Alert Name : SSH Brute-force Attempt

Trigger : More than 10 failed SSH login attempts from the same external IP within 5 minutes.

Verification Steps : Check /var/log/auth.log for sshd entries, confirm failed password attempts, and verify whether the source IP is external or local.

Severity Logic : Create alert, document findings, and recommend mitigation steps without making system changes.

Escalation Criteria : Escalate to L2 if attempts continue, multiple users are targeted, or a successful SSH login is detected.