|  |  |
| --- | --- |
| Pattern (1) | 2019-06-30T01:19:23.155Z Jun 29 19:19:22 hp090 node sshd[22326]: Disconnected from invalid user mattl 182.254.225.230 port 58766 [preauth] |
|  | %{SYSLOGTIMESTAMP:timestamp} %{WORD:target} %{WORD:b} sshd\[%{INT:c}\]: Disconnected from invalid user %{WORD:user\_name} %{IP:ip} port %{INT:d} \[%{WORD:w}\] |
| Pattern (2) | 2019-06-30T01:19:25.265Z Jun 29 21:19:22 clnode008 vm1 sshd[78400]: input\_userauth\_request: invalid user seng [preauth] |
|  | %{SYSLOGTIMESTAMP:timestamp} %{WORD:target} %{WORD:b} sshd\[%{INT:c}\]: input\_userauth\_request: invalid user %{WORD:user\_name} \[%{WORD:w}\] |
| Pattern (3) | 2019-06-30T01:19:50.875Z Jun 29 19:19:50 ms0809 node sshd[14381]: Failed password for invalid user test from 178.128.96.131 port 59396 ssh2 |
|  | %{SYSLOGTIMESTAMP:timestamp} %{WORD:target} %{WORD:b} sshd\[%{INT:c}\]: Failed password for invalid user %{WORD:user\_name} from %{IP:ip} port %{INT:d} ssh2 |
| Pattern (4) | 2019-10-27T02:51:20.916Z Oct 26 20:51:20 hp184 localhost sshd[7719]: Accepted publickey for friedj from 128.110.155.28 port 36864 ssh2: ED25519 SHA256:qBKmRFs1HT/QpPR94cUcyV9lSUWEKbZo2bF+DBhAx5c |
|  | %{SYSLOGTIMESTAMP:timestamp} %{WORD:target} %{WORD:b} sshd\[%{INT:c}\]: Accepted publickey for %{WORD:user\_name} from %{IP:ip} port %{INT:d} %{GREEDYDATA:greedy} |