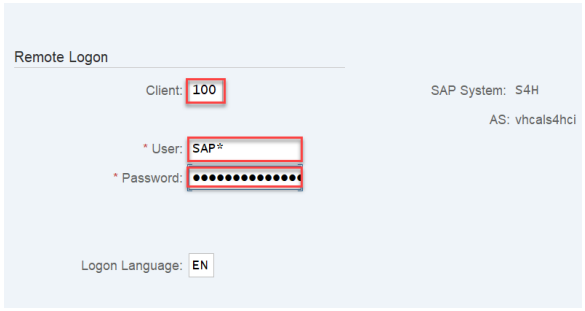
Explanation	Screenshot
79. Click on *Add new subset* and create a filter using the value list *DemoCriticalSystems.* Enter the following Subset Selection: Field: *System ID, Actor* Operator: *IN VALUE LIST* Value: *DemoCriticalSystems*	
80. Click on link *Add new subset* and enter the following Subset Selection: Field: *Service, Transaction Name* Operator: *IN VALUE LIST* Value: *ABAPBlacklistedTransactions*	

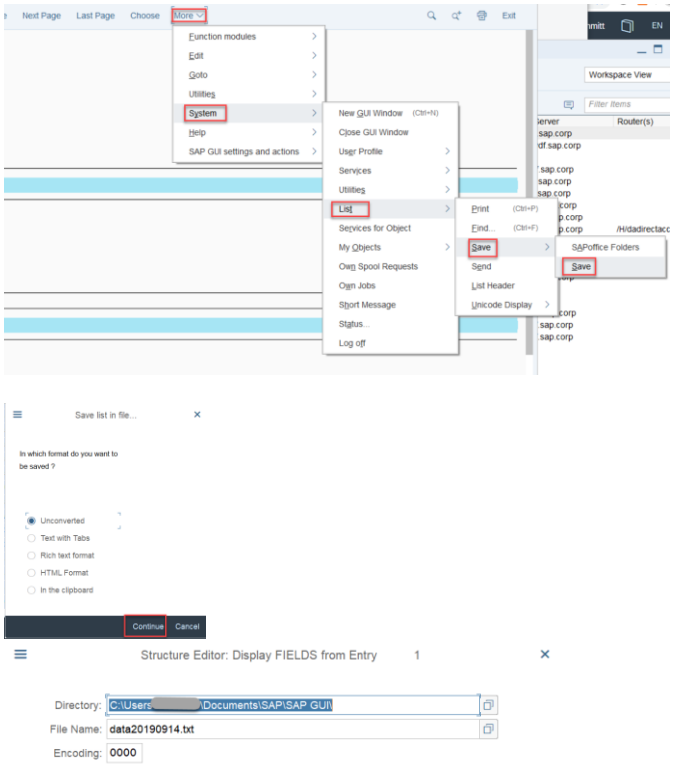
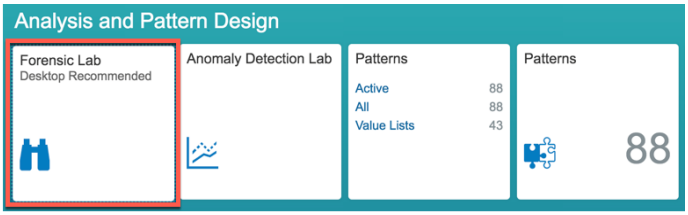
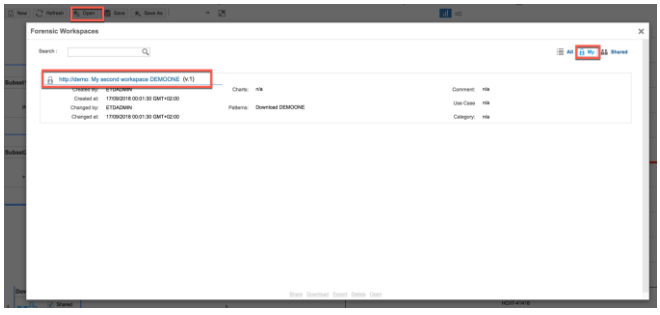
Explanation	Screenshot
81. Push the button right to the subset number  . This opens a drop-down menu with all available operations you can perform on the subset. Select menu item *Create Pattern.*	
82. Change the pattern name: *Download DEMO**<YOUR_USERNR>***	

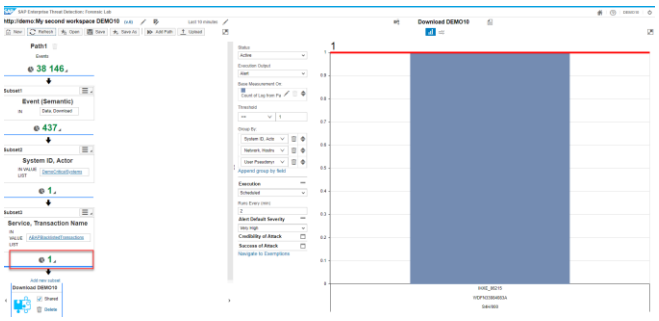
Explanation	Screenshot
83. Change the following values: Status: *Active* Execution Output: *Alert* Group By: *System ID, Actor* *Network, Hostname, Initiator* *Account Name Pseudonym, Acting* Runs Every (min): *2* Alert Default Severity: *Very High*	
84. Change time period to 10 Minutes.	
85. You can now save your changes as you are done with modeling your pattern and workspace. On the left lower area enable checkbox *Shared*. This allows other users to access your pattern. Push button *Save*.	

Explanation	Screenshot
86. Provide name and namespace for your workspace and push button *OK.* Name: *My second workspace DEMO**<YOUR_USERNR>*** Namespace: *http://demo*	

Explanation	Screenshot
87. Open SAP GUI, go to 'Workspace View' and select system for Hands-On Session SEC262 for your Group (1, 2, 3, 4, or 5).	
88. Logon to S4H Client 000 with the following user: User: Demo***<YOUR_USERNR>*** Password: Welcome1	
89. Start transaction SE37 – ABAP Function Modules. Enter value *RFC_READ_TABLE* and push button Test/*Execute.*	
90. Add the following values and push button *Execute*. RFC target sys: *S4HCLNT100* Query Table: *USR02*	

Explanation	Screenshot
91. Now try to logon with SAP Standard user SAP*. Client: *100* User: *SAP** Password: *Master1234* Press Enter	
92. Click on the result of your RFC query to see the details.	

Explanation	Screenshot
93. To download the content, choose More→System→List→Save→Save. Save content on your local file system.	
94. Open SAP Enterprise Threat Detection Launchpad and click on tile *Forensic Lab* to verify the download events.	
95. Push button *Open.* In the workspace explorer select view *My* and click on the name of the workspace to open it in the forensic lab.	

Explanation	Screenshot
96. Look at *Path1* and find the download events.	
97. Open SAP Enterprise Detection Launchpad and see that the tiles *Open Alerts* and *Threat Situation Last Hour* have been updated.	

3.1. Browse through the data and model your own individual Attack Detection Pattern

In your newly created workspace *My second 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 and your own pattern.

Hint: Create a Pattern about semantic events that are already seen within the Forensic Lab, so that later, you can test the Pattern by use of the incoming data or by being able to trigger the events within the connected SAP ERP system (see below).

Make use of the following pattern name for your own created Attack Detection Patterns:

<Attack Detection Pattern name> *DEMO****<YOUR_USERNR>***

Save **and share** your charts, patterns and workspace as soon as you are finished with your changes.

Now you can additionally access the SAP system and do some actions within the S4H system to simulate the attack.

3.2. Summary

Security Aspect: In the role of a Security Expert you have found suspicious behavior by Browsing through the data and you created/invented a Pattern based on these new findings. Then you did a hacking scenario/simulation to check whether your alert was raised.

Tool Aspect: You got familiar with *Forensic Lab*, how to find very different kinds of data within the logs, and how to use the tools to build patterns and charts, and how to check the Alerts with *Open Alerts* and *Threat Situation Last Hour* applications.

4. 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?

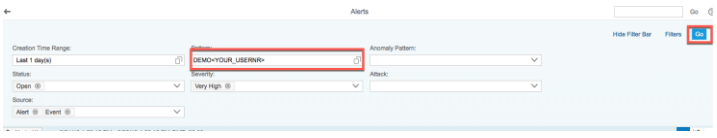
Then you may need to collect the evidences and to follow a Standard Operation Procedure for the further actions.

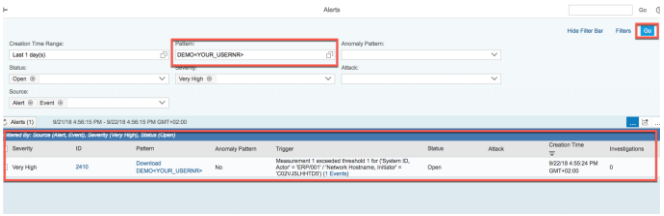
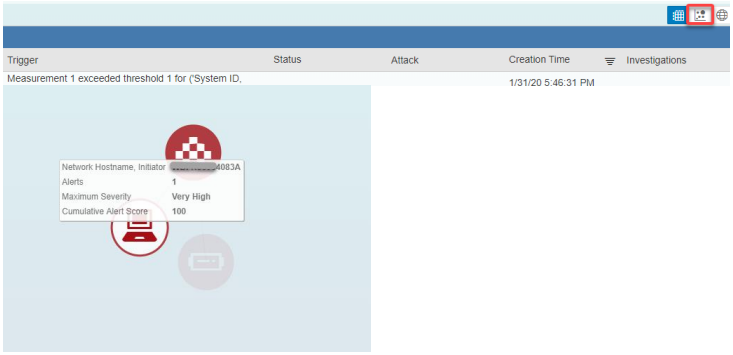
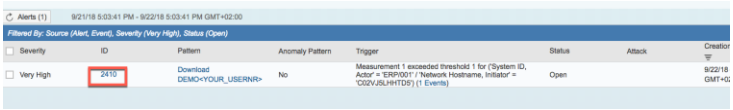
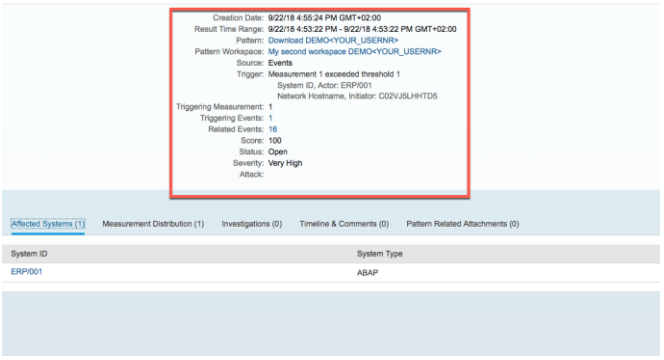
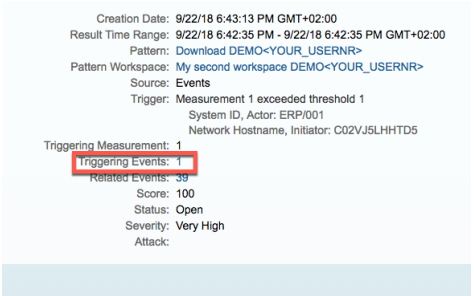
Tool Aspect: SAP Enterprise Threat Detection raises alerts as notification for potential attacks as they are happening. An alert includes references to the log events and the attack detection patterns or the anomaly detection patterns that led to its creation. Alerts are processed and analyzed by making 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).

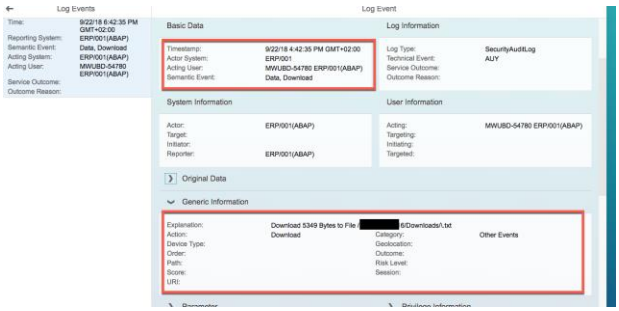
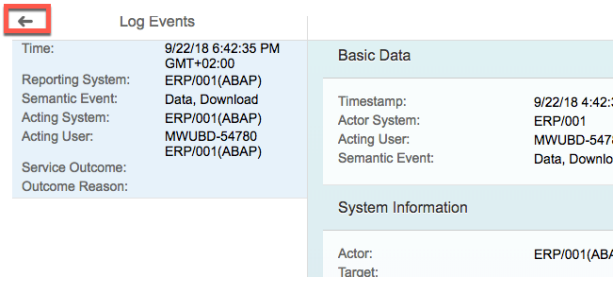
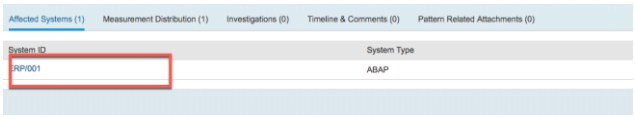
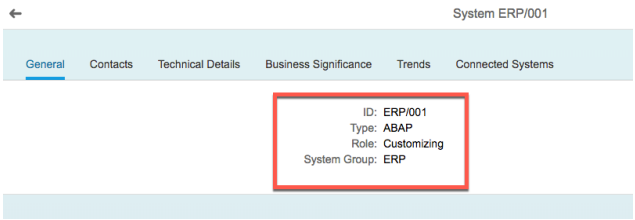
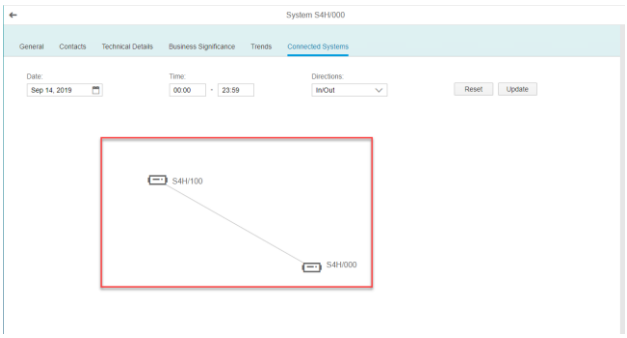
4.1. Viewing Alerts

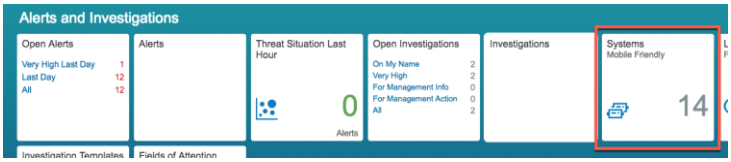
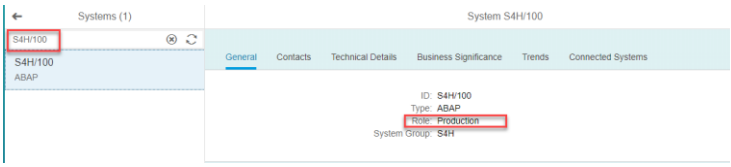
As the monitoring agent of a company, you need to monitor the alerts and react immediately. In the case of a suspected attack, it is usually the user or the hostname behind it or the system affected that you need to identify.

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

Explanation	Screenshot
98. Open tile *Open Alerts – Very High Last Day.*	
99. Open Filter Bar. Add the pattern you have created in step 24 as filter and push button *GO.* *Download DEMO**<YOUR_USERNR>*** *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.*	

Explanation	Screenshot
100. 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 you can see the system on which a suspicious download activity has taken place. Further you can see, which hostname has triggered the download.	
101. Push button *View Threat Situation* and see e.g. the *Network Hostname Initiator* that has been used for downloading data.	
102. Switch back to the *Alerts List View* and click on alert *ID* to see more details about the alerts	
103. 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.	
104. Click on the *Triggering Events* to see more details.	

Explanation	Screenshot
105. See the details of the events that has led to the alert creation e.g. the system where a download activity has been detected or the size of data that has been downloaded.	
106. Click on button *Back* to return to the alert details view.	
107. Click on *System ID* to see the details of the affected system.	
108. Look at the details of the affected system.	
109. Under tab *Connected Systems* you can see that the affected system has done a remote communication.	

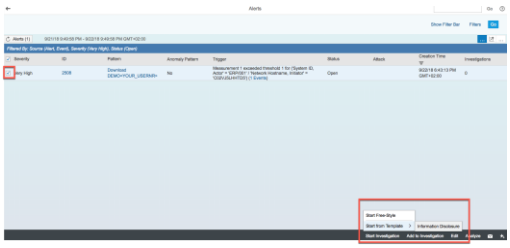
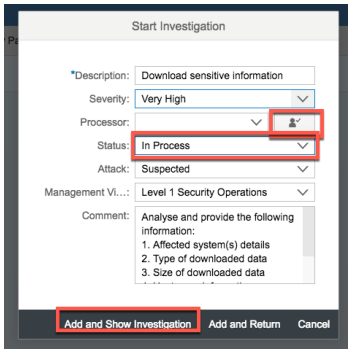
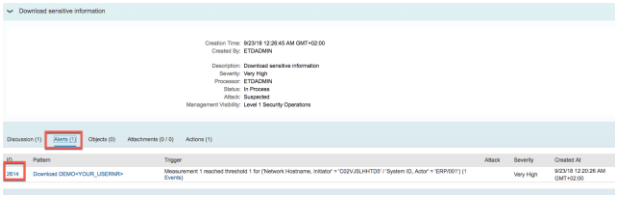
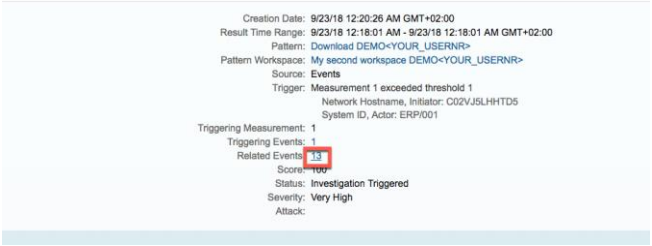
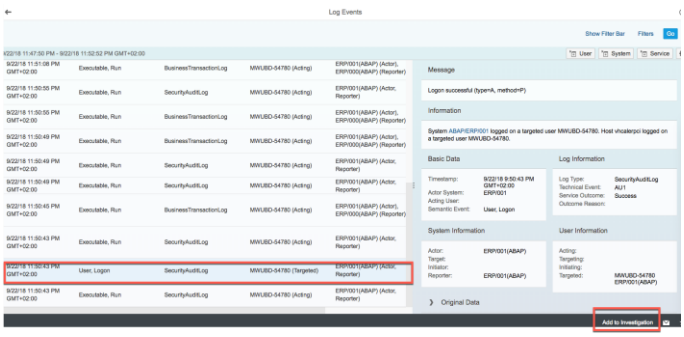
Explanation	Screenshot
110. Open a new browser tab and open SAP Enterprise Threat Detect Launchpad. Open tile *Systems* to see the details of the system to which a remote communication has taken place.	
111. Enter the System ID in the search field an select the system to see the details. *(Hint: if there 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)*	

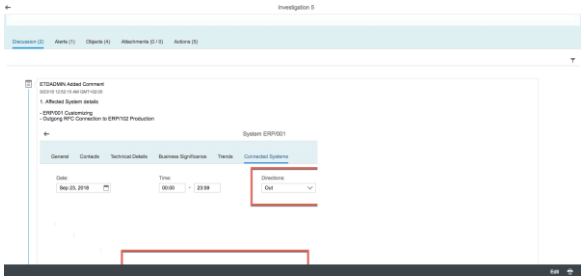
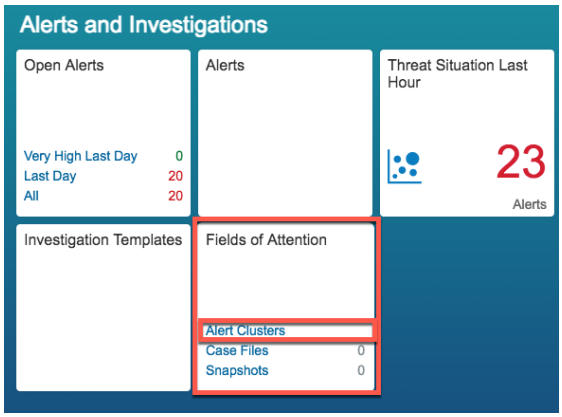
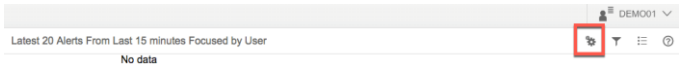
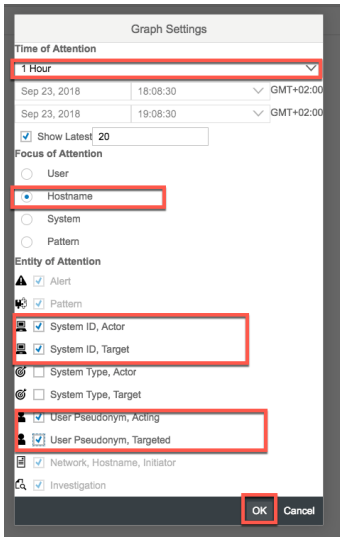
4.2. Investigating Alerts

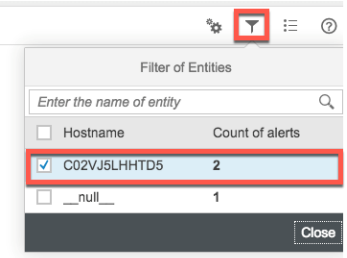
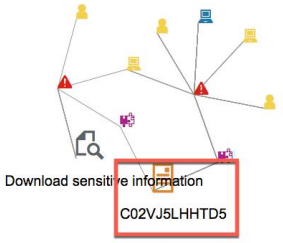
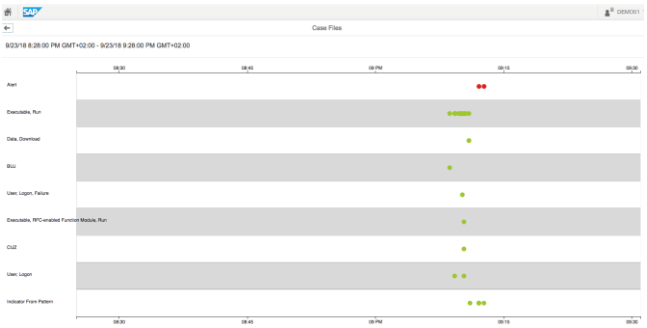
Investigations are collections of related material such as alerts, case files, and snapshots. They are the central item with which the monitoring agents and/or the security expert starts his forensic research, as they can lead to an incident.

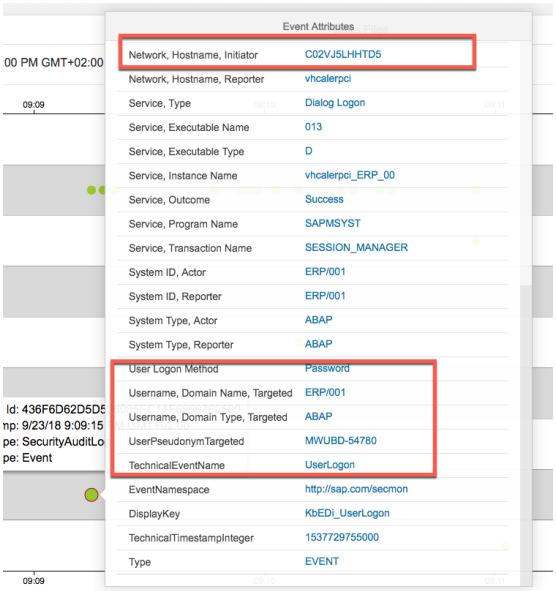
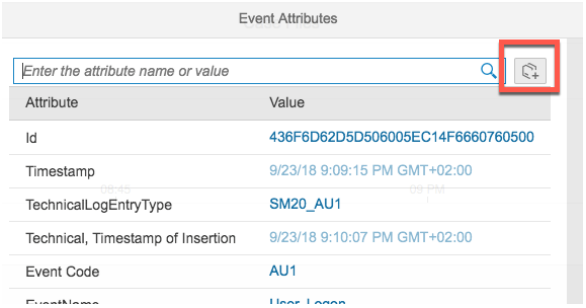
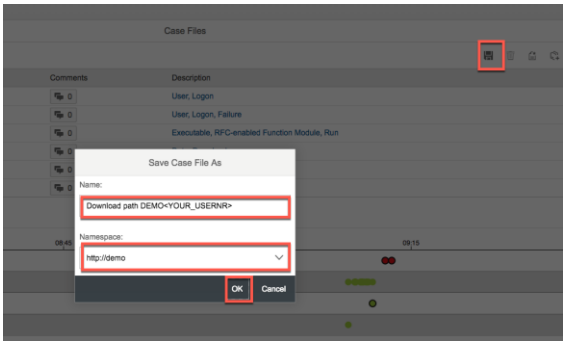
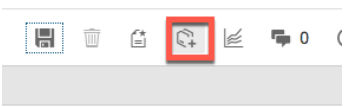
When the monitoring agent considers an alert suspicious, an investigation gets started. The investigation gets a description, a severity, a status and comments can be added. The investigation can be shared easily, either in emails or as tiles in the launchpad, or even as a PDF file. More alerts and other 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.

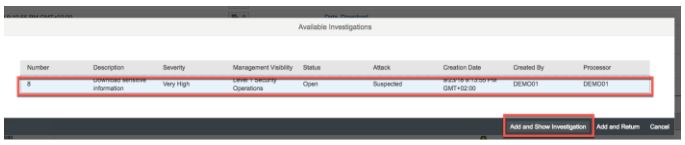
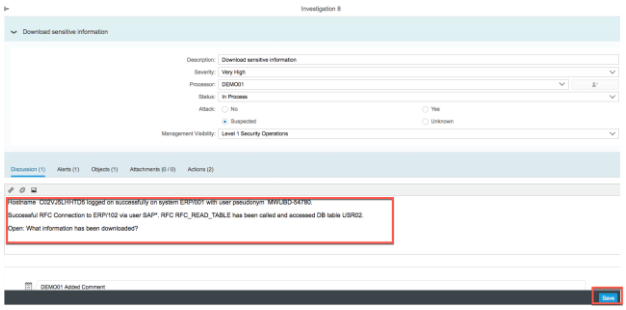
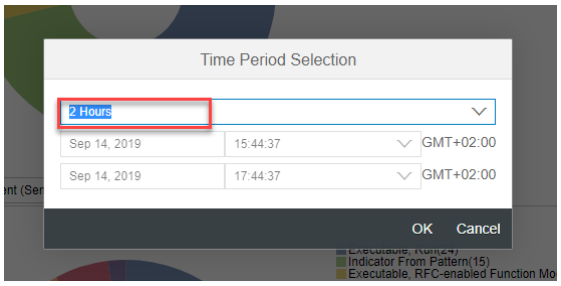
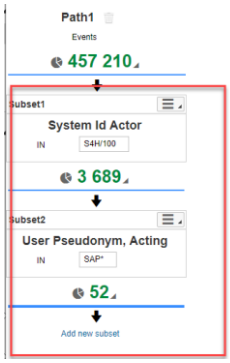
As the investigation is an item that more than one person might work with, there is a discussion and timeline tab in which manual comments as well as changes to the investigation are tracked.

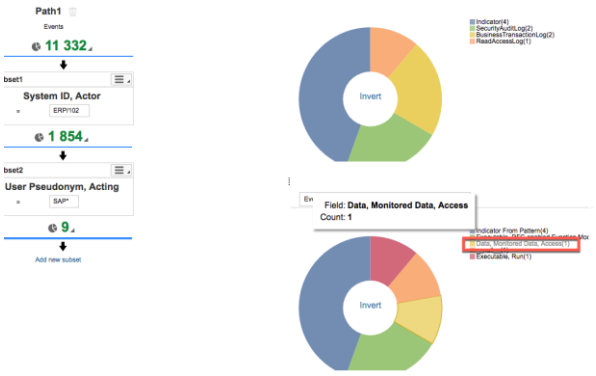
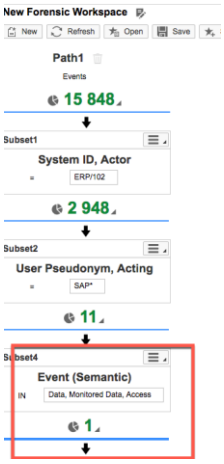
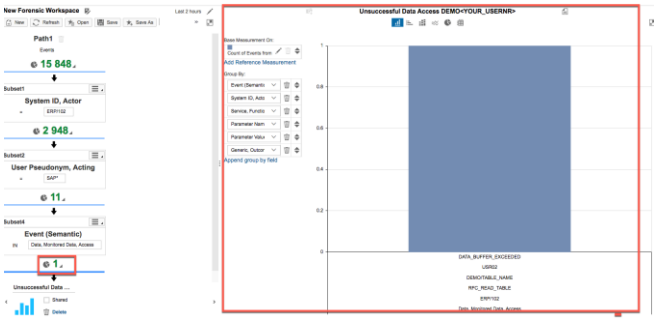
Explanation	Screenshot
112. In the Alerts worklist view, select the alert and push button *Start Investigation.* Choose *Start From Template → Information Disclosure*	
113. Set yourself as processor of the investigation, set the Status to In Process and check the instructions how to handle this type of alert. Push button *Add and Show Investigation.*	
114. Click on tab *Alerts* and click on alert *ID* to further investigate details of the alert.	
115. Click on related events to gain more insight about the potential threat.	
116. Select the event row to see more details. Add to your investigation if relevant.	

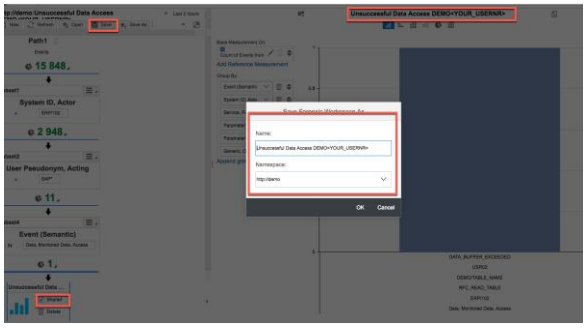
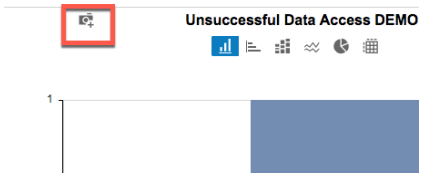
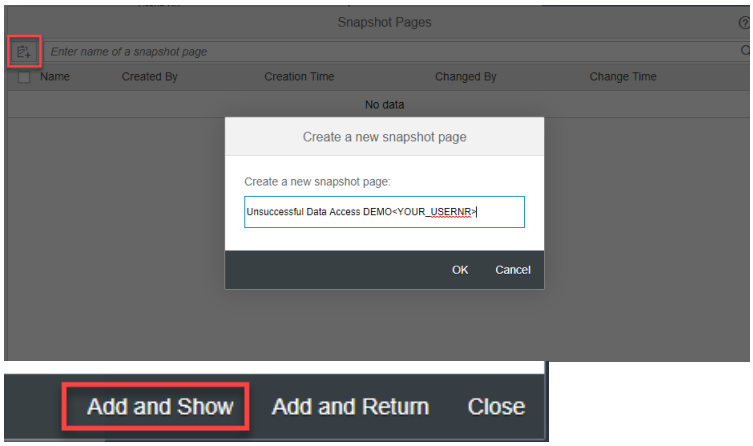
Explanation	Screenshot
117. Update Investigations with your current investigation analysis results. E.g. use the tab discussions and add comments or screenshots to affected system details, size of downloaded data, hostname or user information. Screenshots can be added via Drag & Drop. *(In the picture on the right you see a screenshot which is pasted into the comment field)*	
118. 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.*	
119. Choose button *Settings.*	
120. 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.*	

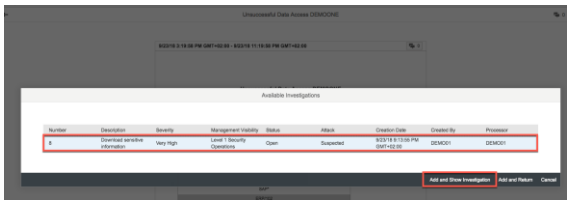
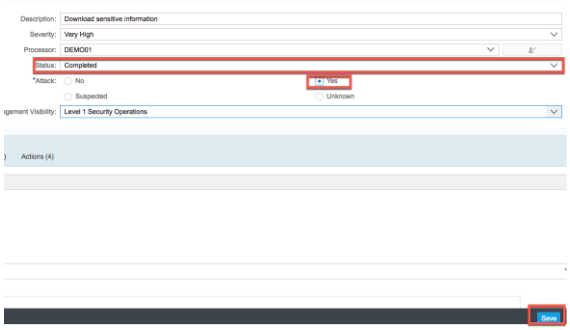
Explanation	Screenshot
121. Push button *Filter* and only enable the hostname that has triggered the alerts.	
122. Look at the alert graph focusing on the selected hostname and see how it is connected to patterns, alerts and systems. Click on the hostname node to see further details.	
123. Look at the alerts and events shown on the timeline where this hostname was involved.	
124. 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.	

Explanation	Screenshot
125. Click on the circle to see the event details.	
126. Push button *Add to Case File*  to add all relevant events that are related to the alert creation.	
127. 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*	
128. Push button *Add to Investigation.*	

Explanation	Screenshot
129. Select your investigation and push button *Add and Show Investigation.*	
130. Update the investigation Discussion with your analysis results.	
131. 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.	
132. Create the following filters: System ID, Actor = *S4H/100* User Pseudonym, Acting = SAP*	

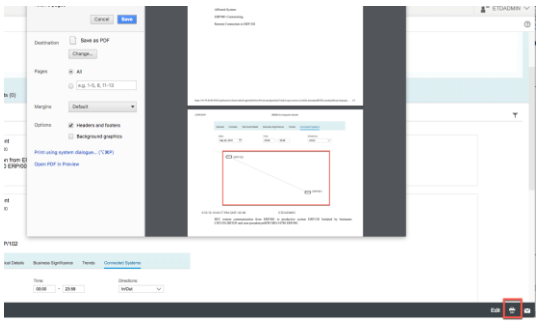
Explanation	Screenshot
133. Look at the browsing chart for *Event (Semantic)* and see the event *Data, Monitored Data, Access.*	
134. Add a filter for this event.	
135. Create a chart with the following *Group By* fields: *Event (Semantic)* *System ID, Actor* *User Pseudonym, Acting* *Service, Function Name* *Parameter Value, String* *Generic, Outcome*	

Explanation	Screenshot
136. Provide the following chart name. Chart name: *Unsuccessful 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*	
137. Push button *Add chart to snapshot page.*	
138. Push button *Create a new snapshot page.* Provide the following snapshot page name and push button *Add and Show.* Snapshot page name: *Unsuccessful Data Access DEMO<YOUR_USERNR>*	

Explanation	Screenshot
139. Push button *Add snapshot page to investigation.*	
140. Select your investigation and push button *Add and Show Investigation.*	
141. Edit and update the investigation with your findings and close it.	

4.3. 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
142. 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*.	

4.4. 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.

5. 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.

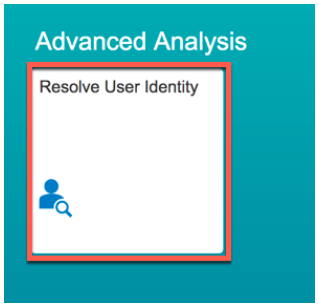
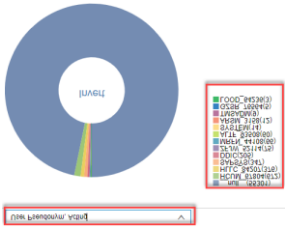
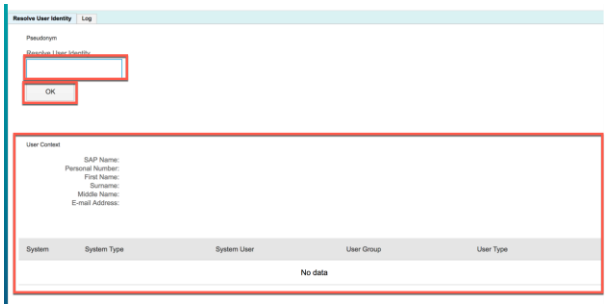
Tool Aspect: You will learn how to resolve the User Pseudonym.

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.

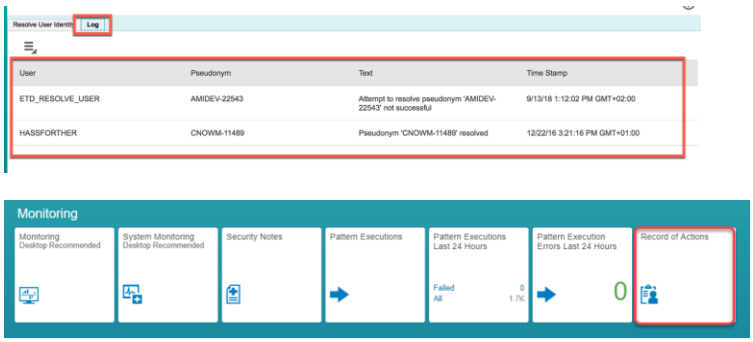
5.1. Determining the True Identity of Users

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
143. Logon to SAP Enterprise Threat Detection Launchpad with the following user and open tile *Resolve User Identity* User: DEMO<*YOUR_USERNR*> Password: Welcome0	
144. Enter user pseudonym and push button *OK*. 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 Pseudonym, Acting* 	

5.2. 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
145. 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*	

5.1. 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”

6. MONITORING DASHBOARDS

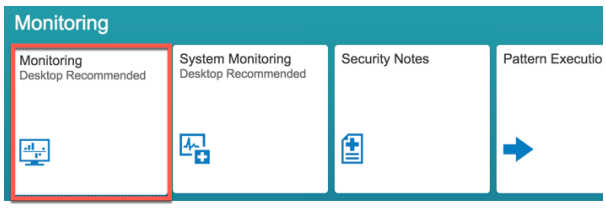
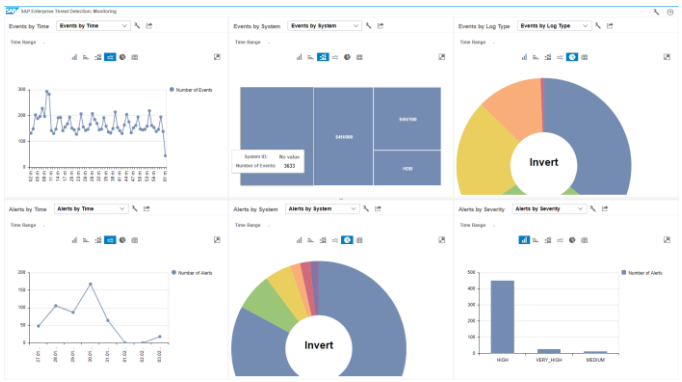
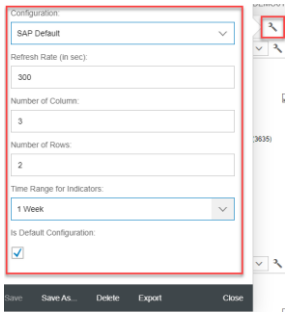
Security Aspect: During the daily operation of security monitoring a Security Agent needs to have an overview of the whole landscape. In ETD they include active alerts, the status of investigations and the log events. Since every agent has his own interested aspect, the content of the monitor must be 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.

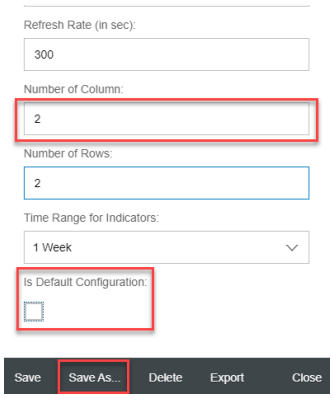
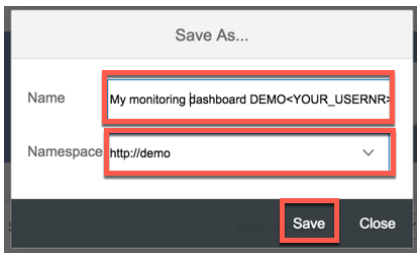
It is possible to define favorite monitoring dashboards by each individual user.

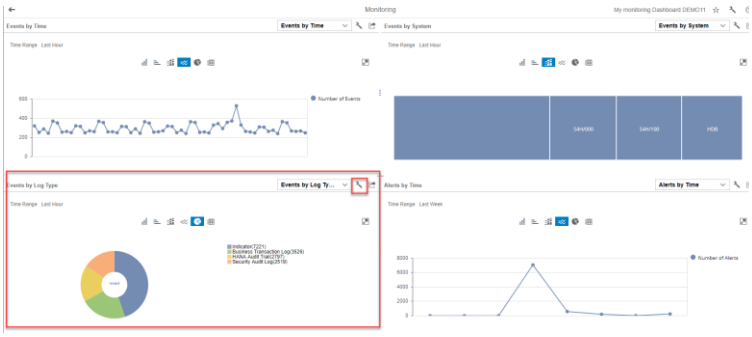
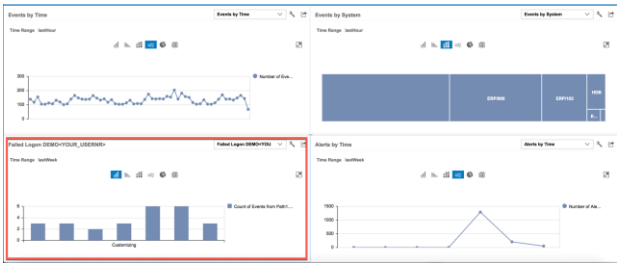
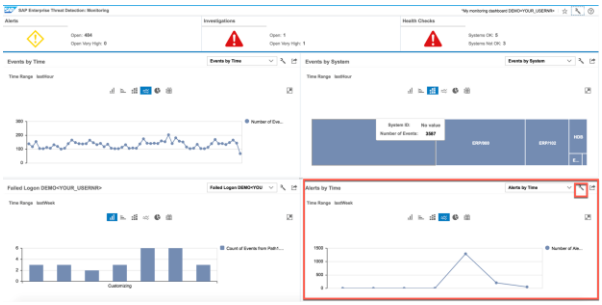
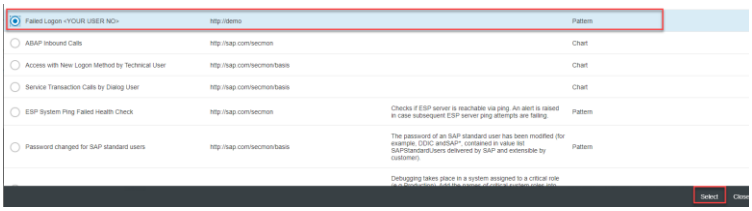
6.1. Viewing Default Monitoring Dashboard

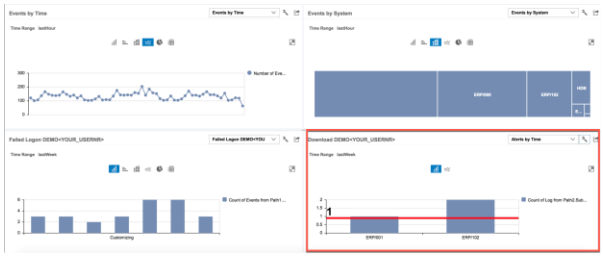
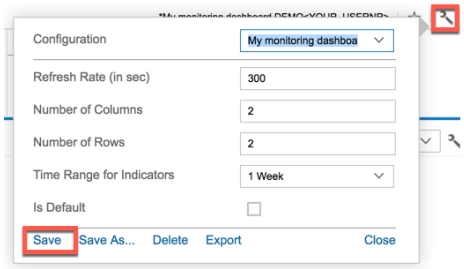
When opening the monitoring tile, a default monitoring dashboard is displayed. The default monitoring dashboard is typically used as a video wall.

Explanation	Screenshot
146. Open tile **Monitoring** in the SAP Enterprise Threat Detection Launchpad.	
147. 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.	
148. Click on the button *Setting* 🔧 to see configuration details of the default monitoring dashboard.	

6.2. Building your own Monitoring Dashboard

Explanation	Screenshot
149. 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*	
150. Enter the name and namespace and push button *Save.* Name: *My monitoring dashboard* DEMO***<YOUR_USERNR>*** Namespace: *http://demo*	

Explanation	Screenshot
151. Push button *Settings* to replace the left chart below.	
152. Search for your chart by scrolling through the list. Mark the chart you created and click on the Select Button	
153. Look at left chart below that has been changed and updated	
154. Push button *Settings* to replace the right chart below.	
155. Select your pattern and push button *Select.*	

Explanation	Screenshot
156. Look at right chart below that has been changed and updated	
157. Click on the button Setting and push button Save to save your monitoring dashboard.	

6.1. 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

THE BEST RUN SAP