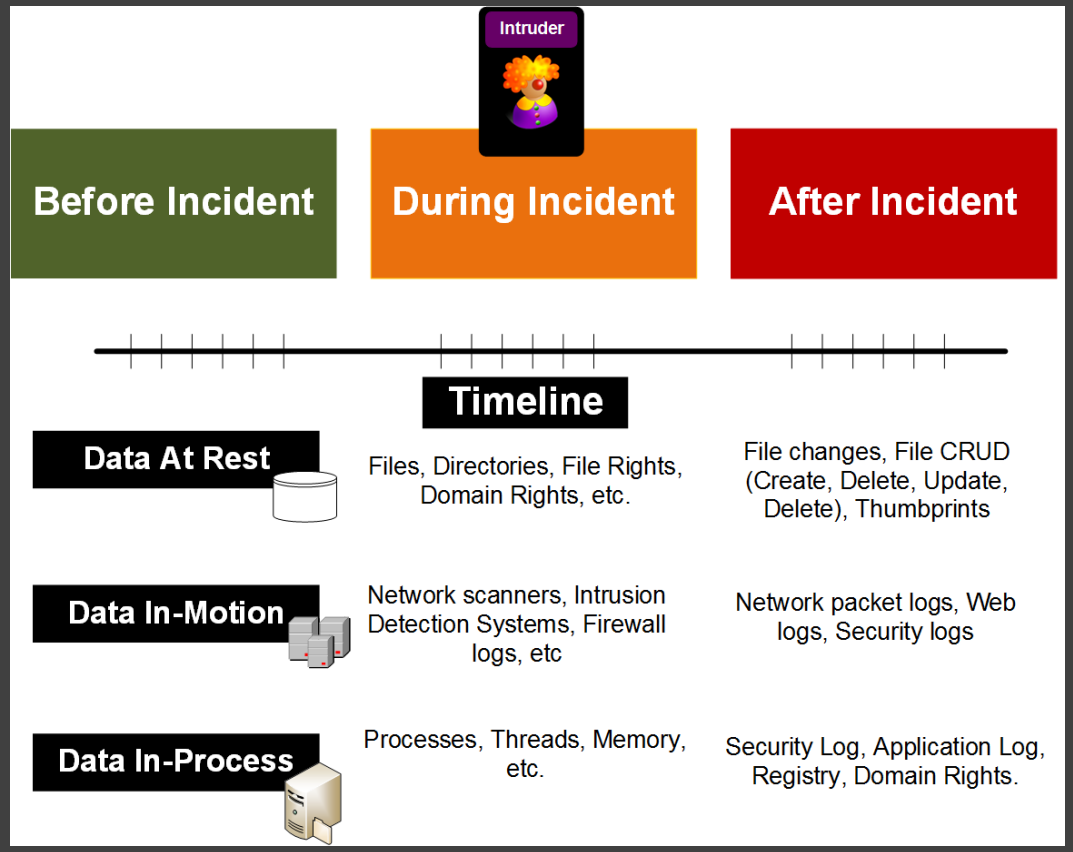
cyber & data

"From bits to information"



Introduction to Splunk

cyber & data

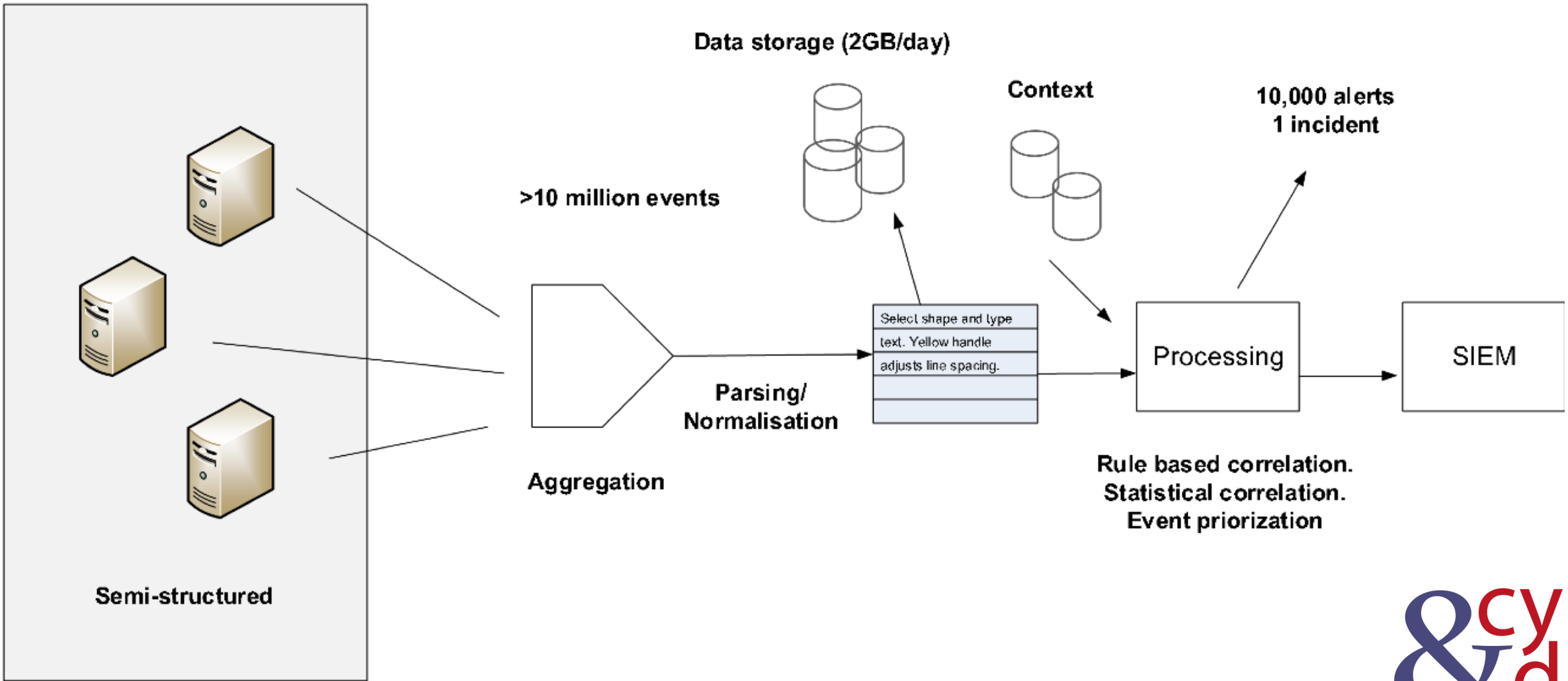
"From bits to information"

Memory, Big Data and SIEM

Outline

- SIEM (Security information and event management) infrastructure.
- Machines and Data.
- Directed Graphs.
- The V’s of Big Data.
- Data gathering.
- Building a timeline.

Outline



&cyber data

cyber & data

"From bits to information"

Machines and Data

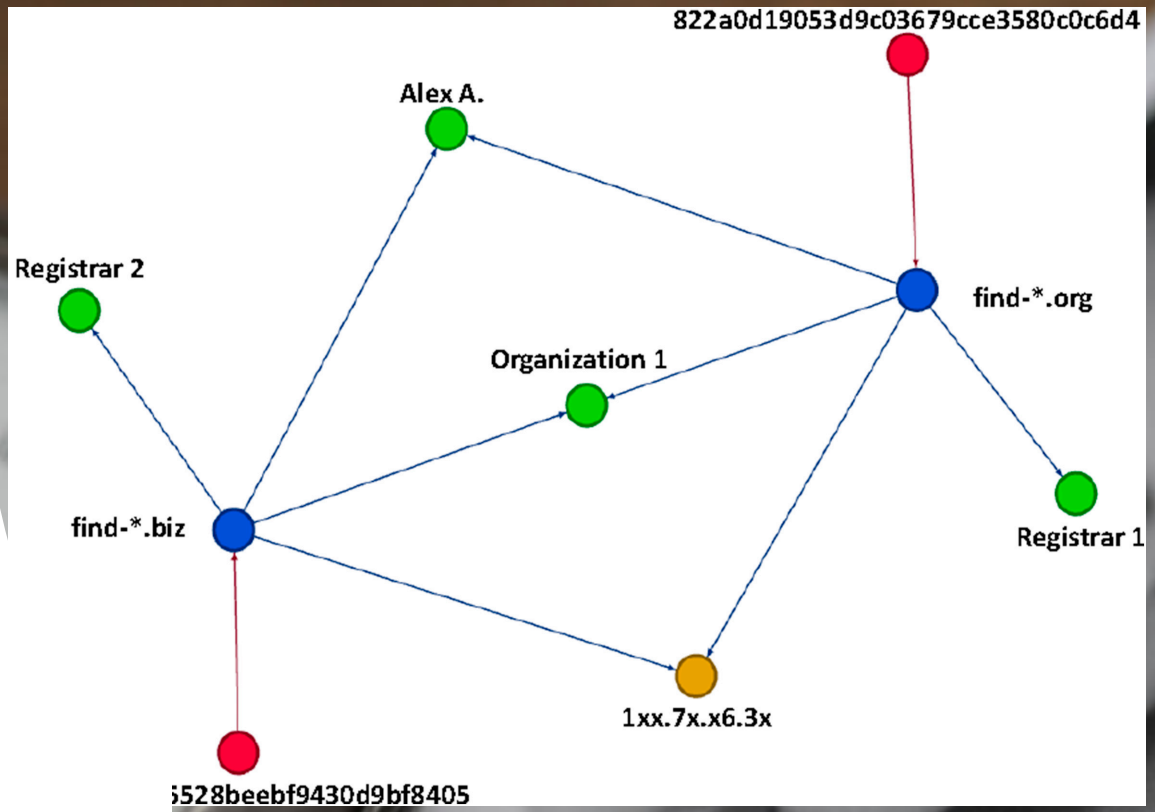
Outline

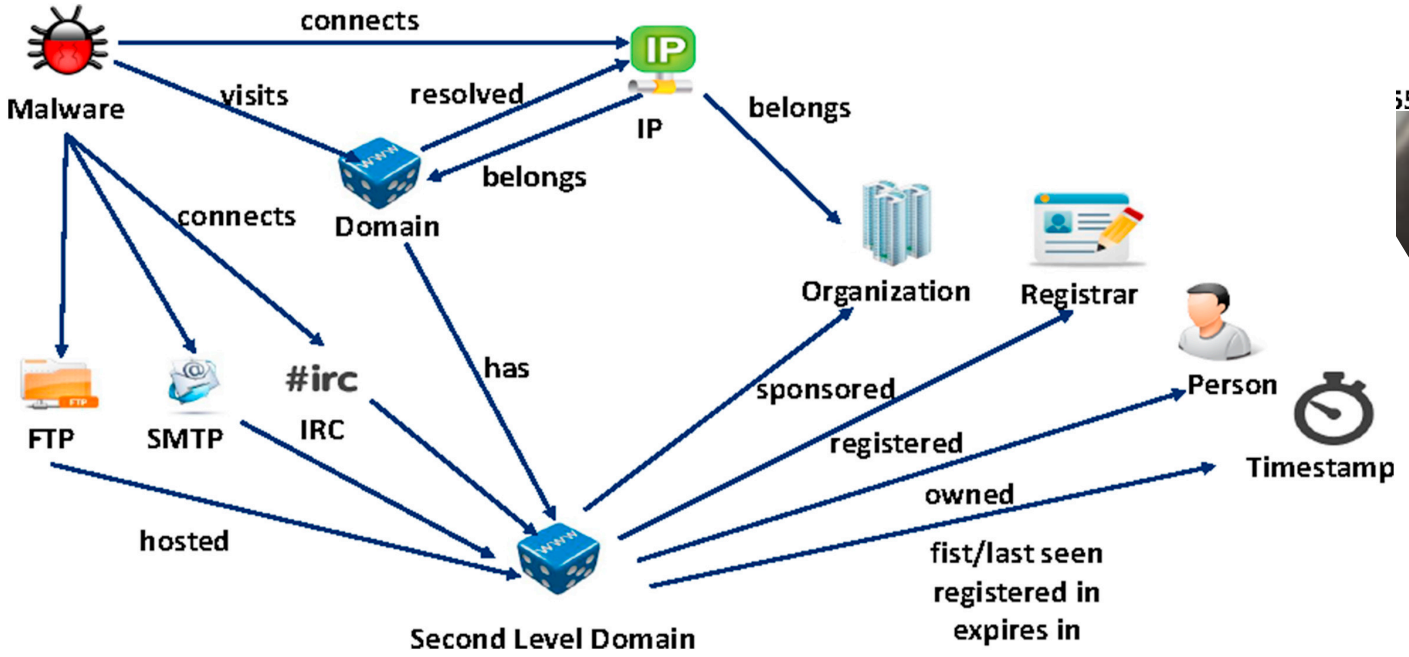
- **Adaptive**. This would allow the machine to learn from changes as new goals and requirements evolve. The engine, too, could also cope with unpredictability and ambiguity, and make reasoned decisions. This adaptability would allow pre-defined rules to be changed and migrated over time, and would also support the strengthening of security when there is a perceived attack, and to reduce it when not under attack.
- **Interactive**. This would support the interaction of the cognitive engine with a whole range of services, people, systems, and so on. A core part of a cognitive engine - as we see in the brain - is the ability for it to take inputs from a range of sources, and then provide outputs in the required way.
- **Iterative and stateful.** This involves understanding previous interactions and be able to sustain future ones, along with plotting the best course and to learn new routes. As humans, our interactions with others are often stateful, and where we remember where we have left things with different people. Within a cognitive engine, we would thus define our interactions as well-defined states, of which we move into and out of.
- **Contextual**. This allows the identification of key contextual elements within the data, including locations, names, dates, and so on. The original data may be in many different formats and could be structured, semi-structured or unstructured.

"From bits to information"

Directed Graphs and Cyber Threats

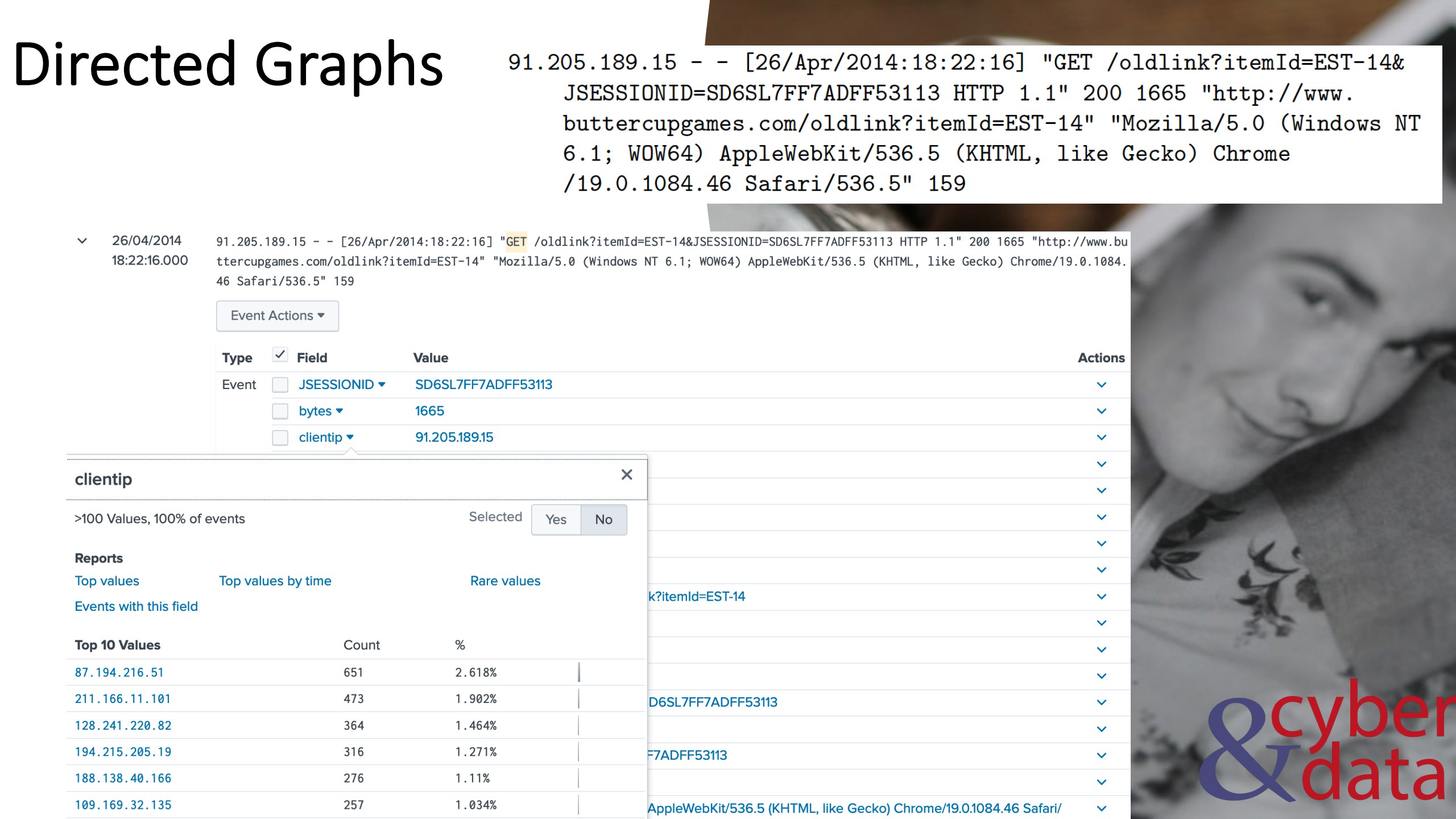
Directed Graphs





Directed Graphs

```
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
```



cyber & data

"From bits to information"

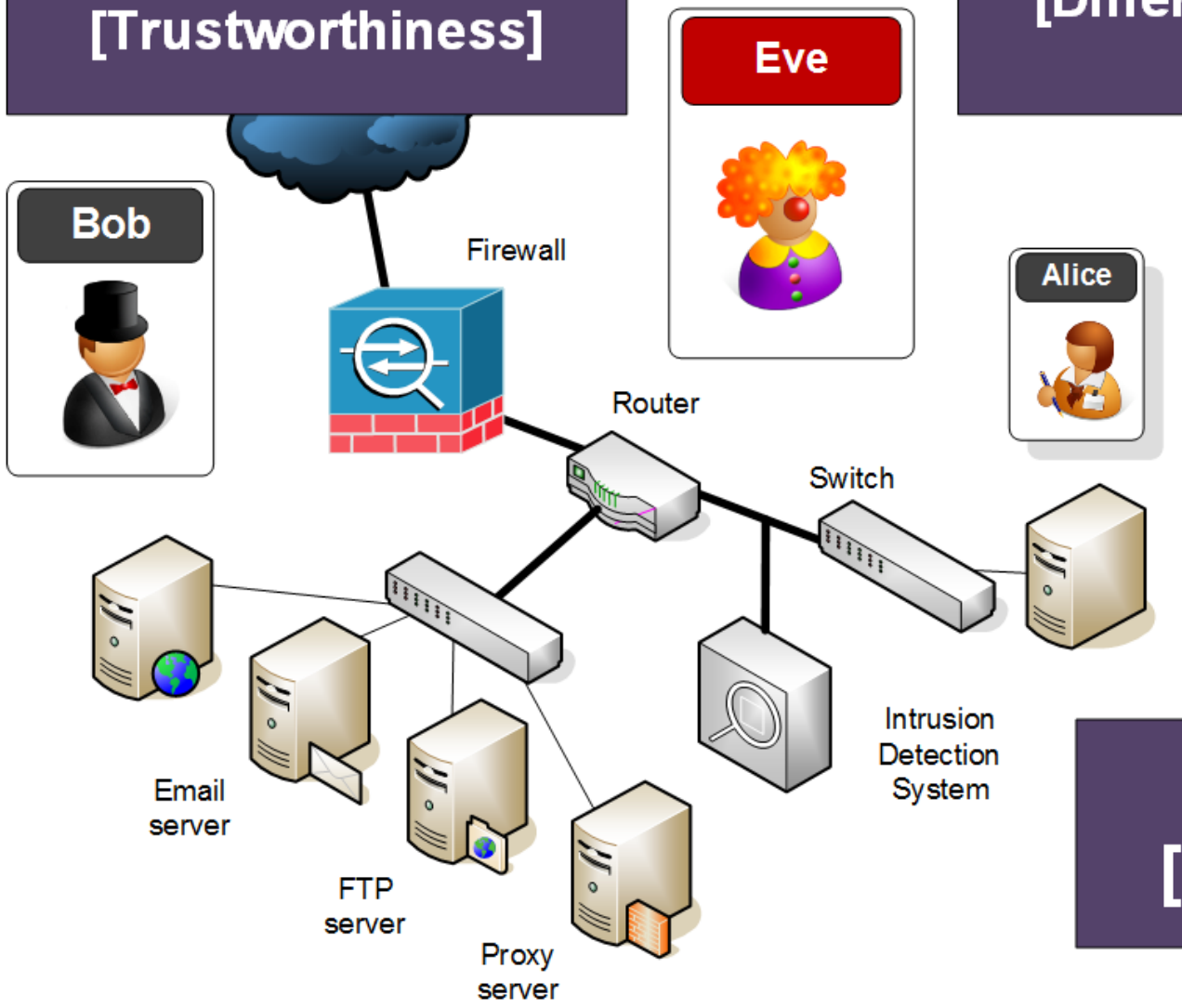
The V's of Data

Outline

V- Velocity
[Speed of data generation]

V- Veracity
[Trustworthiness]

V- Variety
[Different forms of data]



- Management report
- Sales analysis
- Targeted marketing
- Trending/Correlation
- Incident Response

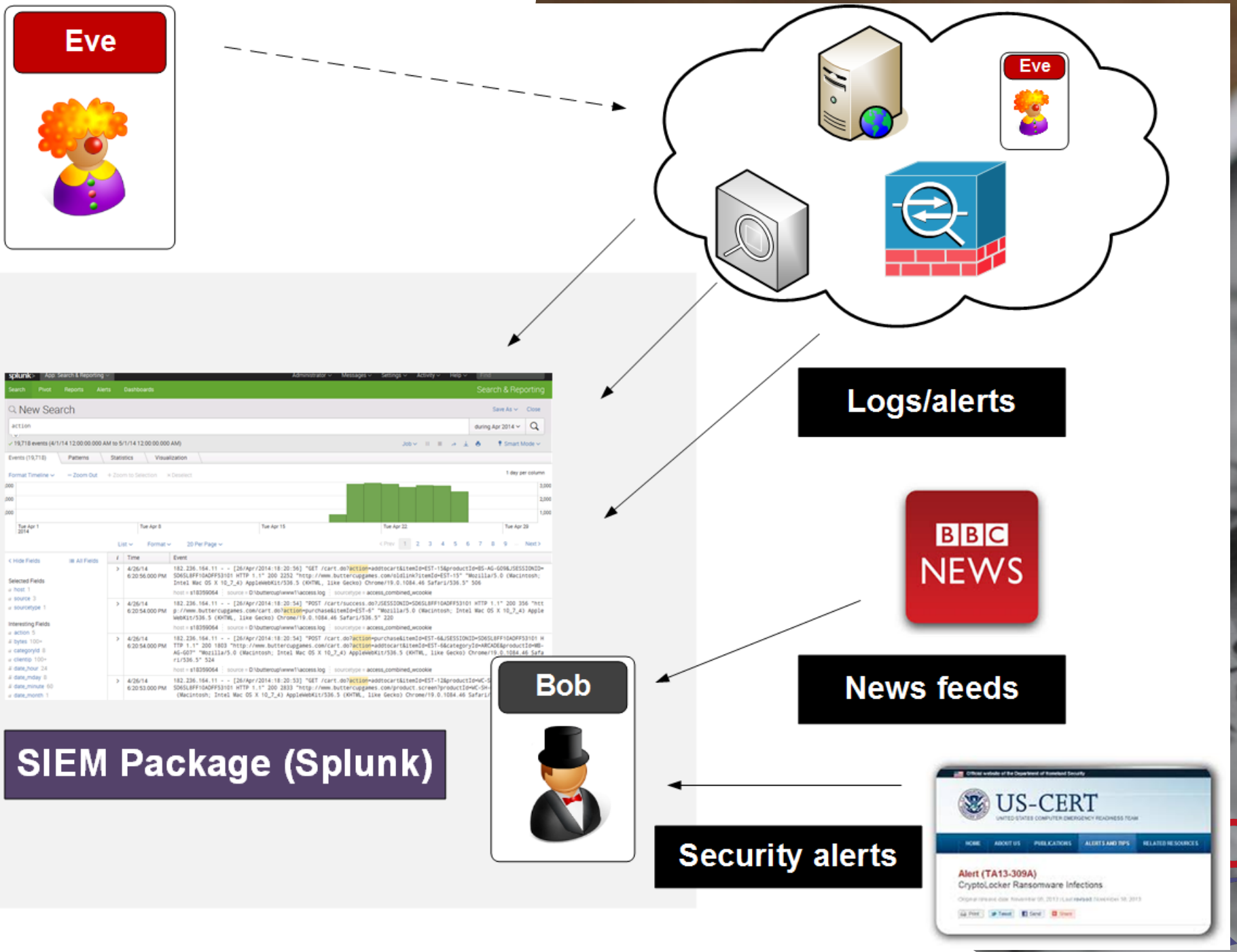
V- Volume
[Scale of data]

cyber & data

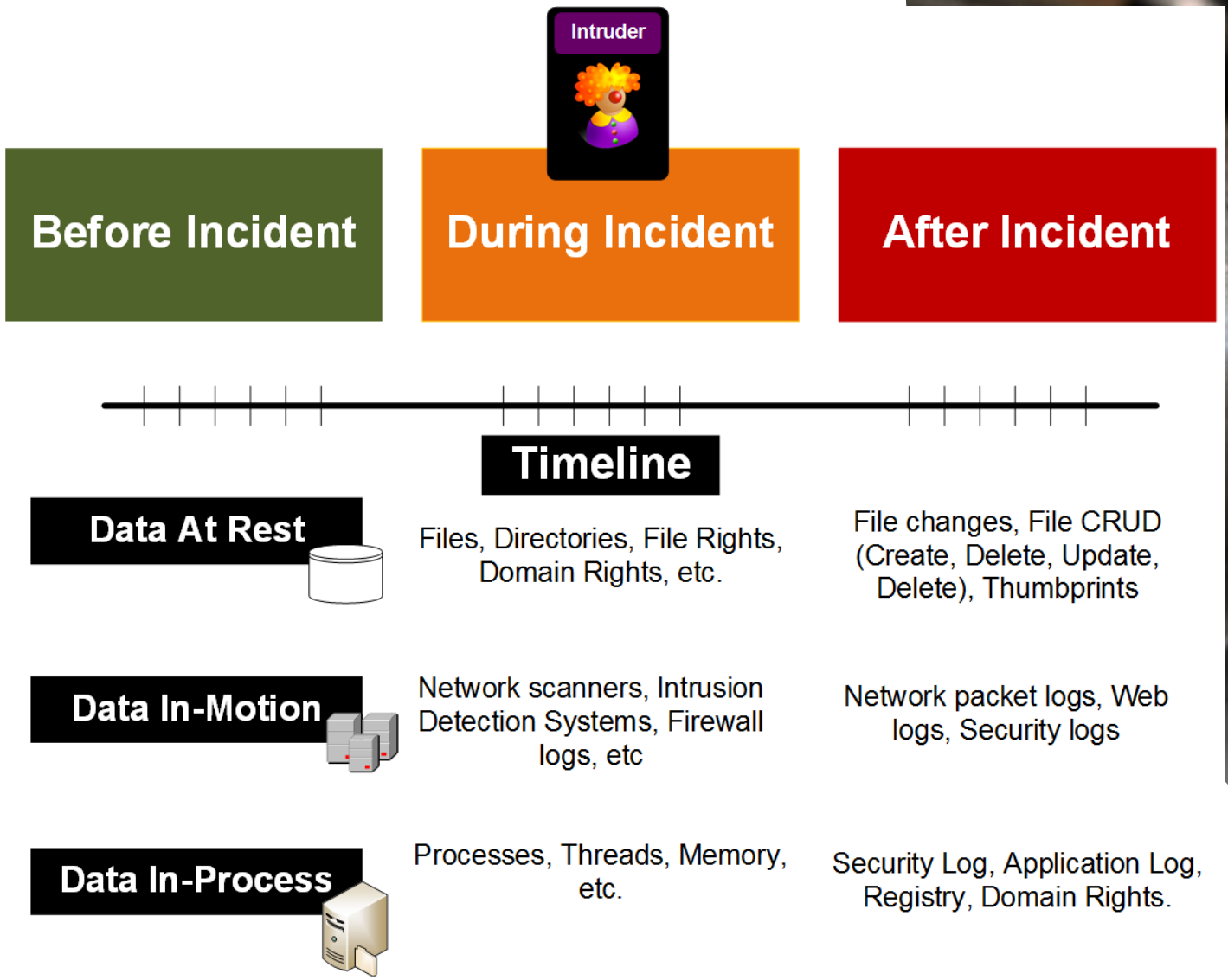
"From bits to information"

Data Gathering

Outline


Eve
Eve
Logs/alerts
BBC NEWS
News feeds
Bob
SIEM Package (Splunk)
Security alerts
US-CERT
Alert (TA13-309A)
CryptoLocker Ransomware Infections

Outline


Intruder
Before Incident
During Incident
After Incident
Timeline
Data At Rest
Files, Directories, File Rights, Domain Rights, etc.
File changes, File CRUD (Create, Delete, Update, Delete), Thumbprints
Data In-Motion
Network scanners, Intrusion Detection Systems, Firewall logs, etc
Network packet logs, Web logs, Security logs
Data In-Process
Processes, Threads, Memory, etc.
Security Log, Application Log, Registry, Domain Rights.


&cyber data

Outline

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

File and Directories
- CRUD.
- Security changes.

Performance
- CPU.
- Memory.
- Threads.

Database Access
- Logs.

TCP/UDP
- Syslog.

Remote Access
- Logs.

Registry Monitoring
- Key changes.
- Updates.

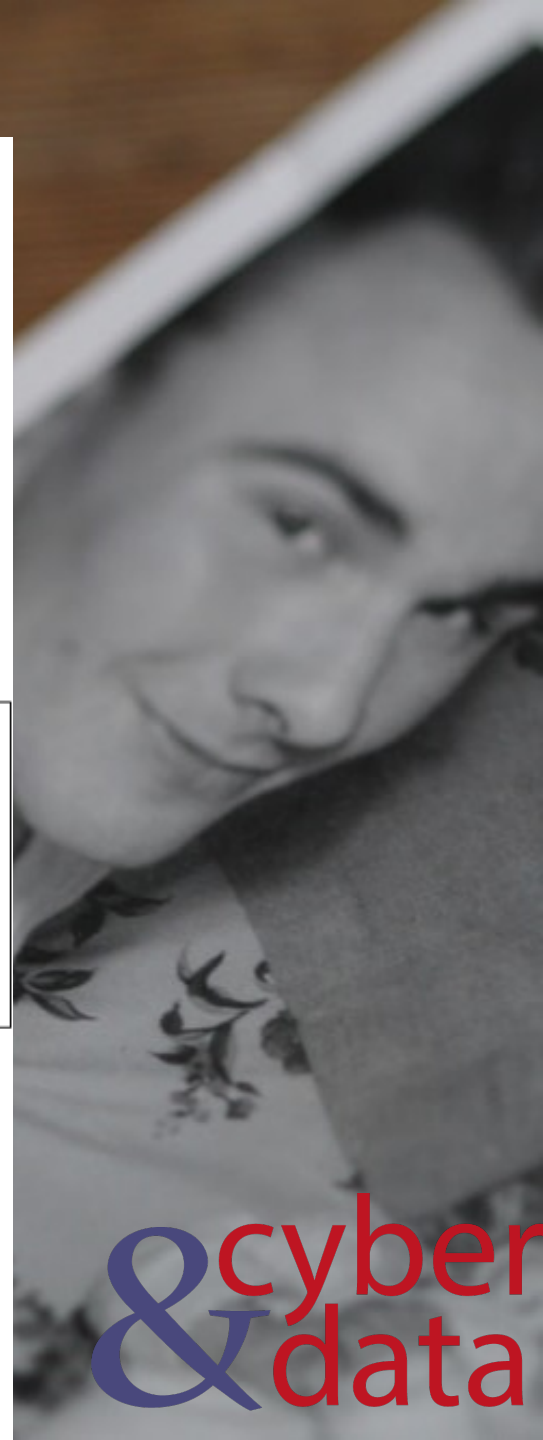
Environmental
- Temp.
- Humidity.

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

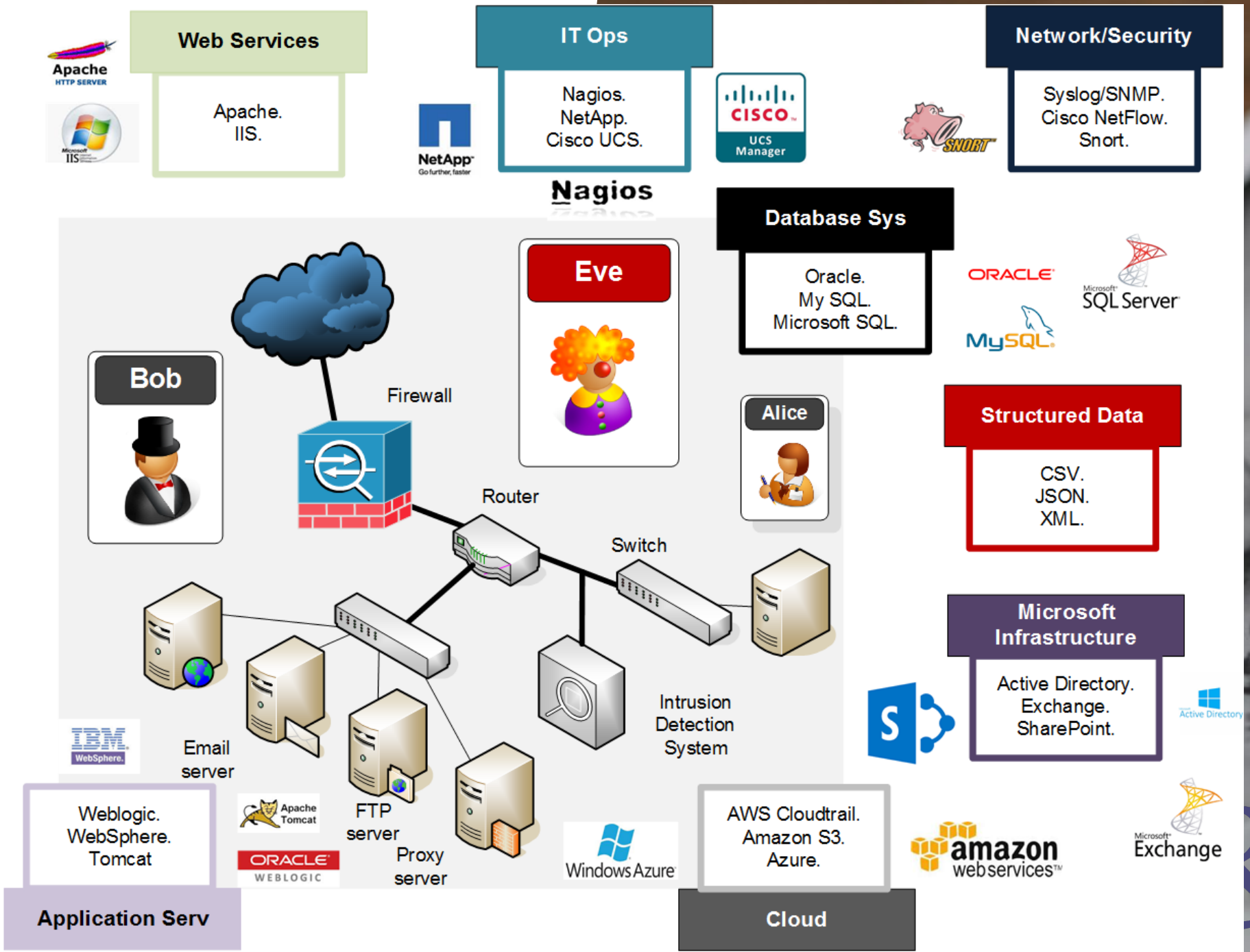
Intrusion Detection
- Alerts

Email
- Logs.

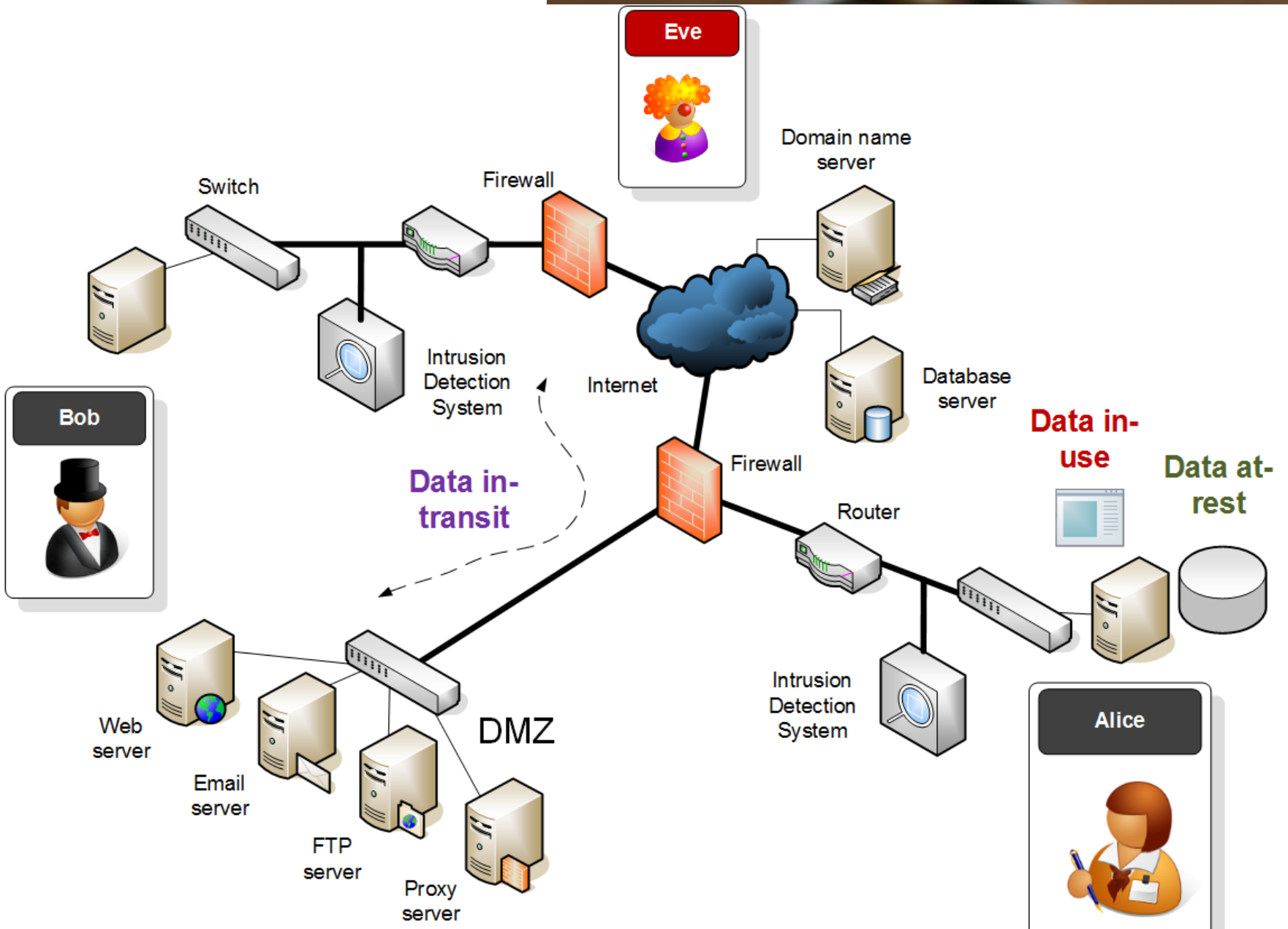
Print Monitoring
- Jobs.



Outline


Web Services
Apache.
IIS.
IT Ops
Nagios.
NetApp.
Cisco UCS.
Network/Security
Syslog/SNMP.
Cisco NetFlow.
Snort.
Database Sys
Oracle.
My SQL.
Microsoft SQL.
Structured Data
CSV.
JSON.
XML.
Microsoft Infrastructure
Active Directory.
Exchange.
SharePoint.
Application Serv
Weblogic.
WebSphere.
Tomcat
Cloud
AWS Cloudtrail.
Amazon S3.
Azure.
Bob
Eve
Alice
Firewall
Router
Switch
Intrusion Detection System
Email server
FTP server
Proxy server

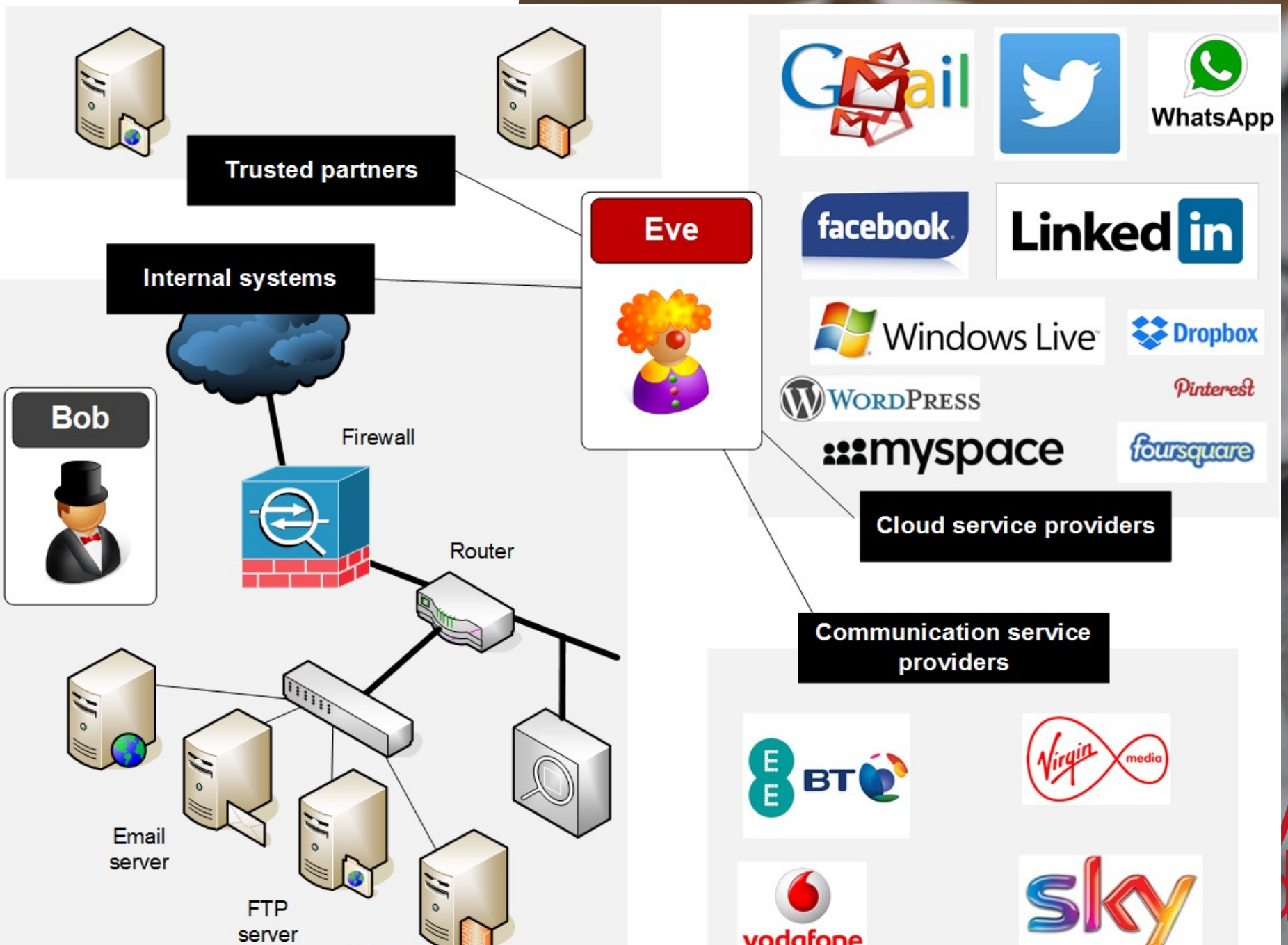
Outline


Eve
Domain name server
Switch
Firewall
Intrusion Detection System
Internet
Database server
Bob
Data in-use
Data at-rest
Data in-transit
Firewall
Router
Web server
Email server
FTP server
Proxy server
DMZ
Intrusion Detection System
Alice

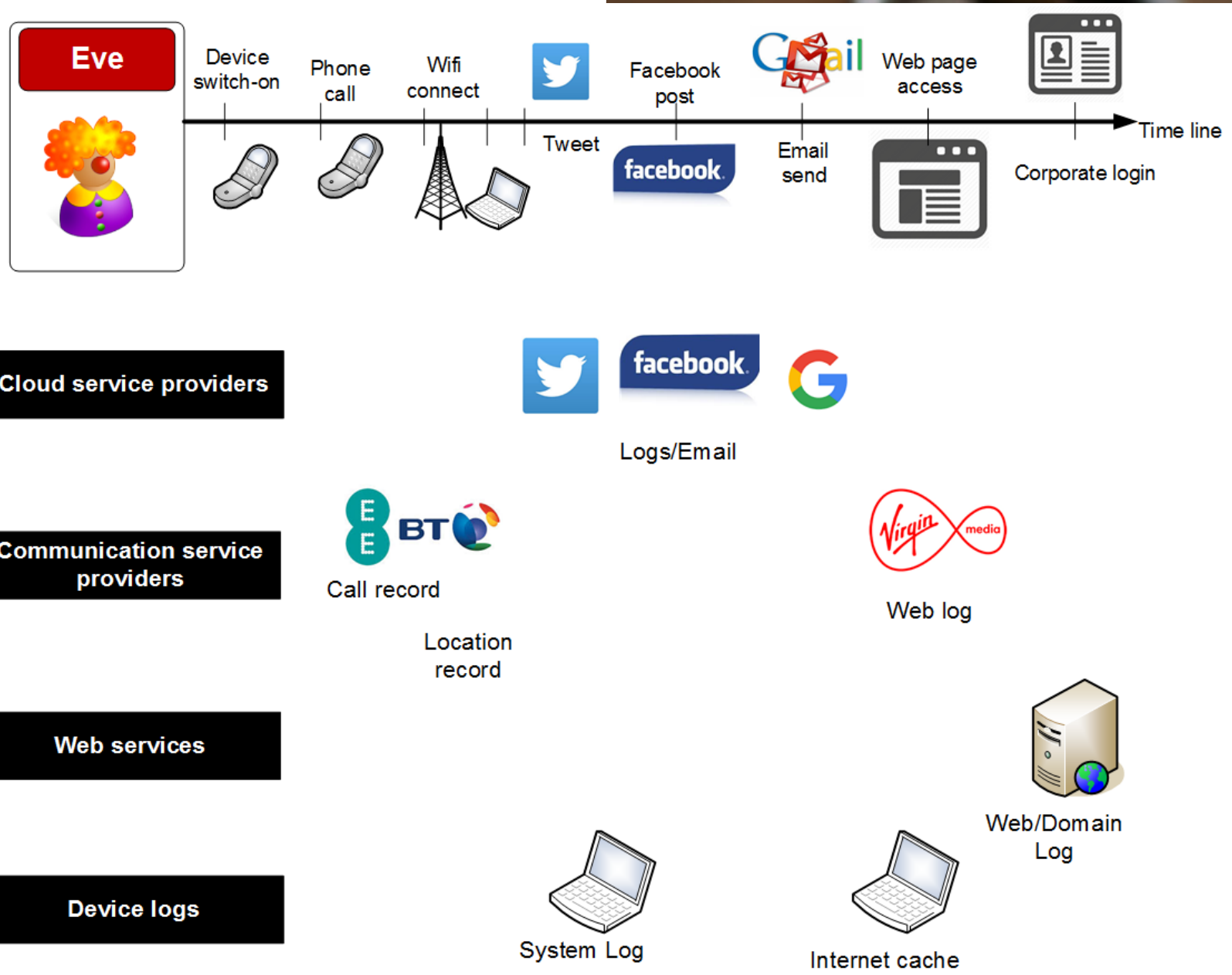
"From bits to information"

Timelines

Outline


Trusted partners
Eve
Internal systems
Bob
Firewall
Router
Email server
FTP server
Cloud service providers
Communication service providers
Gmail
WhatsApp
facebook
LinkedIn
Windows Live
Dropbox
WordPress
Pinterest
myspace
foursquare
BT
Virgin media
vodafone
sky

Outline


Eve
Device switch-on
Phone call
Wifi connect
Tweet
Facebook post
Email send
Web page access
Corporate login
Time line
Cloud service providers
Logs/Email
Communication service providers
Call record
Location record
Web log
Web services
Web/Domain Log
Device logs
System Log
Internet cache

cyber & data

"From bits to information"

Introduction to Splunk

Here: https://www.youtube.com/watch?v=HeWfkPeDQbY
Threat model: https://threatmap.checkpoint.com/
Threat model: https://cybermap.kaspersky.com/

Outline

- Why use Splunk?
- Application of Splunk.

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.

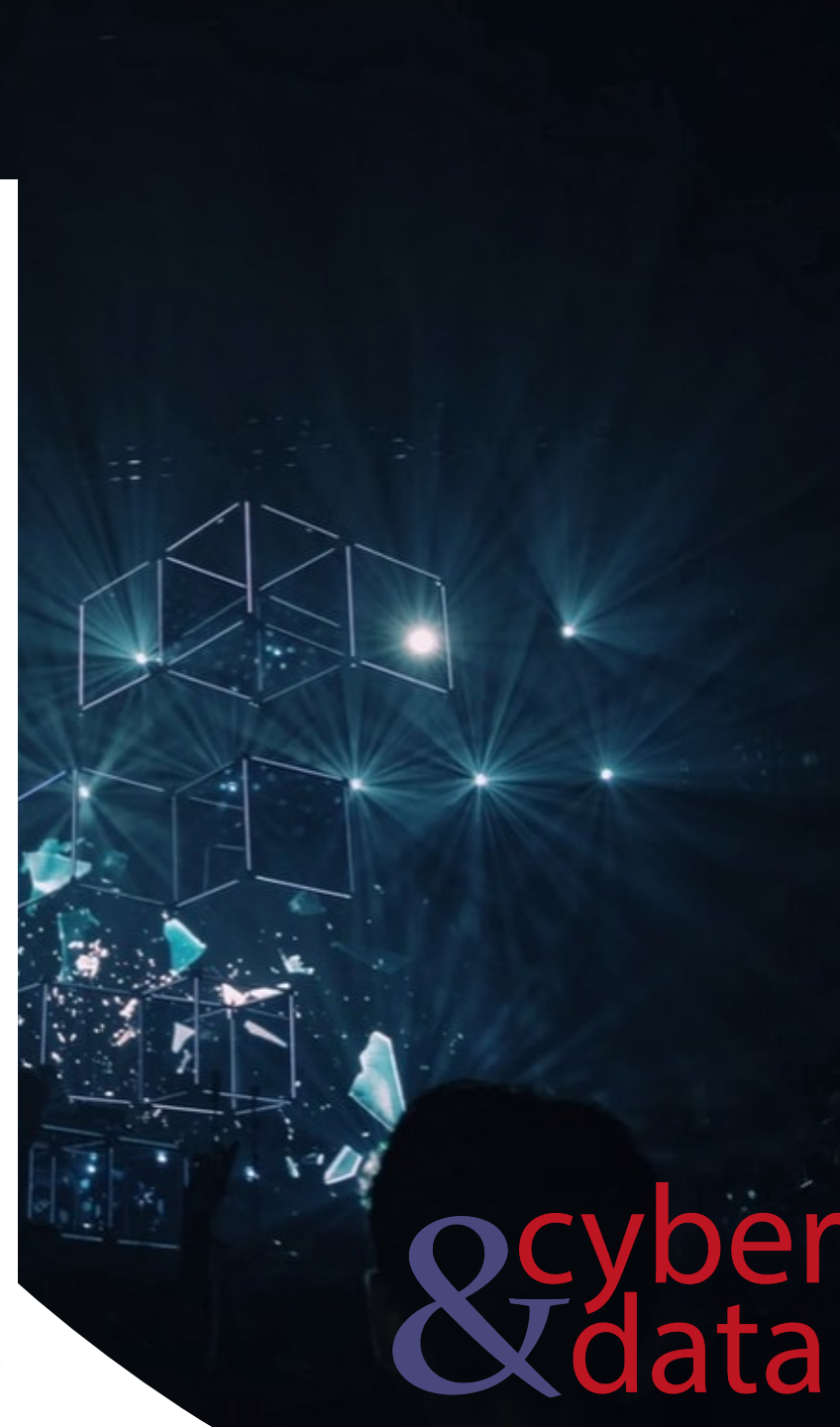
PCI DSS COMPLIANT

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

Define/Maintain Security Policy
Design and implement a policy which focuses on security.

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

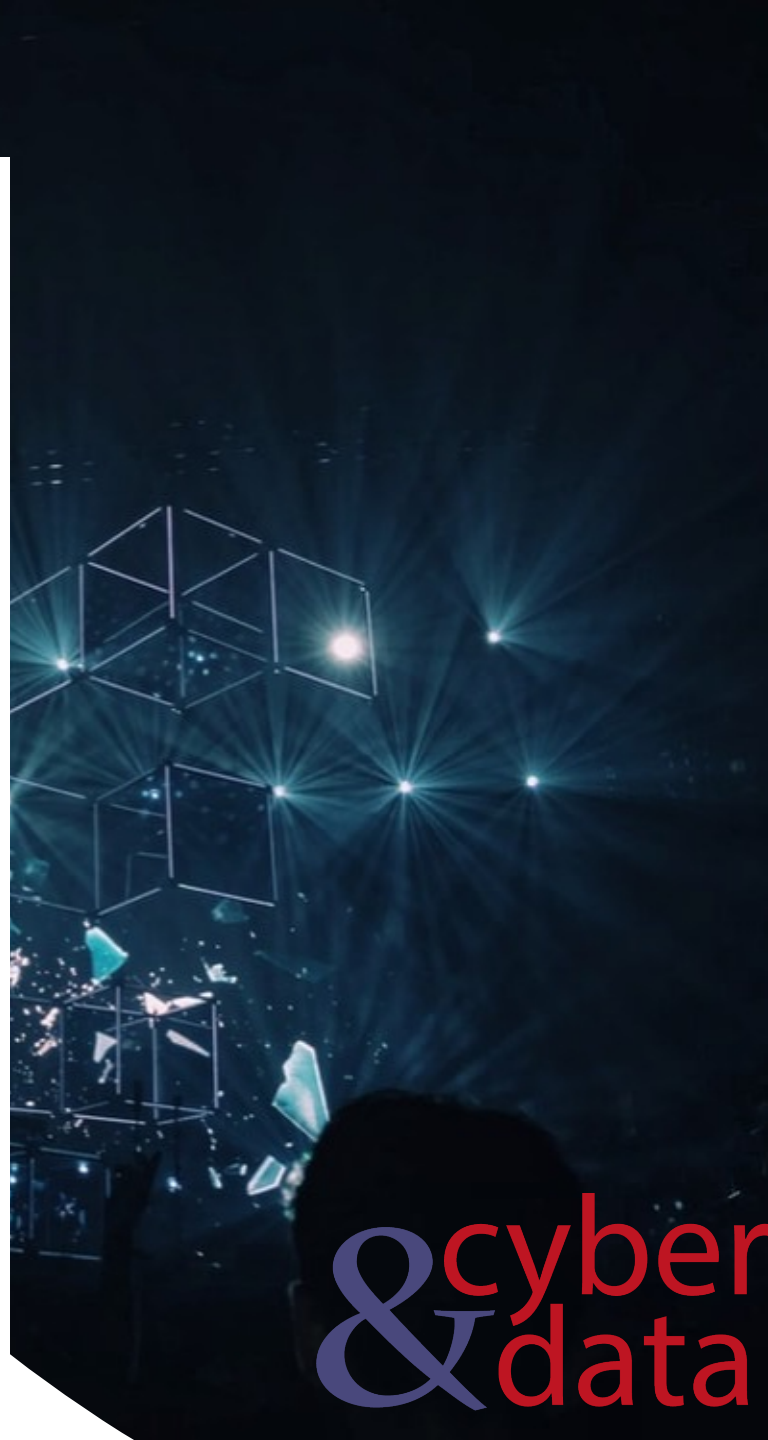
VISA MasterCard DELTA VISA Electron Maestro SOLO



&cyber data

Before, During and After

Before Incident	During Incident	After Incident
Timeline		
Data At Rest	Files, Directories, File Rights, Domain Rights, etc.	File changes, File CRUD (Create, Delete, Update, Delete), Thumbprints
Data In-Motion	Network scanners, Intrusion Detection Systems, Firewall logs, etc	Network packet logs, Web logs, Security logs
Data In-Process	Processes, Threads, Memory, etc.	Security Log, Application Log, Registry, Domain Rights.



cyber & data

Logs

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

File and Directories
- CRUD.
- Security changes.

Performance
- CPU.
- Memory.
- Threads.

Database Access
- Logs.

TCP/UDP
- Syslog.

Remote Access
- Logs.

Registry Monitoring
- Key changes.
- Updates.

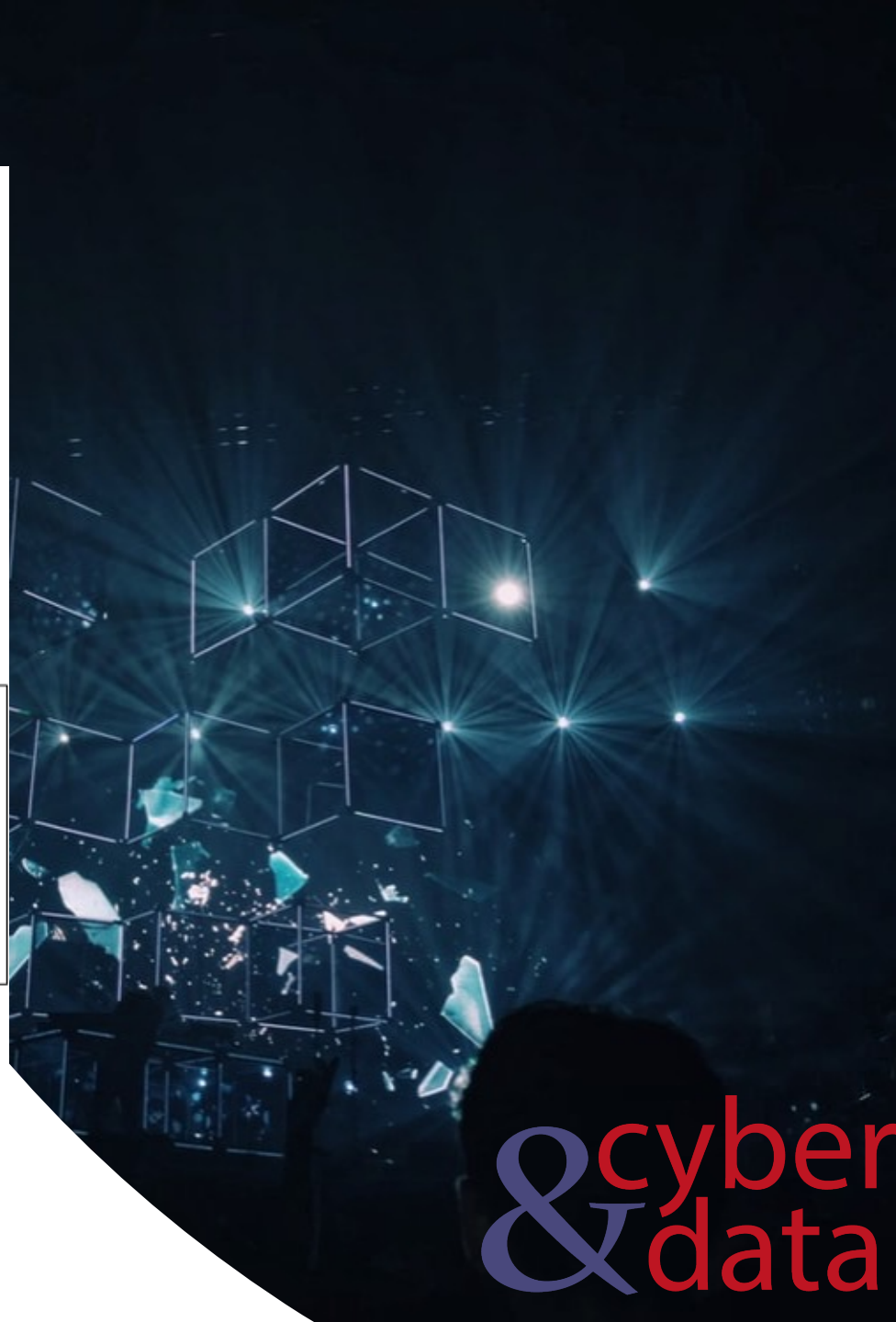
Environmental
- Temp.
- Humidity.

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

Intrusion Detection
- Alerts

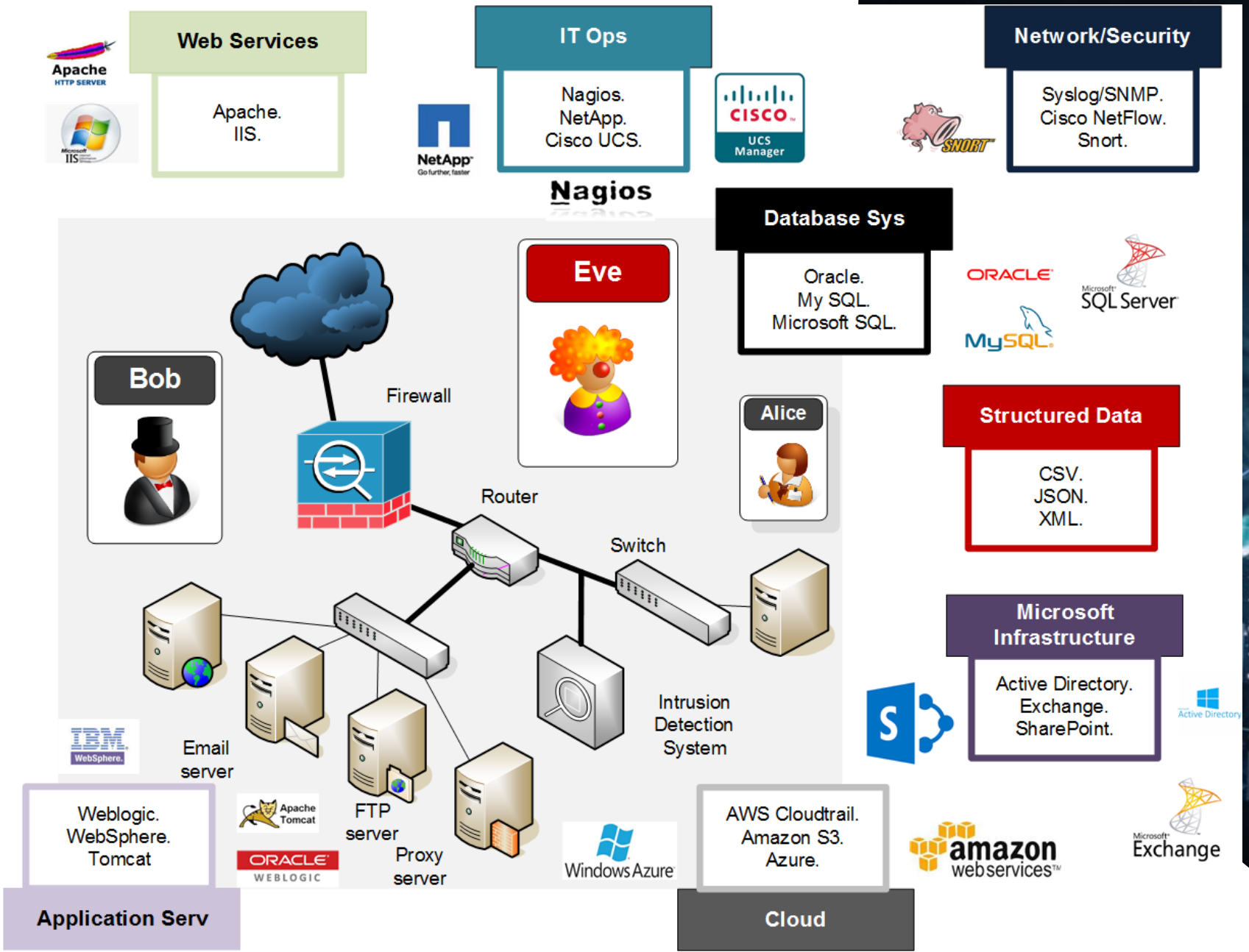
Email
- Logs.

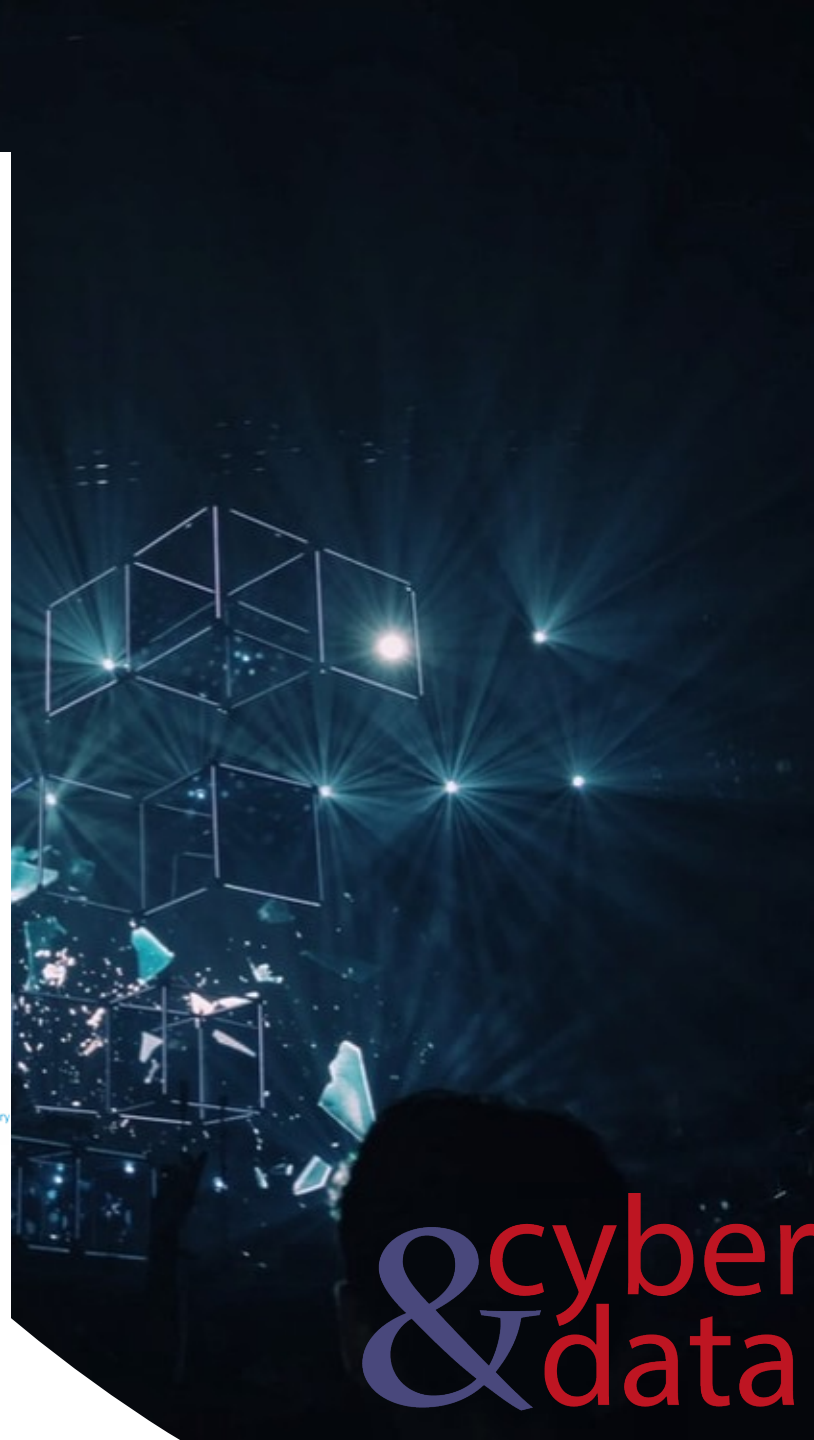
Print Monitoring
- Jobs.



&cyber data

And the complexity …





cyber & data

"From bits to information"

Get

Introduction to Splunk

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}

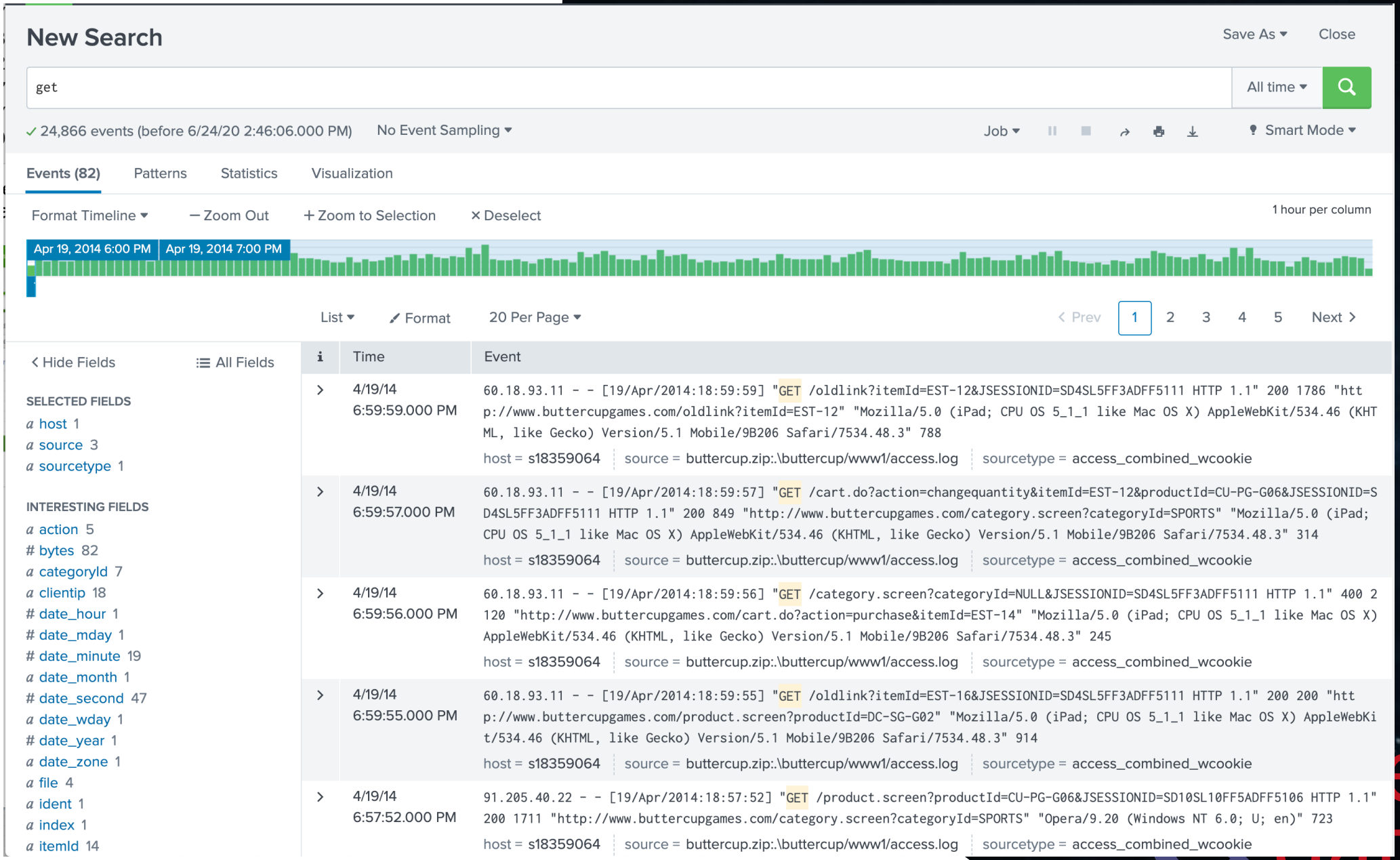
POST → action={addtocart, purchase, view, remove, changequantity} categoryID, productID

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.

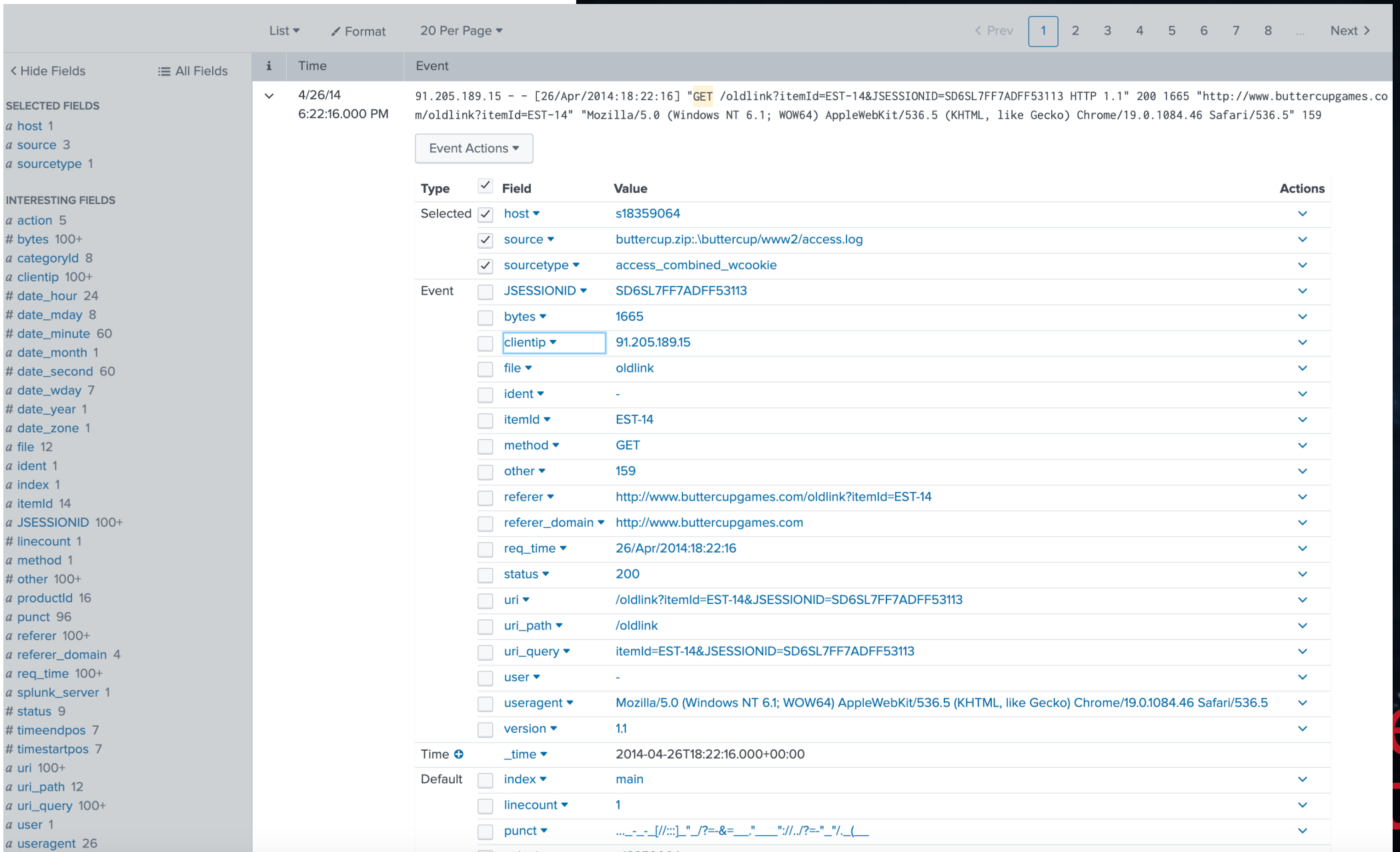
Get

Splunk

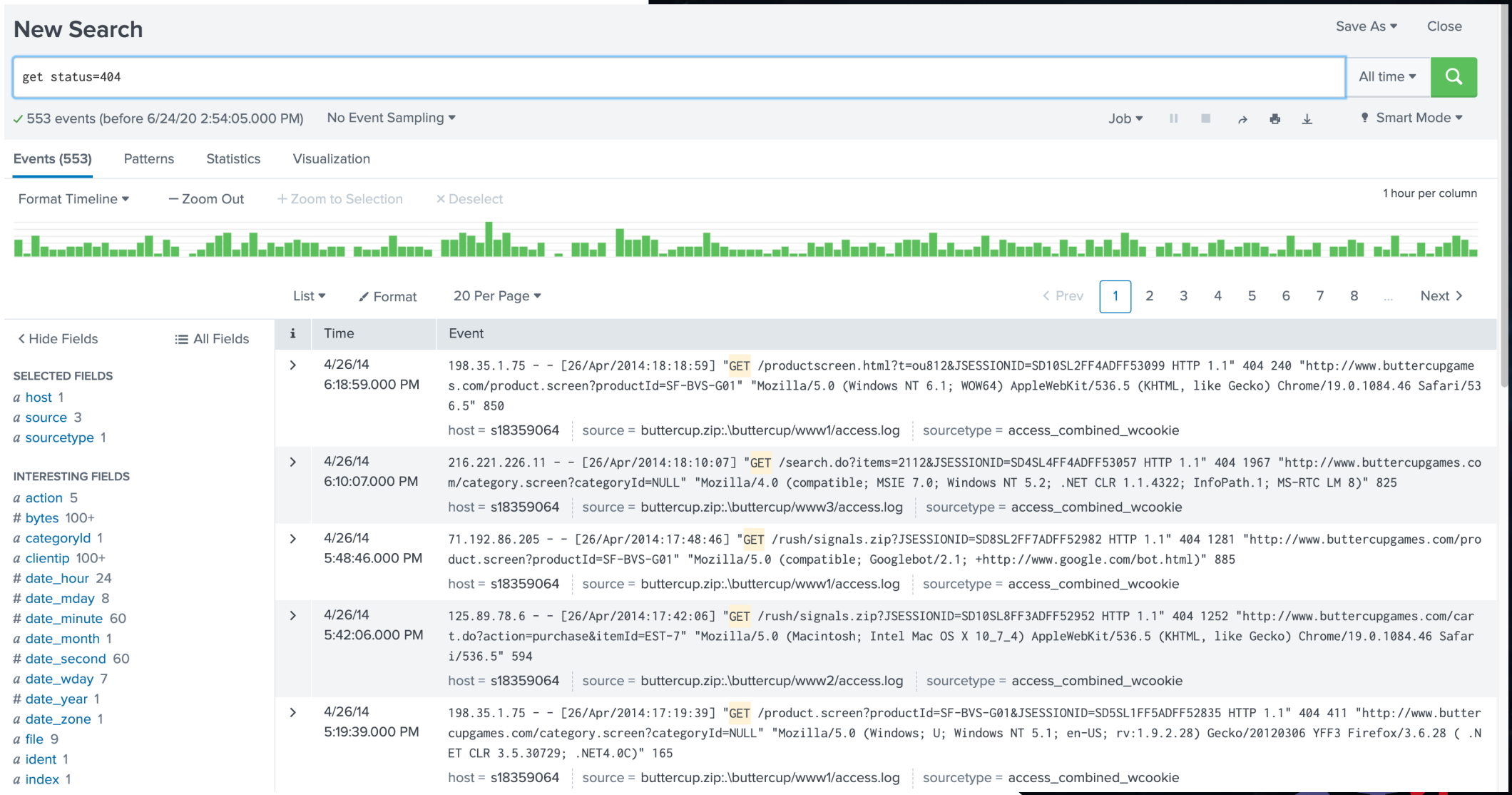

New Search
Save As
Close
get
All time
24,866 events (before 6/24/20 2:46:06.000 PM)
No Event Sampling
Job
Smart Mode
Events (82)
Patterns
Statistics
Visualization
Format Timeline
Zoom Out
Zoom to Selection
Deselect
1 hour per column
Apr 19, 2014 6:00 PM
Apr 19, 2014 7:00 PM
List
Format
20 Per Page
Prev
1
2
3
4
5
Next
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
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=SD4SL5FF3ADFF5111 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

Get

Splunk


List
Format
20 Per Page
Prev
1 2 3 4 5 6 7 8 ... Next
Hide Fields
All Fields
SELECTED FIELDS
a host 1
a source 3
a sourcetype 1
INTERESTING FIELDS
a action 5
bytes 100+
a categoryId 8
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 12
a ident 1
a index 1
a itemId 14
a JSESSIONID 100+
linecount 1
a method 1
other 100+
a productId 16
a punct 96
a referer 100+
a referer_domain 4
a req_time 100+
a splunk_server 1
status 9
timeendpos 7
timestartpos 7
a uri 100+
a uri_path 12
a uri_query 100+
a user 1
a useragent 26
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

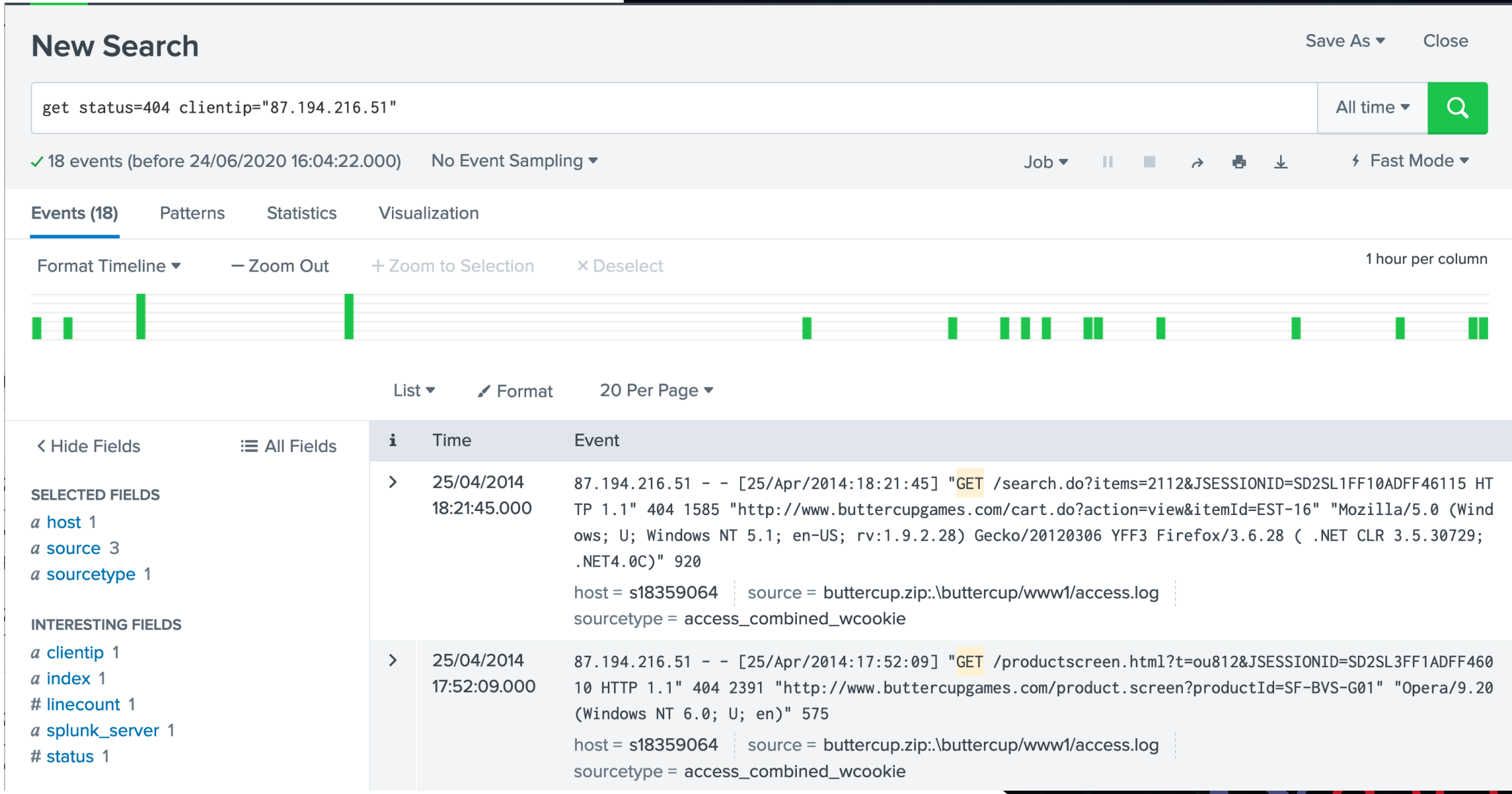
Splunk



Get

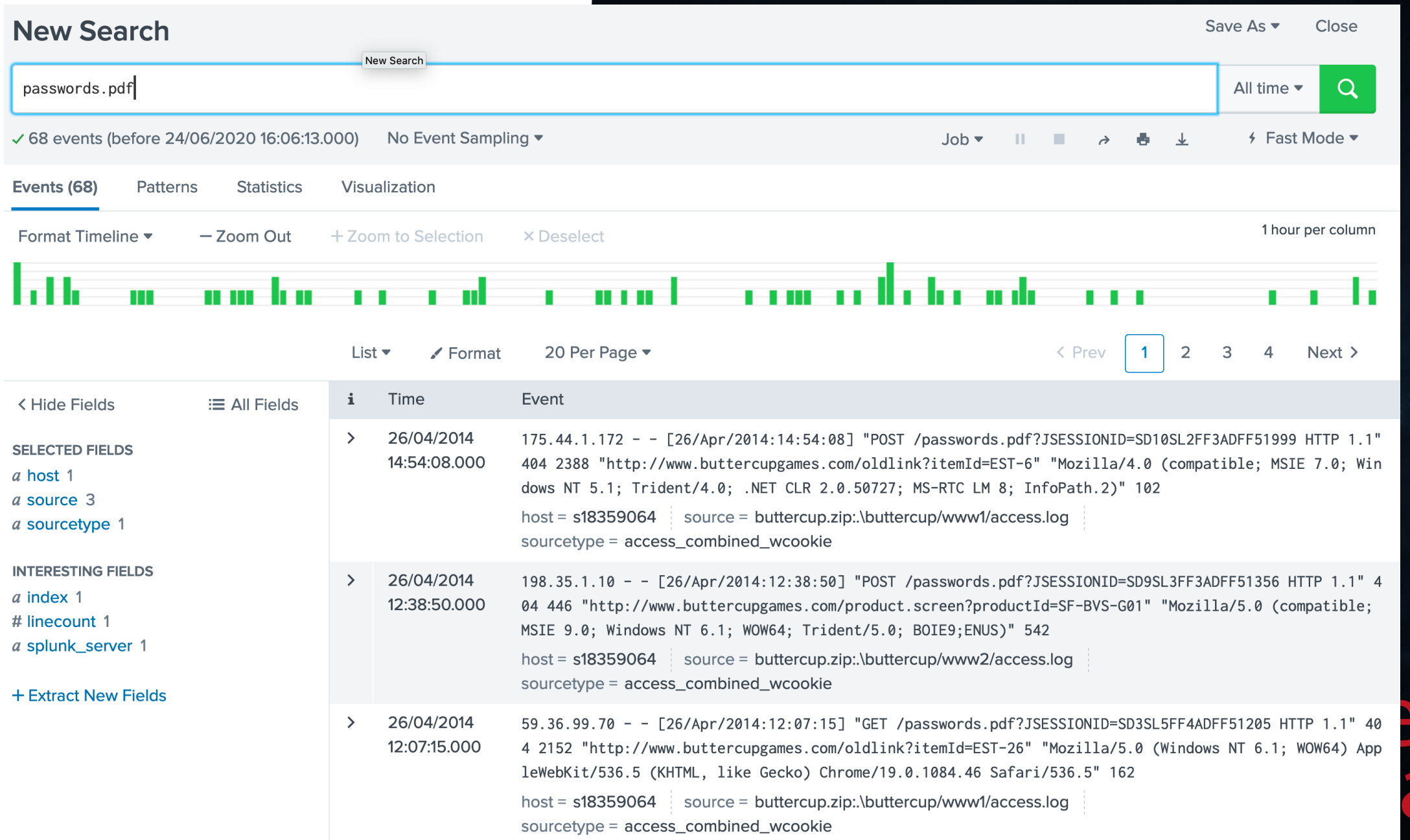
er
&data

Splunk


New Search
Save As
Close
get status=404 clientip="87.194.216.51"
All time
✓ 18 events (before 24/06/2020 16:04:22.000)
No Event Sampling
Job
Fast Mode
Events (18)
Patterns
Statistics
Visualization
Format Timeline
– Zoom Out
+ Zoom to Selection
× Deselect
1 hour per column
List
Format
20 Per Page
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
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 HTTP 1.1" 404 1585 "http://www.buttercupgames.com/cart.do?action=view&itemId=EST-16" "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)" 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=SD2SL3FF1ADFF46010 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

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
Fast Mode
Events (68)
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
Next
Hide Fields
All 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
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

Get

Splunk

New Search

Save As ▾ Close

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

All time ▾

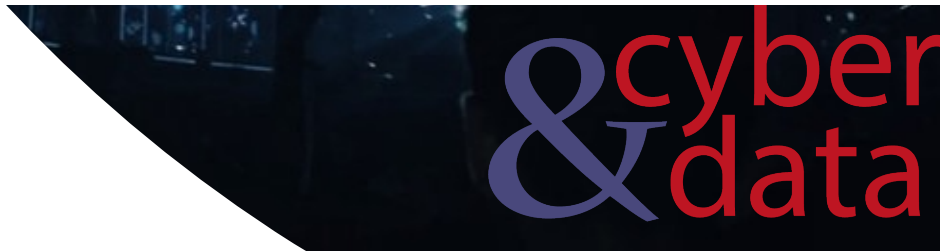
✓ 5,224 events (before 24/06/2020 16:07:35.000) No Event Sampling ▾ Job ▾ Fast Mode ▾

Events Patterns **Statistics (7)** Visualization

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

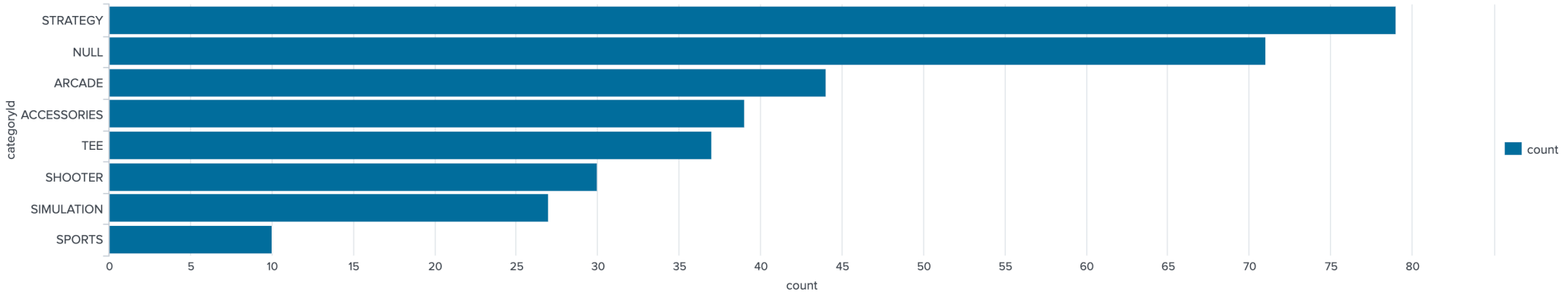
```
sourcetype=access_* status!=200 action=purchase | top categoryId
```

All time

✓ 513 events (before 6/24/20 2:55:46.000 PM) No Event Sampling Job Smart Mode

Events Patterns Statistics (8) **Visualization**

Bar Chart Format Trellis

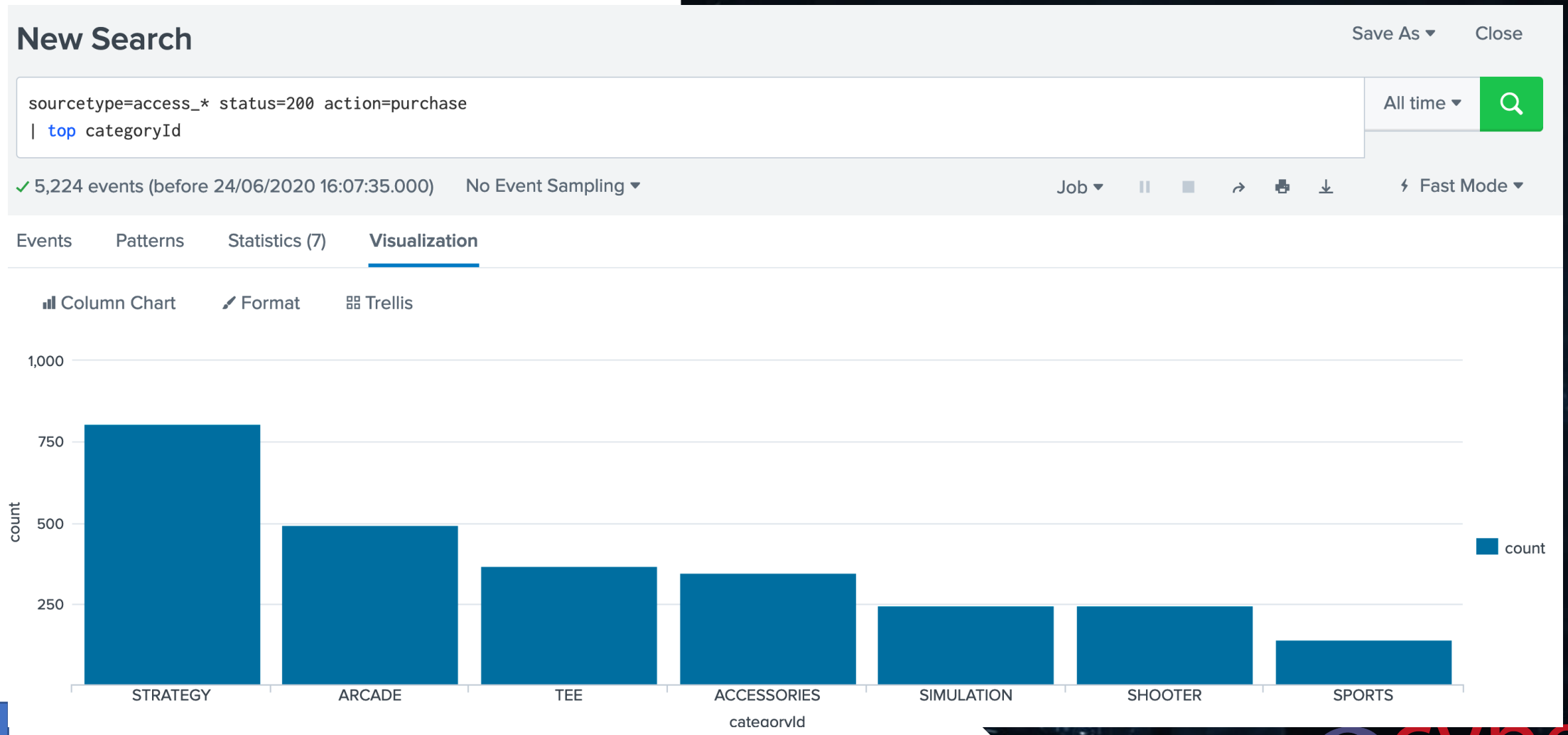


categoryId	count	percent
STRATEGY	79	23.442136
NULL	71	21.068249
ARCADE	44	13.056380
ACCESSORIES	39	11.572700
TEE	37	10.979228
SHOOTER	30	8.902077
SIMULATION	27	8.011869
SPORTS	10	2.967359

Get

&data

Splunk



Get

Splunk

New Search

Save As Close

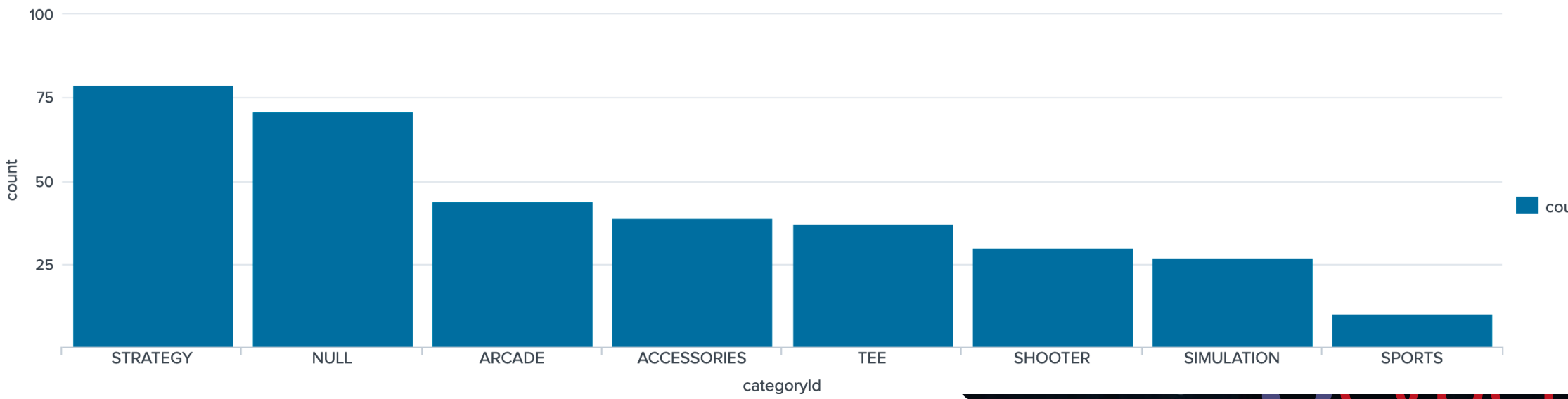
```
sourcetype=access_* status!=200 action=purchase
| top categoryId
```

All time

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

Events Patterns Statistics (8) **Visualization**

Column Chart Format Trellis



Get

&data

Splunk

New Search

New Search

Save As Close

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

All time

✓ 24,866 events (before 24/06/2020 16:11:50.000) No Event Sampling Job Fast Mode

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

Get

&data

Splunk

New Search

Save As Close

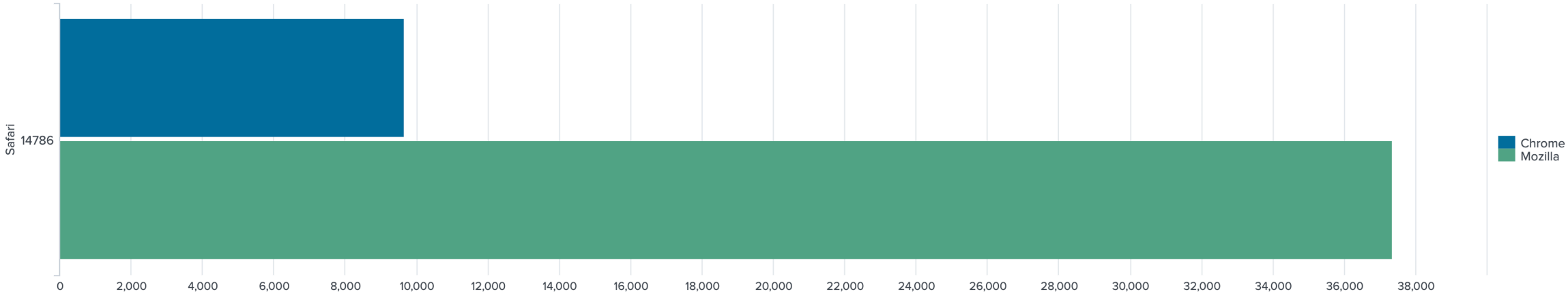
```
sourcetype=access_*
| chart  count(eval(searchmatch("Safari")))  AS Safari,
count(eval(searchmatch("Chrome")))  AS Chrome, count(eval(searchmatch("Mozilla"))) AS Mozilla
```

All time

✓ 39,532 events (before 6/24/20 2:56:56.000 PM) No Event Sampling Job Smart Mode

Events Patterns Statistics (1) **Visualization**

Bar Chart Format Trellis



Safari	Chrome	Mozilla
14786	9651	37346

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

cyber & data

"From bits to information"

Introduction to Splunk