New Search

```
sourcetype="job sim"
| rex "user=(?<user>\w+)\s+\|\s+ip=(?<ip>[\d\.]+)\s+\|\s+action=(?<action>[^|]+)(?:\s+\|\s+threat=(?<threat
    >.+))?"
| eval action=trim(action), threat=trim(threat), ip=trim(ip)
| eval severity=case(
    action="malware detected" AND like(threat, "%Rootkit%"), "High",
    action="malware detected" AND like(threat, "%Ransomware%"), "High",
    action="malware detected" AND like(threat, "%Worm%"), "High",
    action="login failed", "Medium",
    action="file accessed" AND (ip LIKE "198.%" OR ip LIKE "203.%"), "Medium",
    1=1, "Low"
)
| stats count by severity, user,action, ip
```

All time

✓ **50 events** (before 7/9/25 10:12:12.000 AM) No Event Sampling

Statistics (43)

severity	user	action	ip	count
Low	david	connection attempt	10.0.0.5	2
Low	david	connection attempt	172.16.0.3	2
Low	david	connection attempt	203.0.113.77	1
Low	david	file accessed	10.0.0.5	1
Low	david	login success	203.0.113.77	2
Low	david	malware detected	172.16.0.3	1
Low	eve	file accessed	172.16.0.3	1
Low	eve	login success	172.16.0.3	1
Low	eve	login success	203.0.113.77	1
Low	eve	malware detected	192.168.1.101	1
Low	eve	malware detected	203.0.113.77	1
Medium	alice	file accessed	203.0.113.77	1
Medium	alice	login failed	203.0.113.77	1
Medium	bob	file accessed	198.51.100.42	2
Medium	bob	file accessed	203.0.113.77	1
Medium	bob	login failed	10.0.0.5	1
Medium	bob	login failed	172.16.0.3	1

severity	user	action	ip	count
Medium	charlie	file accessed	203.0.113.77	1

severity	user	action	ip	count
Medium	charlie	file accessed	203.0.113.77	1
Medium	charlie	login failed	198.51.100.42	1
Medium	david	file accessed	198.51.100.42	1

New Search

```
sourcetype="job sim"
| rex "user=(?<user>\w+)\s+\|\s+ip=(?<ip>[\d\.]+)\s+\|\s+action=(?<action>[^|]+)(?:\s+\|\s+threat=(?<threat
    >.+))?"
| eval action=trim(action), threat=trim(threat), ip=trim(ip)
| eval severity=case(
    action="malware detected" AND like(threat, "%Rootkit%"), "High",
    action="malware detected" AND like(threat, "%Ransomware%"), "High",
    action="malware detected" AND like(threat, "%Worm%"), "High",
    action="login failed", "Medium",
    action="file accessed" AND (ip LIKE "198.%" OR ip LIKE "203.%"), "Medium",
    1=1, "Low"
)
| stats count by severity, user,action, ip
```

All time

✓ **50 events** (before 7/9/25 10:12:12.000 AM) No Event Sampling

Statistics (43)

severity	user	action	ip	count
Medium	david	file accessed	203.0.113.77	1
Medium	david	login failed	203.0.113.77	1
Medium	eve	file accessed	203.0.113.77	1

New Search

```
sourcetype="job sim"
| rex "user=(?<user>\w+)\s+\|\s+ip=(?<ip>[\d\.]+)\s+\|\s+action=(?<action>[^|]+)(?:\s+\|\s+threat=(?<threat
    >.+))?"
| eval action=trim(action), threat=trim(threat), ip=trim(ip)
| eval severity=case(
    action="malware detected" AND like(threat, "%Rootkit%"), "High",
    action="malware detected" AND like(threat, "%Ransomware%"), "High",
    action="malware detected" AND like(threat, "%Worm%"), "High",
    action="login failed", "Medium",
    action="file accessed" AND (ip LIKE "198.%" OR ip LIKE "203.%"), "Medium",
    1=1, "Low"
)
| stats count by severity, user,action, ip
```

All time

✓ **50 events** (before 7/9/25 10:12:12.000 AM) No Event Sampling

Statistics (43)

severity	user	action	ip	count
High	alice	malware detected	198.51.100.42	1
High	bob	malware detected	172.16.0.3	1
High	bob	malware detected	203.0.113.77	1
High	eve	malware detected	10.0.0.5	1
Low	alice	login success	198.51.100.42	2
Low	alice	login success	203.0.113.77	1
Low	alice	malware detected	172.16.0.3	1
Low	alice	malware detected	192.168.1.101	1
Low	bob	connection attempt	192.168.1.101	1
Low	bob	connection attempt	203.0.113.77	1
Low	bob	file accessed	172.16.0.3	1
Low	bob	login success	10.0.0.5	1
Low	bob	login success	192.168.1.101	1
Low	bob	login success	198.51.100.42	1
Low	bob	malware detected	10.0.0.5	1
Low	charlie	connection attempt	10.0.0.5	1
Low	charlie	connection attempt	172.16.0.3	1

severity	user	action	ip	count
Low	charlie	connection attempt	192.168.1.101	3
Low	charlie	login success	172.16.0.3	1
Low	charlie	malware detected	172.16.0.3	1