

“From bits to information”

Introduction to Splunk

Outline

- Why use Splunk?
- Application of Splunk.



cyber
& data

Why? PCI

Build and Maintain and Secure Network
Firewall. System passwords.

Protect Cardholder Data
Stored cardholder data. Encrypt data.

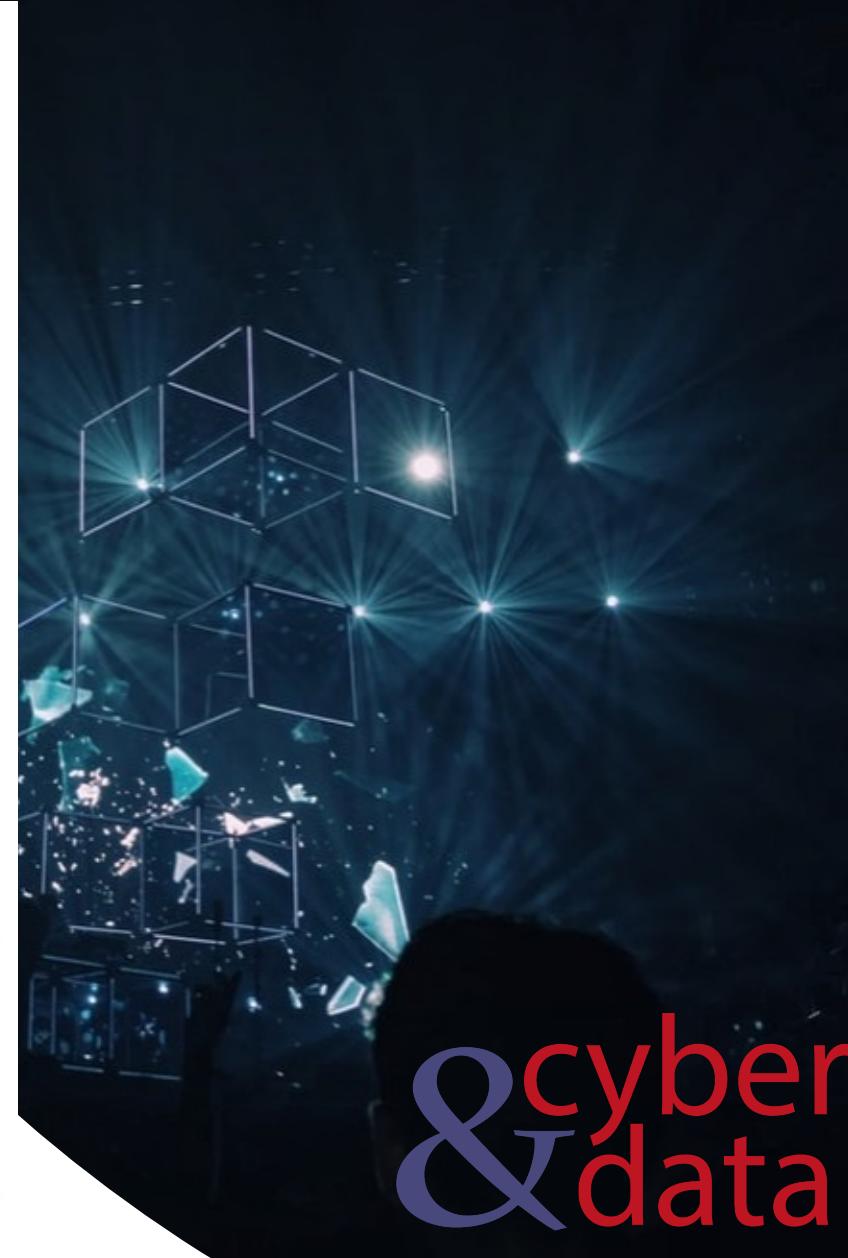
Monitor and Test Networks
Track/monitor accesses. Perform security tests.



Maintain Vulnerability Management Program
Anti-virus. Develop/maintain secure systems and apps.

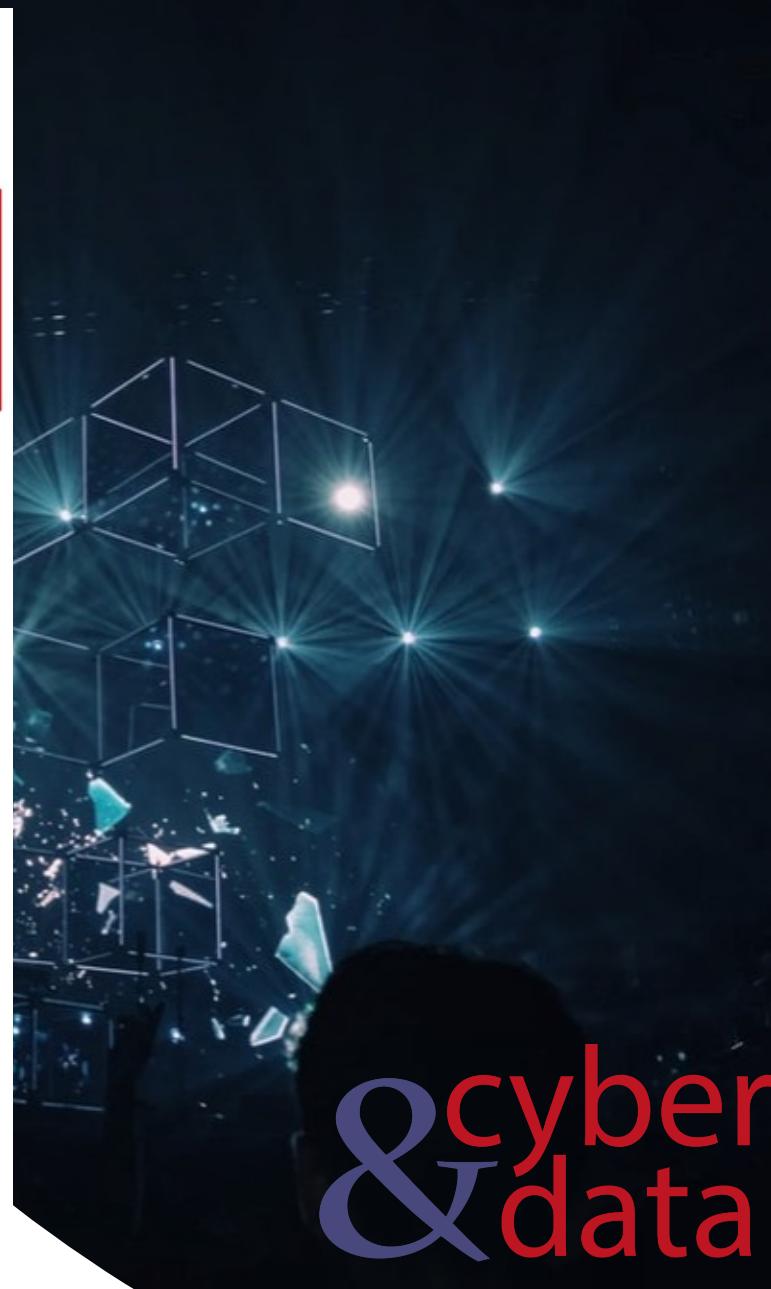
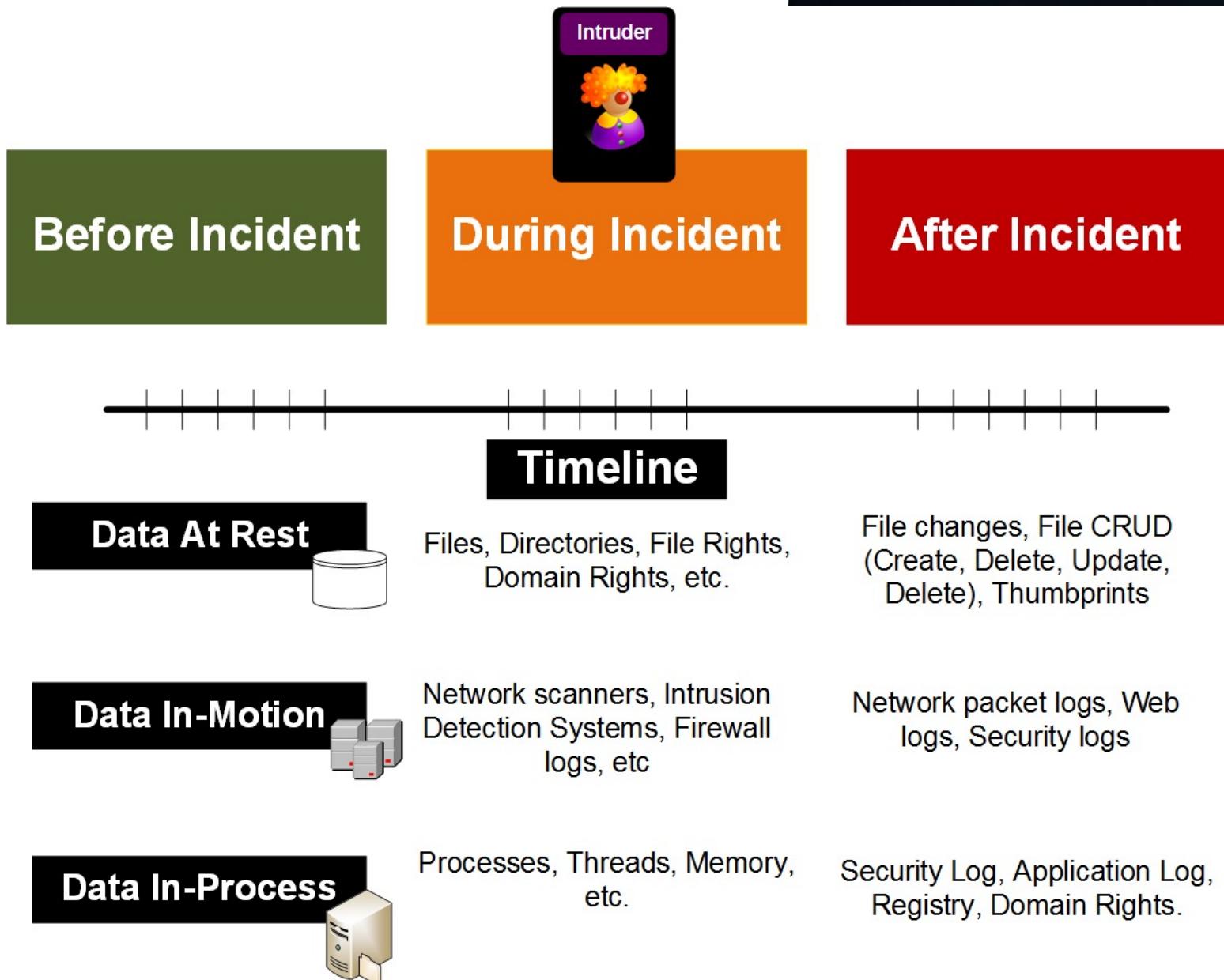


Strong Access Control
Restrict access to cardholder data. Assign unique ID for each user who accesses. Restrict physical access.



cyber
& data

Before, During and After



Logs

Local host logs
- Application.
- Security.
- System
- etc

File and Directories
- CRUD.
- Security changes.

Performance
- CPU.
- Memory.
- Threads.

Database Access
- Logs.

TCP/UDP
- Syslog.



Environmental
- Temp.
- Humidity.

Active Directory
- User additions.
- Host changes.
- Logins

Remote Access
- Logs.

Registry Monitoring
- Key changes.
- Updates.

Print Monitoring
- Jobs.

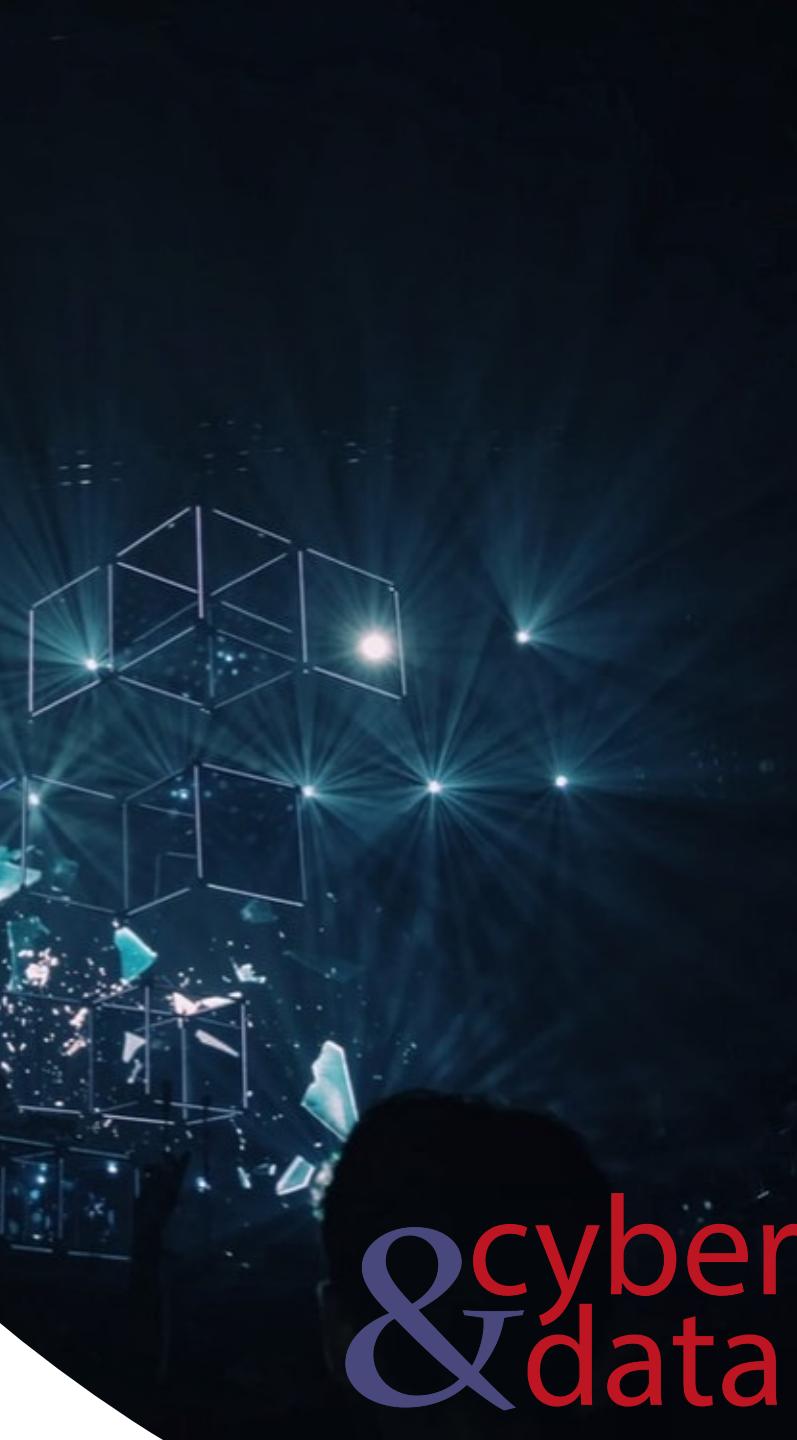
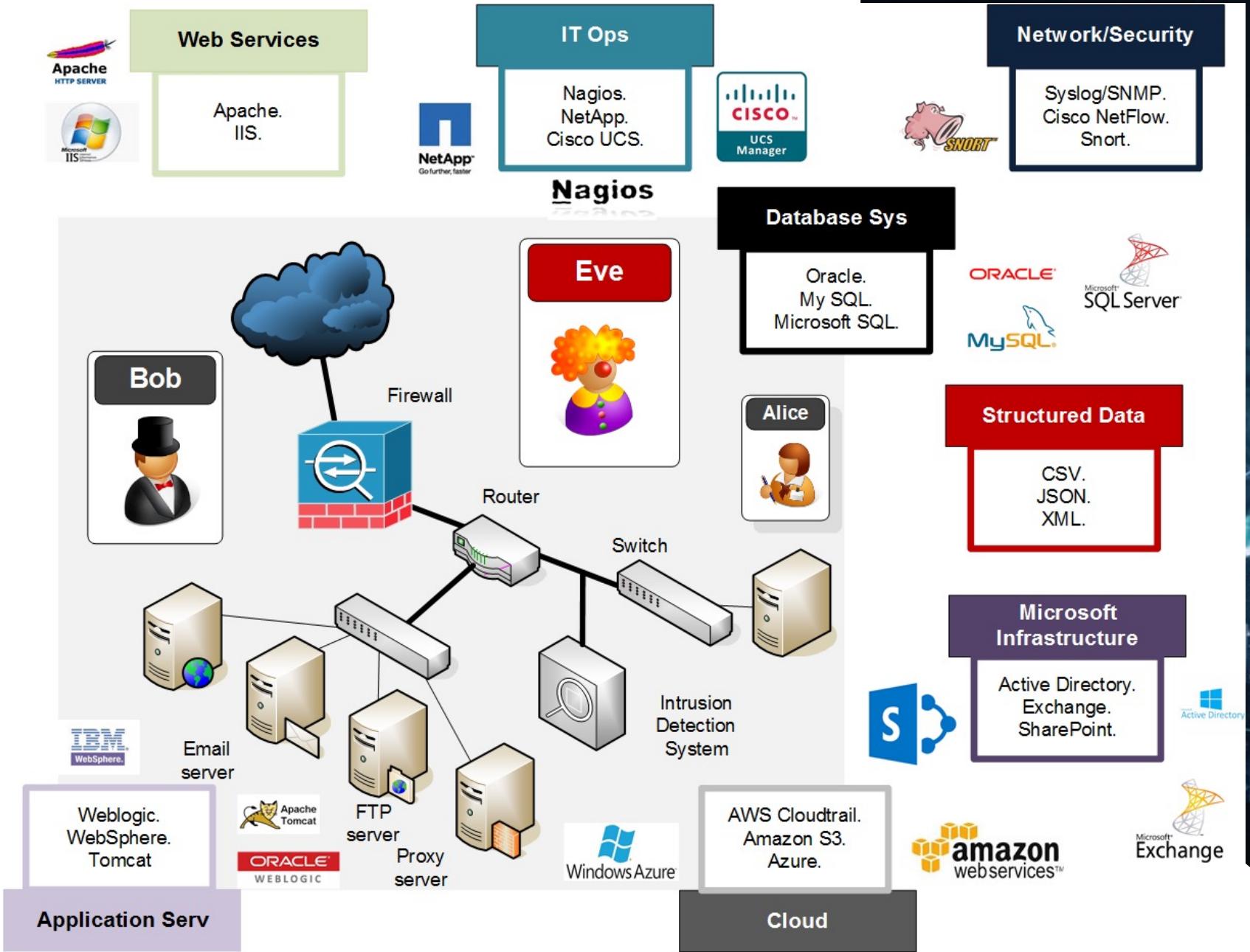
Intrusion Detection
- Alerts

Email
- Logs.



cyber
&
data

And the complexity ...



cyber
&
data



“From bits to information”

Get

Introduction to Splunk

Buttercup Games



Get

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, categoryID, productID
remove,
changequantity}

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.

New Search

get

24,866 events (before 6/24/20 2:46:06.000 PM) No Event Sampling ▾

Save As ▾ Close

All time ▾

Events (82) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

Apr 19, 2014 6:00 PM Apr 19, 2014 7:00 PM

List ▾ Format 20 Per Page ▾ 1 2 3 4 5 Next >

Time	Event
4/19/14 6:59:59.000 PM	60.18.93.11 - - [19/Apr/2014:18:59:59] "GET /oldlink?itemId=EST-12&JSESSIONID=SD4SL5FF3ADFF5111 HTTP 1.1" 200 1786 "http://www.buttercupgames.com/oldlink?itemId=EST-12" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 788 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/19/14 6:59:57.000 PM	60.18.93.11 - - [19/Apr/2014:18:59:57] "GET /cart.do?action=changequantity&itemId=EST-12&productId=CU-PG-G06&JSESSIONID=D4SL5FF3ADFF5111 HTTP 1.1" 200 849 "http://www.buttercupgames.com/category.screen?categoryId=SPORTS" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 314 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/19/14 6:59:56.000 PM	60.18.93.11 - - [19/Apr/2014:18:59:56] "GET /category.screen?categoryId=NULL&JSESSIONID=SD4SL5FF3ADFF5111 HTTP 1.1" 400 2120 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-14" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 245 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/19/14 6:59:55.000 PM	60.18.93.11 - - [19/Apr/2014:18:59:55] "GET /oldlink?itemId=EST-16&JSESSIONID=SD4SL5FF3ADFF5111 HTTP 1.1" 200 200 "http://www.buttercupgames.com/product.screen?productId=DC-SG-G02" "Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3" 914 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/19/14 6:57:52.000 PM	91.205.40.22 - - [19/Apr/2014:18:57:52] "GET /product.screen?productId=CU-PG-G06&JSESSIONID=SD10SL10FF5ADFF5106 HTTP 1.1" 200 1711 "http://www.buttercupgames.com/category.screen?categoryId=SPORTS" "Opera/9.20 (Windows NT 6.0; U; en)" 723 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
a action 5
bytes 82
a categoryId 7
a clientip 18
date_hour 1
date_mday 1
date_minute 19
a date_month 1
date_second 47
a date_wday 1
date_year 1
a date_zone 1
a file 4
a ident 1
a index 1
a itemId 14

Get

Splunk

List ▾ Format 20 Per Page ▾

◀ Prev 1 2 3 4 5 6 7 8 ... Next ▾

Time	Event		
4/26/14 6:22:16.000 PM	91.205.189.15 - [26/Apr/2014:18:22:16] "GET /oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113 HTTP/1.1" 200 1665 "http://www.buttercupgames.com/oldlink?itemId=EST-14" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 159		
Event Actions ▾			
Type	Field	Value	Actions
Selected	host	s18359064	▼
	source	buttercup.zip:\buttercup\www2\access.log	▼
	sourcetype	access_combined_wcookie	▼
Event	JSESSIONID	SD6SL7FF7ADFF53113	▼
	bytes	1665	▼
	clientip	91.205.189.15	▼
	file	oldlink	▼
	ident	-	▼
	itemid	EST-14	▼
	method	GET	▼
	other	159	▼
	referer	http://www.buttercupgames.com/oldlink?itemId=EST-14	▼
	referer_domain	http://www.buttercupgames.com	▼
	req_time	26/Apr/2014:18:22:16	▼
	status	200	▼
	uri	/oldlink?itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113	▼
	uri_path	/oldlink	▼
	uri_query	itemId=EST-14&JSESSIONID=SD6SL7FF7ADFF53113	▼
	user	-	▼
	useragent	Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	▼
	version	1.1	▼
Time +	_time	2014-04-26T18:22:16.000+00:00	
Default	index	main	▼
	linecount	1	▼
	punct	..._-_[:::_]_/_?=&=__."__"://.?=-"_.(_	▼

Splunk

New Search

get status=404

✓ 553 events (before 6/24/20 2:54:05.000 PM) No Event Sampling ▾

Save As ▾ Close All time ▾

Events (553) Patterns Statistics Visualization

Format Timeline ▾ - Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ Format 20 Per Page ▾ < Prev 1 2 3 4 5 6 7 8 ... Next >

Time	Event
4/26/14 6:18:59.000 PM	> 198.35.1.75 - - [26/Apr/2014:18:18:59] "GET /productscreen.html?t=ou812&JSESSIONID=SD10SL2FF4ADFF53099 HTTP 1.1" 404 240 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 850 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/26/14 6:10:07.000 PM	> 216.221.226.11 - - [26/Apr/2014:18:10:07] "GET /search.do?items=2112&JSESSIONID=SD4SL4FF4ADFF53057 HTTP 1.1" 404 1967 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)" 825 host = s18359064 source = buttercup.zip:\buttercup\www3\access.log sourcetype = access_combined_wcookie
4/26/14 5:48:46.000 PM	> 71.192.86.205 - - [26/Apr/2014:17:48:46] "GET /rush/signals.zip?JSESSIONID=SD8SL2FF7ADFF52982 HTTP 1.1" 404 1281 "http://www.buttercupgames.com/protocol.screen?productId=SF-BVS-G01" "Mozilla/5.0 (compatible; Googlebot/2.1; +http://www.google.com/bot.html)" 885 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
4/26/14 5:42:06.000 PM	> 125.89.78.6 - - [26/Apr/2014:17:42:06] "GET /rush/signals.zip?JSESSIONID=SD10SL8FF3ADFF52952 HTTP 1.1" 404 1252 "http://www.buttercupgames.com/cart.do?action=purchase&itemId=EST-7" "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 594 host = s18359064 source = buttercup.zip:\buttercup\www2\access.log sourcetype = access_combined_wcookie
4/26/14 5:19:39.000 PM	> 198.35.1.75 - - [26/Apr/2014:17:19:39] "GET /product.screen?productId=SF-BVS-G01&JSESSIONID=SD5SL1FF5ADFF52835 HTTP 1.1" 404 411 "http://www.buttercupgames.com/category.screen?categoryId=NULL" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 165 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
a action 5
bytes 100+
a categoryId 1
a clientip 100+
date_hour 24
date_mday 8
date_minute 60
a date_month 1
date_second 60
a date_wday 7
date_year 1
a date_zone 1
a file 9
a ident 1
a index 1

Get

er data

New Search

get status=404 clientip="87.194.216.51"

✓ 18 events (before 24/06/2020 16:04:22.000) No Event Sampling ▾

Events (18) Patterns Statistics Visualization

Format Timeline ▾ — Zoom Out + Zoom to Selection × Deselect 1 hour per column

List ▾ ✎ Format 20 Per Page ▾

Time	Event
25/04/2014 18:21:45.000	87.194.216.51 - - [25/Apr/2014:18:21:45] "GET /search.do?items=2112&JSESSIONID=SD2SL1FF10ADFF46115 HT TP 1.1" 404 1585 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-16" "Mozilla/5.0 (Wind ows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)" 920 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
25/04/2014 17:52:09.000	87.194.216.51 - - [25/Apr/2014:17:52:09] "GET /productscreen.html?t=ou812&JSESSIONID=SD2SL3FF1ADFF460 10 HTTP 1.1" 404 2391 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Opera/9.20 (Windows NT 6.0; U; en)" 575 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie

< Hide Fields All Fields

SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
a clientip 1
a index 1
linecount 1
a splunk_server 1
status 1

Get

Splunk

New Search

Save As ▾ Close

New Search

passwords.pdf All time

✓ 68 events (before 24/06/2020 16:06:13.000) No Event Sampling ▾ Job ▾ 1 hour per column

Events (68) Patterns Statistics Visualization

Format Timeline ▾

List ▾ 20 Per Page ▾ 1 2 3 4 Next >

< Hide Fields

SELECTED FIELDS
a host 1
a source 3
a sourcetype 1

INTERESTING FIELDS
a index 1
linecount 1
a splunk_server 1

+ Extract New Fields

	i Time	Event
>	26/04/2014 14:54:08.000	175.44.1.172 - - [26/Apr/2014:14:54:08] "POST /passwords.pdf?JSESSIONID=SD10SL2FF3ADFF51999 HTTP 1.1" 404 2388 "http://www.buttercupgames.com/oldlink?itemId=EST-6" "Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)" 102 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie
>	26/04/2014 12:38:50.000	198.35.1.10 - - [26/Apr/2014:12:38:50] "POST /passwords.pdf?JSESSIONID=SD9SL3FF3ADFF51356 HTTP 1.1" 404 446 "http://www.buttercupgames.com/product.screen?productId=SF-BVS-G01" "Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)" 542 host = s18359064 source = buttercup.zip:\buttercup\www2\access.log sourcetype = access_combined_wcookie
>	26/04/2014 12:07:15.000	59.36.99.70 - - [26/Apr/2014:12:07:15] "GET /passwords.pdf?JSESSIONID=SD3SL5FF4ADFF51205 HTTP 1.1" 404 2152 "http://www.buttercupgames.com/oldlink?itemId=EST-26" "Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5" 162 host = s18359064 source = buttercup.zip:\buttercup\www1\access.log sourcetype = access_combined_wcookie

New Search Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase  
| top categoryId
```

All time ▾ 🔍

✓ 5,224 events (before 24/06/2020 16:07:35.000) No Event Sampling ▾ Job ▾ II ■ ↗ ✚ ⬇ ⚡ Fast Mode ▾

Events Patterns **Statistics (7)** Visualization

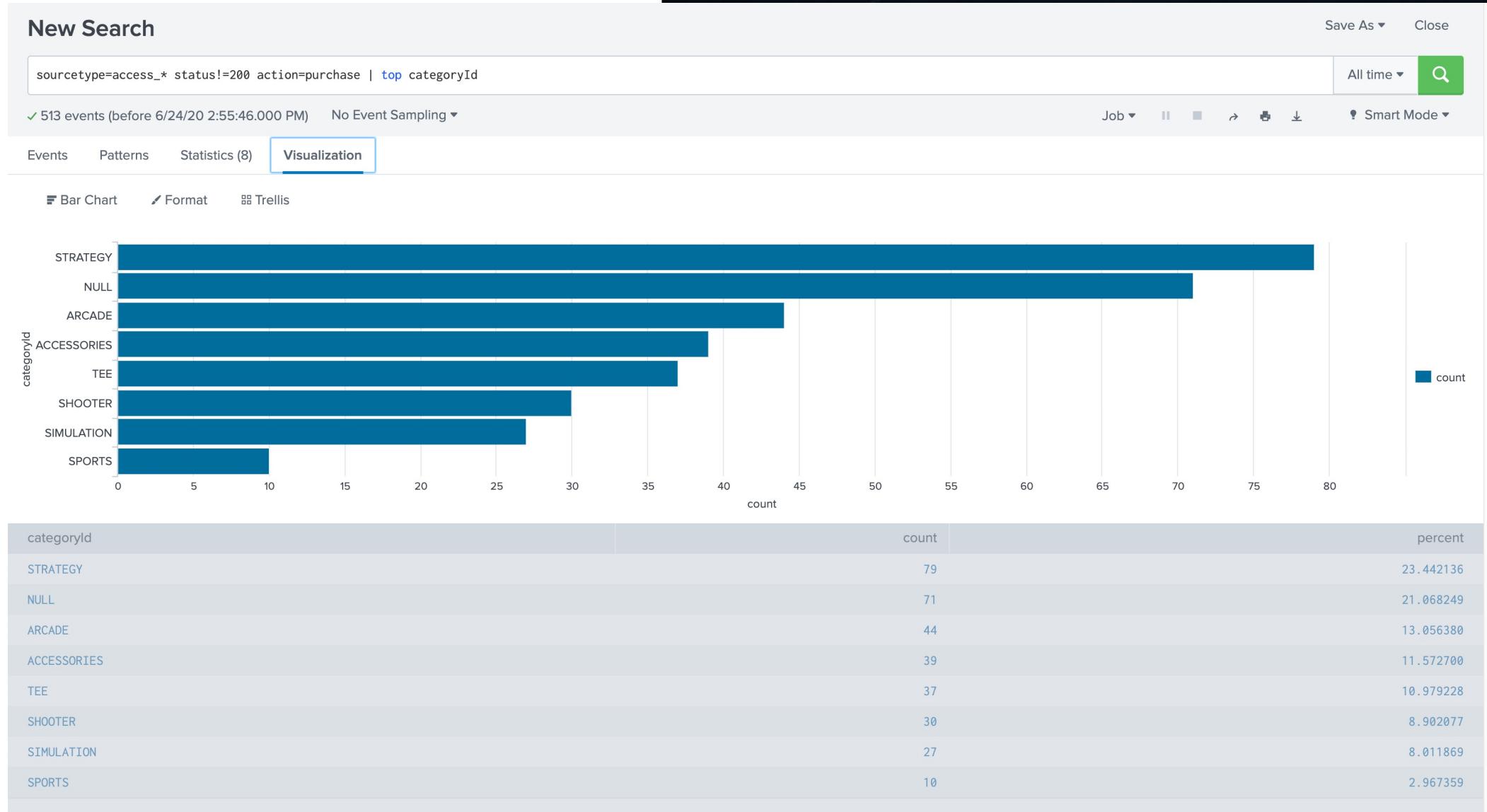
20 Per Page ▾ ✍ Format Preview ▾

categoryId	count	percent
STRATEGY	806	30.495649
ARCADE	493	18.653046
TEE	367	13.885736
ACCESSORIES	348	13.166856
SIMULATION	246	9.307605
SHOOTER	245	9.269769
SPORTS	138	5.221339

Get



Splunk



New Search Save As ▾ Close

```
sourcetype=access_* status=200 action=purchase  
| top categoryId
```

All time ▼ 🔍

✓ 5,224 events (before 24/06/2020 16:07:35.000) No Event Sampling ▾ Job ▾ || ⤒ ⤓ ⤔ ⤕ ⤖ ⤗ ⤘ Fast Mode ▾

Events Patterns Statistics (7) **Visualization**

柱状图 Format Trellis

categoryId	count
STRATEGY	750
ARCADE	500
TEE	350
ACCESSORIES	350
SIMULATION	250
SHOOTER	250
SPORTS	150

Get

cyber & data

Splunk

New Search

Save As ▾ Close

```
sourcetype=access_* status!=200 action=purchase  
| top categoryId
```

All time ▾



✓ 513 events (before 24/06/2020 16:10:47.000) No Event Sampling ▾

Job ▾ || ■ ↗ ✎ ↓ ⚡ Fast Mode ▾

Events

Patterns

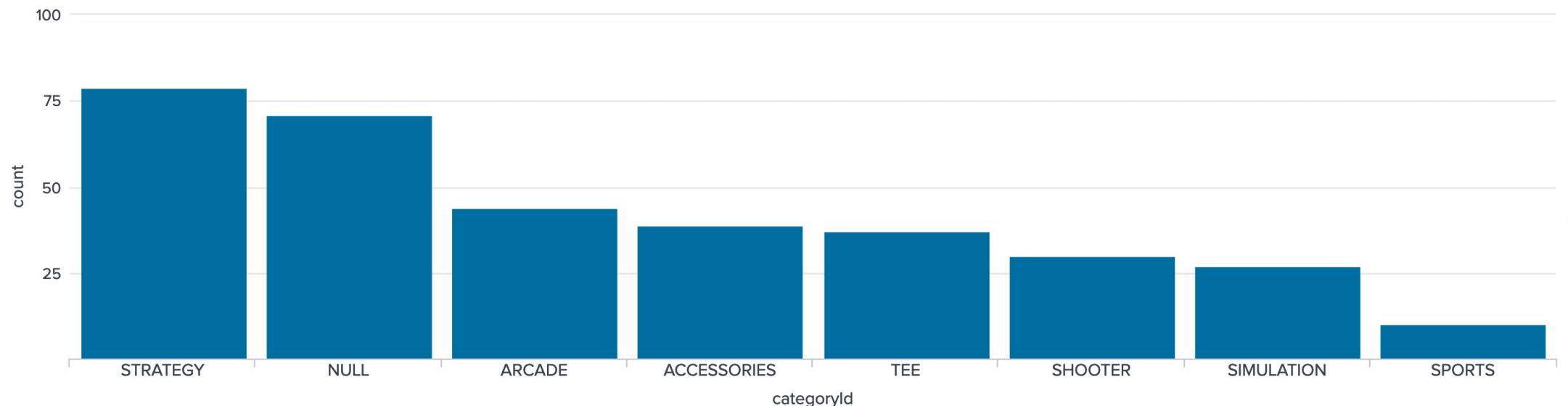
Statistics (8)

Visualization

柱状图

Format

 Trellis



Get

cyber & data

Splunk

New Search

New Search

```
| top limit=20 useragent
```

Save As ▾

Close

✓ 24,866 events (before 24/06/2020 16:11:50.000)

No Event Sampling ▾

Job ▾



All time ▾



Events Patterns

Statistics (20)

Visualization

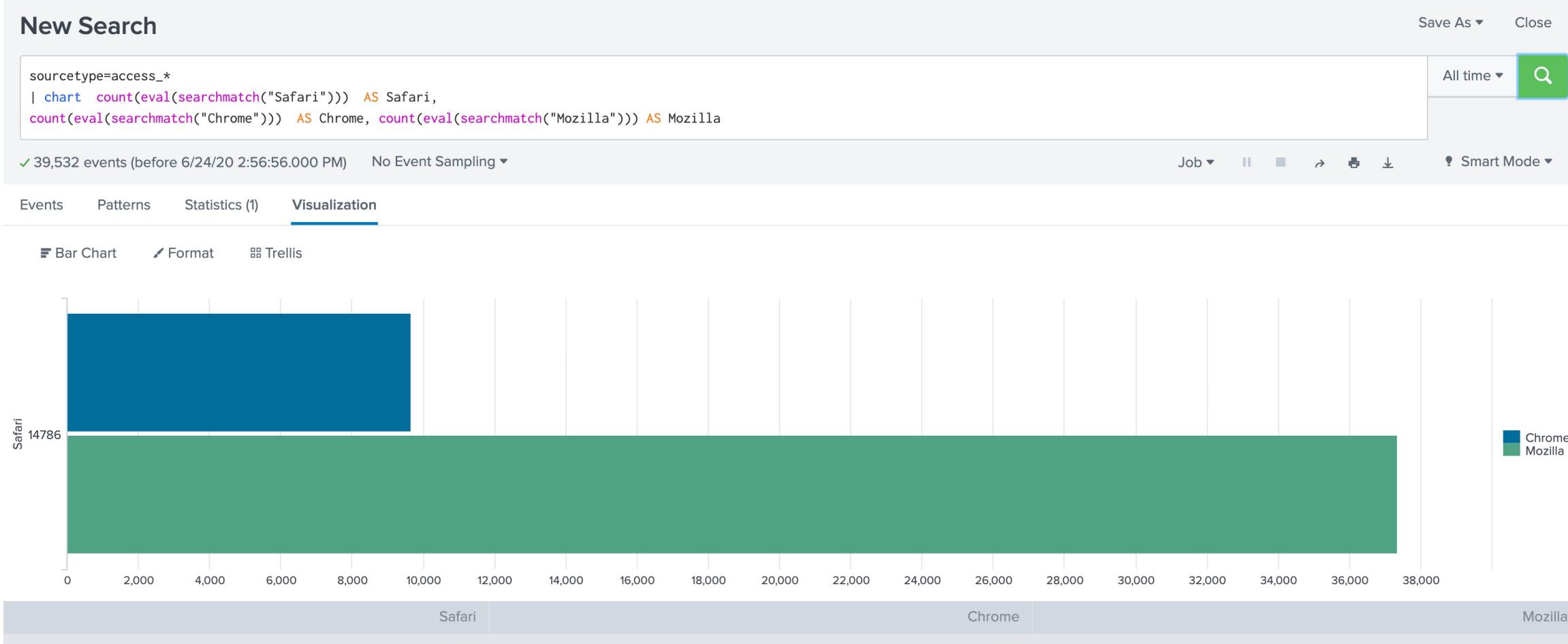
20 Per Page ▾

 Format

Preview ▾

useragent	count	percent
Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.28) Gecko/20120306 YFF3 Firefox/3.6.28 (.NET CLR 3.5.30729; .NET4.0C)	5282	21.241856
Mozilla/5.0 (Windows NT 6.1; WOW64) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	2383	9.583367
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.2; .NET CLR 1.1.4322; InfoPath.1; MS-RTC LM 8)	2130	8.565913
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_7_4) AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/536.5	2021	8.127564
Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; Trident/4.0; .NET CLR 2.0.50727; MS-RTC LM 8; InfoPath.2)	1898	7.632912
Mozilla/5.0 (compatible; MSIE 9.0; Windows NT 6.1; WOW64; Trident/5.0; BOIE9;ENUS)	1770	7.118153
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_6_8) AppleWebKit/534.55.3 (KHTML, like Gecko) Version/5.1.5 Safari/534.55.3	1121	4.508164
Mozilla/5.0 (iPad; U; CPU OS 4_3_5 like Mac OS X; en-us) AppleWebKit/533.17.9 (KHTML, like Gecko) Version/5.0.2 Mobile/8L1 Safari/6533.18.5	1064	4.278935
Mozilla/5.0 (iPad; CPU OS 5_1_1 like Mac OS X) AppleWebKit/534.46 (KHTML, like Gecko) Version/5.1 Mobile/9B206 Safari/7534.48.3	1000	4.021556

Splunk



Get

cyber
& data

Splunk

New Search

Save As ▾ Close

```
get cart.do productId="WC-SH-G04" | top categoryId
```

All time ▾



✓ 692 events (before 6/25/20 5:56:31.000 AM) No Event Sampling ▾

Job ▾ || ■ ↻ + ↓

! Smart Mode ▾

Events Patterns Statistics (1) Visualization

20 Per Page ▾ ✎ Format Preview ▾

categoryId	count	percent
SHOOTER	171	100.000000

Get



Splunk

New Search Save As ▾ Close

get cart.do categoryId="STRATEGY" | **top** productId All time ▾ 🔍

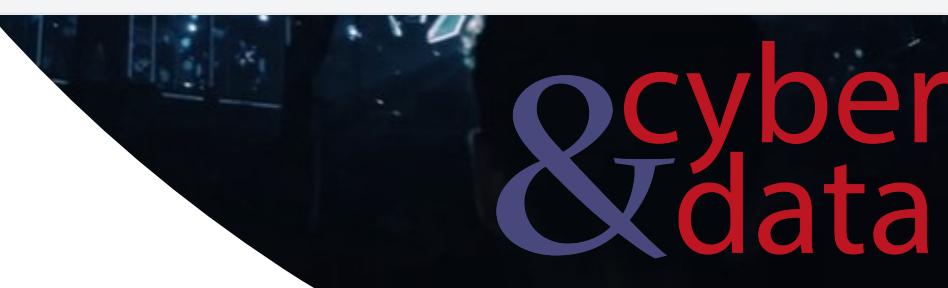
✓ 568 events (before 6/25/20 6:06:42.000 AM) No Event Sampling ▾ Job ▾ || ↶ ↷ ⤒ ⤓ ! Smart Mode ▾

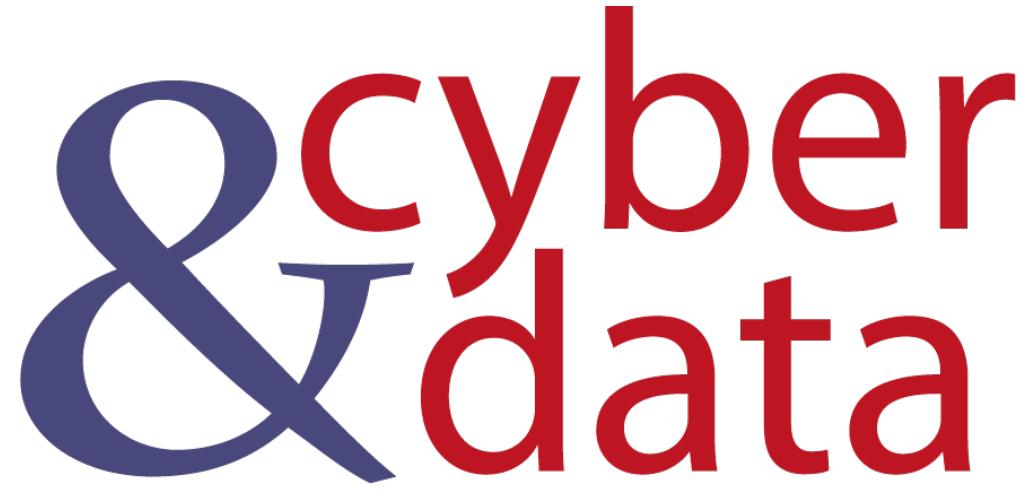
Events Patterns **Statistics (4)** Visualization

20 Per Page ▾ ✓ Format Preview ▾

productId	count	percent
DB-SG-G01	171	30.105634
DC-SG-G02	157	27.640845
FS-SG-G03	131	23.063380
PZ-SG-G05	109	19.190141

Get





“From bits to information”

Introduction to Splunk