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

```
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
```

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

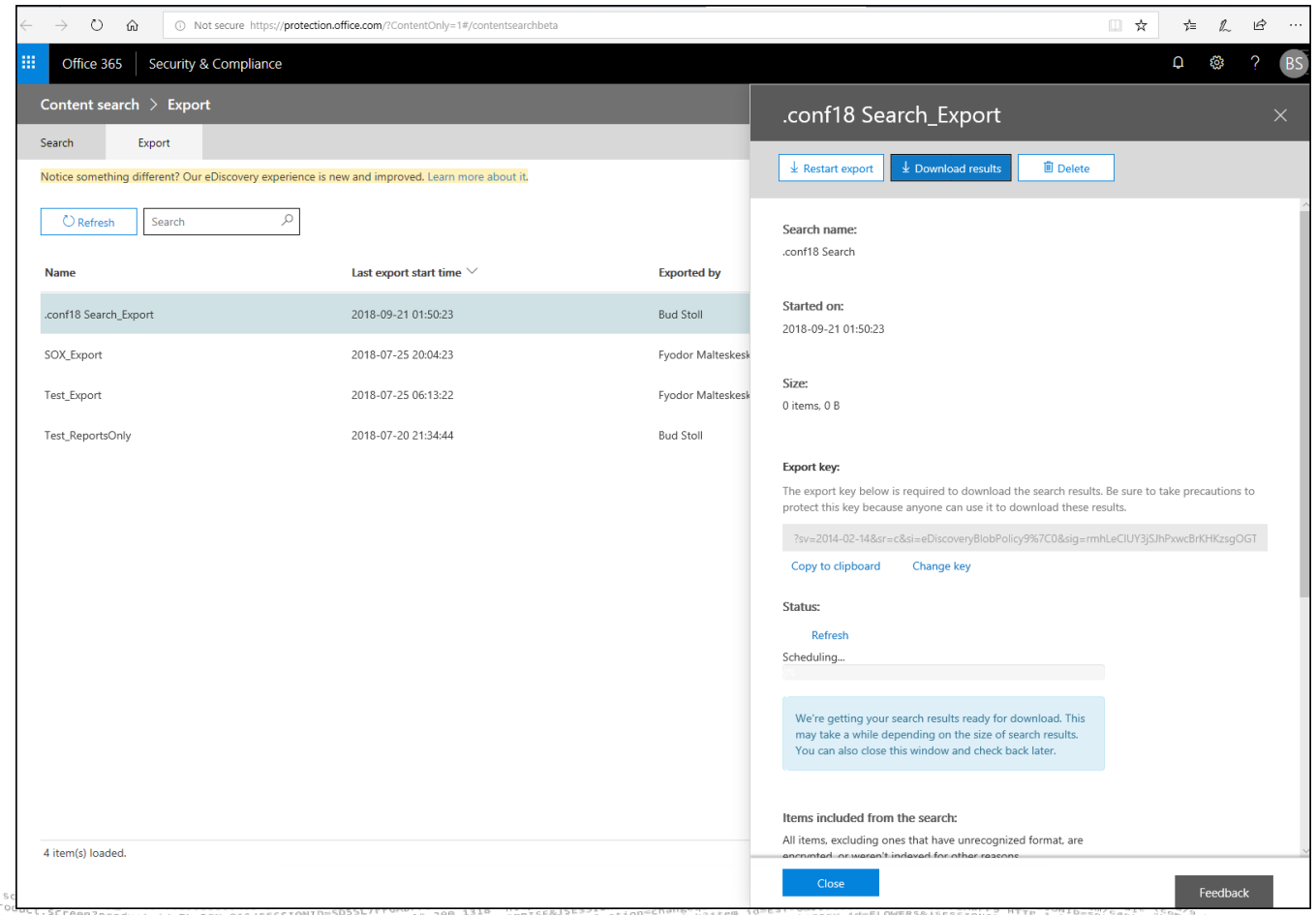
✓ 36,083 events (9/13/18 9:00:00.000 PM to 9/20/18 9:25:05.000 PM) No Event Sampling Job Smart Mode

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

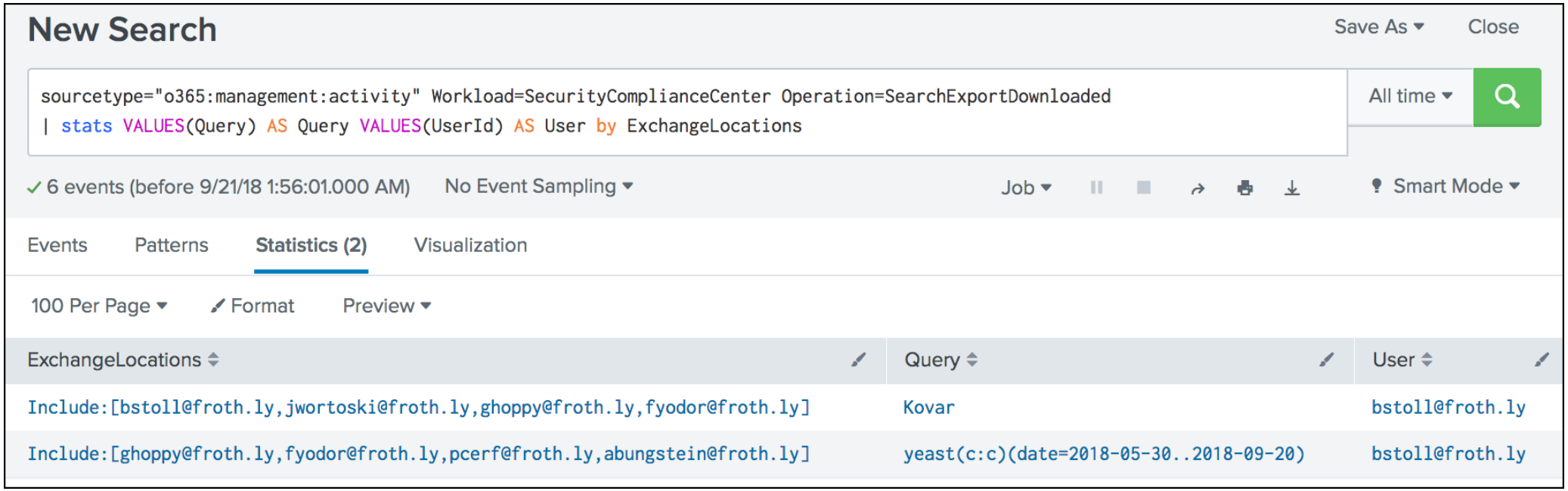


splunk> .conf18

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
```

Exporting of PSTs from Office 365



splunk> .conf18

Successful Logins from Rare Countries

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

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 Format Preview

Country	VALUES(userDisplayName)	count
Netherlands	Fyodor Malteskesko	1
Singapore	Jacob Smythe	2
Australia	Bud Stoll Jacob Smythe	50
Hong Kong	Bruce Gist Fyodor Malteskesko Jacob Smythe	55
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(rlat/2) + 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) / 3600,2), speed=round(distance/ (
time_difference_hours),2)
| fields - rlat* a c
| 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
```

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(rlat/2) + 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) / 3600,2), speed=round(distance/ ( time_difference_hours),2)
| fields - rlat* a c
| 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
```

during Thu, Aug 23, 2018

✓ 2 events (8/23/18 12:00:00.000 AM to 8/24/18 12:00:00.000 AM) No Event Sampling

Job 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

```
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*$", "")]
```

during Thu, Aug 23, 2018

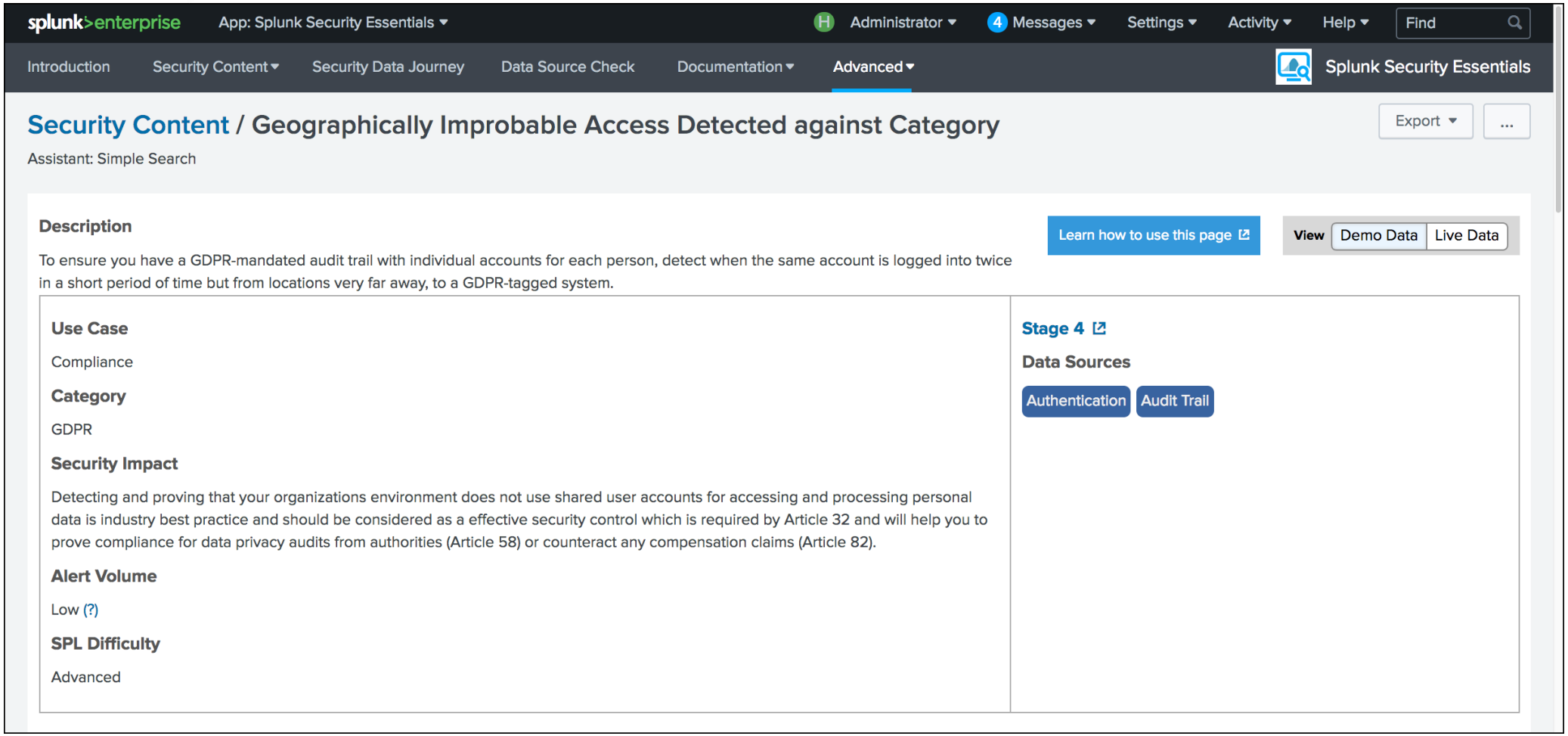
user	distance	day	time_difference_hours	speed	location_one	location_two	last_src_ip	src_ip	firstTime
jacobsmythe@jacobsmythe111.onmicrosoft.com	14231.05	08/23/2018	0.32	44472.03	Australia	San Antonio, United States, Texas	59.100.156.162	40.84.156.9	1534990340.698434
jacobsmythe@jacobsmythe111.onmicrosoft.com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



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 ▾ 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
```

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

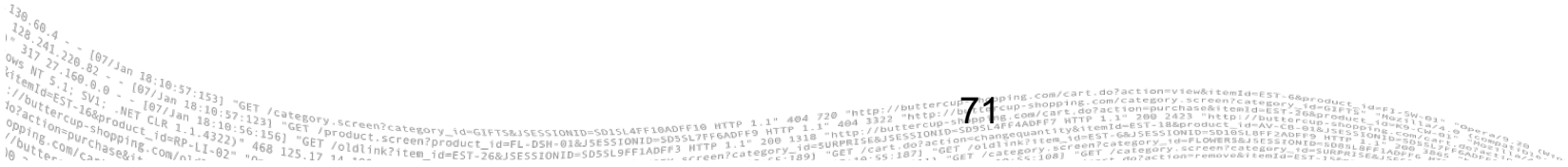
Events Patterns **Statistics (48)** Visualization

100 Per Page Format Preview

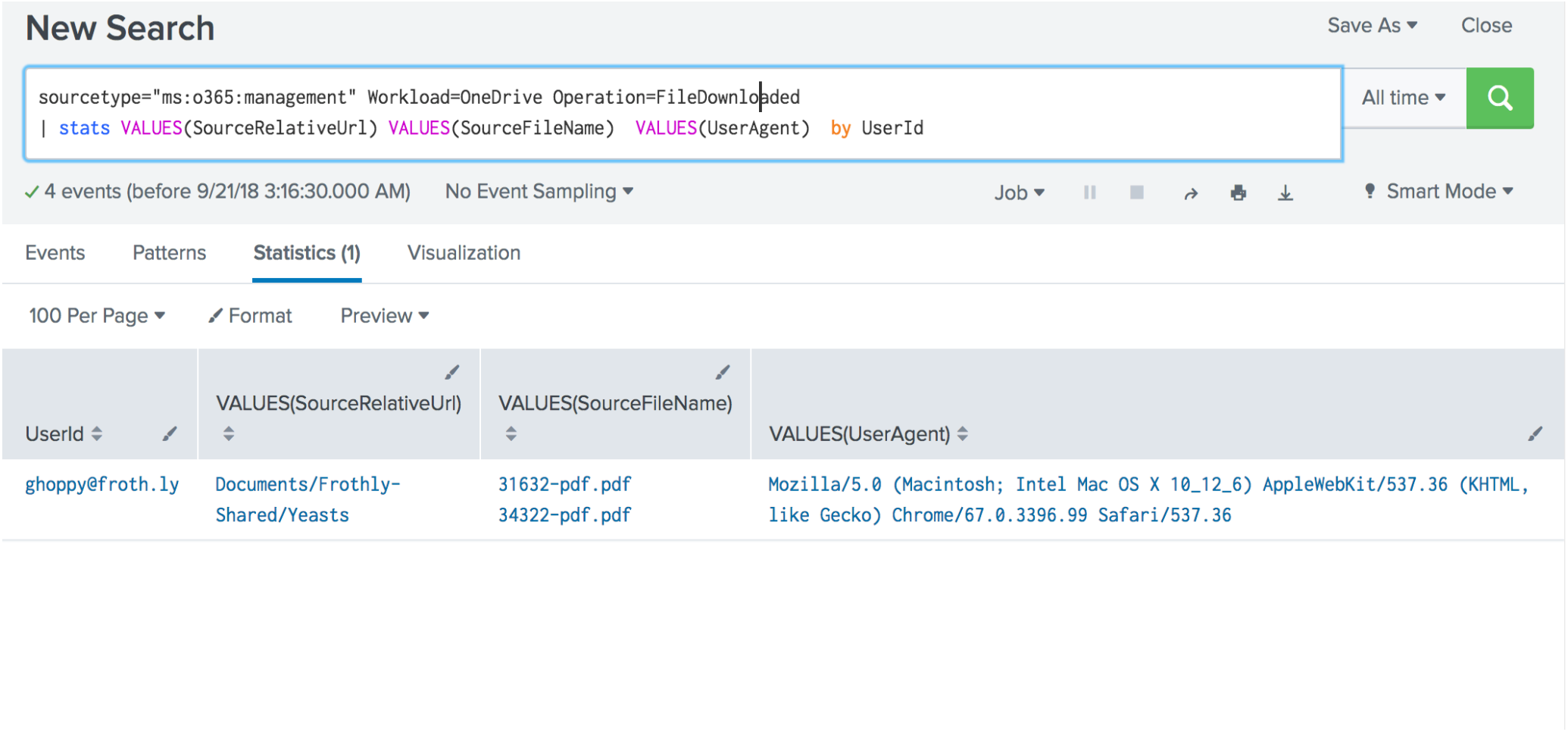
dest	UserId	modtype
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg	ry@froth.ly	Contribute
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg	ry@froth.ly	Limited Access
https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg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

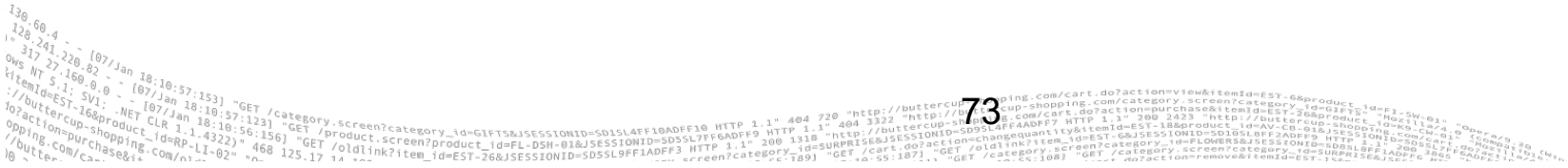


Downloads from OneDrive



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 Format 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
```

New Org BCC Rules added

New Search

Save As

```
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
```

All time

✓ 5 events (before 9/21/18 4:18:50.000 AM) No Event Sampling Job

Events Patterns **Statistics (4)** Visualization

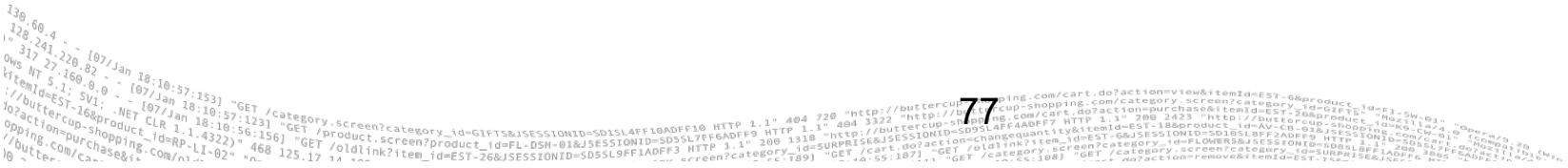
100 Per Page Format Preview

_time	BCC To	Rule Name
2018-08-03 16:31:52	ubuntu@ec2-52-38-112-145.us-west-2.compute.amazonaws.com	all
2018-07-17 14:16:13	rkovar@gmail.com	All

splunk> .conf18

Password Spraying

```
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
```



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	