

Forum:[Hack Forums](#)

Thread: [Using AI to Analyze Suspicious Linux Logs](#)

FatCat - October 6, 2026, 7:42 pm

AI is becoming increasingly useful in cybersecurity, especially when dealing with large amounts of information.

One practical use is helping analysts understand and organize Linux logs during an investigation.

Here is a simple example of how I would approach it.

1. COLLECT THE LOGS

First, I would collect the relevant information from the system.

For SSH activity:

```
journalctl -u ssh --since "1 hour ago"
```

Or search for failed authentication:

```
journalctl -u ssh | grep -i "failed"
```

The goal is to collect the evidence before making assumptions.

2. SANITIZE THE DATA

Before sending logs to an external AI service, sensitive information should be removed or anonymized.

For example:

- Internal IP addresses
- Usernames
- Hostnames
- Email addresses
- Tokens
- Passwords
- API keys
- Other confidential information

This is important because logs can contain information that should not be shared outside the organization.

3. ASK AI TO EXPLAIN THE EVENTS

Instead of asking:

"Is this hacker?"

I would ask something more specific:

"Analyze these authentication events and identify unusual patterns. Group repeated failures by source IP and explain what additional evidence should be collected."

This gives the AI a defined task.

4. LOOK FOR PATTERNS

For example, imagine the logs contain:

Failed password for user admin from 10.0.0.50
Failed password for user root from 10.0.0.50
Failed password for user test from 10.0.0.50

An AI could help identify that multiple usernames are being targeted from the same source.

That could be consistent with brute-force activity.

However, this does NOT automatically prove that the system has been compromised.

5. VERIFY THE AI'S CONCLUSION

This is where human analysis becomes important.

If AI suggests that an IP address is suspicious, I would verify the finding using other evidence.

For example:

`sudo ss -tunap`

I could check whether the same system has active connections.

I could also investigate:

- Successful logins
- User accounts

- Running processes
- Listening ports
- File modifications
- DNS activity
- Other relevant logs

6. BUILD A TIMELINE

One of the most useful applications of AI is helping organize events chronologically.

For example:

20:10 — Multiple failed SSH attempts
20:14 — Successful authentication
20:16 — New outbound connection
20:18 — Suspicious process appears

A timeline can make relationships between events much easier to understand.

7. AI IS AN ASSISTANT, NOT THE INVESTIGATOR

There is an important difference between:

"AI says this is an attack."

and:

"Evidence shows repeated authentication failures, followed by a successful login and suspicious outbound activity."

The second statement is based on evidence.

AI can help analyze and organize that evidence, but the analyst still needs to verify the results.

FINAL THOUGHT

I think AI will become increasingly useful for SOC analysts because security environments generate huge amounts of data.

The important skill will not simply be knowing how to use AI.

It will be knowing:

- What data to provide

- What questions to ask
- How to protect sensitive information
- How to verify the response
- How to connect AI output with actual evidence

Used correctly, AI can reduce repetitive work while allowing the analyst to focus more on investigation and decision-making.

How would you use AI in a SOC environment: log analysis, alert triage, threat intelligence, scripting, or something else?