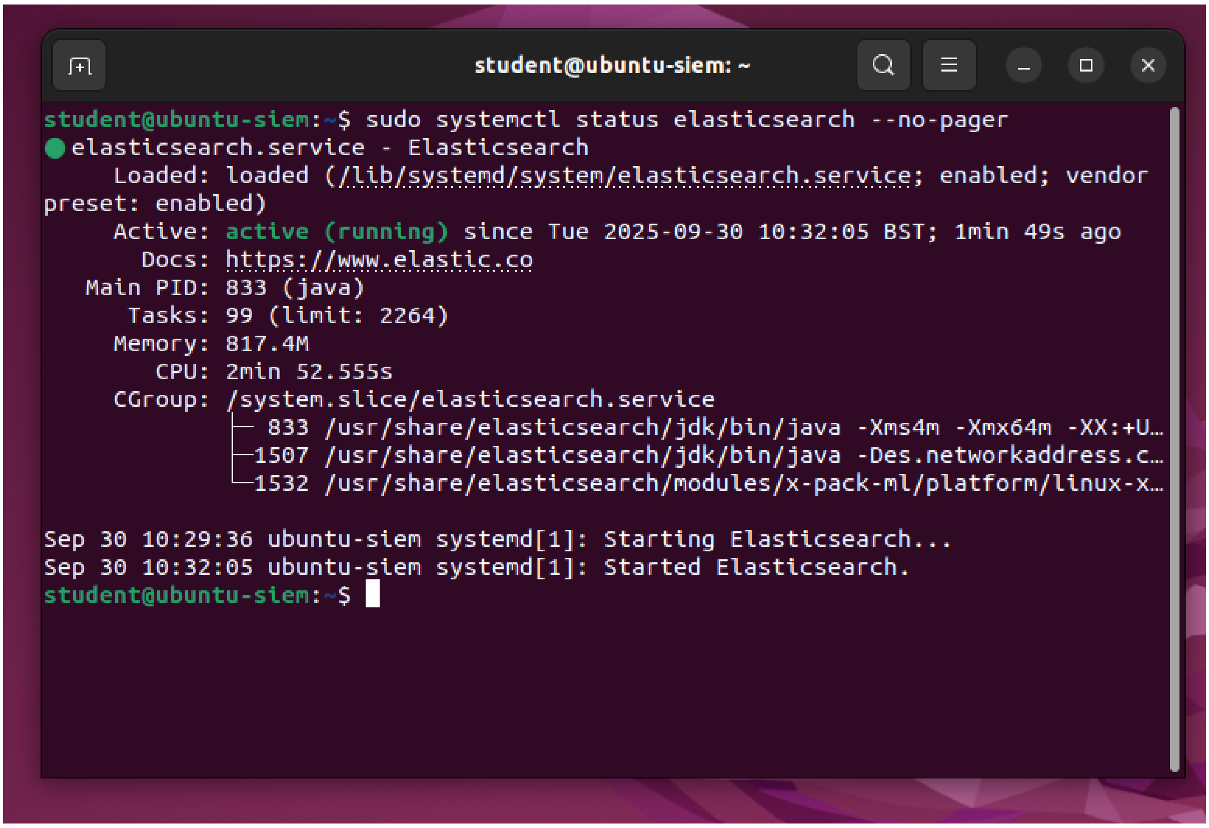
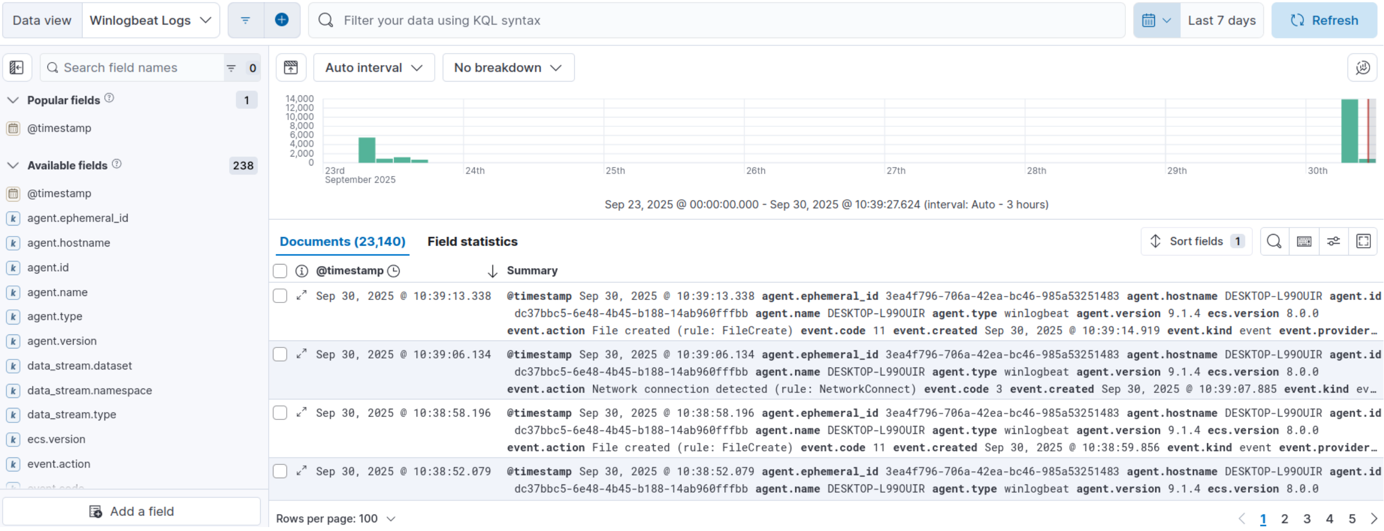
Windows SIEM Project screenshots



```
student@ubuntu-siem:~$ sudo systemctl status elasticsearch --no-pager
● elasticsearch.service - Elasticsearch
     Loaded: loaded (/lib/systemd/system/elasticsearch.service; enabled; vendor
preset: enabled)
     Active: active (running) since Tue 2025-09-30 10:32:05 BST; 1min 49s ago
       Docs: https://www.elastic.co
   Main PID: 833 (java)
      Tasks: 99 (limit: 2264)
     Memory: 817.4M
        CPU: 2min 52.555s
     CGroup: /system.slice/elasticsearch.service
             ├─ 833 /usr/share/elasticsearch/jdk/bin/java -Xms4m -Xmx64m -XX:+U…
             ├─1507 /usr/share/elasticsearch/jdk/bin/java -Des.networkaddress.c…
             └─1532 /usr/share/elasticsearch/modules/x-pack-ml/platform/linux-x…

Sep 30 10:29:36 ubuntu-siem systemd[1]: Starting Elasticsearch...
Sep 30 10:32:05 ubuntu-siem systemd[1]: Started Elasticsearch.
student@ubuntu-siem:~$ 
```

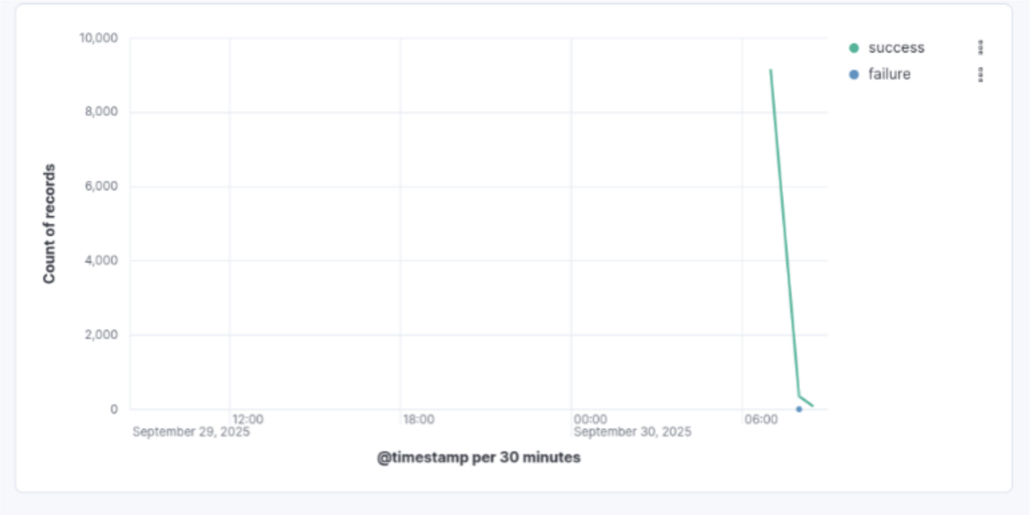
- The **status command** shows Elasticsearch as `active (running)`.
- The **ss command** shows Elasticsearch is listening on port **9200**.

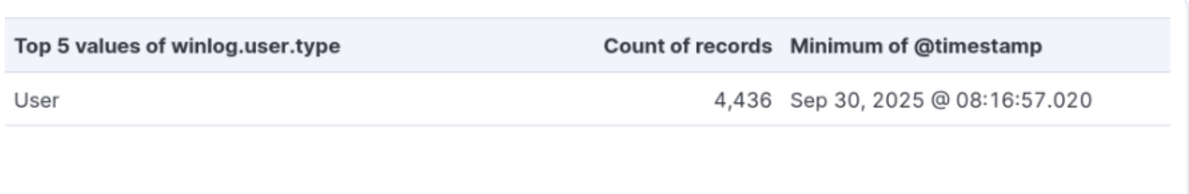


Sep 23, 2025 @ 00:00:00.000 - Sep 30, 2025 @ 10:39:27.624 (interval: Auto - 3 hours)

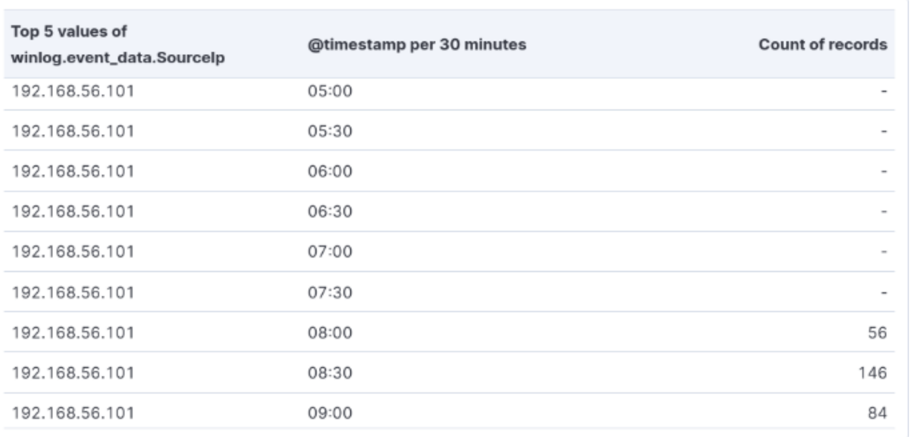
```
Sep 30, 2025 @ 10:39:13.338  @timestamp Sep 30, 2025 @ 10:39:13.338 agent.ephemeral_id 3ea4f796-706a-42ea-bc46-985a53251483 agent.hostname DESKTOP-L99OUIR agent.id
                              dc37bbc5-6e48-4b45-b188-14ab960fffbb agent.name DESKTOP-L99OUIR agent.type winlogbeat agent.version 9.1.4 ecs.version 8.0.0
                             event.action File created (rule: FileCreate) event.code 11 event.created Sep 30, 2025 @ 10:39:14.919 event.kind event event.provider…
Sep 30, 2025 @ 10:39:06.134  @timestamp Sep 30, 2025 @ 10:39:06.134 agent.ephemeral_id 3ea4f796-706a-42ea-bc46-985a53251483 agent.hostname DESKTOP-L99OUIR agent.id
                              dc37bbc5-6e48-4b45-b188-14ab960fffbb agent.name DESKTOP-L99OUIR agent.type winlogbeat agent.version 9.1.4 ecs.version 8.0.0
                             event.action Network connection detected (rule: NetworkConnect) event.code 3 event.created Sep 30, 2025 @ 10:39:07.885 event.kind ev…
Sep 30, 2025 @ 10:38:58.196  @timestamp Sep 30, 2025 @ 10:38:58.196 agent.ephemeral_id 3ea4f796-706a-42ea-bc46-985a53251483 agent.hostname DESKTOP-L99OUIR agent.id
                              dc37bbc5-6e48-4b45-b188-14ab960fffbb agent.name DESKTOP-L99OUIR agent.type winlogbeat agent.version 9.1.4 ecs.version 8.0.0
                             event.action File created (rule: FileCreate) event.code 11 event.created Sep 30, 2025 @ 10:38:59.856 event.kind event event.provider…
Sep 30, 2025 @ 10:38:52.079  @timestamp Sep 30, 2025 @ 10:38:52.079 agent.ephemeral_id 3ea4f796-706a-42ea-bc46-985a53251483 agent.hostname DESKTOP-L99OUIR agent.id
                              dc37bbc5-6e48-4b45-b188-14ab960fffbb agent.name DESKTOP-L99OUIR agent.type winlogbeat agent.version 9.1.4 ecs.version 8.0.0
```

Data view/discover Kibana

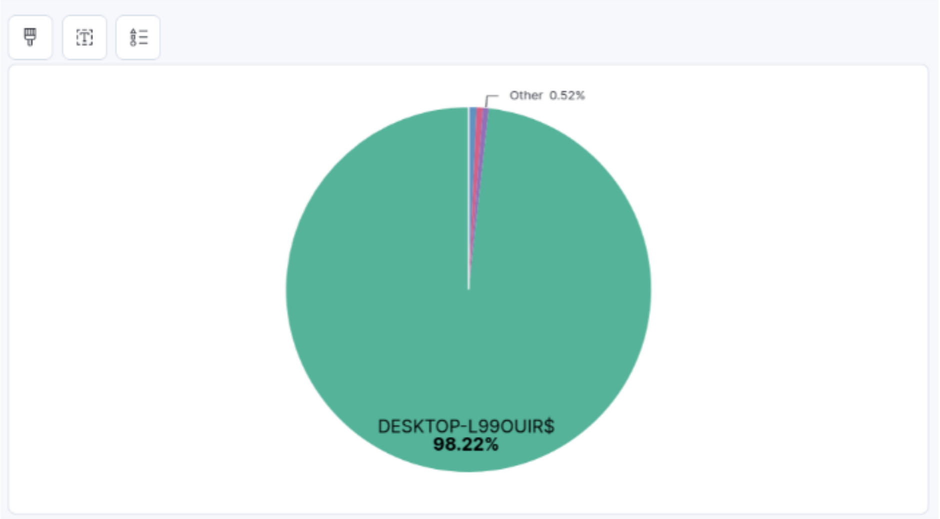


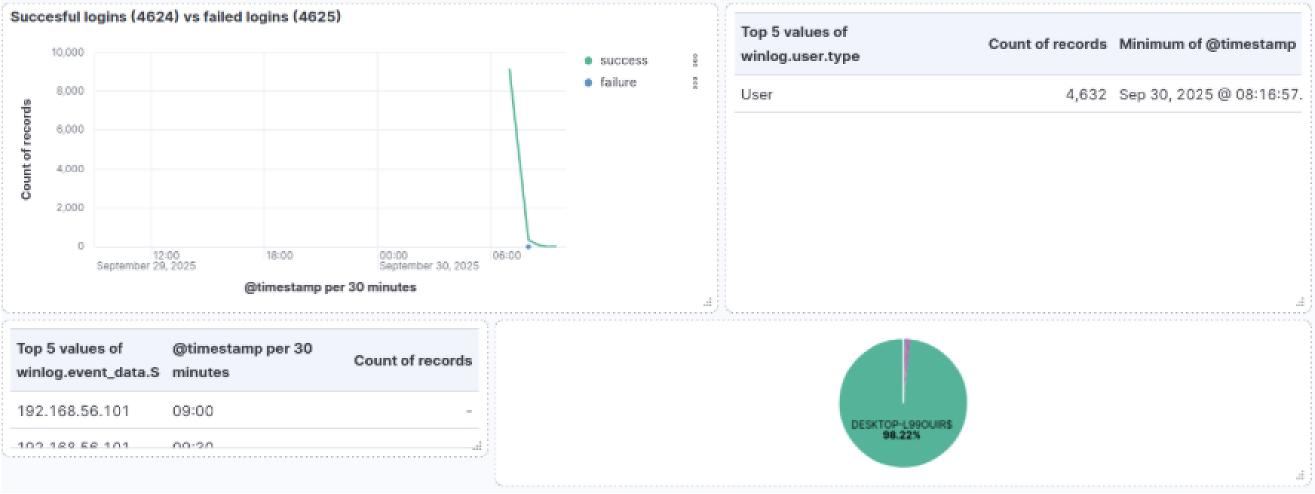


Top 5 values of winlog.user.type	Count of records	Minimum of @timestamp
User	4,436	Sep 30, 2025 @ 08:16:57.020



Top 5 values of winlog.event_data.SourceIp	@timestamp per 30 minutes	Count of records
192.168.56.101	05:00	-
192.168.56.101	05:30	-
192.168.56.101	06:00	-
192.168.56.101	06:30	-
192.168.56.101	07:00	-
192.168.56.101	07:30	-
192.168.56.101	08:00	56
192.168.56.101	08:30	146
192.168.56.101	09:00	84





Succesful logins (4624) vs failed logins (4625)

Top 5 values of winlog.user.type	Count of records	Minimum of @timestamp
User	4,632	Sep 30, 2025 @ 08:16:57.

Top 5 values of winlog.event_data.S	@timestamp per 30 minutes	Count of records
192.168.56.101	09:00	-
192.168.56.101	09:30	