Summary

Most important information

Level 2: Weighted Severities by Unique IP: Σ(k_s*a_s)

Average

- Metric: Weighted Severities by Unique IP
- Max for 24 hours
- Min for 24 hours
- q:severity:1 > cardinality(geoip.ip)

(y-axis: 1500, 1000, 500, 0; x-axis: 16:00, 18:00, 20:00, 22:00, 00:00, 02:00, 04:00, 06:00, 08:00, 10:00, 12:00, 14:00)

Level 3: Risk

- Risk [bytes], logarithmic scale

(y-axis: 1.0, 0.5, 0.0, -0.5, -1.0; x-axis: 16:00, 20:00, 00:00, 04:00, 08:00, 12:00)
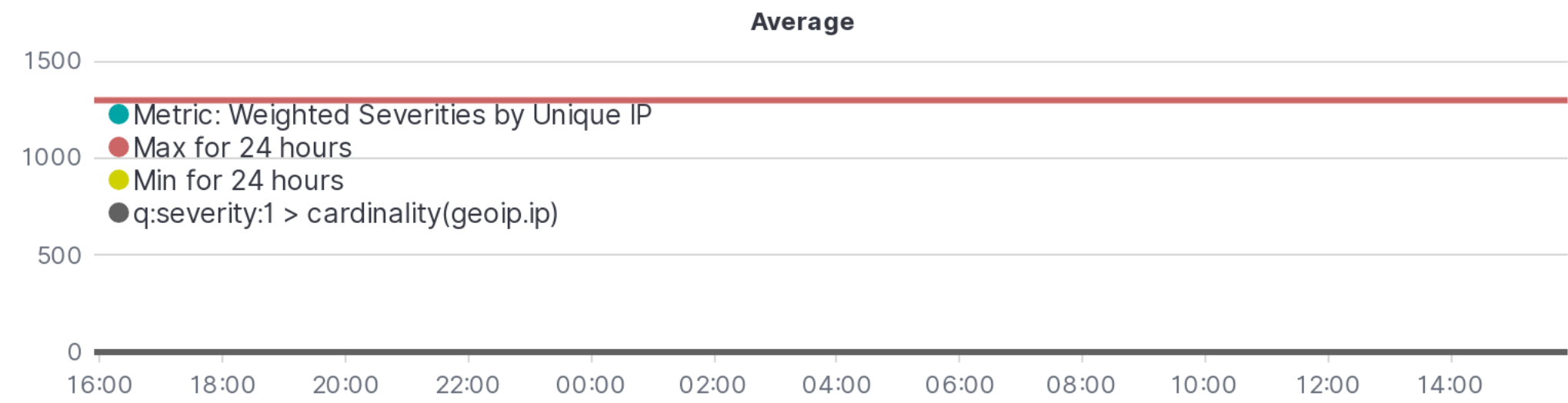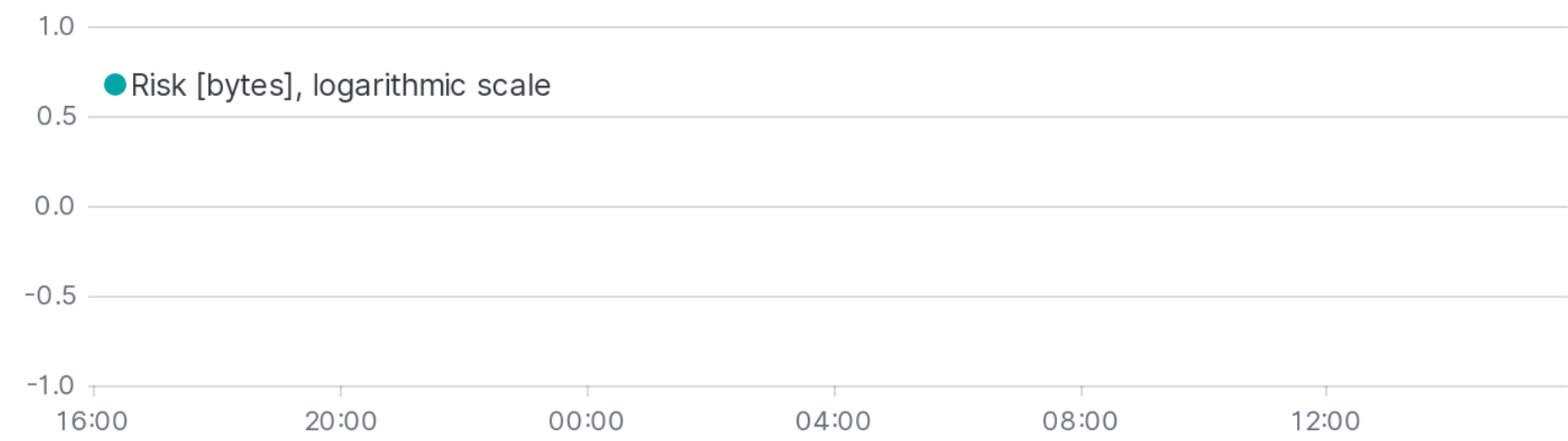
Top attacking IP addresses table

No results found

Total Count of Routers

0

Total Count of Routers

Total Count of Routers over Time

No results found

Request Packets by Destination Port

No results found

Total Alerts by Category

No results found

Flows over Time

No results found

Flow Counts by Strategy

No data to display for the selected metrics

elastic