Down in the Weeds, Up in the Cloud

Splunking Office 365 & Azure

Ryan Lait | Senior Sales Engineer

Ry@splunk.com

October 2018

Forward-Looking Statements

During the course of this presentation, we may make forward-looking statements regarding future events or the expected performance of the company. We caution you that such statements reflect our current expectations and estimates based on factors currently known to us and that actual events or results could differ materially. For important factors that may cause actual results to differ from those contained in our forward-looking statements, please review our filings with the SEC.

The forward-looking statements made in this presentation are being made as of the time and date of its live presentation. If reviewed after its live presentation, this presentation may not contain current or accurate information. We do not assume any obligation to update any forward-looking statements we may make. In addition, any information about our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment. Splunk undertakes no obligation either to develop the features or functionality described or to include any such feature or functionality in a future release.

splunk> .conf18

#whoami

RYAN LAIT

Senior Sales Engineer – Brisbane, Australia

Splunk Chief Converse Officer*

- Former Splunk customer
- Cyber Security Analyst

PRODUCT OF AUSTRALIA

* Self-appointed title

Content Overview

Security, and some not-so-security focused content

- Office 365
  - Using O365 with Splunk
  - O365 Workloads
  - Exchange Message Tracking
  - Security Essentials
  - Enterprise Security
  - IT Service Intelligence
- Azure
  - Using Azure with Splunk
  - Inventory & Asset Management
  - Resource Mapping
  - Runbook Automation
- Appendix
  - Additional use cases
  - Blog Posts
  - GitHub Repo's
  - App List

Splunk & Office 365

Microsoft SaaS

Exchange Online

OneDrive

Skype for Business

Azure Active Directory

Microsoft Teams

Power BI

Microsoft Dynamics 365

yammer

SharePoint Online

splunk> .conf18

How Splunk Customers are Using Office 365 Data

Content Analytics

- Adoption metrics, usage statistics, service status, subscription metrics, cost & spend analysis

Security Analytics

- Compromised account monitoring, improbable access, usage anomalies, Message tracking, DLP, threat correlation

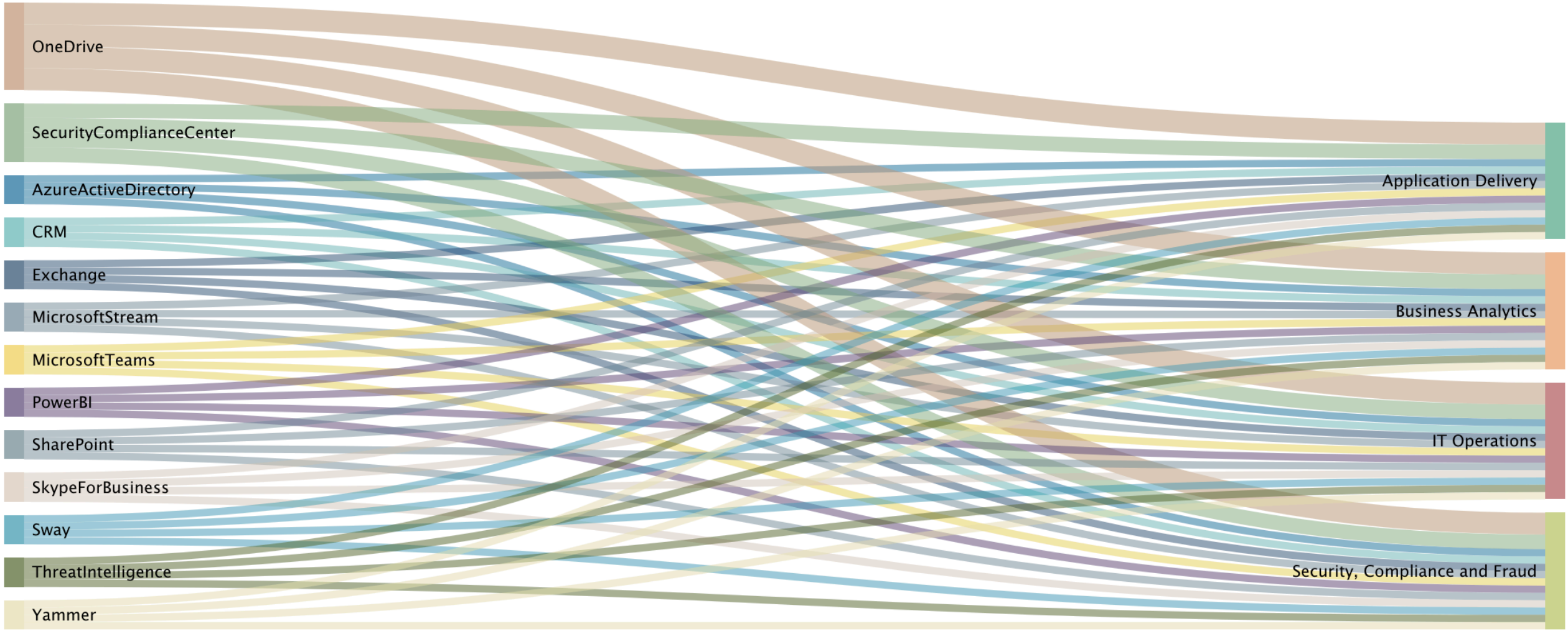
Compliance Reporting

- System and user access auditing for compliance reporting

Data Correlation & Enrichment

- Correlating O365 data with existing Splunk data and relational lookup data

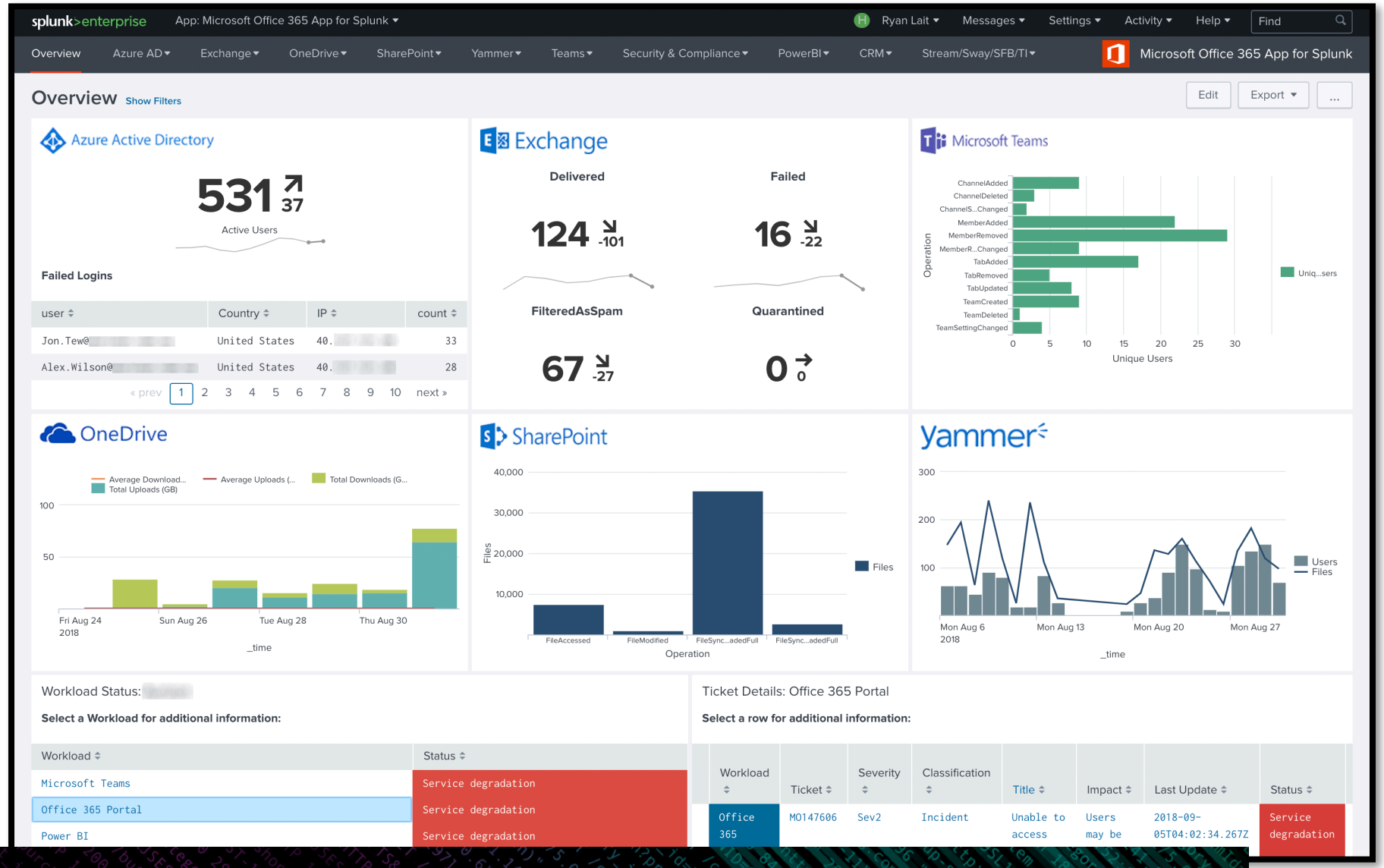
Workloads



Depending on your subscription!

E1/E3/E5 etc.

Single Glass of Pain OR Single Pane of Glass



The Why

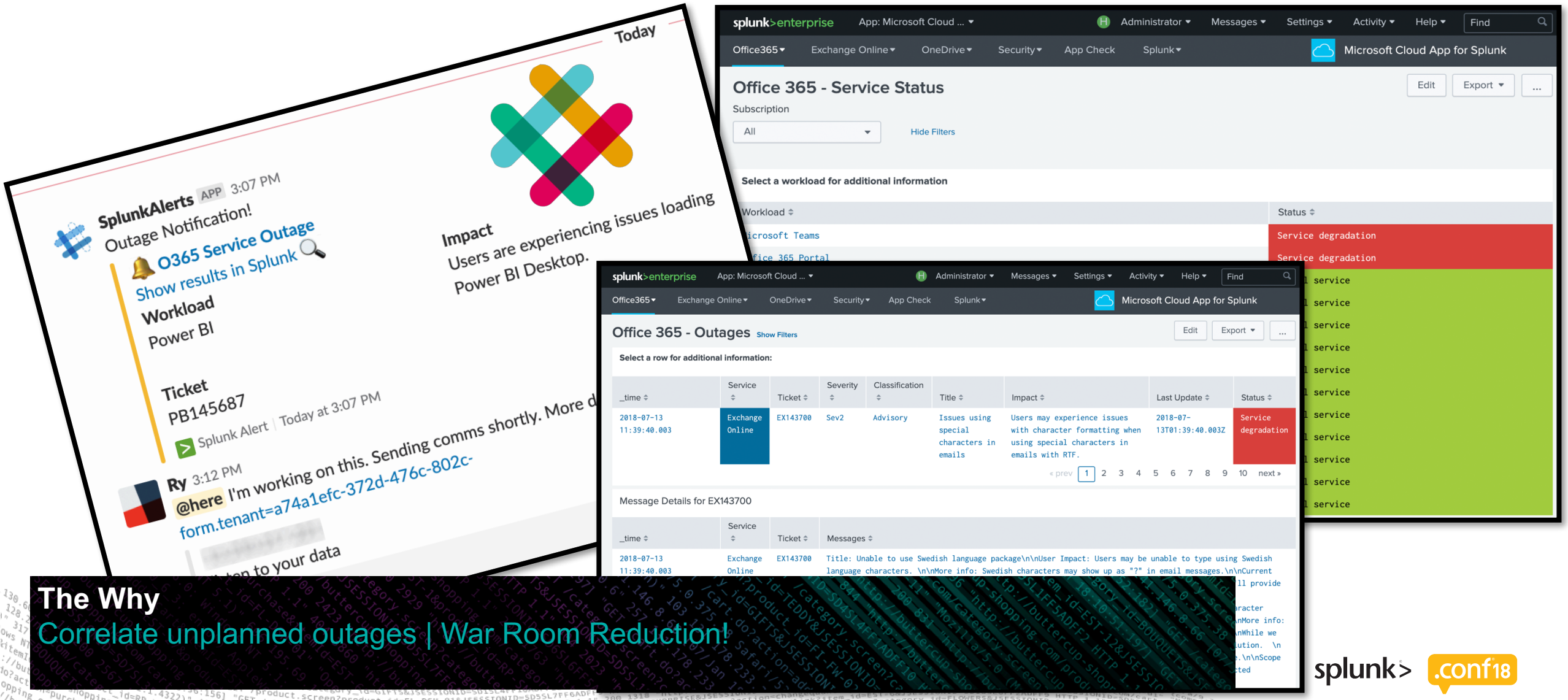
Login anomalies | Data exfiltration |

Instant service health | Usage adoption | Correlate on-prem data with O365

splunk> .conf18

Service Status

Is it us, or is it them?



The Why

Correlate unplanned outages | War Room Reduction!

splunk> .conf18

Azure Active Directory

{ [-]
  Actor: [[+]
  ]
  ActorContextId: d51ef8df-6617-4356-b8d4-89ad7efef31e
  AzureActiveDirectoryEventType: 1
  CreationTime: 2018-06-22T16:57:37
  Id: 274b971c-d57c-49e0-878b-58bceed7b654
  InterSystemsId: f103b4eb-1285-4bdb-8001-655bffb85059
  IntraSystemId: 76522644-af27-4f80-b51c-4b70c157b15b
  ObjectId: mkraeusen@froth.ly
  Operation: Reset user password.
  OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
  RecordType: 8
  ResultStatus: success
  Target: [[-]
    { [+]
    }
    { [-]
      ID: mkraeusen@froth.ly
      Type: 5
    }
    { [+]
    }
  ]
  TargetContextId: 225e05a1-5914-4688-a404-7030e60f3143
  UserId: fim_password_service@support.onmicrosoft.com
  UserKey: 100300008060F582@support.onmicrosoft.com
  UserType: 0

Add OAuth2PermissionGrant.
Add app role assignment grant to user.
Add app role assignment to service principal.
Add application. >
Add device configuration.
Add device. >
Add group.
Add member to group. >
Add member to role.
Add owner to group.
Add registered owner to device.
Add registered users to device.
Add service principal.
Add user. >
Change user license.
Change user password. >
Consent to application.
Create application password for user.
Delete device. >
Delete group.
Delete user. >
Disable account.
Enable Strong Authentication.
Finish applying group based license to users.
ForeignRealmIndexLogonInitialAuthUsingADFSFederatedToken
Hard Delete group.
PasswordLogonInitialAuthUsingADFSFederatedToken
PasswordLogonInitialAuthUsingPassword
Remove OAuth2PermissionGrant.
Remove member from group.
Remove member from role.
Remove owner from group.
Reset user password. >
Set Company Information.
Set domain authentication.
Set federation settings on domain.
Set user manager.
Start applying group based license to users.
Trigger group license recalculation.
Update StsRefreshTokenValidFrom Timestamp.
Update application.
Update device configuration.
Update device.
Update domain.
Update group.
Update service principal.
Update user.
UserLoggedIn
UserLoginFailed >

The Why

Login activity | Geographical activity | License usage | Device auditing | User auditing | ADFS auditing | etc

splunk> .conf18

Exchange Online

{ [-]
  AffectedItems: [[-]
    { [-]
      Attachments: [redacted].pdf
      Id: RgAAAADzDJswFhr6TYbUC0t7ad3aBwBKRAWKlNTlQ4SatmX5ZKHEAAAQMLCTAAA1Cz4/
      InternetMessageId: <1546522443.1095.1532310697837.JavaMail.gsadmin@pgsas204.asxprod.asx.com.au>
      ParentFolder: { [+]
      }
      Subject: [redacted]
    }
  ]
  ClientIPAddress: [redacted]
  ClientInfoString: Client=OWA;Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; Touch; rv:11.0) like Gecko[AppId=00000002-0000-0ff1-ce00-000000000000];
  CreationTime: 2018-07-23T05:49:40
  CrossMailboxOperation: false
  ExternalAccess: false
  Folder: { [+]
  }
  Id: 07d9178c-138d-4fda-d42b-
  InternalLogonType: 0
  LogonType: 2
  LogonUserSid: S-1-5-21-3551695864-665769943-
  MailboxGuid: 91810413-f0b3-47b5-a438-
  MailboxOwnerSid: S-1-5-21-3551695864-665769943-
  MailboxOwnerUPN: [redacted].com.au
  Operation: HardDelete
  OrganizationId: a74a1efc-372d-476c-802c-
  OrganizationName: [redacted].onmicrosoft.com
  OriginatingServer: SYXPR01MB1408 (15.20.0973.010)

  RecordType: 3
  ResultStatus: Succeeded
  UserId: [redacted].com.au
  UserKey: 1003000093F

Add-DistributionGroupMember
Add-MailboxFolderPermission
Add-MailboxPermission
Add-RecipientPermission
AddFolderPermissions
Create
Enable-AddressListPaging
FolderBind
HardDelete
Install-AdminAuditLogConfig
Install-DataClassificationConfig
Install-DefaultSharingPolicy
Install-ResourceConfig
MailboxLogin
ModifyFolderPermissions
Move
New-ExchangeAssistanceConfig
New-InboxRule
New-Mailbox
New-MailboxRelocationRequest
New-MailboxRestoreRequest
New-MigrationBatch
Remove-App
Remove-MailboxLocation
Remove-MoveRequest
Remove-UnifiedGroup
SendAs
Set-AdminAuditLogConfig
Set-DistributionGroup
Set-ExchangeAssistanceConfig
Set-MailUser
Set-Mailbox
Set-OwaMailboxPolicy
Set-RecipientEnforcementProvisioningPolicy
Set-SyncUser
Set-TenantObjectVersion
Set-TransportConfig
Set-UnifiedGroup
Set-User
SoftDelete
Update
Update-DistributionGroupMember

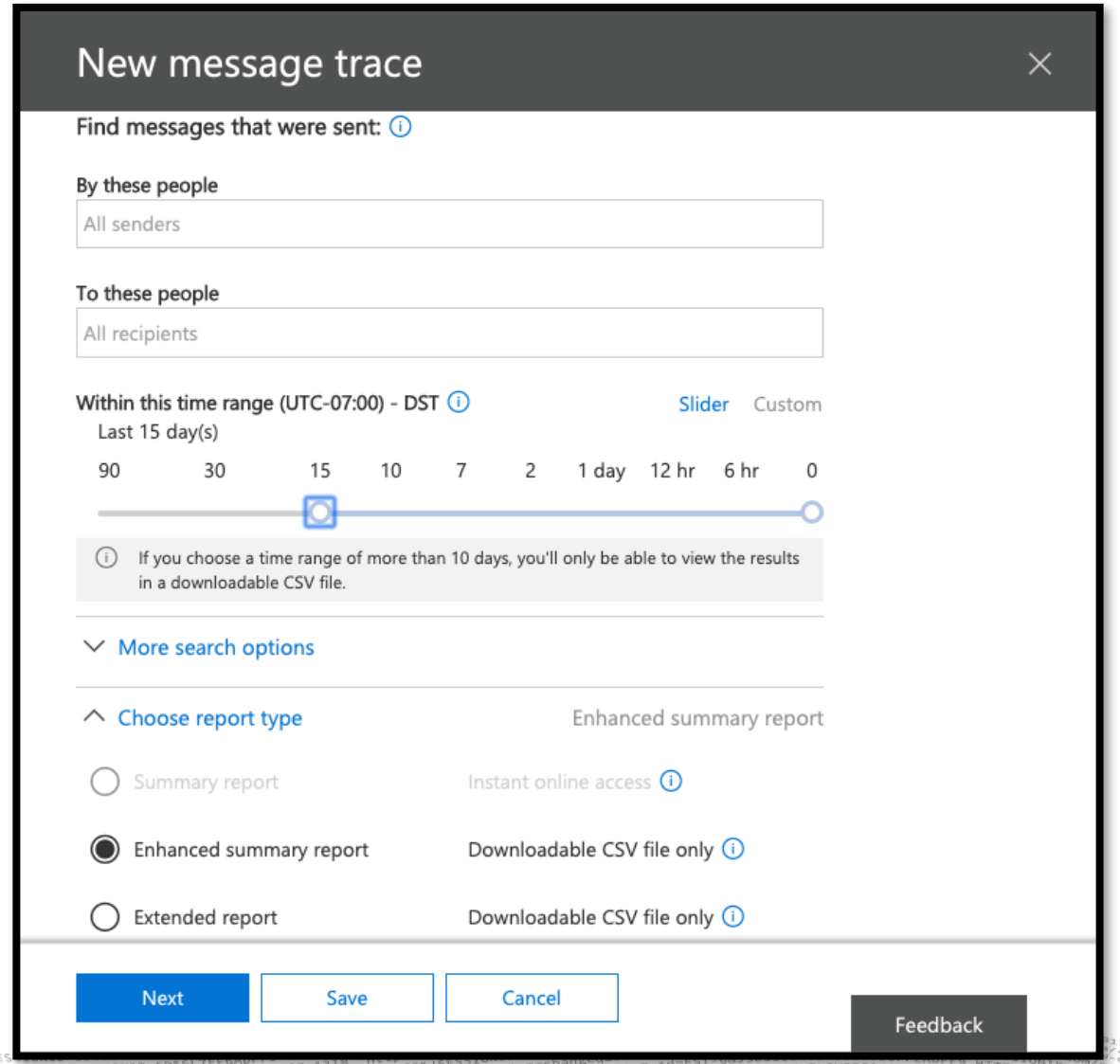
The Why

Mailbox investigations | Spam & phishing | Account compromise | Misconfigurations | Device Management | Capacity planning | etc

splunk> .conf18

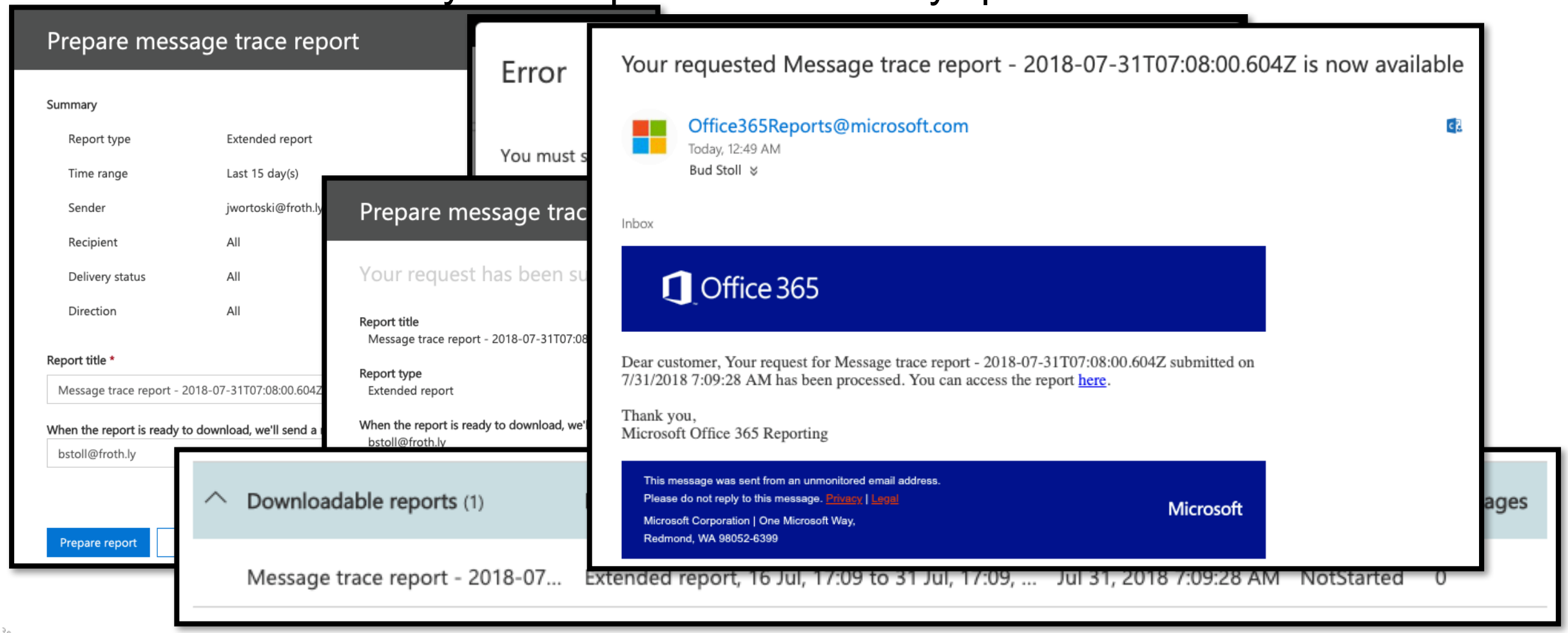
Exchange Admin Center – Message Trace

Searching over last 10 days works fine, BUT



Exchange Admin Center – Message Trace

Any search prior to last 10 days presents this:



Portal message traces can take hours to be returned!

splunk> .conf18

Exchange Online

splunk>enterprise App: Microsoft Cloud App for Splunk - SB 1.0.1 ▾ | Administrator ▾ | Messages ▾ | Settings ▾ | Activity ▾ | Help ▾ | Find

Office365 ▾ | Exchange Online ▾ | OneDrive ▾ | Security ▾ | App Check | Splunk ▾ | Microsoft Cloud App for Splunk - SB 1.0.1

Exchange Online - Message Trace

Edit | Export ▾ | ...

Option: Sender ✕ | Sender: paidemail@inboxdollars.com | Sep 11 through 30, 2017 ▾ | Hide Filters

_time	SenderAddress	RecipientAddress	Subject	Status
2017-09-19 04:24:04.422	paidemail@inboxdollars.com	jwortoski@froth.ly	Come back and keep earning with InboxDollars	Failed
2017-09-19 04:25:20.000	paidemail@inboxdollars.com	ubuntu@ec2-34-212-75-178.us-west-2.compute.amazonaws.com	Come back and keep earning with InboxDollars	Delivered
2017-09-19 04:25:20.000	paidemail@inboxdollars.com	ghoppy@froth.ly	Come back and keep earning with InboxDollars	Delivered
2017-09-18 06:05:27.000	paidemail@inboxdollars.com	ubuntu@ec2-34-212-75-178.us-west-2.compute.amazonaws.com	Get your complimentary copy of The Economist	Delivered
2017-09-18 06:05:27.000	paidemail@inboxdollars.com	ghoppy@froth.ly	Get your complimentary copy of The Economist	Delivered
2017-09-18 06:05:27.000	paidemail@inboxdollars.com	klagerfield@froth.ly	Get your complimentary copy of The Economist	Failed
2017-09-18 06:05:27.000	paidemail@inboxdollars.com	jwortoski@froth.ly	Get your complimentary copy of The Economist	Failed
2017-09-16 06:35:35.000	paidemail@inboxdollars.com	jwortoski@froth.ly	Apply for a RushCard PrePaid Visa	Failed
2017-09-16 06:35:35.000	paidemail@inboxdollars.com	klagerfield@froth.ly	Apply for a RushCard PrePaid Visa	Failed
2017-09-16 06:35:35.000	paidemail@inboxdollars.com	ubuntu@ec2-34-212-75-178.us-west-2.compute.amazonaws.com	Apply for a RushCard PrePaid Visa	Delivered

OneDrive

{ [-]
  ClientIP: [redacted]
  CorrelationId: ae207c9e-0054-6000-3667-3ef231038918
  CreationTime: 2018-07-19T00:08:42
  EventSource: SharePoint
  Id: 1c0c33fe-daa3-4d11-b586-08d5ed0bc9c3
  ItemType: File
  ListId: 67091393-e290-421e-ac6a-2734e2b12a94
  ListItemUniqueId: 933f7827-29c5-47a0-b41b-c977a7f70420
  ObjectId: https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/Documents/office365.jpg
  Operation: FileDeleted
  OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
  RecordType: 6
  Site: 66079e37-e489-49f1-b266-513657d785bb
  SiteUrl: https://jacobsmythe111-my.sharepoint.com/personal/ry_froth_ly/
  SourceFileExtension: jpg
  SourceFileName: office365.jpg
  SourceRelativeUrl: Documents
  UserAgent: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_14_0) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/67.0.3396.99 Safari/537.36
  UserId: ry@froth.ly
  UserKey: i:0h.f|membership|10033fffac46b0e1@live.com
  UserType: 0
  Version: 1
  WebId: 7acb35b6-e1ec-44ed-9099-38580e330ed0
  Workload: OneDrive
}

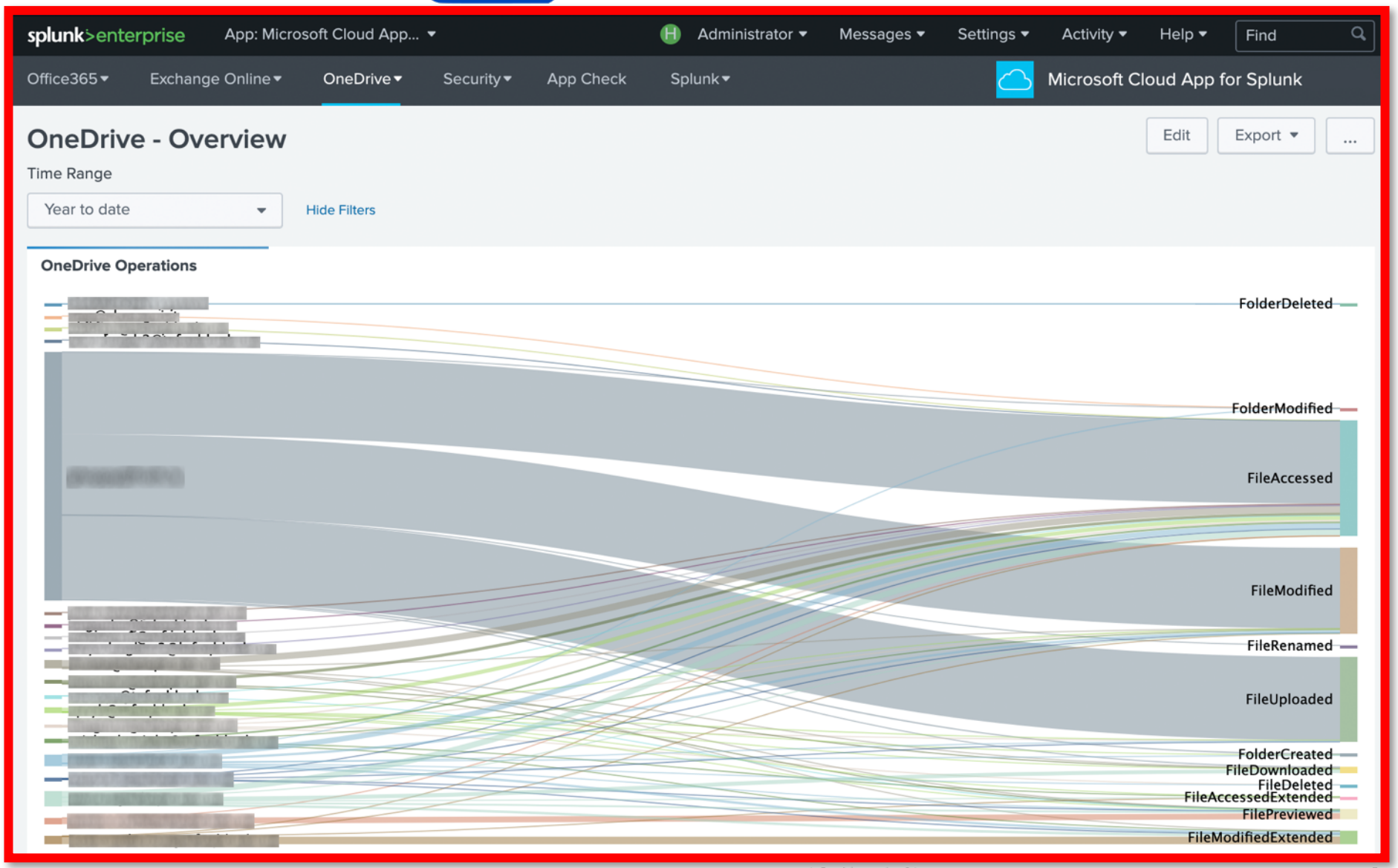
AccessRequestApproved
AccessRequestCreated
AddedToGroup
AddedToSecureLink
AnonymousLinkCreated
CompanyLinkCreated
CompanyLinkUsed
FileAccessed
FileAccessedExtended
FileCheckedIn
FileCheckedOut
FileCopied
FileDeleted
FileDeletedFirstStageRecycleBin
FileDownloaded
FileMalwareDetected
FileModified
FileModifiedExtended
FileMoved
FilePreviewed
FileRenamed
FileRestored
FileSyncDownloadedFul
FileSyncDownloadedPartia
FileSyncUploadedFul
FileUploaded
FolderCreated
FolderDeleted
FolderModified
FolderMoved
FolderRenamed
FolderRestored
GroupAdded
ListCreated
ListUpdated
PageViewed
PageViewedExtended
PermissionLevelAdded
RemovedFromSecureLink
RemovedFromSharedWithMe
RemovedFromSiteCollection
SecureLinkCreated
SecureLinkDeleted
SecureLinkUsed
SharingInheritanceBroken
SharingRevoked
SharingSet
SiteCollectionAdminAdded
SiteCollectionAdminRemoved
SiteCollectionCreated
WACTokenShared

The Why

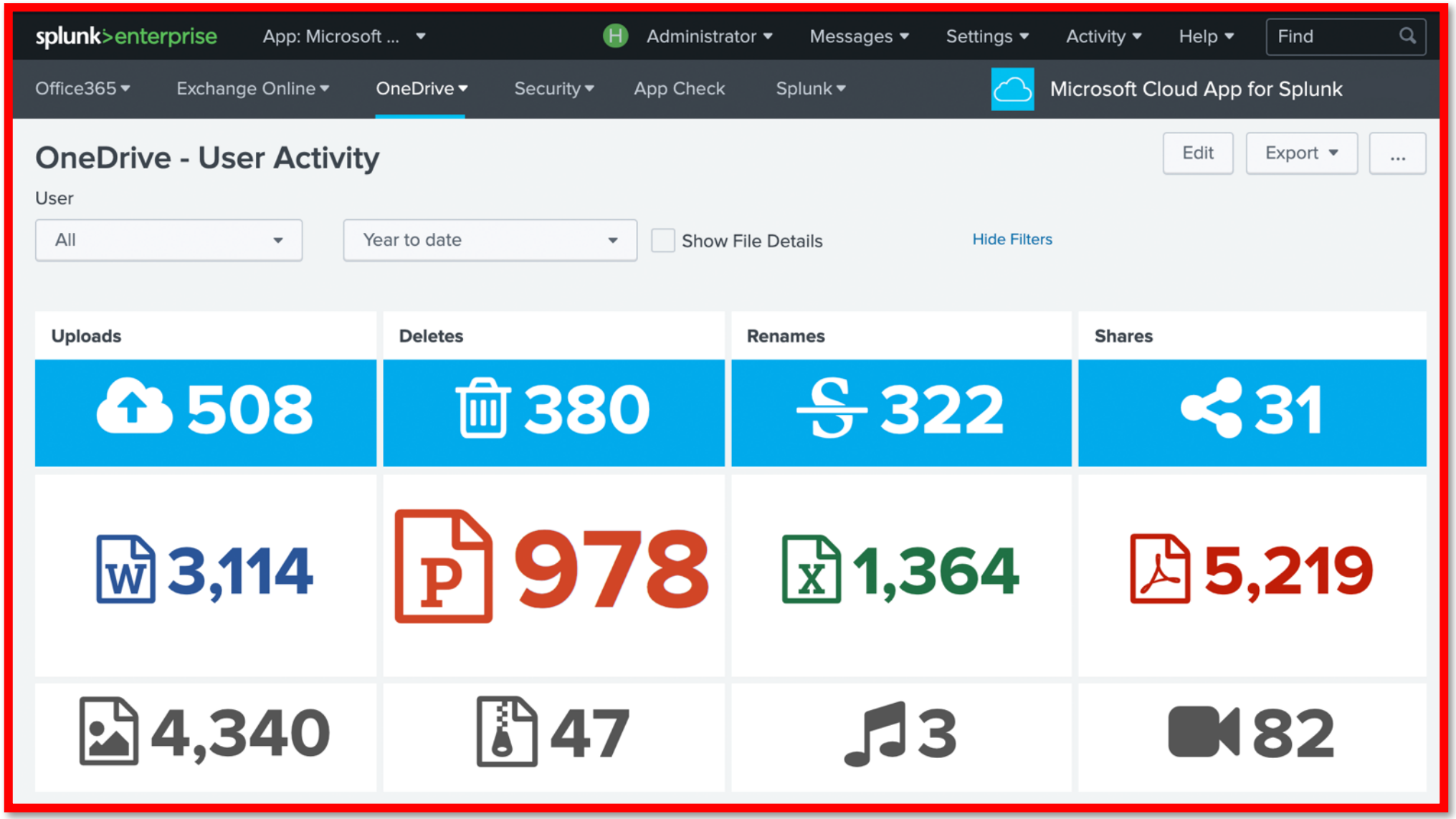
File auditing | External access | Geographical tracking | Policy enforcement | Adoption | Capacity planning | etc

splunk> .conf18

OneDrive



OneDrive



{ [-]
ClientIP:
CorrelationId: adea799e-2086-6000-36d2-
CreationTime: 2018-07-12T03:17:10
EventData: <Sharing level> </Sharing level><ExpirationDate>10/10/2018 3:17:07 AM</ExpirationDate>
EventSource: SharePoint
Id: 4f478f4b-31de-486f-dfcb-
ItemType: Web
ObjectId: .sharepoint.com/sites/
Operation: SharingInvitationCreated
OrganizationId: a74a1efc-372d-476c-802c-
RecordType: 14
Site: a2edde81-b268-4584-a7a8-
SiteUrl: .sharepoint.com/sites/
TargetUserOrGroupName: @rhombergrail.com
TargetUserOrGroupType: Guest
UniqueSharingId: 00000000-0000-0000-0000-
UserAgent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729;
.NET CLR 3.5.30729; Tablet PC 2.0; wbx 1.0.0)
UserId: .com.au
UserKey: @live.com
UserType: 0
Version: 1
WebId: d2f1ea5a-57e0-41e0-92e6-
Workload: SharePoint
}

AccessRequestApproved
AccessRequestCreated
AccessRequestUpdated
AddedToGroup
AddedToSecureLink
CommentCreated
CommentsDisabled
CompanyLinkCreated
CompanyLinkUsed
FileAccessed
FileAccessedExtended
FileCheckOutDiscarded
FileCheckedIn
FileCheckedOut
FileCopied
FileDeleted
FileDownloaded
FileModified
FileModifiedExtended
FileMoved
FilePreviewed
FileRenamed
FileRestored
FileSyncDownloadedFull
FileSyncUploadedFull
FileUploaded
FolderCreated
FolderDeleted
FolderModified
FolderMoved
FolderRenamed
GroupAdded
GroupRemoved
GroupUpdated
ListCreated
ListDeleted
ListUpdated
PageViewed
PageViewedExtended
RemovedFromGroup
SearchQueryPerformed
SecureLinkCreated
SecureLinkUsed
SharingInheritanceBroken
SharingInvitationCreated
SharingRevoked
SharingSet
SiteCollectionAdminAdded
SiteCollectionAdminRemoved
SiteCollectionCreated
WACTokenShared

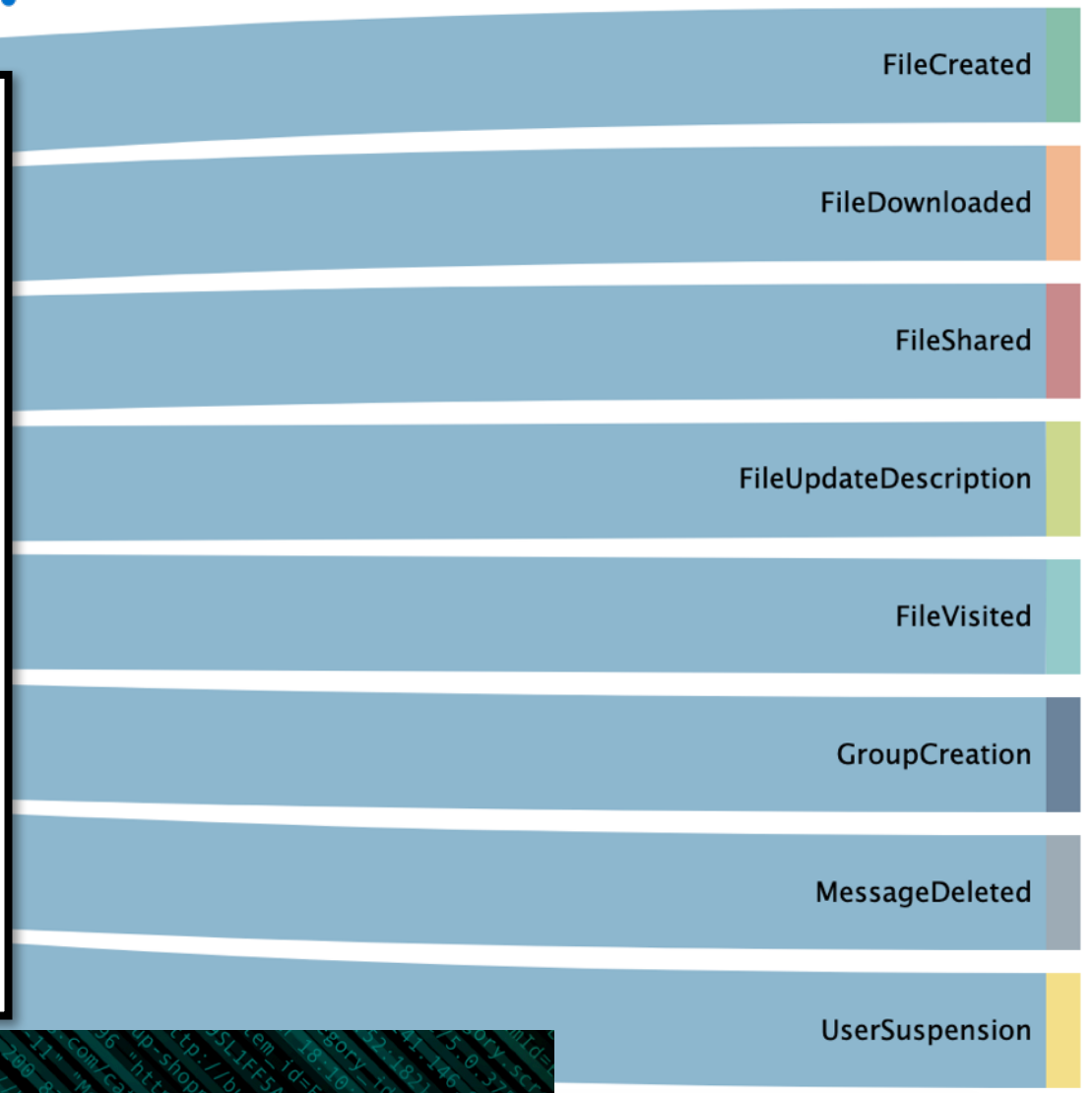
The Why

File/Folder/List/Page/Site auditing | External access | Adoption metrics | Content management | Capacity planning | etc

splunk> .conf18

Yammer

{ [-]
ActorUserId: ry@froth.ly
ActorYammerUserId: 1676211209
ClientIP: [redacted]
CreationTime: 2018-06-24T22:51:40
GroupName: Australian Beers
Id: 8d290ecf-0c5d-436e-ab42-eb56b94e8884
ObjectId: Australian Beers
Operation: GroupCreation
OrganizationId: 225e05a1-5914-4688-a404-7030e60f3143
RecordType: 22
ResultStatus: True
UserId: ry@froth.ly
UserKey: 10033fffac46b0e1
UserType: 0
Version: 1
Workload: Yammer
YammerNetworkId: 9987608
}
Show as raw text



The Why

File auditing | User auditing | Message tracking | Adoption | etc

splunk> .conf18

Skype for Business

{ [-]
  CmdletVersion: 7.0.2111.9
  CreationTime: 2018-07-12T04:44:06
  ExternalAccess: false
  Id: 923268c3-fc26-4e50-83a0-
  ObjectName: CsOnlineUser
  Operation: Get-CsOnlineUser
  OrganizationId: d3565d8f-13a5-40f4-97f6-
  Parameters: [[-]
    { [-]
      Name: Filter
      Value: ((TenantId -eq "[redacted]") -and (Enabled -eq $True) -and (UserRoutingGroupId -ne $null))
    }
    { [+]
    }
  ]
  RecordType: 23
  ResultStatus: Succeeded
  SkypeForBusinessEventType: 2
  TenantName: d3565d8f-13a5-40f4-97f6-
  UserId: [redacted]
  UserKey: 10033FFF9
  UserType: 2
  Version: 1

- Get-CSTenantFederationConfiguration
- Get-CSTenantLicensingConfiguration
- Get-CsMeetingConfiguration
- Get-CsOnlineUser
- Get-CsTenant
- Get-CsTenantLicensingConfiguration
- Set-CsOnlineDirectoryTenant
- Set-CsTenantLicensingConfiguration

The Why

File auditing | User auditing | Message tracking | Adoption | Licensing | etc

splunk> .conf18

Microsoft Teams

{ [-]
  CreationTime: 2018-07-23T06:41:03
  Id: 9095e8e0-4f23-4076-bc38-
  Operation: TeamCreated
  OrganizationId: a74a1efc-372d-476c-802c-
  RecordType: 25
  TeamGuid: 19:172cf34bf6f14d31a8a1b097348b11cc@thread.skype
  TeamName: [redacted]
  UserId: [redacted].com.au
  UserKey: 28032c53-fb3e-48cc-b328-
  UserType: 0
  Version: 1
  Workload: MicrosoftTeams
}
Show as raw text

ChannelAdded
ChannelDeleted
ChannelSettingChanged
MemberAdded
MemberRemoved
MemberRoleChanged
TabAdded
TabRemoved
TabUpdated
TeamCreated
TeamDeleted
TeamSettingChanged
TeamsSessionStarted

The Why

File auditing | User auditing | Message tracking | Adoption | etc

Power BI

{ [-]
  Activity: CreateDataset
  ClientIP: [redacted]
  CreationTime: 2018-07-23T05:10:47
  DataConnectivityMode: Import
  DatapoolRefreshScheduleType: None
  DatapoolType: Undefined
  DatasetId: 38a1bec2-2825-46ac-9f9d-[redacted]
  DatasetName: [redacted]
  Id: 8fff97f8-c413-419a-884a-
  IsSuccess: true
  ItemName: [redacted]
  ObjectId: [redacted]
  Operation: CreateDataset
  OrganizationId: a74a1efc-372d-476c-802c-
  RecordType: 20
  UserAgent:
  UserId: [redacted].com.au
  UserKey: 10033FFF9B[redacted]
  UserType: 0
  WorkSpaceName: My Workspace
  Workload: PowerBI
  WorkspaceId: My Workspace

AnalyzedByExternalApplication
ChangeGatewayDatasourceUsers
CreateApp
CreateDashboard
CreateDataset
CreateEmailSubscription
CreateGroup
CreateOrgApp
CreateReport
DeleteDashboard
DeleteDataset
DeleteGateway
DeleteReport
DownloadReport
EditDataset
EditReport
ExportReport
ExportTile
Import
InstallApp
OptInForProTrial
PrintDashboard
PrintReport
RefreshDataset
RemoveDatasourceFromGateway
RenameDashboard
SetScheduledRefresh
ShareDashboard
ShareReport
UpdateApp
ViewDashboard
ViewReport
ViewTile
ViewUsageMetrics

The Why

User Auditing | Usage metrics | Dataset auditing | Adoption | Workspace planning | Dashboard views | etc

splunk> .conf18

Microsoft Dynamics 365

{ [-]
  ClientIP: [redacted]:43604
  CorrelationId: 00000000-0000-0000-0000-000000000000
  CreationTime: 2018-07-19T01:03:07
  CrmOrganizationUniqueName: [redacted]
  EntityId: df5f827d-ef8a-e811-a841-
  EntityName: incident
  Fields: [[+]
  ]
  Id: 254a952d-b26d-4a4e-b290-
  InstanceUrl: [redacted].crm6.dynamics.com/
  ItemType: Dynamics365
  ItemUrl: [redacted] crm6.dynamics.com/main.aspx?etn=incident&pagetype=entityrecord&id=df5f827d-ef8a-e811-a841-
  Message: Create
  ObjectId: Create incident
  Operation: CrmDefaultActivity
  OrganizationId: a74a1efc-372d-476c-802c-
  PrimaryFieldValue:
  Query:
  QueryResults:
  RecordType: 21
  ResultStatus: Success
  ServiceContextId: 00000000-0000-0000-0000-

Associate
CheckIncomingEmail
CheckPromoteEmail
CleanUpBulkOperation
Create
CreateActivitiesList
CreateMiniCampaign
CreateResourceGroupsForTeams
CreateResourcesForUsers
DeliverIncomingEmail
DeliverPromoteEmail
ExecuteQuickFind
ExecuteTransaction
ExecuteWorkflow
ExpandWorkflows
Get
ImportSolution
InitializeFrom
InstantiateTemplate
IsPrimaryClientSubscriptionClients
IsSystemAdministratorRole
LogFailureBulkOperation
PostOutlookSyncSubscriptionClients
PrepareOutlookSyncSubscriptionClients
ProcessInboundEmail
ProcessOneMemberBulkOperation
SaveEntityGroupConfiguration
SendEmail
SetActionCardState
SetState
ShouldDisplaySLALimitNotification
StatusUpdateBulkOperation
Update
UpdateRecentItems
msdyn_GetLegalAcceptanceStatus
msdyn_GetSIPackageStatus
msdyn_GetTalkingPoints
aryNameFieldForOQOIDetailEntities
msdyncrm_LitmusGetListOfClients
msdyncrm_LitmusGetUserDetails

The Why

User auditing | Workflow auditing | Campaign tracking | Adoption | etc

splunk> .conf18

Microsoft Stream

{ [-]
  ClientApplicationId: cf53fce8-def6-4aeb-8d30-
  ClientIP:
  CreationTime: 2018-07-23T06:35:26
  EntityPath: /api/videos
  Id: 11c57be8-c946-4f58-a93f-
  ObjectId: 78c15917-10fa-4b0c-aae0-
  Operation: StreamCreateVideo
  OperationDetails: {"Name":"
  OrganizationId: a74a1efc-372d-476c-802c-
  RecordType: 32
  ResourceTitle:
  ResourceUrl: https://www.microsoftstream.com/videos/78c15917-10fa-4b0c-aae0-
  ResultStatus: Succeeded
  UserId:
  UserKey: a09938d3-8646-4a92-a95b-
  UserType: 0
  Version: 1
  Workload: MicrosoftStream
}

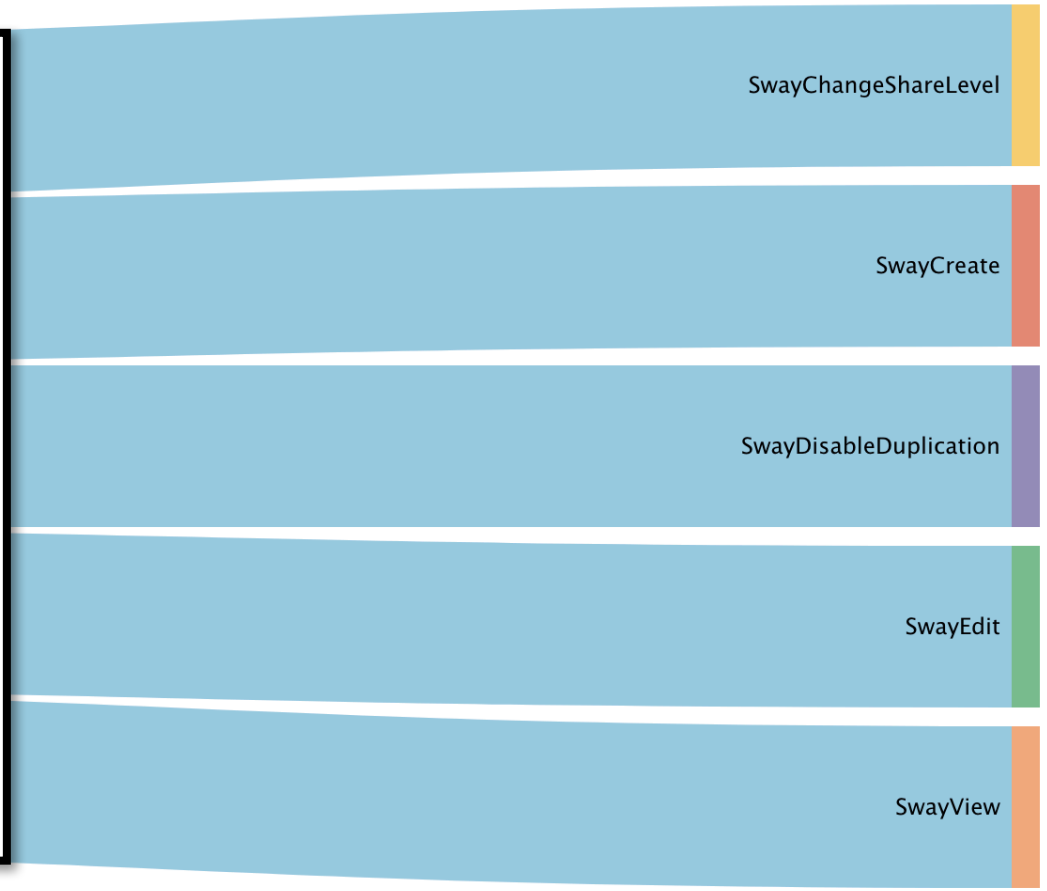
- StreamCreateChannel
- StreamCreateVideo
- StreamEditGroup
- StreamEditUserSettings
- StreamEditVideo
- StreamInvokeChannelSetThumbnail
- StreamInvokeVideoSetLink
- StreamInvokeVideoUpload
- StreamInvokeVideoView

The Why

stream auditing | User auditing | Capacity planning | Adoption | External access | etc

Sway

{ [-]
  BrowserName: Chrome
  ClientIP:
  CreationTime: 2018-07-20T06:12:39
  Id: db64e3b7-ed6f-4a7f-5f59-
  ObjectId: DFeTnIPduf2
  Operation: SwayCreate
  OrganizationId: a74a1efc-372d-476c-
  RecordType: 12
  SiteUrl: https://sway.com/
  UserId: .com.au
  UserKey: 10037ffeab6
  UserType: 0
  Version: 1
  Workload: Sway
}



The Why

File auditing | User auditing | Adoption | etc

splunk> .conf18

Security & Compliance Center

{ [-]
  Case:
  CreationTime: 2018-07-23T07:37:40
  ExchangeLocations: Include:[All]
  ExtendedProperties: [[+]
  ]
  Id: 69945c16-fcb1-4f88-e028-
  ObjectId: [redacted]@gmail.com
  ObjectType: Search
  Operation: SearchStarted
  OrganizationId: a74a1efc-372d-476c-802c-
  Parameters: [[-]
    { [+]
    }
    { [-]
      Name: Cmdlet
      Value: Start-ComplianceSearch
    }
    { [+]
    }
  ]
  PublicFolderLocations:
  Query: (c:c)(date=2018-06-22..2018-07-23)(from=[redacted]@gmail.com)
  RecordType: 24
  SharepointLocations:
  UserId: [redacted].com.au
  UserKey: 1c54da9e-9b24-46e7-ba13-
  UserType: 0
  Version: 1
  Workload: SecurityComplianceCenter

- Get-ComplianceSearch
- Get-ComplianceSearchAction
- Get-QuarantineMessage
- New-ComplianceSearch
- New-ComplianceSearchAction
- SearchCreated
- SearchExportDownloaded
- SearchPreviewed
- SearchReport
- SearchResultsPurged
- SearchStarted
- SearchUpdated
- SearchViewed
- Start-ComplianceSearch
- UserSubmission
- ViewedSearchPreviewed
- ViewedSearchReport

The Why

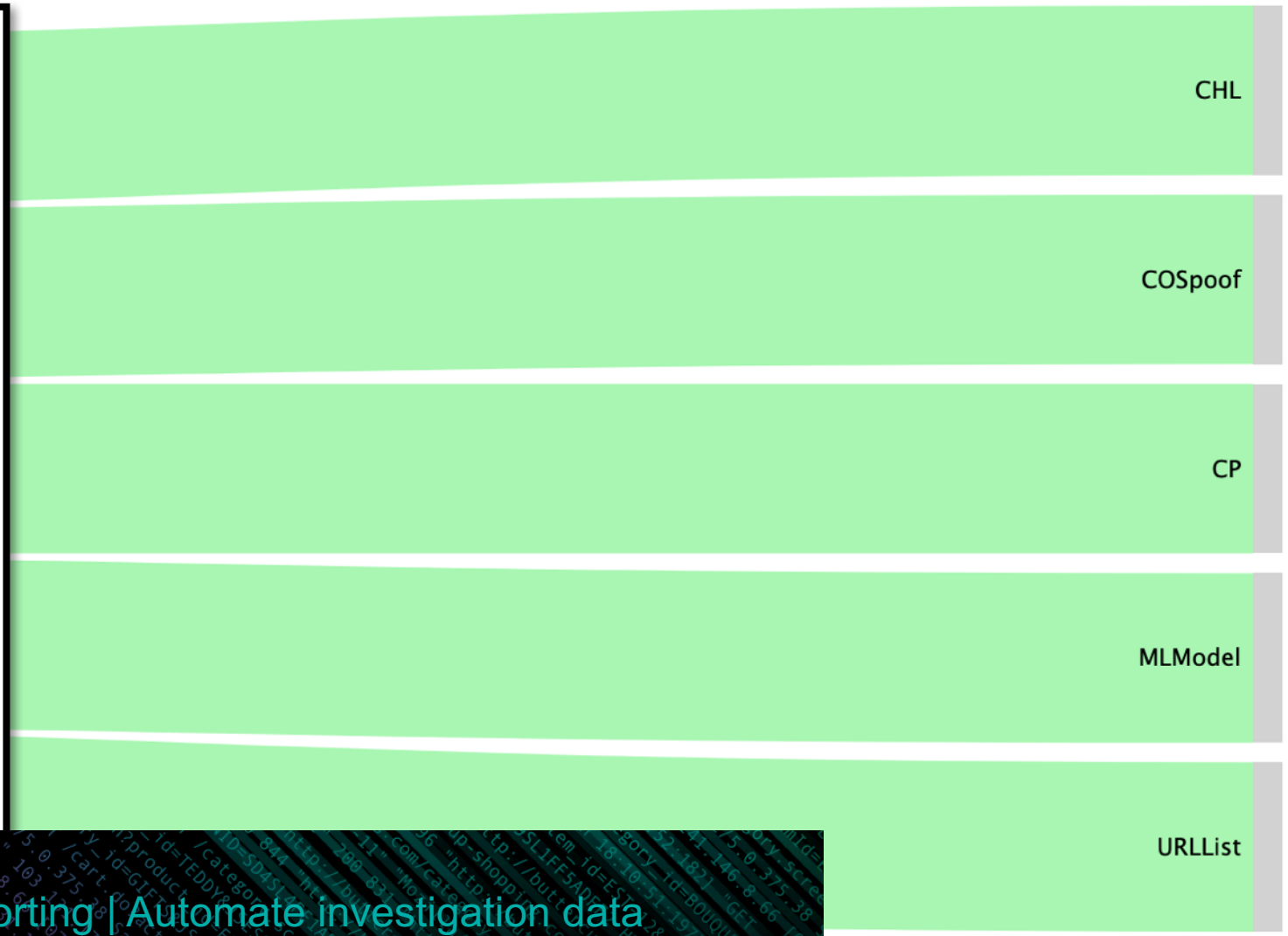
User auditing | Email auditing | Auditor auditing | Compliance reporting

splunk> .conf18

Threat Intelligence

Detection methods:


```
{ [-]
  AttachmentData: [ [-]
    { [-]
      FileName: ProjectEmailLogo.png
      FileType: Png
      FileVerdict: 0
      MalwareFamily:
      SHA256: 740D68688A344A409E5628E8665AAC95902D1D4B4CD6
    }
  ]
  CreationTime: 2018-07-23T10:08:47
  DetectionMethod: COSpoof
  DetectionType: Inline
  Id: 0e1d62ee-058b-491c-a060-
  InternetMessageId: <
  MessageTime: 2018-07-23T10:05:49
  NetworkMessageId: ad048189-d17d-4243-1323-
  ObjectId: ad048189-d17d-4243-1323-
  Operation: TIMailData
  OrganizationId: a74a1efc-372d-476c-802c-
  P1Sender:
  P2Sender:
  Recipients: [ [+]
  ]
  RecordType: 28
  SenderIp:
  Subject:
  ThreadDetectionMethods: [ [+]
  ]
  UserId:
  UserKey: ThreatIntel
```

The Why

Correlate feeds with internal data | Security reporting | Automate investigation data collection | etc

splunk> .conf18

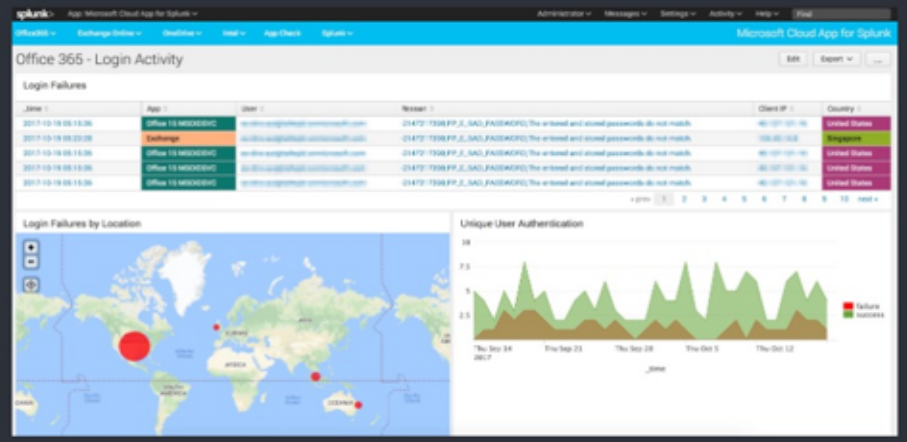
splunkbase

Search App by keyword, technology...

My Account | My Splunk | Support & Services

Microsoft Cloud App for Splunk

★★★★★ 2 ratings



ADMINISTRATOR TOOLS: Manage App | View App | View Analytics

Overview | Details

The Microsoft Cloud App for Splunk provides out of the box visualisations for event data from:

* Splunk Add-on for Microsoft Cloud Services
* Microsoft Office 365 Reporting Add-on for Splunk

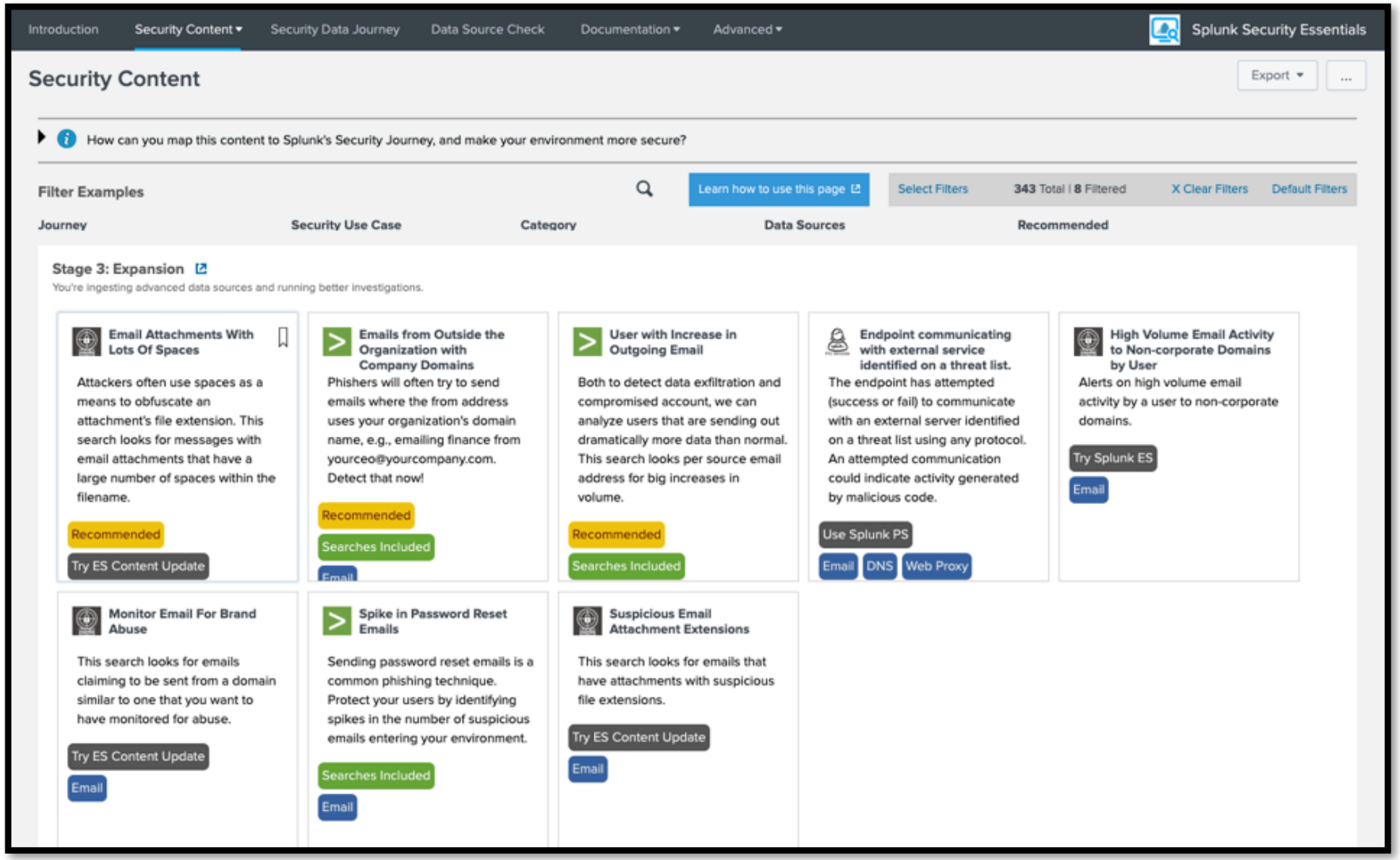
139 Installs

254 Downloads

Download | Rate this App

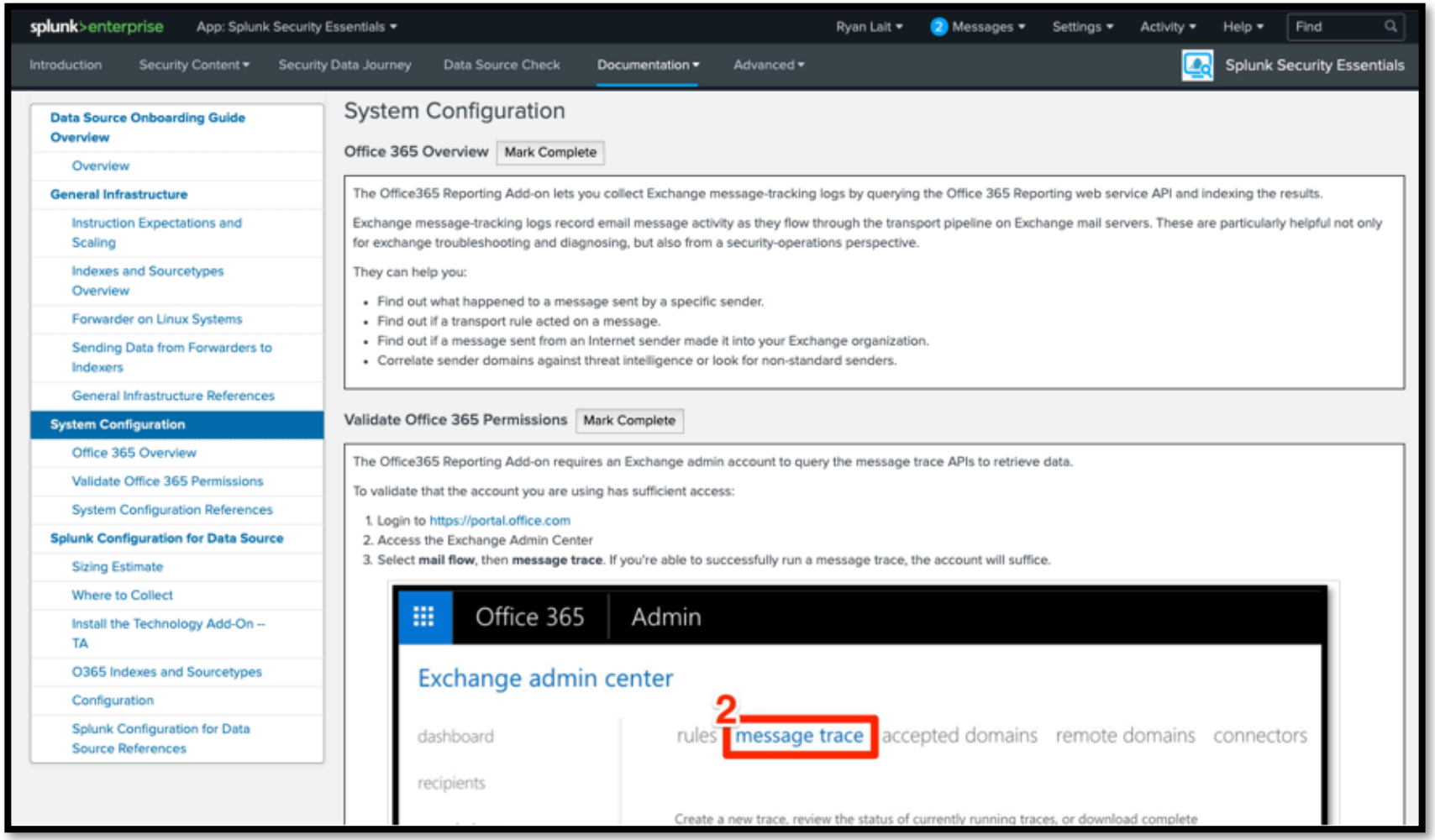
splunk> .conf18

Office 365 ‘ing with Splunk Security Essentials



Office 365 ‘ing with Splunk Security Essentials

Data onboarding guide – Exchange message tracking logs



splunk> .conf18

Office 365 & Splunk Enterprise Security

Data onboarding guide – Exchange message tracking logs

CIM

Change Analysis
Authentication

Correlation Searches

Abnormally High Number of Endpoint Changes By User
Account Deleted
Anomalous Audit Trail Activity Detected
Brute Force Access Behavior Detected and Detected Over One Day
Concurrent Login Attempts Detected
Default Account Activity Detected
Excessive Failed Logins
Geographically Improbable Access Detected
High or Critical Priority Individual Logging into Infected Machine
Insecure Or Cleartext Authentication Detected
Network Change Detected and Network Device Rebooted
Same Error On Many Servers Detected
Short-lived Account Detected

Dashboards

access_anomalies
access_center
access_search
access_tracker
account_management
default_accounts
endpoint_changes
network_changes
user_activity

Office 365 & Splunk IT Service Intelligence

Data Sources

O365 Management API
Exchange Message Tracking Logs

Example KPI's

Failed vs Successful logins
Unique users
Subscription metrics
Adoption of O365 workloads
Mail counts – delivered Vs failed
CRM campaign metrics
Capacity planning
Predictive billing

ITSI Module COMING SOON!

Splunk & Azure

Microsoft IaaS + PaaS

splunk> .conf18

How Can You Use Data

Platform Analytics

- Diagnostic troubleshooting, alerting, capacity planning

Security Analytics

- Resource activity, DLP, threat correlation, compromised account monitoring, usage / billing anomalies

Compliance Reporting

- System and user access auditing for compliance reporting

Billing Insights

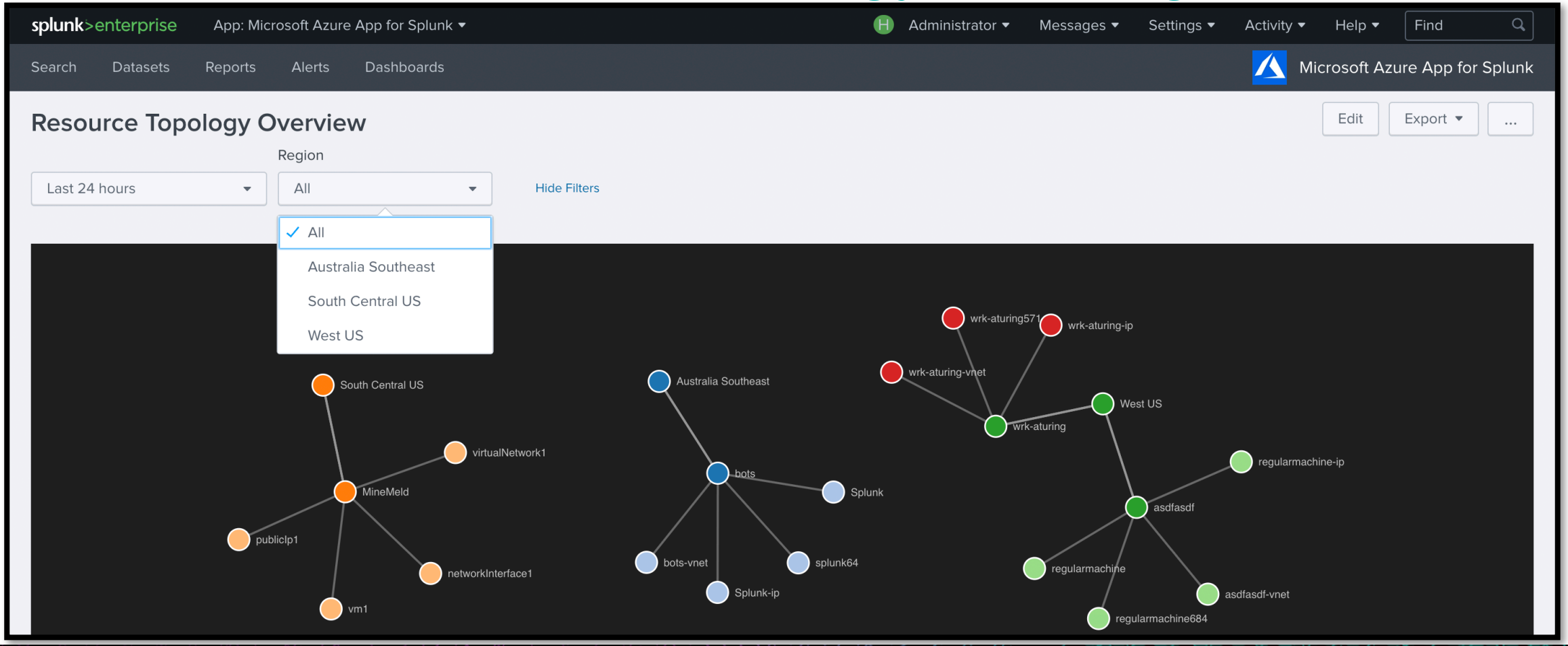
- Spend analysis
- Capacity planning
- On-prem vs cloud ROI

Azure Inventory & Asset Management

This is where the subtitle goes

Chase Mickey re: custom viz and asset mapping?

Resource Topology Mapping



The How

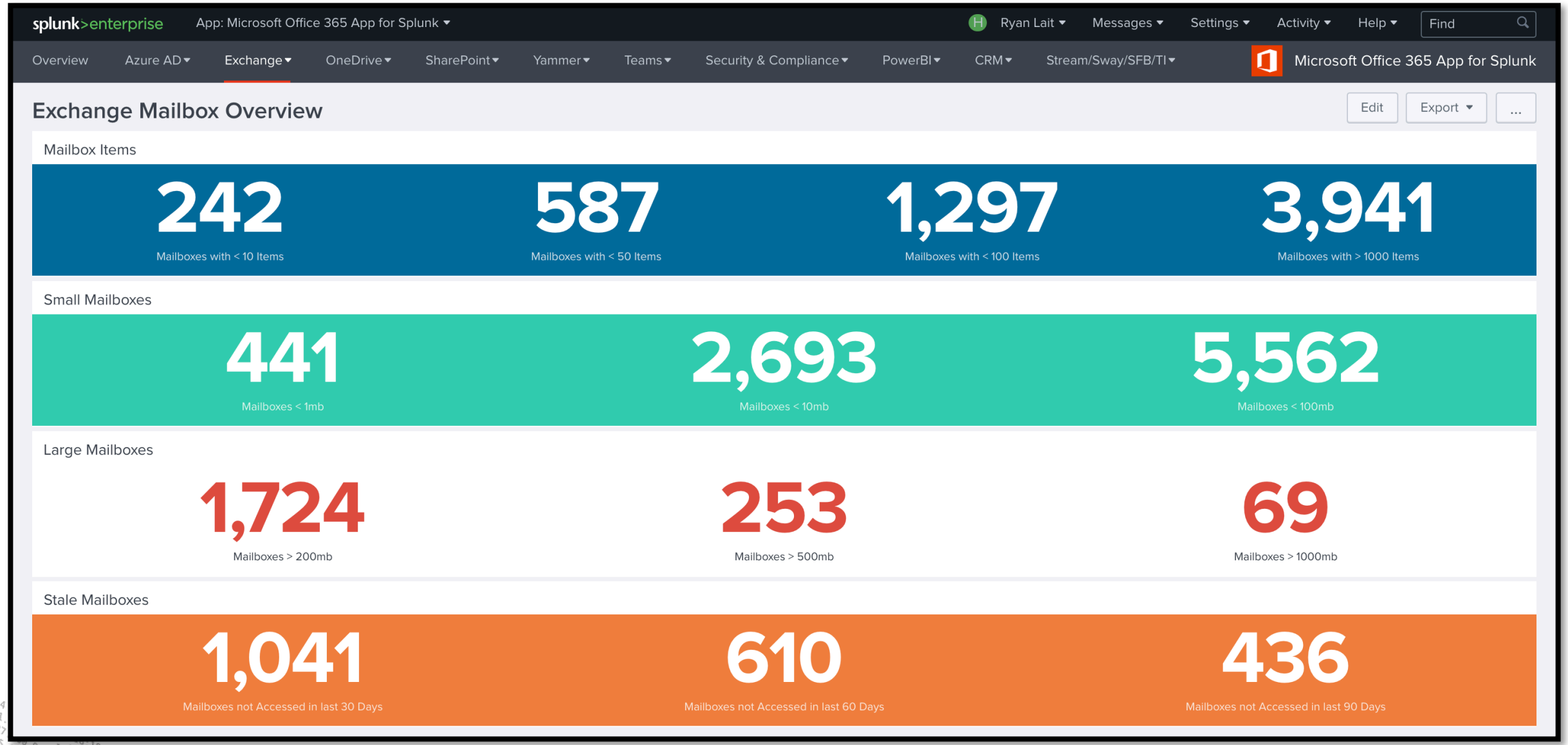
Install Force Directed App for Splunk

sourcetype=mscs:resource | stats count by location_name, resource_group_name, resource_name*

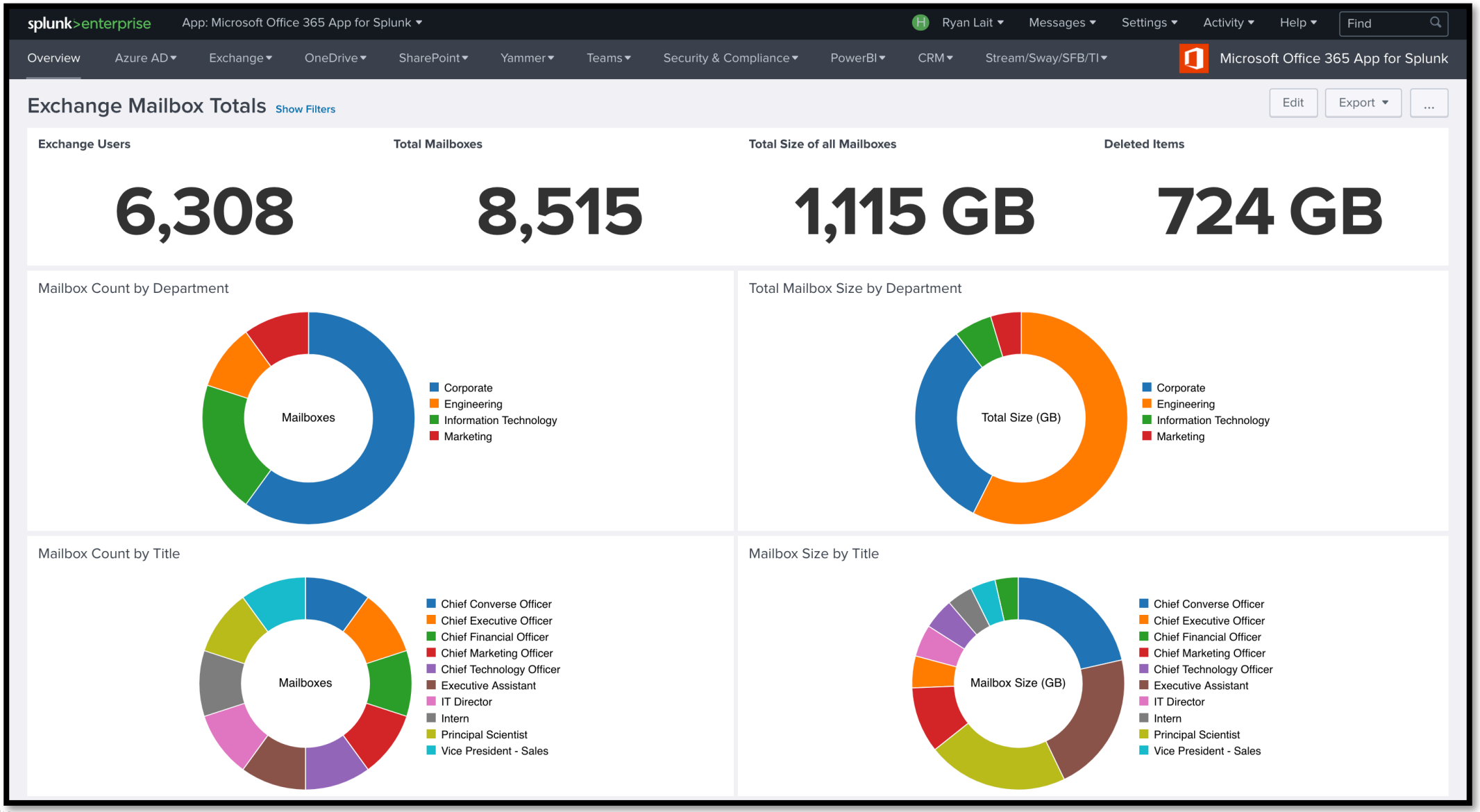
What If I Want More?

```powershell
$SplunkHost="13.210.[redacted]"
$SplunkEventCollectorPort ="8088"
$SplunkEventCollectorToken="6e5ef8d0-[redacted]"
$TenantCredentials = Get-AutomationPSCredential -Name "Exchange"
# Remove any existing Exchange Online sessions
Get-PSSession  | ?{$_.ComputerName -like "*.office365.com"} | Remove-PSSession | out-null

# Create a new Exchange Online session
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $TenantCredentials -Authentication Basic -AllowRedirection
Import-PSSession $Session -DisableNameChecking -AllowClobber | out-null
Connect-AzureAD -Credential $TenantCredentials

# Get all AzureADUsers
$UserList = Get-AzureADUser -All $true

# Append mailbox usage statistics to user information
$OutputArray = @()
Foreach($User in $UserList)
    {
    $totalsize = ([string](Get-MailboxStatistics -Identity $User.UserPrincipalName).Totalitemsize.value).split(" ")[0]
    $totaldeletedsize = ([string](Get-MailboxStatistics -Identity $User.UserPrincipalName).TotalDeletedItemSize.value).split(" ")[0]
    $Lastloggedondate = (Get-MailboxStatistics -Identity $User.UserPrincipalName).LastLogonTime
    $MailObject = "" | Select DisplayName, JobTitle, Department, PhysicalDeliveryOfficeName, StreetAddress, UserPrincipalName, TotalSize, TotalDeletedSize, LastLoggedOnDate
    $MailObject.DisplayName = $User.DisplayName
    $MailObject.JobTitle = $User.JobTitle
    $MailObject.Department = $User.Department
    $MailObject.PhysicalDeliveryOfficeName = $User.PhysicalDeliveryOfficeName
    $MailObject.StreetAddress = $User.StreetAddress
    $MailObject.UserPrincipalName = $User.UserPrincipalName
    $MailObject.TotalSize = $totalsize
    $MailObject.TotalDeletedSize = $totaldeletedsize
    $MailObject.LastLoggedOnDate = $Lastloggedondate
    $OutputArray += $MailObject
    $MailObject = $null
    }
Get-PSSession | ?{$_.ComputerName -like "*.office365.com"} | Remove-PSSession | out-null

# Throw events to Splunk HTTP Event Collector in JSON format
foreach ($m in $OutputArray) {
    $body = @{
        event =(ConvertTo-Json $m)
    }
    $uri = "http://" + $SplunkHost + ":" + $SplunkEventCollectorPort + "/services/collector"
    $header = @{"Authorization"="Splunk " + $SplunkEventCollectorToken}

    Invoke-RestMethod -Method Post -Uri $uri -Body (ConvertTo-Json $body) -Header $header
```

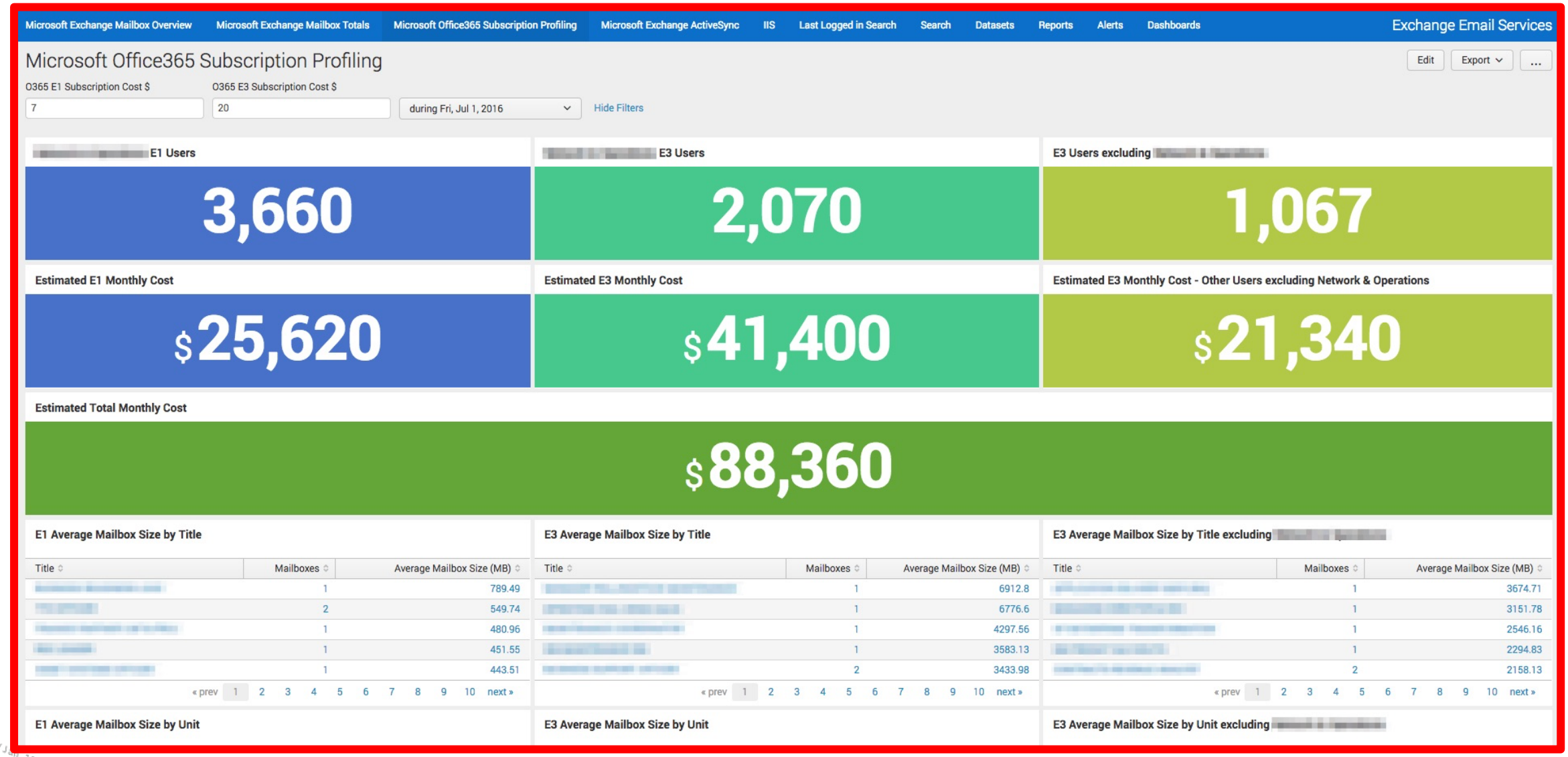
Mailbox Migration & Capacity Planning



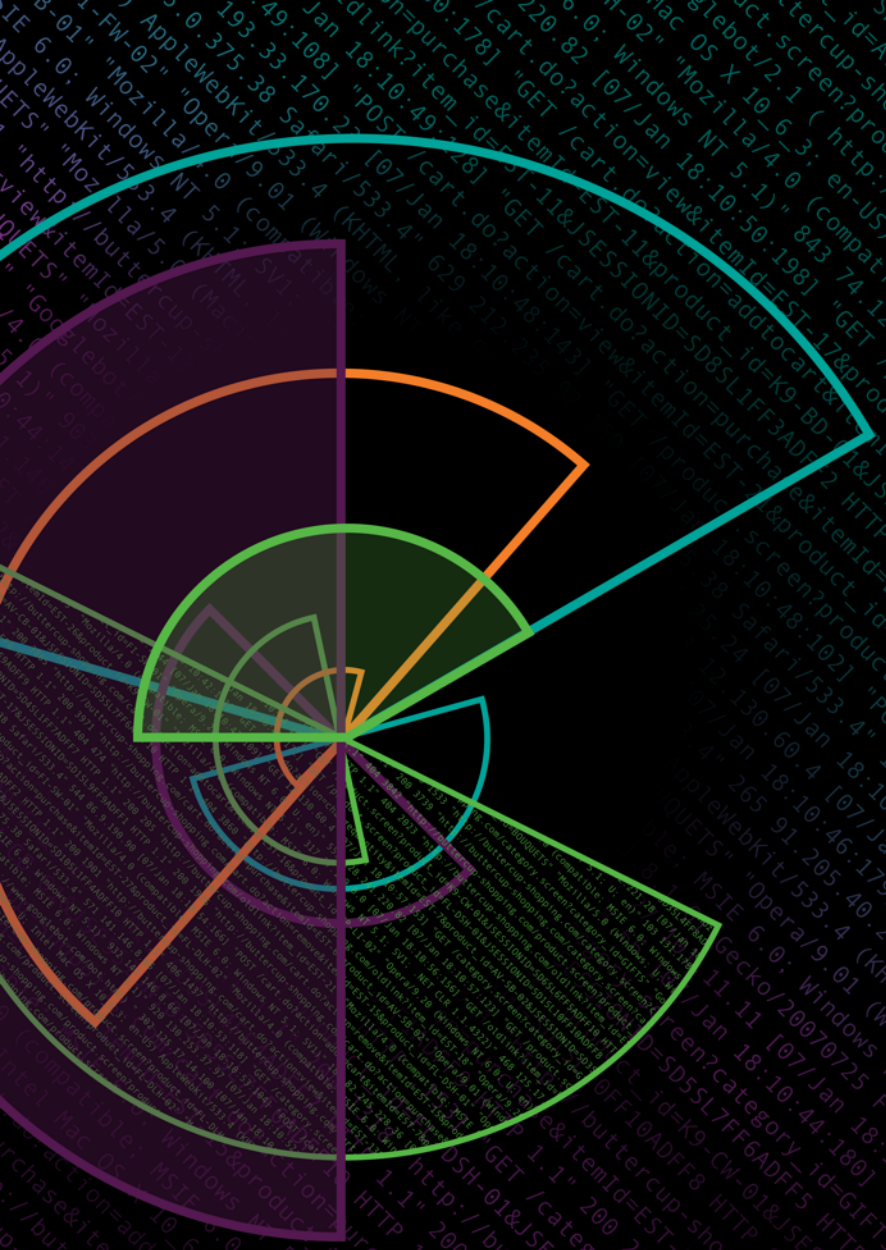
splunk> .conf18



Subscription Cost Modelling



splunk> .conf18



What next?

I want it all! Give it to me!

Splunk Resources

Blog Posts

- Step-by-step configuration guides
- Search & dashboard examples

Whitepapers & Docs

- Industry documentation provides context and resources to push ahead?

Splunkbase

- Pre-built dashboards, reports, alerts and actions to hit the ground running!

Boss of the SOC 3.0!

- Blue-team CTF specifically for Azure & O365!

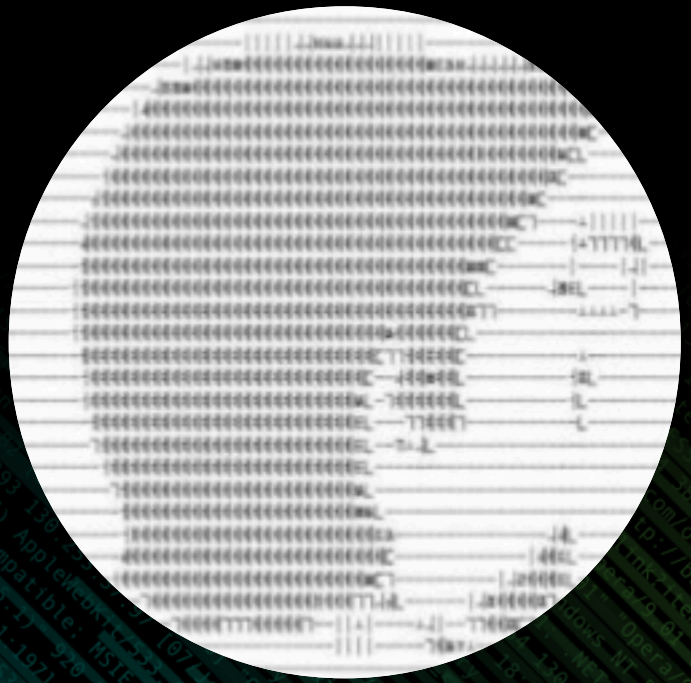
Key Takeaways

1. First level bullets should be sentence case, 28pt
2. First level bullets should be sentence case, 28pt
3. First level bullets should be sentence case, 28pt
4. Check out the other Azure & O365 sessions too!

More .conf18 Sessions!

GAIN END-TO-END VISIBILITY INTO YOUR AZURE CLOUD ENVIRONMENT USING SPLUNK

Jason Conger – Staff Solutions Architect



HUNTING THE KNOWN UNKNOWN: MICROSOFT CLOUD

Ryan Kovar – Principal Security Strategist

splunk> .conf18

ry@splunk.com

Don't forget to rate this session
in the .conf18 mobile app

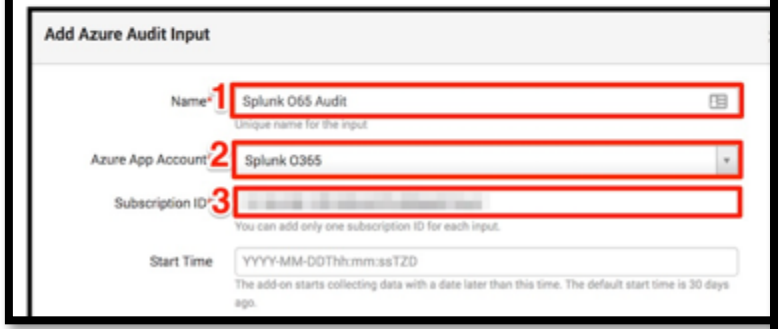
How Do I Splunk My Office 365 Data?

Configure the Inputs

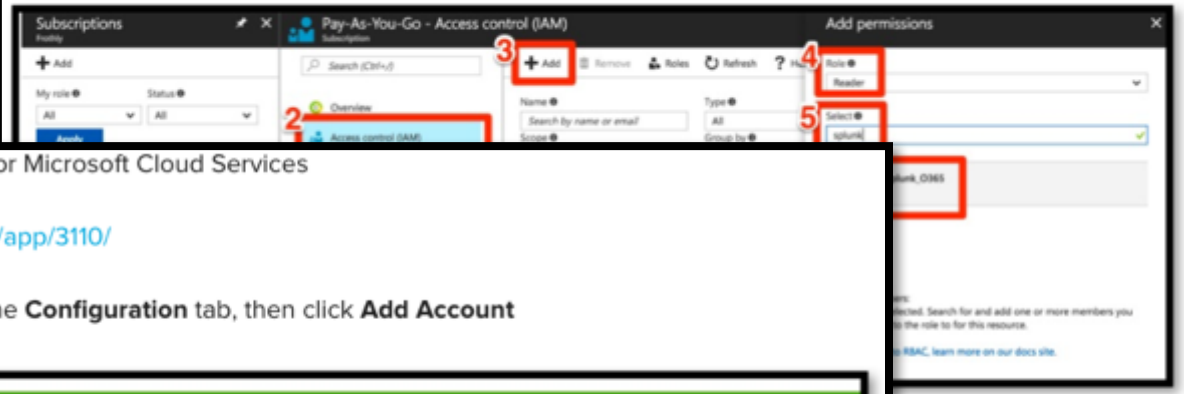
Now that we've created our AD app and have working credentials, we can configure the inputs.

36) Select **Inputs** > **Create New Input** > **Azure Audit**

37) Enter **Name**, specify **Account**, **Subscription ID** and **Index**. If required, modify t
Select **Add**.



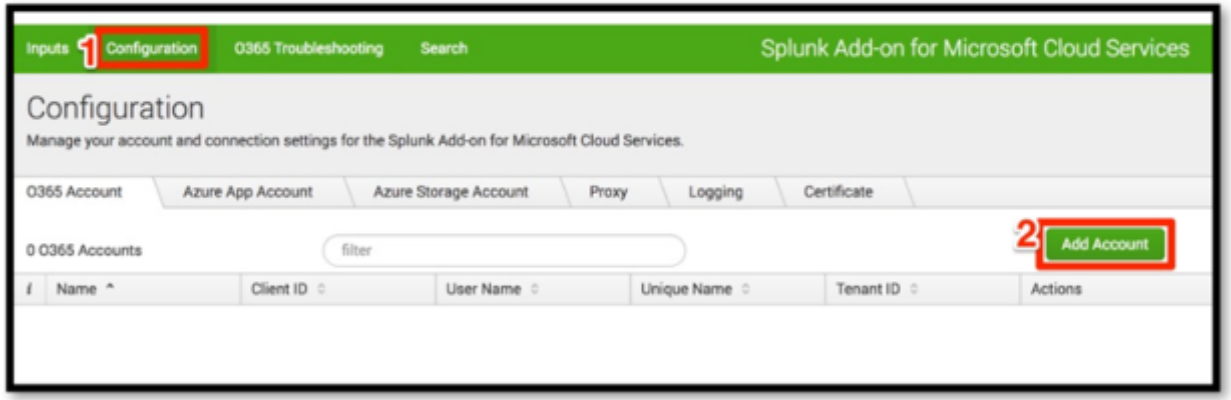
14) Select your **Subscription**, Select **Access Control (IAM)**, Select **Add**, Select **Reader Role**, search for **Application Name**, Select **Application**



1) Install the Splunk Add-on for Microsoft Cloud Services

https://splunkbase.splunk.com/app/3110/

2) Inside the Add-on, open the **Configuration** tab, then click **Add Account**

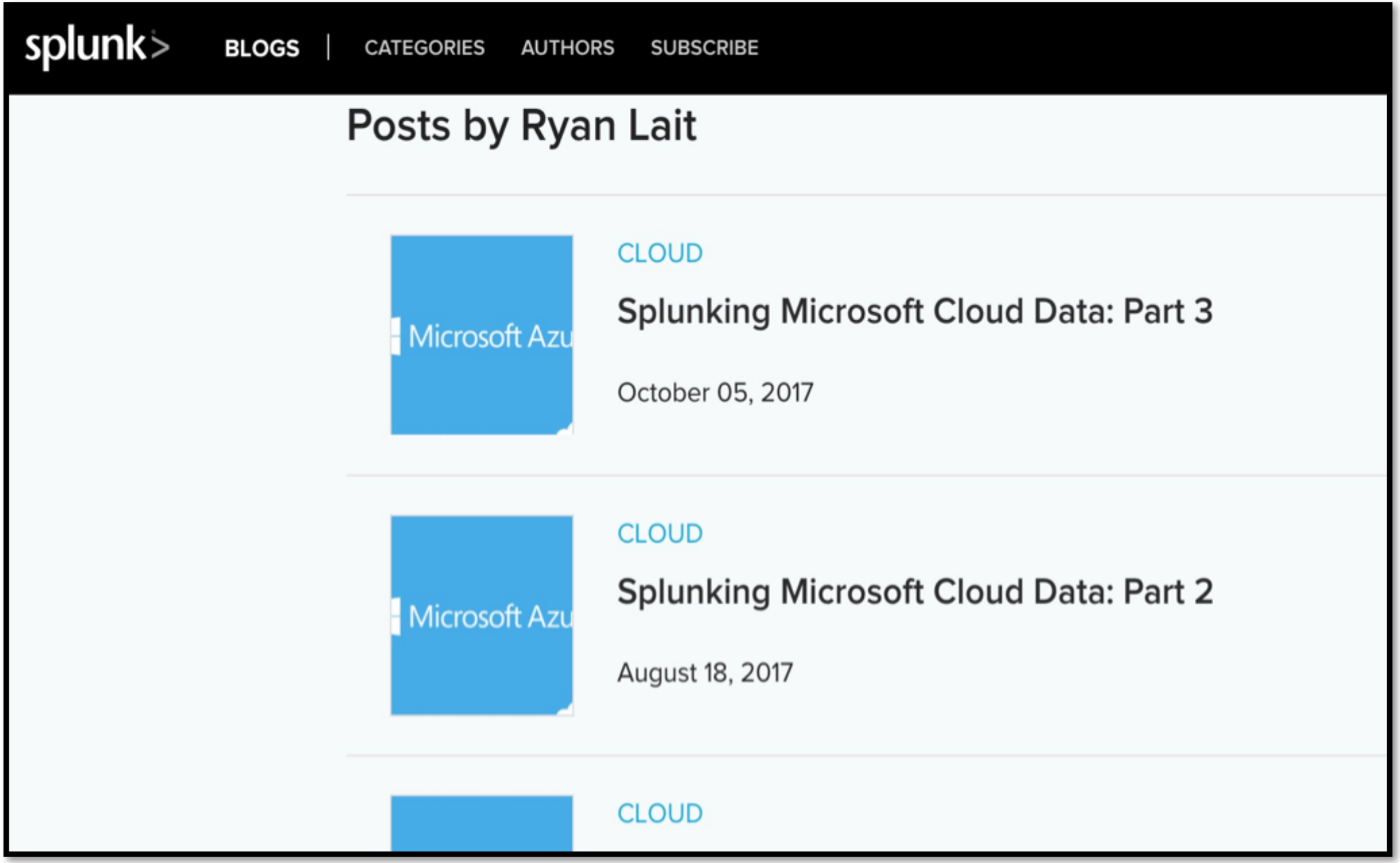


3) Copy the **Redirect URL**. – We'll need this shortly!

configured to retrieve.
for the specified

bit.ly/splunko365

splunk> .conf18



Thank You

Don't forget to rate this session in the .conf18 mobile app