

Secure the Intelligent Enterprise with SAP Enterprise Threat Detection

Exercise: Working with SAP Enterprise Threat Detection

Version December 2020

TABLE OF CONTENTS

1.	SECURITY EXPERT - WORKING WITH THE FORENSIC LAB	3
1.1.	Filtering Data.....	3
1.2.	Modelling Charts.....	5
1.3.	Browse through the data and model your own individual charts.....	7
1.4.	Working with Value Lists.....	8
1.5.	Modeling Attack Detection Patterns	9
1.6.	Summary.....	15
2.	BROWSE AND MODEL.....	15
2.1.	Browse through the data and model your own individual Attack Detection Pattern.....	15
2.2.	Summary.....	19
3.	PROCESSING ALERTS AND INVESTIGATIONS.....	19
3.1.	Viewing Alerts.....	20
3.2.	Investigating Alerts	23
3.3.	Saving Evidence for Attacks	31
3.4.	Summary.....	32
4.	PSEUDONYMIZATION OF USER DATA	32
4.1.	Determining the True Identity of Users.....	32
4.2.	Logging Access to User Identities.....	36
4.1.	Summary.....	36
5.	MONITORING DASHBOARDS	36
5.1.	Viewing Default Monitoring Dashboard.....	36
5.2.	Building your own Monitoring Dashboard	38
5.1.	Summary:.....	40
6.	LOG LEARNING – HOW TO LEARN A NEW LOG SOURCE	41
6.1.	Creating a new Log Type in the Knowledge Base.....	41
6.2.	Creating a new Log Learning Run from Unrecognized Logs	43
6.3.	Interpreting Semantic Events in the Log	44
6.4.	Verifying the new Log Type in the Forensic Lab.....	49
6.5.	Summary:.....	49

ETD Demo Users in the ETD System

- **Username:** Demo01, ..., Demo20
- **Password:** Welcome0

Connected S4H-System

- **Username:** Demo01, ..., Demo20
- **Password:** Welcome1

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

- DEMO01 → DEMOONE
- DEMO02 → DEMOTWO
-
- DEMO10 → DEMOTEN

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. 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.


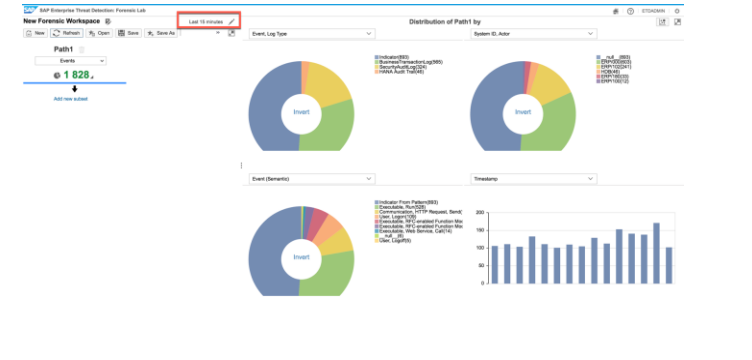
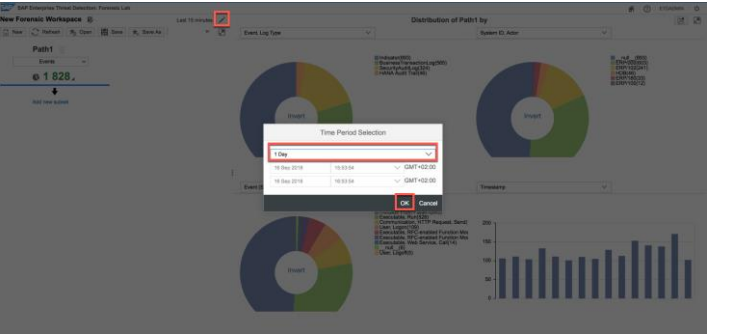
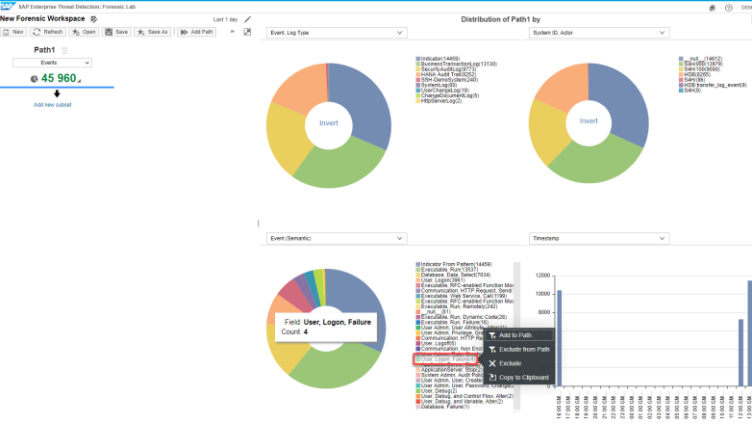
Tool Aspect: The forensic lab is one the most important application in SAP Enterprise Threat Detection and helps you to gain insight about what is going on at present in your system landscape.

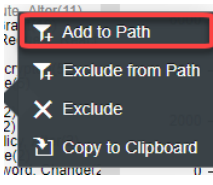
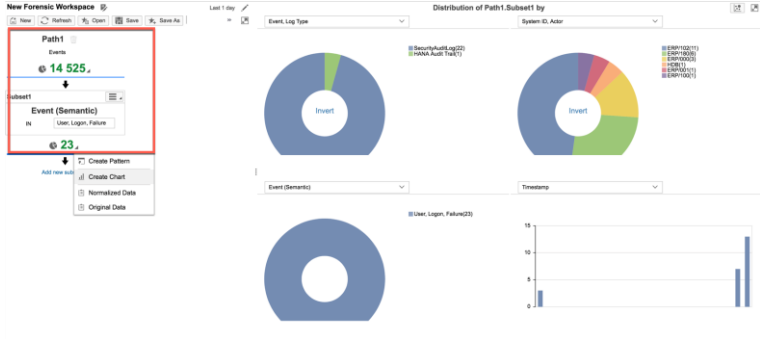
Forensic lab supports workspaces for identifying and analyzing weaknesses or attacks and supports the modelling of charts or attack detection patterns. For attack detection patterns, you create the configurations, which you want SAP Enterprise Threat Detection to use to scan for events that match the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

1.1. Filtering Data


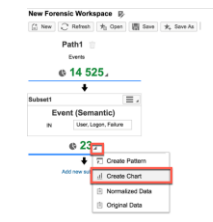
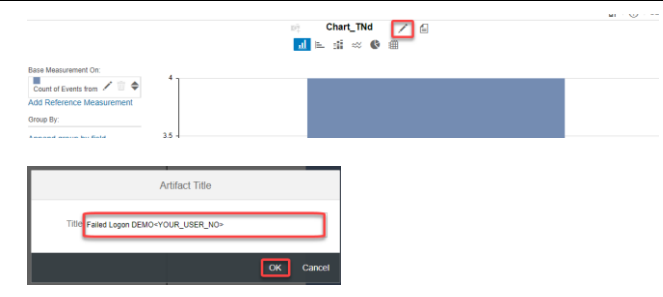
In this exercise, you will display failed log on attempts, and you will learn how filters can be created.


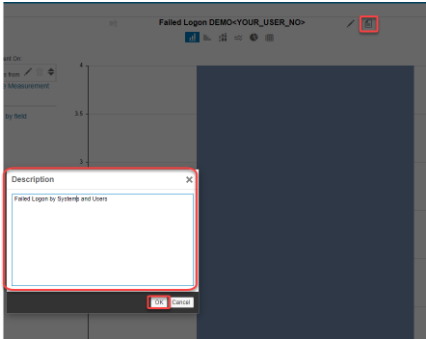
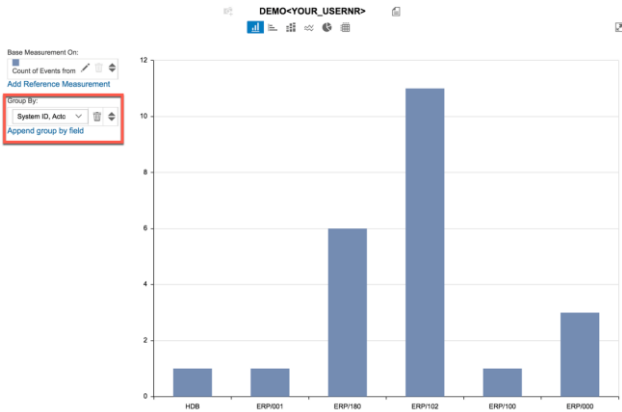
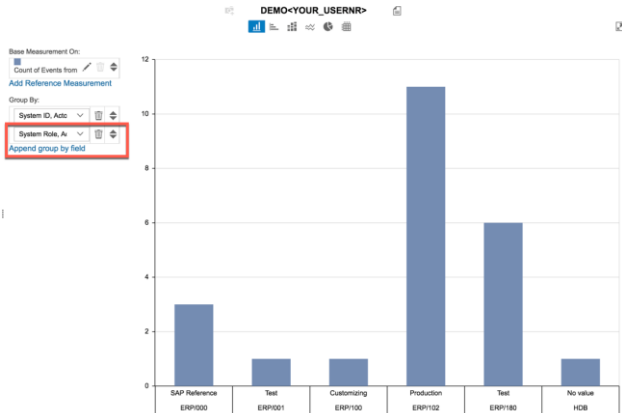
Explanation	Screenshot
<p>1. Open tile Forensic Lab in the SAP Enterprise Threat Detection Launchpad.</p>	
<p>2. The initial screen of the forensic lab shows the log events from last 15 minutes. The left part of the workspace contains the filter paths. The right part of the workspace is used to display the log events. They are called browsing charts. You can e.g. see which log types – <i>Event</i>, <i>Log Type</i> - are received, from which systems - <i>System ID</i>, <i>Actor</i> - or which actions - <i>Event (Semantic)</i> - have been performed. Change the drop-down value in one of the browsing charts to see information about other semantic attributes.</p>	
<p>3. Push button <i>Change time period</i>. Change time period selection to 1 hour and push button <i>OK</i> to analyze the log events from last day.</p> <p>Look at the path and the browsing charts that have been updated.</p>	
<p>4. To add a filter for failed logon events, click on legend <i>User Logon, Failure</i>.</p>	

Explanation	Screenshot
5. Select menu item <i>Add to Path</i> . This will create a filter for failed logons that have been occurred in the last day. It is shown as <i>Subset</i> in the filter path.	 A screenshot of a context menu with four options: 'Add to Path' (highlighted with a red box), 'Exclude from Path', 'Exclude', and 'Copy to Clipboard'.
6. Look at <i>Path1</i> and see the subset that has been added. Observe that the browsing charts have been updated as well.	 A screenshot of the 'New Forensic Workspace' interface. On the left, the 'Path1' tree shows a subset of 23 events. The main area displays several charts: two donut charts labeled 'Invest' and 'Event (Semantic)', and a bar chart labeled 'User Logon Failure(23)'. The charts are updated to reflect the selected subset.

1.2. 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
7. 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 <i>Create Chart</i>	 A screenshot of the 'New Forensic Workspace' interface. The 'Create Chart' button (a small square with a plus sign) is highlighted with a red box. A dropdown menu is open, showing options: 'Create Pattern', 'Create Chart' (highlighted with a red box), 'Normalized Date', and 'Original Date'.
8. Change the chart name: <i>Click on the pencil symbol</i> <i>In the Popup enter:</i> <i>Failed Logon DEMO<YOUR_USERNR></i> Press o.k.	 A screenshot showing the chart editing process. The top part shows the 'Chart_TND' chart with a pencil icon highlighted. Below, a 'Chart_TND' chart is shown with a blue bar. At the bottom, a 'Title' dialog box is open, showing the title 'Failed Logon DEMO<YOUR_USER_NO>' and 'OK' and 'Cancel' buttons.

Explanation	Screenshot														
<p>9. Push button . Add the following description and push button <i>OK</i>.</p> <p>Description: <i>Failed Logon Events by Systems and Users</i></p>															
<p>10. Click on link <i>Append group by field</i> and add field <i>System ID, Actor</i>. The chart will be updated with the system information on which failed logon attempts have been observed.</p>	 <table border="1"> <thead> <tr> <th>System ID, Actor</th> <th>Count of Events</th> </tr> </thead> <tbody> <tr> <td>HCB</td> <td>1</td> </tr> <tr> <td>ERP001</td> <td>1</td> </tr> <tr> <td>ERP180</td> <td>6</td> </tr> <tr> <td>ERP182</td> <td>11</td> </tr> <tr> <td>ERP180</td> <td>1</td> </tr> <tr> <td>ERP000</td> <td>3</td> </tr> </tbody> </table>	System ID, Actor	Count of Events	HCB	1	ERP001	1	ERP180	6	ERP182	11	ERP180	1	ERP000	3
System ID, Actor	Count of Events														
HCB	1														
ERP001	1														
ERP180	6														
ERP182	11														
ERP180	1														
ERP000	3														
<p>11. Click on link <i>Append group by field</i> and add field <i>System Role, Actor</i>. The chart will be updated with additional system role information.</p>	 <table border="1"> <thead> <tr> <th>System Role, Actor</th> <th>Count of Events</th> </tr> </thead> <tbody> <tr> <td>SAP Reference</td> <td>3</td> </tr> <tr> <td>Test</td> <td>1</td> </tr> <tr> <td>Customizing</td> <td>1</td> </tr> <tr> <td>Production</td> <td>11</td> </tr> <tr> <td>Test</td> <td>6</td> </tr> <tr> <td>No value</td> <td>1</td> </tr> </tbody> </table>	System Role, Actor	Count of Events	SAP Reference	3	Test	1	Customizing	1	Production	11	Test	6	No value	1
System Role, Actor	Count of Events														
SAP Reference	3														
Test	1														
Customizing	1														
Production	11														
Test	6														
No value	1														

Explanation	Screenshot
<p>12. Click on link <i>Append group by field</i> and add field <i>Account Name Pseudonym, Targeted</i>. The chart will be updated with additional user information.</p>	
<p>13. You can now save your changes. On the left lower area enable checkbox <i>Shared</i>. This allows other users to access your charts. Push button <i>Save</i>.</p>	
<p>14. Provide name and namespace for your workspace and push button <i>OK</i>.</p> <p>Name: <i>My first workspace</i> DEMO<YOUR_USERNR></p> <p>Namespace: <i>http://demo</i></p>	

1.3. 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):

Subset Selection

Current Subset

Path1.Subset1

Field

Service, Transaction Name

?

Excluded

☒ Value
☐ Reference

Operator

=

Read Values from

☒ Logs
☐ Knowledge Base

Value

SE37

OK

Cancel

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:

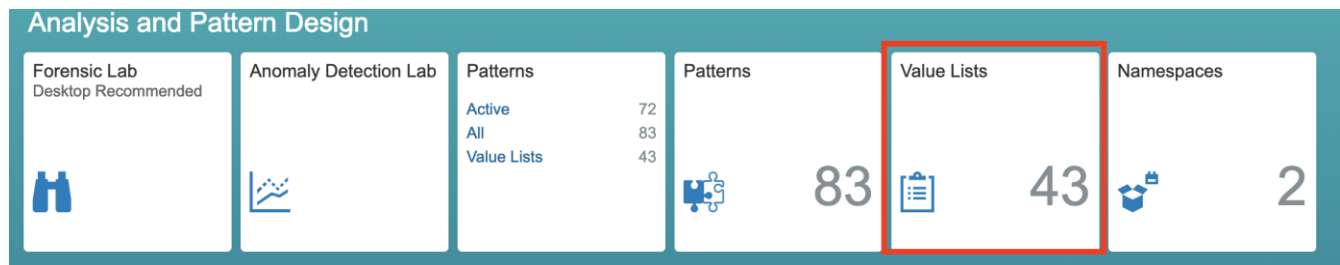
<Chart name> DEMO<YOUR_USERNR>

1.4. 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*:




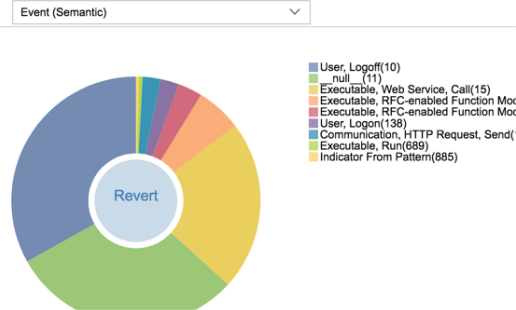
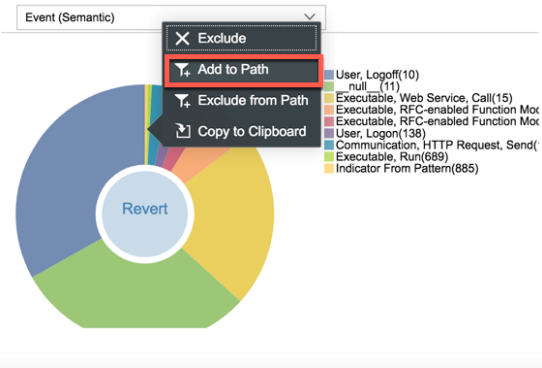
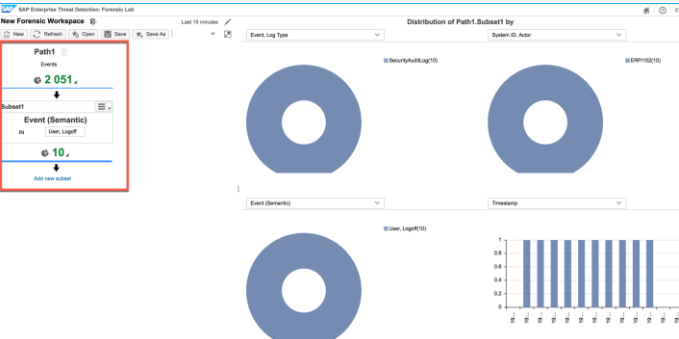
In the *Value List* application, you can view existing ones that are delivered with SAP Enterprise Threat Detection


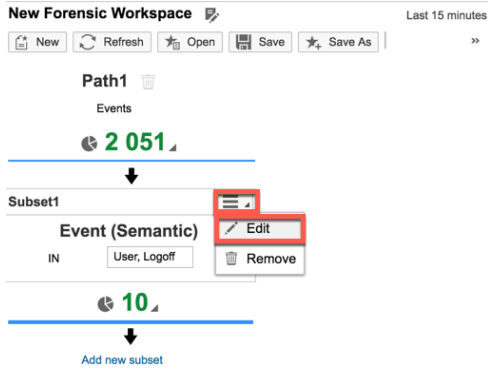


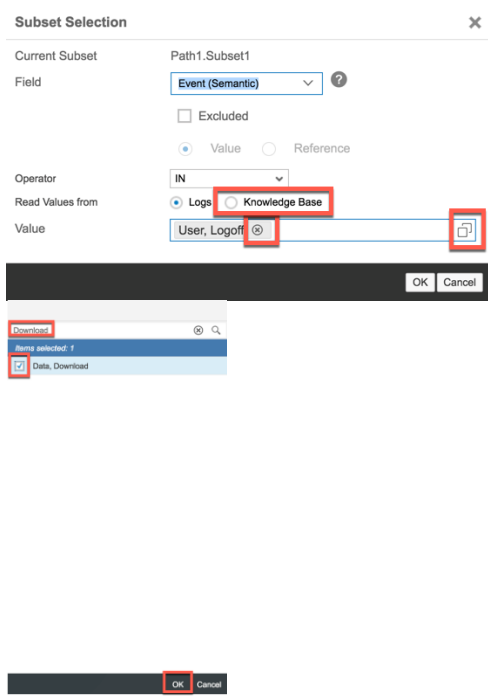
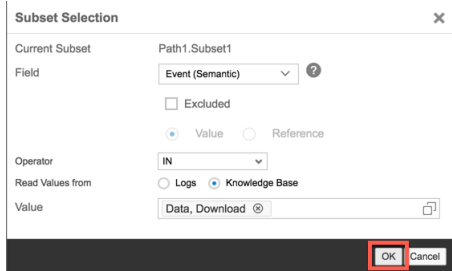
The value lists delivered with SAP Enterprise Threat Detection have pre-defined values, that can be adjusted and enhanced

You can also create your own value lists

1.5. 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 a download of data exceeds a suspicious volume threshold.

Explanation	Screenshot
15. Push button <i>New</i> to create a new workspace.	
16. Look at the left lower bottom chart. If the <i>_null_</i> value dominates the chart, click <i>Invert</i> in the middle of the chart.	
17. Click on a section of the chart and select menu item <i>Add to Path</i> .	
18. Look at <i>Path1</i> and see that the subset has been added. Observe that the browsing charts have been updated as well.	

Explanation	Screenshot
<p>19. Change the subset to filter for download events. Click on the top right button of the subset  and select menu item <i>Edit</i>.</p>	
<p>20. Change selection of <i>Read Values From</i> from <i>Logs</i> to <i>Knowledge Base</i>. This is needed in case no download events can be found in the forensic lab. In <i>Value</i> remove the entry by clicking on button  and push button for <i>F4-Help</i>.</p> <p>Enter search term <i>Download</i> and click on button . Enable selection for <i>Data, Download</i> and push button <i>OK</i>.</p>	
<p>21. Push button <i>OK</i> to apply filter for download events.</p>	

Explanation

22. 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*

Screenshot

The screenshot shows the 'Subset Selection' dialog for 'Path1.Subset1'. The 'Field' is set to 'System ID, Actor'. The 'Operator' is set to 'IN VALUE LIST'. The 'Value' is set to 'DemoCriticalSystems'. The 'Read values from' section has 'Logs' selected. The 'OK' button is highlighted with a red box.


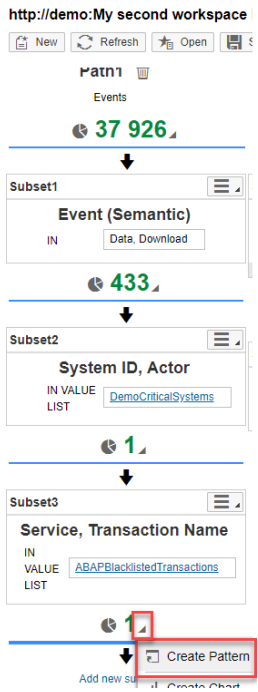
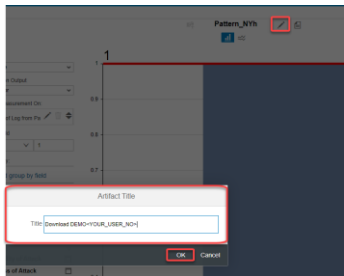
23. Click on link *Add new subset* and enter the following Subset Selection:

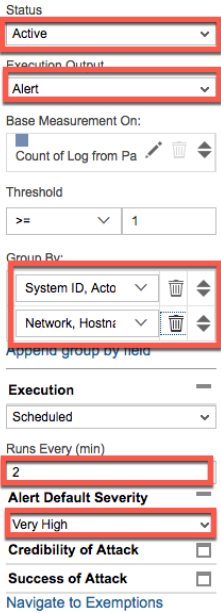
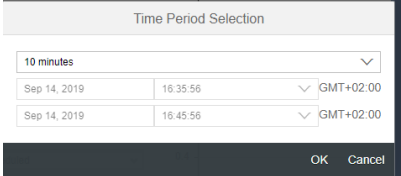
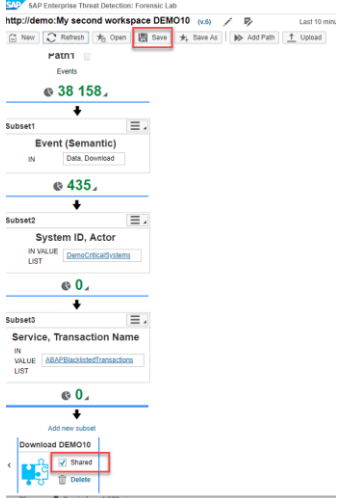
Field: *Service, Transaction Name*

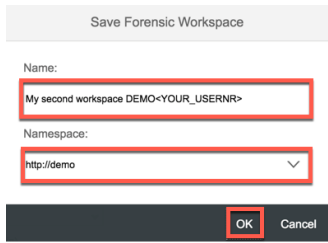
Operator: *IN VALUE LIST*

Value: *ABAPBlacklistedTransactions*

The screenshot shows the 'Subset Selection' dialog for 'Path1.Subset3'. The 'Field' is set to 'Service, Transaction Name'. The 'Operator' is set to 'IN VALUE LIST'. The 'Value' is set to 'ABAPBlacklistedTransactions'. The 'Read values from' section has 'Logs' selected. The 'OK' button is highlighted with a red box.

Explanation	Screenshot
<p>24. 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 <i>Create Pattern</i>.</p>	
<p>25. Change the pattern name:</p> <p><i>Download DEMO<YOUR_USERNR></i></p>	

Explanation	Screenshot
<p>26. Change the following values:</p> <p>Status: <i>Active</i></p> <p>Execution Output: <i>Alert</i></p> <p>Group By: <i>System ID, Actor</i> <i>Network, Hostname, Initiator</i> <i>Account Name Pseudonym, Acting</i></p> <p>Runs Every (min): 2</p> <p>Alert Default Severity: <i>Very High</i></p>	
<p>27. Change time period to 10 Minutes.</p>	
<p>28. You can now save your changes as you are done with modeling your pattern and workspace.</p> <p>On the left lower area enable checkbox <i>Shared</i>. This allows other users to access your pattern.</p> <p>Push button <i>Save</i>.</p>	

Explanation	Screenshot
<p>29. Provide name and namespace for your workspace and push button <i>OK</i>.</p> <p>Name: <i>My second workspace</i> <i>DEMO<YOUR_USERNR></i></p> <p>Namespace: <i>http://demo</i></p>	

1.6. 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

2. BROWSE AND MODEL

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 of your choice, and then simulate the attack within an SAP S/4H system to verify that your first and/or your second Pattern works.

2.1. 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 . On the new path you can create new filters and your own pattern.

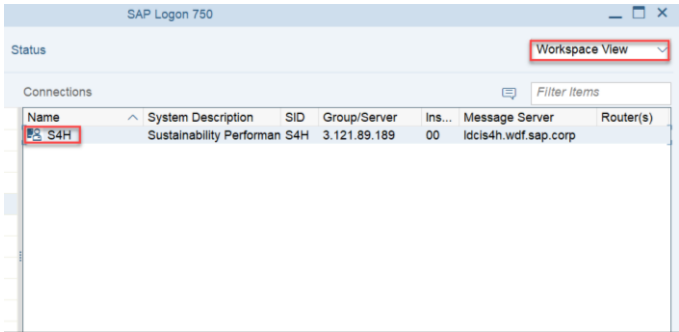
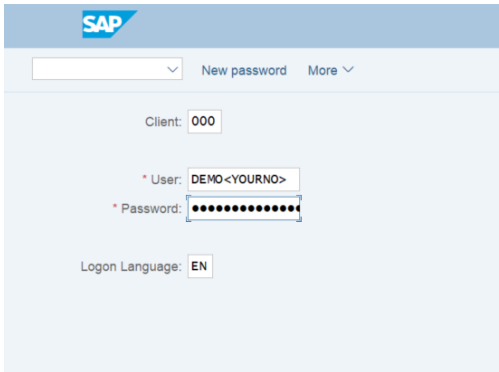
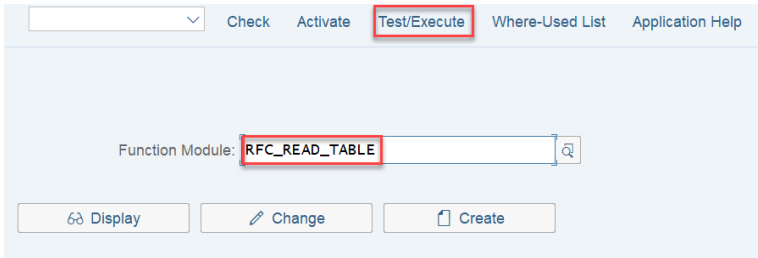

Hint: Create a Pattern about semantic events that are already seen within the Forensic Lab, so that later, you can test the Pattern by use of the incoming data or by being able to trigger the events within the connected SAP ERP system (see below).

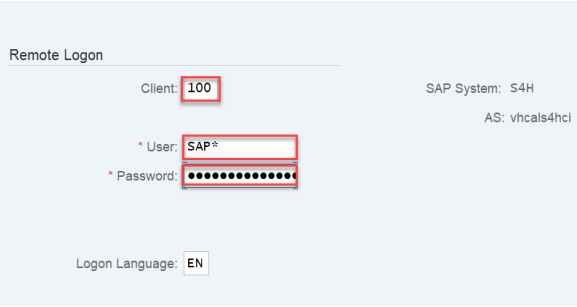
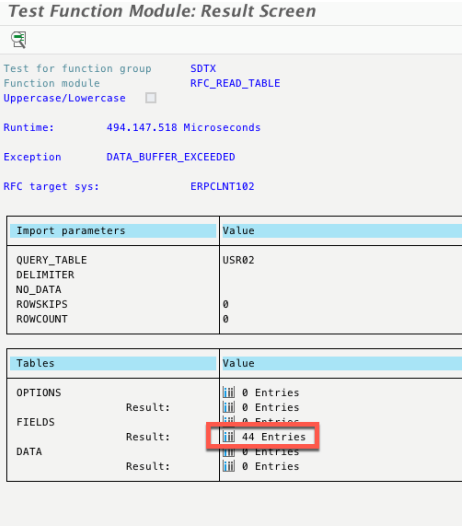
Make use of the following pattern name for your own created Attack Detection Patterns:

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

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

In this exercise you will put yourself in the role of the hacker and try to download sensitive information from an ERP system.

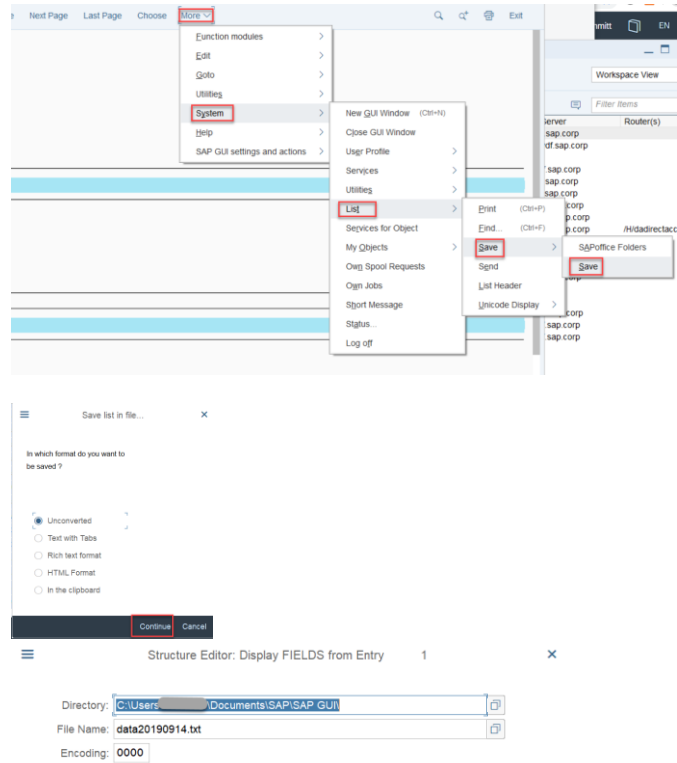
Explanation	Screenshot
30. Open SAP GUI, and enter the SAP system connect into the SAP Logon System list, as to the group you are related to (as to the distribution done at the beginning)	
31. Logon to S4H Client 000 with the following user: User: DEMO<YOUR Number>, (e.g. DEMO12) Password: Welcome1	
32. Start transaction SE37 – ABAP Function Modules. Enter value <i>RFC_READ_TABLE</i> and push button <i>Test/Execute</i> .	
33. Add the following values and push button <i>Execute</i> . RFC target sys: <i>S4HCLNT100</i> Query Table: <i>USR02</i>	

Explanation	Screenshot																				
<p>34. Now try to logon with SAP Standard user SAP*.</p> <p>Client: 100 User: SAP* Password: Master1234</p> <p>Press Enter</p>																					
<p>35. Click on the result of your RFC query to see the details.</p>	 <p>Test Function Module: Result Screen</p> <p>Test for function group SDTX Function module RFC_READ_TABLE Uppercase/Lowercase <input type="checkbox"/></p> <p>Runtime: 494.147.518 Microseconds Exception DATA_BUFFER_EXCEEDED RFC target sys: ERPCLNT102</p> <table border="1"> <thead> <tr> <th>Import parameters</th><th>Value</th></tr> </thead> <tbody> <tr> <td>QUERY_TABLE</td><td>USR02</td></tr> <tr> <td>DELIMITER</td><td></td></tr> <tr> <td>NO_DATA</td><td></td></tr> <tr> <td>ROWSKIPS</td><td>0</td></tr> <tr> <td>ROWCOUNT</td><td>0</td></tr> </tbody> </table> <table border="1"> <thead> <tr> <th>Tables</th><th>Value</th></tr> </thead> <tbody> <tr> <td>OPTIONS</td><td>0 Entries</td></tr> <tr> <td>FIELDS</td><td>44 Entries</td></tr> <tr> <td>DATA</td><td>0 Entries</td></tr> </tbody> </table>	Import parameters	Value	QUERY_TABLE	USR02	DELIMITER		NO_DATA		ROWSKIPS	0	ROWCOUNT	0	Tables	Value	OPTIONS	0 Entries	FIELDS	44 Entries	DATA	0 Entries
Import parameters	Value																				
QUERY_TABLE	USR02																				
DELIMITER																					
NO_DATA																					
ROWSKIPS	0																				
ROWCOUNT	0																				
Tables	Value																				
OPTIONS	0 Entries																				
FIELDS	44 Entries																				
DATA	0 Entries																				

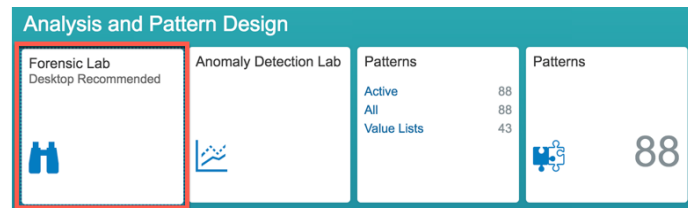
Explanation

36. To download the content, choose
More→System→List→Save→Save.
Save content on your local file system.

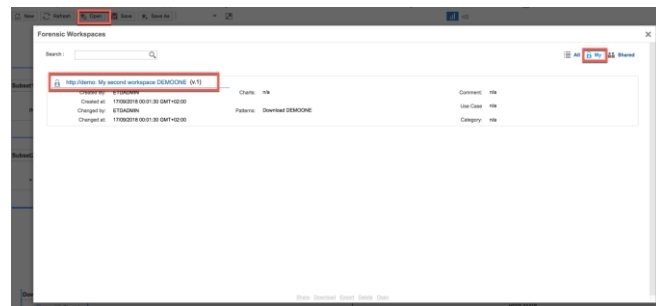
Screenshot

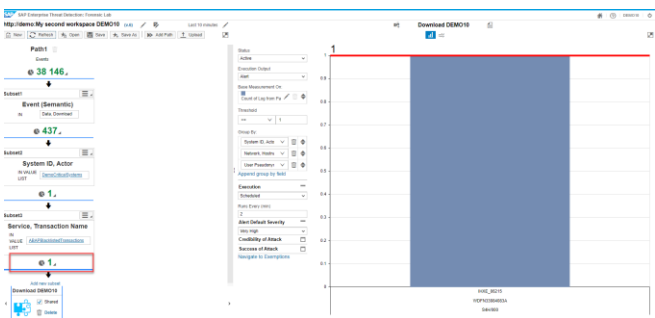



37. Open SAP Enterprise Threat Detection Launchpad and click on tile *Forensic Lab* to verify the download events.



38. 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
39. Look at <i>Path1</i> and find the download events.	
40. Open SAP Enterprise Detection Launchpad and see that the tiles <i>Open Alerts</i> and <i>Threat Situation Last Hour</i> have been updated.	

2.2. 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.

3. PROCESSING ALERTS AND INVESTIGATIONS

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

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

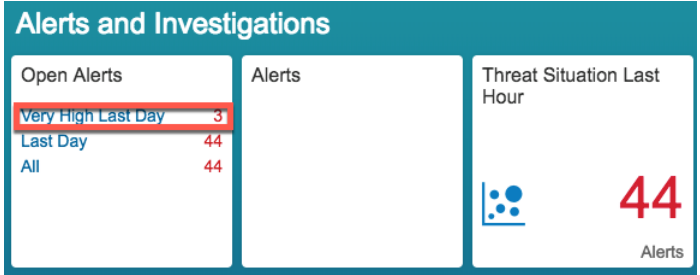
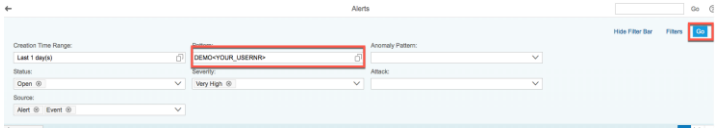
Then you may need to collect the evidences and to follow a Standard Operation Procedure for the further actions.

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

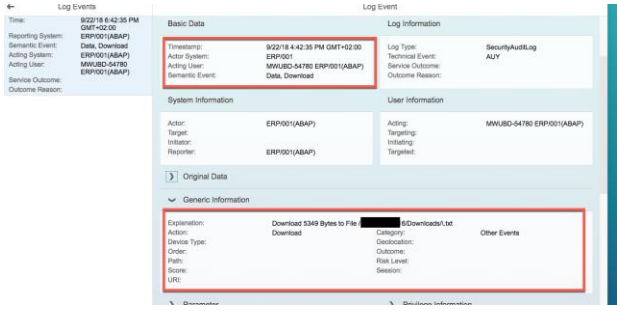
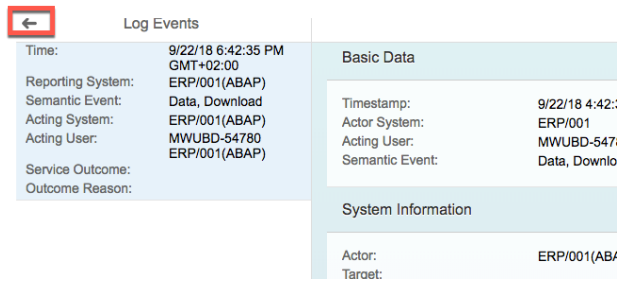
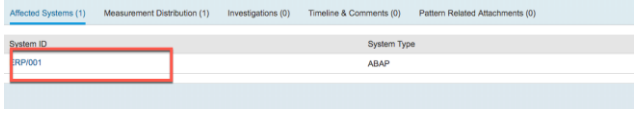
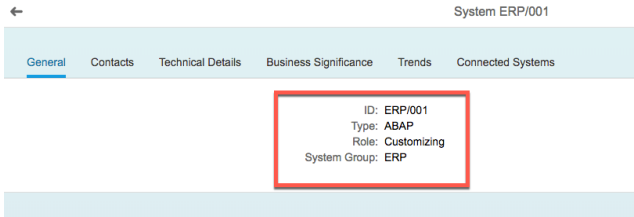
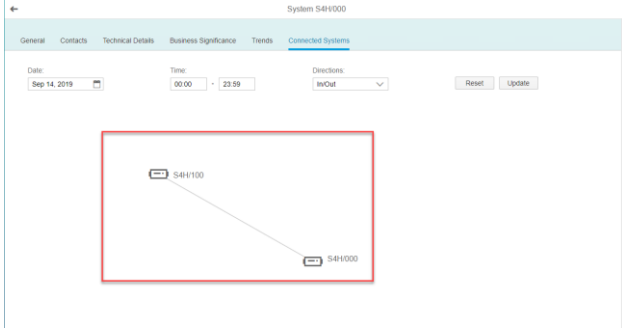
3.1. Viewing Alerts

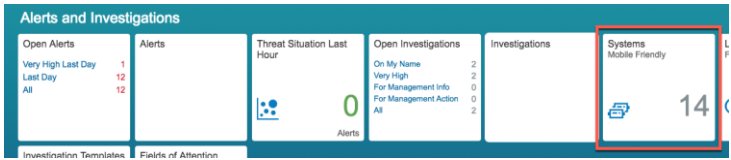
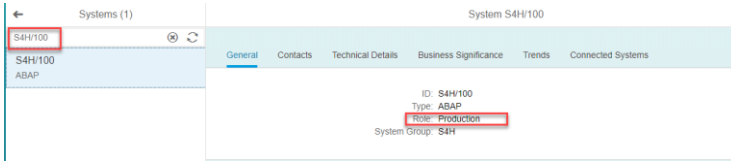
As the monitoring agent of a company, you need to monitor the alerts and react immediately. In the case of a suspected attack, it is usually the user or the hostname behind it or the system affected that you need to identify.

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

Explanation	Screenshot
<p>41. Open tile <i>Open Alerts – Very High Last Day</i>.</p>	
<p>42. Open Filter Bar. Add the pattern you have created in step 24 as filter and push button GO.</p> <p><i>Download DEMO<YOUR_USERNR></i></p> <p><i>Comment:</i> <i>This is only needed for this exercise due to having multiple users working on the same exercise. In general the Alerts List User Interface is used as a worklist for alerts by the monitoring agent.</i></p>	

Explanation	Screenshot
<p>43. Look at the alert that has been raised. The severity of the alert provides the first 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.</p>	
<p>44. Push button <i>View Threat Situation</i> and see e.g. the <i>Network Hostname Initiator</i> that has been used for downloading data.</p>	
<p>45. Switch back to the <i>Alerts List View</i> and click on alert <i>ID</i> to see more details about the alerts</p>	
<p>46. 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.</p>	
<p>47. Click on the <i>Triggering Events</i> to see more details.</p>	

Explanation	Screenshot
<p>48. 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.</p>	
<p>49. Click on button <i>Back</i> to return to the alert details view.</p>	
<p>50. Click on <i>System ID</i> to see the details of the affected system.</p>	
<p>51. Look at the details of the affected system.</p>	
<p>52. Under tab <i>Connected Systems</i> you can see that the affected system has done a remote communication.</p>	

Explanation	Screenshot
53. Open a new browser tab and open SAP Enterprise Threat Detect Launchpad. Open tile <i>Systems</i> to see the details of the system to which a remote communication has taken place.	
54. Enter the System ID in the search field and select the system to see the details.	

3.2. Investigating Alerts

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

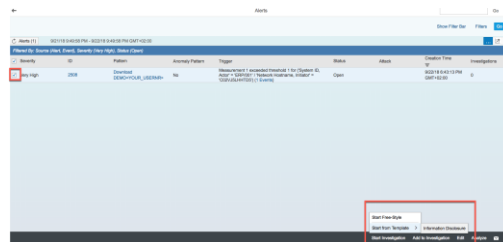
When the monitoring agent considers an alert suspicious, an investigation gets started. The investigation gets a description, a severity, a status and comments can be added. The investigation can be shared easily, either in emails or as tiles in the launchpad, or even as a PDF file. More alerts and other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

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

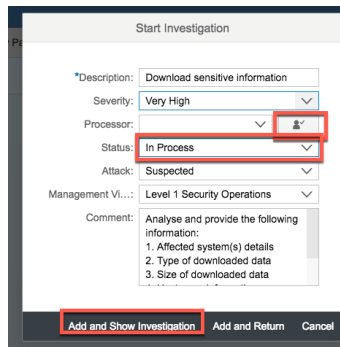
Explanation

Screenshot

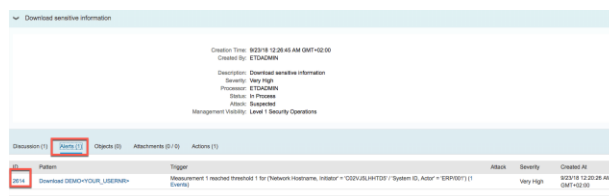
55. In the Alerts worklist view, select the alert and push button *Start Investigation*. Choose *Start From Template* → *Information Disclosure*



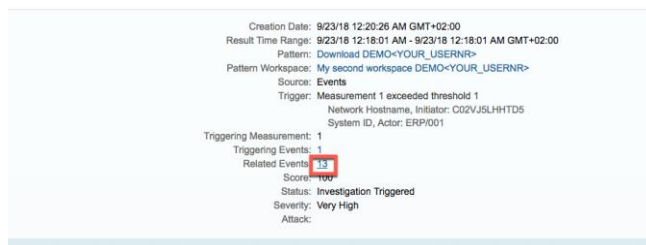
56. Set yourself as processor of the investigation and check the instructions how to handle this type of alert. Push button *Add and Show Investigation*.



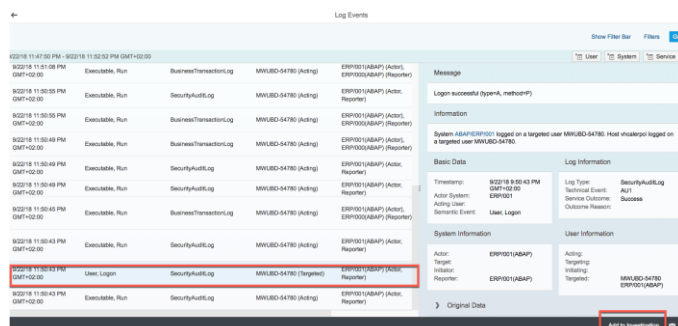
57. Click on tab *Alerts* and click on alert *ID* to further investigate details of the alert.

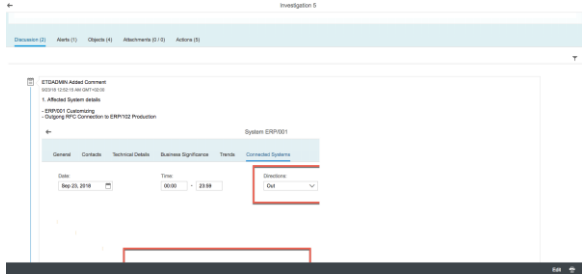
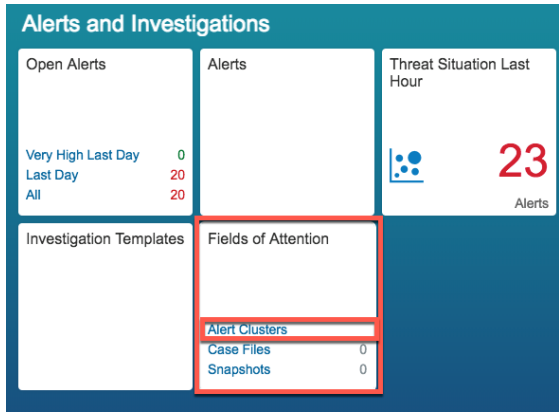
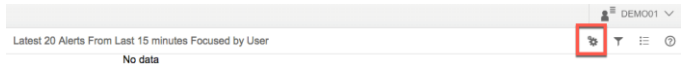
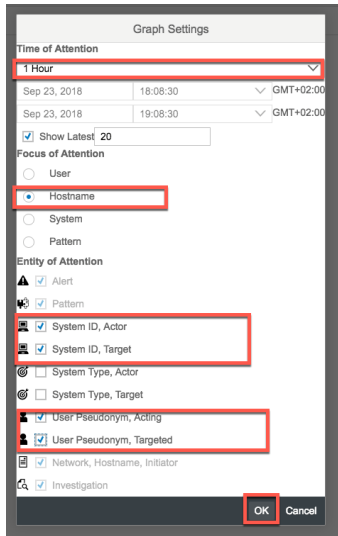


58. Click on related events to gain more insight about the potential threat.

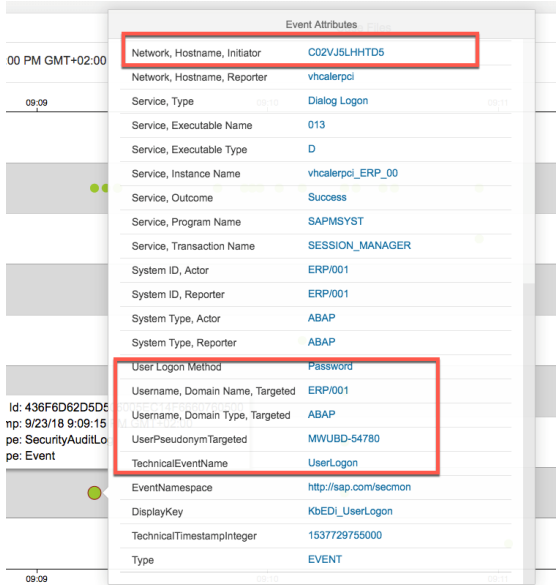

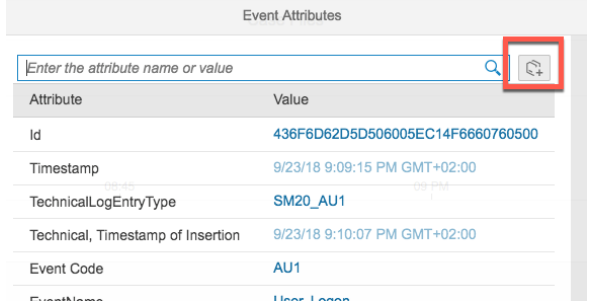
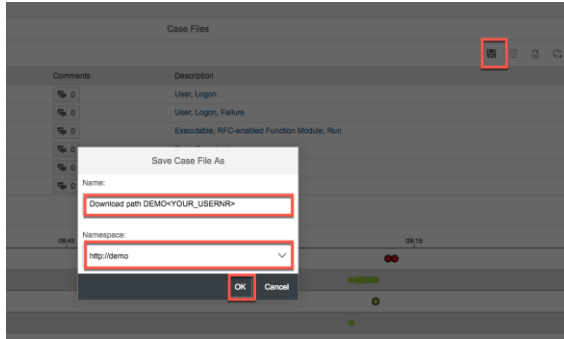
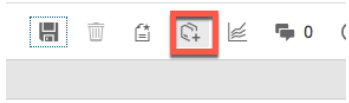


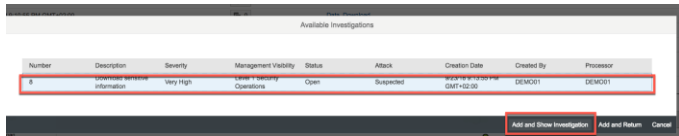
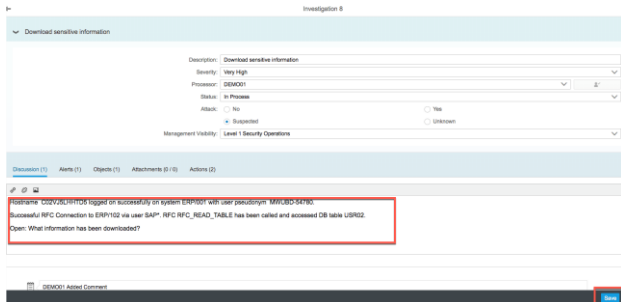
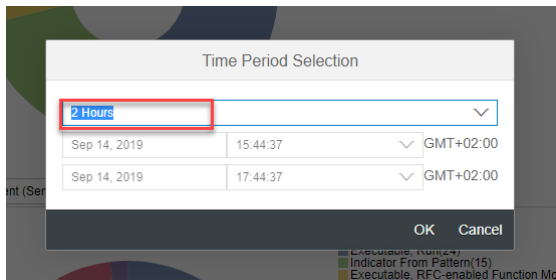
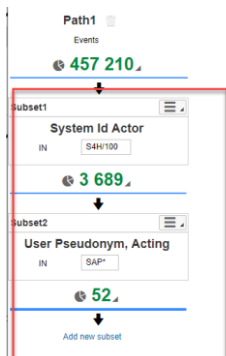
59. Select the event row to see more details. Add to your investigation if relevant.



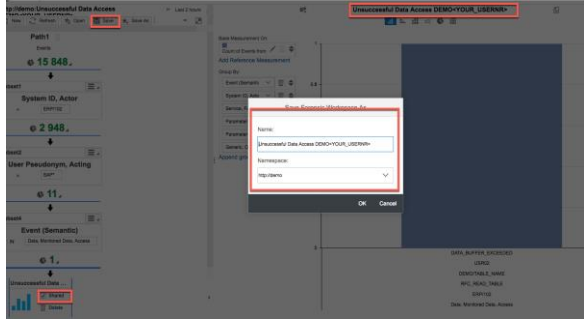
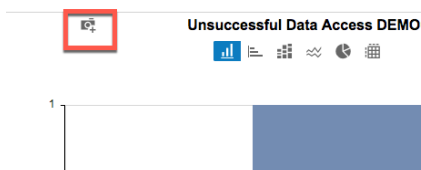
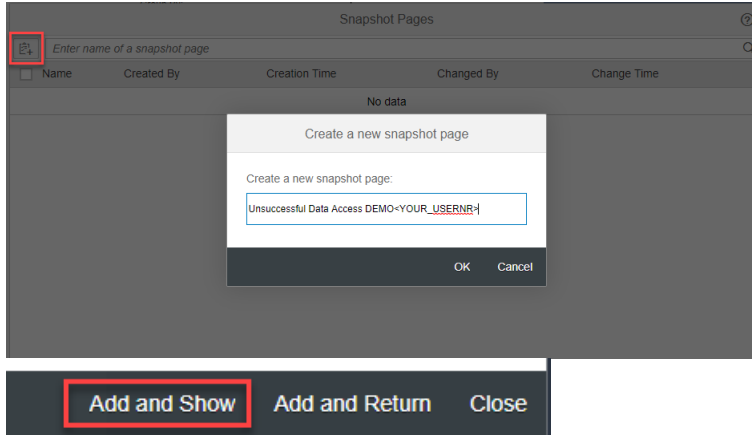
Explanation	Screenshot
<p>60. Update Investigations with your current investigation analysis results. E.g. use the tab discussions and add comments or screenshots to affected system details, size of downloaded data, hostname or user information. Screenshots can be added via Drag & Drop.</p>	
<p>61. Make 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 <i>Fields of Attention – Alert Clusters</i>.</p>	
<p>62. Choose button <i>Settings</i>.</p>	
<p>63. Change Graph Settings as follows:</p> <p>Time range: <i>1 Hour</i></p> <p>Focus of attention: <i>Hostname</i></p> <p>Entity of attention: <i>System ID, Actor</i> <i>System ID, Target</i> <i>User Pseudonym, Acting</i> <i>User Pseudonym, Targeted</i></p> <p>Push button <i>OK</i>.</p>	

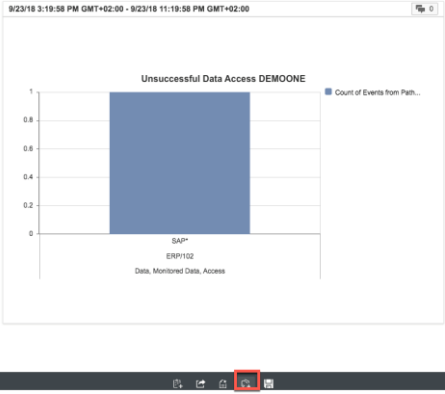
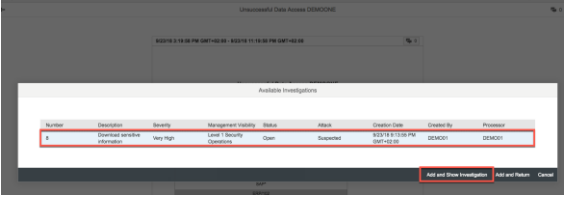
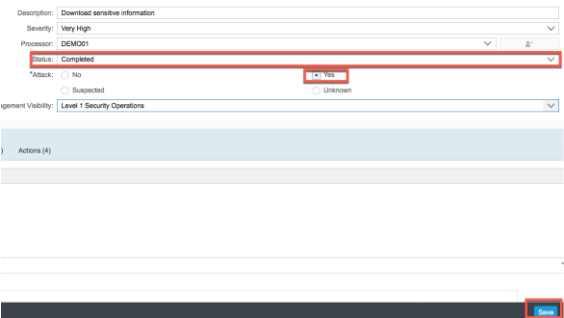
Explanation	Screenshot
<p>64. Push button <i>Filter</i> and only enable the hostname that has triggered the alerts.</p>	
<p>65. Look at the alert graph focusing on the selected hostname and see how it is connected to patterns, alerts and systems. Click on the hostname node to see further details.</p>	
<p>66. Look at the alerts and events shown on the timeline where this hostname was involved.</p>	
<p>67. 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.</p>	

Explanation	Screenshot
68. Click on the circle to see the event details.	
69. Push button <i>Add to Case File</i>  to add all relevant events that are related to the alert creation.	
70. Save your case file by pushing the button <i>Save</i> . Provide name and namespace as follows and push button <i>OK</i> . Name: Download path <i>DEMO<YOUR_USERNR></i> Namespace: <i>http://demo</i>	
71. Push button <i>Add to Investigation</i> .	

Explanation	Screenshot
72. Select your investigation and push button <i>Add and Show Investigation</i> .	
73. Update the investigation with your analysis results.	
74. 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.	
75. Create the following filters: System ID, Actor = S4H/100 User Pseudonym, Acting = SAP*	

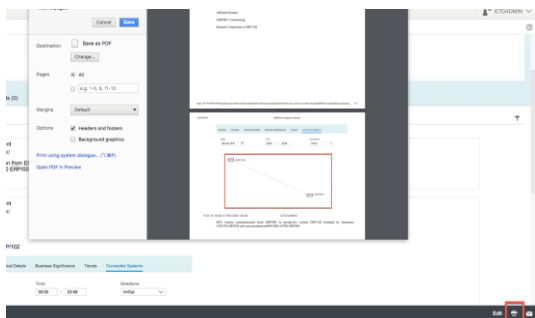
Explanation	Screenshot
76. Look at the browsing chart for <i>Event (Semantic)</i> and see the event <i>Data, Monitored Data, Access</i> .	
77. Add a filter for this event.	
78. Create a chart with the following <i>Group By</i> fields: <i>Event (Semantic)</i> <i>System ID, Actor</i> <i>User Pseudonym,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

Explanation	Screenshot
<p>79. Provide the following chart name.</p> <p>Chart name: <i>Unsuccessful Data Access</i> <i>DEMO<YOUR_USERNR></i></p> <p>Enable checkbox <i>Shared</i> and push button <i>Save</i>. Provide the following workspace name.</p> <p>Name: <i>Unsuccessful Data Access</i> <i>DEMO<YOUR_USERNR></i> Namespace: <i>http://demo</i></p>	
<p>80. Push button <i>Add chart to snapshot page</i>.</p>	
<p>81. Push button <i>Create a new snapshot page</i>. Provide the following snapshot page name and push button <i>Add and Show</i>.</p> <p>Snapshot page name: <i>Unsuccessful Data Access</i> <i>DEMO<YOUR_USERNR></i></p>	

Explanation	Screenshot
82. Push button <i>Add snapshot page to investigation.</i>	
83. Select your investigation and push button <i>Add and Show Investigation.</i>	
84. Edit and update the investigation with your findings and close it.	

3.3. Saving Evidence for Attacks

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

Explanation	Screenshot
<p>85. Within an investigation details push button <i>Print</i>. Push <i>Save</i> to save the content of an investigation as PDF file.</p> <p>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*.</p>	

3.4. Summary

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

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

4. PSEUDONYMIZATION OF USER DATA

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

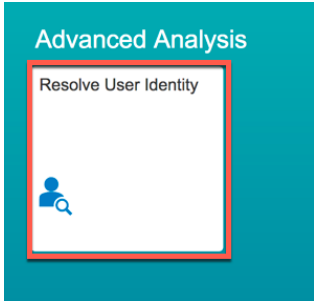
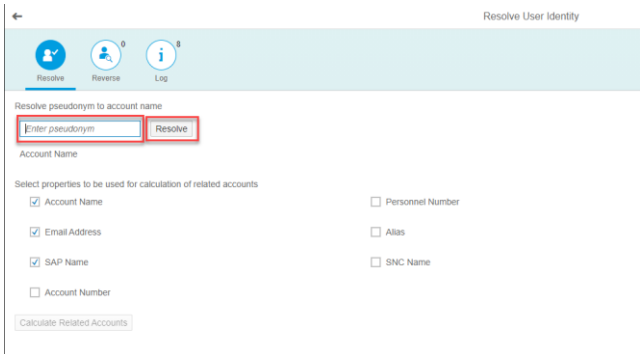
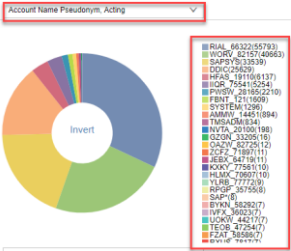
Tool Aspect: You will learn how to resolve the User Pseudonym.

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

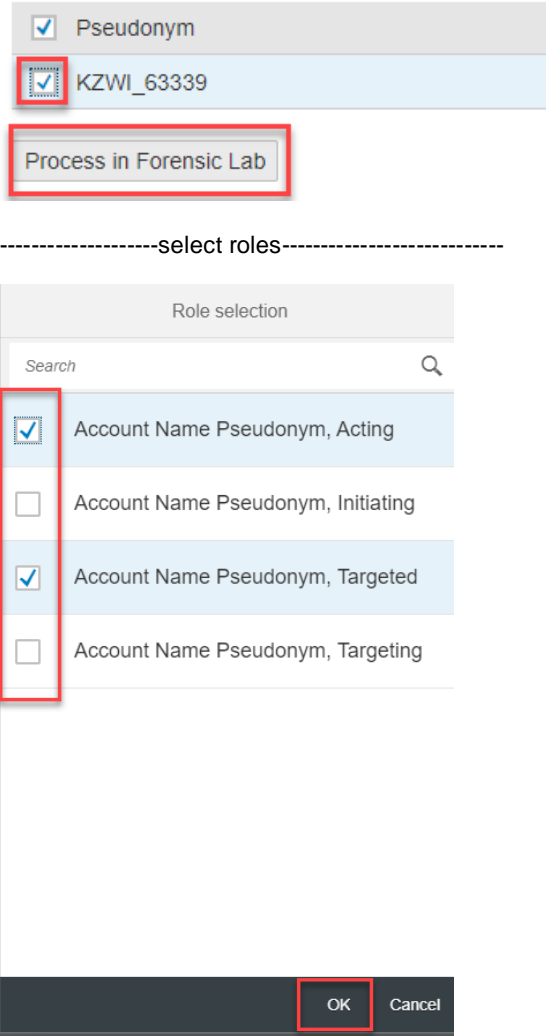
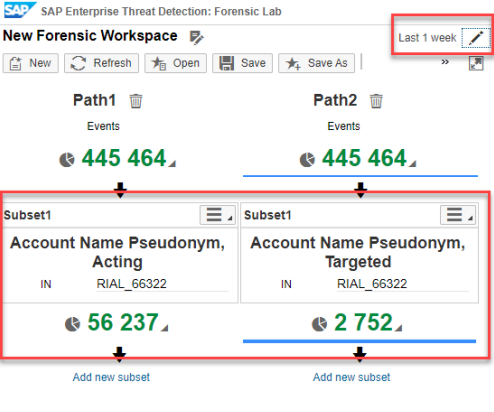
SAP Enterprise Threat Detection frequently changes the pseudonym associated with a user. The applications of SAP Enterprise Threat Detection, such as the forensic lab, can only access the current pseudonym of a user. You cannot use your past knowledge of user pseudonyms to pursue a user. SAP Enterprise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

4.1. Determining the True Identity of Users

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


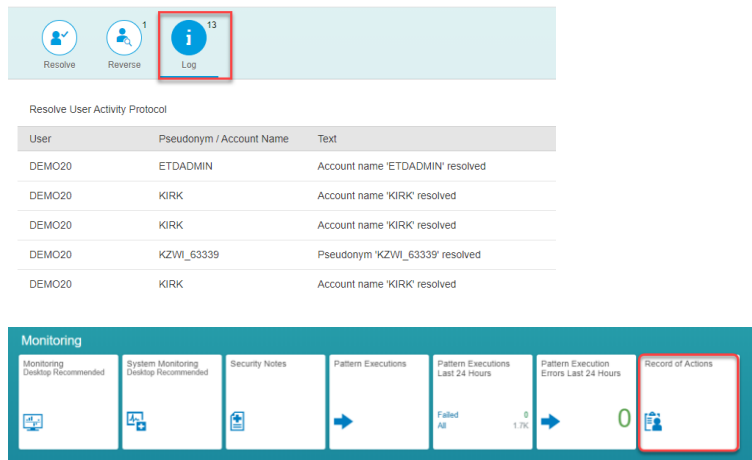
Explanation	Screenshot
<p>86. Logon to SAP Enterprise Threat Detection Launchpad with the following user and open tile <i>Resolve User Identity</i></p> <p>User: DEMO<YOUR_USERNR> Password: Welcome0</p>	
<p>87. Enter user pseudonym and push button <i>Resolve</i>. The clear user name is then shown below</p> <p>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 <i>User Pseudonym, Acting</i></p>	
	

Explanation	Screenshot
<p>88. You can check the complete user account information about correlations between Account Names, Mail Addresses, SAP Name IDs, Personal Numbers, Aliases, SNC Names, as far as these are maintained fully or partly within any SAP ERP systems, and a correlation can be established.</p> <p>Mark the corresponding Check Boxes and click on Button <i>Calculate Related Accounts</i></p> <p>Hint: It might even happen that for one resolved pseudonym several user-IDs appear as one account, because these IDs can e.g. be correlated via the same Mails Address maintained for several IDs in different SAP systems</p>	
<p>89. Do a Reverse Resolution from a clear User ID to a currently used Pseudonym.</p> <div data-bbox="203 959 336 1115" data-label="Image"> </div> <p>Enter a user ID and click on <i>Resolve</i>. The corresponding Pseudonym is shown.</p> <p>Hint: The functionality can be used in case of ad-hoc analysis, where a suspicious user behavior occurred outside ETD, and a user behavioral Analysis shall be executed</p>	

Explanation	Screenshot
<p>90. By marking the Pseudonym with the CheckBox, you can jump into the Forensic Lab, already pre-filtered on the desired roles of the User ID.</p> <p>After marking the CheckBox of the Pseudonym, click on <i>Process in Forensic Lab</i>. In Forensic Lab different filter paths are created for the selected roles, and the corresponding Events are shown in the selected time frame for the Pseudonym</p>	 <p>The screenshot shows the 'Process in Forensic Lab' button highlighted with a red box. Below it, the 'Role selection' dialog is displayed, showing a list of roles with checkboxes. The roles 'Account Name Pseudonym, Acting' and 'Account Name Pseudonym, Targeted' are selected, indicated by red boxes around their checkboxes. The 'OK' button is also highlighted with a red box.</p> <p>-----select roles-----</p> <p>-----Forensic Lab, see Events for each role of the User ID-----</p>  <p>The screenshot shows the 'New Forensic Workspace' interface. It displays two paths, Path1 and Path2, each with a count of 445,464 events. Below these, two subsets are shown: 'Account Name Pseudonym, Acting' with 56,237 events and 'Account Name Pseudonym, Targeted' with 2,752 events. The 'Last 1 week' filter is highlighted with a red box.</p>

4.2. Logging Access to User Identities

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

Explanation	Screenshot																		
<p>91. Click on tab <i>Log</i> and see the audit log for user resolutions</p> 	 <table><tr><th>User</th><th>Pseudonym / Account Name</th><th>Text</th></tr><tr><td>DEMO20</td><td>ETDADMIN</td><td>Account name 'ETDADMIN' resolved</td></tr><tr><td>DEMO20</td><td>KIRK</td><td>Account name 'KIRK' resolved</td></tr><tr><td>DEMO20</td><td>KIRK</td><td>Account name 'KIRK' resolved</td></tr><tr><td>DEMO20</td><td>KZWl_63339</td><td>Pseudonym 'KZWl_63339' resolved</td></tr><tr><td>DEMO20</td><td>KIRK</td><td>Account name 'KIRK' resolved</td></tr></table>	User	Pseudonym / Account Name	Text	DEMO20	ETDADMIN	Account name 'ETDADMIN' resolved	DEMO20	KIRK	Account name 'KIRK' resolved	DEMO20	KIRK	Account name 'KIRK' resolved	DEMO20	KZWl_63339	Pseudonym 'KZWl_63339' resolved	DEMO20	KIRK	Account name 'KIRK' resolved
User	Pseudonym / Account Name	Text																	
DEMO20	ETDADMIN	Account name 'ETDADMIN' resolved																	
DEMO20	KIRK	Account name 'KIRK' resolved																	
DEMO20	KIRK	Account name 'KIRK' resolved																	
DEMO20	KZWl_63339	Pseudonym 'KZWl_63339' resolved																	
DEMO20	KIRK	Account name 'KIRK' resolved																	

Hint: The same information plus furthermore about who was doing what within ETD is found in Tile *Record of Actions*

4.1. Summary

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

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

5. MONITORING DASHBOARDS

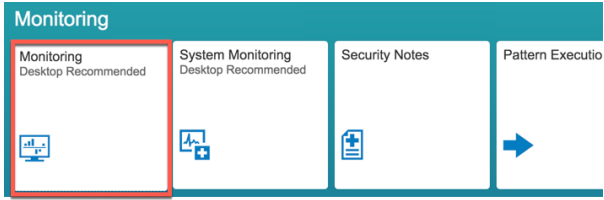
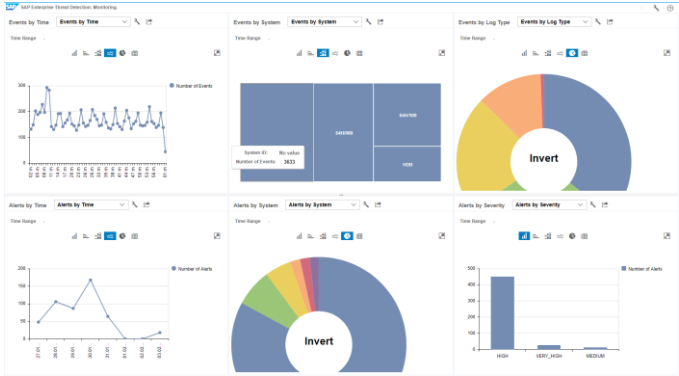

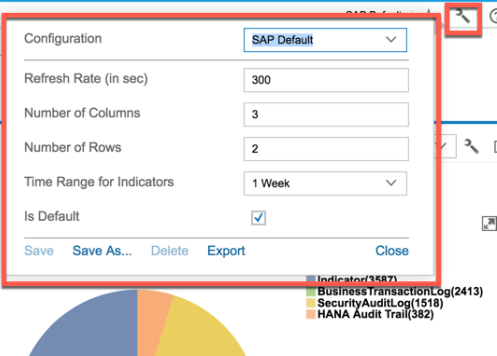
Security Aspect: During the daily operation of security monitoring a Security Agent needs to have an overview of the whole landscape. In ETD they include active alerts, the status of investigations and the log events. Since every agent has his own interested aspect, the content of the monitor must be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

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

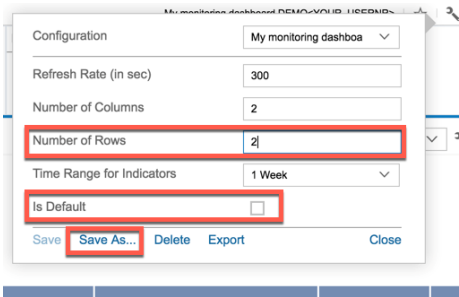
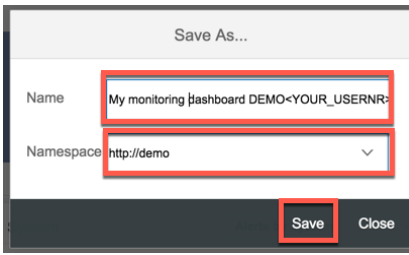
It is possible to define favorite monitoring dashboards by each individual user.

5.1. Viewing Default Monitoring Dashboard


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

Explanation	Screenshot
92. Open tile Monitoring in the SAP Enterprise Threat Detection Launchpad.	 <p>The screenshot shows the SAP Enterprise Threat Detection Launchpad interface. The 'Monitoring' tile is highlighted with a red rectangular box. Other visible tiles include 'System Monitoring Desktop Recommended', 'Security Notes', and 'Pattern Execution'.</p>
93. 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.	 <p>The screenshot displays the SAP Enterprise Threat Detection Monitoring dashboard. It features several charts: 'Events by Time' (line chart), 'Events by System' (treemap), 'Events by Log Type' (donut chart), 'Alerts by Time' (line chart), 'Alerts by System' (treemap), and 'Alerts by Severity' (bar chart). The dashboard is titled 'SAP Enterprise Threat Detection Monitoring'.</p>
94. Click on the button <i>Setting</i>  to see configuration details of the default monitoring dashboard.	 <p>The screenshot shows the 'Configuration' dialog box for the 'SAP Default' monitoring dashboard. The dialog includes the following settings:</p> <ul style="list-style-type: none"> Configuration: SAP Default Refresh Rate (in sec): 300 Number of Columns: 3 Number of Rows: 2 Time Range for Indicators: 1 Week Is Default: <input checked="" type="checkbox"/> <p>Buttons at the bottom include 'Save', 'Save As...', 'Delete', 'Export', and 'Close'. A legend at the bottom right lists indicators: BusinessTransactionLog(2413), SecurityAuditLog(1518), and HANA Audit Trail(382).</p>

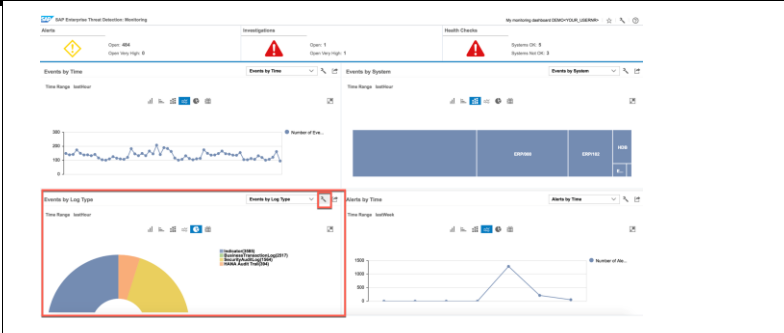
5.2. Building your own Monitoring Dashboard

Explanation	Screenshot
<p>95. Use the default monitoring dashboard to create you individual one. Change the values as follows and push button Save As ...</p> <p>Number of Columns: 2</p> <p>Number of Rows: 2</p> <p>Is Default: <i>not checked</i></p>	
<p>96. Enter the name and namespace and push button Save.</p> <p>Name: <i>My monitoring dashboard DEMO<YOUR_USERNR></i></p> <p>Namespace: <i>http://demo</i></p>	

Explanation

97. Push button *Settings*  to replace the left chart below.

Screenshot



98. Search for your chart by using the filter for column *Name*. Enter *DEMO*<*YOUR USERNR*> and push *ENTER*.

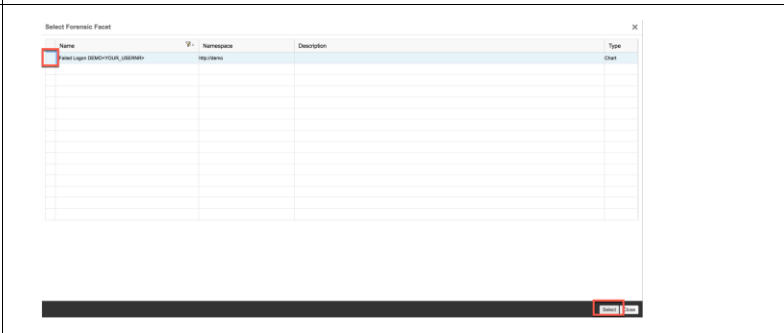
Select Forensic Facet

Name	Namespace	Description
Sort Ascending	http://sap.com/secmon	
Sort Descending	http://sap.com/secmon	
Filter DEMO<YOUR_USERN	http://sap.com/secmon/basis	Brute force login u
Columns	http://sap.com/secmon	Checks if the ABAI
	http://sap.com/secmon	
ABAP critical FM calls per SOAP rfc	http://sap.com/secmon/basis	Client calls critical
ABAP deactivated or deleted function modules	http://sap.com/secmon/basis	A user has tried to
ABAP deactivated or deleted reports	http://sap.com/secmon/basis	A user has tried to
ABAP function modules with removed RFC enablement	http://sap.com/secmon/basis	A user has tried to
ABAPLogonFailed	http://sap.com/secmon	
Access to Generic Path (Distinct) by Dialog User	http://sap.com/secmon/basis	
Access to Generic Path (Distinct) by Technical User	http://sap.com/secmon/basis	
Access to Generic Path by Dialog User	http://sap.com/secmon/basis	
Access to Generic Path by Technical User	http://sap.com/secmon/basis	
Access to New Application Component by Dialog User	http://sap.com/secmon/basis	

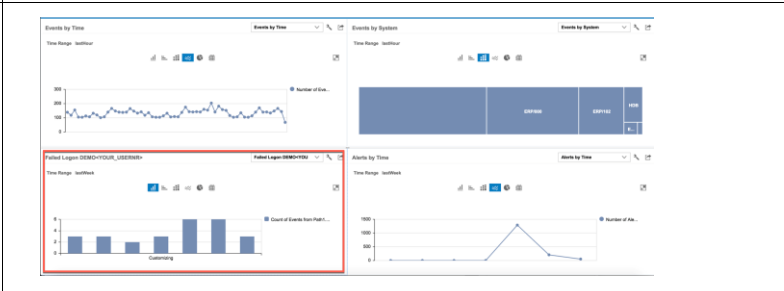
Select Forensic Facet


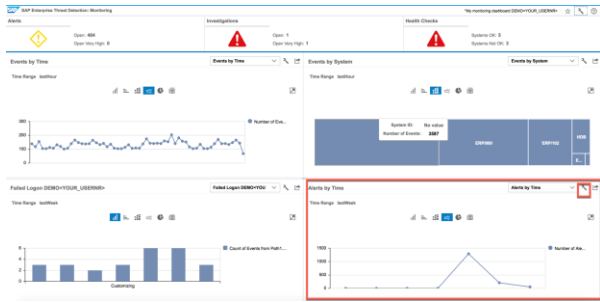
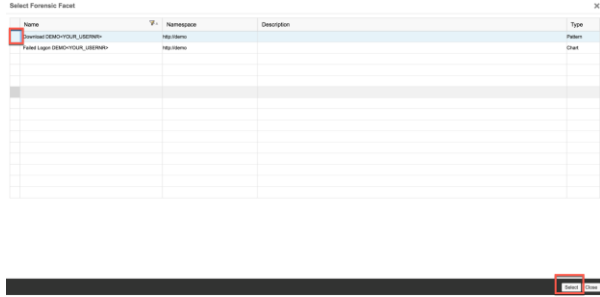
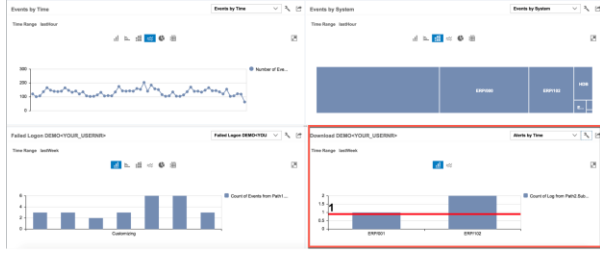

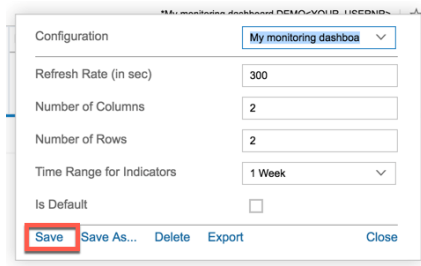
Name	Namespace	Description
Sort Ascending	http://sap.com/secmon	
Sort Descending	http://sap.com/secmon	
Filter DEMO<YOUR_USERN	http://sap.com/secmon/basis	Brute force login u
Columns	http://sap.com/secmon	Checks if the ABAI
	http://sap.com/secmon	
ABAP critical FM calls per SOAP rfc	http://sap.com/secmon/basis	Client calls critical
ABAP deactivated or deleted function modules	http://sap.com/secmon/basis	A user has tried to
ABAP deactivated or deleted reports	http://sap.com/secmon/basis	A user has tried to
ABAP function modules with removed RFC enablement	http://sap.com/secmon/basis	A user has tried to
ABAPLogonFailed	http://sap.com/secmon	
Access to Generic Path (Distinct) by Dialog User	http://sap.com/secmon/basis	
Access to Generic Path (Distinct) by Technical User	http://sap.com/secmon/basis	
Access to Generic Path by Dialog User	http://sap.com/secmon/basis	
Access to Generic Path by Technical User	http://sap.com/secmon/basis	
Access to New Application Component by Dialog User	http://sap.com/secmon/basis	

99. Choose your chart and push button *Select*.



100. Look at left chart below that has been changed and updated



Explanation	Screenshot
101. Push button <i>Settings</i>  to replace the right chart below.	
102. Select your pattern and push button <i>Select</i> .	
103. Look at right chart below that has been changed and updated	
104. Click on the button <i>Setting</i>  and push button <i>Save</i> to save your monitoring dashboard.	

5.1. Summary:

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

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

6. LOG LEARNING – HOW TO LEARN A NEW LOG SOURCE

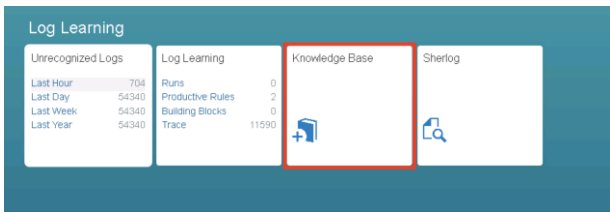
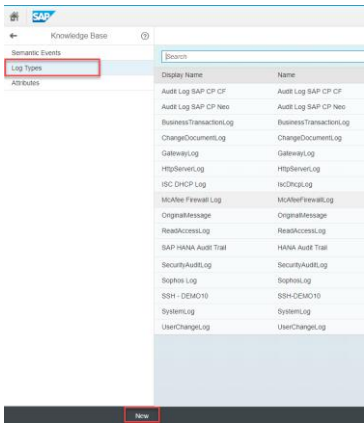
Security Aspect: In the daily life of a Security Expert you have to monitor a lot of systems, devices and networks. It is pretty possible, that at certain point of time some logs written by an application or device cannot be interpreted by current ETD. ETD Log Learning application fills this gap and allows you to parse any text-based logs and normalize such log data into the semantic data model of SAP ETD with its semantic events and attributes. With common semantic model you can correlate newly normalized log with other known logs. In this way, ETD can be extended to monitor potentially any systems which logs are learned by ETD.

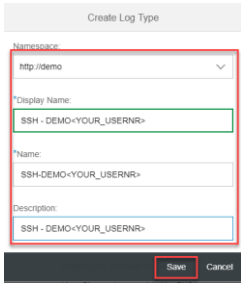
Tool Aspect: The Log Learning application analyzes each entry in the log to find elements like variables and key-value lists. It represents the discovered elements as what are called **annotations**. For example, a timestamp is represented by the annotation. During analysis each log entry is analyzed into a sequence of annotations, which might be interspersed with fixed text. This sequence is called the **markup** for the log entry. Entries with the same markup are grouped together and are considered to be instances of the same **entry type**. The entry type is a technical artefact with an ID. As a user, you work with the markup to specify how to normalize the log entry type to the semantic data model of SAP Enterprise Threat Detection.

In this exercise you are going to learn an SSH log which protocols a successful login.

6.1. Creating a new Log Type in the Knowledge Base

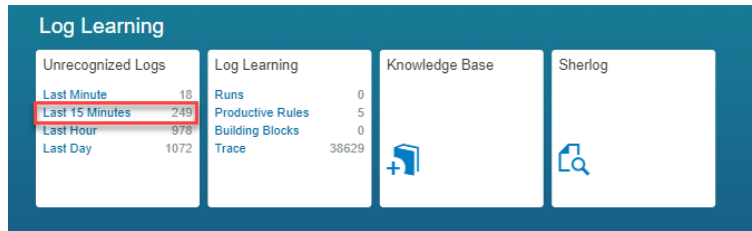
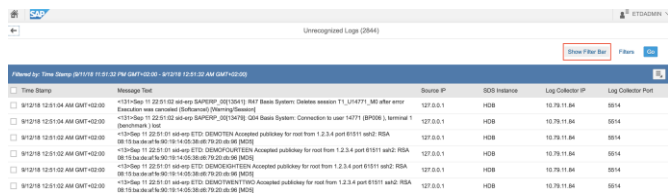
Log types enable you to identify the kind of log that produced a log entry when working with anything other than the standard log types provided by SAP. Create a log type **SSH – DEMO<YOUR_NUMBER>** using the Knowledge Base tile.

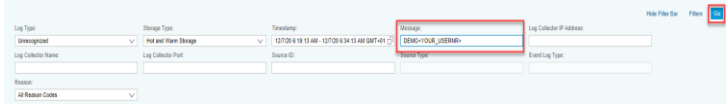
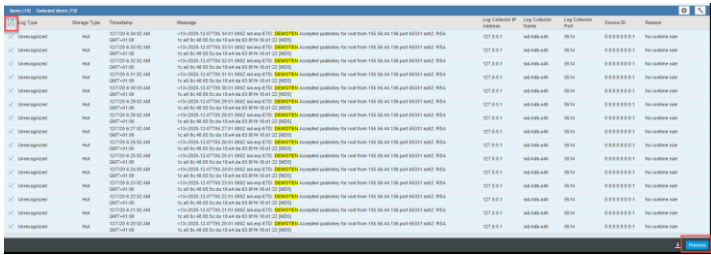
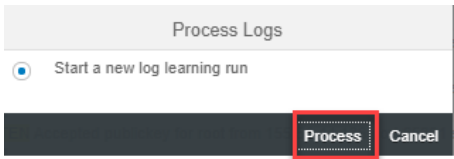
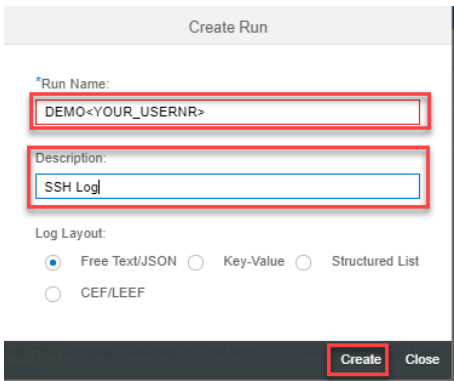
Explanation	Screenshot
105. Open tile Knowledge Base in the SAP Enterprise Threat Detection Launchpad	
106. In the list click on <i>Log Types</i> and choose button <i>New</i>	

Explanation	Screenshot
<p>107. Add the following entries in the pop-up <i>Create Log Type</i> and push button <i>OK</i></p> <p>Namespace: <u><i>http://demo</i></u></p> <p>Name/Display Name/Description: <i>SSH - DEMO<YOUR_USERNR></i></p>	

6.2. Creating a new Log Learning Run from Unrecognized Logs

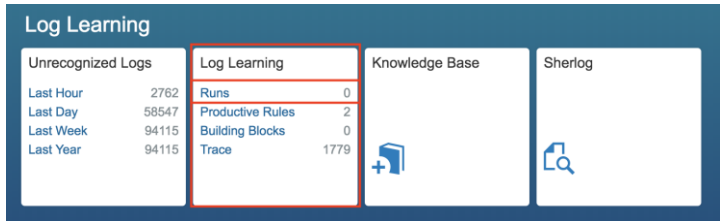

Learning a new log requires loading sample log data into SAP Enterprise Threat Detection. You can use the unrecognized logs as a worklist for learning a new log. In this exercise you will learn how to include sample log data from the unrecognized logs worklist.

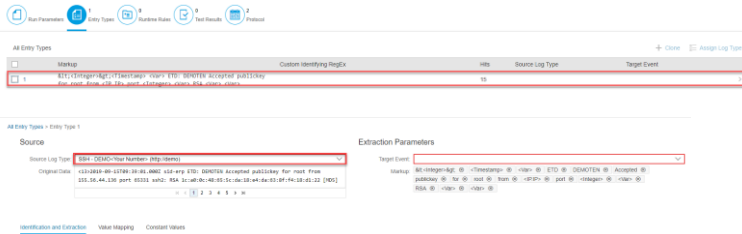
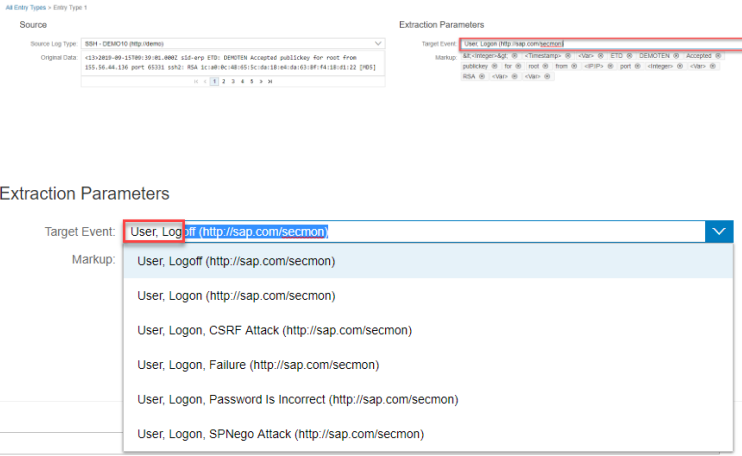
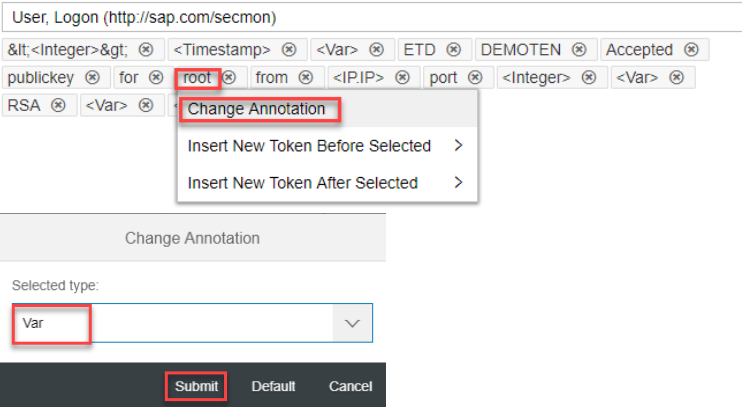
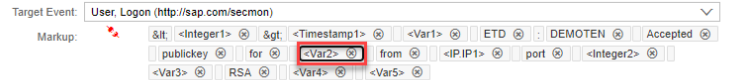
Explanation	Screenshot
108. Open tile Unrecognized Logs – Last 15 Minutes in the SAP Enterprise Threat Detection Launchpad	
109. Click on button <i>Show Filter Bar</i> . Use the filter options to select the log events that you want to include	

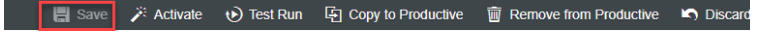
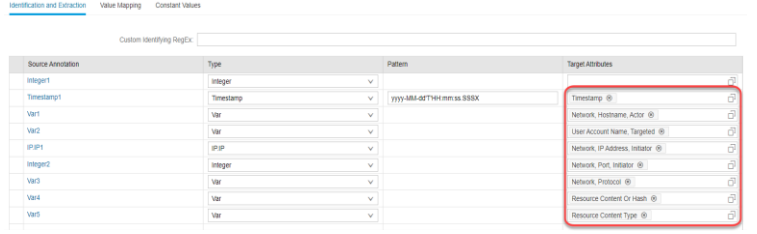

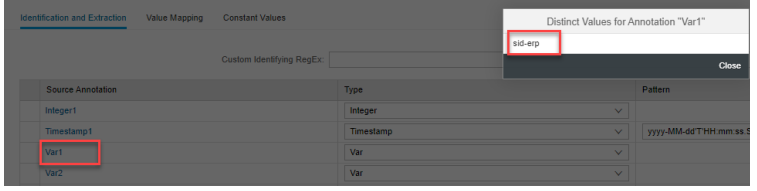
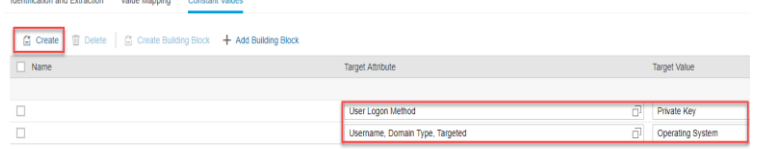
Explanation	Screenshot
<p>110. For filtering the logs that you want to learn, enter a Message search term and push button Go</p> <p>Message Text: DEMO<YOUR_USERNR>, e.g. DEMOTWO</p>	
<p>111. In this exercise the table result contains SSH messages for successful logins. Mark all entries in the table by using the mass selection checkbox and push button Process. In the popup click on the Process Button.</p>	 
<p>112. Add a name and description for your run and push button Create</p> <p>Name: DEMO<YOUR_USERNR></p> <p>Description: SSH Log</p>	

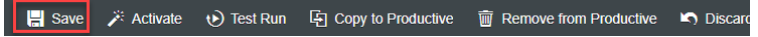
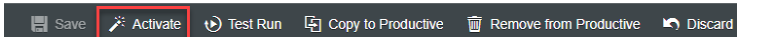
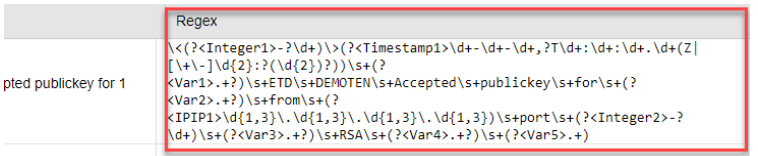
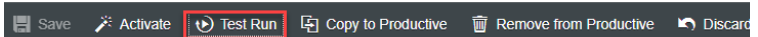
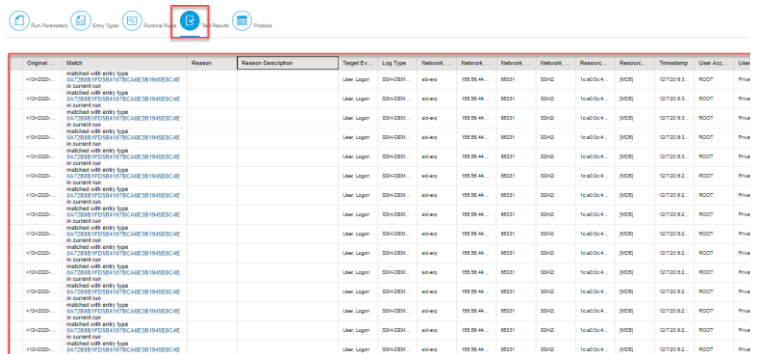
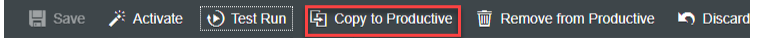
6.3. Interpreting Semantic Events in the Log

In the Log Learning staging area, you teach SAP Enterprise Threat Detection how to parse and normalize sample log data such as log data from the unrecognized logs worklist into individual semantic events and - attributes. In this exercise you will learn how sample log data for SSH log successful login are mapped to the semantic data model of SAP Enterprise Threat Detection. As soon as this log data is learned, analysis can directly start.

Explanation	Screenshot																
<p>113. From the Unrecognized Logs tile, you will be automatically navigated to the Log Learning staging area of the run you have created in step 112.</p> <p>The Log Learning staging area can be as well reached by opening the tile Log Learning– Run. Select the run DEMO<YOUR_USERNR>, you have created in step 112.</p>	 <table><caption>Unrecognized Logs</caption><tr><td>Last Hour</td><td>2762</td></tr><tr><td>Last Day</td><td>58547</td></tr><tr><td>Last Week</td><td>94115</td></tr><tr><td>Last Year</td><td>94115</td></tr></table> <table><caption>Log Learning</caption><tr><td>Runs</td><td>0</td></tr><tr><td>Productive Rules</td><td>2</td></tr><tr><td>Building Blocks</td><td>0</td></tr><tr><td>Trace</td><td>1779</td></tr></table>	Last Hour	2762	Last Day	58547	Last Week	94115	Last Year	94115	Runs	0	Productive Rules	2	Building Blocks	0	Trace	1779
Last Hour	2762																
Last Day	58547																
Last Week	94115																
Last Year	94115																
Runs	0																
Productive Rules	2																
Building Blocks	0																
Trace	1779																
<p>114. Log Learning application analyzes all the sample log data that has been included into the run. It recognizes similar log scheme and summarizes similar sample log data into one markup.</p> <p>By clicking on the markup, the mapping UI opens.</p> <p>So-called annotations are recognized for each markup entry and help you to better understand the components of the log. Annotation are e.g. timestamps, IP-Addresses, variables, key-values, etc. For each markup you can now define how it is interpreted, which components are relevant and how they are mapped to the semantic events and – attributes of SAP Enterprise Threat Detection</p>	 <table><tr><th></th><th>Markup</th><th>Custom Identif...</th><th>Hits</th><th>Source Log Type</th></tr><tr><td>1</td><td>\$!t;+integer+&t;+timestamp+ <var> \$!D: DENOTEN accepted publickey for root from <IP> port <integer> <var> \$!A <var> <var></td><td></td><td>15</td><td></td></tr></table>		Markup	Custom Identif...	Hits	Source Log Type	1	\$!t;+integer+&t;+timestamp+ <var> \$!D: DENOTEN accepted publickey for root from <IP> port <integer> <var> \$!A <var> <var>		15							
	Markup	Custom Identif...	Hits	Source Log Type													
1	\$!t;+integer+&t;+timestamp+ <var> \$!D: DENOTEN accepted publickey for root from <IP> port <integer> <var> \$!A <var> <var>		15														

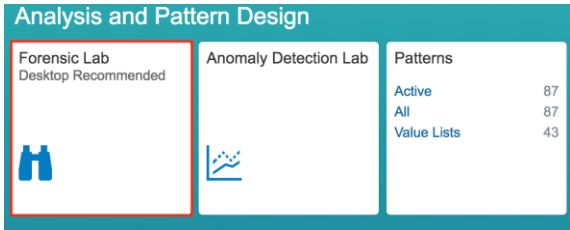

Explanation	Screenshot
<p>115. Click on the line with the fond markup, to go into the details screen. Then Add the Log Type you have created in step 104.</p> <p>Log Type: SSH - DEMO<YOUR_USERNR></p>	
<p>116. Add Event <i>User, Logon</i> as the selected markup is reporting a successful login.</p> <p>Enter the name of the event <i>User, Logon</i> or make use of entering free text help to quickly find the appropriate semantic event. Use e.g. <i>User, Logon</i> as filter for column <i>Name</i>. Select the row.</p>	
<p>117. In the markup click on the word <i>root</i>. By that the annotations can be changed. Change the annotation to type <i>Var</i> and click <i>Submit</i>. By that the Var value can be mapped to a user.</p>	 <p>----- Result -----</p> 

Explanation	Screenshot
<p>118. Save your changes by pushing button Save</p>	
<p>119. Map the relevant annotations to the appropriate semantic attributes of the semantic event <i>User, Logon</i></p> <p>Row 2 - Timestamp: <i>Timestamp</i></p> <p>Row 3 – Var1: <i>Network, Hostname, Actor Username, Domain Name, Targeted</i> (i.e. mark the two)</p> <p>Row 4 – Var2: <i>User Account Name, Targeted</i></p> <p>Row 5 – IP.IP: <i>Network, IP Address, Initiator</i></p> <p>Row 6 – Integer: <i>Network, Port, Initiator</i></p> <p>Row 7 – Var3: <i>Network, Protocol</i></p> <p>Row 8 – Var4: <i>Resource Content Or Hash</i></p> <p>Row 9 – Var5: <i>Resource Content Type</i></p> <p>Hint 1: By clicking on the <i>Copy</i> sign for each target Attribute</p> <p>Hint 2: By clicking on the different Annotations in the list, you can find out if the assumed values are in, which helps mapping the correct attributes</p>	 <p>----- Click on <i>Copy-Sign</i> -----</p>  <p>----- Click on Source Annotation and see related values -----</p> 
<p>120. Select tab <i>Constant Values</i> and push button Create twice</p> <p>Add the following constant values:</p> <p><i>User Logon Method:</i> <i>Private Key</i></p> <p><i>Username, Domain Type, Targeted:</i> <i>Operating System</i></p>	

Explanation	Screenshot
121. Push button Save	
122. Push button Activate . The result about the created RegEx is shown	 
123. Push button Test Run to check result of your log learning Hint: In case errors occur during Regular Expression Interpretation, the columns <i>Reason</i> and <i>Reason Description</i> provide corresponding information	 
124. Now you are done. Push button Copy to Productive .	

6.4. Verifying the new Log Type in the Forensic Lab

As soon as your log learning run has been set to productive, logs are normalized and mapped to the semantic events and – attributes the way have defined. These logs can then be analyzed using e.g. the Forensic Lab tile.

Explanation	Screenshot
125. Open tile Forensic Lab	
126. In the Forensic Lab you find the events you have learned. Use the forensic lab to check the details of your newly learned log type <i>SSH - DEMO<YOUR_USERNR></i>	

6.5. Summary:

Security Aspect: As a Security Expert you have extended your monitoring boundary to include a new log - SSH log - into the system. Based on the data in the SSH log you can monitor the activities of ssh access in your system landscape. Patterns can be built to trigger alerts if disallowed ssh login happens.

Tool Aspect: You learned how to use the Log Learning application to parse a Unrecognized Log, assign this log to a new Log Type, associate the log to a Semantic Event and link Annotation to Semantic Attributes. You can now create a Run, and follow the workflow of activation, testing and productive deployment to finish the Log Learning process. The verification is done in Forensic Lab.

www.sap.com/contactsap

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

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

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

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

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platforms, directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

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

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