

Security Monitoring & SIEM Fundamentals:

Link to challenge: <https://academy.hackthebox.com/module/211/>

(log in required)

Class: Tier II | Easy | Defensive

SIEM & SOC Fundamentals

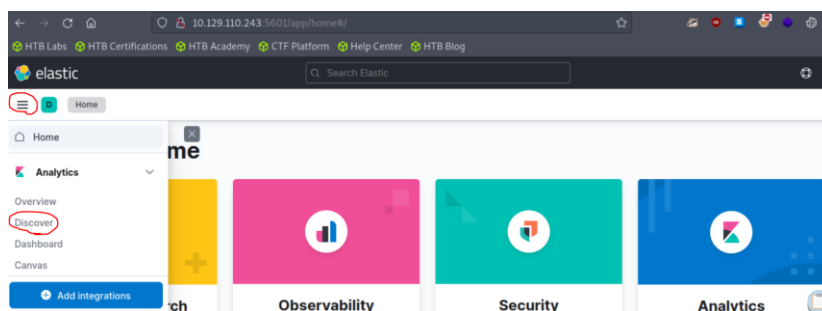
Introduction To The Elastic Stack:

Question: Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Discover". Then, click on the calendar icon, specify "last 15 years", and click on "Apply". Finally, choose the "windows*" index pattern. Now, execute the KQL query that is mentioned in the "Comparison Operators" part of this section and enter the username of the disabled account as your answer. Just the username; no need to account for the domain.

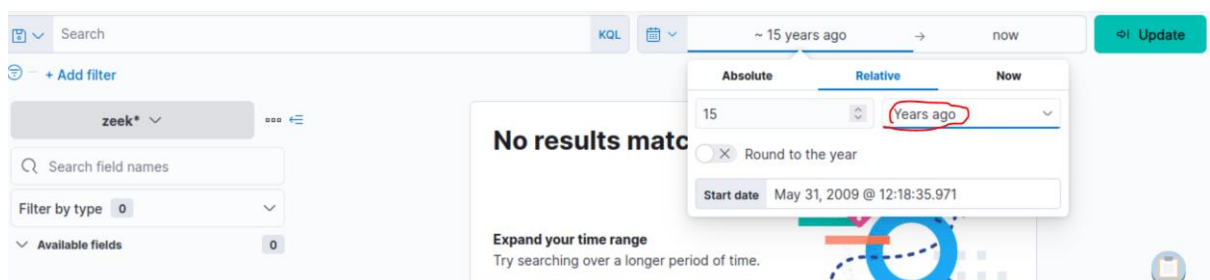
Answer: anni

Method:

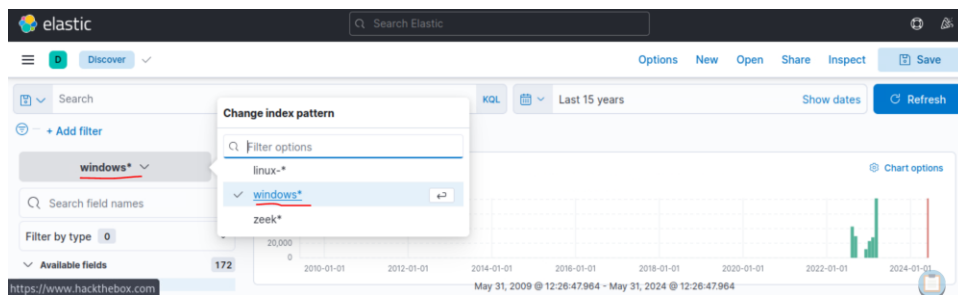
First when we open the tool – we click on the side navigation button, then on discover:



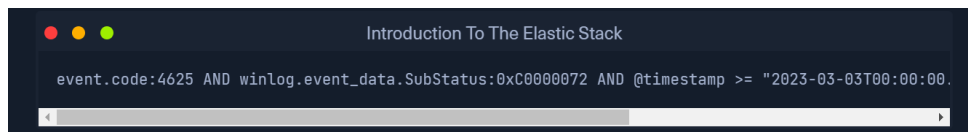
Then we change the filter calendar to specify 'last 15 years':



Then – we choose “Winodws* index pattern search:



Now that we have that, we need to take the query from the section:



```
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072
AND @timestamp >= "2023-03-03T00:00:00.000Z" AND @timestamp
<= "2023-03-06T23:59:59.999Z"
```

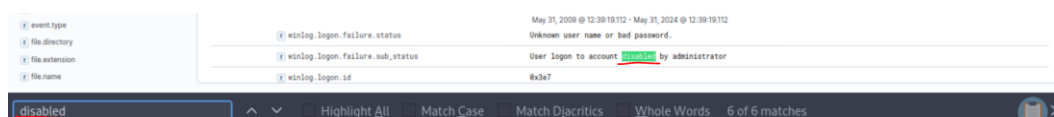
and paste it on the KQL (Kibana Query Language) field:



We get 1 search result, lets investigate it, we search for user.name:



To confirm the result, we gonna search for the word ‘disabled’ in the page with ctrl+f:



That indeed confirms the user ‘anni’ was disabled from the system.

Question: Now, execute the KQL query that is mentioned in the "Wildcards and Regular Expressions" part of this section and enter the number of returned results (hits) as your answer.

Answer: 2

Method:

First – we take the wildcard and regular expression from the page section:

- **Wildcards and Regular Expressions:** KQL supports **wildcards and regular expressions** to search for patterns in field values. For example:



Introduction To The Elastic Stack

```
event.code:4625 AND user.name: admin*
```

```
event.code:4625 AND user.name: admin*
```

upon pasting it on the search field on the web-page, we get 8 hits:



SIEM Visualization Development

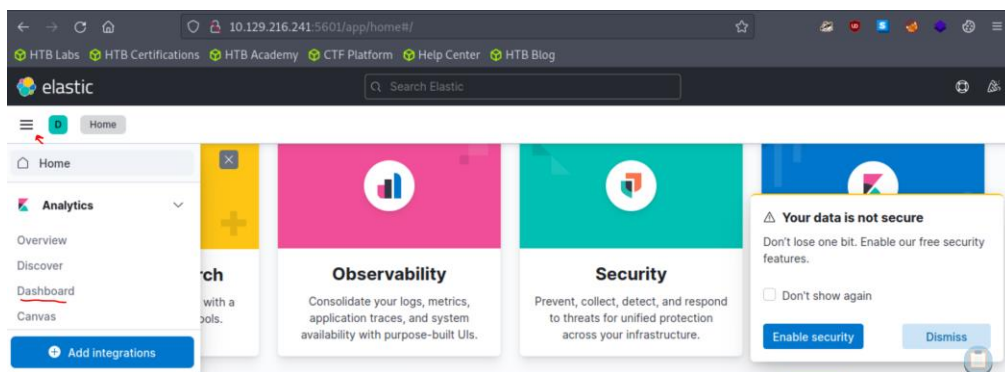
SIEM Visualization Example 1: Failed Logon Attempts (All Users):

Question: Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard". Browse the refined visualization we created or the "Failed logon attempts [All users]" visualization, if it is available, and enter the number of logins for the `sql-svc1` account as your answer.

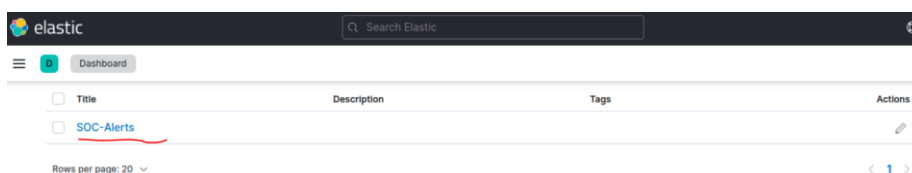
Answer: 2

Method:

First – we enter the side navigation bar, and then enter dashboard:



Then enter SOC-Alerts:



Then for 'sql-svc1' user, the number of logins is 2.

A screenshot of the Elastic SIEM SOC-Alerts page showing a table of failed logon attempts. The table has columns: Username, Event logged by, Logon type, and # of logins. The row for 'sql-svc1' is highlighted with a red arrow and a red circle around the value '2' in the '# of logins' column. The table is titled 'Failed logon attempts [All users]'.

Username	Event logged by	Logon type	# of logins
PAW	DC2	Network	4
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PKI	Network	2
Administrator	DC1	Unlock	1

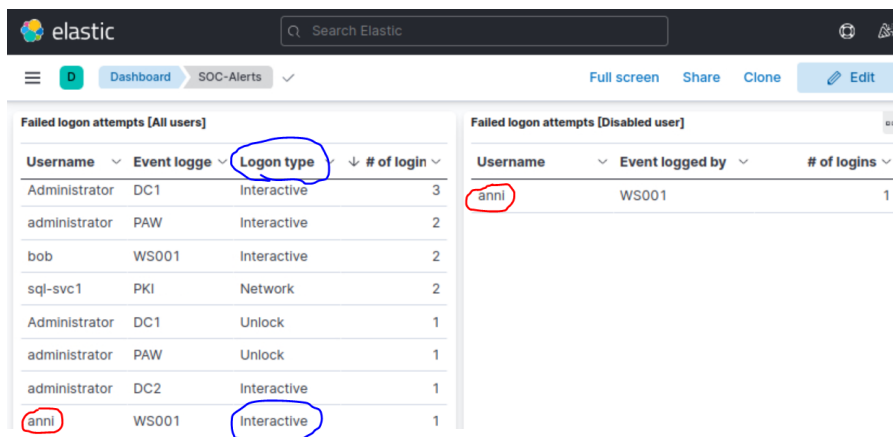
SIEM Visualization Example 2: Failed Logon Attempts (Disabled Users):

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Either create a new visualization or edit the "Failed logon attempts [Disabled user]" visualization, if it is available, so that it includes failed logon attempt data related to disabled users including the logon type. What is the logon type in the returned document?

Answer: Interactive

Method:

Method 1: Observe for 'Anni' in the disables users list, and search for her name in the overall list that includes the login type:

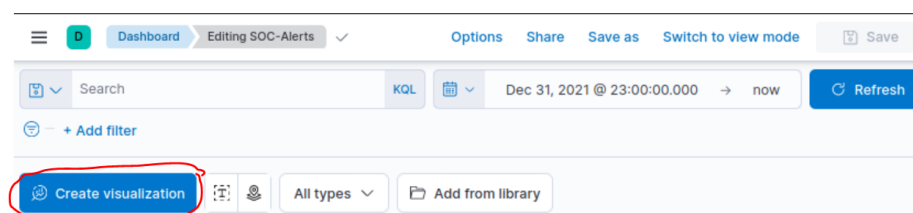


Username	Event logge	Logon type	# of login
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PKI	Network	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1
anni	WS001	Interactive	1

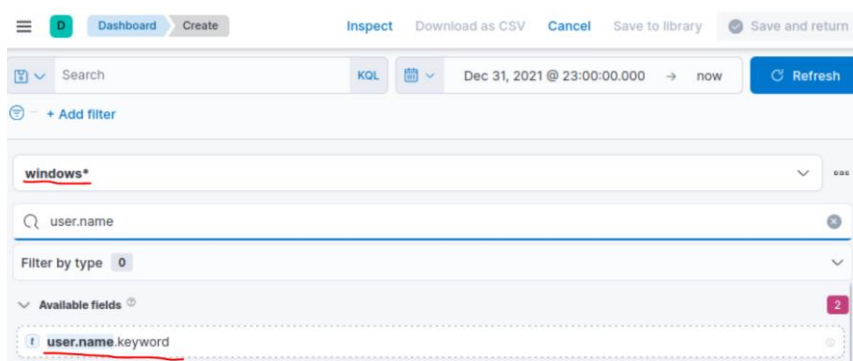
Username	Event logged by	# of logins
anni	WS001	1

Method 2:

We create virtualization:



We set the machine target for 'Windows*'



And we add the fields: 'user.name.keyword' for username and 'winlog.Logon_type.keyword' for logon type.

and we add filter of 'winlog.event_data.SubStatus', operator 'is' and value '0xC0000072' (for disabled), that will display only disabled users.



Then we save the virtualization:

Top values of use ▾	Top values of win ▾	# of logins ▾
anni	Interactive	1

Clean result, display the disabled user, and Logon type.

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Either create a new visualization or edit the "Failed logon attempts [Admin users only]" visualization, if it is available, so that it includes failed logon attempt data where the username field contains the keyword "admin" anywhere within it. What should you specify after user.name: in the KQL query?

Answer: *admin*

Method: basic wildcard use

SIEM Visualization Example 3: Successful RDP Logon Related To Service Accounts:

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Browse the visualization we created or the "RDP logon for service account" visualization, if it is available, and enter the IP of the machine that initiated the successful RDP logon using service account credentials as your answer.

Answer: 192.168.28.130

Method:



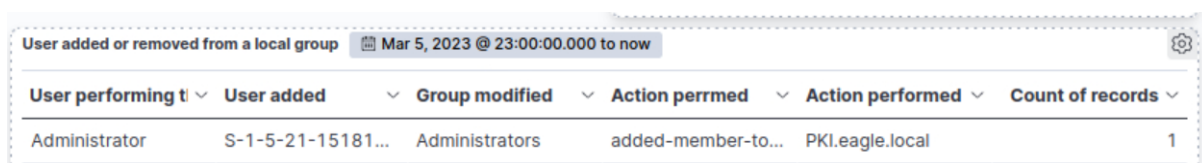
Username	Connect from	# of logins
svc-sql1	PKI 192.168.28.130	2

SIEM Visualization Example 4: Users Added Or Removed From A Local Group (Within A Specific Timeframe):

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Extend the visualization we created or the "User added or removed from a local group" visualization, if it is available, and enter the common date on which all returned events took place as your answer. Answer format: 20XX-0X-0X

Answer: 2023-03-05

Method:



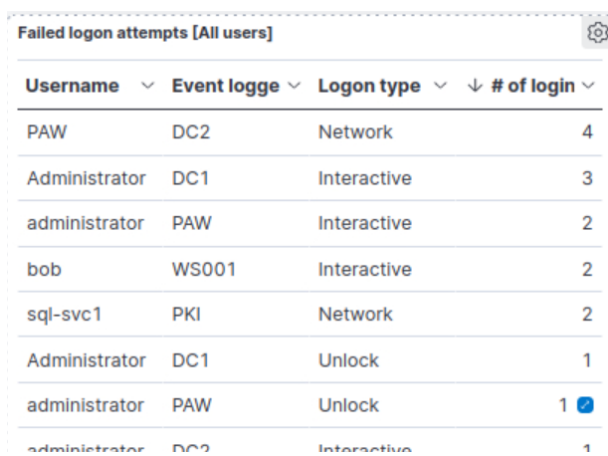
User performing	User added	Group modified	Action permed	Action performed	Count of records
Administrator	S-1-5-21-15181...	Administrators	added-member-to...	PKI.eagle.local	1

Skills Assessment

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [All users]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Consult with IT Operations

Method:



The screenshot shows a dashboard titled "Failed logon attempts [All users]" with a settings icon. Below the title is a table with the following columns: Username, Event logge, Logon type, and # of login. The table contains the following data rows:

Username	Event logge	Logon type	# of login
PAW	DC2	Network	4
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
bob	WS001	Interactive	2
sql-svc1	PKI	Network	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1

3-4 login attempts to machines are seem enough to raise an eyebrow, especially when there is administrator user involved.

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Disabled user]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Escalate to a Tier 2/3 analyst

Method: disabled user should not be able to login(?)

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "Failed logon attempts [Admin users only]" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Nothing suspicious

Method: only the 'PAW' machines are worthy on consideration here, as DC1 and 2 machines are not used in this scenario.

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "RDP logon for service account" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Escalate to a Tier 2/3 analyst

Method: as all hosts are in the cloud, how the hell local IP is attempting to login to PKI (public key infrastructure) machine

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "User added or removed from a local group" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Consult with IT Operations

Method: what is this username??

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "Admin logon not from PAW" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Consult with IT Operations

Method: admin connected not from PAW 51 times..

Question: Navigate to [http://\[Target IP\]:5601](http://[Target IP]:5601), click on the side navigation toggle, and click on "Dashboard". Review the "SSH Logins" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier 2/3 analyst"

Answer: Escalate to a Tier 2/3 analyst

Method: someone tried to login to root account, not knowing it was deactivated, clearly breach attempt.