Labs - Security Monitoring & SIEM Fundamentals

Skills Assessment

Dashboard Review & Critical Thinking Exercise

Context

You have been hired in Eagle as a SOC Tier 1 analyst. Yesterday was your on-boarding day with the company, and today you will be familiarized with the SOC. Your day will begin by meeting up with a senior analyst, who will provide insights into the environment, and afterwards, you are expected to begin monitoring alerts and security events in our home-cooked SOC dashboards.

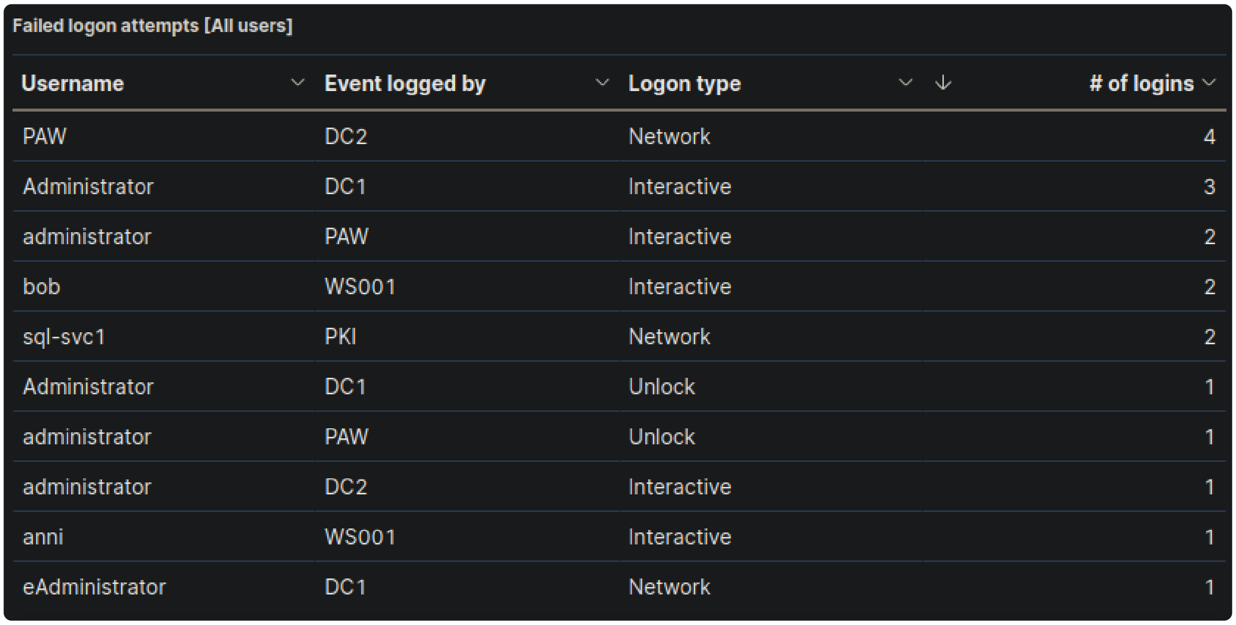
The following are your notes after meeting the senior analyst, who provided insights into the environment:

- The organization has moved all hosting to the cloud; the old DMZ network is closed down, so no more servers exist there.
- The IT operation team (the core IT admins) consists of four people. They are the only ones with high privileges in the environment.
- The IT operation team often tends to use the default administrator account(s) even if they are told otherwise.
- All endpoint devices are hardened according to CIS hardening baselines. Whitelisting exists to a limited extent.
- IT security has created a privileged admin workstation (PAW) and requires that all admin activities be performed on this machine.
- The Linux environment is primarily 'left over' servers from back in the day, which have very little, if any, activity on a regular day. The root user account is not used; due to audit findings, the account was blocked from connecting remotely, and users who require those rights will need to escalate via the sudo command.
- Naming conventions exist and are strictly followed; for example, service accounts contain '-svc' as part of their name. Service accounts are created with long, complex passwords, and they perform a very specific task (most likely running services locally on machines).
- Now you are free to take your seat and start monitoring. Navigate to `http://[Target IP]:5601`, click on the side navigation toggle, and click on "Dashboard". Review the `SOC-Alerts` dashboard.

  - `Visualization 1: Failed logon attempts (All users)` Such a visualization might reveal potential brute force attacks. It's important to identify any single user with numerous failed attempts or perhaps, various users connecting to (or from) the same endpoint device. However, the current data does not point towards any such scenario. One anomaly is noticeable though. **Hint**: It is related to the "sql-svc1" account.
  - `Visualization 2: Failed logon attempts (Disabled user)` It seems that there is one incident where the user "Anni" has tried to authenticate, despite the account being disabled.
  - `Visualization 3: Failed logon attempts (Admin users only)` **Hint**: Check if all events took place on either Privileged Access Workstations (PAWs) or Domain Controllers.
  - `Visualization 4: RDP logon for service account` Service accounts in this environment serve a very specialized function. Do you notice anything that warrants suspicion?
  - `Visualization 5: User added or removed from a local group` An administrator has incorporated an individual (who is only represented by the SID value) into the "Administrators" group. Should you escalate to a Tier 2/3 analyst or consult with the IT Operations department first?
  - `Visualization 6: Admin logon not from PAW` Administrators should exclusively utilize PAWs for server remote connections. Should you escalate to a Tier 2/3 analyst or consult with the IT Operations department first?
  - `Visualization 7: SSH Logins` Be reminded that the root user account is not typically in use.

Questions

- Navigate to 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"

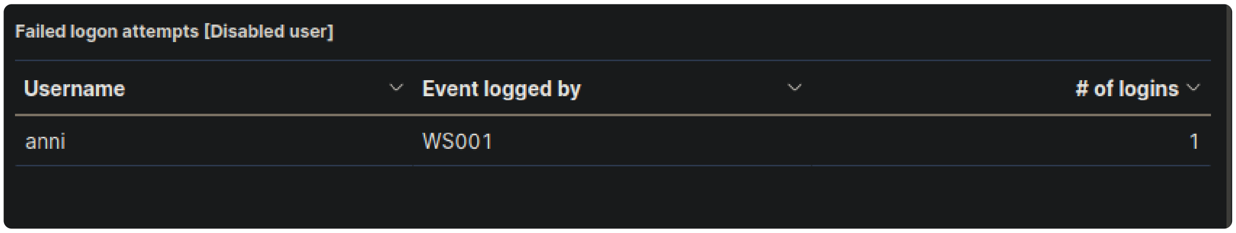


Failed logon attempts [All users]

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
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1
anni	WS001	Interactive	1
eAdministrator	DC1	Network	1

-> We see that the service account `sql-svc1` has been attempted to logon through network, which is very suspicious.
-> Some possibility include password spraying attack on an active directory domain (twice to avoid being lock out).
-> However we're not fully sure about it and we will consult the IT operations team for more detail. Service account attempting to access remote file shares or printers is something odd.

- Navigate to 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"

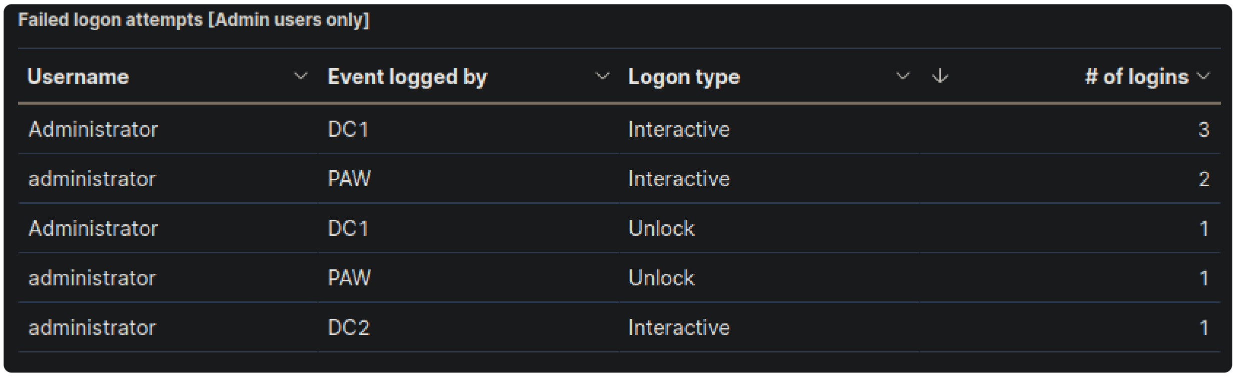


Failed logon attempts [Disabled user]

Username	Event logged by	# of logins
anni	WS001	1

-> We see that the disabled user, anni has attempted to login.
-> This indicates that the attacker has somehow gained figured out the credential of the anni, as normal user generally would not login to using an disabled account and the failed logon attempts could be an typo.
-> Or in the extreme case, it could just be that an normal user doing some extremely random things, but it is more likley that this is an breach and should be escalated to escalate to Tier 2/3 analyst"

- Navigate to 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"

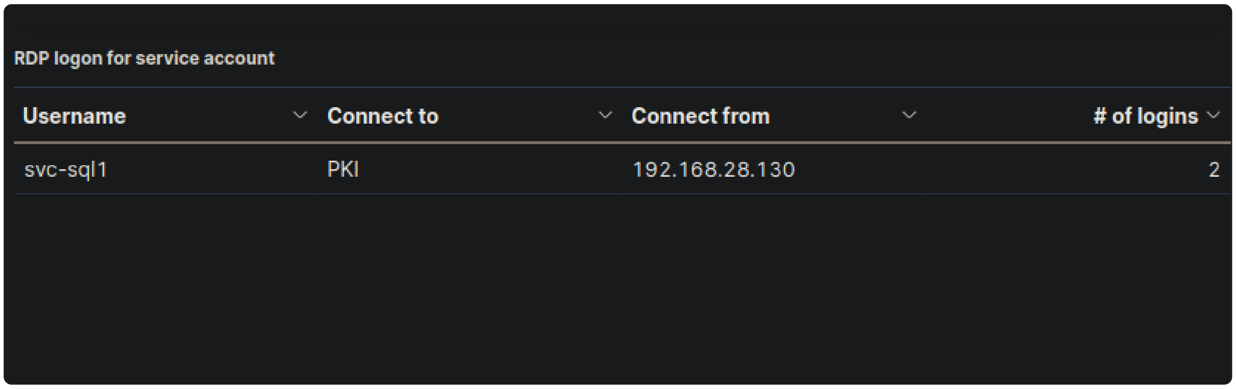


Failed logon attempts [Admin users only]

Username	Event logged by	Logon type	# of logins
Administrator	DC1	Interactive	3
administrator	PAW	Interactive	2
Administrator	DC1	Unlock	1
administrator	PAW	Unlock	1
administrator	DC2	Interactive	1

-> We don't see anything suspicious, as logins are usual and the IT team usually use the default administrator account.

- Navigate to 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"

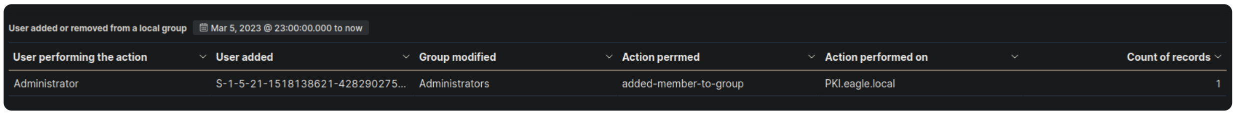


RDP logon for service account

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

-> This is a huge one, we see service account doing rdp logon which it never should do, this is a 1000% confirmed breach and needs to be escalated to Tier2/3 analyst.

- Navigate to 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"



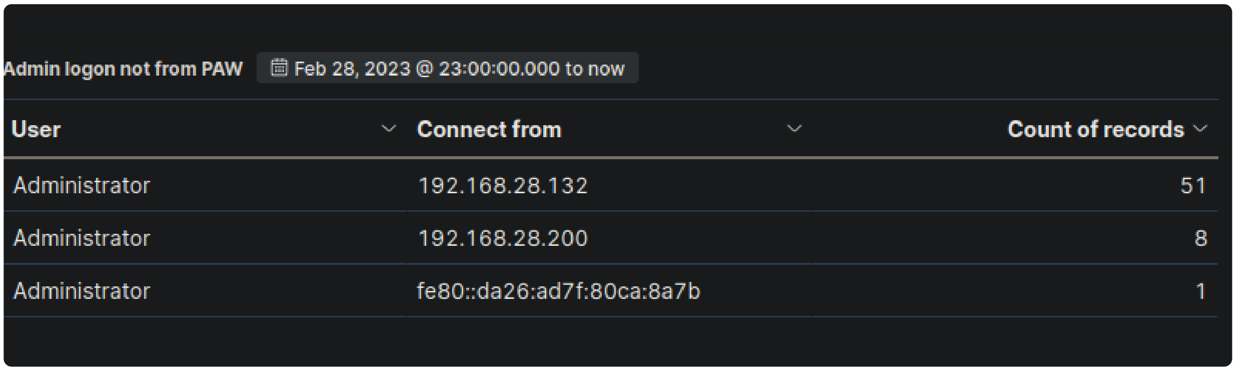
User added or removed from a local group Mar 5, 2023 @ 23:00:00.000 to now

User performing the action	User added	Group modified	Action perrmed	Action performed on	Count of records
Administrator	S-1-5-21-1518138621-428290275...	Administrators	added-member-to-group	PKI.eagle.local	1

-> Here we see an administrator user being added to the group done on the machine PKI.eagle.local.
-> We can see from the context that all admin activities are done in the PAW are required all admin activities to be performed there.
-> We also know that IT operations team tend to use just the default administrator group.
-> Hence, some probability includes the ADCS server got compromised through some ad attack (e.g. acl attacks) and the domain may be compromised. We will esclate to a Tier 2/3 analyst.
-> However before we do so, it would be a ideal to consult the IT team to see if they

performed such activities. If they didn't, then its likely a domain compromise where the attacker achieved persistence that needs to be fixed ASAP.

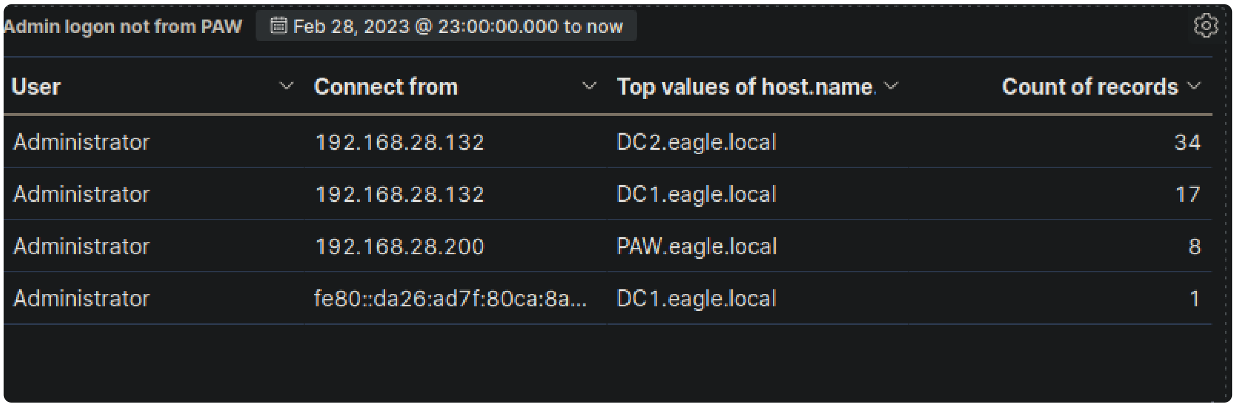
- Navigate to http://[Target IP]:5601, click on the side navigation toggle, and click on "Dashboard". Review the "Admin logon not from PAW" visualization of the "SOC-Alerts" dashboard. Choose one of the following as your answer: "Nothing suspicious", "Consult with IT Operations", "Escalate to a Tier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



Admin logon not from PAW Feb 28, 2023 @ 23:00:00.000 to now

User	Connect from	Count of records
Administrator	192.168.28.132	51
Administrator	192.168.28.200	8
Administrator	fe80::da26:ad7f:80ca:8a7b	1

-> We know that all admin activities needs to be performed from PAW, so this is indeed a very weird behaviour.
-> Examining the results in a more detailed manner (through editing the visualisation), we see that

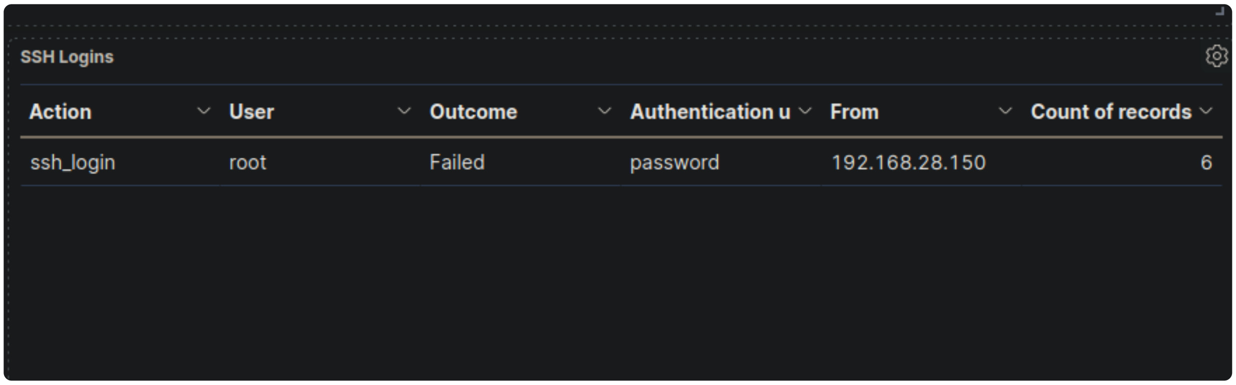


Admin logon not from PAW Feb 28, 2023 @ 23:00:00.000 to now

User	Connect from	Top values of host.name	Count of records
Administrator	192.168.28.132	DC2.eagle.local	34
Administrator	192.168.28.132	DC1.eagle.local	17
Administrator	192.168.28.200	PAW.eagle.local	8
Administrator	fe80::da26:ad7f:80ca:8a...	DC1.eagle.local	1

-> It is the domain controller that is being accessed, which indicates domain compromise.
-> However, it would be wise to consult the IT operations team first to gain additional context before doing so, as there still could be some reasonable probability that they logged in and did work.

- Navigate to 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.



SSH Logins

Action	User	Outcome	Authentication u	From	Count of records
ssh_login	root	Failed	password	192.168.28.150	6

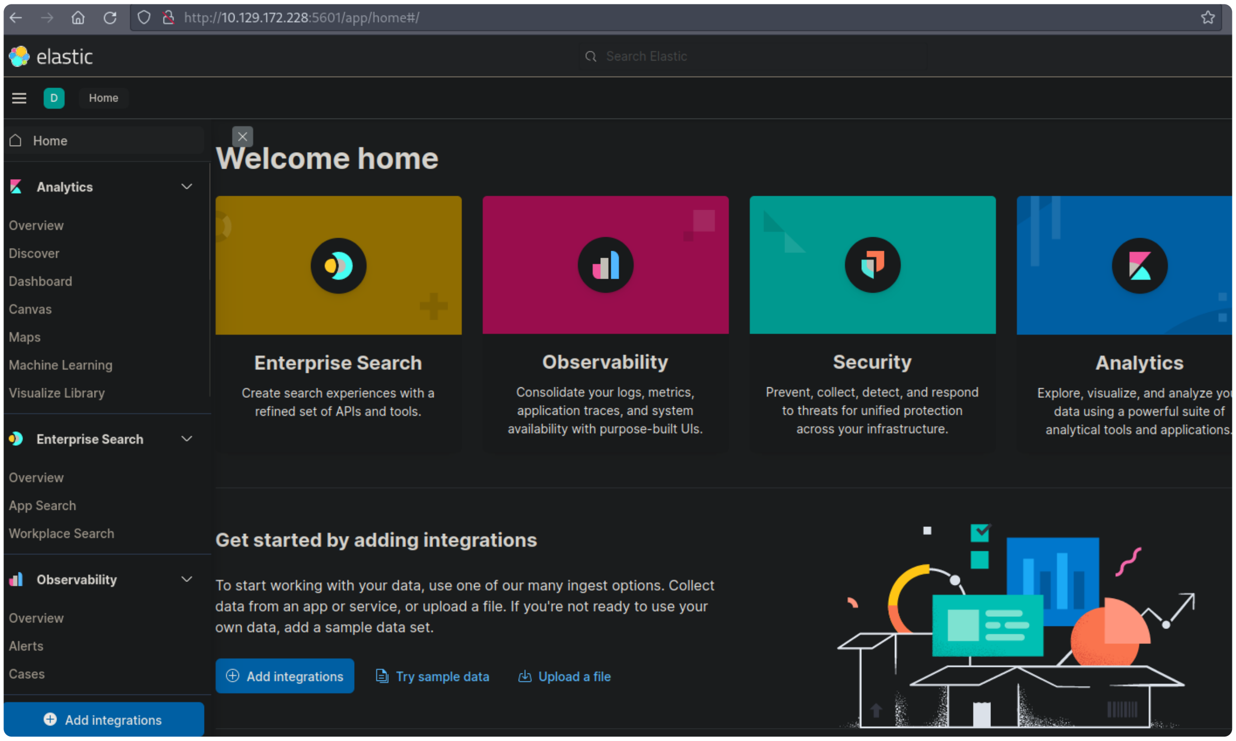
-> We know that the root account has never been used for the Linux environment and is an left-over server.
-> We see that there is an log on attempt of 6, so this is very irregular and most likely some form of password attacks and should be escalated further.
-> Attackers may try to utilize this host to pillage information for lateral movement or set it as an pivot point.
-> As this is an internal environment (not the web external environment), it is likely that attackers have landed a foothold in AD and are seeking to dive deeper to the network.

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.
  -> We go to the web page as follows:



Welcome home

Enterprise Search

Create search experiences with a refined set of APIs and tools.

Observability

Consolidate your logs, metrics, application traces, and system availability with purpose-built UIs.

Security

Prevent, collect, detect, and respond to threats for unified protection across your infrastructure.

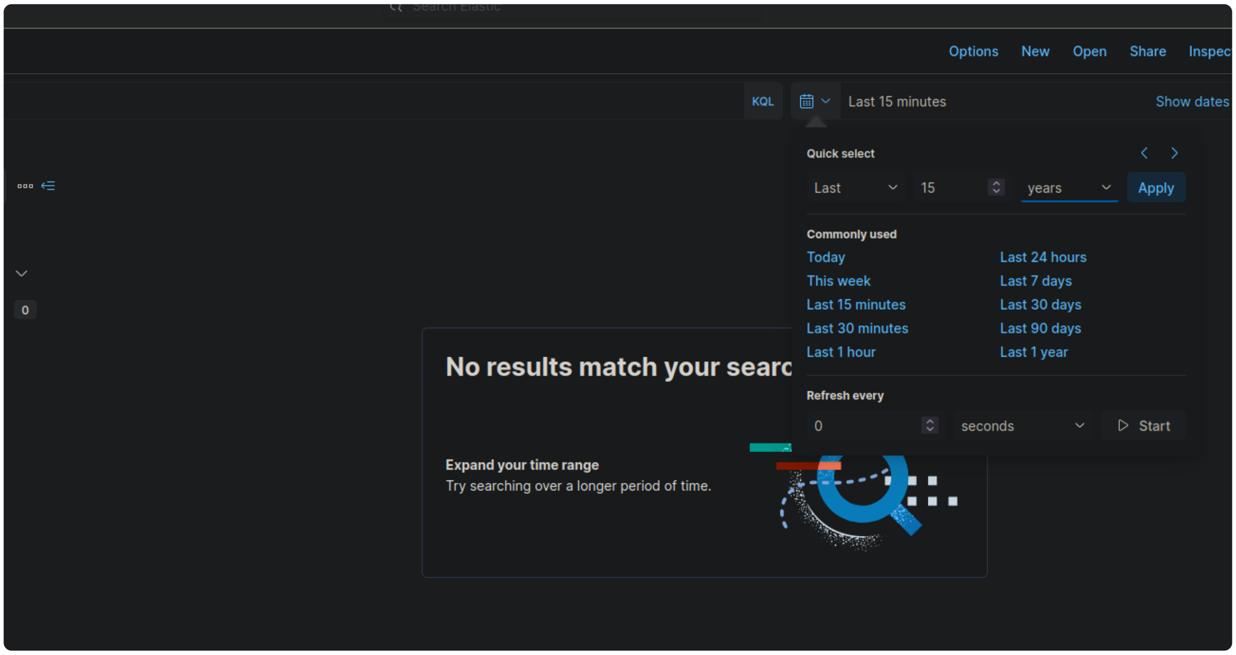
Analytics

Explore, visualize, and analyze yo data using a powerful suite of analytical tools and applications.

Get started by adding integrations

To start working with your data, use one of our many ingest options. Collect data from an app or service, or upload a file. If you're not ready to use your own data, add a sample data set.

-> We specify last 15 years:



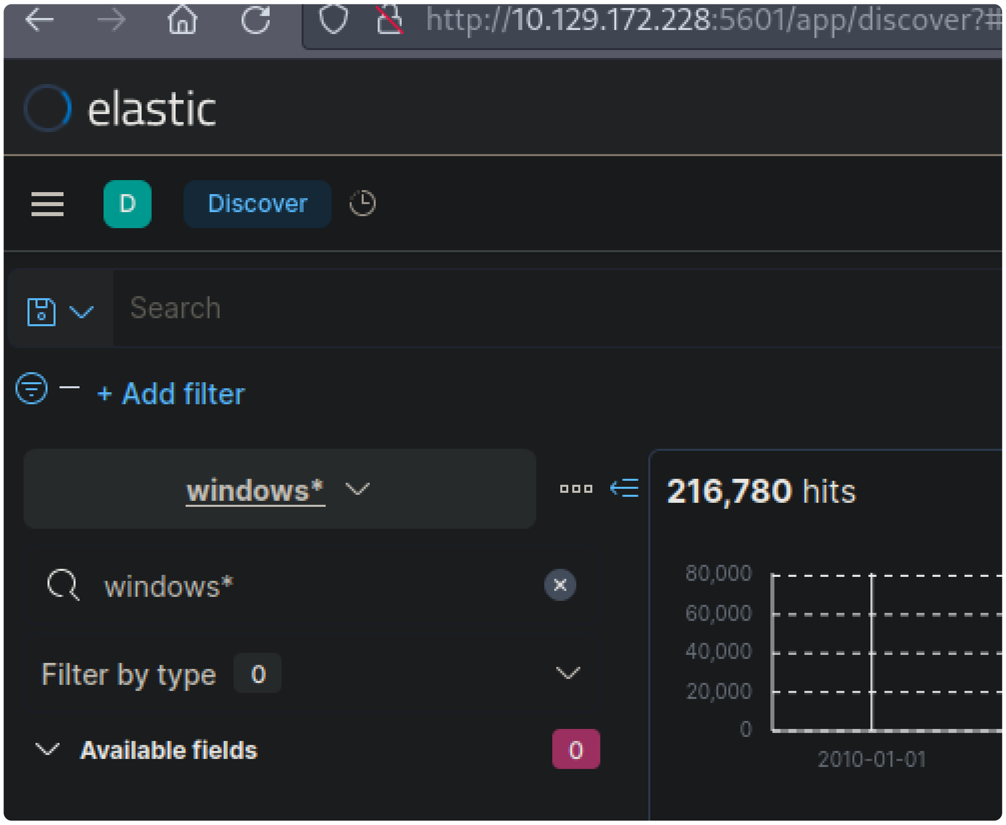
Last 15 years

Refresh every 0 seconds

No results match your searc

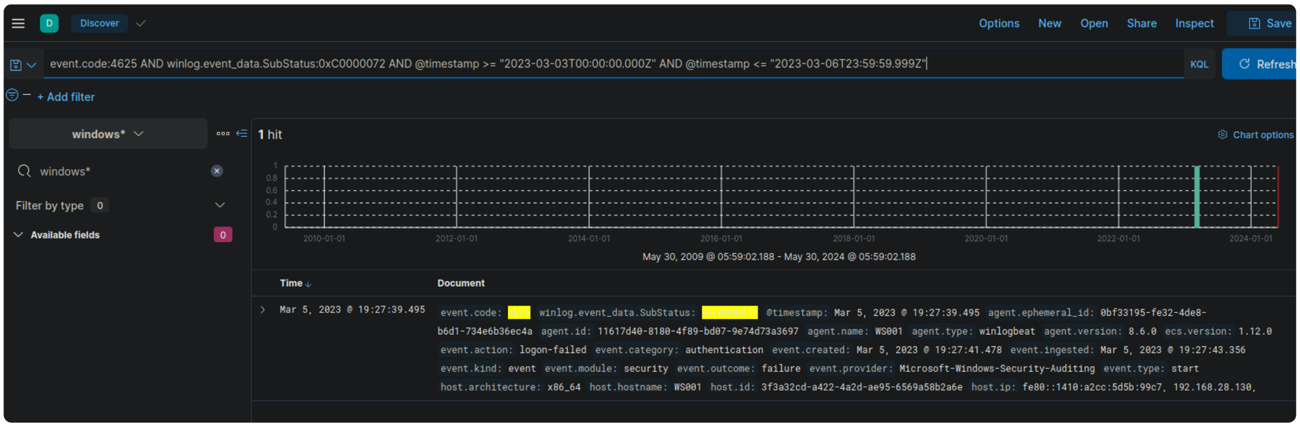
Expand your time range
Try searching over a longer period of time.

-> We choose the windows index pattern



-> Now we execute the KQL query that is mentioned in the "Comparison Operators" part of 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"
```

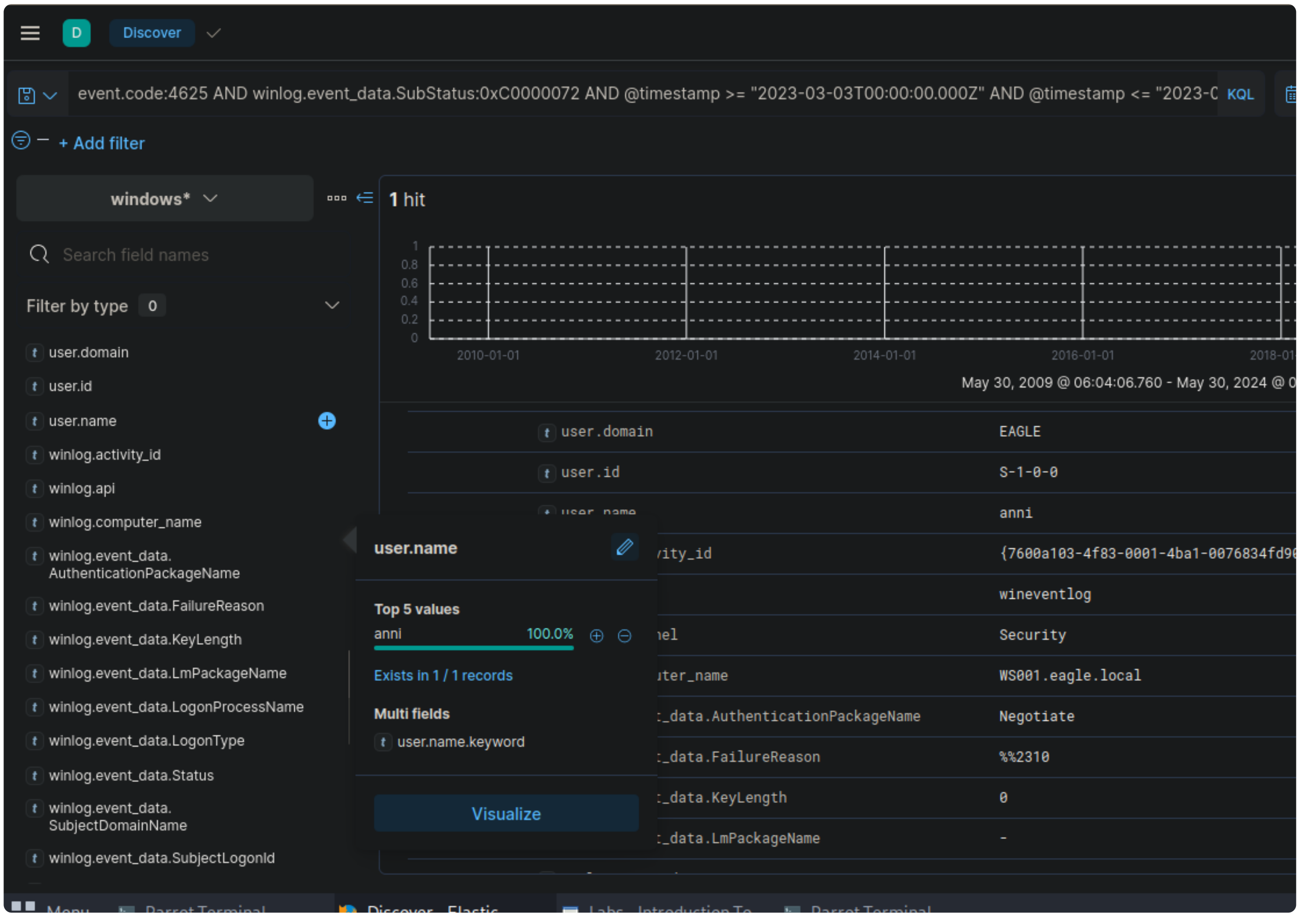


```
event.code:4625 AND winlog.event_data.SubStatus:0xC0000072 AND @timestamp >= "2023-03-03T00:00:00.000Z" AND @timestamp <= "2023-03-06T23:59:59.999Z"
```

1 hit

May 30, 2009 @ 05:59:02.188 - May 30, 2024 @ 05:59:02.188

```
Time ↓                     Document
Mar 5, 2023 @ 19:27:39.495 event.code: 4625 winlog.event_data.SubStatus: 0xc0000072 @timestamp: Mar 5, 2023 @ 19:27:39.495 agent.ephemeral_id: 0bf33195-fe32-4de8-
b6d1-734e6b36ec4a agent.id: 11617d40-8180-4f89-bd07-9e74d73a3697 agent.name: WS001 agent.type: winlogbeat agent.version: 8.6.0 ecs.version: 1.12.0
event.action: logon-failed event.category: authentication event.created: Mar 5, 2023 @ 19:27:41.478 event.ingested: Mar 5, 2023 @ 19:27:43.356
event.kind: event event.module: security event.outcome: failure event.provider: Microsoft-Windows-Security-Auditing event.type: start
host.architecture: x86_64 host.hostname: WS001 host.id: 3f3a32cd-a422-4a2d-ae95-6569a58b2a6e host.ip: fe80::1410:a2cc:5d5b:99c7, 192.168.28.130,
```



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

1 hit

May 30, 2009 @ 06:04:06.760 - May 30, 2024 @ 0

- user.domain
- user.id
- user.name
- winlog.activity_id
- winlog.api
- winlog.computer_name
- winlog.event_data.AuthenticationPackageName
- winlog.event_data.FailureReason
- winlog.event_data.KeyLength
- winlog.event_data.LmPackageName
- winlog.event_data.LogonProcessName
- winlog.event_data.LogonType
- winlog.event_data.Status
- winlog.event_data.SubjectDomainName
- winlog.event_data.SubjectLogonId

user.name

Top 5 values

anni 100.0%

Exists in 1 / 1 records

Multi fields

user.name.keyword

Visualize

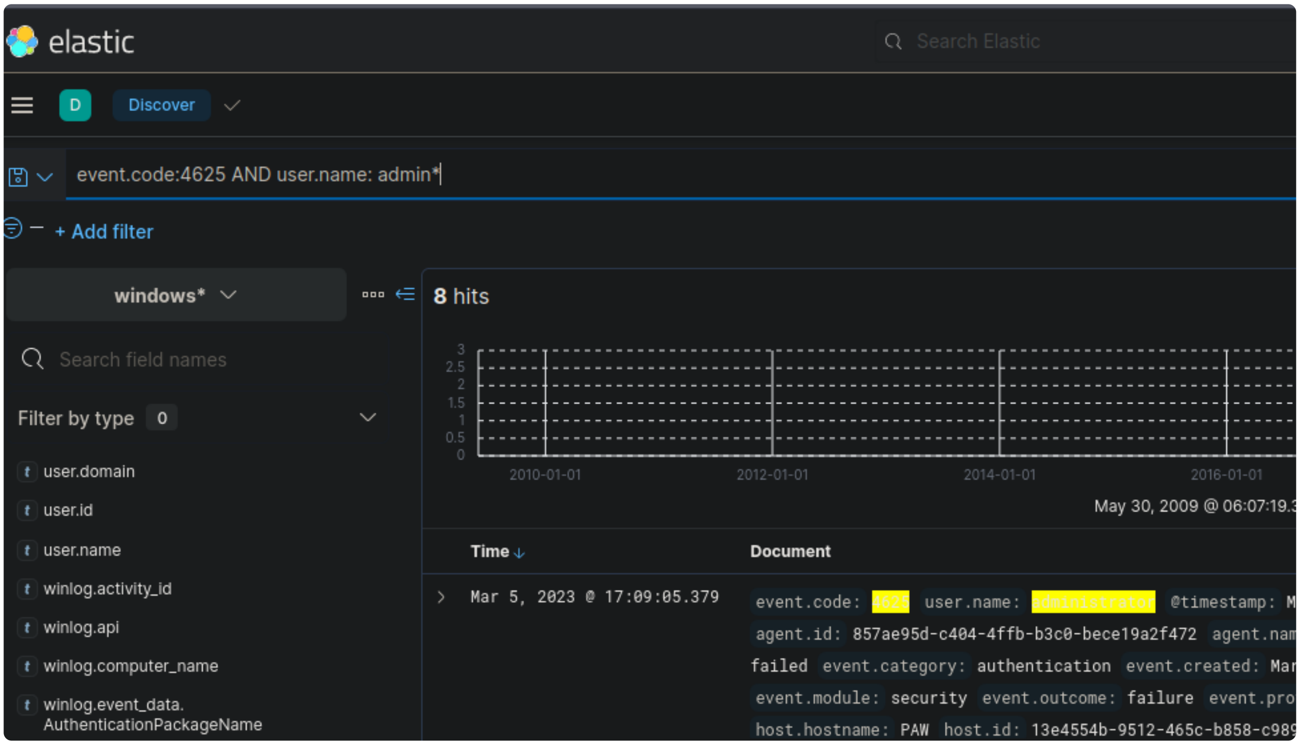
```
user.domain                              EAGLE
user.id                                  S-1-0-0
user.name                                anni
ity_id                                   {7600a103-4f83-0001-4ba1-0076834fd9
                                         wineventlog
el                                       Security
ter_name                                 WS001.eagle.local
_data.AuthenticationPackageName          Negotiate
_data.FailureReason                      %%2310
_data.KeyLength                          0
_data.LmPackageName                      -
```

-> Expanding the result through the available fields or expanding the document, we see the username is anni.

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.
  -> We execute the query as follows:

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



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

user.domain
user.id
user.name
winlog.activity_id
winlog.api
winlog.computer_name
winlog.event_data.AuthenticationPackageName

8 hits

Time ↓	Document
Mar 5, 2023 @ 17:09:05.379	event.code: 4625 user.name: administrator @timestamp: M agent.id: 857ae95d-c404-4ffb-b3c0-bece19a2f472 agent.nam failed event.category: authentication event.created: Mar event.module: security event.outcome: failure event.pro host.hostname: PAW host.id: 13e4554b-9512-465c-b858-c989

-> We see we have 8 hits.

SOC Definition & Fundamentals

Question

- True or false? SOC 2.0 follows a proactive defense approach.
  -> True, we can see shifting for SOC 2.0, emphasis is placed on complete situational awareness, pre-event preparedness through vulnerability management, configuration management, and dynamic risk management, as well as post-event analysis and learning through incident response and in-depth forensics

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

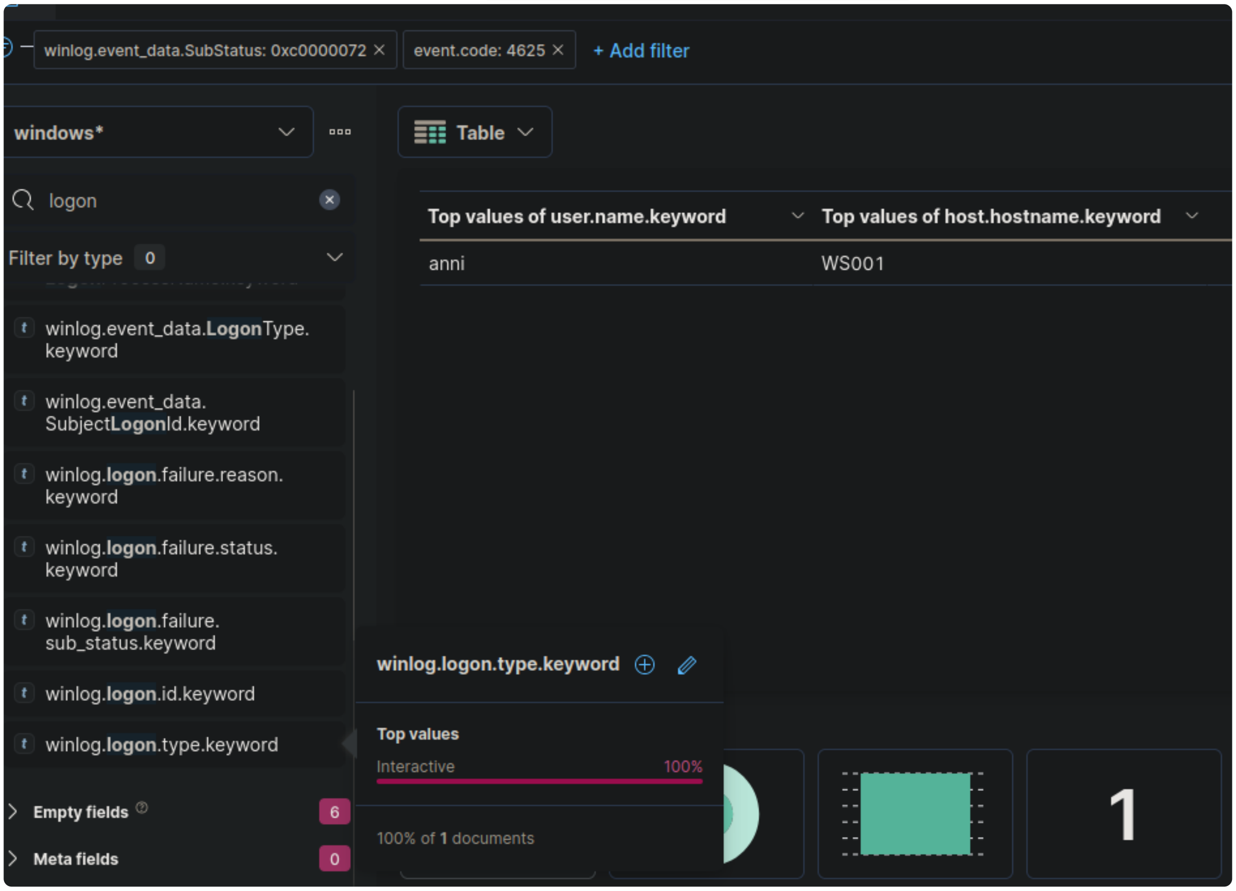
Question

- 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.
  -> The process is an direct follow through of the section in `SIEM Visualization Example 1: Failed Logon Attempts (All Users)`, where we obtain 2 as the answer.

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

Question

- Navigate to 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?
  -> We directly follow from the section in the notes, then we filter for the logon type, in which we obtain 'interactive' from `winlog.logon.type.keyword`



winlog.event_data.SubStatus: 0xc0000072 ✕ event.code: 4625 ✕

Top values of user.name.keyword	Top values of host.hostname.keyword
anni	WS001

winlog.logon.type.keyword

Top values

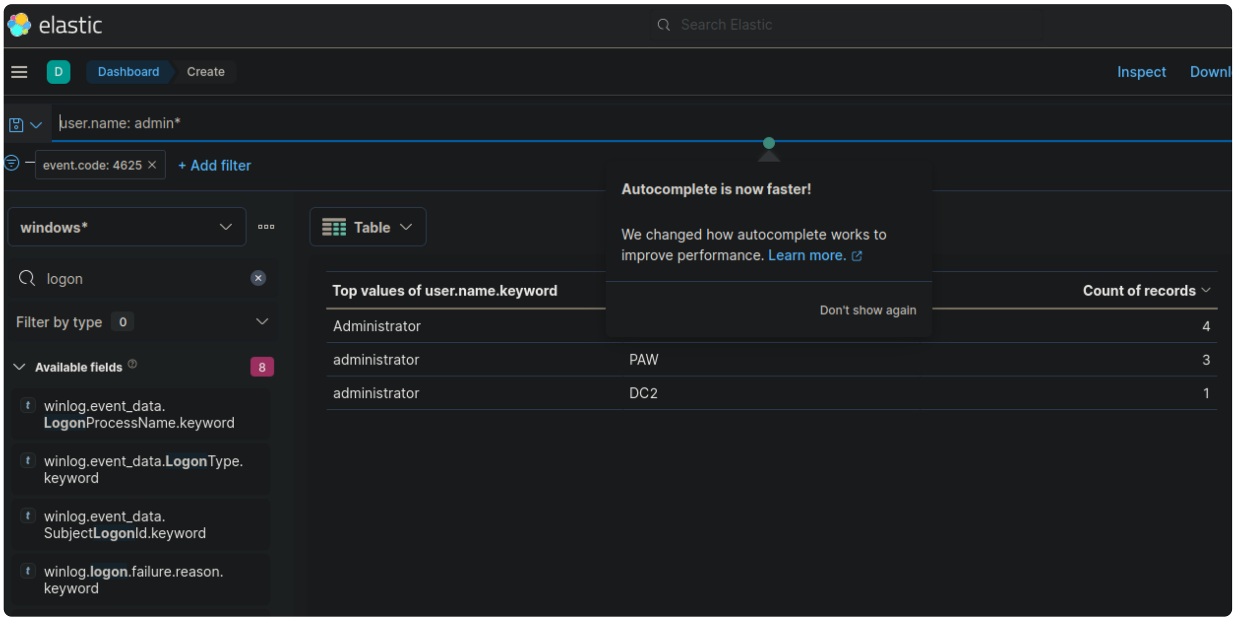
Interactive 100%

100% of 1 documents

+ Add filter
windows*
Table
logon
Filter by type 0
winlog.event_data.LogonType.keyword
winlog.event_data.SubjectLogonId.keyword
winlog.logon.failure.reason.keyword
winlog.logon.failure.status.keyword
winlog.logon.failure.sub_status.keyword
winlog.logon.id.keyword
winlog.logon.type.keyword
Empty fields 6
Meta fields 0
1

- Navigate to 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?
  -> We continue with what we left off in the previous question and delete the substatus

value of `0xC0000072` and query for the user admin in the KQL query as follows:



user.name: admin*

event.code: 4625

Autocomplete is now faster!

We changed how autocomplete works to improve performance. Learn more.

winlog.event_data.LogonProcessName.keyword

winlog.event_data.LogonType.keyword

winlog.event_data.SubjectLogonId.keyword

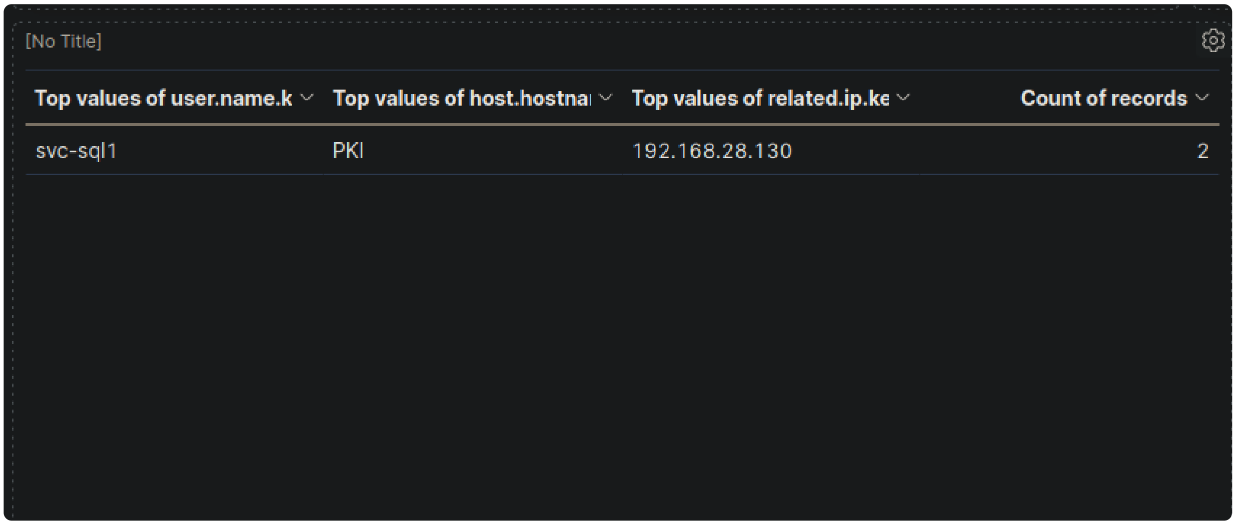
winlog.logon.failure.reason.keyword

Top values of user.name.keyword		Count of records
Administrator		4
administrator	PAW	3
administrator	DC2	1

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

Question

- Navigate to 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.
  -> We follow the steps exactly as given in the section and we get 192.168.28.130



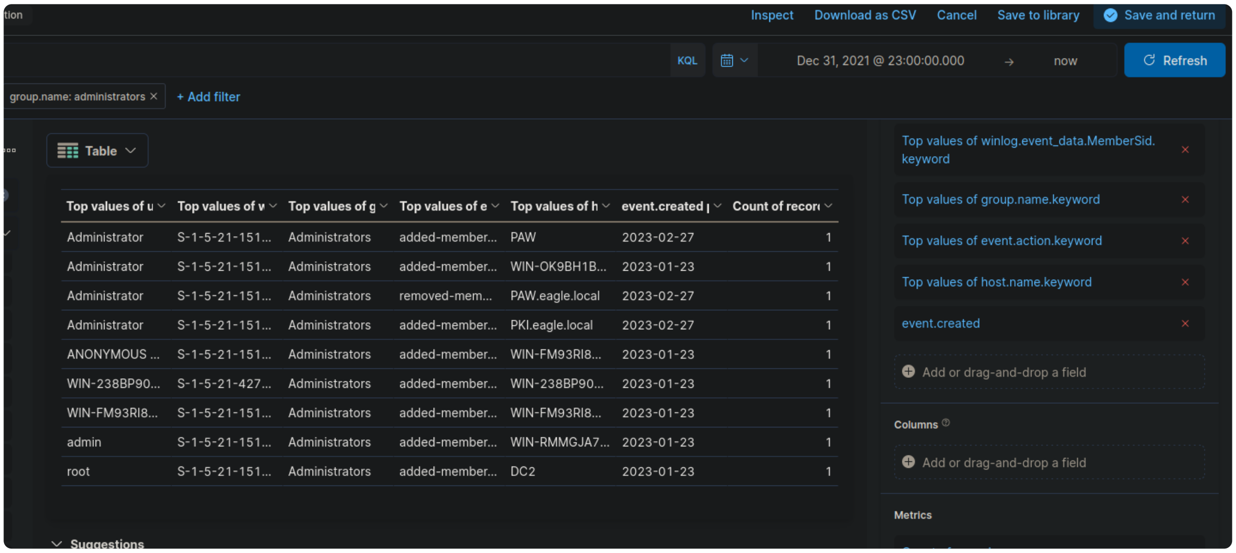
[No Title]

Top values of user.name.k	Top values of host.hostnai	Top values of related.ip.ke	Count of records
svc-sql1	PKI	192.168.28.130	2

-> 192.168.28.130

Question

- Navigate to 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
  -> We extend upon the visualisation we created through adding when the event was created.

  Top values of winlog.event_data.MemberSid.keyword
  Top values of group.name.keyword
  Top values of event.action.keyword
  Top values of host.name.keyword
  event.created

Top values of u	Top values of w	Top values of g	Top values of e	Top values of h	event.created p	Count of record
Administrator	S-1-5-21-151...	Administrators	added-member...	PAW	2023-02-27	1
Administrator	S-1-5-21-151...	Administrators	added-member...	WIN-OK9BH1B...	2023-01-23	1
Administrator	S-1-5-21-151...	Administrators	removed-mem...	PAW.eagle.local	2023-02-27	1
Administrator	S-1-5-21-151...	Administrators	added-member...	PKI.eagle.local	2023-02-27	1
ANONYMOUS ...	S-1-5-21-151...	Administrators	added-member...	WIN-FM93RI8...	2023-01-23	1
WIN-238BP90...	S-1-5-21-427...	Administrators	added-member...	WIN-238BP90...	2023-01-23	1
WIN-FM93RI8...	S-1-5-21-151...	Administrators	added-member...	WIN-FM93RI8...	2023-01-23	1
admin	S-1-5-21-151...	Administrators	added-member...	WIN-RMMGJA7...	2023-01-23	1
root	S-1-5-21-151...	Administrators	added-member...	DC2	2023-01-23	1

  -> Through which after filtering we get 2023-03-05 after creating the visualisation.