```
Ubuntu VM
├── FastAPI AI Application
    └── Logs: ai_app.log
├── Splunk Universal Forwarder
    └── Monitors ai_app.log
↓
Splunk Enterprise
├── Custom Index: ai_security
├── Field Extractions
├── Searches & Reports
└── Security Dashboard
```

AI Logging, Monitoring and Incident Readiness

Kate Amarachukwu Igwilo

Overview

Modern AI-powered applications introduce new security challenges due to their heavy reliance on APIs, automation, and large volumes of user-generated compiler and inference requests. Traditional infrastructure monitoring alone is insufficient; **application-level logging and security visibility are critical**.

This project demonstrates how to design and implement **logging, monitoring, and incident readiness for an AI-powered API** using Splunk as a SIEM. A FastAPI-based AI application was deployed on an Ubuntu server, configured to generate security-relevant logs, and integrated with Splunk using the Splunk Universal Forwarder.

The goal of this project is to simulate how AI application telemetry can be operationalized in a **SOC environment** for detection, investigation, and response readiness.

This project demonstrates how to implement centralized logging, monitoring, and basic incident readiness for an AI-powered API using Splunk. The goal is to simulate how AI application logs can be operationalized in a SOC environment for visibility, detection, and investigation.

A FastAPI-based AI application was deployed on Ubuntu, configured to generate structured security-relevant logs, which were forwarded to Splunk Enterprise using the Splunk Universal Forwarder.

Objectives

1. Generate structured application security logs from an AI API
2. Forward logs securely to Splunk
3. Perform field extraction for security analysis
4. Build dashboards for monitoring AI application behavior
5. Simulate detection logic for abnormal or suspicious activity
6. Demonstrate incident readiness workflows

Environment Setup

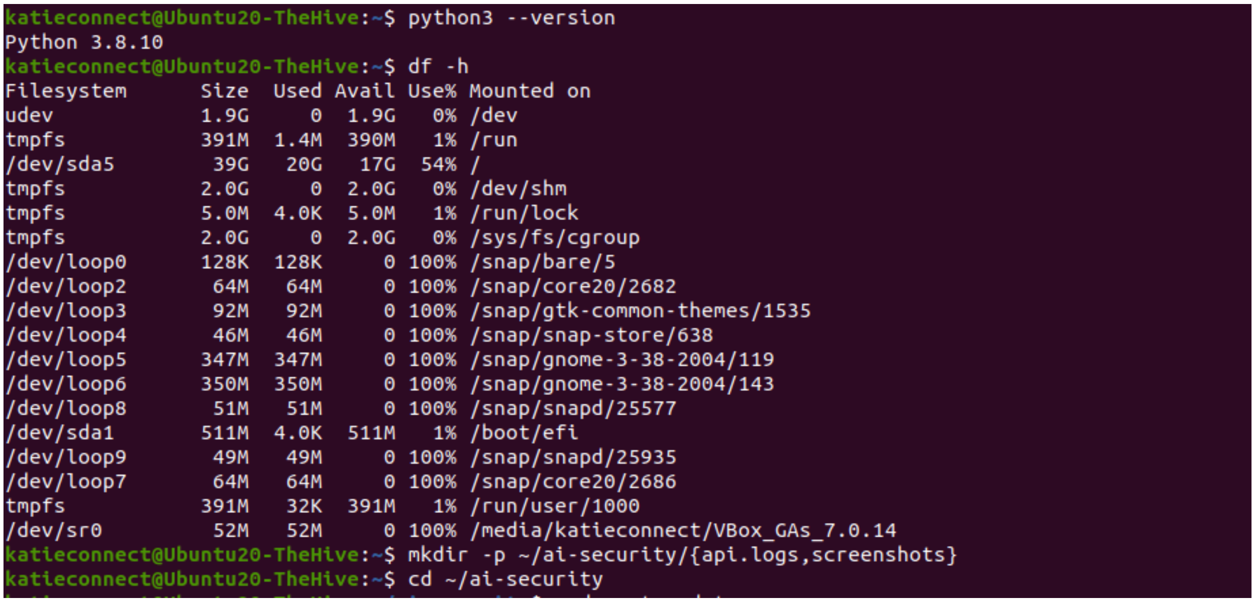
- OS: Ubuntu 20.04
- AI Framework: FastAPI (Uvicorn ASGI server)
- Logging: Python logging module
- SIEM: Splunk Enterprise (Free)
- Log Forwarding: Splunk Universal Forwarder

AI Application Deployment and Validation

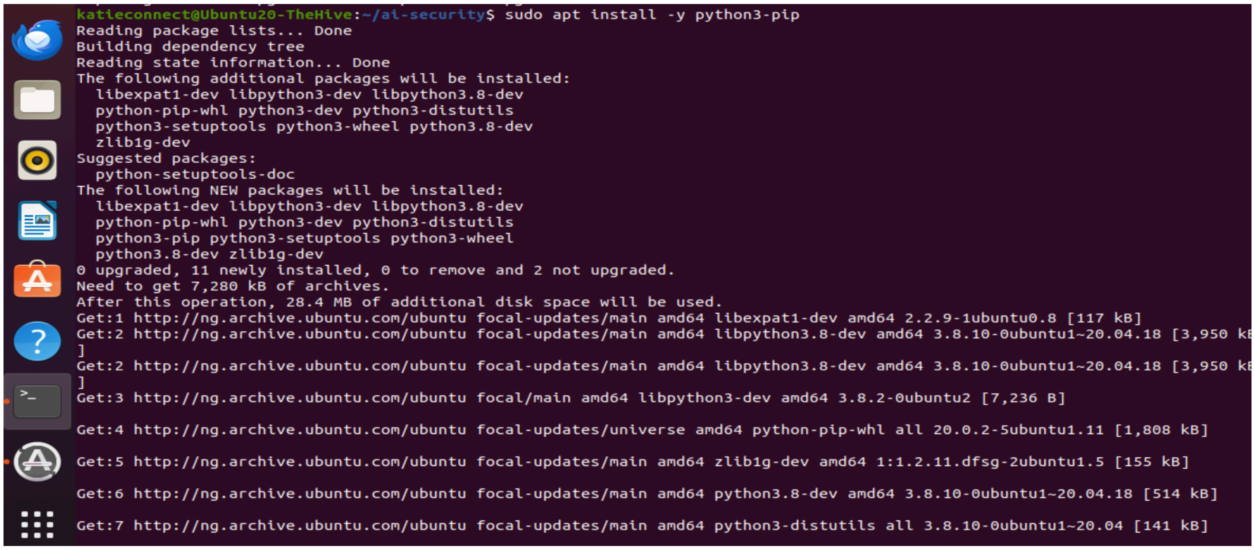
The FastAPI application was deployed on Ubuntu and exposed on port `8000`. Uvicorn was used as the ASGI server to handle incoming API requests.

The API was validated using:

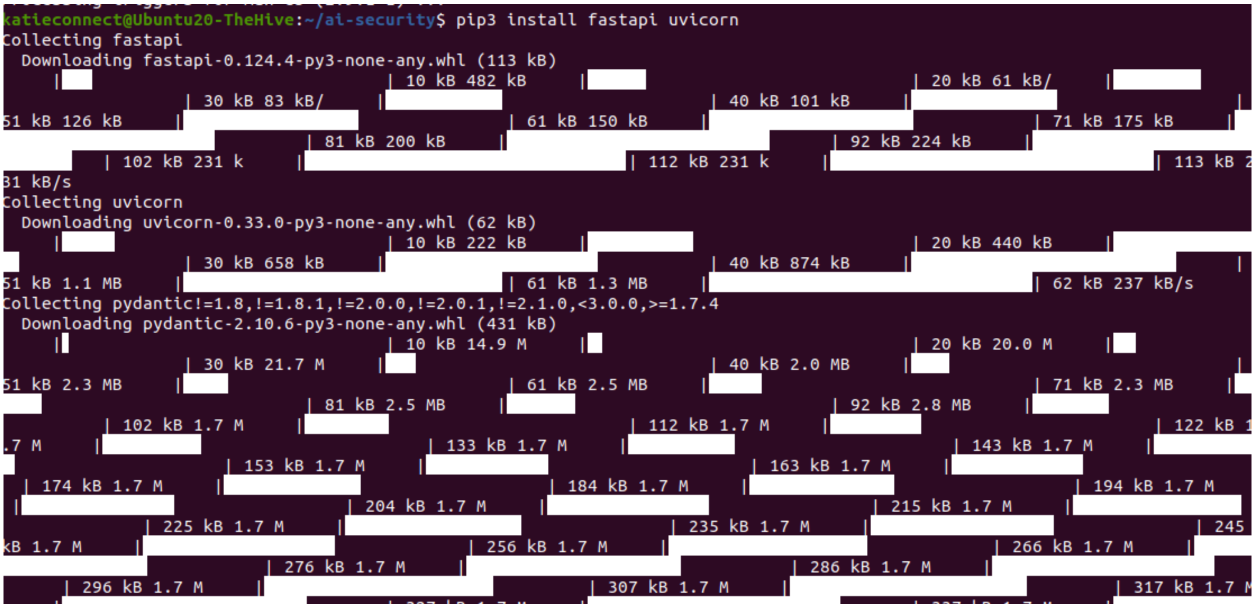
- FastAPI interactive documentation
- Direct `curl` requests to generate traffic and logs



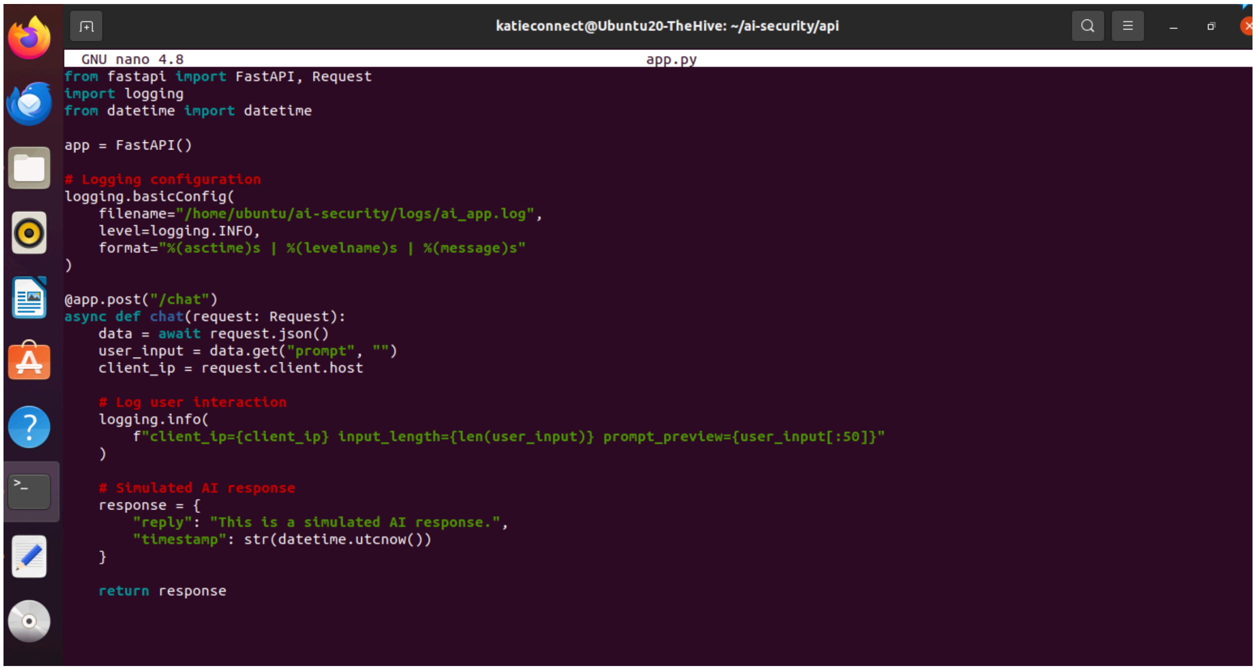
```
katieconnect@Ubuntu20-TheHive:~$ python3 --version
Python 3.8.10
katieconnect@Ubuntu20-TheHive:~$ df -h
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G     0  1.9G   0% /dev
tmpfs           391M  1.4M  390M   1% /run
/dev/sda5        39G   20G   17G  54% /
tmpfs           2.0G     0  2.0G   0% /dev/shm
tmpfs           5.0M  4.0K  5.0M   1% /run/lock
tmpfs           2.0G     0  2.0G   0% /sys/fs/cgroup
/dev/loop0      128K  128K     0 100% /snap/bare/5
/dev/loop2       64M   64M     0 100% /snap/core20/2682
/dev/loop3       92M   92M     0 100% /snap/gtk-common-themes/1535
/dev/loop4       46M   46M     0 100% /snap/snap-store/638
/dev/loop5      347M  347M     0 100% /snap/gnome-3-38-2004/119
/dev/loop6      350M  350M     0 100% /snap/gnome-3-38-2004/143
/dev/loop8       51M   51M     0 100% /snap/snapd/25577
/dev/sda1       511M  4.0K  511M   1% /boot/efi
/dev/loop9       49M   49M     0 100% /snap/snapd/25935
/dev/loop7       64M   64M     0 100% /snap/core20/2686
tmpfs           391M   32K  391M   1% /run/user/1000
/dev/sr0         52M   52M     0 100% /media/katieconnect/VBox_GAs_7.0.14
katieconnect@Ubuntu20-TheHive:~$ mkdir -p ~/ai-security/{api.logs,screenshots}
katieconnect@Ubuntu20-TheHive:~$ cd ~/ai-security
```



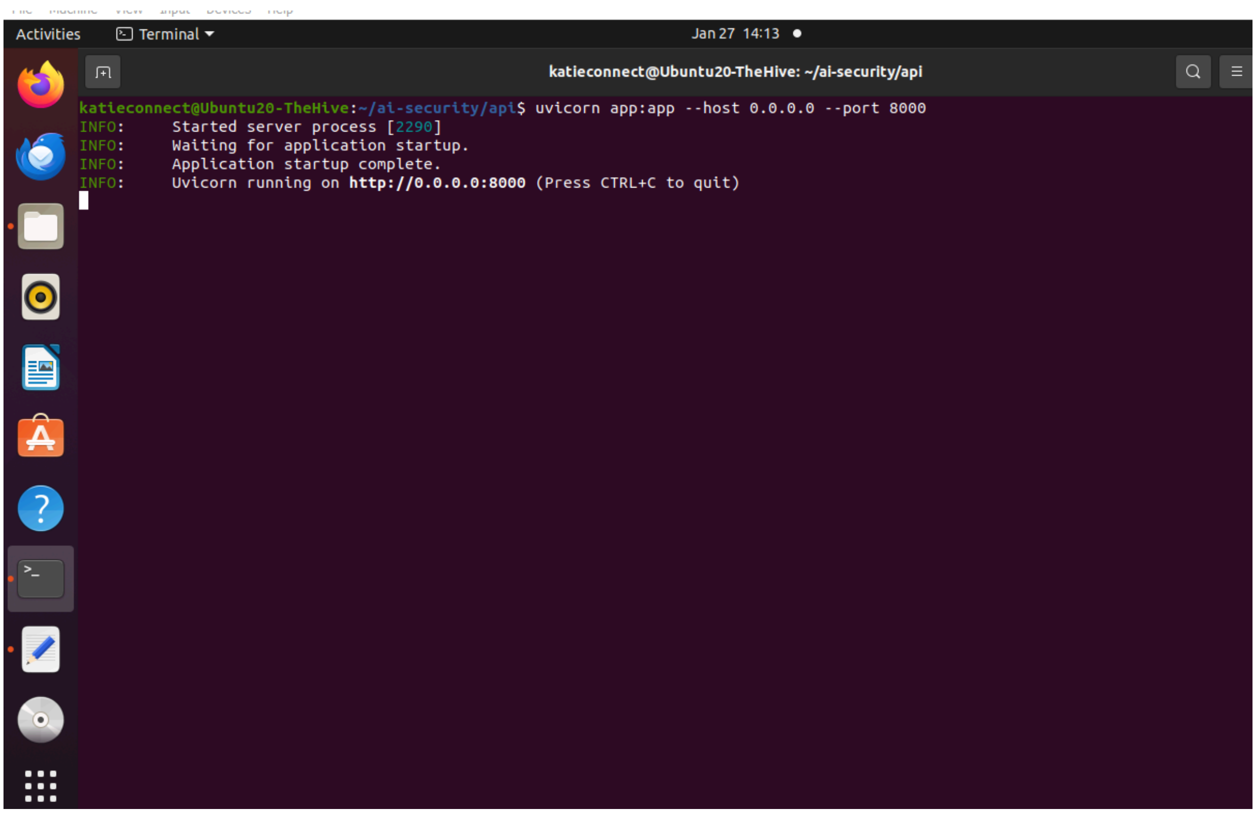
```
katieconnect@Ubuntu20-TheHive:~/ai-security$ sudo apt install -y python3-pip
Reading package lists... Done
Building dependency tree
Reading state information... Done
The following additional packages will be installed:
  libexpat1-dev libpython3-dev libpython3.8-dev
  python-pip-whl python3-dev python3-distutils
  python3-setuptools python3-wheel python3.8-dev
  zlib1g-dev
Suggested packages:
  python-setuptools-doc
The following NEW packages will be installed:
  libexpat1-dev libpython3-dev libpython3.8-dev
  python-pip-whl python3-dev python3-distutils
  python3-pip python3-setuptools python3-wheel
  python3.8-dev zlib1g-dev
0 upgraded, 11 newly installed, 0 to remove and 2 not upgraded.
Need to get 7,280 kB of archives.
After this operation, 28.4 MB of additional disk space will be used.
Get:1 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 libexpat1-dev amd64 2.2.9-1ubuntu0.8 [117 kB]
Get:2 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8-dev amd64 3.8.10-0ubuntu1~20.04.18 [3,950 kB
]
Get:2 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 libpython3.8-dev amd64 3.8.10-0ubuntu1~20.04.18 [3,950 kB
]
Get:3 http://ng.archive.ubuntu.com/ubuntu focal/main amd64 libpython3-dev amd64 3.8.2-0ubuntu2 [7,236 B]

Get:4 http://ng.archive.ubuntu.com/ubuntu focal-updates/universe amd64 python-pip-whl all 20.0.2-5ubuntu1.11 [1,808 kB]

Get:5 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 zlib1g-dev amd64 1:1.2.11.dfsg-2ubuntu1.5 [155 kB]

Get:6 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3.8-dev amd64 3.8.10-0ubuntu1~20.04.18 [514 kB]

Get:7 http://ng.archive.ubuntu.com/ubuntu focal-updates/main amd64 python3-distutils all 3.8.10-0ubuntu1~20.04 [141 kB]
```



```
katieconnect@Ubuntu20-TheHive:~/ai-security$ pip3 install fastapi uvicorn
Collecting fastapi
  Downloading fastapi-0.124.4-py3-none-any.whl (113 kB)
     |                              | 10 kB 482 kB     |                              | 20 kB 61 kB/     |
                    | 30 kB 83 kB/     |                              | 40 kB 101 kB     |                              |
51 kB 126 kB     |                              | 61 kB 150 kB     |                              | 71 kB 175 kB     |
                              | 81 kB 200 kB     |                              | 92 kB 224 kB     |
          | 102 kB 231 k     |                              | 112 kB 231 k     |                              | 113 kB 2
31 kB/s
Collecting uvicorn
  Downloading uvicorn-0.33.0-py3-none-any.whl (62 kB)
     |                              | 10 kB 222 kB     |                              | 20 kB 440 kB     |
                    | 30 kB 658 kB     |                              | 40 kB 874 kB     |                              |
51 kB 1.1 MB     |                              | 61 kB 1.3 MB     |                              | 62 kB 237 kB/s
Collecting pydantic!=1.8,!=1.8.1,!=2.0.0,!=2.0.1,!=2.1.0,<3.0.0,>=1.7.4
  Downloading pydantic-2.10.6-py3-none-any.whl (431 kB)
     ||                             | 10 kB 14.9 M     |                              | 20 kB 20.0 M     |
                    | 30 kB 21.7 M     |                              | 40 kB 2.0 MB     |                              |
51 kB 2.3 MB     |                              | 61 kB 2.5 MB     |                              | 71 kB 2.3 MB     |
                              | 81 kB 2.5 MB     |                              | 92 kB 2.8 MB     |
          | 102 kB 1.7 M     |                              | 112 kB 1.7 M     |                              | 122 kB 1
.7 M     |                              | 133 kB 1.7 M     |                              | 143 kB 1.7 M     |
                         | 153 kB 1.7 M     |                              | 163 kB 1.7 M     |
  | 174 kB 1.7 M     |                              | 184 kB 1.7 M     |                              | 194 kB 1.7 M
 |                              | 204 kB 1.7 M     |                              | 215 kB 1.7 M     |
                 | 225 kB 1.7 M     |                              | 235 kB 1.7 M     |                              | 245
kB 1.7 M     |                              | 256 kB 1.7 M     |                              | 266 kB 1.7 M     |
                             | 276 kB 1.7 M     |                              | 286 kB 1.7 M     |
      | 296 kB 1.7 M     |                              | 307 kB 1.7 M     |                              | 317 kB 1.7 M
```

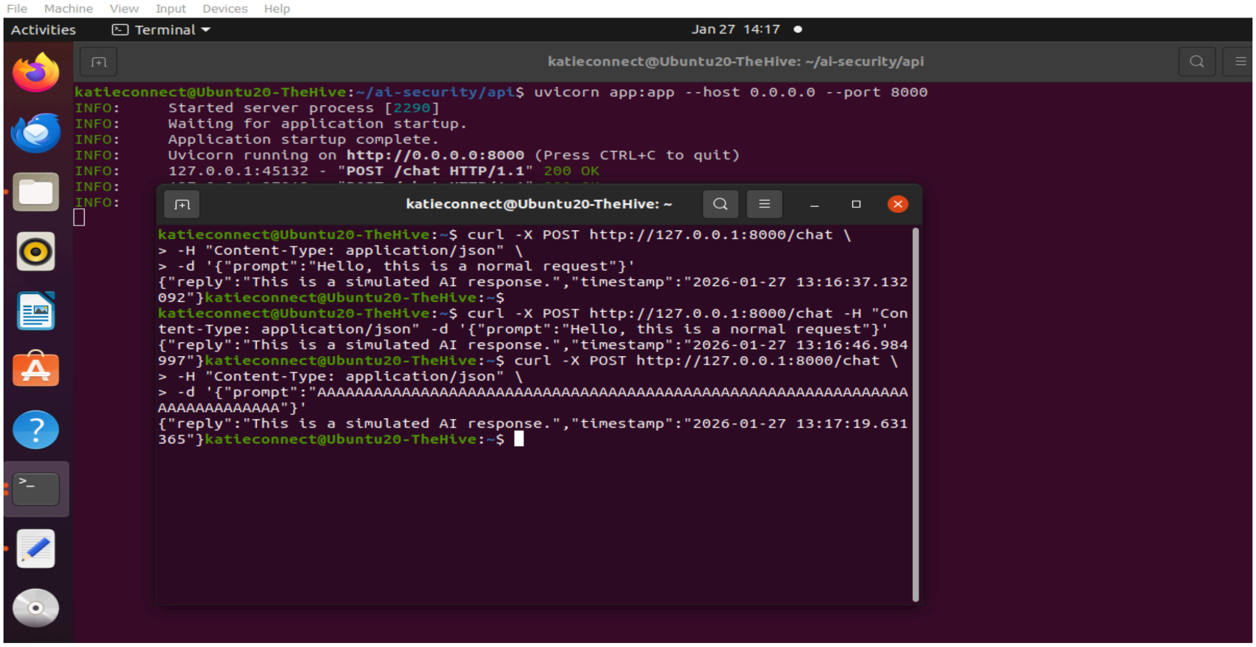


```
from fastapi import FastAPI, Request
import logging
from datetime import datetime

app = FastAPI()

# Logging configuration
logging.basicConfig(
    filename="/home/ubuntu/ai-security/logs/ai_app.log",
    level=logging.INFO,
    format="%(asctime)s | %(levelname)s | %(message)s"
)

@app.post("/chat")
async def chat(request: Request):
    data = await request.json()
    user_input = data.get("prompt", "")
    client_ip = request.client.host

    # Log user interaction
    logging.info(
        f"client_ip={client_ip} input_length={len(user_input)} prompt_preview={user_input[:50]}"
    )

    # Simulated AI response
    response = {
        "reply": "This is a simulated AI response.",
        "timestamp": str(datetime.utcnow())
    }

    return response
```


File Machine View Input Devices Help
Activities
Terminal
Jan 27 14:13
katieconnect@Ubuntu20-TheHive: ~/ai-security/api

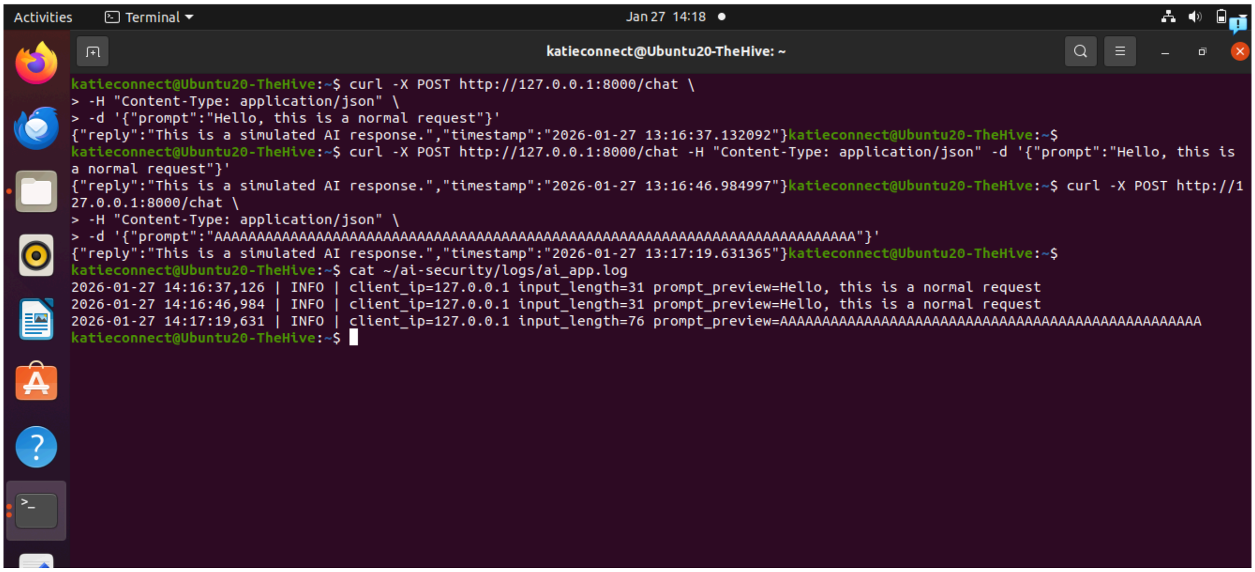
```
katieconnect@Ubuntu20-TheHive:~/ai-security/api$ uvicorn app:app --host 0.0.0.0 --port 8000
INFO:     Started server process [2290]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:8000 (Press CTRL+C to quit)
```

AI Application Running on Ubuntu

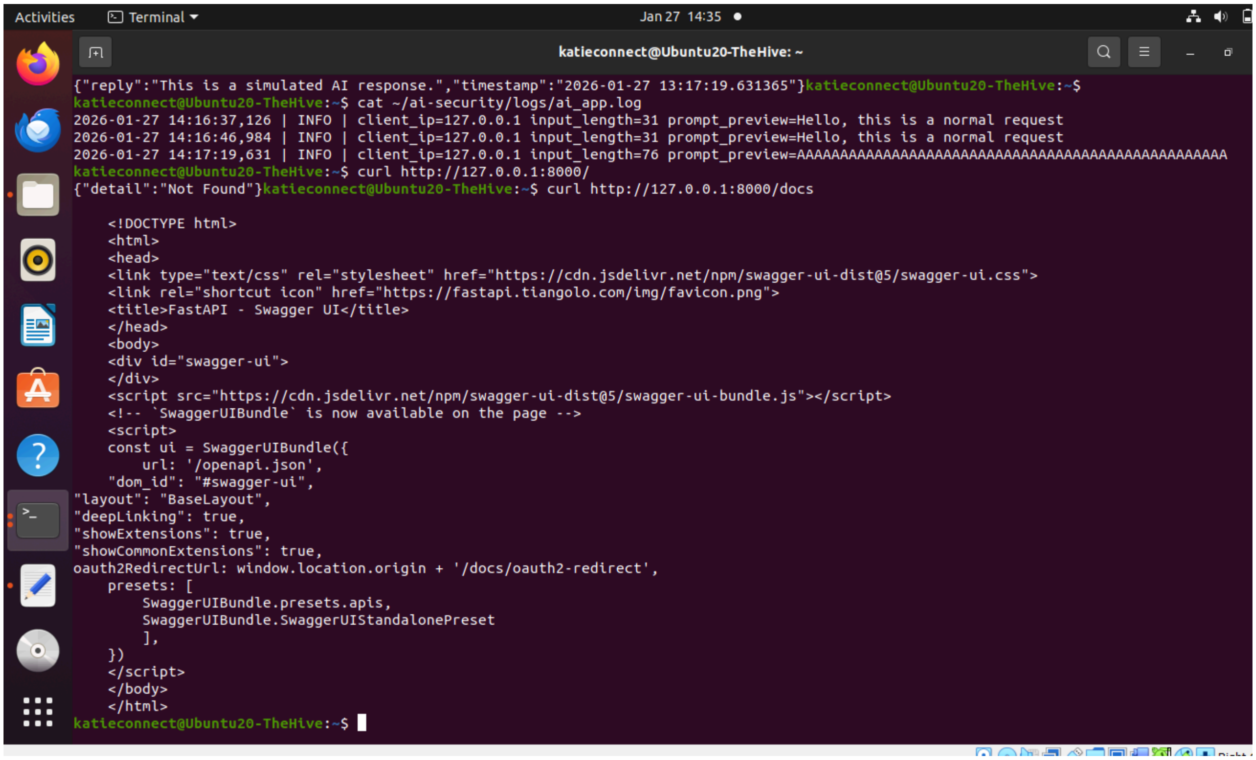

File
Machine
View
Input
Devices
Help
Activities
Terminal
Jan 27 14:17
katieconnect@Ubuntu20-TheHive: ~/ai-security/api
katieconnect@Ubuntu20-TheHive: ~

```
katieconnect@Ubuntu20-TheHive:~/ai-security/api$ uvicorn app:app --host 0.0.0.0 --port 8000
INFO:     Started server process [2290]
INFO:     Waiting for application startup.
INFO:     Application startup complete.
INFO:     Uvicorn running on http://0.0.0.0:8000 (Press CTRL+C to quit)
INFO:     127.0.0.1:45132 - "POST /chat HTTP/1.1" 200 OK
INFO:
INFO:
```

```
katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://127.0.0.1:8000/chat \
> -H "Content-Type: application/json" \
> -d '{"prompt":"Hello, this is a normal request"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:16:37.132
092"}katieconnect@Ubuntu20-TheHive:~$
katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://127.0.0.1:8000/chat -H "Con
tent-Type: application/json" -d '{"prompt":"Hello, this is a normal request"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:16:46.984
997"}katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://127.0.0.1:8000/chat \
> -H "Content-Type: application/json" \
> -d '{"prompt":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAA"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:17:19.631
365"}katieconnect@Ubuntu20-TheHive:~$
```



```
katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://127.0.0.1:8000/chat \
> -H "Content-Type: application/json" \
> -d '{"prompt":"Hello, this is a normal request"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:16:37.132092"}katieconnect@Ubuntu20-TheHive:~$
katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://127.0.0.1:8000/chat -H "Content-Type: application/json" -d '{"prompt":"Hello, this is
a normal request"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:16:46.984997"}katieconnect@Ubuntu20-TheHive:~$ curl -X POST http://1
27.0.0.1:8000/chat \
> -H "Content-Type: application/json" \
> -d '{"prompt":"AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA"}'
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:17:19.631365"}katieconnect@Ubuntu20-TheHive:~$
katieconnect@Ubuntu20-TheHive:~$ cat ~/ai-security/logs/ai_app.log
2026-01-27 14:16:37,126 | INFO | client_ip=127.0.0.1 input_length=31 prompt_preview=Hello, this is a normal request
2026-01-27 14:16:46,984 | INFO | client_ip=127.0.0.1 input_length=31 prompt_preview=Hello, this is a normal request
2026-01-27 14:17:19,631 | INFO | client_ip=127.0.0.1 input_length=76 prompt_preview=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
katieconnect@Ubuntu20-TheHive:~$
```



```
{"reply":"This is a simulated AI response.","timestamp":"2026-01-27 13:17:19.631365"}katieconnect@Ubuntu20-TheHive:~$
katieconnect@Ubuntu20-TheHive:~$ cat ~/ai-security/logs/ai_app.log
2026-01-27 14:16:37,126 | INFO | client_ip=127.0.0.1 input_length=31 prompt_preview=Hello, this is a normal request
2026-01-27 14:16:46,984 | INFO | client_ip=127.0.0.1 input_length=31 prompt_preview=Hello, this is a normal request
2026-01-27 14:17:19,631 | INFO | client_ip=127.0.0.1 input_length=76 prompt_preview=AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
katieconnect@Ubuntu20-TheHive:~$ curl http://127.0.0.1:8000/
{"detail":"Not Found"}katieconnect@Ubuntu20-TheHive:~$ curl http://127.0.0.1:8000/docs

    <!DOCTYPE html>
    <html>
    <head>
    <link type="text/css" rel="stylesheet" href="https://cdn.jsdelivr.net/npm/swagger-ui-dist@5/swagger-ui.css">
    <link rel="shortcut icon" href="https://fastapi.tiangolo.com/img/favicon.png">
    <title>FastAPI - Swagger UI</title>
    </head>
    <body>
    <div id="swagger-ui">
    </div>
    <script src="https://cdn.jsdelivr.net/npm/swagger-ui-dist@5/swagger-ui-bundle.js"></script>
    <!-- `SwaggerUIBundle` is now available on the page -->
    <script>
    const ui = SwaggerUIBundle({
        url: '/openapi.json',
    "dom_id": "#swagger-ui",
"layout": "BaseLayout",
"deepLinking": true,
"showExtensions": true,
"showCommonExtensions": true,
oauth2RedirectUrl: window.location.origin + '/docs/oauth2-redirect',
    presets: [
        SwaggerUIBundle.presets.apis,
        SwaggerUIBundle.SwaggerUIStandalonePreset
        ],
    })
    </script>
    </body>
    </html>
katieconnect@Ubuntu20-TheHive:~$
```

FastAPI interactive documentation confirming API availability

Log Ingestion into Splunk

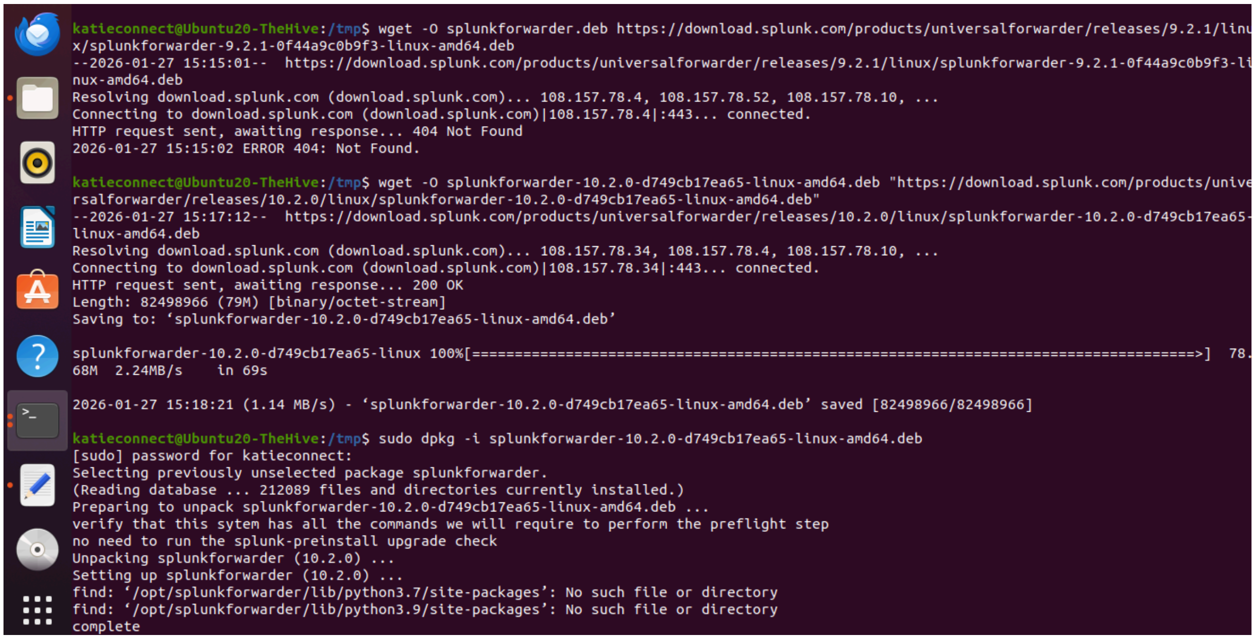
Forwarder Configuration

The Splunk Universal Forwarder was configured to monitor the AI application log file:

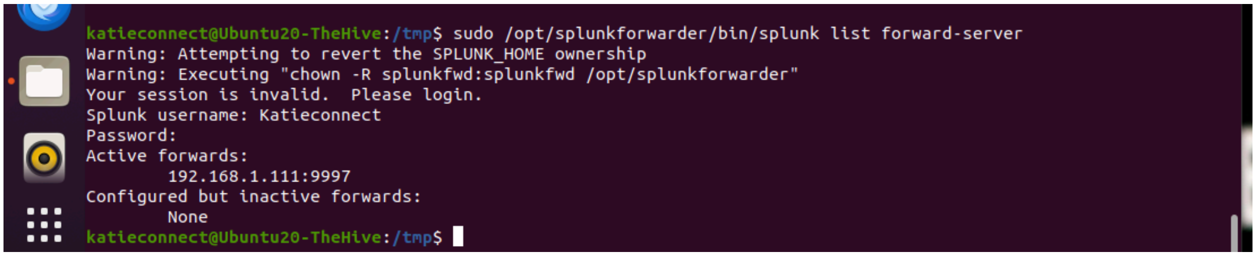
monitor:///home/katieconnect/ai-security/logs/ai_app.log

index=ai_security

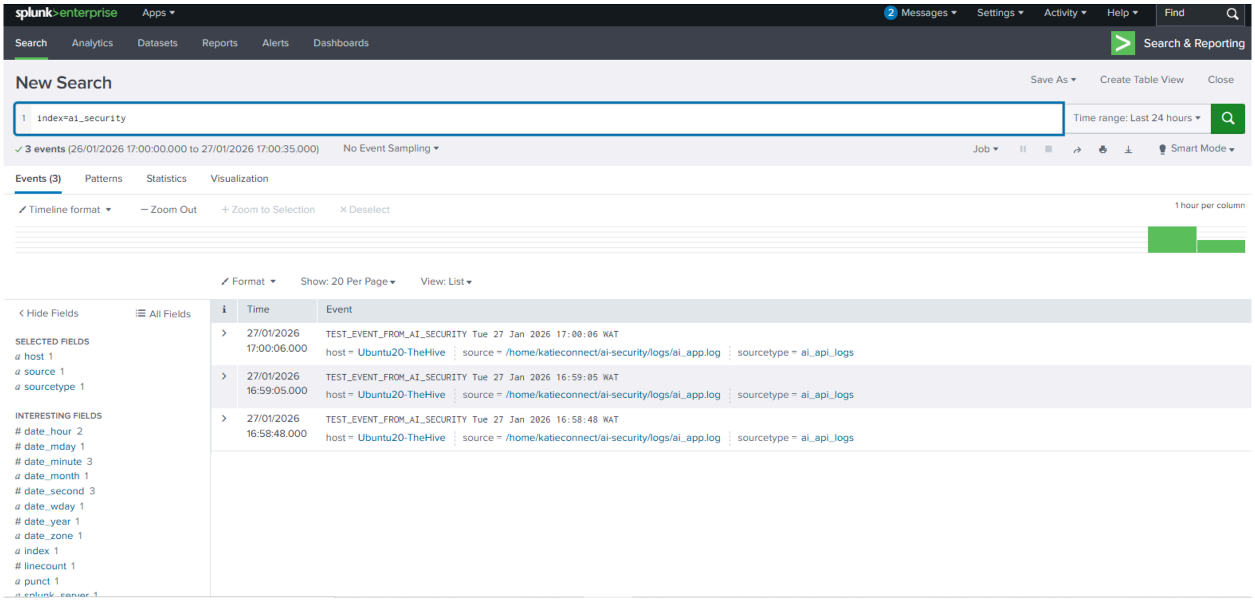
sourcetype=ai_api_logs



```
katieconnect@Ubuntu20-TheHive:/tmp$ wget -O splunkforwarder.deb https://download.splunk.com/products/universalforwarder/releases/9.2.1/linu
x/splunkforwarder-9.2.1-0f44a9c0b9f3-linux-amd64.deb
--2026-01-27 15:15:01--  https://download.splunk.com/products/universalforwarder/releases/9.2.1/linux/splunkforwarder-9.2.1-0f44a9c0b9f3-li
nux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 108.157.78.4, 108.157.78.52, 108.157.78.10, ...
Connecting to download.splunk.com (download.splunk.com)|108.157.78.4|:443... connected.
HTTP request sent, awaiting response... 404 Not Found
2026-01-27 15:15:02 ERROR 404: Not Found.

katieconnect@Ubuntu20-TheHive:/tmp$ wget -O splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb "https://download.splunk.com/products/unive
rsalforwarder/releases/10.2.0/linux/splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb"
--2026-01-27 15:17:12--  https://download.splunk.com/products/universalforwarder/releases/10.2.0/linux/splunkforwarder-10.2.0-d749cb17ea65-
linux-amd64.deb
Resolving download.splunk.com (download.splunk.com)... 108.157.78.34, 108.157.78.4, 108.157.78.10, ...
Connecting to download.splunk.com (download.splunk.com)|108.157.78.34|:443... connected.
HTTP request sent, awaiting response... 200 OK
Length: 82498966 (79M) [binary/octet-stream]
Saving to: ‘splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb’

splunkforwarder-10.2.0-d749cb17ea65-linux 100%[=====================================================================================>]  78.
68M  2.24MB/s    in 69s

2026-01-27 15:18:21 (1.14 MB/s) - ‘splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb’ saved [82498966/82498966]

katieconnect@Ubuntu20-TheHive:/tmp$ sudo dpkg -i splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb
[sudo] password for katieconnect:
Selecting previously unselected package splunkforwarder.
(Reading database ... 212089 files and directories currently installed.)
Preparing to unpack splunkforwarder-10.2.0-d749cb17ea65-linux-amd64.deb ...
verify that this sytem has all the commands we will require to perform the preflight step
no need to run the splunk-preinstall upgrade check
Unpacking splunkforwarder (10.2.0) ...
Setting up splunkforwarder (10.2.0) ...
find: ‘/opt/splunkforwarder/lib/python3.7/site-packages’: No such file or directory
find: ‘/opt/splunkforwarder/lib/python3.9/site-packages’: No such file or directory
complete
```



```
katieconnect@Ubuntu20-TheHive:/tmp$ sudo /opt/splunkforwarder/bin/splunk list forward-server
Warning: Attempting to revert the SPLUNK_HOME ownership
Warning: Executing "chown -R splunkfwd:splunkfwd /opt/splunkforwarder"
Your session is invalid.  Please login.
Splunk username: Katieconnect
Password:
Active forwards:
        192.168.1.111:9997
Configured but inactive forwards:
        None
katieconnect@Ubuntu20-TheHive:/tmp$
```



New Search

```
index=ai_security
```

Time range: Last 24 hours

✓ 3 events (26/01/2026 17:00:00.000 to 27/01/2026 17:00:35.000) No Event Sampling

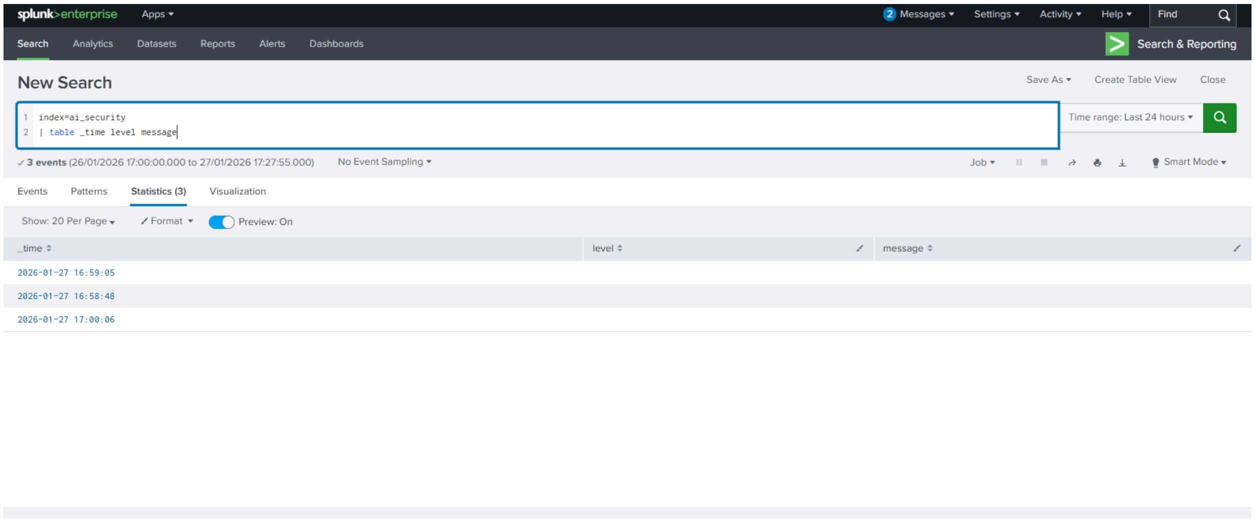
```
i  Time                     Event
>  27/01/2026               TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 WAT
   17:00:06.000             host = Ubuntu20-TheHive | source = /home/katieconnect/ai-security/logs/ai_app.log | sourcetype = ai_api_logs
>  27/01/2026               TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 WAT
   16:59:05.000             host = Ubuntu20-TheHive | source = /home/katieconnect/ai-security/logs/ai_app.log | sourcetype = ai_api_logs
>  27/01/2026               TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 WAT
   16:58:48.000             host = Ubuntu20-TheHive | source = /home/katieconnect/ai-security/logs/ai_app.log | sourcetype = ai_api_logs
```

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 3
a date_month 1
# date_second 3
a date_wday 1
# date_year 1
a date_zone 1
a index 1
# linecount 1
a punct 1
a splunk_server 1

Field Extraction

To enable meaningful analysis, custom field extractions were created. These fields allow filtering, aggregation, and correlation of AI security events across time and sources.

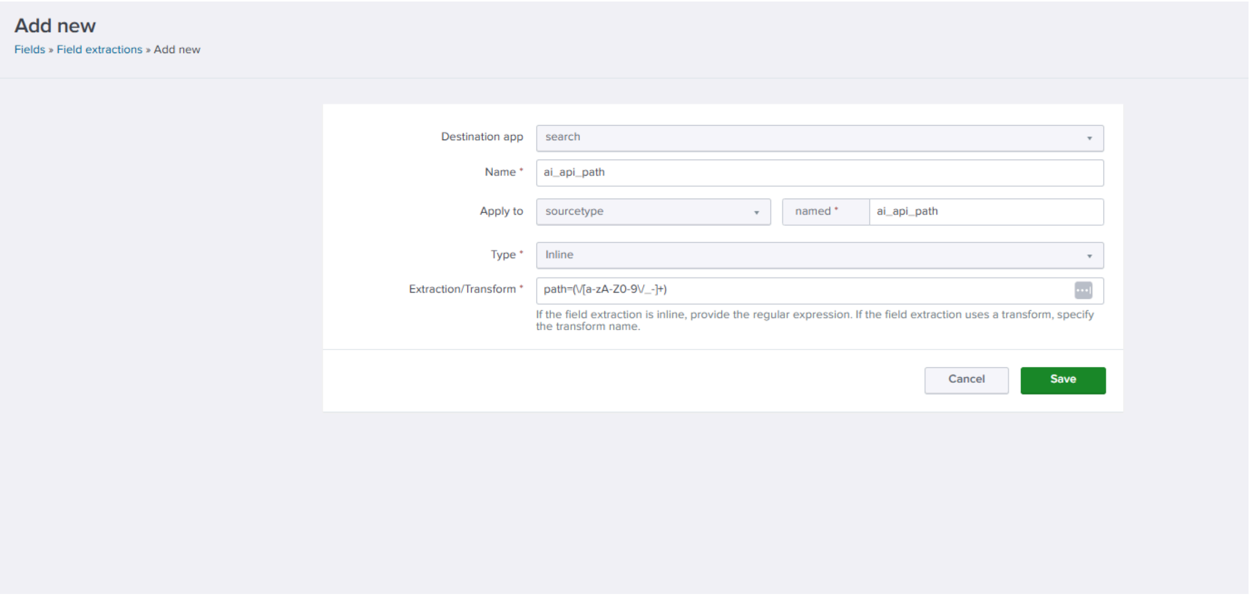


New Search

```
index=ai_security
| table _time level message
```

✓ 3 events (26/01/2026 17:00:00.000 to 27/01/2026 17:27:55.000)

_time	level	message
2026-01-27 16:59:05		
2026-01-27 16:58:48		
2026-01-27 17:00:06		

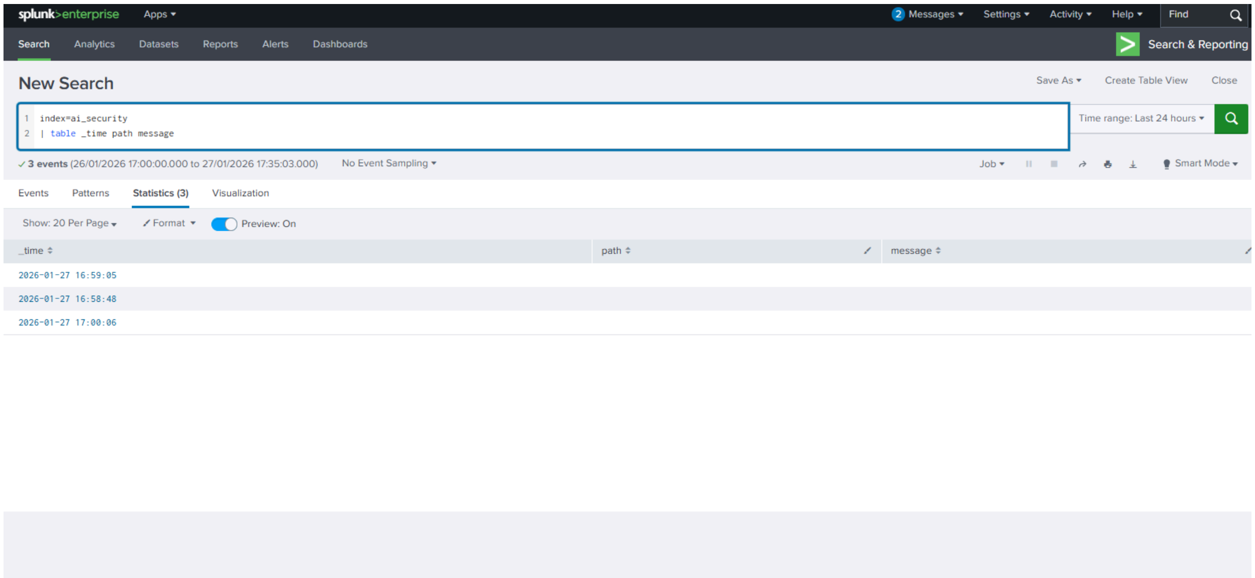


Add new

Fields » Field extractions » Add new

Destination app	search
Name *	ai_api_path
Apply to	sourcetype — named * ai_api_path
Type *	Inline
Extraction/Transform *	path=(\/[a-zA-Z0-9\/_-]+)

If the field extraction is inline, provide the regular expression. If the field extraction uses a transform, specify the transform name.

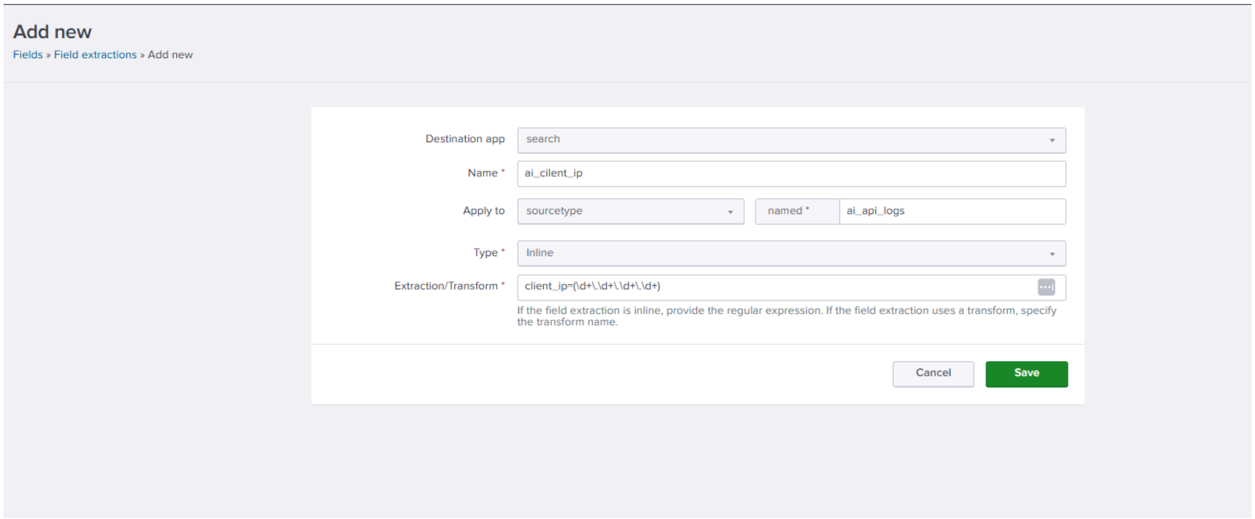


New Search

```
index=ai_security
| table _time path message
```

✓ 3 events (26/01/2026 17:00:00.000 to 27/01/2026 17:35:03.000) No Event Sampling ▾

_time	path	message
2026-01-27 16:59:05		
2026-01-27 16:58:48		
2026-01-27 17:00:06		

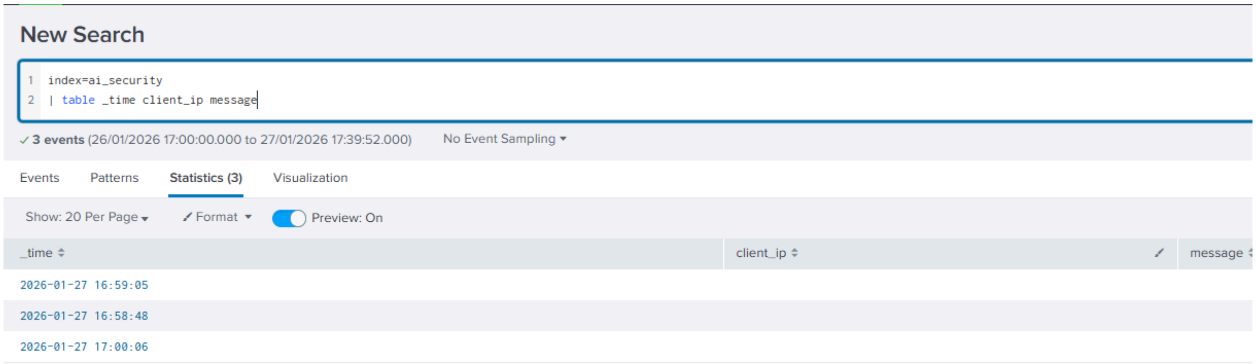


Add new

Fields » Field extractions » Add new

Destination app	search		
Name *	ai_cilent_ip		
Apply to	sourcetype	named *	ai_api_logs
Type *	Inline		
Extraction/Transform *	client_ip=(\d+\.\d+\.\d+\.\d+)		

If the field extraction is inline, provide the regular expression. If the field extraction uses a transform, specify the transform name.



New Search

```
index=ai_security
| table _time client_ip message
```

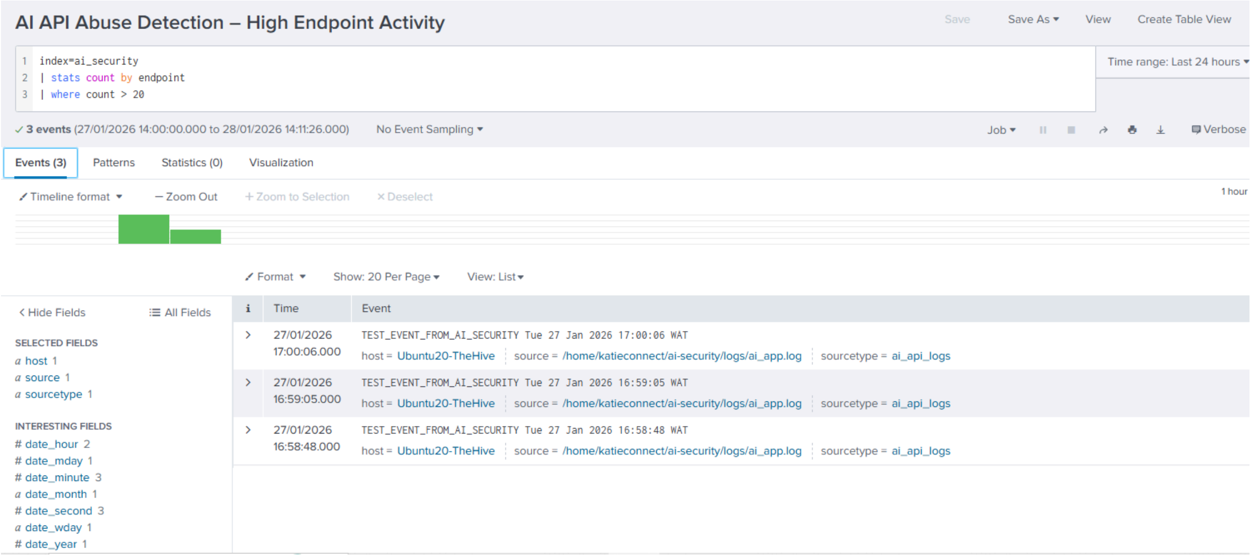
✓ 3 events (26/01/2026 17:00:00.000 to 27/01/2026 17:39:52.000)

_time	client_ip	message
2026-01-27 16:59:05		
2026-01-27 16:58:48		
2026-01-27 17:00:06		

Volume-Based Detection

Events were returned, confirming repeated access to specific endpoints during testing.

Key Insight:
This highlights how different detection strategies behave depending on data volume and activity patterns.



AI API Abuse Detection – High Endpoint Activity

```
index=ai_security
| stats count by endpoint
| where count > 20
```

Time range: Last 24 hours

✓ 3 events (27/01/2026 14:00:00.000 to 28/01/2026 14:11:26.000)

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 3
a date_month 1
# date_second 3
a date_wday 1
# date_year 1

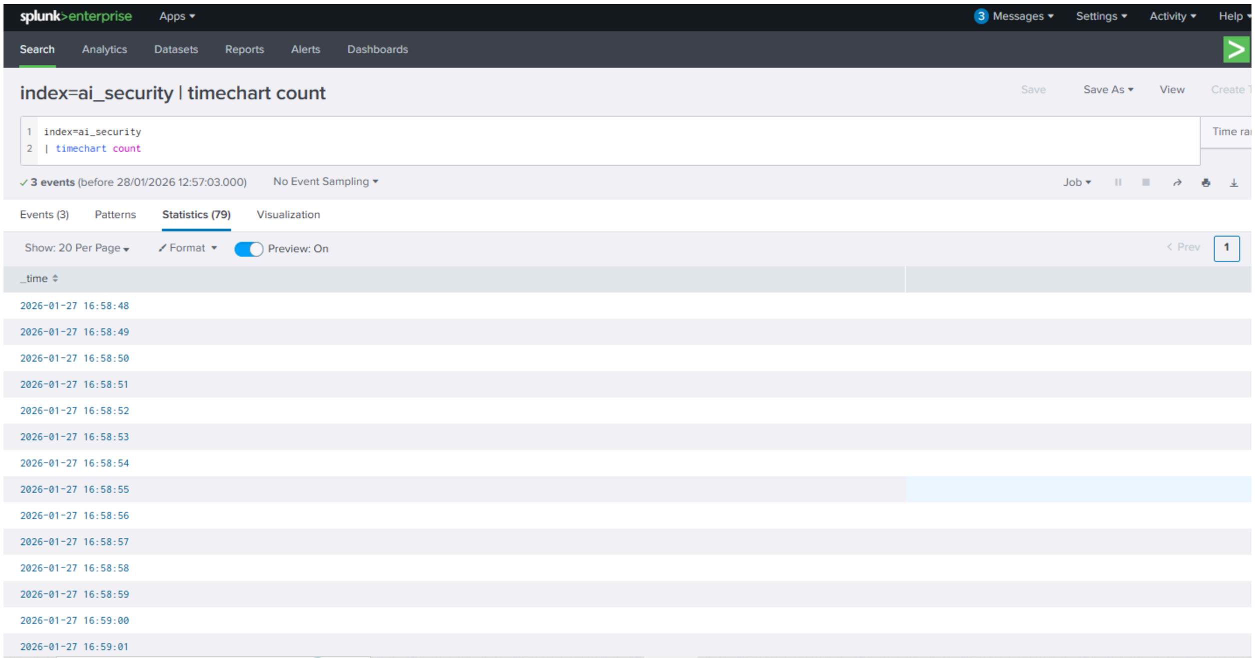
i	Time	Event
>	27/01/2026 17:00:06.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 WAT host = Ubuntu20-TheHive source = /home/katieconnect/ai-security/logs/ai_app.log sourcetype = ai_api_logs
>	27/01/2026 16:59:05.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 WAT host = Ubuntu20-TheHive source = /home/katieconnect/ai-security/logs/ai_app.log sourcetype = ai_api_logs
>	27/01/2026 16:58:48.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 WAT host = Ubuntu20-TheHive source = /home/katieconnect/ai-security/logs/ai_app.log sourcetype = ai_api_logs

Dashboards

An **AI API Security Monitoring Dashboard** was created to provide continuous visibility.

Dashboard Panels

- Total events over time
- Most accessed API endpoints
- Client IP activity

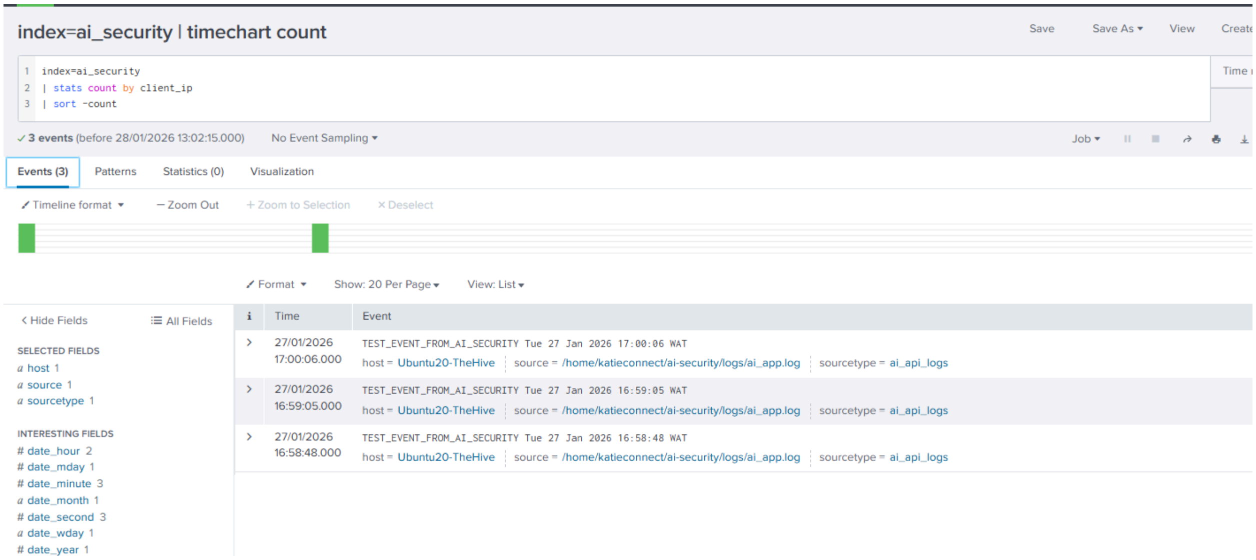


index=ai_security | timechart count

```
index=ai_security
| timechart count
```

✓ 3 events (before 28/01/2026 12:57:03.000)

_time ≑	
2026-01-27 16:58:48	
2026-01-27 16:58:49	
2026-01-27 16:58:50	
2026-01-27 16:58:51	
2026-01-27 16:58:52	
2026-01-27 16:58:53	
2026-01-27 16:58:54	
2026-01-27 16:58:55	
2026-01-27 16:58:56	
2026-01-27 16:58:57	
2026-01-27 16:58:58	
2026-01-27 16:58:59	
2026-01-27 16:59:00	
2026-01-27 16:59:01	



index=ai_security | timechart count

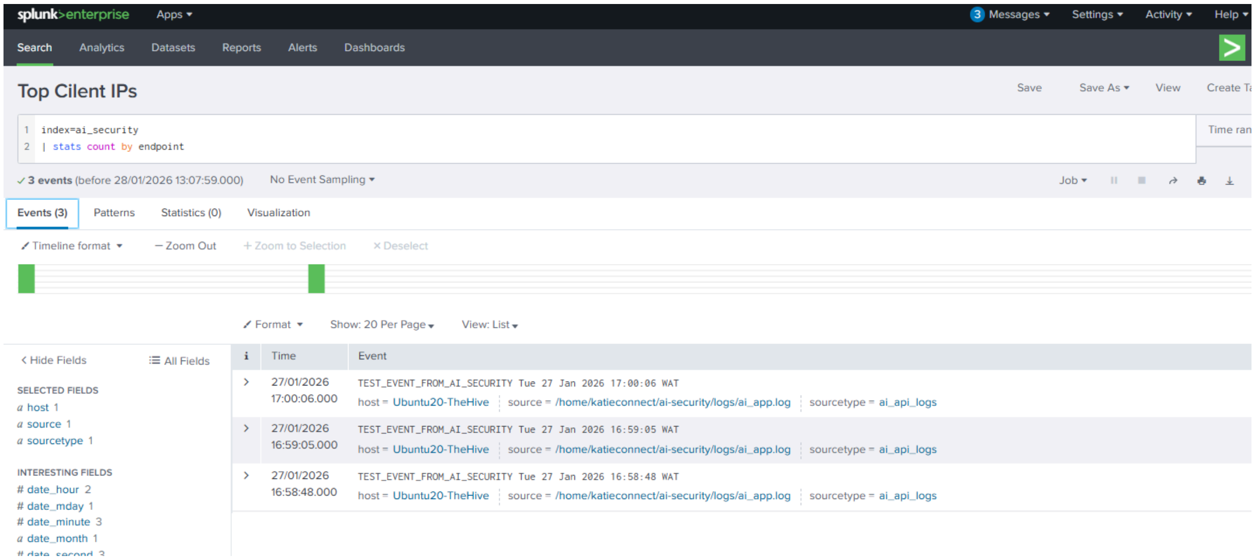
```
index=ai_security
| stats count by client_ip
| sort -count
```

✓ 3 events (before 28/01/2026 13:02:15.000) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 3
a date_month 1
# date_second 3
a date_wday 1
# date_year 1

i	Time	Event
›	27/01/2026 17:00:06.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs
›	27/01/2026 16:59:05.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs
›	27/01/2026 16:58:48.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs



Top Cilent IPs

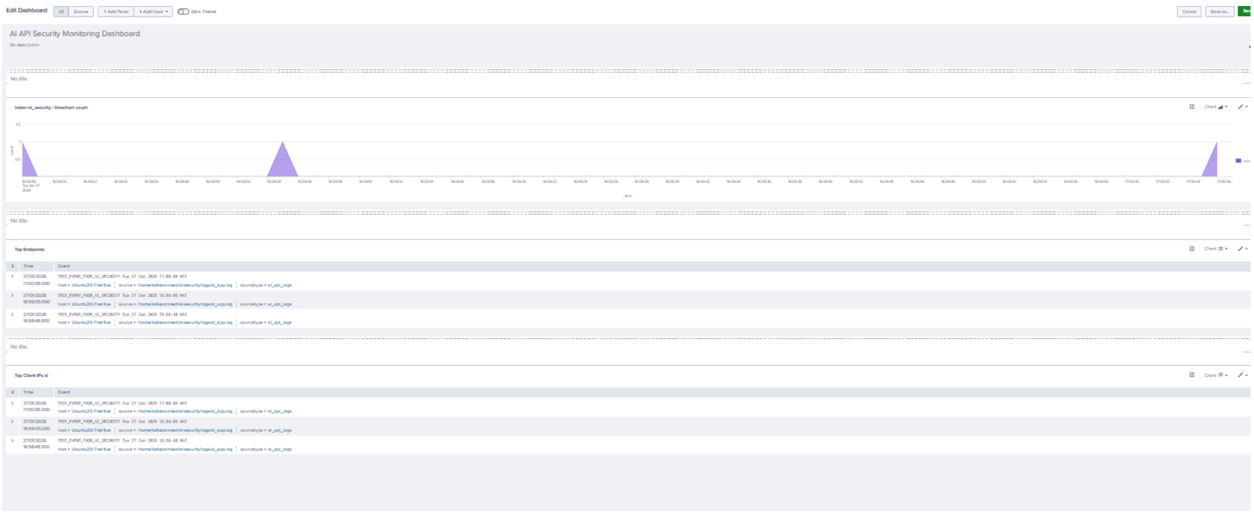
```
index=ai_security
| stats count by endpoint
```

✓ 3 events (before 28/01/2026 13:07:59.000) No Event Sampling ▾

SELECTED FIELDS
a host 1
a source 1
a sourcetype 1

INTERESTING FIELDS
# date_hour 2
# date_mday 1
# date_minute 3
a date_month 1
# date_second 3

i	Time	Event
›	27/01/2026 17:00:06.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs
›	27/01/2026 16:59:05.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs
›	27/01/2026 16:58:48.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 WAT host = Ubuntu20-TheHive · source = /home/katieconnect/ai-security/logs/ai_app.log · sourcetype = ai_api_logs



AI API Security Monitoring Dashboard

No description

No title

index=ai_security | timechart count

No title

Top Endpoints

i	Time	Event
>	27/01/2026 17:00:06.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs
>	27/01/2026 16:59:05.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs
>	27/01/2026 16:58:48.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs

No title

Top Client IPs ai

i	Time	Event
>	27/01/2026 17:00:06.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 17:00:06 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs
>	27/01/2026 16:59:05.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:59:05 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs
>	27/01/2026 16:58:48.000	TEST_EVENT_FROM_AI_SECURITY Tue 27 Jan 2026 16:58:48 MAT host = Ubuntu20-Thel-live ¦ source = /home/katleconnect/ai-security/logs/ai_app.log ¦ sourcetype = ai_api_logs

Alerting Limitations

Splunk Enterprise Free does not support scheduled alerts. As a result:

- Detection logic was saved as **Reports**
- Dashboards were used for continuous monitoring
- Alert behavior was documented conceptually

Conclusion

This project demonstrates how AI application logs can be transformed into actionable security telemetry using Splunk. It reflects real SOC activities including:

- Log ingestion troubleshooting
- Field extraction design
- Detection logic development
- Dashboard-driven monitoring
- Incident readiness planning

The project highlights the growing importance of **AI security observability** and provides a foundation for more advanced detection, alerting, and response workflows.