

Nov 15 22:11

Haxcamp - Cybersecurity | Splunk Enterprise | Splunk | Search | Splunk 10.0.2

http://localhost:8000/en-US/app/search/search?q=search%20index%3Dssh_logs%20event_type%3D"Mu

New Search

Save As Alert

Settings

Title: brute force

Description: Optional

Permissions: Private Shared in App

Alert type: Scheduled Real-time

Expires: 24 hour(s)

Trigger Conditions

Trigger alert when: Per-Result

Throttle:

Trigger Actions

Cancel Save

303 events (before 11/15/25)

Events Patterns Statistics

Show: 20 Per Page

id.orig_h

- 10.0.0.28
- 10.0.0.11
- 10.0.0.21
- 10.0.0.22
- 10.0.0.24
- 10.0.0.33
- 10.0.0.35
- 10.0.0.39
- 10.0.0.48
- 10.0.0.53
- 10.0.0.56
- 10.0.0.11
- 10.0.0.11

count

- 5
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 3
- 2
- 2

Smart Mode

6 7 8 ... Next >