

ENGELBERT HUMPERDINCK

■ 16 MOST REQUESTED Microsoft ■
Cloud
Searches



```
130 60 4 ~ 107/Jan 18:10:57  
128 241 229 82 ~ 107/Jan 18:10:57  
1 ~ 317 27 168 0 0 ~ 107/Jan 18:10:57  
0wv NT 5 1 SV1 .NET CLR 1 1:10:57:1231 "GET /category.screen?category  
&itemIds=57-168&product_id=R-1-4322" 468 125 17 4 1  
//buttercup-shopping_id=R-1-4322" 468 125 17 4 1  
0zactionspurchase.com/act... 10  
/buttercup-shopping_id=R-1-4322" 468 125 17 4 1  
opping.com/f... 10
```

splunk> conf18

Finding out the delta between “Event Creation” and Event Indexed”

New Search Save As ▾ Close

```
index=main sourcetype="ms*"
| eval time=_time
| eval itime=_indextime
| eval lag=(itime - time)/60
| stats avg(lag), min(lag), median(lag), max(lag) by host sourcetype
```

Last 7 days 🔍

✓ 36,083 events (9/13/18 9:00:00.000 PM to 9/20/18 9:25:05.000 PM) No Event Sampling ▾ Job ▾ Smart Mode ▾

Events Patterns **Statistics (5)** Visualization

100 Per Page ▾ Format Preview ▾

host	sourcetype	avg(lag)	min(lag)	median(lag)	max(lag)
splunk.froth.ly	ms:aad:audit	3.8079070687294014	1.80841328	3.85397300	5.38621150
splunk.froth.ly	ms:aad:signin	6.752147092063344	1.20790657	6.81368809	35.08231527
splunk.froth.ly	ms:o365:management	1167.851448730746	0.3533333	1439.9993650	1771.0166667
splunk.froth.ly	ms:o365:reporting:messagetrace	5.519223220741661	3	6	16
splunk.froth.ly	mscs:azure:audit	4.016381979982058	3.63405008	4.01657450	4.39832847

Exporting of PSTs from Office 365

The screenshot shows the Office 365 Content search Export interface. On the left, there's a list of previous exports:

Name	Last export start time	Exported by
.conf18 Search_Export	2018-09-21 01:50:23	Bud Stoll
SOX_Export	2018-07-25 20:04:23	Fyodor Malteskesk
Test_Export	2018-07-25 06:13:22	Fyodor Malteskesk
Test_Reportsonly	2018-07-20 21:34:44	Bud Stoll

The main panel displays details for the current search named ".conf18 Search_Export":

- Search name:** .conf18 Search
- Started on:** 2018-09-21 01:50:23
- Size:** 0 items, 0 B
- Export key:** A URL is provided for download: ?sv=2014-02-14&sr=c&si=eDiscoveryBlobPolicy9%7C0&sig=rmhLeCIUY3jShPxwBrHKzsgOGT. Buttons for "Copy to clipboard" and "Change key" are available.
- Status:** Refresh, Scheduling...
- A message box indicates: "We're getting your search results ready for download. This may take a while depending on the size of search results. You can also close this window and check back later."
- Items included from the search:** All items, excluding ones that have unrecognized format, are annotated. Newer annotations are shown at the top.

splunk> conf18

```

130.60.4 ~ ~ [07/Jan 18:10:57:153] "GET /category.sc
128.241.220.82 ~ ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=F-DSH-01&JSESSIONID=5D55L771
1" 317 27.160.0.0 ~ ~ [07/Jan 18:10:57:123] "GET /product.screen?product_id=F-DSH-01&JSESSIONID=5D55L9FF1ADF3 HTTP/1.1" 200 3316
ows NT 5.1; SV1; .NET CLR 1.1.4322) 468 125.17 1x ~ ~
kitemId=EST-16&product_id=RP-L1-02" "n
://buttercup-shopping.com/nr
o2action=purchase&ie=opp
/buttercup-shopping.com/nr
)0 ~

```

Exporting of PSTs from Office 365

```
sourcetype="o365:management:activity"
Workload=SecurityComplianceCenter
Operation=SearchExportDownloaded
| stats VALUES(Query) AS Query
VALUES(UserId) AS User BY
ExchangeLocations
```

```
130.60.4 - - [07/Jan/18:10:57:153] "GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemI...
```

```
128.241.220.82 - - [07/Jan/18:10:57:123] "GET /product.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart.do?action=purchase&itemI...
```

```
1" 317 27.160.0.0 - - [07/Jan/18:10:57:123] "GET /buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
ows NT 5.1; SV1; .NET CLR 1.1.4322)" 468 125.17 1x +-- //buttercup-shopping.com/cart-do?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
(itemId=EST-16&product_ids=RP-L1-02" "n----- screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
//buttercup-shopping.com/cart-do?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /category.screen?category_id=G1CTSAJSESSIONID=SD15LAFF10ADFFF10 HTTP/1.1" 404 338 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

```
-----> GET /oldlink?item_id=EST-26&JSESSIONID=SD59L9FF1ADFF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart-do?item_id=EST-26&product_id=EST-26&product_type=...
```

Exporting of PSTs from Office 365

New Search

sourcetype="o365:management:activity" Workload=SecurityComplianceCenter Operation=SearchExportDownloaded | stats **VALUES(Query)** AS Query **VALUES(UserId)** AS User by ExchangeLocations

All time ▼

✓ 6 events (before 9/21/18 1:56:01.000 AM) No Event Sampling ▼ Job ▼ || ▼ ▼ ▼ Smart Mode ▼

Events Patterns **Statistics (2)** Visualization

100 Per Page ▼ Preview ▼

ExchangeLocations	Query	User
Include:[bstoll@froth.ly,jwortoski@froth.ly,ghoppy@froth.ly,fyodor@froth.ly]	Kovar	bstoll@froth.ly
Include:[ghoppy@froth.ly,fyodor@froth.ly,pcerf@froth.ly,abungstein@froth.ly]	yeast(c:c)(date=2018-05-30..2018-09-20)	bstoll@froth.ly

splunk> conf18

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=G1C1S&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemID=EST-26&product_id=F3-5W-3" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=G1C1S&JSESSIONID=SD55L7F6A0FF9 HTTP/1.1" 404 339 "http://buttercup-shopping.com/cart.do?action=purchase&itemID=EST-26&product_id=F3-5W-3" "MS NT 5.1; SV!; .NET CLR 1.1.4322;" "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity?productId=EST-6&JSESSIONID=SD55L9FF2ADEF9 HTTP/1.1" 200 130 "http://buttercup-shopping.com/cart.do?action=remove&itemID=EST-18&product_id=F3-5W-3" //buttercup-shopping.com/nr... 60 130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=G1C1S&JSESSIONID=SD15L4FF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&itemID=EST-26&product_id=F3-5W-3" 128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=G1C1S&JSESSIONID=SD55L7F6A0FF9 HTTP/1.1" 404 339 "http://buttercup-shopping.com/cart.do?action=purchase&itemID=EST-26&product_id=F3-5W-3" "MS NT 5.1; SV!; .NET CLR 1.1.4322;" "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changequantity?productId=EST-6&JSESSIONID=SD55L9FF2ADEF9 HTTP/1.1" 200 130 "http://buttercup-shopping.com/cart.do?action=remove&itemID=EST-18&product_id=F3-5W-3" //buttercup-shopping.com/nr... 60

Successful Logins from Rare Countries

```
sourcetype="ms:aad:signin"
loginStatus=Success
| iplocation src
| stats VALUES(userDisplayName)
COUNT BY Country
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=61&SESSIONID=SD15L AFF10ADFF10 HTTP 1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=61&SESSIONID=SD15L AFF10ADFF10" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:123] "GET /product.screen?category_id=61&SESSIONID=SD15L AFF10ADFF10 HTTP 1.1" 404 334 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&SESSIONID=SD55L9FF1ADDF3" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&SESSIONID=SD55L9FF1ADDF3" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:182] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:183] "GET /oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:184] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:185] "GET /oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:186] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:187] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:188] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4] - [07/Jan 18:10:57:189] "GET /category.screen?category_id=51&SESSIONID=SD55L7FF6ADF9 HTTP 1.1" 200 1318 "http://buttercup-shopping.com/oldlink?item_id=EST-26&SESSIONID=SD55L7FF6ADF9" "buttercup-shopping.com[130.60.4.4]"

Successful Logins from Rare Countries

sourcetype="ms:aad:signin" loginStatus=Success
| iplocation src
| stats VALUES(userDisplayName) count by Country

All time 

✓ 619 events (before 9/21/18 2:04:30.000 AM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns Statistics (6) Visualization

100 Per Page ▾  Preview ▾

Country	VALUES(userDisplayName)	count
Netherlands	Fyodor Malteskesko	1
Singapore	Jacob Smythe	2
Australia	Bud Stoll	50
	Jacob Smythe	
Hong Kong	Bruce Gist	55
	Fyodor Malteskesko	
	Jacob Smythe	
Canada	Fyodor Malteskesko	88

Geographically Improbable Access

sourceType="ms:aad:signin" loginStatus=Success
| rename ipAddress AS src_ip
| sort 0 user, _time
| streamstats window=1 current=f values(_time) as last_time values(src_ip) as last_src_ip by user
| iplocation last_src_ip
| eval last_location = if(isnotnull(City) AND City!="", City . " , " , "") . if(isnotnull(Country) AND Country!="", Country . " , " , "") . if(isnotnull(Region) AND Region!="", Region, "")
| rename lat as last_lat lon as last_lon Country as last_Country
| iplocation src_ip
| eval location = if(isnotnull(City) AND City!="", City . " , " , "") . if(isnotnull(Country) AND Country!="", Country . " , " , "") . if(isnotnull(Region) AND Region!="", Region, "")
| foreach *location [| eval <>FIELD>> = replace(replace(<>FIELD>>, "\^s*,\s*", ""), "\s*,\s\$*", "")]
| eval rlat1 = pi()*last_lat/180, rlat2=pi()*lat/180, rlat = pi()*(lat-last_lat)/180, rlon= pi()*(lon-last_lon)/180
| eval a = sin(rlat/2) * sin(rlat2) + cos(rlat1) * cos(rlat2) * sin(rlon/2) * sin(rlon/2)
| eval c = 2 * atan2(sqrt(a), sqrt(1-a))
| eval distance = 6371 * c, time_difference_hours = round(_time - last_time) / 3600, speed=round(distance/ (time_difference_hours),2)
| fields - rlat* a
| eval day=strftime(_time, "%m/%d/%Y")
| search last_Country!=Country distance!=0 speed>1000
| stats values(time_difference_hours) as time_difference_hours values(speed) as speed first(last_location) as location_one first(location) as location_two values(*src_ip) as *src_ip min
(_time) as firstTime by user distance day

2 events (8/23/18 12:00:00.000 AM to 8/24/18 12:00:00.000 AM) No Event Sampling ▾ Job ▾ II ■ ▾ ▾ ▾ Smart Mode ▾

Events	Patterns	Statistics (2)	Visualization						
100 Per Page ▾	Format	Preview ▾							
user	distance	day	time_difference_hours	speed	location_one	location_two	last_src_ip	src_ip	firstTime
jacobsmythe@jacobsmythe111.onmicrosoft.com	14231.05	08/23/2018	0.32	44472.03	Australia	San Antonio, United States, Texas	59.100.156.162	40.84.156.9	1534990340.698434
jacobsmythe@jacobsmythe111.onmicrosoft.com	2596.948	08/23/2018	1.56	1664.71	San Antonio, United States, Texas	Boardman, United States, Oregon	40.84.156.9	34.215.24.225	1534996396.353531

splunk> conf18

Geographically Improbable Access

during Thu, Aug 23, 2018 ▾										
user	distance	day	time_difference_hours	speed	location_one	location_two	last_src_ip	src_ip	firstTime	
jacobsmythe@jacobsmythe111.onmicrosoft.com	14231.05	08/23/2018	0.32	44472.03	Australia	San Antonio, United States, Texas	59.100.156.162	40.84.156.9	1534990340.698434	
jacobsmythe@jacobsmythe111.onmicrosoft.com	2596.948	08/23/2018	1.56	1664.71	San Antonio, United States, Texas	Boardman, United States, Oregon	40.84.156.9	34.215.24.225	1534996396.353531	

100 Per Page ▾ Format Preview ▾

user	distance	day	time_difference_hours	speed	location_one	location_two	last_src_ip	src_ip	firstTime
jacobsmythe@jacobsmythe111.onmicrosoft.com	14231.05	08/23/2018	0.32	44472.03	Australia	San Antonio, United States, Texas	59.100.156.162	40.84.156.9	1534990340.698434
jacobsmythe@jacobsmythe111.onmicrosoft.com	2596.948	08/23/2018	1.56	1664.71	San Antonio, United States, Texas	Boardman, United States, Oregon	40.84.156.9	34.215.24.225	1534996396.353531

splunk> conf18



Geographically Improbable Access

splunk>enterprise App: Splunk Security Essentials ▾

H Administrator ▾ 4 Messages ▾ Settings ▾ Activity ▾ Help ▾ Find

Introduction Security Content ▾ Security Data Journey Data Source Check Documentation ▾ Advanced ▾ Splunk Security Essentials

Export ▾ ...

Security Content / Geographically Improbable Access Detected against Category

Assistant: Simple Search

Description

To ensure you have a GDPR-mandated audit trail with individual accounts for each person, detect when the same account is logged into twice in a short period of time but from locations very far away, to a GDPR-tagged system.

Learn how to use this page

View Demo Data Live Data

Use Case
Compliance

Category
GDPR

Security Impact
Detecting and proving that your organization's environment does not use shared user accounts for accessing and processing personal data is industry best practice and should be considered as an effective security control which is required by Article 32 and will help you to prove compliance for data privacy audits from authorities (Article 58) or counteract any compensation claims (Article 82).

Alert Volume
Low

SPL Difficulty
Advanced

Stage 4

Data Sources

Authentication Audit Trail

Adding Permissions to Mailboxes

```
sourcetype=ms:* Operation="Add-
MailboxPermission" "Parameters{} .Name"="* "
| mvexpand Parameters{} .Value
| search Parameters{} .Value=FullAccess
| stats COUNT BY object, UserId,
"Parameters{} .Value" Operation
| rename UserId AS "Account Making Change",
"Parameters{} .Value" AS "Access Level"
```

Adding Permissions to Mailboxes

New Search

Save As ▾ Close

```
sourcetype=ms:* Operation="Add-MailboxPermission" "Parameters{}".Name="*"
| mvexpand Parameters{}.Value
| search Parameters{}.Value=FullAccess
| stats count by object, UserId, "Parameters{}.Value" Operation
| rename UserId AS "Account Making Change", "Parameters{}.Value" AS "Access Level"
```

All time ▾



✓ 29 events (before 9/21/18 2:47:08.000 AM) No Event Sampling ▾

Job ▾ II ⌂ ⌂ ⌂ ⌂ ⌂ ⌂ Smart Mode ▾

Events Patterns Statistics (6) Visualization

100 Per Page ▾ Format Preview ▾

object ▾	Account Making Change	Access Level	Operation	count
ry	jacobsmythe@jacobsmythe111.onmicrosoft.com	FullAccess	Add-MailboxPermission	3
ghoppy	bstoll@froth.ly	FullAccess	Add-MailboxPermission	2
ghoppy	fyodor@froth.ly	FullAccess	Add-MailboxPermission	3
ghoppy	jacobsmythe@jacobsmythe111.onmicrosoft.com	FullAccess	Add-MailboxPermission	1
bstoll	jacobsmythe@jacobsmythe111.onmicrosoft.com	FullAccess	Add-MailboxPermission	1

Sharing of OneDrive Files

sourcetype="ms:o365:management" Workload=OneDrive Operation=SharingSet
| rex field=EventData "\>(?<modtype>[^<\>/]+)\<\/"
| stats count by dest, UserId, modtype

All time ▼ 🔍

✓ 72 events (before 9/21/18 4:51:11.000 AM) No Event Sampling ▼ Job ▼ || ■ ⟳ ✚ ⤓ ? Smart Mode ▼

Events Patterns **Statistics (48)** Visualization

100 Per Page ▼ ✍ Format Preview ▼

dest ▼ ✍	UserId ▼ ✍	modtype ▼ ✍
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg	ry@froth.ly	Contribute
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg	ry@froth.ly	Limited Access
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg	ry@froth.ly	System.LimitedEdi

Downloads from OneDrive

```
sourcetype="ms:o365:management"
Workload=OneDrive
Operation=FileDownloaded
| stats VALUES(SourceRelativeUrl)
VALUES(SourceFileName)
VALUES(UserAgent) BY UserId
```

130.60.4 - - [07/Jan 18:10:57:153] "GET /category.screen?category_id=6165A1SESSIONID=SD15AFF10ADFF10 HTTP/1.1" 404 720 "http://buttercup-shopping.com/cart.do?action=view&item_id=EST-26&product_id=F3-5W-31"
128.241.220.82 - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=G1FTS1JSESSIONID=SD15AFF10ADFF10 HTTP/1.1" 404 334 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&product_id=F3-5W-31&order_id=EST-16&product_id=EST-18&product_id=A1FFAADFF7"
1" 317 27.169.0.0 - - [07/Jan 18:10:57:123] "GET /buttercup-shopping.com/cart.do?action=changequantity?item_id=EST-6&SESSIONID=SD55L7FF6ADFF9 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/cart.do?action=changecategory?item_id=EST-6&SESSIONID=SD55L7FF6ADFF9"
1" 317 27.169.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 334 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3"
1" 317 27.169.0.0 - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3 HTTP/1.1" 200 334 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADFF3"
1" 317 27.169.0.0 - - [07/Jan 18:10:57:187] "GET /category.screen?category_id=5UBBL1FF1ADFF6 HTTP/1.1" 200 202 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=F3-5W-31&order_id=EST-16&product_id=A1FFAADFF7"
1" 317 27.169.0.0 - - [07/Jan 18:10:57:189] "GET /category.screen?category_id=5UBBL1FF1ADFF6 HTTP/1.1" 200 202 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=F3-5W-31&order_id=EST-16&product_id=A1FFAADFF7"
1" 317 27.169.0.0 - - [07/Jan 18:10:57:191] "GET /category.screen?category_id=5UBBL1FF1ADFF6 HTTP/1.1" 200 202 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-14&product_id=F3-5W-31&order_id=EST-16&product_id=A1FFAADFF7"

Downloads from OneDrive

New Search Save As ▾ Close

```
sourcetype="ms:o365:management" Workload=OneDrive Operation=FileDownloaded  
| stats VALUES(SourceRelativeUrl) VALUES(SourceFileName) VALUES(UserAgent) by UserId
```

All time ▼ Q

✓ 4 events (before 9/21/18 3:16:30.000 AM) No Event Sampling ▾ Job ▾ II ⌂ ↗ ⌄ ⌅ ⌆ Smart Mode ▾

Events Patterns **Statistics (1)** Visualization

100 Per Page ▾ Format Preview ▾

UserId	VALUES(SourceRelativeUrl)	VALUES(SourceFileName)	VALUES(UserAgent)
ghoppy@froth.ly	Documents/Frothly-Shared/Yeasts	31632-pdf.pdf 34322-pdf.pdf	Mozilla/5.0 (Macintosh; Intel Mac OS X 10_12_6) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36

Deletion/Creation of Users

```
sourcetype="ms:o365:management"
Operation="Add user." OR Operation="Delete
User."
| stats COUNT BY ObjectId, Operation,
UserId
| rename ObjectId AS "Affected Account",
UserId AS "Account Making Change"
```

Deletion/Creation of Users

sourcetype="ms:o365:management" Operation="Add user." OR Operation="Delete User."
| stats count BY ObjectId, Operation, UserId
| rename ObjectId AS "Affected Account", UserId AS "Account Making Change"

All time ▾ 

✓ 22 events (before 9/21/18 3:51:25.000 AM) No Event Sampling ▾ Job ▾  Smart Mode ▾

Events Patterns **Statistics (21)** Visualization

100 Per Page ▾  Preview ▾

Affected Account	Operation	Account Making Change
15345ea6bdb74cbe9a1b957e207defcbjadoe@froth.ly	Delete user.	jacobsmythe@jacobsmythe111.onmicrosoft.com
a72ab76da3314204a802808fe9f1e4d2jdoe@froth.ly	Delete user.	jacobsmythe@jacobsmythe111.onmicrosoft.com
dmerritt@froth.ly	Add	jacobsmythe@jacobsmythe111.onmicrosoft.com

New Org BCC Rules added

```
sourcetype="ms:o365:management" Operation="New-TransportRule" BlindCopyTo
| spath path="Parameters{}.Name" output=parameters_name
| spath path="Parameters{}.Value"
output=parameters_value
| eval firstValue=mvIndex(parameters_name,0)
| eval Email=mvIndex(parameters_value,0)
| eval Description=mvIndex(parameters_value,1)
| search firstValue=BlindCopyTo
| stats VALUES(Email) AS "BCC To" VALUES(Description) AS "Rule Name" BY _time
```

130.60.4 ~ [07/Jan 18:10:57:153] "GET /category.screen?category_id=61675&JSESSIONID=SD15L4FF10ADFF30 HTTP/1.1" 404 720 "http://buttercup-shopping.com/category.screen?category_id=61675&JSESSIONID=SD15L4FF10ADFF30" "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-26&JSESSIONID=SD15L4FF10ADFF30" - - [07/Jan 18:10:57:123] "GET /product.screen?category_id=61675&JSESSIONID=SD15L4FF10ADFF30 HTTP/1.1" 404 335 "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-18&product_id=EST-26&JSESSIONID=SD15L4FF10ADFF30" "http://buttercup-shopping.com/cart.do?action=purchase&item_id=EST-18&product_id=EST-26&JSESSIONID=SD15L4FF10ADFF30" - - [07/Jan 18:10:56:156] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 1318 "http://buttercup-shopping.com/changedquare?category_id=61675&JSESSIONID=SD55L9FF1ADEF3" "http://buttercup-shopping.com/cart.do?action=changequare?category_id=61675&JSESSIONID=SD55L9FF1ADEF3" - - [07/Jan 18:10:56:187] "GET /oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3 HTTP/1.1" 200 1253 "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3" "http://buttercup-shopping.com/cart.do?action=oldlink?item_id=EST-26&JSESSIONID=SD55L9FF1ADEF3" - - [07/Jan 18:10:55:187] "GET /category.screen?category_id=5088L4FF1ADEF6 HTTP/1.1" 200 425 "http://buttercup-shopping.com/cart.do?action=category.screen?category_id=5088L4FF1ADEF6" "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-12&product_id=EST-12&JSESSIONID=SD55L9FF1ADEF6" - - [07/Jan 18:10:55:188] "GET /category.screen?category_id=5088L4FF1ADEF6 HTTP/1.1" 200 425 "http://buttercup-shopping.com/cart.do?action=remove&item_id=EST-12&product_id=EST-12&JSESSIONID=SD55L9FF1ADEF6" "http://buttercup-shopping.com/cart.do?action=category.screen?category_id=5088L4FF1ADEF6" - - [07/Jan 18:10:55:188]

Password Spraying

```
index=main sourcetype=ms:o365:management AzureActiveDirectoryEventType=1 ClientIP!="<null>"  
| iplocation ClientIP  
| stats values(src_user) values(Country) dc(src_user) AS ucount values(City) by ClientIP  
| search ucount>1
```

All time ▾



✓ 22,474 events (before 9/21/18 4:34:38.000 AM) No Event Sampling ▾

Job ▾



Smart Mode ▾

Events Patterns Statistics (41) Visualization

100 Per Page ▾ Format Preview ▾

ClientIP	values(src_user)	values(Country)	ucount	values(City)
203.37.61.132	jacobsmythe@jacobsmythe111.onmicrosoft.com ry@froth.ly	Australia	2	Horsham
117.24.39.208	fyodor@froth.ly jwortoski@froth.ly	China	2	Quanzhou
5.101.40.7	fyodor@froth.ly ghoppy@froth.ly jwortoski@froth.ly mkraeusen@froth.ly pcerf@froth.ly	Russia	5	
5.101.40.9	fyodor@froth.ly ghoppy@froth.ly jwortoski@froth.ly mkraeusen@froth.ly	Russia	5	