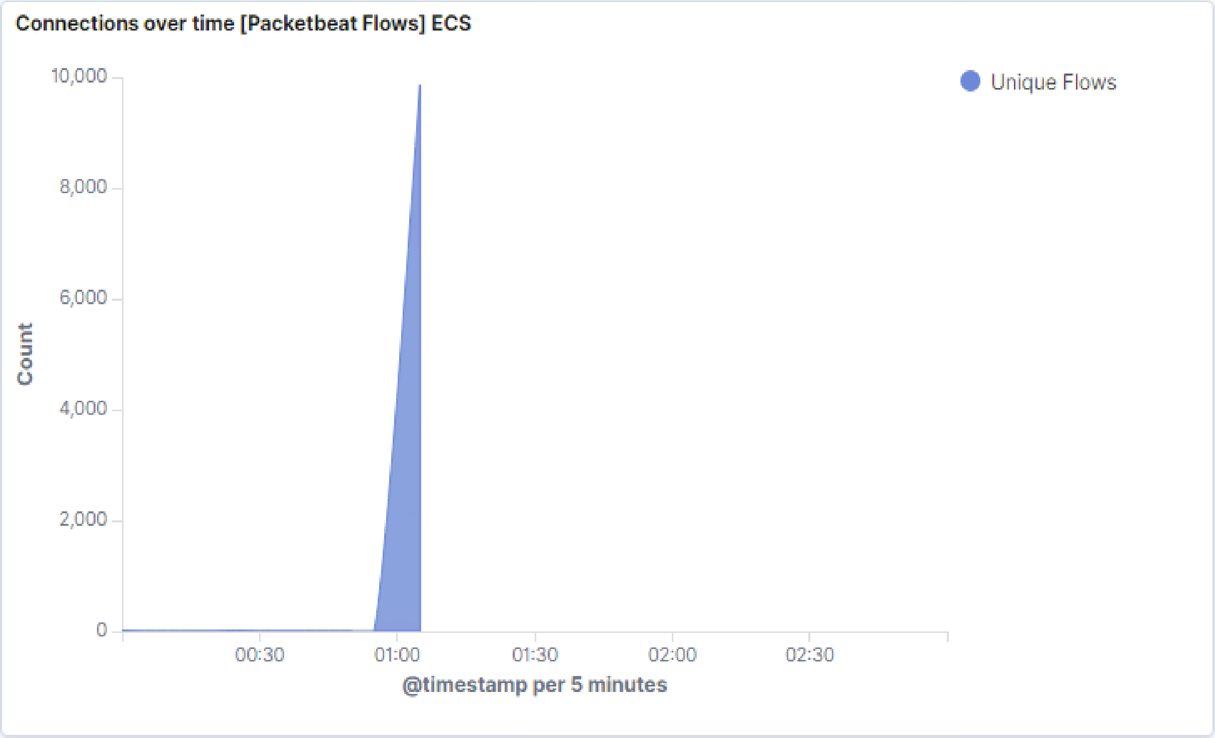
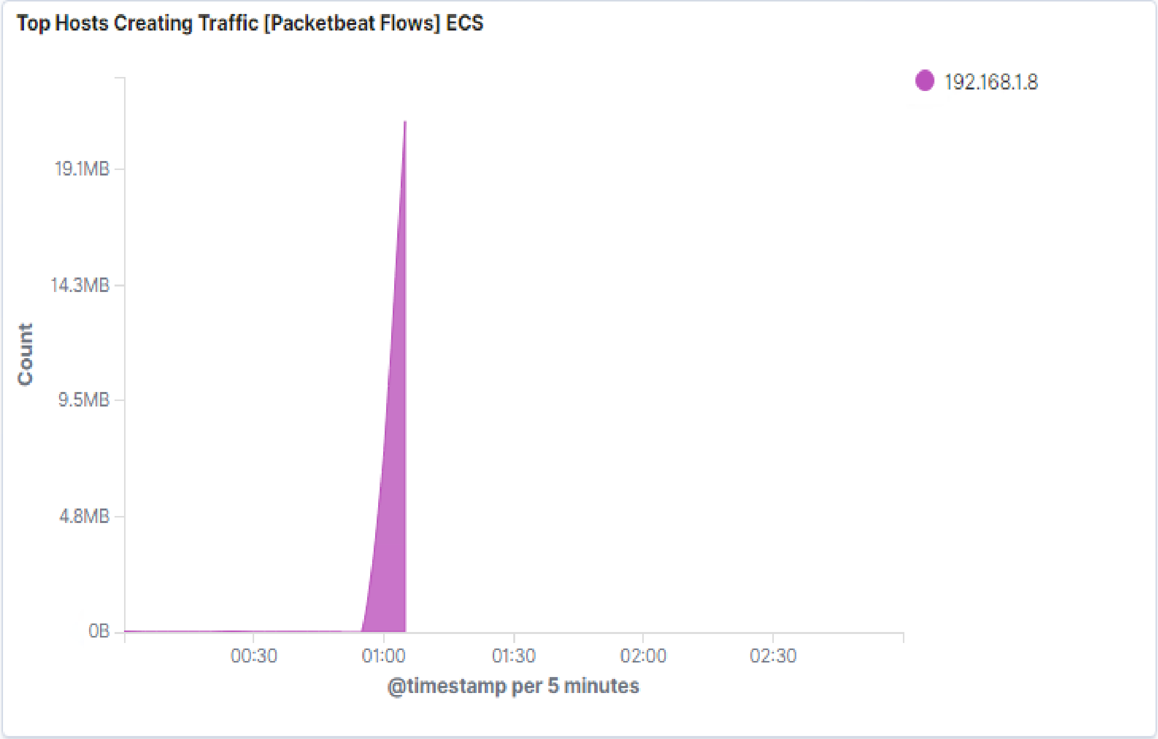
Blue Team

Log Analysis and Attack Characterization

Analysis: Identifying the Port Scan



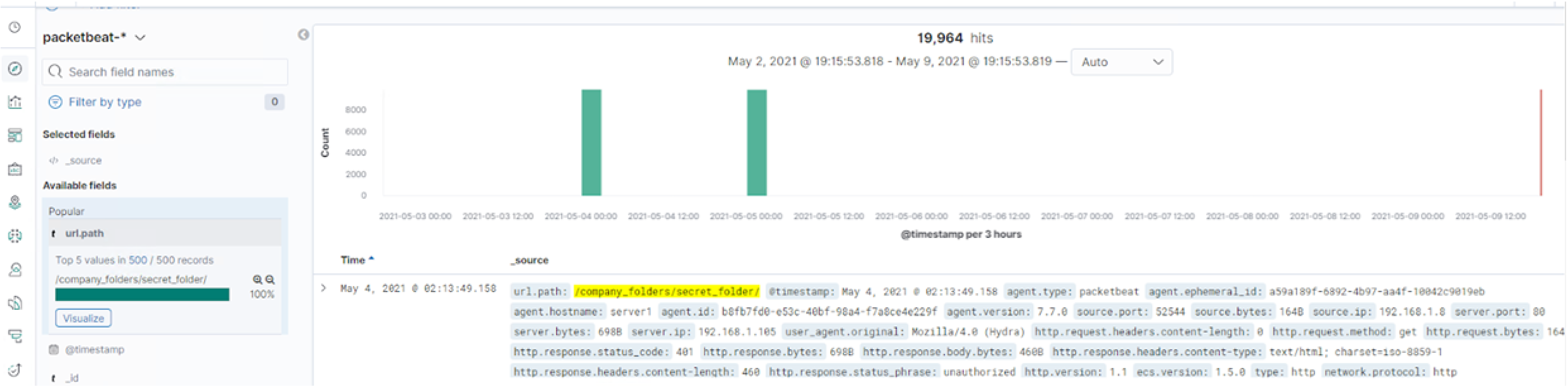
Connections over time [Packetbeat Flows] ECS



Top Hosts Creating Traffic [Packetbeat Flows] ECS

At the 1:05 mark we can observe spikes in activity and how it directly correlates to the IP Address: **192.168.1.8** (Attacker Machine).

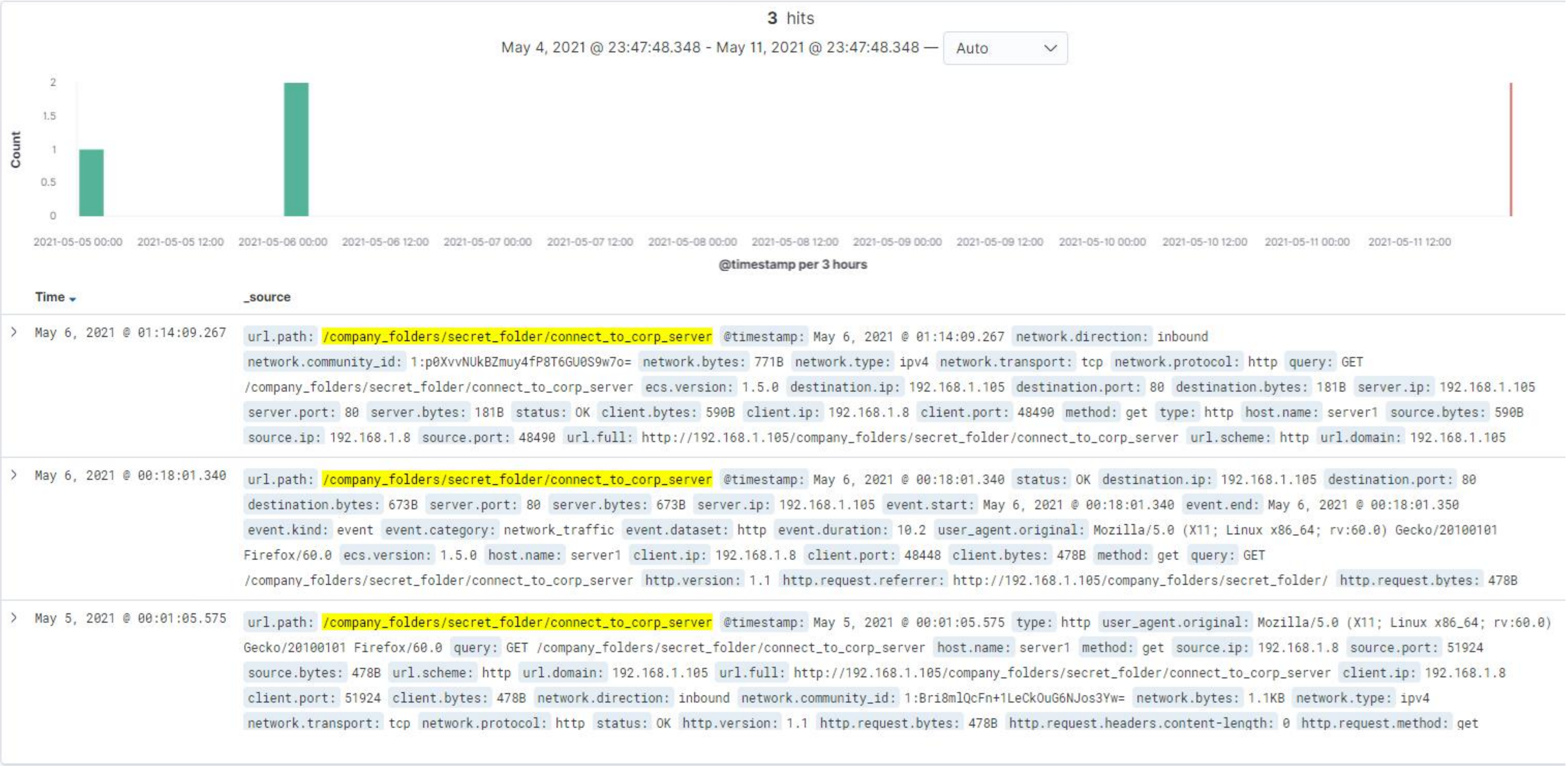
Analysis: Finding the Request for the Hidden Directory



```
May 4, 2021 @ 02:13:49.158   url.path: /company_folders/secret_folder/ @timestamp: May 4, 2021 @ 02:13:49.158 agent.type: packetbeat agent.ephemeral_id: a59a189f-6892-4b97-aa4f-10042c9019eb
                             agent.hostname: server1 agent.id: b8fb7fd0-e53c-40bf-98a4-f7a8ce4e229f agent.version: 7.7.0 source.port: 52544 source.bytes: 164B source.ip: 192.168.1.8 server.port: 80
                             server.bytes: 698B server.ip: 192.168.1.105 user_agent.original: Mozilla/4.0 (Hydra) http.request.headers.content-length: 0 http.request.method: get http.request.bytes: 164
                             http.response.status_code: 401 http.response.bytes: 698B http.response.body.bytes: 460B http.response.headers.content-type: text/html; charset=iso-8859-1
                             http.response.headers.content-length: 460 http.response.status_phrase: unauthorized http.version: 1.1 ecs.version: 1.5.0 type: http network.protocol: http
```

See additional slide next

Analysis: Finding the Request for the Hidden Directory



3 hits

May 4, 2021 @ 23:47:48.348 - May 11, 2021 @ 23:47:48.348 — Auto

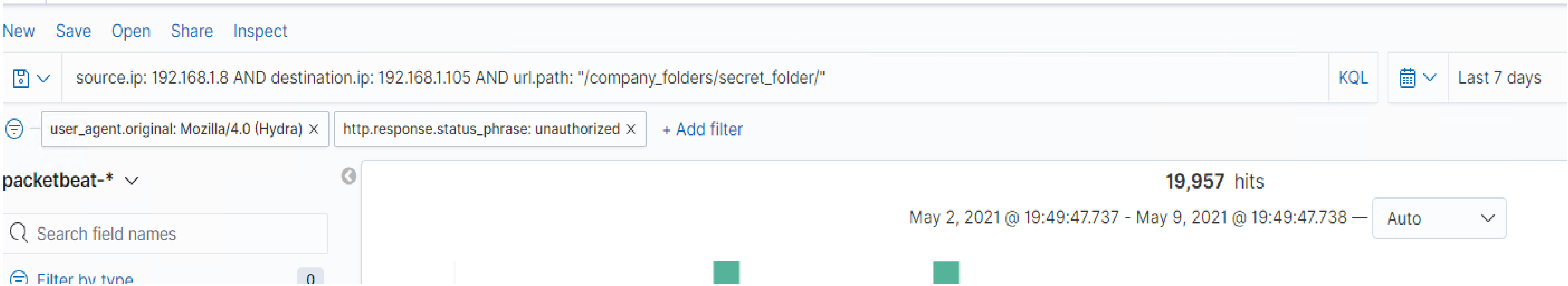
```
Time      _source

> May 6, 2021 @ 01:14:09.267   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 6, 2021 @ 01:14:09.267 network.direction: inbound
  network.community_id: 1:p0XvvNUkBZmuy4fP8T6GU0S9w7o= network.bytes: 771B network.type: ipv4 network.transport: tcp network.protocol: http query: GET
  /company_folders/secret_folder/connect_to_corp_server ecs.version: 1.5.0 destination.ip: 192.168.1.105 destination.port: 80 destination.bytes: 181B server.ip: 192.168.1.105
  server.port: 80 server.bytes: 181B status: OK client.bytes: 590B client.ip: 192.168.1.8 client.port: 48490 method: get type: http host.name: server1 source.bytes: 590B
  source.ip: 192.168.1.8 source.port: 48490 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server url.scheme: http url.domain: 192.168.1.105

> May 6, 2021 @ 00:18:01.340   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 6, 2021 @ 00:18:01.340 status: OK destination.ip: 192.168.1.105 destination.port: 80
  destination.bytes: 673B server.port: 80 server.bytes: 673B server.ip: 192.168.1.105 event.start: May 6, 2021 @ 00:18:01.340 event.end: May 6, 2021 @ 00:18:01.350
  event.kind: event event.category: network_traffic event.dataset: http event.duration: 10.2 user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0) Gecko/20100101
  Firefox/60.0 ecs.version: 1.5.0 host.name: server1 client.ip: 192.168.1.8 client.port: 48448 client.bytes: 478B method: get query: GET
  /company_folders/secret_folder/connect_to_corp_server http.version: 1.1 http.request.referrer: http://192.168.1.105/company_folders/secret_folder/ http.request.bytes: 478B

> May 5, 2021 @ 00:01:05.575   url.path: /company_folders/secret_folder/connect_to_corp_server @timestamp: May 5, 2021 @ 00:01:05.575 type: http user_agent.original: Mozilla/5.0 (X11; Linux x86_64; rv:60.0)
  Gecko/20100101 Firefox/60.0 query: GET /company_folders/secret_folder/connect_to_corp_server host.name: server1 method: get source.ip: 192.168.1.8 source.port: 51924
  source.bytes: 478B url.scheme: http url.domain: 192.168.1.105 url.full: http://192.168.1.105/company_folders/secret_folder/connect_to_corp_server client.ip: 192.168.1.8
  client.port: 51924 client.bytes: 478B network.direction: inbound network.community_id: 1:Bri8mlQcFn+1LeCkOuG6NJos3Yw= network.bytes: 1.1KB network.type: ipv4
  network.transport: tcp network.protocol: http status: OK http.version: 1.1 http.request.bytes: 478B http.request.headers.content-length: 0 http.request.method: get
```

Analysis: Uncovering the Brute Force Attack



source.ip: 192.168.1.8 AND destination.ip: 192.168.1.105 AND url.path: "/company_folders/secret_folder/"

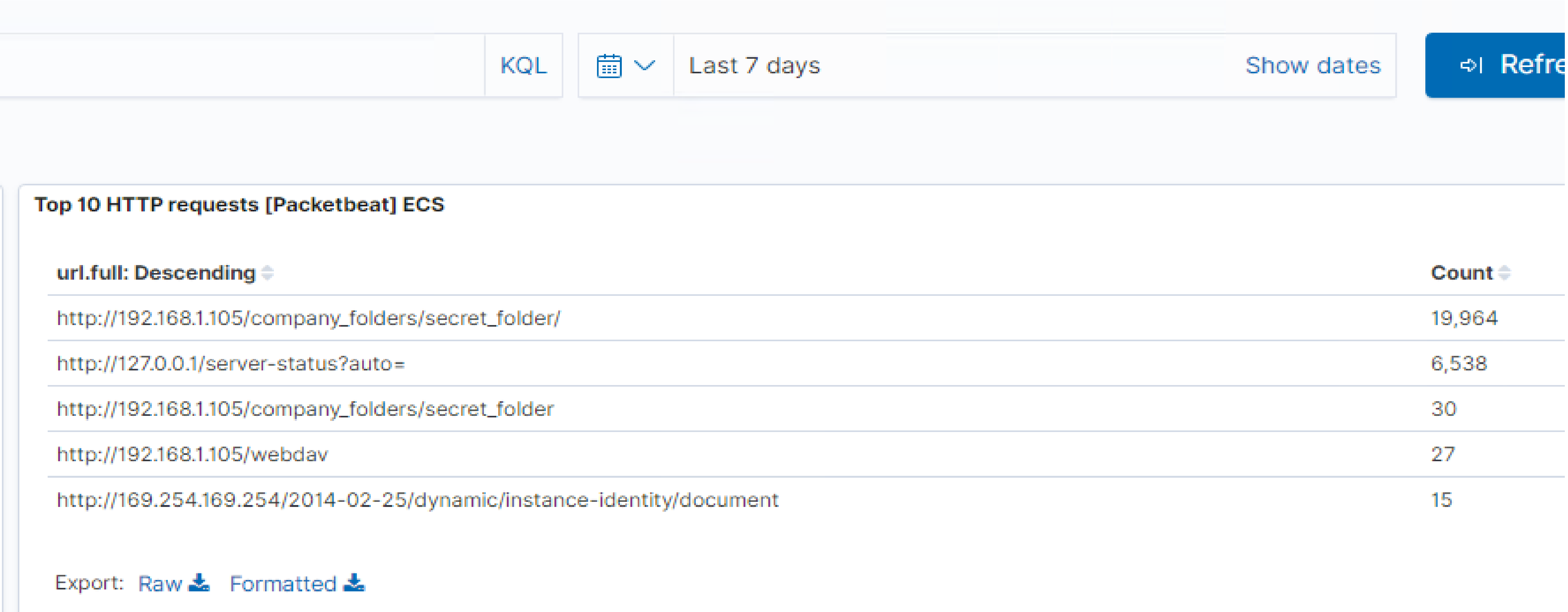
user_agent.original: Mozilla/4.0 (Hydra)

http.response.status_phrase: unauthorized

19,957 hits

May 2, 2021 @ 19:49:47.737 - May 9, 2021 @ 19:49:47.738

Analysis: Finding the WebDAV Connection



Top 10 HTTP requests [Packetbeat] ECS

url.full: Descending	Count
http://192.168.1.105/company_folders/secret_folder/	19,964
http://127.0.0.1/server-status?auto=	6,538
http://192.168.1.105/company_folders/secret_folder	30
http://192.168.1.105/webdav	27
http://169.254.169.254/2014-02-25/dynamic/instance-identity/document	15

Export: Raw Formatted