cyber & data

"From bits to information"

Splunk: Visualisation and Charting

Outline

- Stats.
- Timeline.
- Chart

Buttercup Games

GET

/oldlink
/category.screen
/cart.do
/product.screen
/show.do
/productscreen.html
/anne_nicole.html
/signals.zip
/numa.html

GET → categoryID={STRATEGY, ARCADE, TEE, ACCESSORIES, SIMULATION, SHOOTER, SPORTS}

POST → action={addtocart, purchase, view, remove, changequantity} categoryID, productID

GET → productID={WC-SH-G04, SC-MG-G10 , DB-SG-G01, MB-AG-T01, DC-SG-G02, MB-AG-G07, FS-SG-G03, WC-SH-A02, WC-SH-A01, WC-SH-T02 , PZ-SG-G05 , FI-AG-G08, BS-AG-G09 , CU-PG-G06, SF-BVS-G01}

- **SHOOTER:** WC-SH-G04
- **STRATEGY:** DB-SG-G01, DC-SG-G02, FS-SG-G03 and PZ-SG-G05
- **TEE:** MB-AG-T01 and WC-SH-T02.
- **ARCADE:** MB-AG-G07, FI-AG-G08, and BS-AG-G09.
- **SPORTS:** CU-PG-G06.
- **SIMULATION:** SC-MG-G10.
- **ACCESSORIES:** WC-SH-A01 and AC-SH-A02.

Get

Splunk to Visualisation

```
post status=200 action=purchase
| top categoryId
```

✓ 5,224 events (before 06/09/2020 19:03:57.000) No Event Sampling ▾ Job ▾

Events Patterns **Statistics (7)** Visualization

20 Per Page ▾ Format Preview ▾

categoryId	count
STRATEGY	806
ARCADE	493
TEE	367
ACCESSORIES	348
SIMULATION	246
SHOOTER	245
SPORTS	138

Get

&cyber data

Aggregation Methods

Aggregation functions
avg(X)
count(X)
dc(X)
estdc(X)
estdc_error(X)
max(X)
mean(X)
median(X)
min(X)
mode(X)
percentile<X>(Y)
range(X)
stdev(X)
stdevp(X)
sum(X)
sumsq(X)
var(X)
varp(X)

Event order functions
first(X)
last(X)

Multivalue stats and chart functions
list(X)
values(X)

Time functions
earliest_time(X)
latest(X)
latest_time(X)
per_day(X)
per_hour(X)
per_minute(X)
per_second(X)
rate(X)
rate_avg(X)
rate_sum(X)

cyber & data

"From bits to information"

Splunk: Stats

Splunk Stats

```
sourcetype=access_*
| stats dc(status),dc(productId),dc(categoryId)
```

All time

✓ 39,532 events (before 06/09/2020 19:32:01.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

dc(status)	dc(productId)	dc(categoryId)
9	16	8

Get

Splunk Stats

```
sourcetype=access_*
| stats dc(status) as Status,dc(productId) as "Product ID",dc(categoryId) as "Category ID"
```

All time

✓ 39,532 events (before 06/09/2020 19:34:22.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

Status	Product ID	Category ID
9	16	8

Get

Splunk Stats

```
sourcetype=access_* action=purchase
| stats dc(clientip) BY categoryId
```

All time

✓ 5,737 events (before 06/09/2020 19:37:09.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (8)** Visualization

20 Per Page Format Preview

categoryId	dc(clientip)
ACCESSORIES	160
ARCADE	173
NULL	58
SHOOTER	133
SIMULATION	136
SPORTS	97
STRATEGY	181
TEE	156

Get

Splunk Stats

```
sourcetype=access_*
| stats count(eval(status="404")) AS count_status BY sourcetype
```

All time

✓ 39,532 events (before 06/09/2020 19:21:53.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

sourcetype	count_status
access_combined_wcookie	690

Get

&cyber data

cyber & data

"From bits to information"

Splunk: Timeline

Splunk Timeline

```
sourcetype=access_*
| timechart count(eval(action="purchase")) BY productName
```

All time

✓ 39,532 events (before 06/09/2020 19:26:08.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (8)** Visualization

20 Per Page Format Preview

_time	NULL
2014-04-19	157
2014-04-20	783
2014-04-21	903
2014-04-22	829
2014-04-23	781
2014-04-24	793
2014-04-25	797
2014-04-26	694

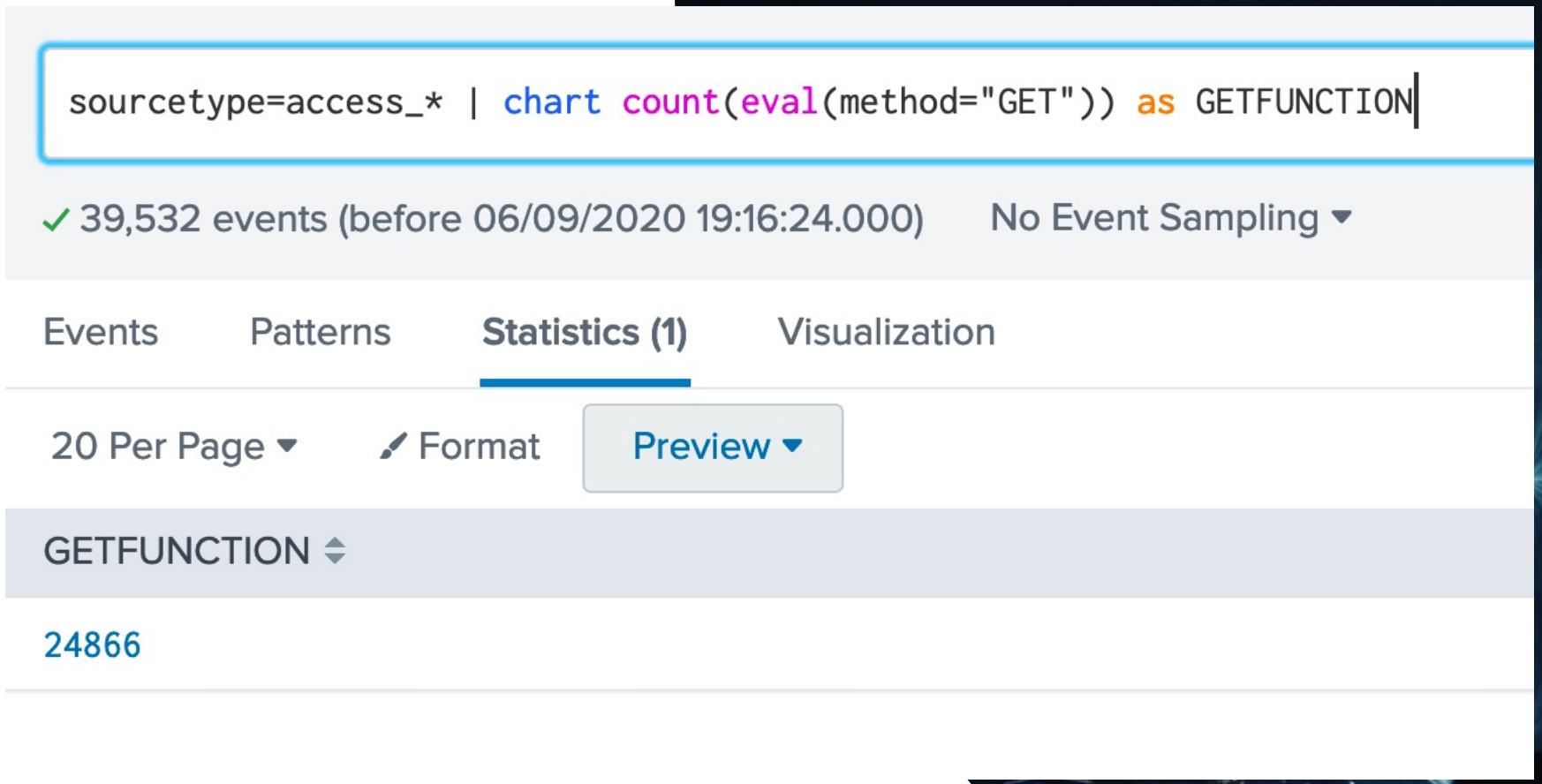
Get

cyber & data

"From bits to information"

Splunk: Charting

Splunk Charting



Get

Splunk Charting

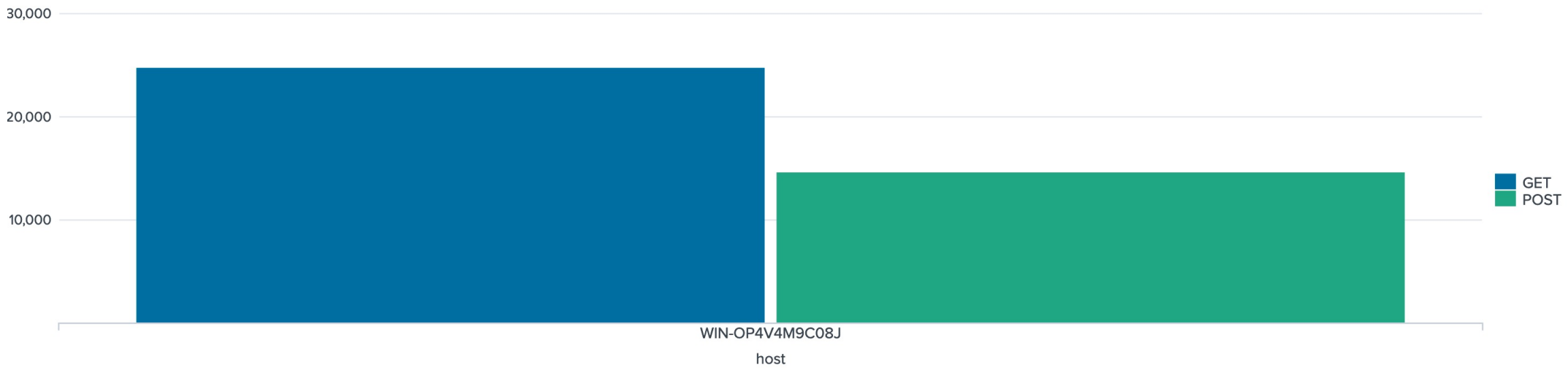
```
sourcetype=access_*
| chart count(eval(method="GET")) AS GET, count(eval(method="POST")) AS POST by host
```

All time

✓ 39,532 events (before 06/09/2020 18:46:21.000) No Event Sampling Job Smart Mode

Events Patterns Statistics (1) Visualization

Column Chart Format Trellis



Get

Splunk Charting: searchmatch()

```
sourcetype=access_*
| chart  count(eval(searchmatch("Safari")))  AS Safari, count(eval(searchmatch("Chrome")))  AS Chrome, count(eval
    (searchmatch("Mozilla"))) AS Mozilla by host
```

All time

✓ 39,532 events (before 06/09/2020 21:02:21.000) No Event Sampling Job Smart Mode

Events Patterns **Statistics (1)** Visualization

20 Per Page Format Preview

host	Safari	Chrome	Mozilla
WIN-OP4V4M9C08J	14786	9651	37346

Get

cyber & data

"From bits to information"

Splunk: Visualisation and Charting