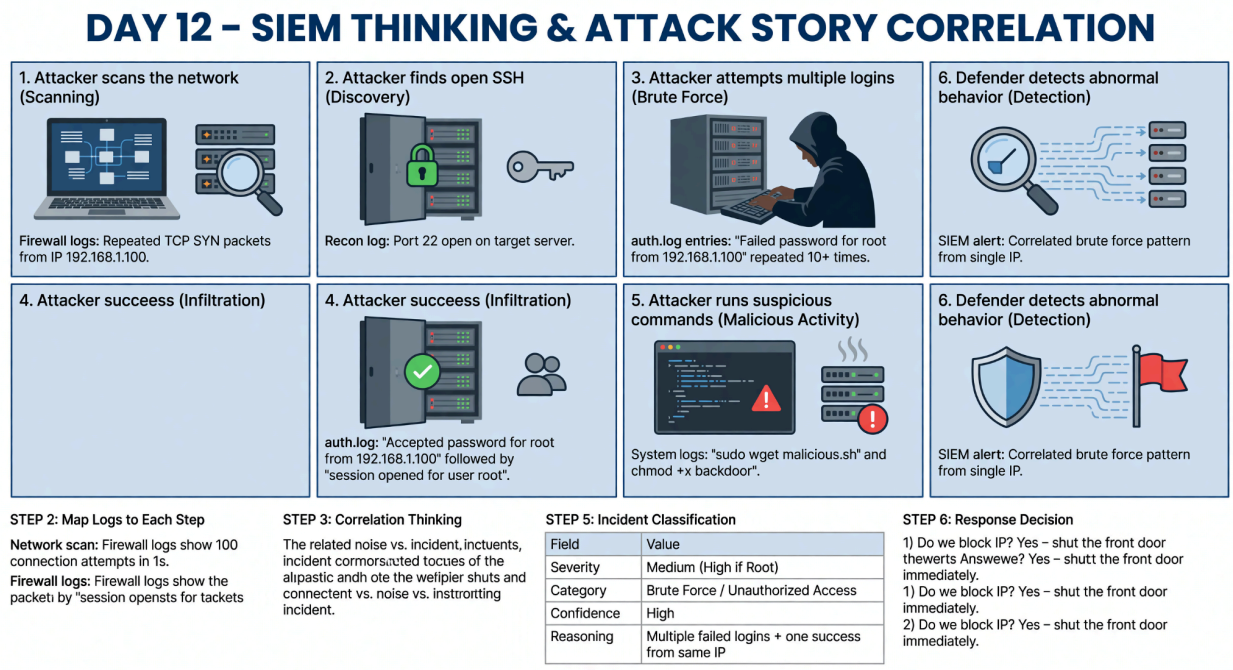


DAY 12 – SIEM THINKING & ATTACK STORY CORRELATION

This training session is about thinking like a security engineer. By the end, you'll be able to look at any incident and instantly pinpoint what happened, prove it, and execute the next steps.

STEP 1 ATTACK STORY CORRELATION :

1. Attacker scans the network (**Scanning**)
2. Attacker finds open SSH (**Discovery**)
3. Attacker attempts multiple logins (**Brute Force)**
4. Attacker succeeds (**Infiltration**)
5. Attacker runs suspicious commands (**Malicious Activity)**
6. Defender detects abnormal behavior (**Detection)**

Why
I am doing this to connect raw data into a story. Security isn't just about logs; it's about seeing the attacker's journey from the outside to the inside.

STEP 2: Map Logs to Each Step

What log would show this?

1. Network scan(Scout):
Firewall logs
IDS logs
Connection attempts from one IP:

why:
Because the Firewall is the Front Gate. It records every single knock.
If you see 100 knocks in 1 second, the firewall log proves it is a bot, not a person.

2. SSH brute force (Guessing):
   auth.log
    Multiple failed login entries

Why:
 This specific file records every time someone tries to log in.
 This log shows Failed password over and over, which is the proof of an attack.

3. Successful login (Entry):
   auth.log (Accepted password)
   New session started

Why:
The same camera that saw them fail now sees a line saying Accepted password. This is the most important log because it tells you exactly what time you were hacked.

STEP 3: Correlation Thinking:
One failed login is noise. (The user forgot their password).
Ten failed logins is suspicious. (A bot is trying to guess).
Ten failed + one success = INCIDENT. (The bot got in).

Why:

Computers are "noisy." Thousands of things happen every second. Correlation means connecting the dots to find the one thing that matters.

STEP 4: Manual Correlation Exercise (Hands-on, No Tools)

On your Ubuntu VM:

```
sudo cat /var/log/auth.log
```
Look for:

- failed password
- accepted password
- session opened

Now imagine:

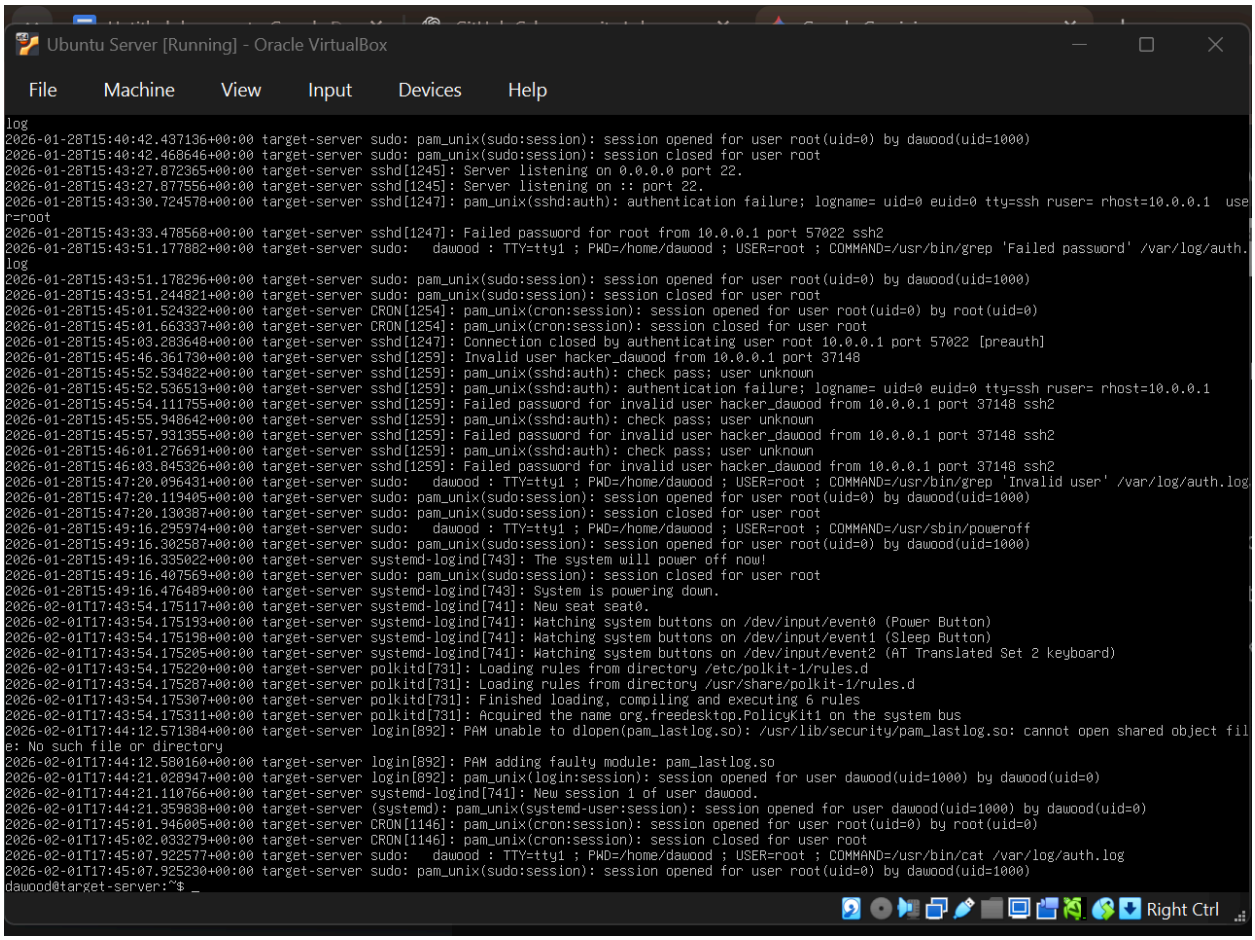
- Same IP

- Short time window

- Pattern
  You are now doing **manual SIEM analysis**.

  Why:
  Security isn't just about reading logs; it's about connecting them to tell a story. This logic is the core of professional Cloud SIEM tools like Splunk and Microsoft Sentinel.

  Proof:



-

STEP 5: Incident Classification

Write this table in your document:

Field	Value
Severity	**Medium** (High if it's a Root account)
Category	Brute Force / Unauthorized Access
Confidence	**High**
Reasoning	Multiple "Failed password" logs followed by "Accepted password" from the same IP.

Why:
Management doesn't have time to read thousands of logs. They need this 4-line summary to make quick decisions.You are translating Digital

Evidence into Business Risk.

STEP 6: Response Decision :

Answer these questions:

1)Do we block IP?
Yes, If a specific address is trying to break in, you shut the front door on them immediately. This stops the attack from getting worse right now.

2)Do we reset credentials?
Yes,Even if the attacker is kicked out, they still know the password. You must change the locks.This ensures the attacker cannot just log back in later from a different address.

3)Do we monitor further?
Yes,You need to check if the attacker left a "backdoor" or created a new user while they were inside.You watch the logs for the next 24–48 hours to make sure the system is truly clean.

4)Do we escalate?
Yes (to the IT/Legal team).

If data was stolen, the company might have to tell the government or the customers.In a big company, you never hide a hack,you report it so the whole team can help.