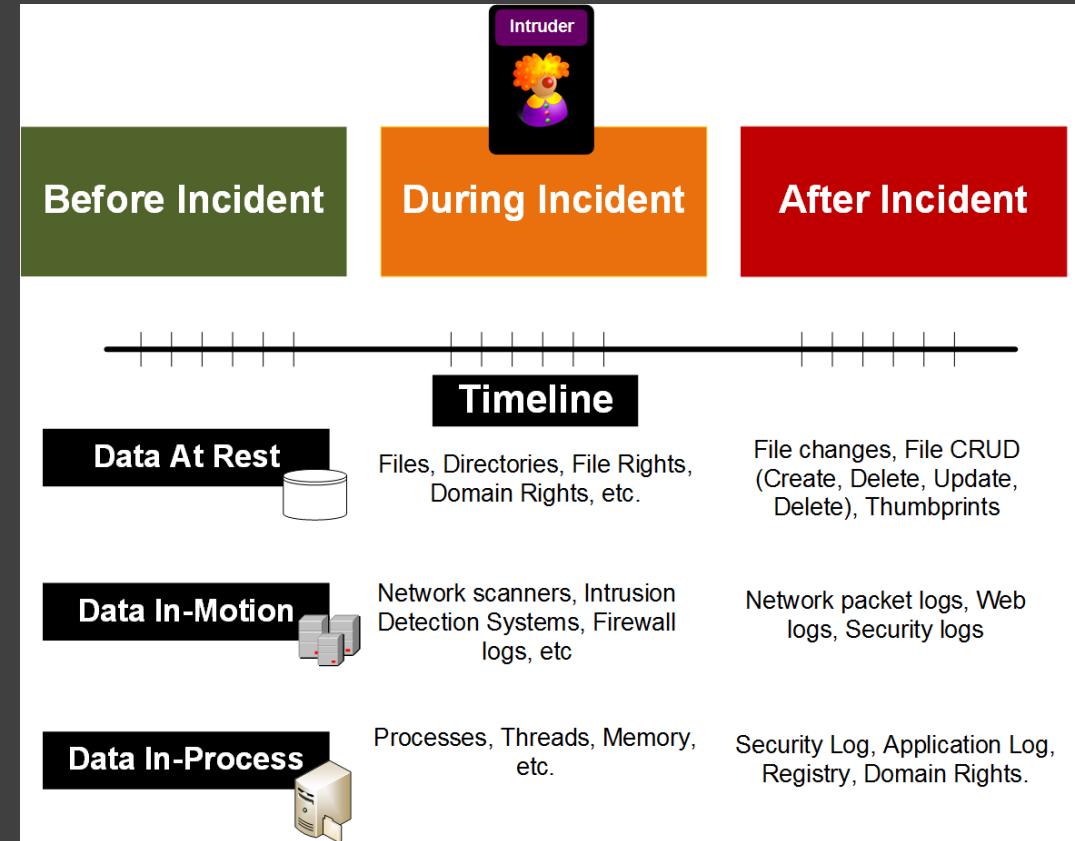
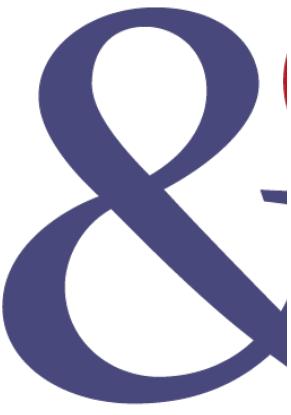


cyber & data

“From bits to information”

Introduction to Splunk





“From bits to

No	Date	Subject	Lab
2	18 Sept 2025	1. Introduction [Link] 2. Intrusion Detection Systems [Link]	Network Security Lab 1
3	25 Sept 2025	3. Network Security (Risks and Models) [Link]	Network Security Lab 2
4	2 Oct 2025	4. Ciphers and Fundamentals [Link]	AWS Security and Server Infrastructure Lab 3
5	9 Oct 2025	5. Secret Key 6. Hashing [Link]	Symmetric Key and Hashing Lab 4
6	16 Oct 2025	7. Public Key [Link] 8. Key Exchange [Link]	Public Key and Key Exchange Lab 5
7	23 Oct 2025	Reading week/Revision session	Reading week/Cipher Challenge
8	30 Oct 2025	9. Digital Certificates	Certificates Lab 6
9	6 Nov 2025	Test 1 here (6-8pm, JKCC)	
10	13 Nov 2025	10 Network Forensics here	Network Forensics Lab 7
11	20 Nov 2025	11. Splunk here	Splunk Lab Lab 8
12	27 Nov 2025	13. Tunnelling Here	Tunnelling Lab 9
13	4 Dec 2025	14. Blockchain and Cryptocurrencies here	Blockchain Lab. here
14	11 Dec 2025		
15	18 Dec 2025	Hand-in: TBC [Here]	

After Incident

changes, File CRUD (Create, Delete, Update, etc), Thumbprints

Network packet logs, Web logs, Security logs

System Log, Application Log, Directory, Domain Rights.

cyber & data

“From bits to information”

Memory, Big Data
and SIEM

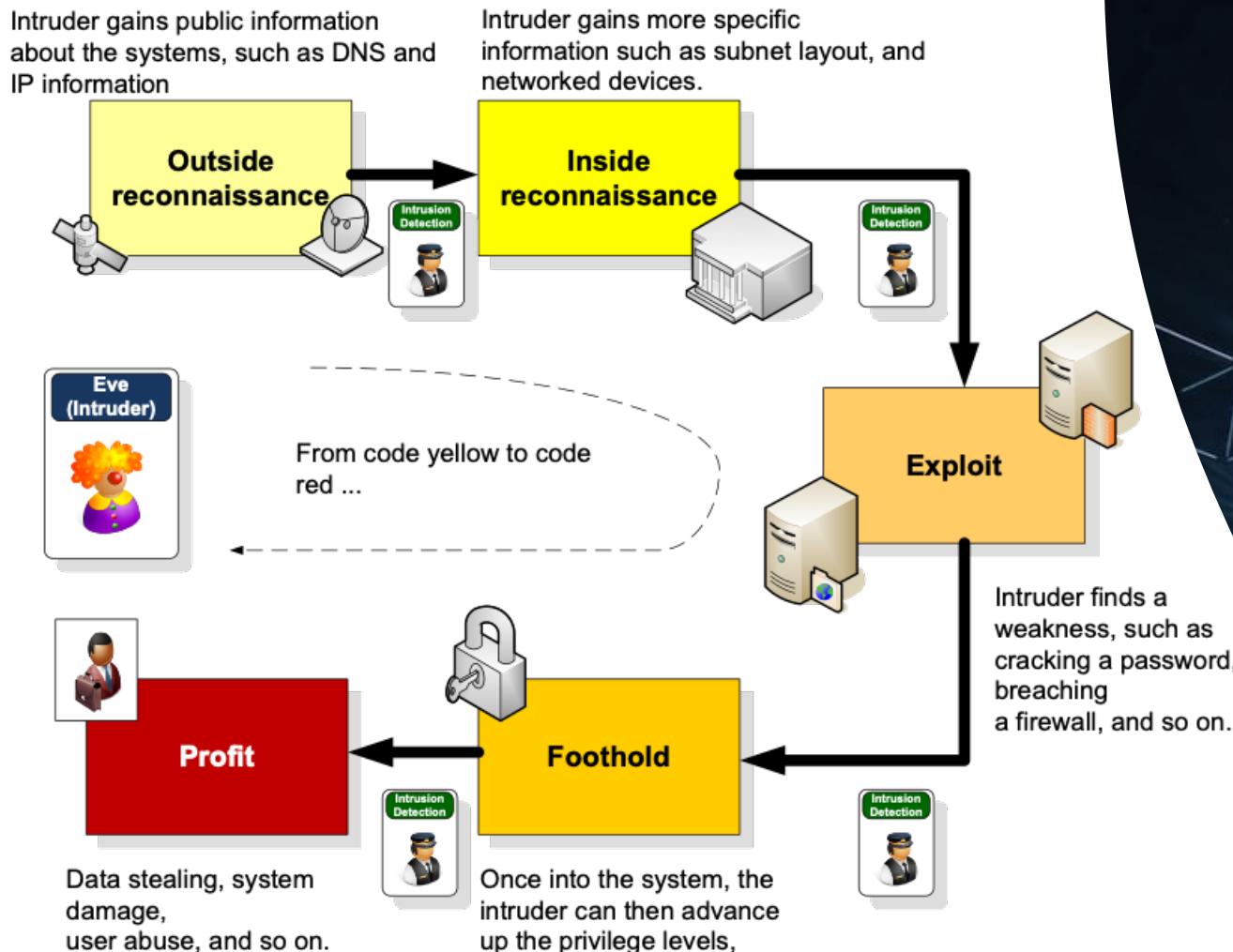
Outline

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



cyber
& data

Intrusion Patterns



Kill Chain graphic: https://en.wikipedia.org/wiki/Kill_chain



cyber
& data

Intrusion Patterns

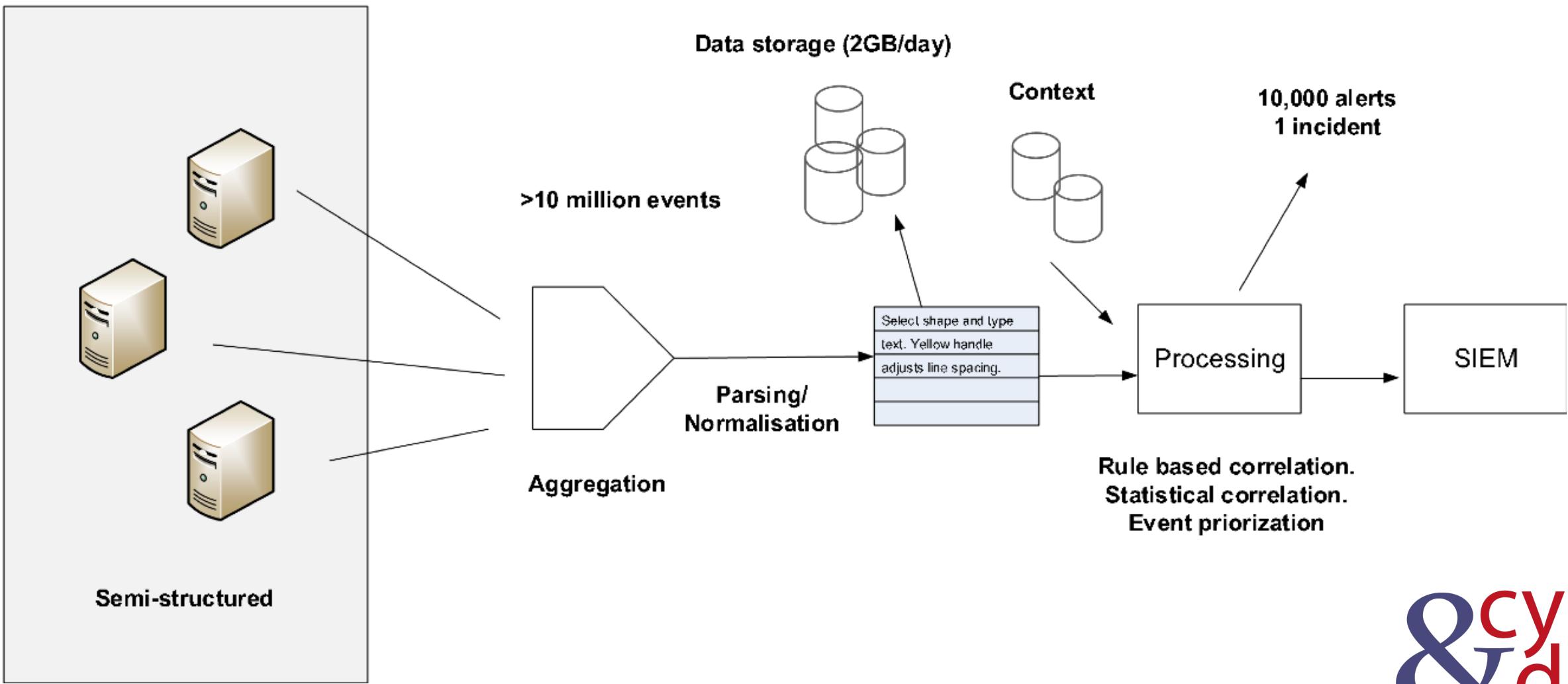
Phases of the Intrusion Kill Chain



Kill Chain graphic: https://en.wikipedia.org/wiki/Kill_chain



Outline



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.



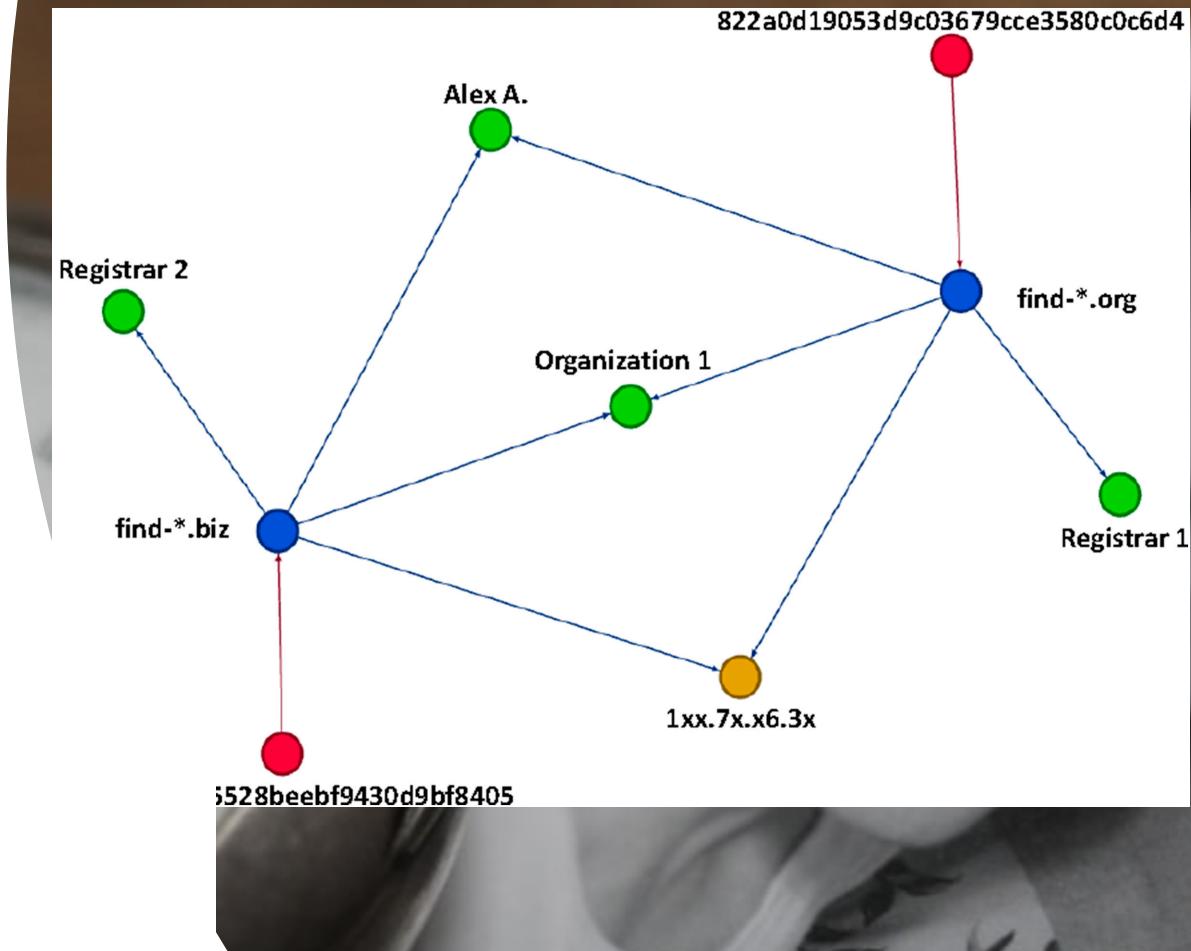
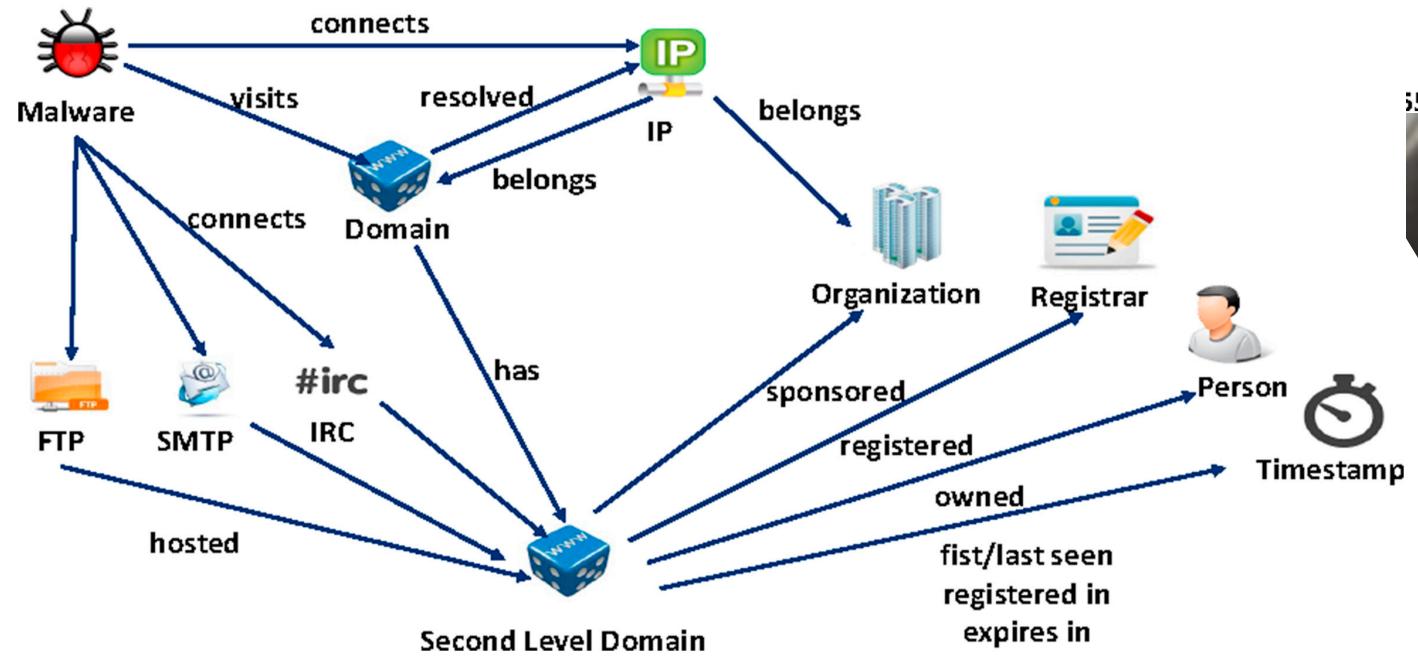
cyber
& data

cyber & data

“From bits to information”

Directed Graphs and Cyber Threats

Directed Graphs



cyber
&
data

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

26/04/2014 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	<input checked="" type="checkbox"/> Field	Value	Actions
Event	<input type="checkbox"/> JSESSIONID ▾	SD6SL7FF7ADFF53113	▼
	<input type="checkbox"/> bytes ▾	1665	▼
	<input type="checkbox"/> clientip ▾	91.205.189.15	▼

clientip X

>100 Values, 100% of events

Selected

Yes

No

Reports

[Top values](#) [Top values by time](#)

[Rare values](#)

[Events with this field](#)

Top 10 Values

Count

%

87.194.216.51

651

2.618%

211.166.11.101

473

1.902%

128.241.220.82

364

1.464%

194.215.205.19

316

1.271%

188.138.40.166

276

1.11%

109.169.32.135

257

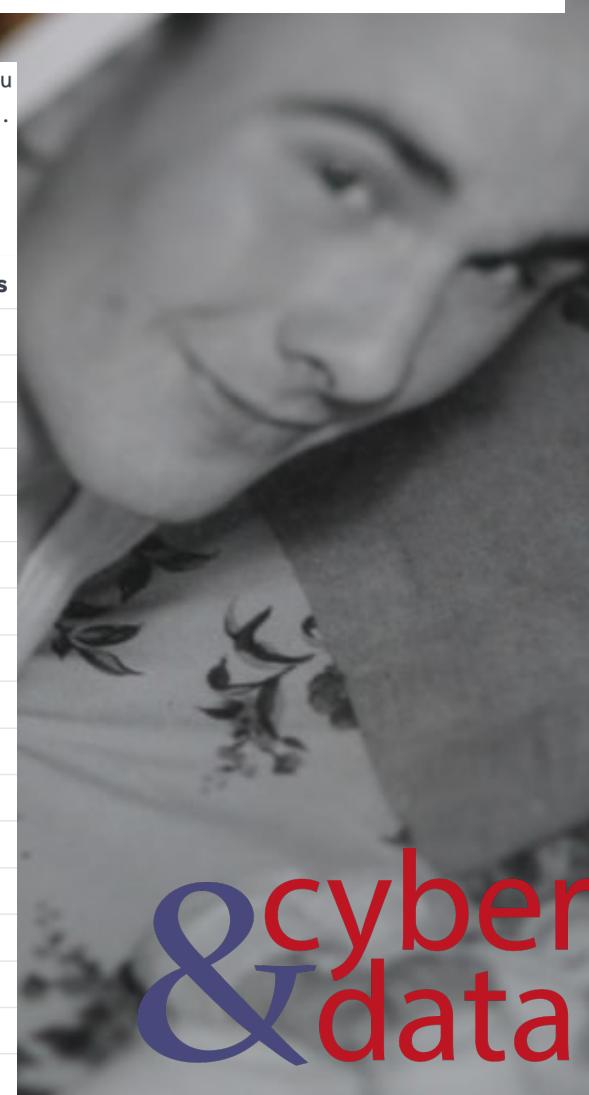
1.034%

k?itemId=EST-14

D6SL7FF7ADFF53113

F7ADFF53113

AppleWebKit/536.5 (KHTML, like Gecko) Chrome/19.0.1084.46 Safari/



cyber
& data

cyber & data

“From bits to information”

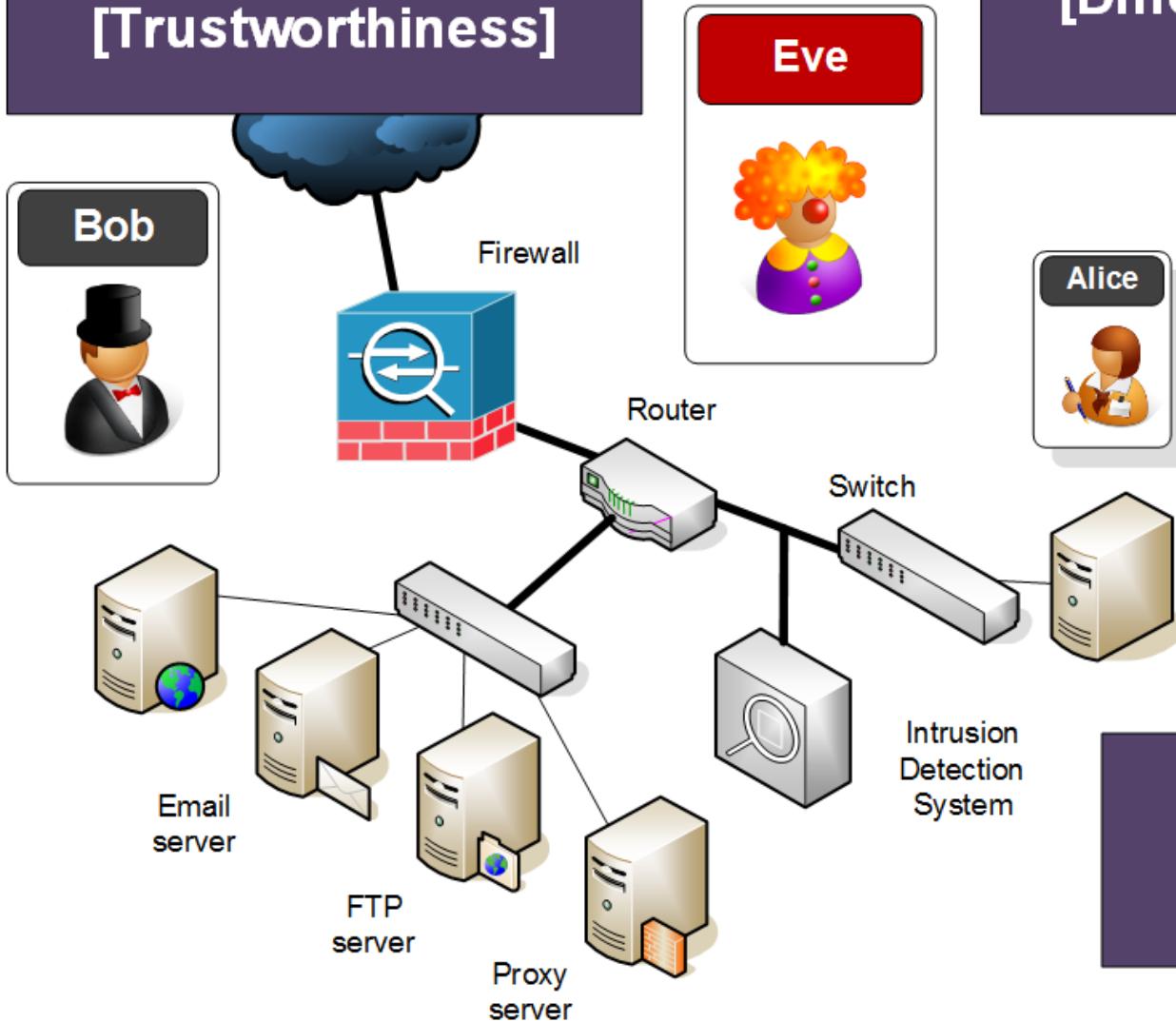
The V's of Data

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]

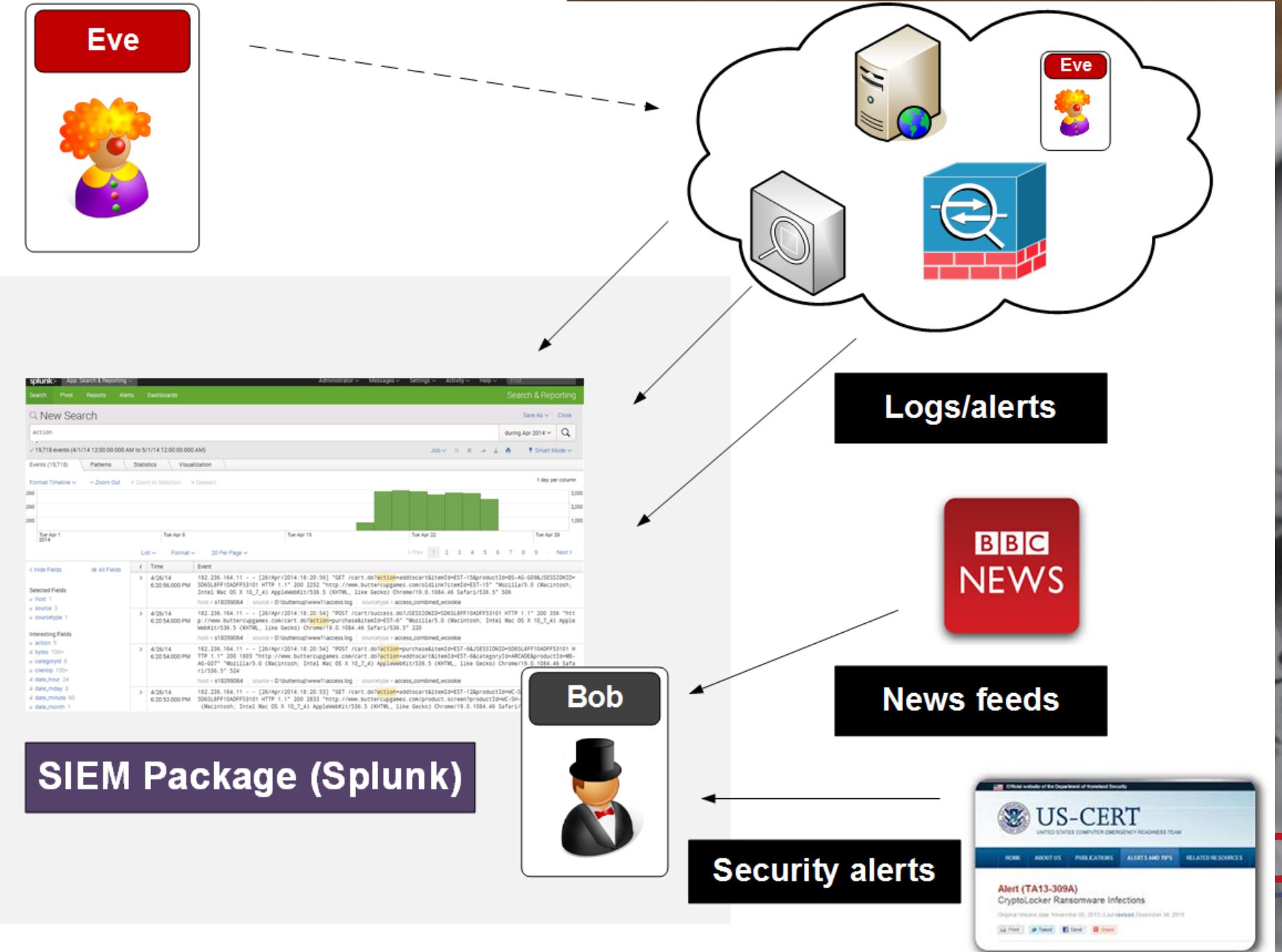
/ber
data

cyber & data

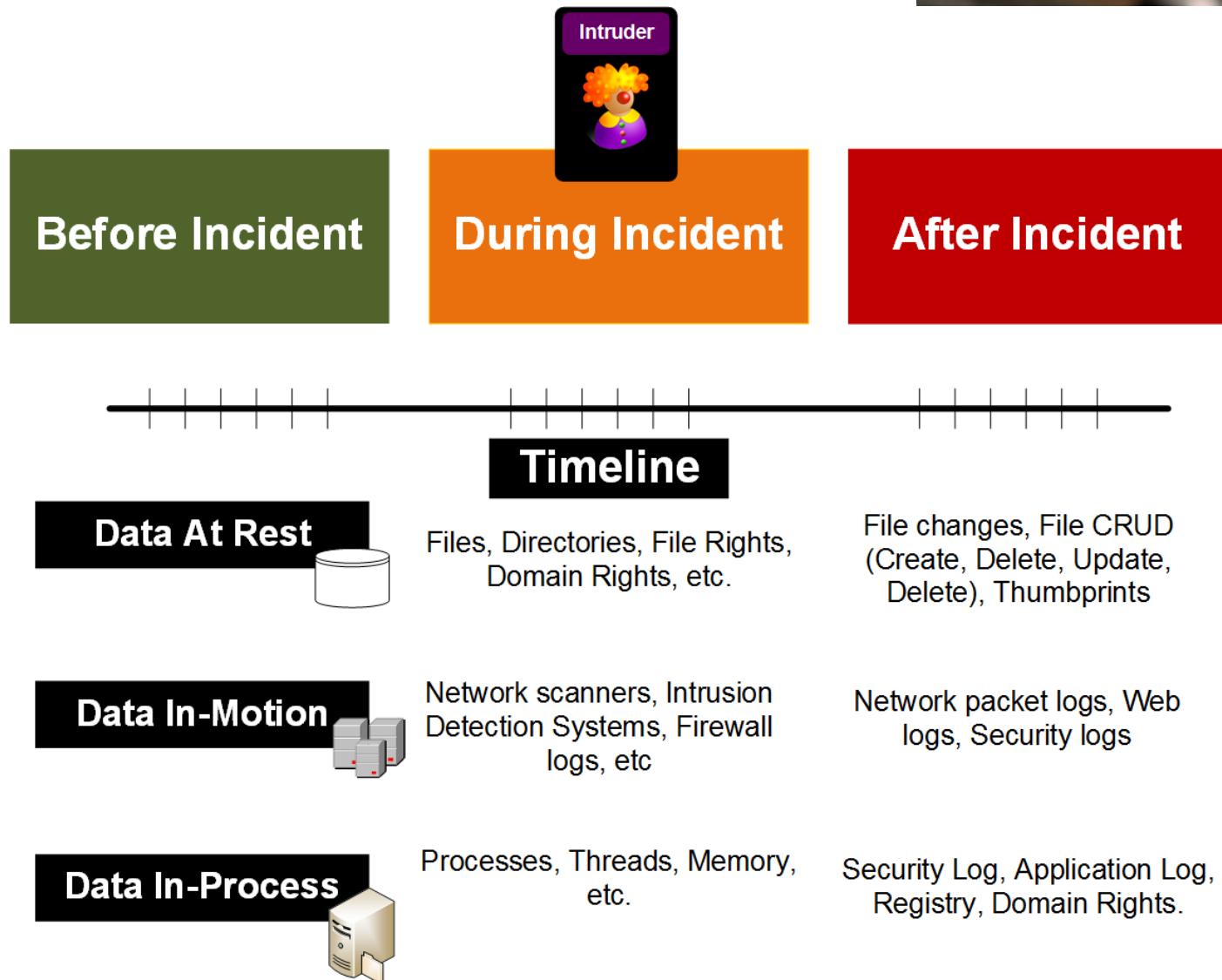
“From bits to information”

Data Gathering

Outline

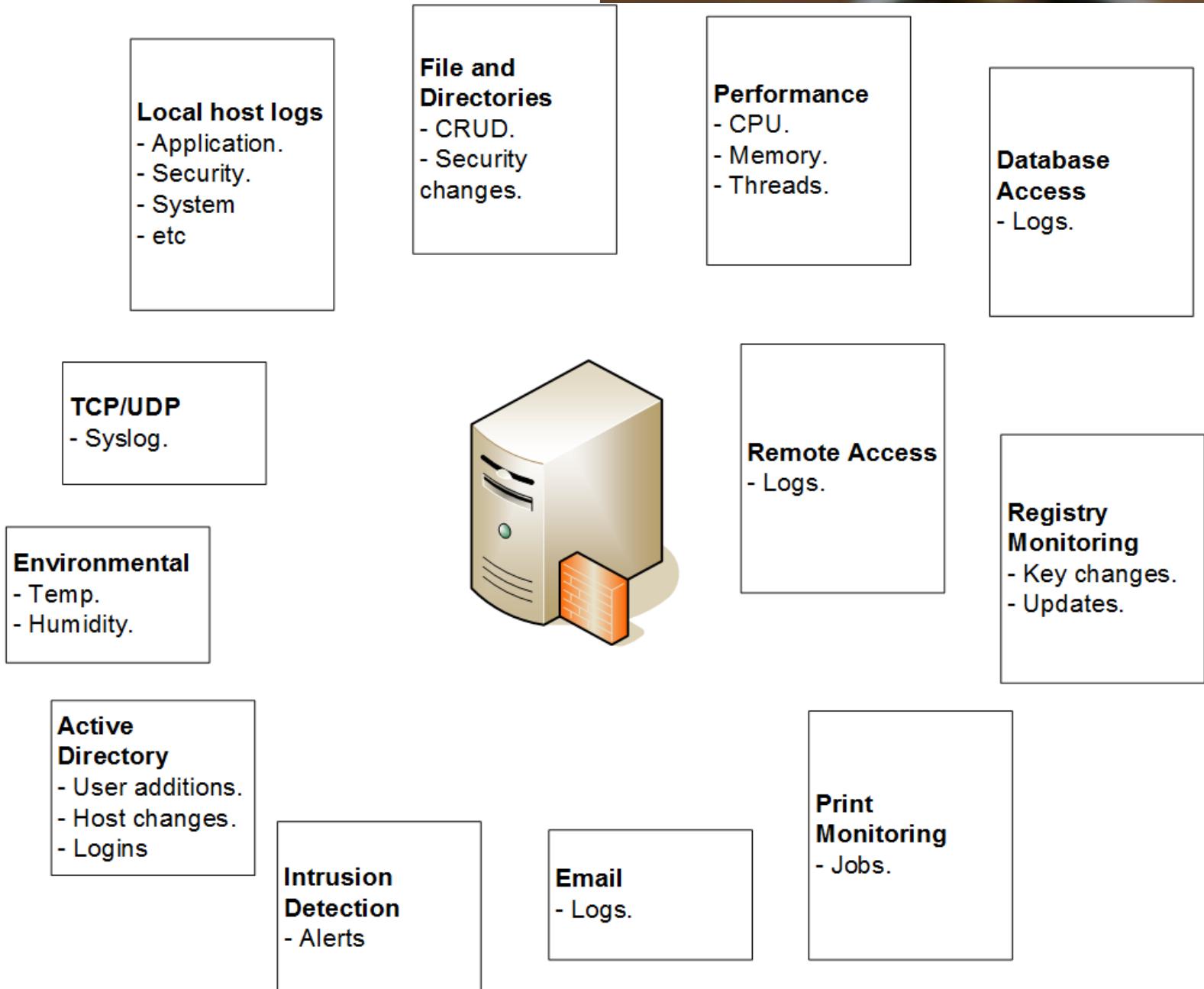


Outline



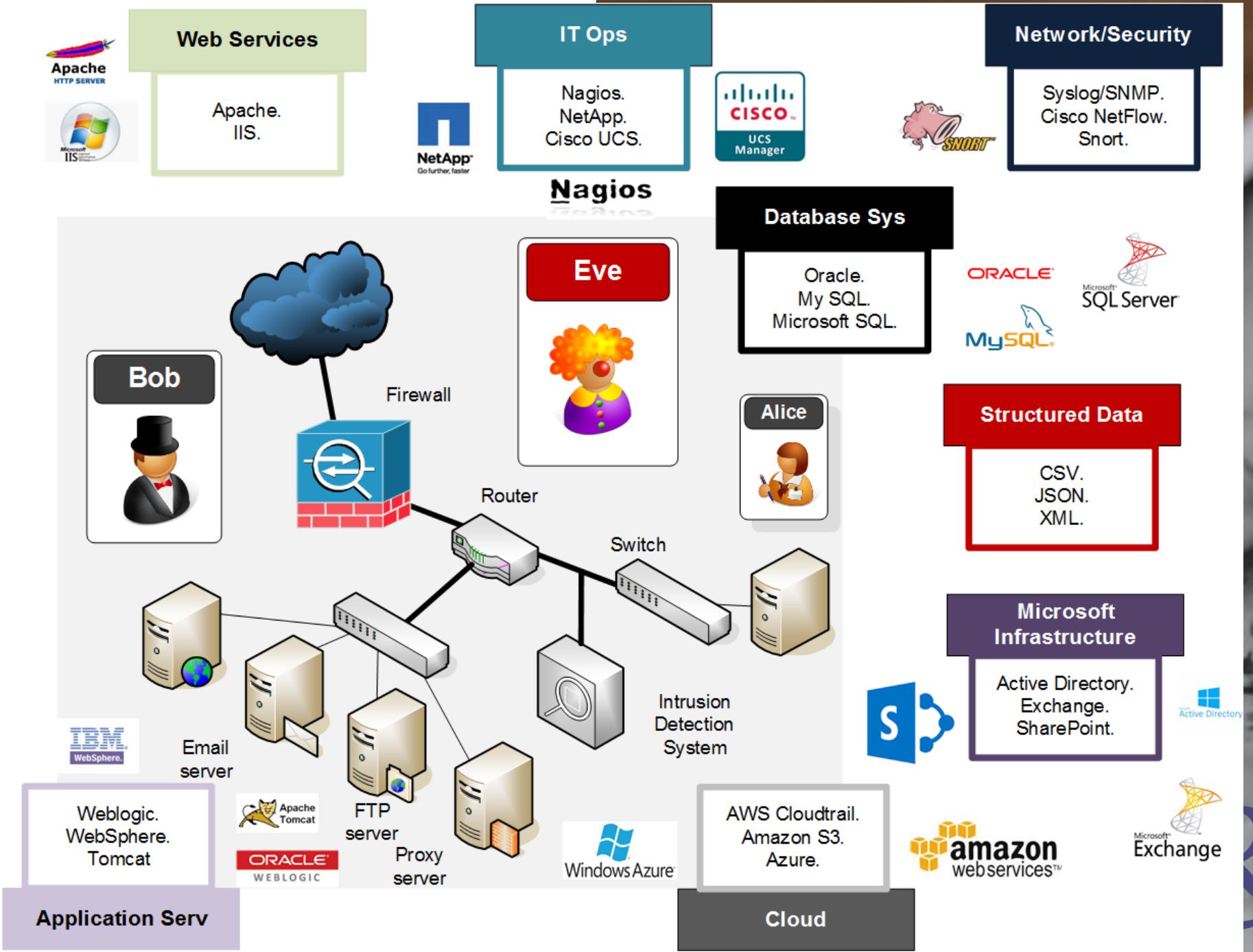
cyber
& data

Outline

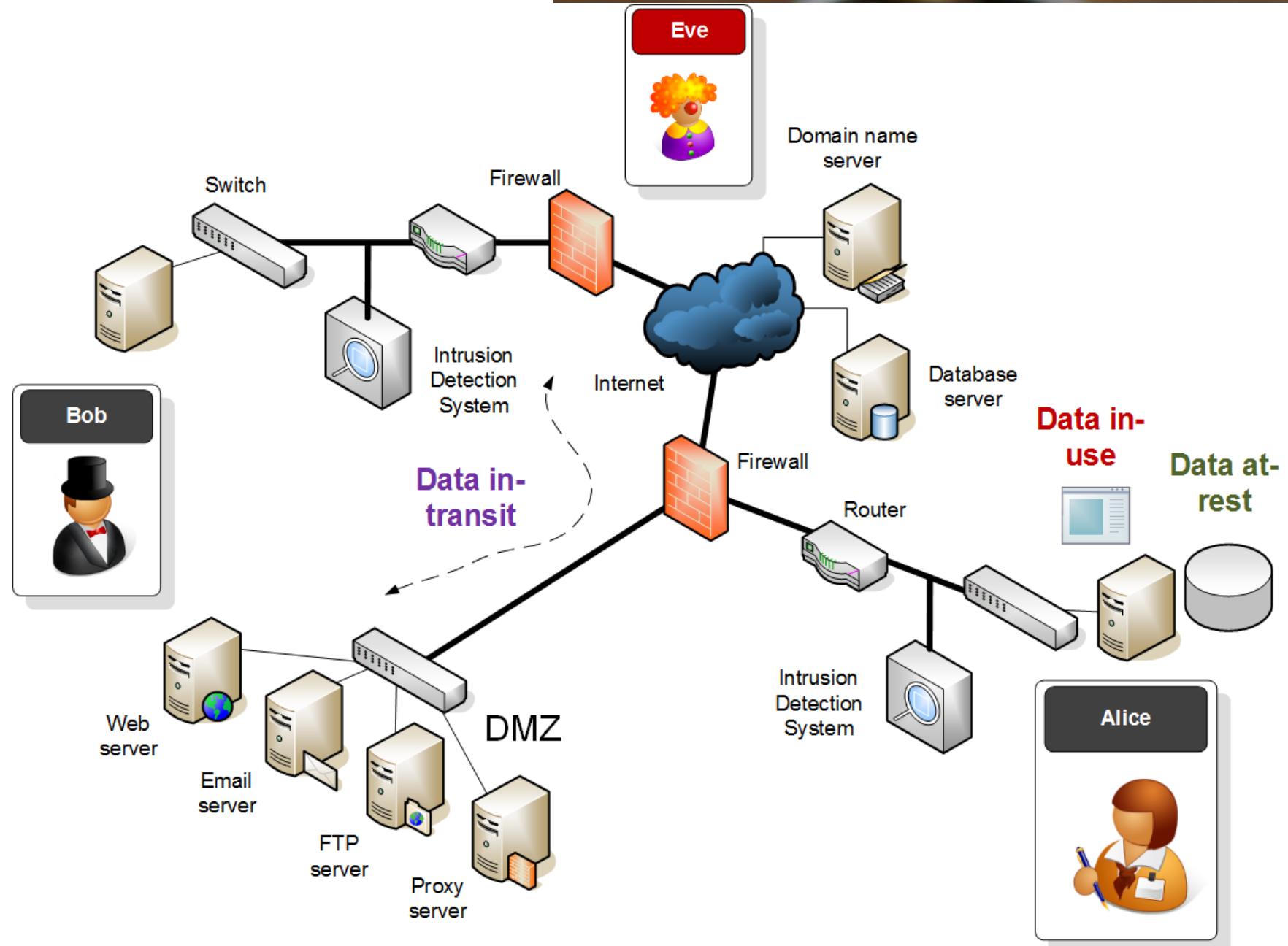


cyber
& data

Outline



Outline

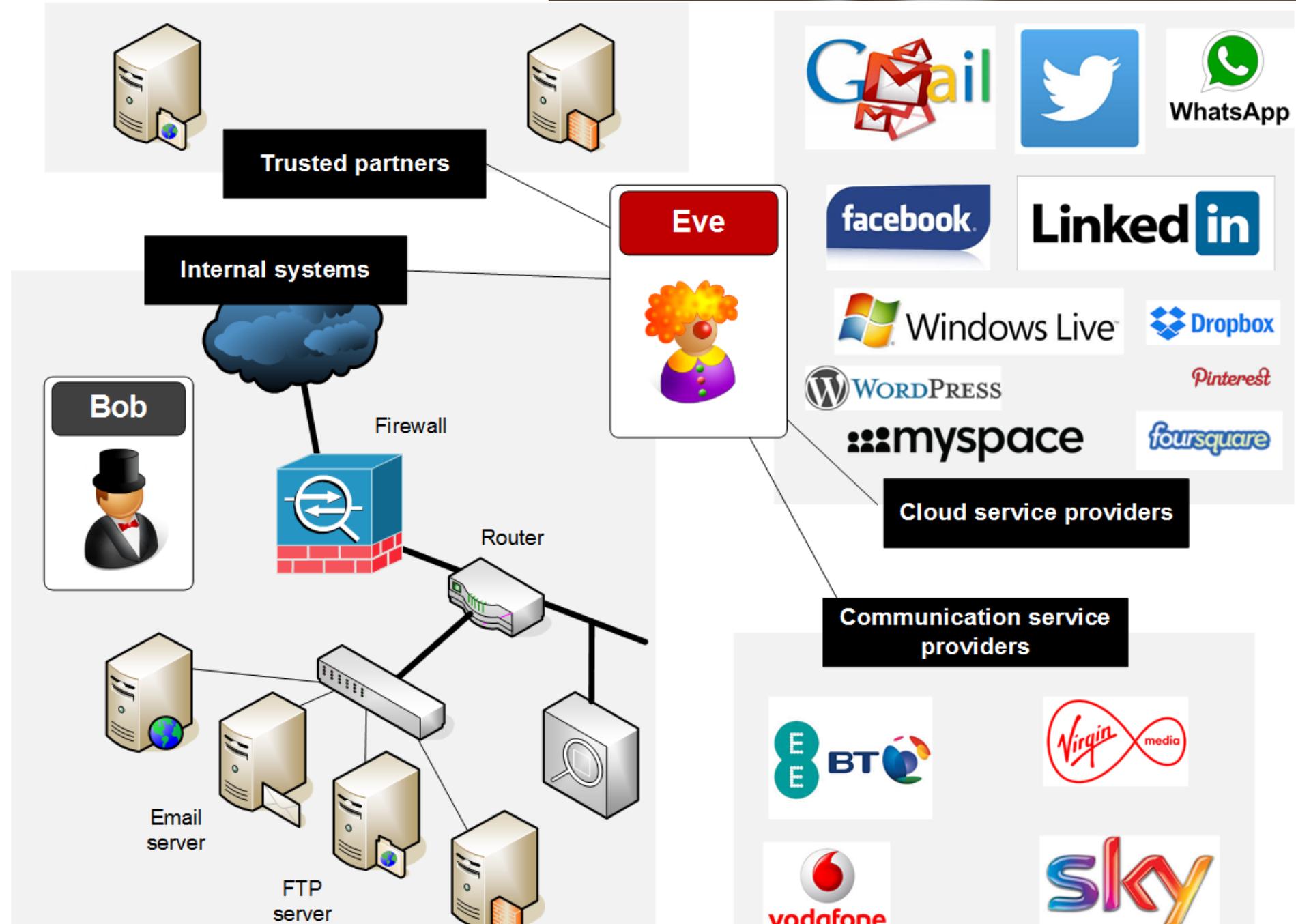


cyber & data

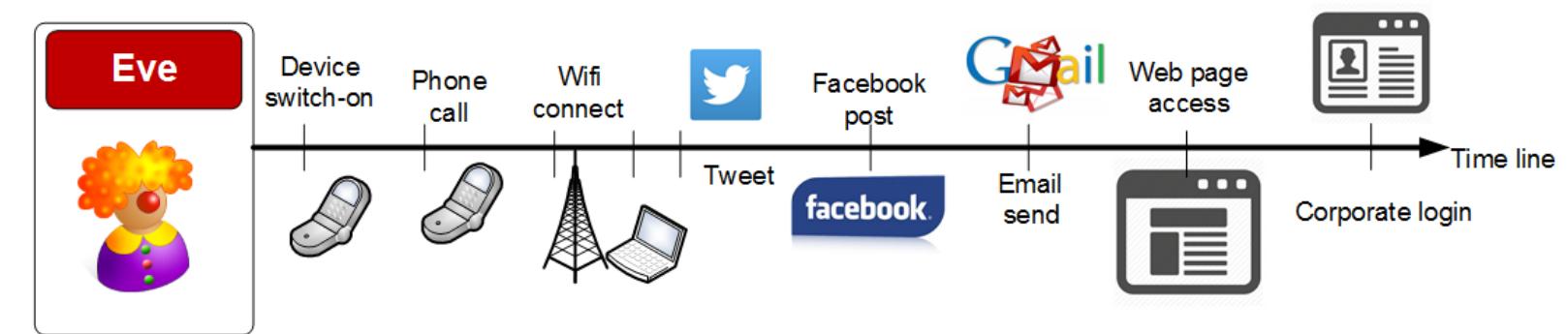
“From bits to information”

Timelines

Outline



Outline



Cloud service providers



Logs/Email

Communication service providers



Call record



Web log

Web services



Web/Domain Log

Device logs

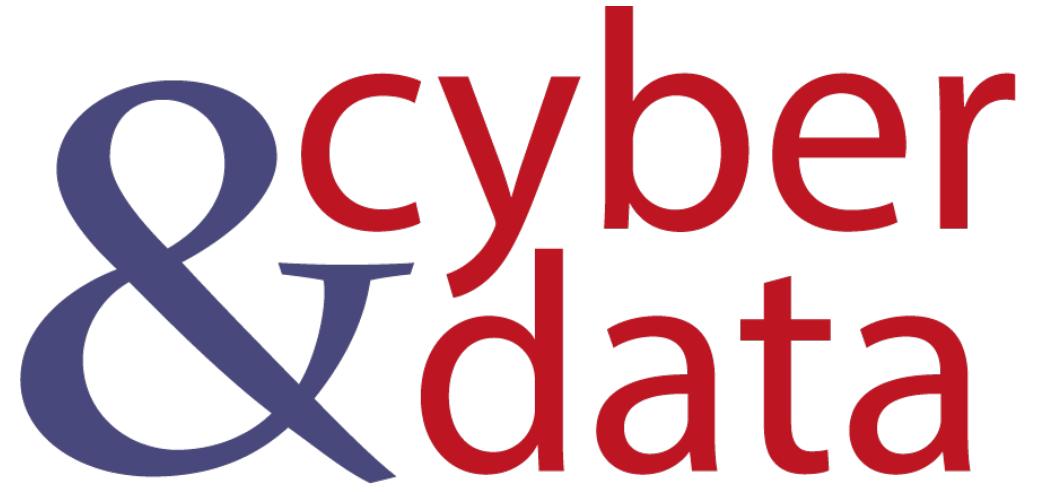


System Log



Internet cache

cyber
& data



“From bits to information”

Introduction to Splunk



Logstalgia: <https://www.youtube.com/watch?v=HeWfkPeDQbY>

Threat model: <https://threatmap.checkpoint.com/>

Threat model: <https://cybermap.kaspersky.com/>

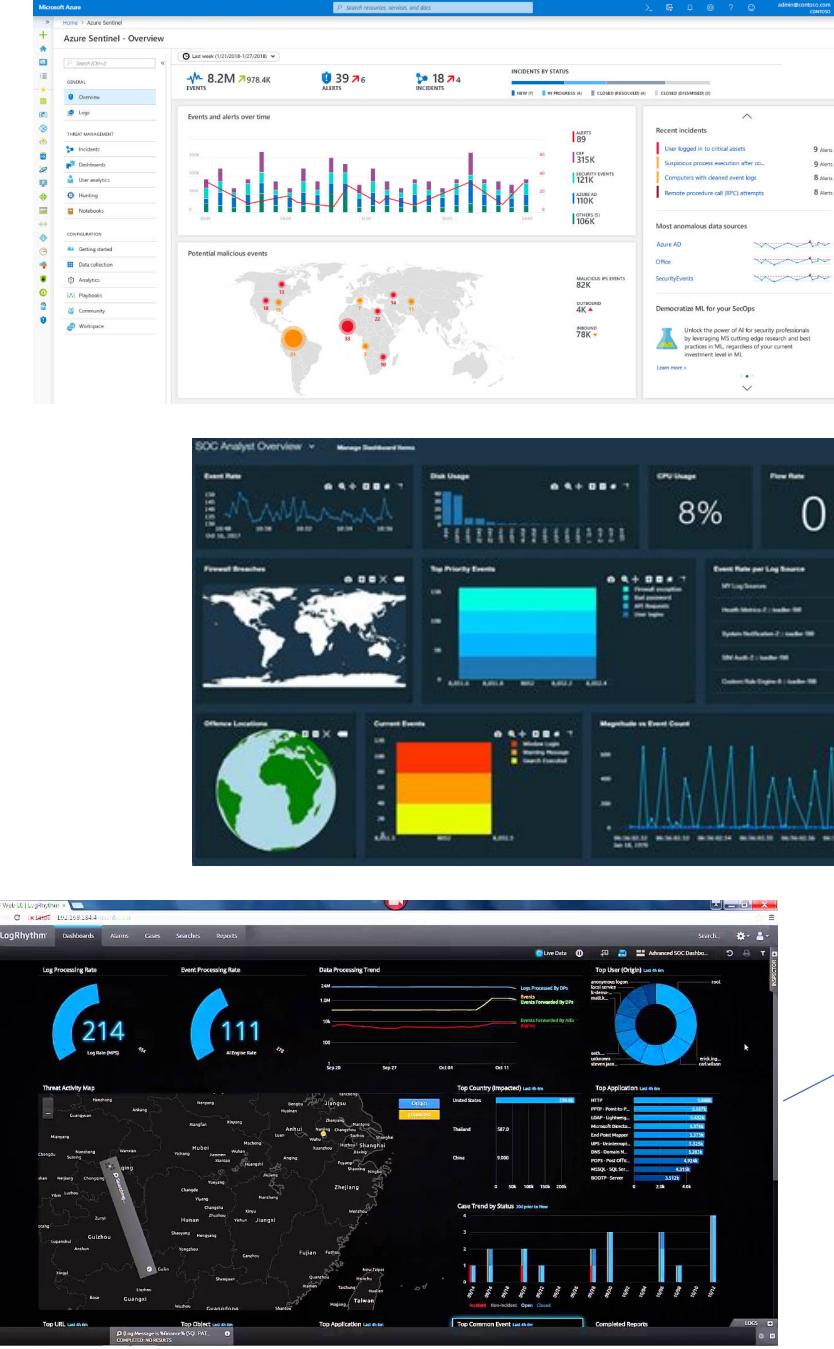


Figure 1: Magic Quadrant for Security Information and Event Management



Get

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.

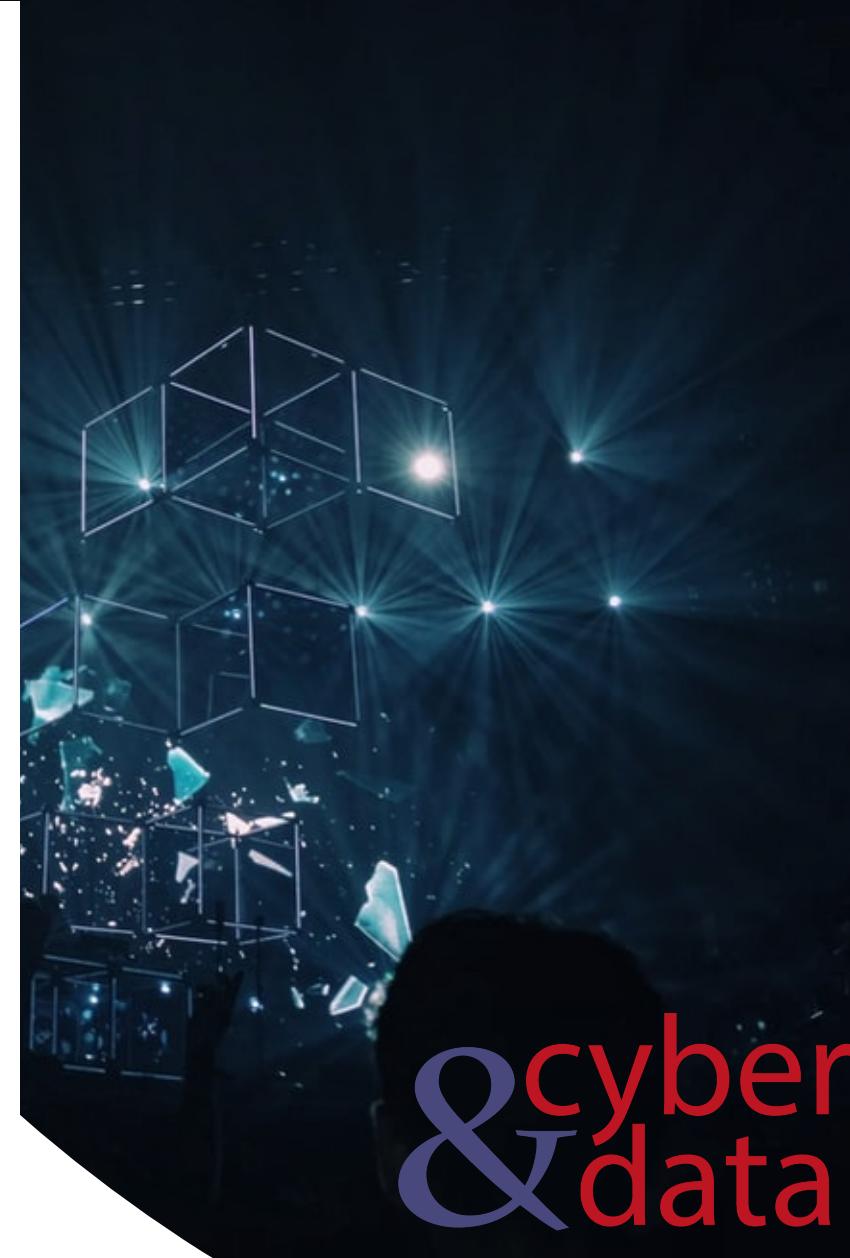
Monitor and Test Networks
Track/monitor accesses. Perform security tests.



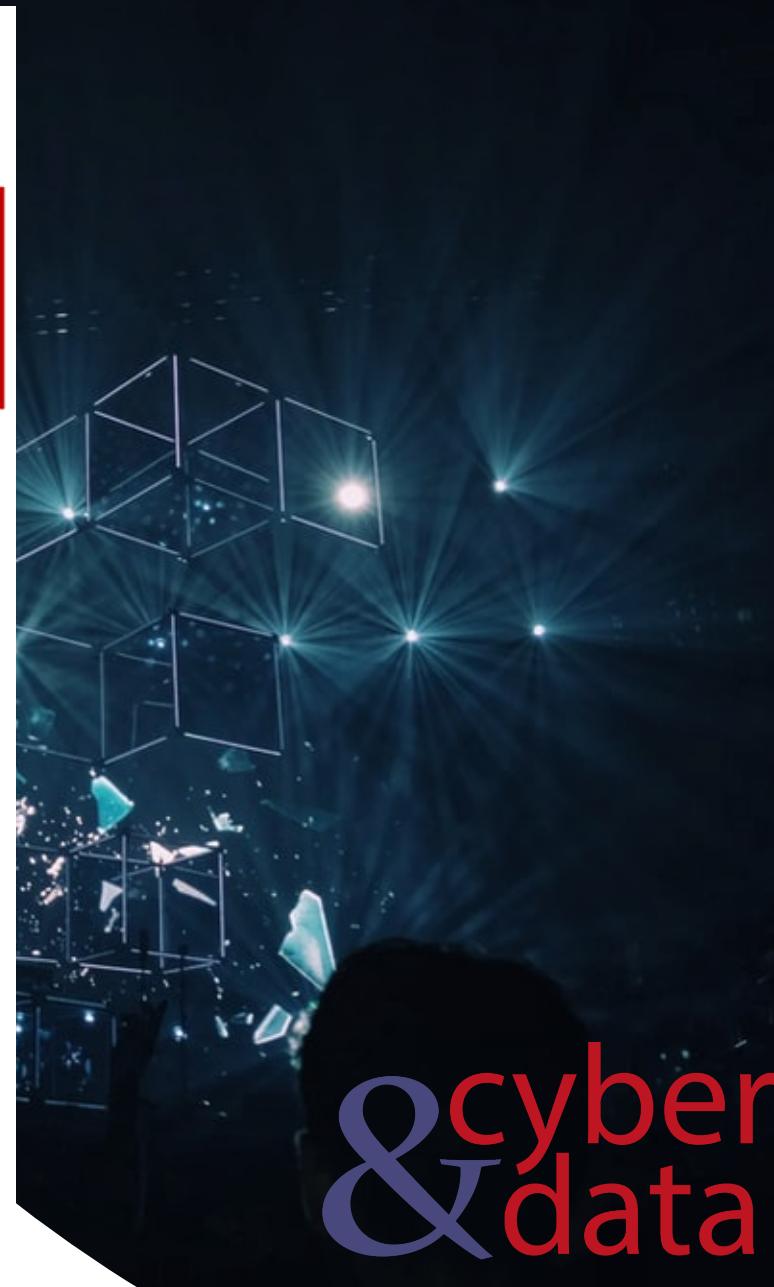
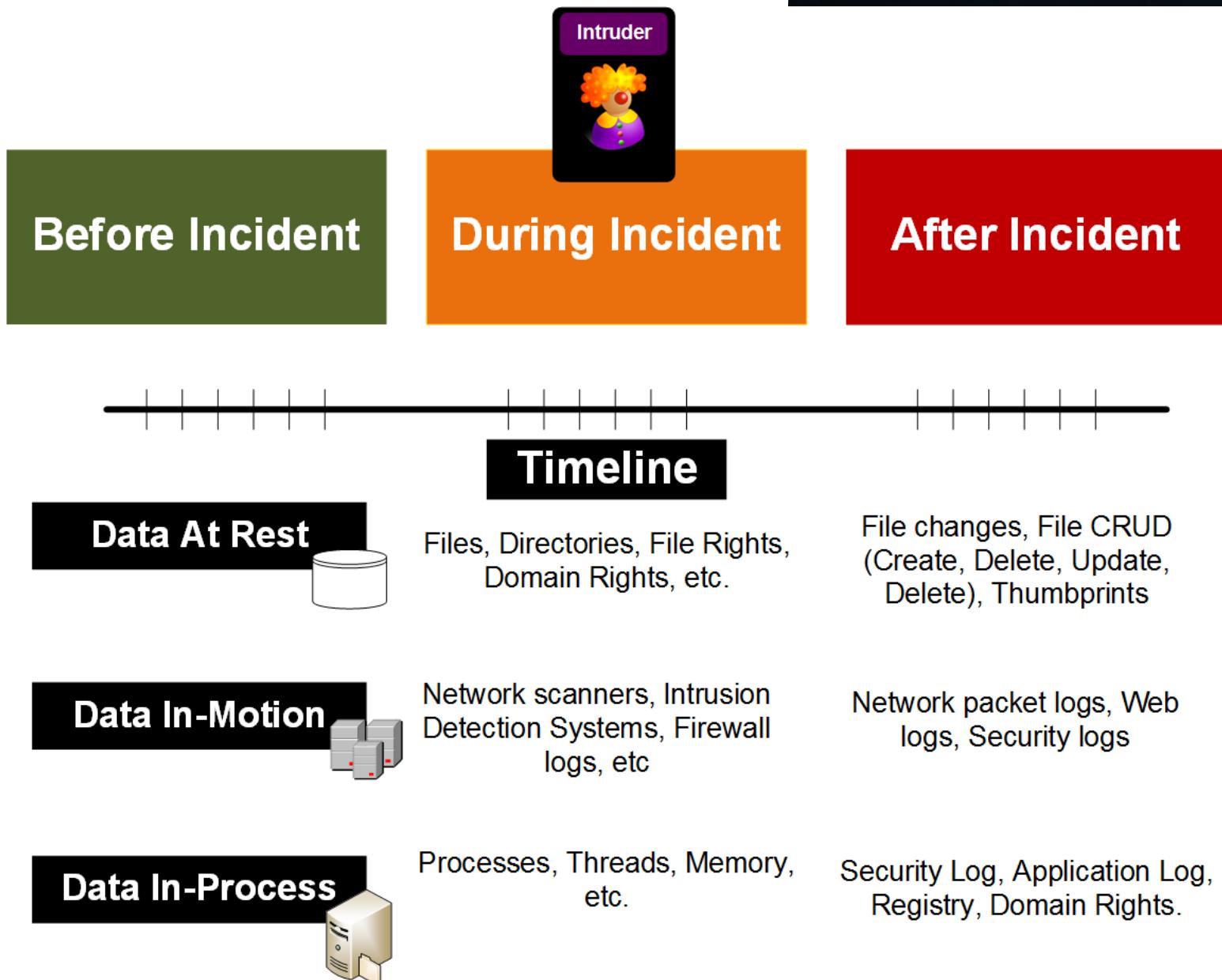
Maintain Vulnerability Management Program
Anti-virus. Develop/maintain secure systems and apps.



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



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.

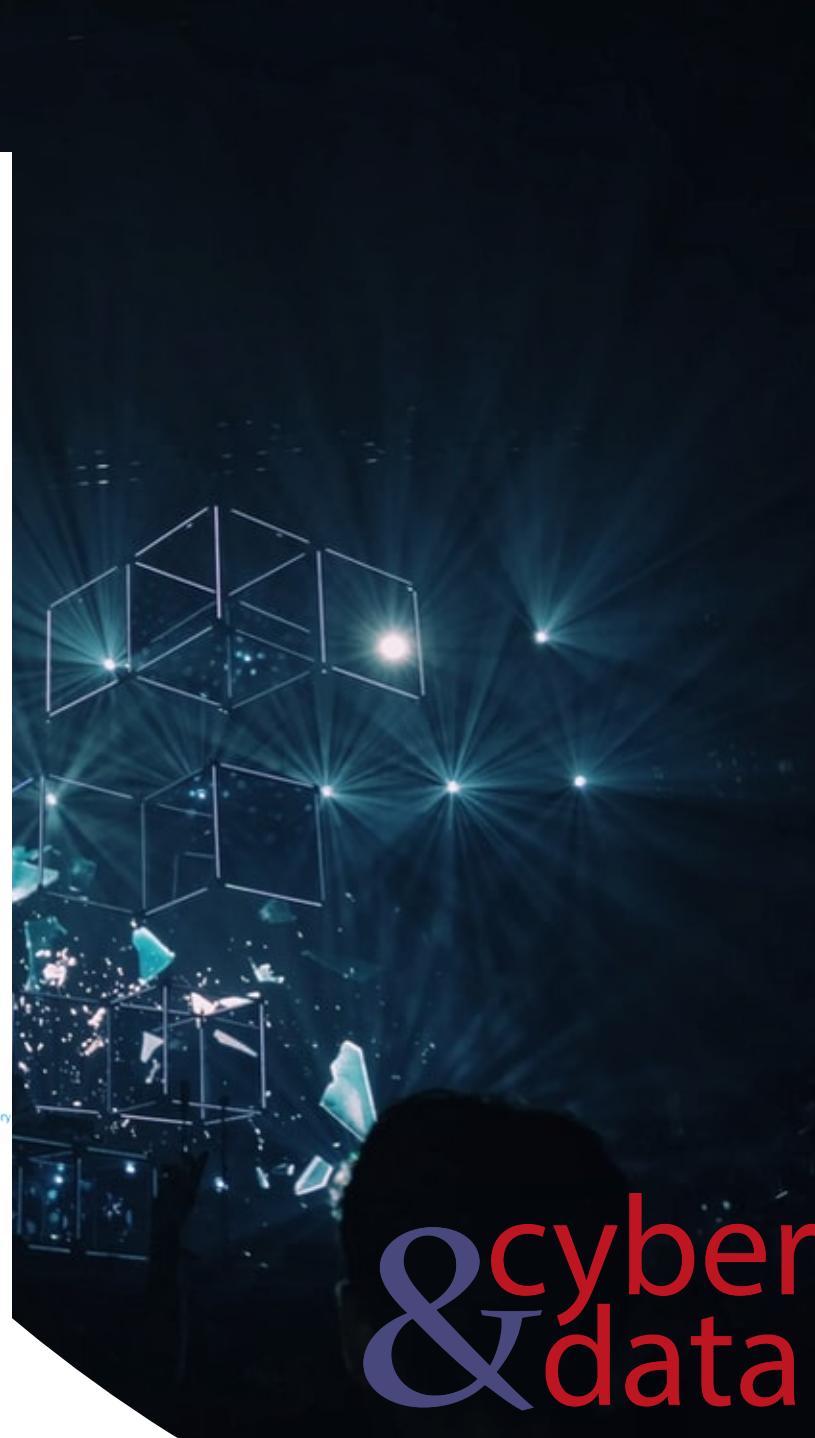
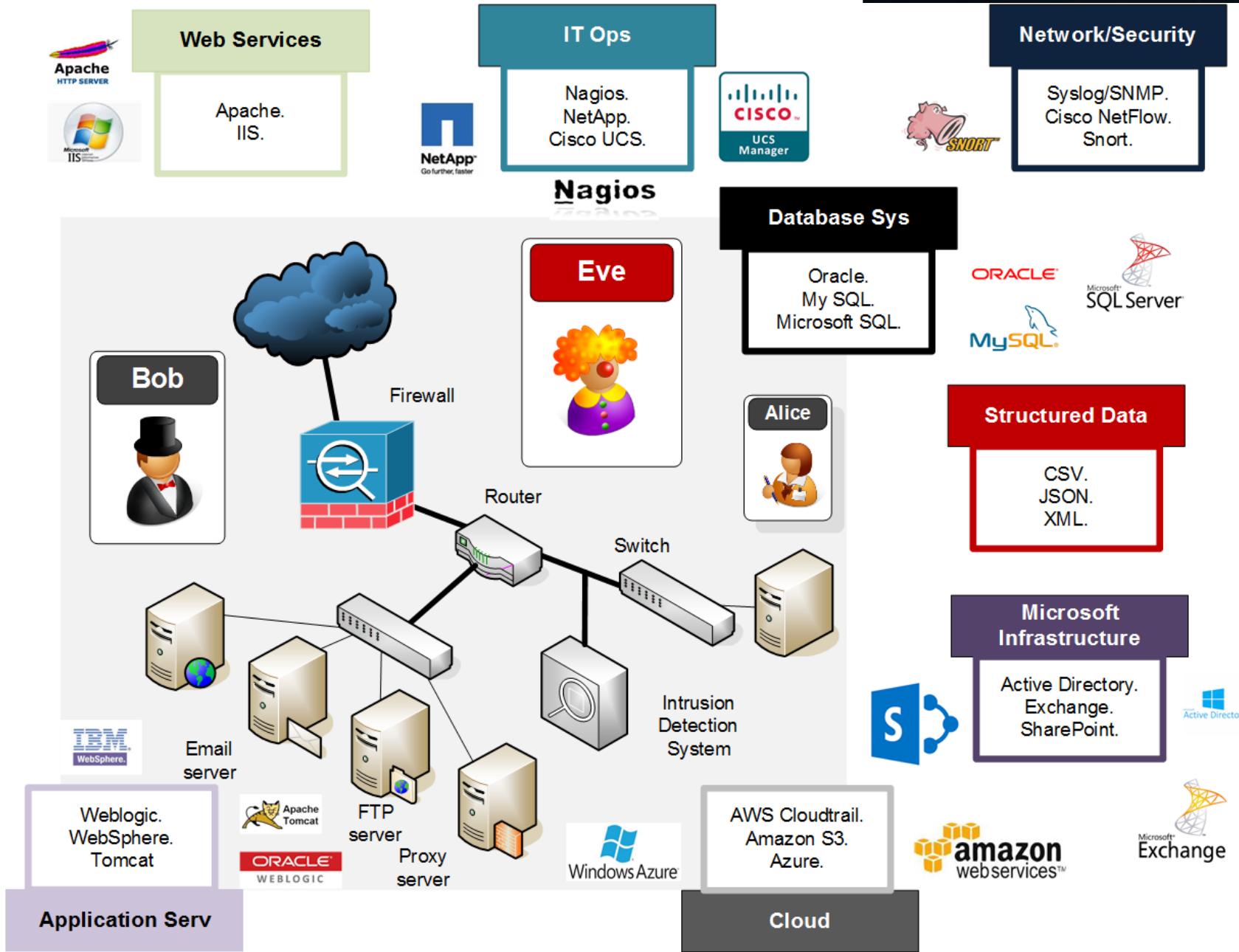
Intrusion Detection
- Alerts

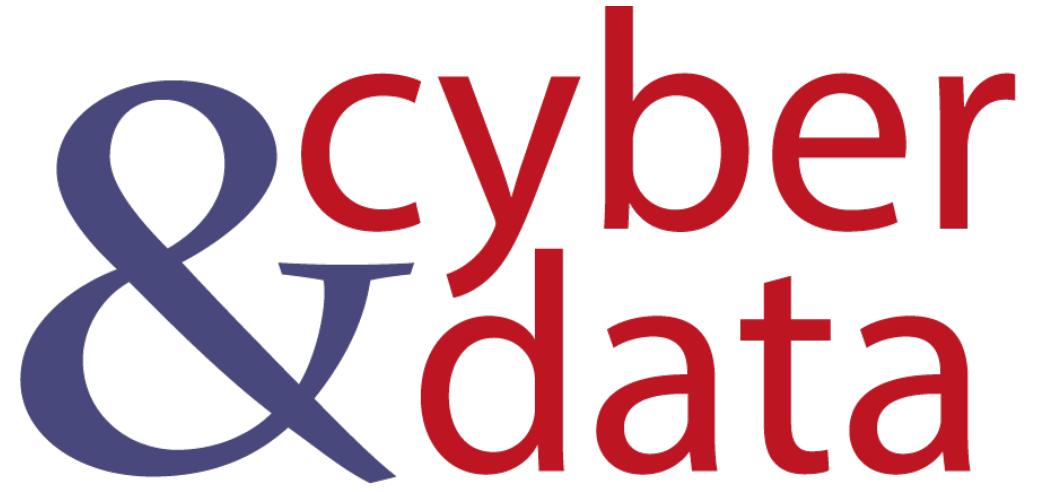
Email
- Logs.



cyber & data

And the complexity ...





“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 ▾ 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

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

Get

er
data

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 Save As ▾ Close

get status=404 All time ▾ Q

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

Events (553) Patterns Statistics Visualization Job ▾ II ■ ↶ ↷ 🖨️ ⬇ Smart Mode ▾

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 >

◀ Hide Fields	☰ All Fields	i Time	Event
SELECTED FIELDS		> 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
INTERESTING FIELDS		> 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

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=SFBVS-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

New Search

passwords.pdf All time

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

Events (68) Patterns Statistics Visualization

Format Timeline ▾ 1 hour per column

List ▾ 20 Per Page ▾

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

< Hide Fields i Time Event

SELECTED FIELDS > 26/04/2014 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

INTERESTING FIELDS > 26/04/2014 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

+ Extract New Fields > 26/04/2014 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

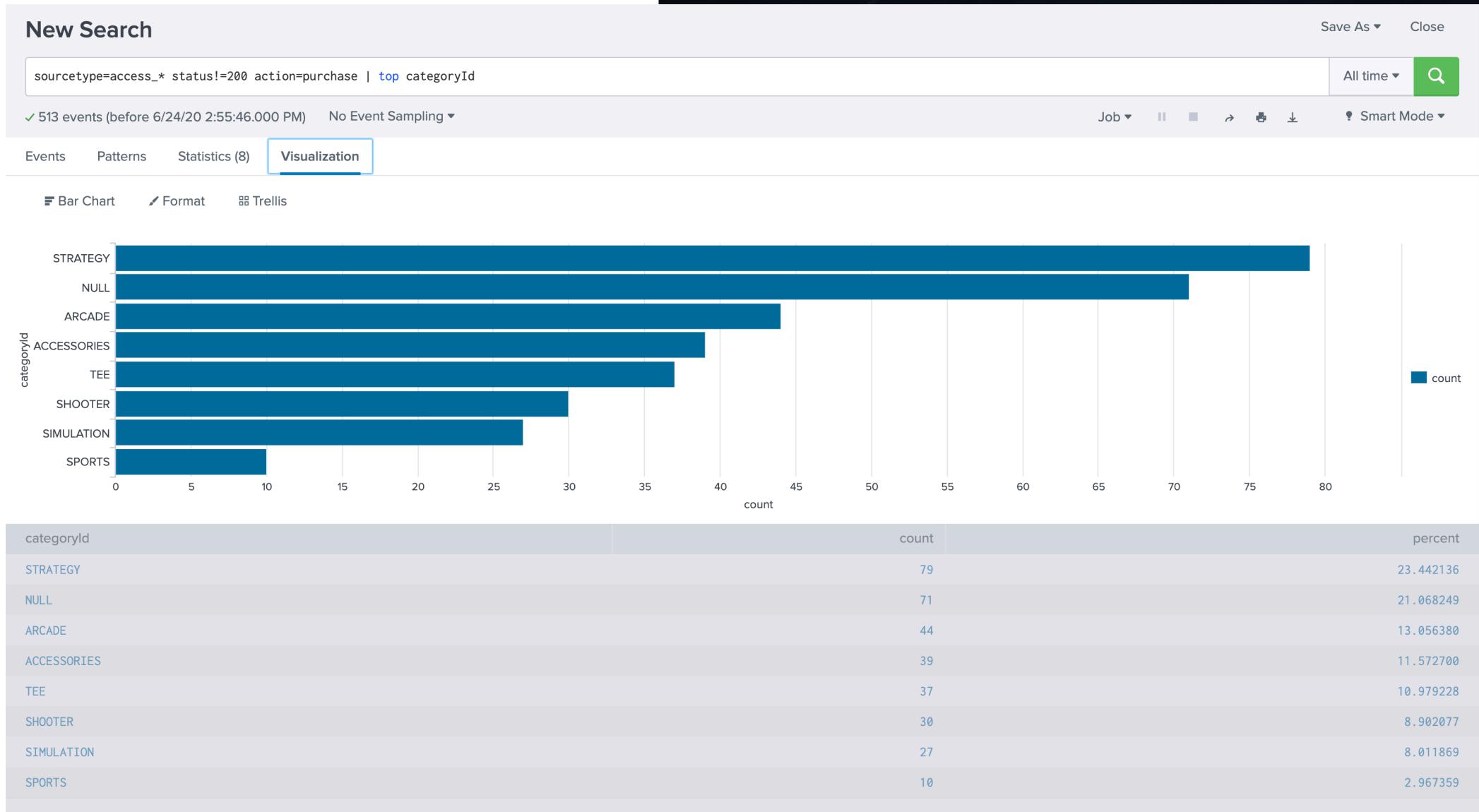
New Search

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 ▾			
Events	Patterns	Statistics (7)	Fast Mode ▾		
20 Per Page ▾			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	



Splunk



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 Treillis

categoryId	count
STRATEGY	750
ARCADE	500
TEE	350
ACCESSORIES	350
SIMULATION	250
SHOOTER	250
SPORTS	180

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

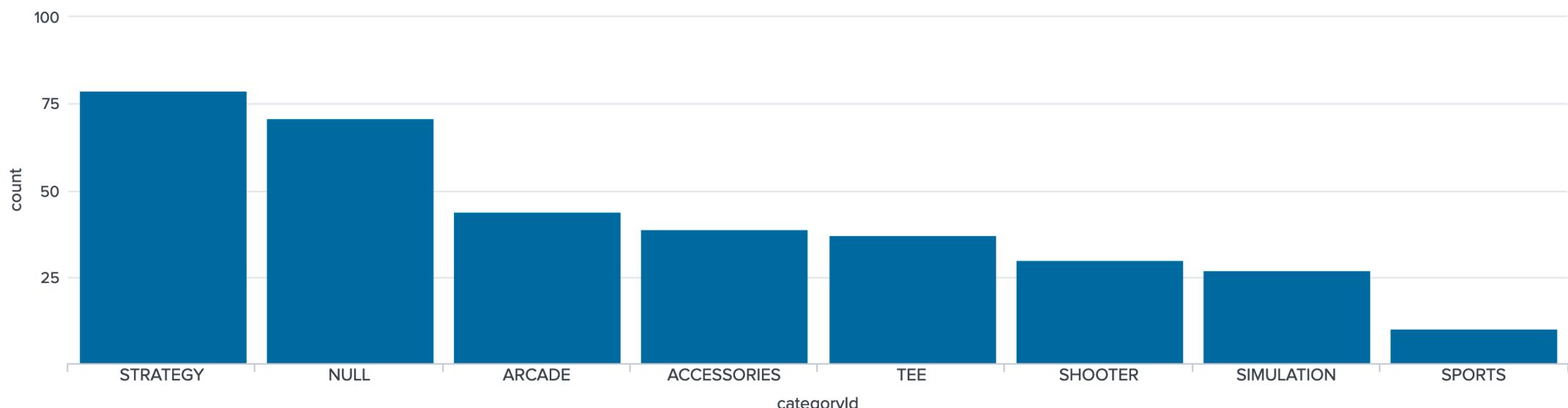
Statistics (8)

Visualization

■ Column Chart

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

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

A horizontal bar chart titled "Visualization" showing browser usage statistics. The y-axis lists the browsers: Safari, Chrome, and Mozilla. The x-axis represents the number of events, ranging from 0 to 38,000. The bars are colored: dark blue for Safari, green for Chrome, and light green for Mozilla. The Mozilla bar extends slightly beyond the 38,000 mark.

Browser	Events
Safari	9,500
Chrome	14,786
Mozilla	36,786

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 ▾  Preview ▾

categoryId	count	percent
SHOOTER	171	100.000000

Get



Splunk

New Search Save As ▾ Close

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

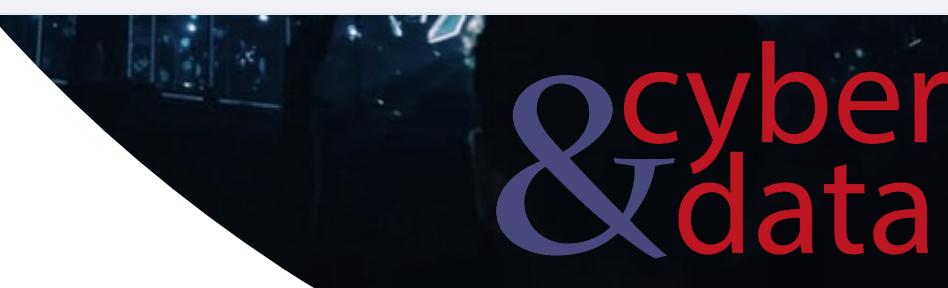
✓ 568 events (before 6/25/20 6:06:42.000 AM) No Event Sampling ▾ Job ▾ || ↶ ↷ ⤒ ⤓ ! Smart Mode ▾

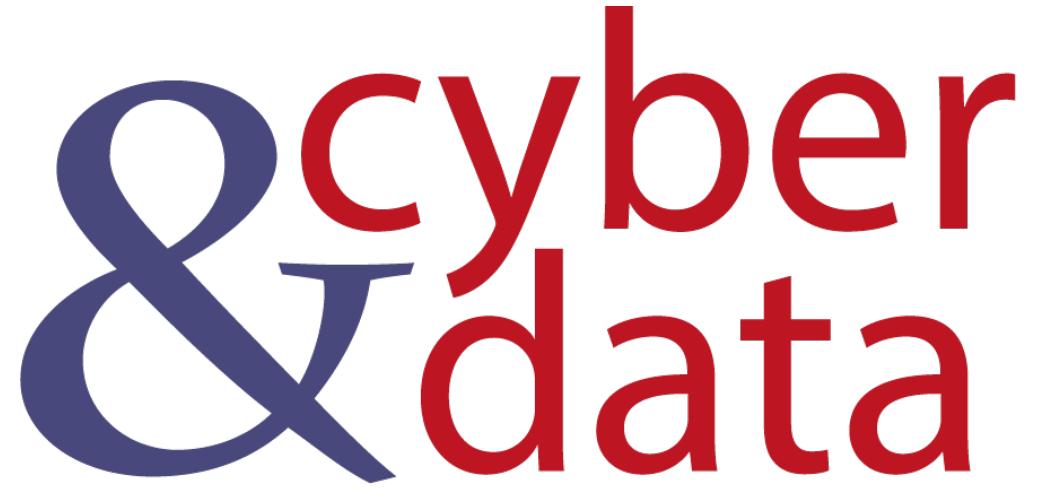
Events Patterns **Statistics (4)** Visualization

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