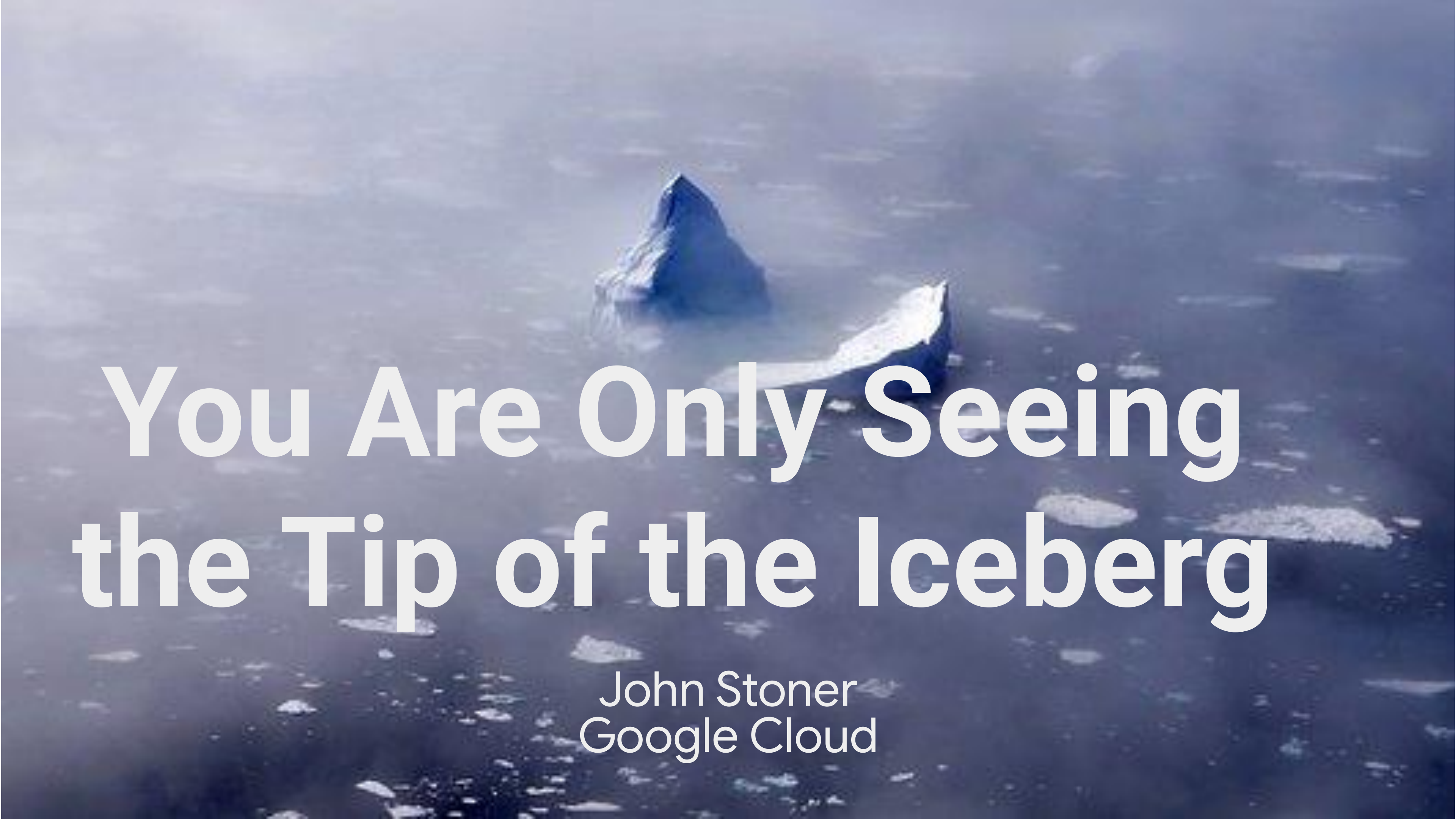


You Are Only Seeing the Tip of the Iceberg

John Stoner
Google Cloud

#whoami - John Stoner

Principal Security Strategist - Adoption Engineering

Worked in SIEM/SecOps space since 2004

Focus on SecOps, Threat Hunting, Threat Intelligence

Built adversary emulations around APT actors

Blog - New to Chronicle series

Presented at BSides (?:SF|LV), FIRST (?:Tech.Symposium|CTI|), SANS Summit (?:THIR|SIEM|Cloud), WWHF, AtlSecCon, DefCon PHV, Splunk .conf(?:2016|2017|2018|2019|2020|2021)

Enjoy Alt80s "sad-timey" music

Let me tell you a tale of a fateful trip...

October 2020

Mandiant & Microsoft identify a supply chain attack targeting the tool SolarWinds

Azure Active Directory was attacked using Active Directory Federation Services (ADFS) as an attack vector

The term GoldenSAML started gaining traction

February 2021

Commence building an APT scenario for a blue team CTF

Wouldn't it be "fun" to emulate something like this?

Imagine what kind of telemetry their must be available to defenders…won't this be great!

Spring-Summer 2021

Design, unit test, end to end data capture of emulation

Supply Chain Compromise

On-Premise Attack

Pivot via ADFS to Azure AD - Cloud Attack

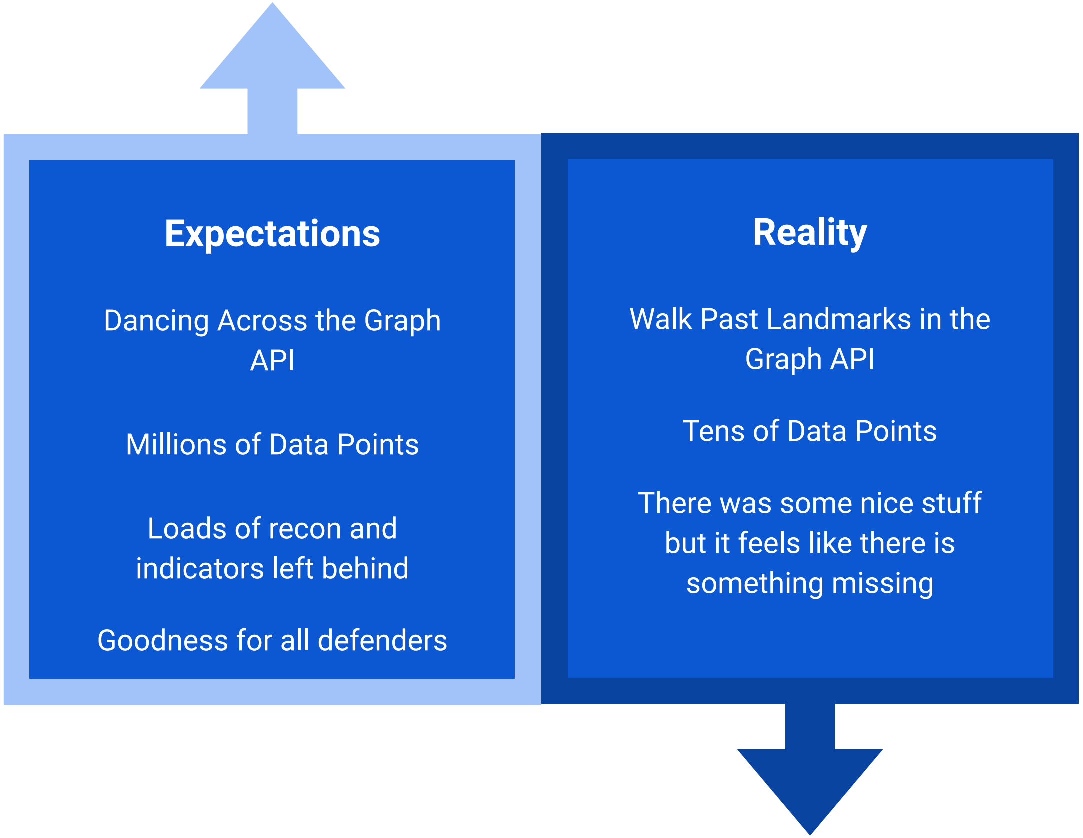
Late Summer 2021

Data validation begins

Loads of data about the on-premise attack!

What about cloud?

Experiencing Highs and Lows



Expectations

Dancing Across the Graph API

Millions of Data Points

Loads of recon and indicators left behind

Goodness for all defenders

Reality

Walk Past Landmarks in the Graph API

Tens of Data Points

There was some nice stuff but it feels like there is something missing

Skepticism (and a Little Paranoia) Sets In

Did Splunk not have the right mechanisms to access the data?

Ran my emulation in Sentinel - Late 2021 - Early 2022

- Very similar logging fidelity

Socialized - December 2021

- SANS FOR509 - Cloud Forensics - Dave Cowen, Co-course author

Fast Forward to September 2022

Revisited this attack

- Chronicle
- Splunk with New/Updated Connectors

Not High Fidelity, Same Fidelity

- GraphAPI alerting was added
- GraphAPI endpoints changed or were added
- Core visibility was very similar

Where Does That Leave Us?

Numerous ADFS implementations interacting with Azure AD

- Legacy applications can’t be migrated overnight
- Microsoft is driving migration away from ADFS to strictly AAD: https://www.youtube.com/watch?v=D0M-N-RQw0I

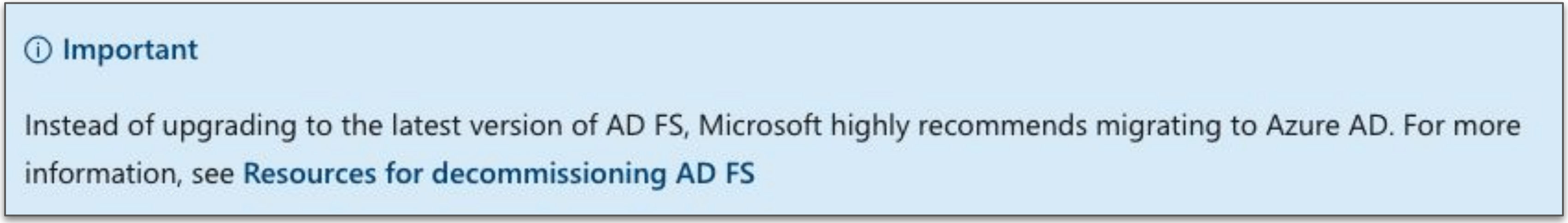
The fidelity is good for key changes, but not what a defender is used coming from an on-premise environment

We need to understand these realities as we hunt and build detections in these new terrains

What is ADFS?

“Active Directory Federation Service (AD FS) enables Federated Identity and Access Management by securely sharing digital identity and entitlements rights across security and enterprise boundaries. AD FS extends the ability to use single sign-on functionality that is available within a single security or enterprise boundary to Internet-facing applications to enable customers, partners, and suppliers a streamlined user experience while accessing the web-based applications of an organization.”

https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/ad-fs-overview



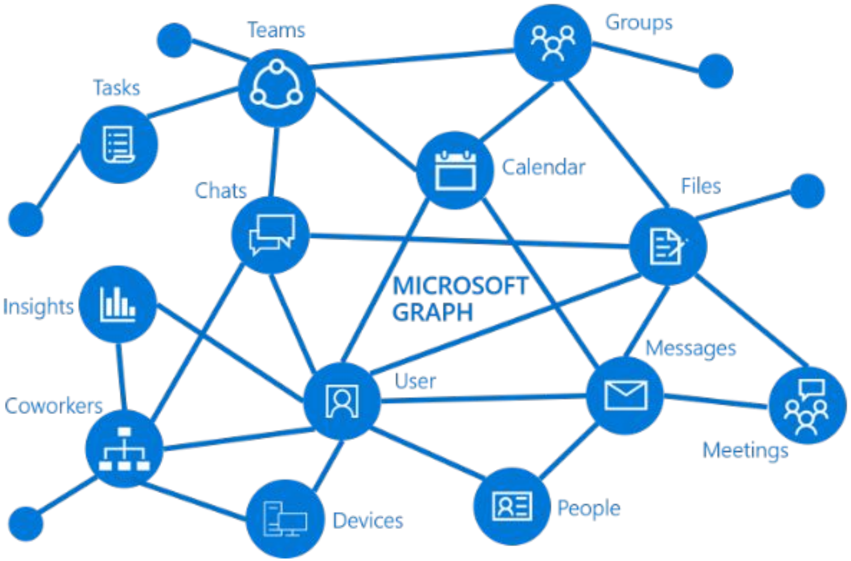
ⓘ **Important**

Instead of upgrading to the latest version of AD FS, Microsoft highly recommends migrating to Azure AD. For more information, see **Resources for decommissioning AD FS**

What is the Microsoft Graph?

Microsoft Graph exposes REST APIs and client libraries to access data on the following Microsoft cloud services:

- Microsoft 365 core services: Bookings, Calendar, Delve, Excel, Microsoft 365 compliance eDiscovery, Microsoft Search, OneDrive, OneNote, **Outlook/Exchange**, People (Outlook contacts), Planner, SharePoint, Teams, To Do, Viva Insights
- Enterprise Mobility + Security services: Advanced Threat Analytics, Advanced Threat Protection, **Azure Active Directory**, Identity Manager, and Intune
- Windows services: activities, devices, notifications, Universal Print
- Dynamics 365 Business Central services



https://learn.microsoft.com/en-us/graph/overview

This Is A Case Study

Using ADFS to compromise a signing key that can then be applied to Azure AD is a novel attack but the lessons learned from this attack need to be applied to monitoring and hunting in cloud environments

This example is Azure, but could apply to other environments as well

Our Environment

Windows Server 2022 Active Directory running ADFS

- At scale, these would likely be different systems and potentially many systems
- Multiple systems and users tied into Active Directory
- Azure AD Connect used to handle federation between AD and AAD
- Users would log into the ADFS portal to gain access to Azure cloud resources
- Followed Microsoft and other sites to properly configure ADFS (not easy!)

Special thanks to Roberto Rodriguez for his Simuland project to help understand the initial stages of this attack and how to emulate it with PowerShell!

API Feeds

Azure AD - Sign-in Audit Logs

Azure AD Audit - Directory Audits

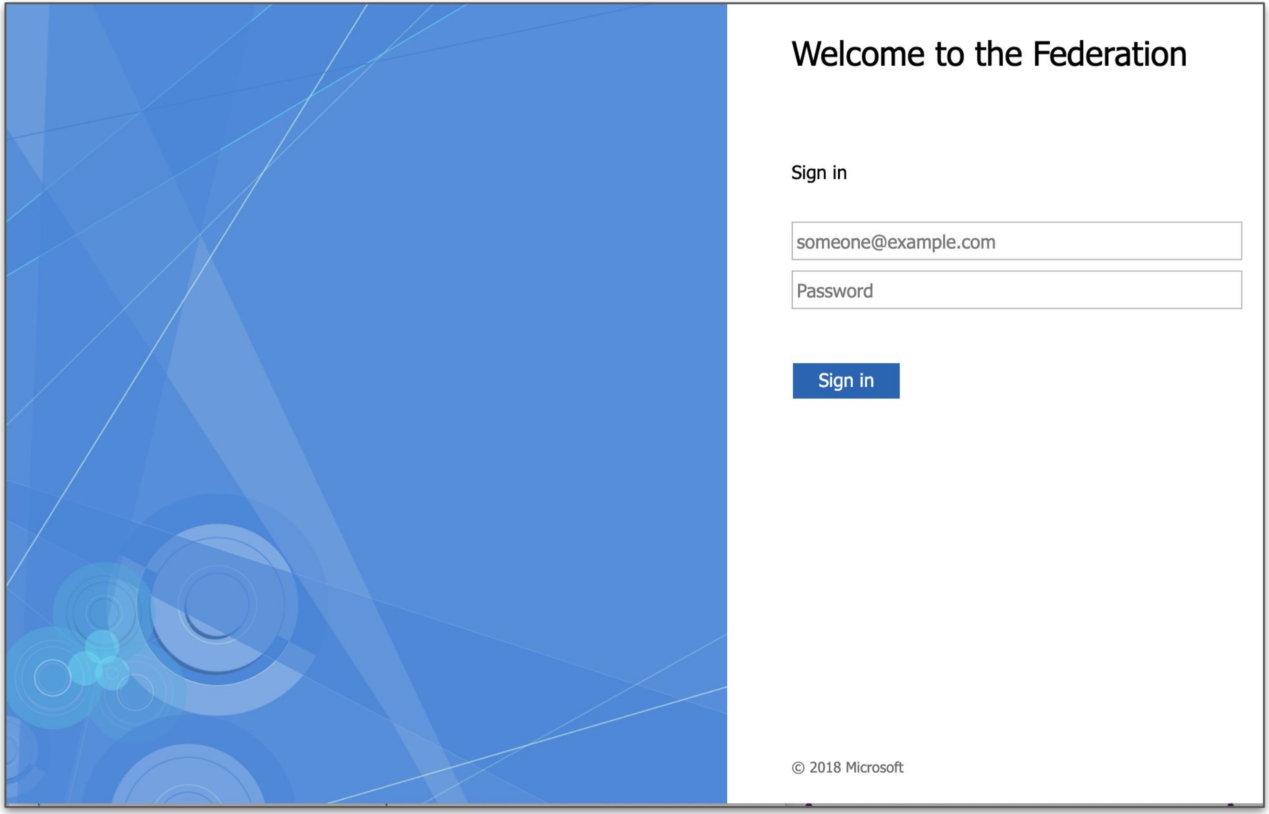
O365 - Azure AD Audit, SharePoint Audit, Exchange Audit, General Audit, DLP

GraphAPI - Security Alerts

Potential Sources of Noise

- Azure AD Connect - Synchronization actions
- Security Compliance Center - Data Insights events were noisy - One useful alert

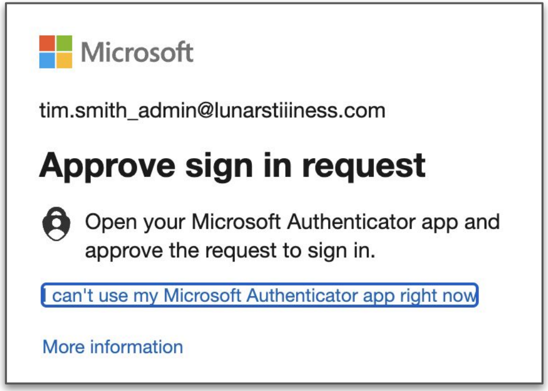
Typical Login to Azure via ADFS



Welcome to the Federation

Sign in

© 2018 Microsoft

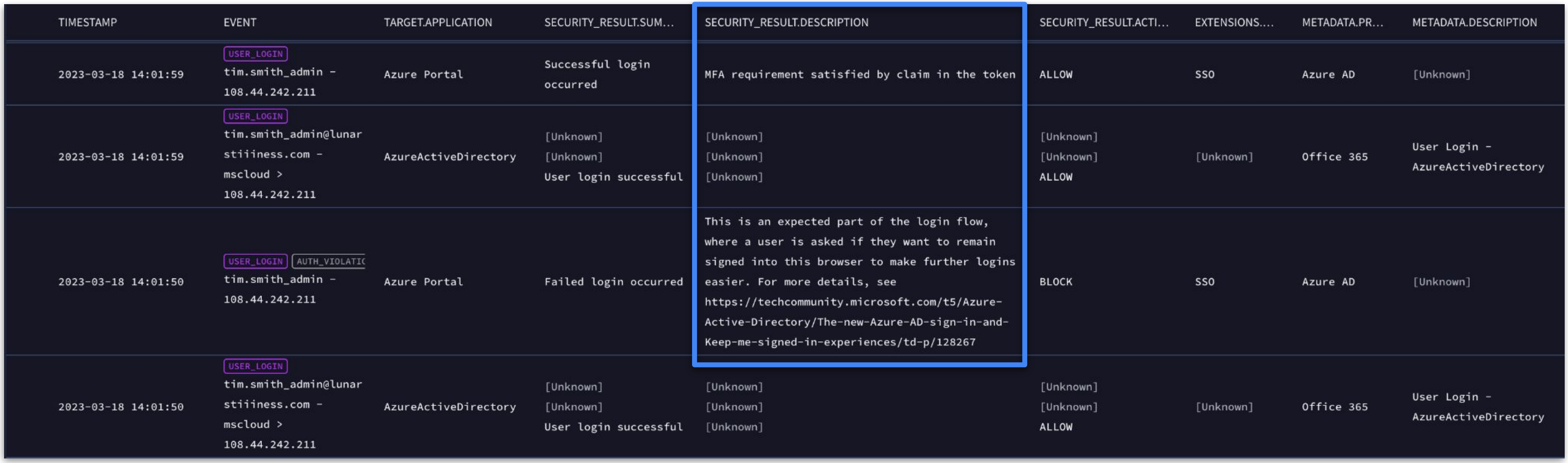


tim.smith_admin@lunarstiiiness.com

Approve sign in request

Open your Microsoft Authenticator app and approve the request to sign in.

Typical Login to Azure via ADFS



TIMESTAMP	EVENT	TARGET.APPLICATION	SECURITY_RESULT.SUM...	SECURITY_RESULT.DESCRIPTION	SECURITY_RESULT.ACTI...	EXTENSIONS....	METADATA.PR...	METADATA.DESCRIPTION
2023-03-18 14:01:59	USER_LOGIN tim.smith_admin - 108.44.242.211	Azure Portal	Successful login occurred	MFA requirement satisfied by claim in the token	ALLOW	SSO	Azure AD	[Unknown]
2023-03-18 14:01:59	USER_LOGIN tim.smith_admin@lunarstiiiness.com - mscloud > 108.44.242.211	AzureActiveDirectory	[Unknown] [Unknown] User login successful	[Unknown] [Unknown] [Unknown]	[Unknown] [Unknown] ALLOW	[Unknown]	Office 365	User Login - AzureActiveDirectory
2023-03-18 14:01:50	USER_LOGIN AUTH_VIOLATIC tim.smith_admin - 108.44.242.211	Azure Portal	Failed login occurred	This is an expected part of the login flow, where a user is asked if they want to remain signed into this browser to make further logins easier. For more details, see https://techcommunity.microsoft.com/t5/Azure-Active-Directory/The-new-Azure-AD-sign-in-and-Keep-me-signed-in-experiences/td-p/128267	BLOCK	SSO	Azure AD	[Unknown]
2023-03-18 14:01:50	USER_LOGIN tim.smith_admin@lunarstiiiness.com - mscloud > 108.44.242.211	AzureActiveDirectory	[Unknown] [Unknown] User login successful	[Unknown] [Unknown] [Unknown]	[Unknown] [Unknown] ALLOW	[Unknown]	Office 365	User Login - AzureActiveDirectory

Attack Path

Obtain Capabilities/ Permission Group Discovery	Credential Access	Configure Access	Establish Persistence	Actions on Objective
Gain access to ADFS signing key Enumerate domain admins	Forge Web Credentials SAML Tokens - Create a SAML Token using signing key Craft an access token	Create application or use existing Service principal creation (if creating app) Add permissions Add administrative consent to permissions	Create client secret in application Create access token with client secret for future use	Enumerate users Account Manipulation: Additional Cloud Roles - Add permissions Delete content Update Whatever you want!

Key Theft

Much of this attack could be local admin with ADFS service account

- “Classic” detections and monitoring all apply

Lots of good content is out there around defending the domain environment already and monitoring for attacks targeting ADFS

- BlackHat EU 2022: Writing Your Own Ticket to the Cloud Like APT: A Deep-dive to AD FS Attacks, Detections, and Mitigations - Nestori Syynimaa and Roberto Rodriguez
- New(er) Graph API Setting
    - “Enforcing Azure AD Multi-Factor Authentication every time assures that a compromised on-premises account cannot bypass Azure AD Multi-Factor Authentication by imitating that a multi factor authentication has already been performed by the identity provider, and is **highly recommended unless you perform MFA for your federated users using a third party MFA provider**.”

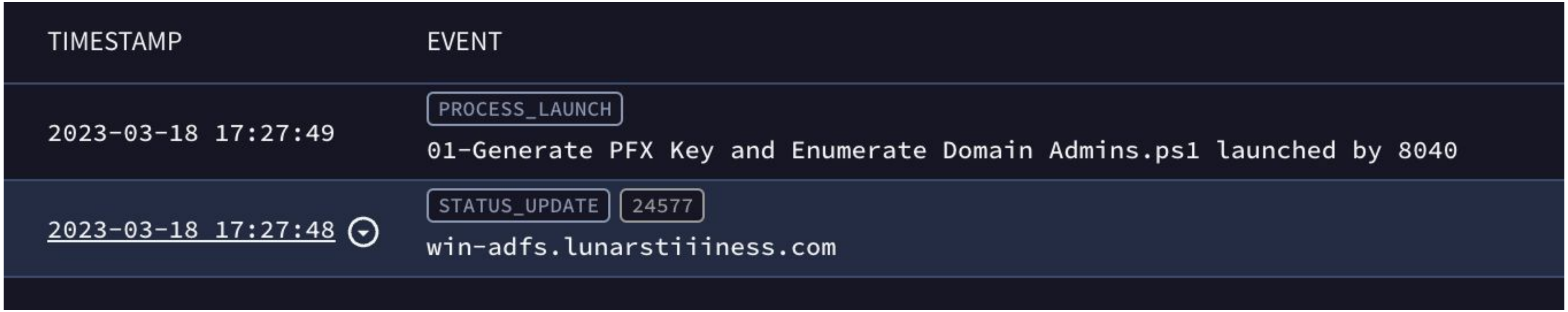
https://github.com/OTRF/BHEU22-ADFS

Visibility Into This Stage of the Attack

Used a PowerShell script to extract the ADFS Token Signing Certificate (pfx), enumerate the domain admins and object GUIDs for a later phase of attack

Possible opportunities for detection

- PowerShell Script block logs - Covenant C2 could prevented visibility
- File Creation or Exfiltration
- Local Pipe Creation to ADFS WID/SQL
- WMI and LDAP utilized; Audit Rules (SQL, **ADFS Key Read**)



TIMESTAMP	EVENT
2023-03-18 17:27:49	PROCESS_LAUNCH 01-Generate PFX Key and Enumerate Domain Admins.ps1 launched by 8040
2023-03-18 17:27:48	STATUS_UPDATE 24577 win-adfs.lunarstiiiness.com

However…

Once access is gained to the pfx key and it is exfiltrated to the adversary…

The Remainder of this Attack Uses An External System

Visibility will be limited to what is available in the cloud

Attack Path

Obtain Capabilities/ Permission Group Discovery

Gain access to ADFS signing key

Enumerate domain admins

Credential Access

Forge Web Credentials

SAML Tokens - Create a SAML Token using signing key

Craft an access token

Configure Access

Create application or use existing

Service principal creation (if creating app)

Add permissions

Add administrative consent to permissions

Establish Persistence

Create client secret in application

Create access token with client secret for future use

Actions on Objective

Enumerate users

Account Manipulation: Additional Cloud Roles - Add permissions

Delete content

Update

Whatever you want!

Creating Your Own SAML Key

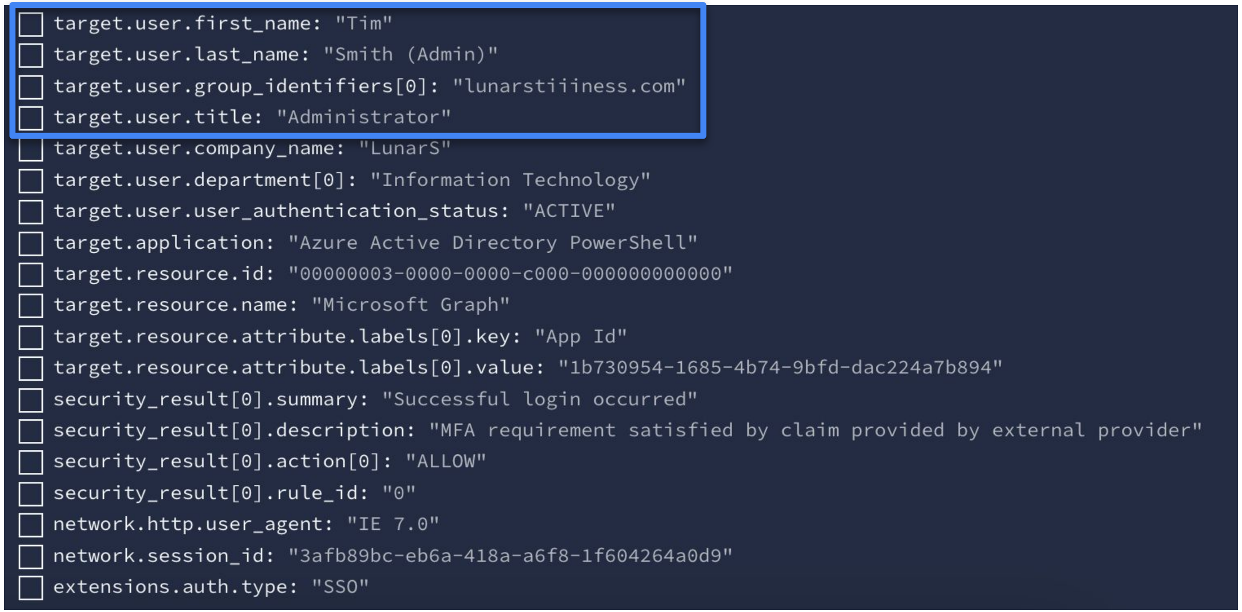
With exfiltrated signing cert from DC/ADFS, we can create our own SAML token

- TenantID
  - Use AAD Internals to get this ID
  - Example syntax: `Get-AADIntTenantID -Domain lunarstiiiness.com`
  - Not logged via Graph
- ObjectGUID
  - Collected when we wrote the pfx file
  - Listing of domain admins - **Can impersonate any of them**
- Certificate (pfx)
- Issuer
  - http://lunarstiiiness.com/adfs/services/trust/ - (`Get-ADFSProperties` at server)

Getting An Access Token

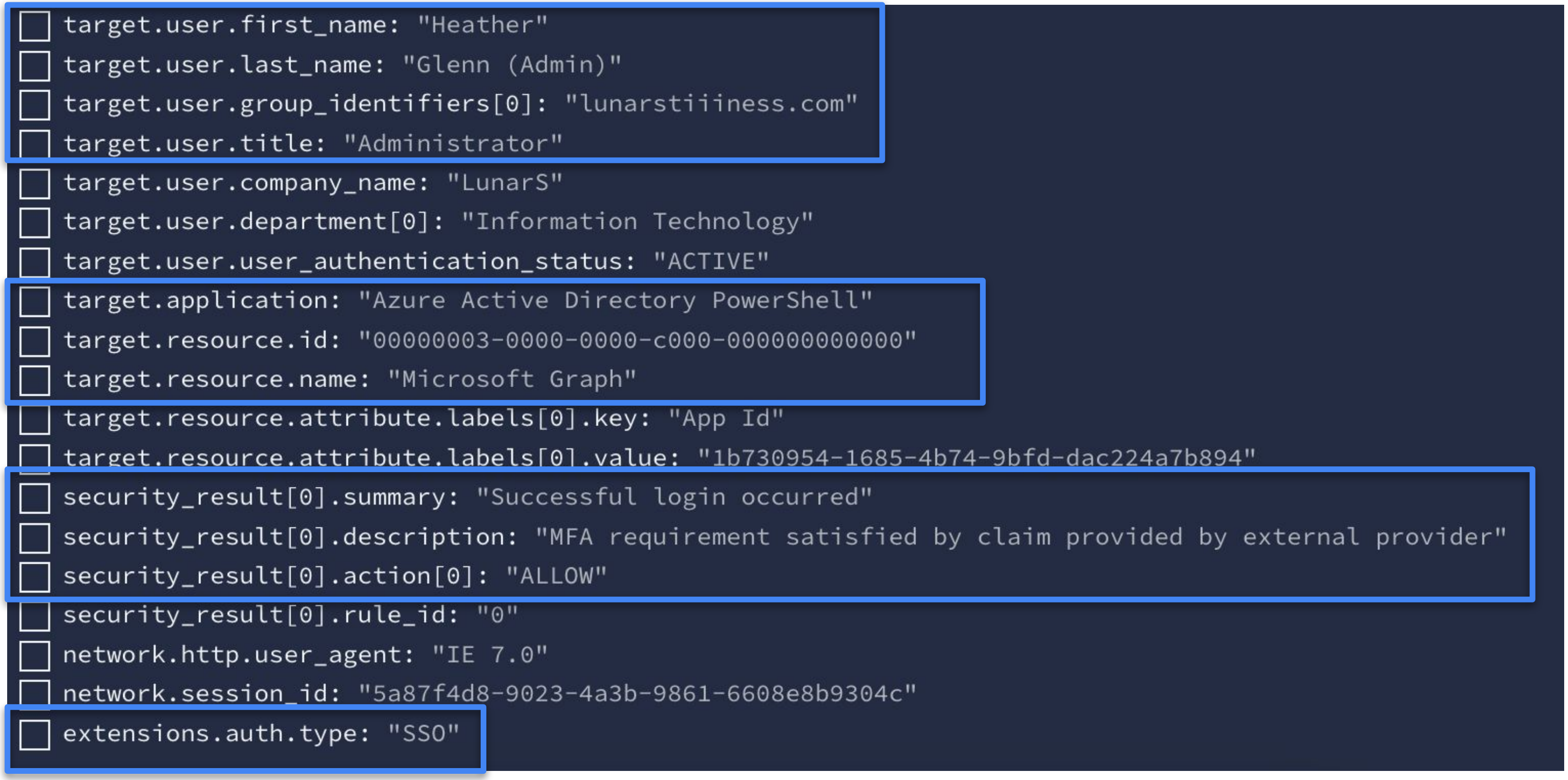
Encode our SAML token, build our http request and get an access token

Access token has 60-90 minute expiration (random)



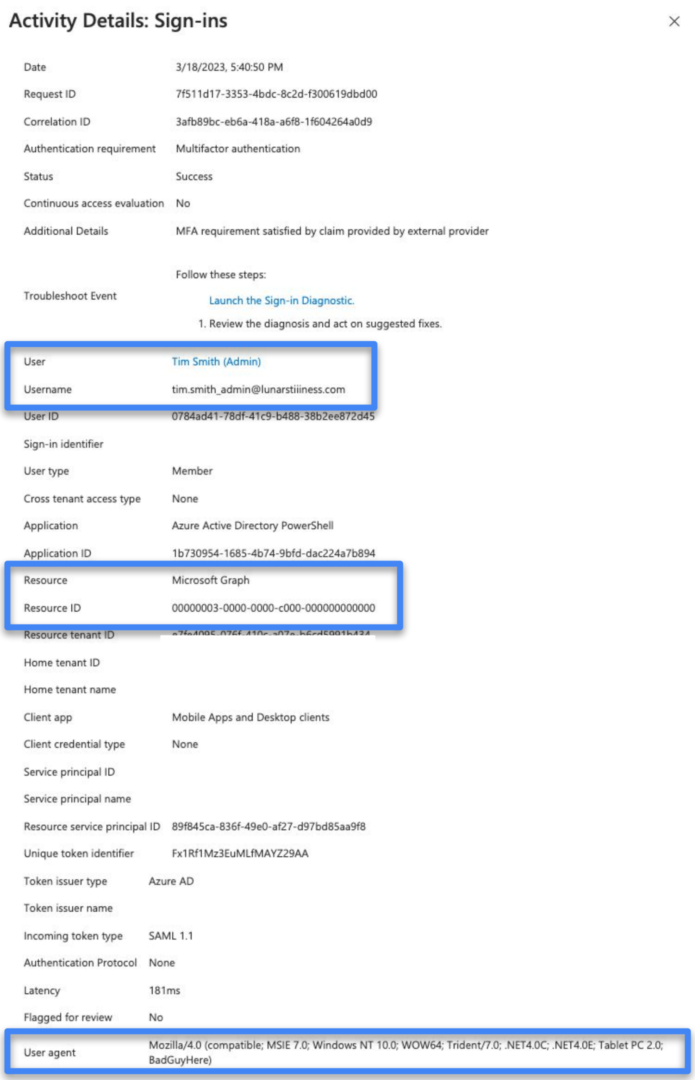
```
□ target.user.first_name: "Tim"
□ target.user.last_name: "Smith (Admin)"
□ target.user.group_identifiers[0]: "lunarstiiiness.com"
□ target.user.title: "Administrator"
□ target.user.company_name: "LunarS"
□ target.user.department[0]: "Information Technology"
□ target.user.user_authentication_status: "ACTIVE"
□ target.application: "Azure Active Directory PowerShell"
□ target.resource.id: "00000003-0000-0000-c000-000000000000"
□ target.resource.name: "Microsoft Graph"
□ target.resource.attribute.labels[0].key: "App Id"
□ target.resource.attribute.labels[0].value: "1b730954-1685-4b74-9bfd-dac224a7b894"
□ security_result[0].summary: "Successful login occurred"
□ security_result[0].description: "MFA requirement satisfied by claim provided by external provider"
□ security_result[0].action[0]: "ALLOW"
□ security_result[0].rule_id: "0"
□ network.http.user_agent: "IE 7.0"
□ network.session_id: "3afb89bc-eb6a-418a-a6f8-1f604264a0d9"
□ extensions.auth.type: "SSO"
```

If I Used A Different ObjectGUID...



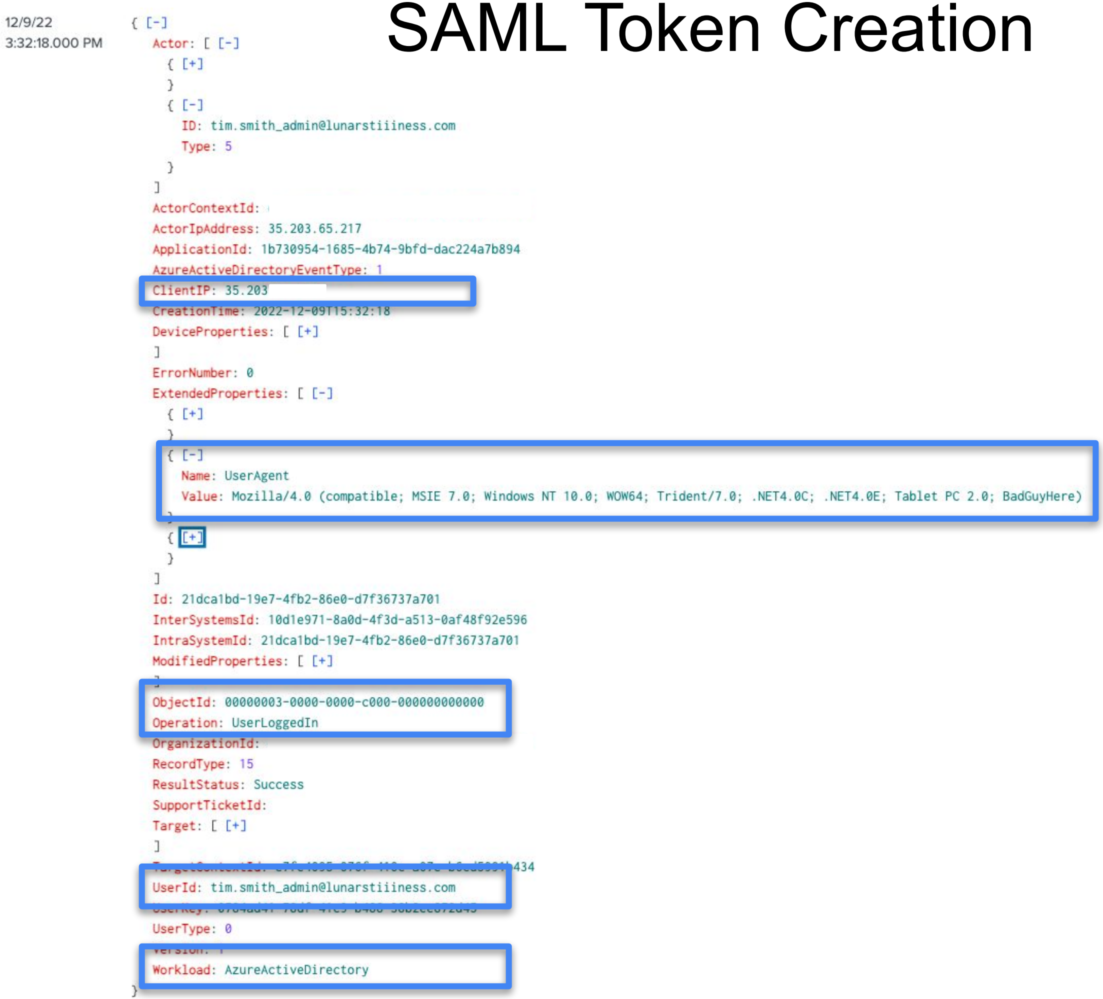
```
□ target.user.first_name: "Heather"
□ target.user.last_name: "Glenn (Admin)"
□ target.user.group_identifiers[0]: "lunarstiiiness.com"
□ target.user.title: "Administrator"
□ target.user.company_name: "LunarS"
□ target.user.department[0]: "Information Technology"
□ target.user.user_authentication_status: "ACTIVE"
□ target.application: "Azure Active Directory PowerShell"
□ target.resource.id: "00000003-0000-0000-c000-000000000000"
□ target.resource.name: "Microsoft Graph"
□ target.resource.attribute.labels[0].key: "App Id"
□ target.resource.attribute.labels[0].value: "1b730954-1685-4b74-9bfd-dac224a7b894"
□ security_result[0].summary: "Successful login occurred"
□ security_result[0].description: "MFA requirement satisfied by claim provided by external provider"
□ security_result[0].action[0]: "ALLOW"
□ security_result[0].rule_id: "0"
□ network.http.user_agent: "IE 7.0"
□ network.session_id: "5a87f4d8-9023-4a3b-9861-6608e8b9304c"
□ extensions.auth.type: "SSO"
```

SAML Token Creation



Activity Details: Sign-ins

Date	3/18/2023, 5:40:50 PM
Request ID	7f511d17-3353-4bdc-8c2d-f300619dbd00
Correlation ID	3afb89bc-eb6a-418a-a6f8-1f604264a0d9
Authentication requirement	Multifactor authentication
Status	Success
Continuous access evaluation	No
Additional Details	MFA requirement satisfied by claim provided by external provider
Troubleshoot Event	Follow these steps: Launch the Sign-in Diagnostic. 1. Review the diagnosis and act on suggested fixes.
User	Tim Smith (Admin)
Username	tim.smith_admin@lunarstiiiness.com
User ID	0784ad41-78df-41c9-b488-38b2ee872d45
Sign-in identifier	
User type	Member
Cross tenant access type	None
Application	Azure Active Directory PowerShell
Application ID	1b730954-1685-4b74-9bfd-dac224a7b894
Resource	Microsoft Graph
Resource ID	00000003-0000-0000-c000-000000000000
Resource tenant ID	[redacted]
Home tenant ID	
Home tenant name	
Client app	Mobile Apps and Desktop clients
Client credential type	None
Service principal ID	
Service principal name	
Resource service principal ID	89f845ca-836f-49e0-af27-d97bd85aa9f8
Unique token identifier	Fx1Rf1Mz3EuMLfMAYZ29AA
Token issuer type	Azure AD
Token issuer name	
Incoming token type	SAML 1.1
Authentication Protocol	None
Latency	181ms
Flagged for review	No
User agent	Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; BadGuyHere)



12/9/22
3:32:18.000 PM

```
{ [-]
  Actor: [ [-]
    { [+]
    }
    { [-]
      ID: tim.smith_admin@lunarstiiiness.com
      Type: 5
    }
  ]
  ActorContextId: [redacted]
  ActorIpAddress: 35.203.65.217
  ApplicationId: 1b730954-1685-4b74-9bfd-dac224a7b894
  AzureActiveDirectoryEventType: 1
  ClientIP: 35.203[redacted]
  CreationTime: 2022-12-09T15:32:18
  DeviceProperties: [ [+]
  ]
  ErrorNumber: 0
  ExtendedProperties: [ [-]
    { [+]
    }
    { [-]
      Name: UserAgent
      Value: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; Tablet PC 2.0; BadGuyHere)
    }
    { [+]
    }
  ]
  Id: 21dca1bd-19e7-4fb2-86e0-d7f36737a701
  InterSystemsId: 10d1e971-8a0d-4f3d-a513-0af48f92e596
  IntraSystemId: 21dca1bd-19e7-4fb2-86e0-d7f36737a701
  ModifiedProperties: [ [+]
  ]
  ObjectId: 00000003-0000-0000-c000-000000000000
  Operation: UserLoggedIn
  OrganizationId:
  RecordType: 15
  ResultStatus: Success
  SupportTicketId:
  Target: [ [+]
  ]
  TargetContextId: [illegible]434
  UserId: tim.smith_admin@lunarstiiiness.com
  UserKey: 0784ad41-78df-41c9-b488-38b2ee872d45
  UserType: 0
  Version: 1
  Workload: AzureActiveDirectory
}
```

Things to Look For...

Azure Active Directory PowerShell application is a Azure app, should users be logging into this?

How frequently do we see these logins occurring? And from where?

Which users are using this application for login and what subsequent activities are we observing?

Attack Path

Obtain Capabilities/ Permission Group Discovery

Gain access to ADFS signing key

Enumerate domain admins

Credential Access

Forge Web Credentials

SAML Tokens - Create a SAML Token using signing key

Craft an access token

Configure Access

Create application or use existing

Service principal creation (if creating app)

Add permissions

Add administrative consent to permissions

Establish Persistence

Create client secret in application

Create access token with client secret for future use

Actions on Objective

Enumerate users

Account Manipulation: Additional Cloud Roles - Add permissions

Delete content

Update

Whatever you want!

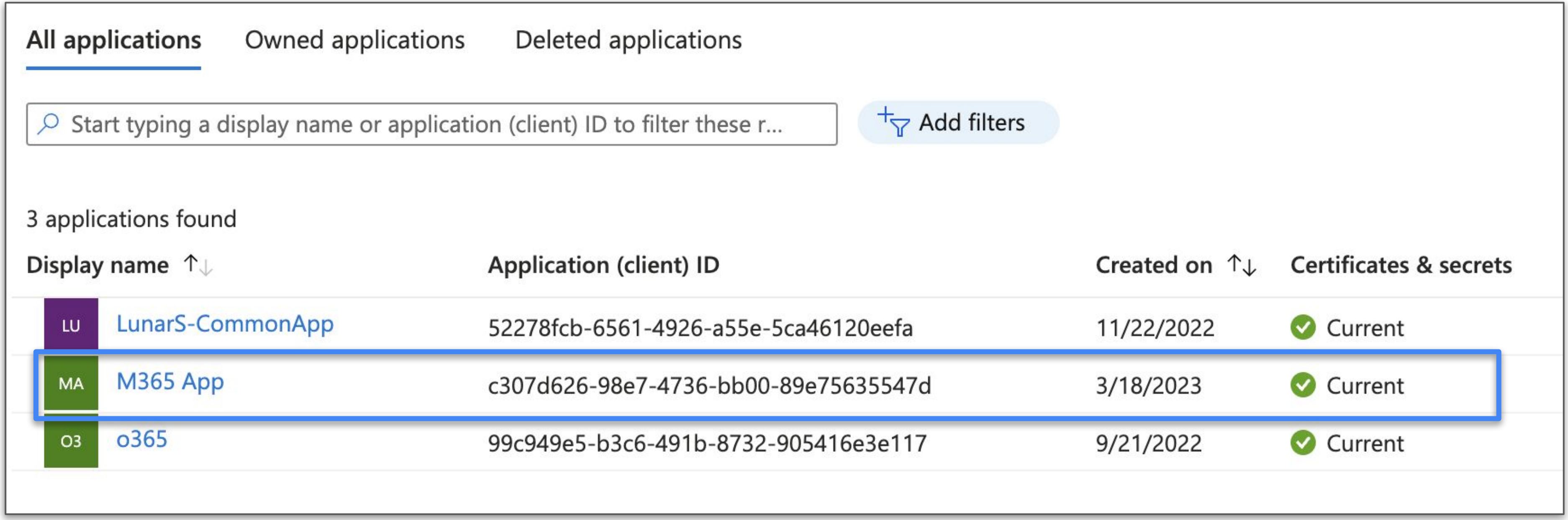
Setting Up Access

Create a New Application
(Logged)

Use an Existing Application
(Not logged)

Access Token Created
(Logged)

New Application Created



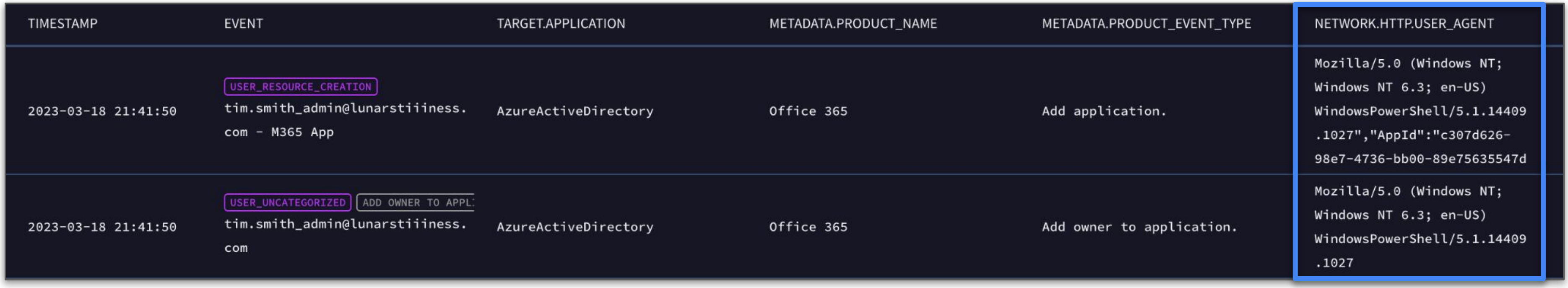
All applications | Owned applications | Deleted applications

Start typing a display name or application (client) ID to filter these r...
Add filters

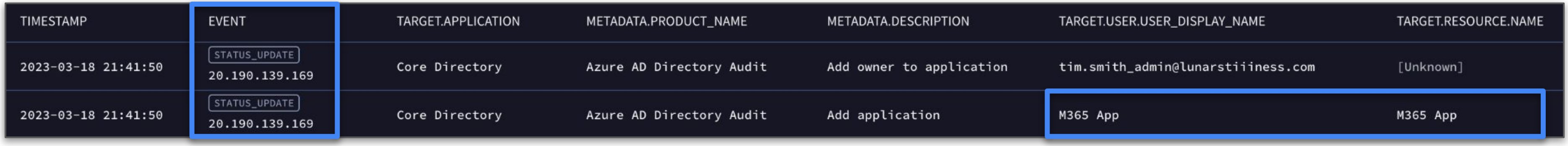
3 applications found

Display name ↑↓	Application (client) ID	Created on ↑↓	Certificates & secrets
LU LunarS-CommonApp	52278fcb-6561-4926-a55e-5ca46120eefa	11/22/2022	✓ Current
MA M365 App	c307d626-98e7-4736-bb00-89e75635547d	3/18/2023	✓ Current
O3 o365	99c949e5-b3c6-491b-8732-905416e3e117	9/21/2022	✓ Current

Application Creation



TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODUCT_NAME	METADATA.PRODUCT_EVENT_TYPE	NETWORK.HTTP.USER_AGENT
2023-03-18 21:41:50	USER_RESOURCE_CREATION tim.smith_admin@lunarstiiiness.com - M365 App	AzureActiveDirectory	Office 365	Add application.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-89e75635547d
2023-03-18 21:41:50	USER_UNCATEGORIZED ADD OWNER TO APPL tim.smith_admin@lunarstiiiness.com	AzureActiveDirectory	Office 365	Add owner to application.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027



TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODUCT_NAME	METADATA.DESCRIPTION	TARGET.USER.USER_DISPLAY_NAME	TARGET.RESOURCE.NAME
2023-03-18 21:41:50	STATUS_UPDATE 20.190.139.169	Core Directory	Azure AD Directory Audit	Add owner to application	tim.smith_admin@lunarstiiiness.com	[Unknown]
2023-03-18 21:41:50	STATUS_UPDATE 20.190.139.169	Core Directory	Azure AD Directory Audit	Add application	M365 App	M365 App

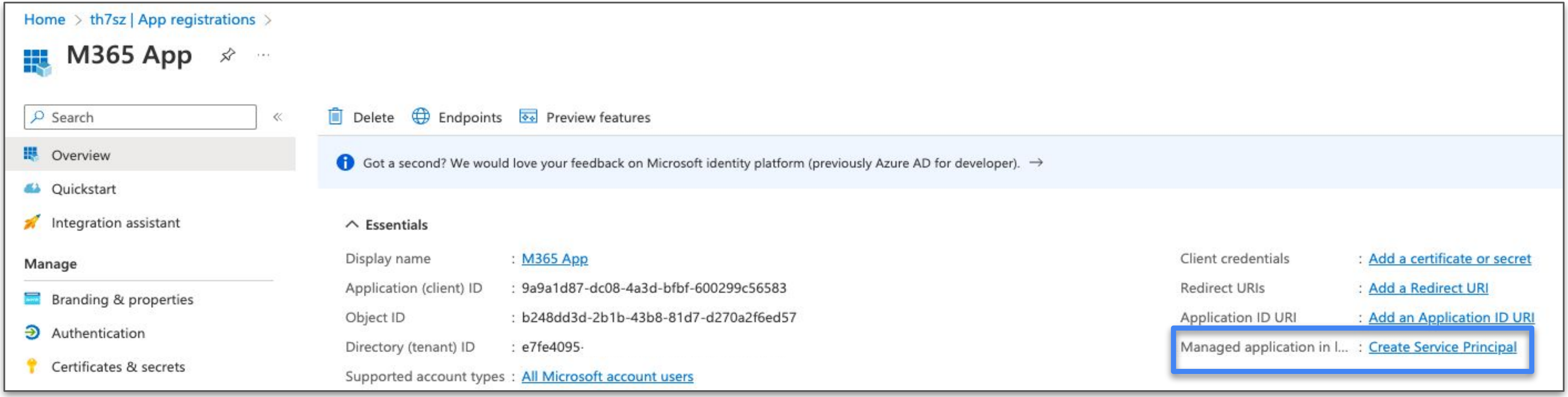
Create a Service Principal for the Application

Defines access policy and permissions in the tenant

- Provides authorization and authentication

Created automatically when the application is created in UI but not when programmatically created via GraphAPI

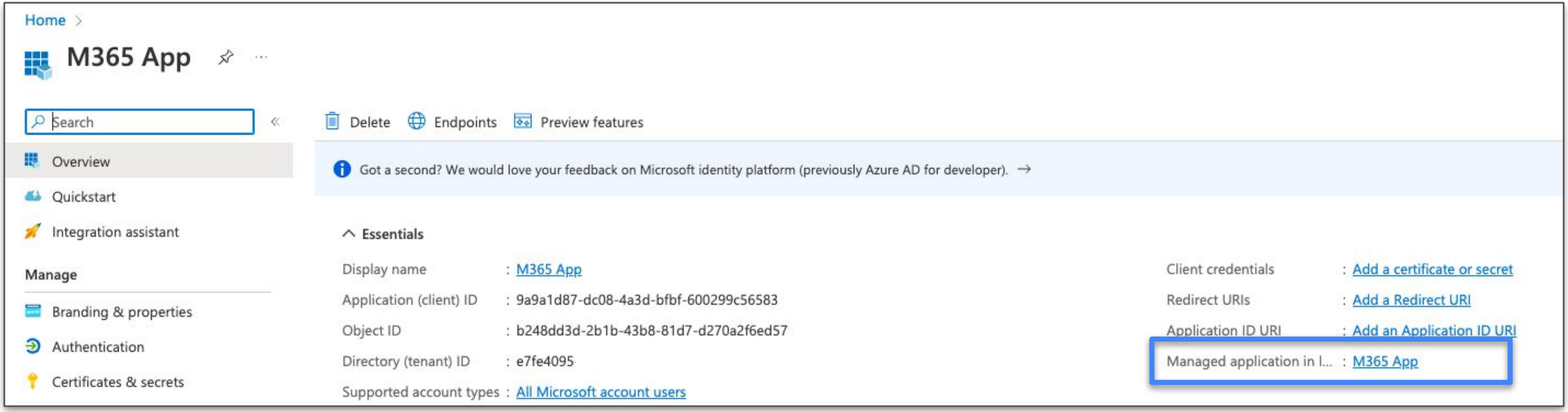
Could programmatically create at the same time as the application; would just need to grab the app id as it is created and flow it to your script



Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Display name	: M365 App
Application (client) ID	: 9a9a1d87-dc08-4a3d-bfbf-600299c56583
Object ID	: b248dd3d-2b1b-43b8-81d7-d270a2f6ed57
Directory (tenant) ID	: e7fe4095
Supported account types	: All Microsoft account users
Client credentials	: Add a certificate or secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in l...	: Create Service Principal

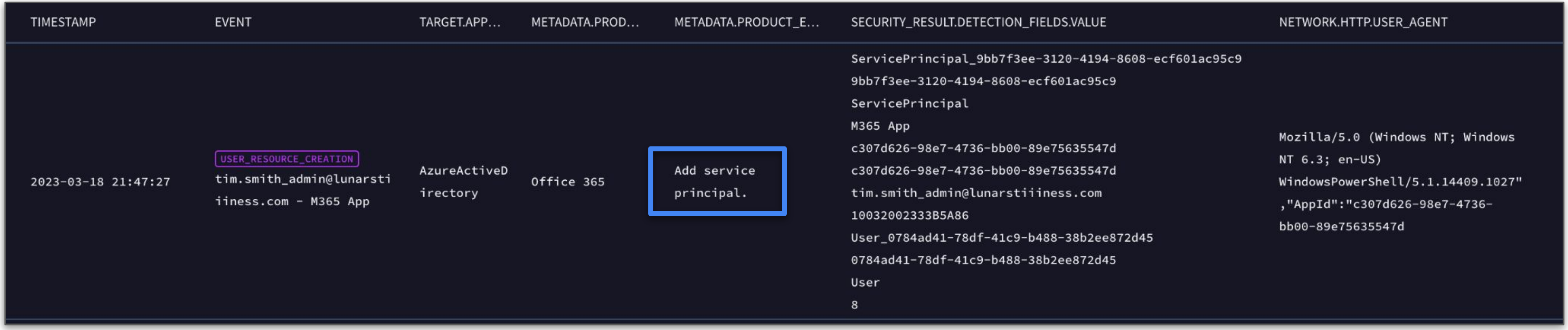


Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

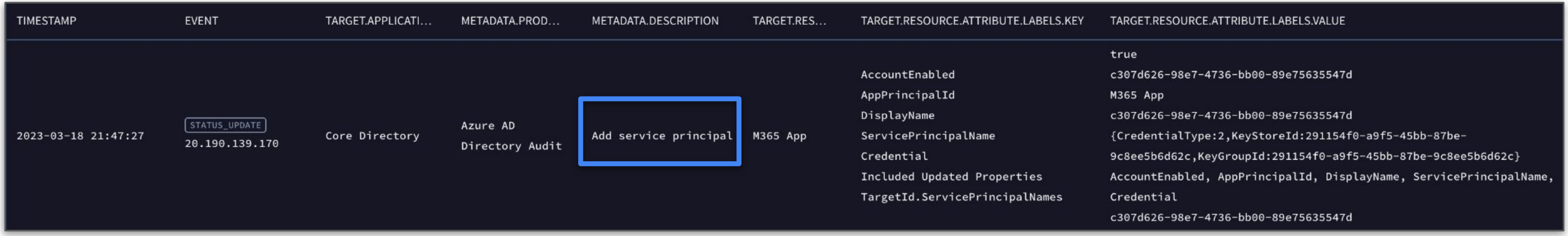
Essentials

Display name	: M365 App
Application (client) ID	: 9a9a1d87-dc08-4a3d-bfbf-600299c56583
Object ID	: b248dd3d-2b1b-43b8-81d7-d270a2f6ed57
Directory (tenant) ID	: e7fe4095
Supported account types	: All Microsoft account users
Client credentials	: Add a certificate or secret
Redirect URIs	: Add a Redirect URI
Application ID URI	: Add an Application ID URI
Managed application in l...	: M365 App

Create a Service Principal for the Application

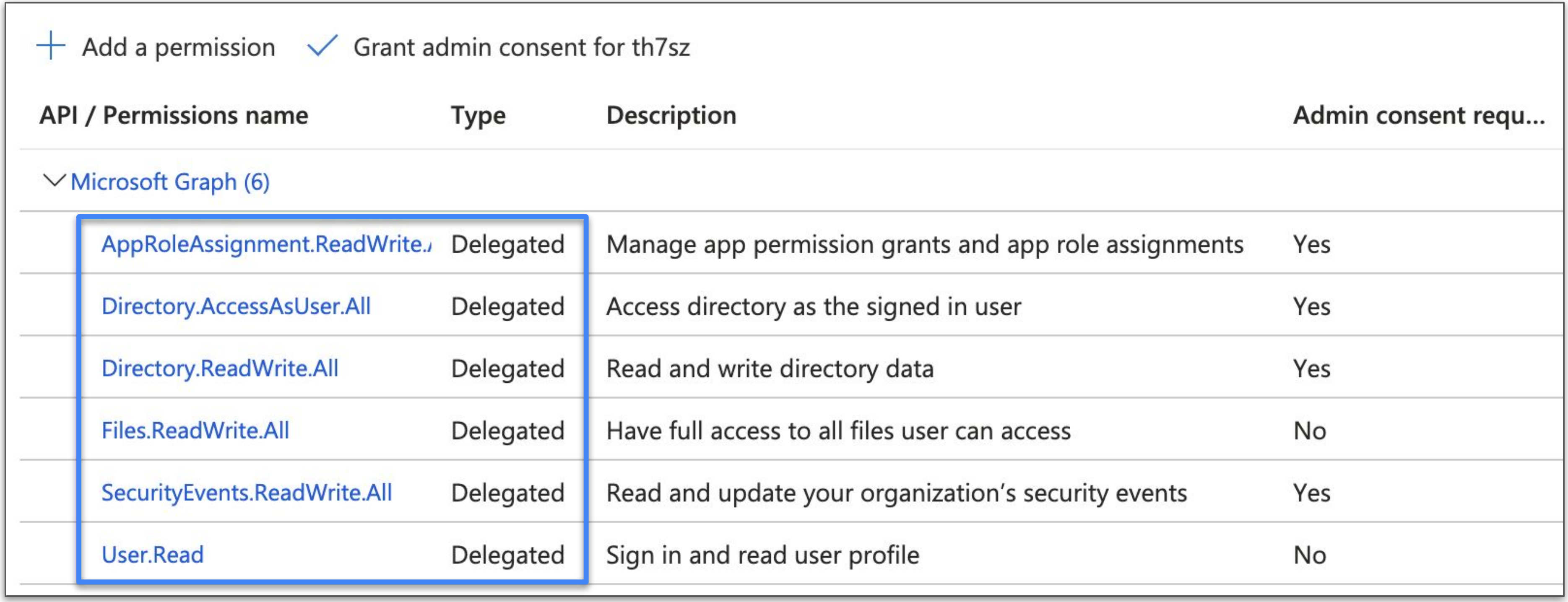


TIMESTAMP	EVENT	TARGET.APP...	METADATA.PROD...	METADATA.PRODUCT_E...	SECURITY_RESULT.DETECTION_FIELDS.VALUE	NETWORK.HTTP.USER_AGENT
2023-03-18 21:47:27	USER_RESOURCE_CREATION tim.smith_admin@lunarstiiiness.com - M365 App	AzureActiveDirectory	Office 365	Add service principal.	ServicePrincipal_9bb7f3ee-3120-4194-8608-ecf601ac95c9 9bb7f3ee-3120-4194-8608-ecf601ac95c9 ServicePrincipal M365 App c307d626-98e7-4736-bb00-89e75635547d c307d626-98e7-4736-bb00-89e75635547d tim.smith_admin@lunarstiiiness.com 10032002333B5A86 User_0784ad41-78df-41c9-b488-38b2ee872d45 0784ad41-78df-41c9-b488-38b2ee872d45 User 8	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-89e75635547d



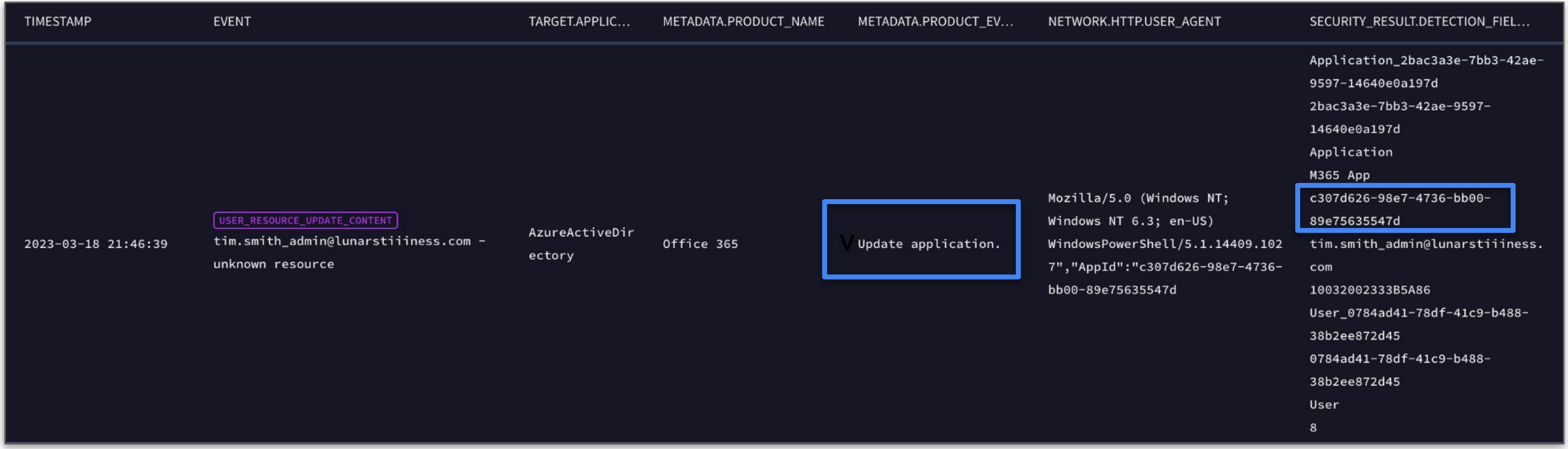
TIMESTAMP	EVENT	TARGET.APPLICATI...	METADATA.PROD...	METADATA.DESCRIPTION	TARGET.RES...	TARGET.RESOURCE.ATTRIBUTE.LABELS.KEY	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2023-03-18 21:47:27	STATUS_UPDATE 20.190.139.170	Core Directory	Azure AD Directory Audit	Add service principal	M365 App	AccountEnabled AppPrincipalId DisplayName ServicePrincipalName Credential Included Updated Properties TargetId.ServicePrincipalNames	true c307d626-98e7-4736-bb00-89e75635547d M365 App c307d626-98e7-4736-bb00-89e75635547d {CredentialType:2,KeyStoreId:291154f0-a9f5-45bb-87be-9c8ee5b6d62c,KeyGroupId:291154f0-a9f5-45bb-87be-9c8ee5b6d62c} AccountEnabled, AppPrincipalId, DisplayName, ServicePrincipalName, Credential c307d626-98e7-4736-bb00-89e75635547d

Apply Graph Permissions to Application



API / Permissions name	Type	Description	Admin consent requ...
Microsoft Graph (6)			
AppRoleAssignment.ReadWrite./	Delegated	Manage app permission grants and app role assignments	Yes
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No
SecurityEvents.ReadWrite.All	Delegated	Read and update your organization's security events	Yes
User.Read	Delegated	Sign in and read user profile	No

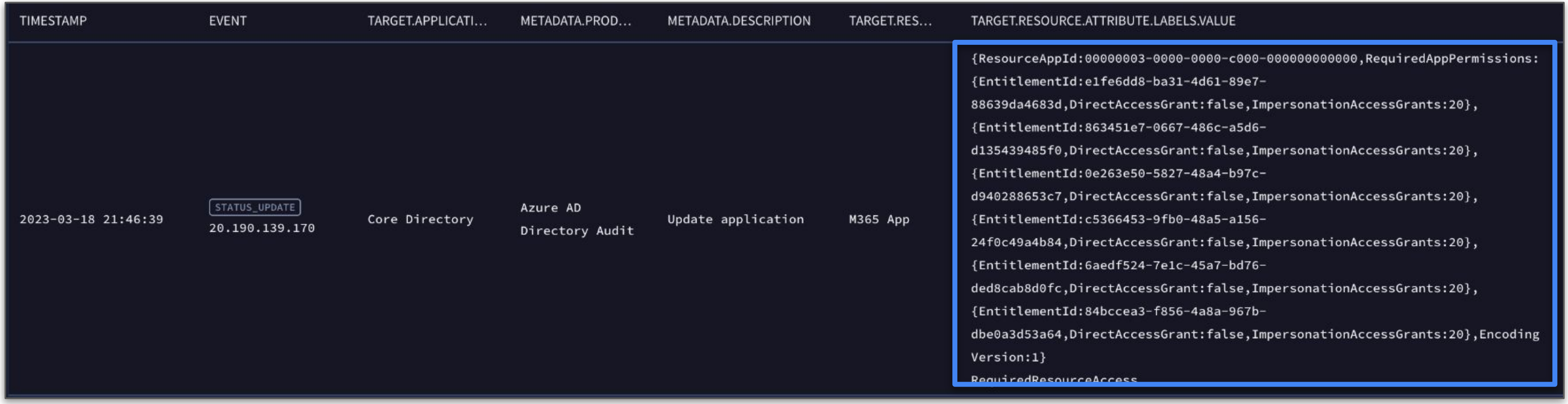
Applying Permissions to Graph - O365



TIMESTAMP	EVENT	TARGET.APPLIC...	METADATA.PRODUCT_NAME	METADATA.PRODUCT_EV...	NETWORK.HTTP.USER_AGENT	SECURITY_RESULT.DETECTION_FIEL...
2023-03-18 21:46:39	USER_RESOURCE_UPDATE_CONTENT tim.smith_admin@lunarstiiiness.com - unknown resource	AzureActiveDirectory	Office 365	Update application.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-89e75635547d	Application_2bac3a3e-7bb3-42ae-9597-14640e0a197d 2bac3a3e-7bb3-42ae-9597-14640e0a197d Application M365 App c307d626-98e7-4736-bb00-89e75635547d tim.smith_admin@lunarstiiiness.com 10032002333B5A86 User_0784ad41-78df-41c9-b488-38b2ee872d45 0784ad41-78df-41c9-b488-38b2ee872d45 User 8

Permissions in the form of a GUID are available in this log stream

Applying Permissions to Graph - Azure AD Audit



TIMESTAMP	EVENT	TARGET.APPLICATI...	METADATA.PROD...	METADATA.DESCRIPTION	TARGET.RES...	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2023-03-18 21:46:39	STATUS_UPDATE 20.190.139.170	Core Directory	Azure AD Directory Audit	Update application	M365 App	{ResourceAppId:00000003-0000-0000-c000-000000000000,RequiredAppPermissions:{EntitlementId:e1fe6dd8-ba31-4d61-89e7-88639da4683d,DirectAccessGrant:false,ImpersonationAccessGrants:20},{EntitlementId:863451e7-0667-486c-a5d6-d135439485f0,DirectAccessGrant:false,ImpersonationAccessGrants:20},{EntitlementId:0e263e50-5827-48a4-b97c-d940288653c7,DirectAccessGrant:false,ImpersonationAccessGrants:20},{EntitlementId:c5366453-9fb0-48a5-a156-24f0c49a4b84,DirectAccessGrant:false,ImpersonationAccessGrants:20},{EntitlementId:6aedf524-7e1c-45a7-bd76-ded8cab8d0fc,DirectAccessGrant:false,ImpersonationAccessGrants:20},{EntitlementId:84bccea3-f856-4a8a-967b-dbe0a3d53a64,DirectAccessGrant:false,ImpersonationAccessGrants:20},EncodingVersion:1} RequiredResourceAccess

Permissions are stored as GUID

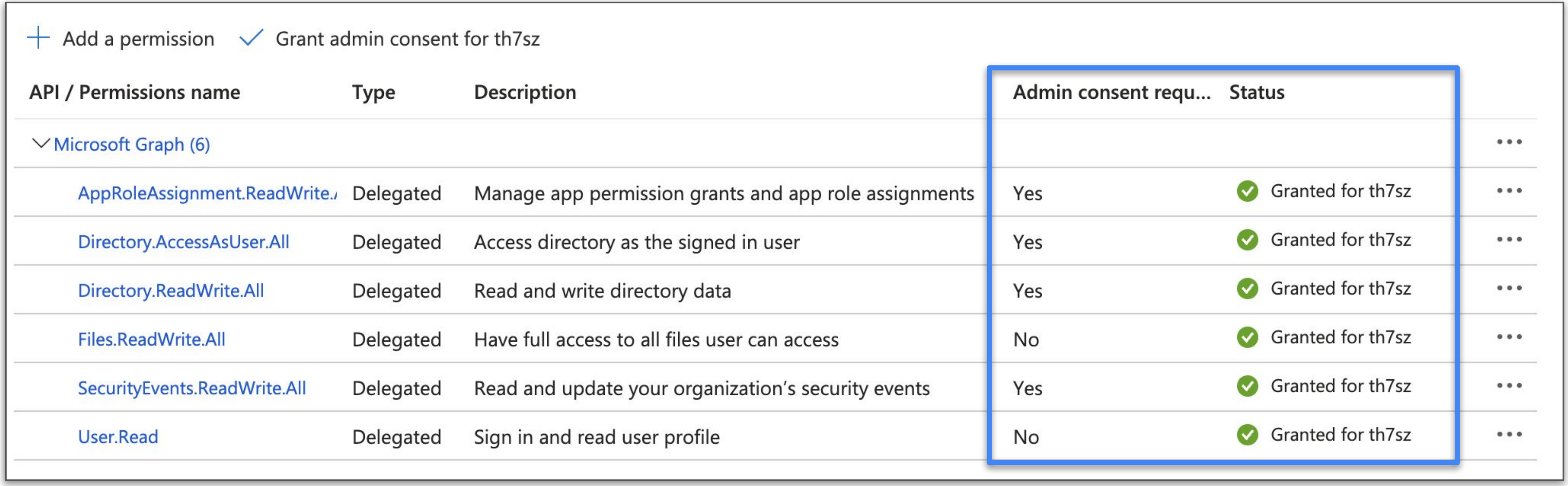
Can leverage reference like this one to perform a reference lookup for these GUIDs

https://learn.microsoft.com/en-us/graph/permissions-reference

Add Admin Consent to Permissions

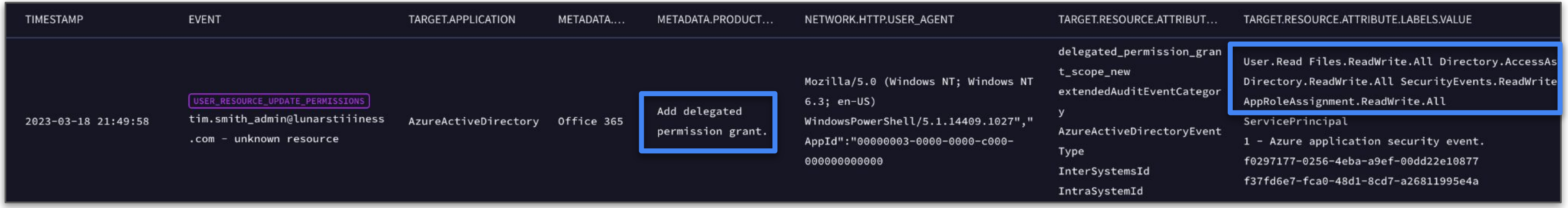
Grant application access to an API

Not all permissions required admin consent

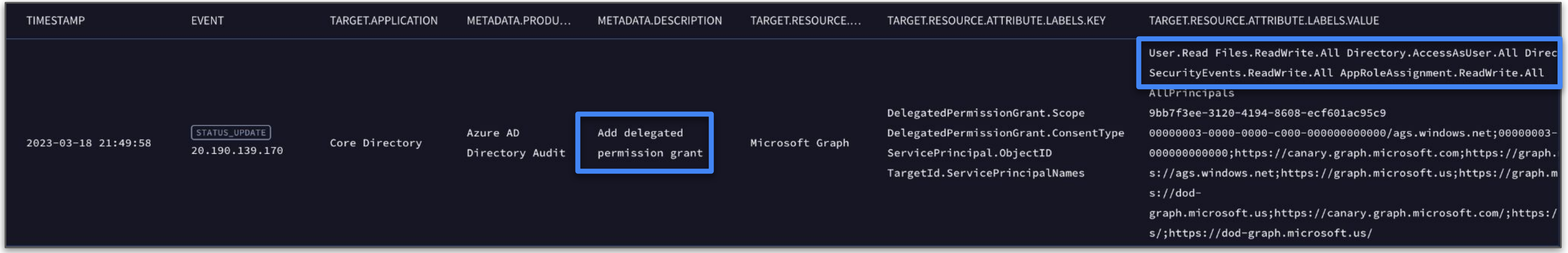


API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (6)				
AppRoleAssignment.ReadWrite./	Delegated	Manage app permission grants and app role assignments	Yes	✓ Granted for th7sz
Directory.AccessAsUser.All	Delegated	Access directory as the signed in user	Yes	✓ Granted for th7sz
Directory.ReadWrite.All	Delegated	Read and write directory data	Yes	✓ Granted for th7sz
Files.ReadWrite.All	Delegated	Have full access to all files user can access	No	✓ Granted for th7sz
SecurityEvents.ReadWrite.All	Delegated	Read and update your organization's security events	Yes	✓ Granted for th7sz
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for th7sz

Add Admin Consent to Permissions

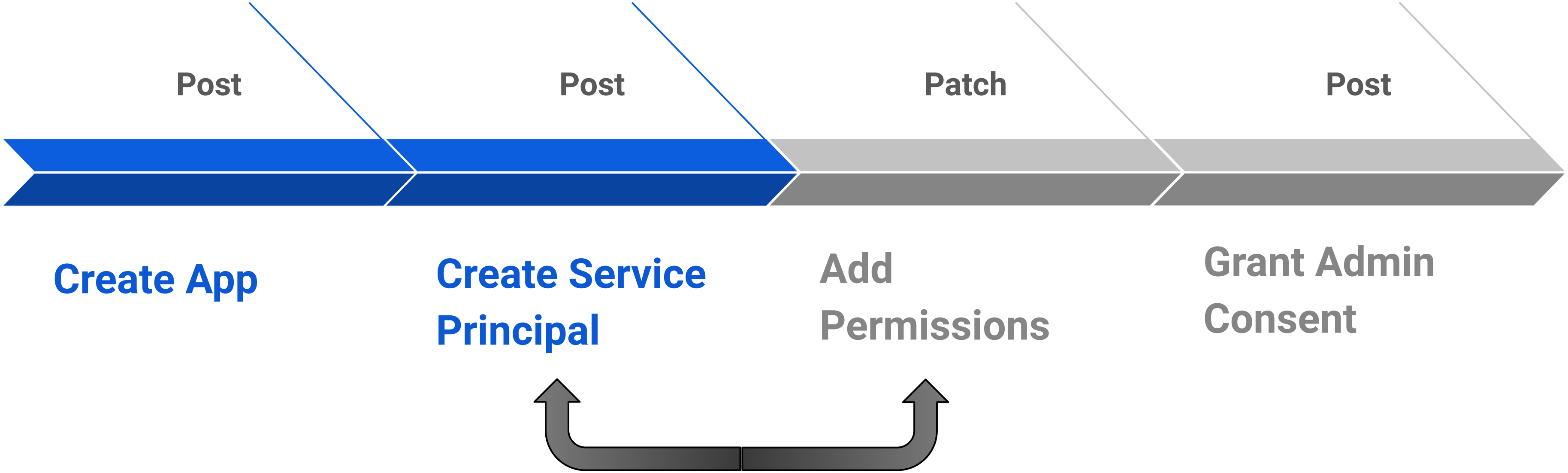


TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA....	METADATA.PRODUCT...	NETWORK.HTTP.USER_AGENT	TARGET.RESOURCE.ATTRIBUT...	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2023-03-18 21:49:58	USER_RESOURCE_UPDATE_PERMISSIONS tim.smith_admin@lunarstiiiness.com - unknown resource	AzureActiveDirectory	Office 365	Add delegated permission grant.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027"," AppId":"00000003-0000-0000-c000-000000000000	delegated_permission_grant_scope_new extendedAuditEventCategory AzureActiveDirectoryEventType InterSystemsId IntraSystemId	User.Read Files.ReadWrite.All Directory.AccessAs Directory.ReadWrite.All SecurityEvents.ReadWrite AppRoleAssignment.ReadWrite.All ServicePrincipal 1 - Azure application security event. f0297177-0256-4eba-a9ef-00dd22e10877 f37fd6e7-fca0-48d1-8cd7-a26811995e4a



TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODU...	METADATA.DESCRIPTION	TARGET.RESOURCE....	TARGET.RESOURCE.ATTRIBUTE.LABELS.KEY	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2023-03-18 21:49:58	STATUS_UPDATE 20.190.139.170	Core Directory	Azure AD Directory Audit	Add delegated permission grant	Microsoft Graph	DelegatedPermissionGrant.Scope DelegatedPermissionGrant.ConsentType ServicePrincipal.ObjectID TargetId.ServicePrincipalNames	User.Read Files.ReadWrite.All Directory.AccessAsUser.All Direc SecurityEvents.ReadWrite.All AppRoleAssignment.ReadWrite.All AllPrincipals 9bb7f3ee-3120-4194-8608-ecf601ac95c9 00000003-0000-0000-c000-000000000000/ags.windows.net;00000003-000000000000;https://canary.graph.microsoft.com;https://graph.s://ags.windows.net;https://graph.microsoft.us;https://graph.ms://dod-graph.microsoft.us;https://canary.graph.microsoft.com/;https://s/;https://dod-graph.microsoft.us/

Setting Up Access



Post

Post

Patch

Post

Create App

Create Service Principal

Add Permissions

Grant Admin Consent

No visibility into enumeration or other actions requiring a Get from the GraphAPI

Things to Look For...

Application creation

- How often are apps created in Azure?
- Can't count on the app being created because an existing one could be leveraged
- Enumeration of those apps isn't logged

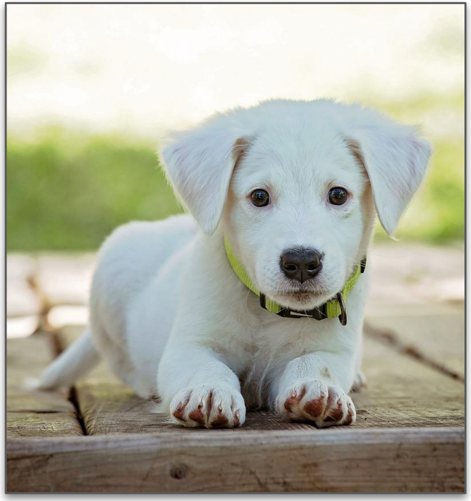
Service Principal creation is to be expected, perhaps a delay might suggest command line v UI

Permission assignment

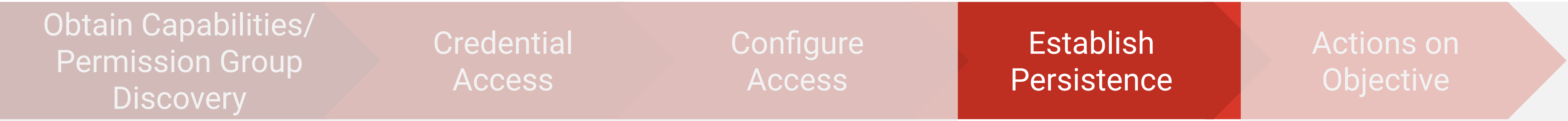
- Possibly one of the better places to monitor
- List of GUIDs exist
- Maybe look at the frequency they get assigned, by whom, from where
- Greedy permission grab or coming back for more and more

Delegated Permission Grant (Admin Consent)

- Focus on the permissions being asked to get admin consent and by which apps, by whom and when and where
- Watchlist is a good way to work with these
- Azure AD Audit & O365 have these permissions in words v GUID



Attack Path



Obtain Capabilities/ Permission Group Discovery

Gain access to ADFS signing key

Enumerate domain admins

Credential Access

Forge Web Credentials

SAML Tokens - Create a SAML Token using signing key

Craft an access token

Configure Access

Create application or use existing

Service principal creation (if creating app)

Add permissions

Add administrative consent to permissions

Establish Persistence

Create client secret in application

Create access token with client secret for future use

Actions on Objective

Enumerate users

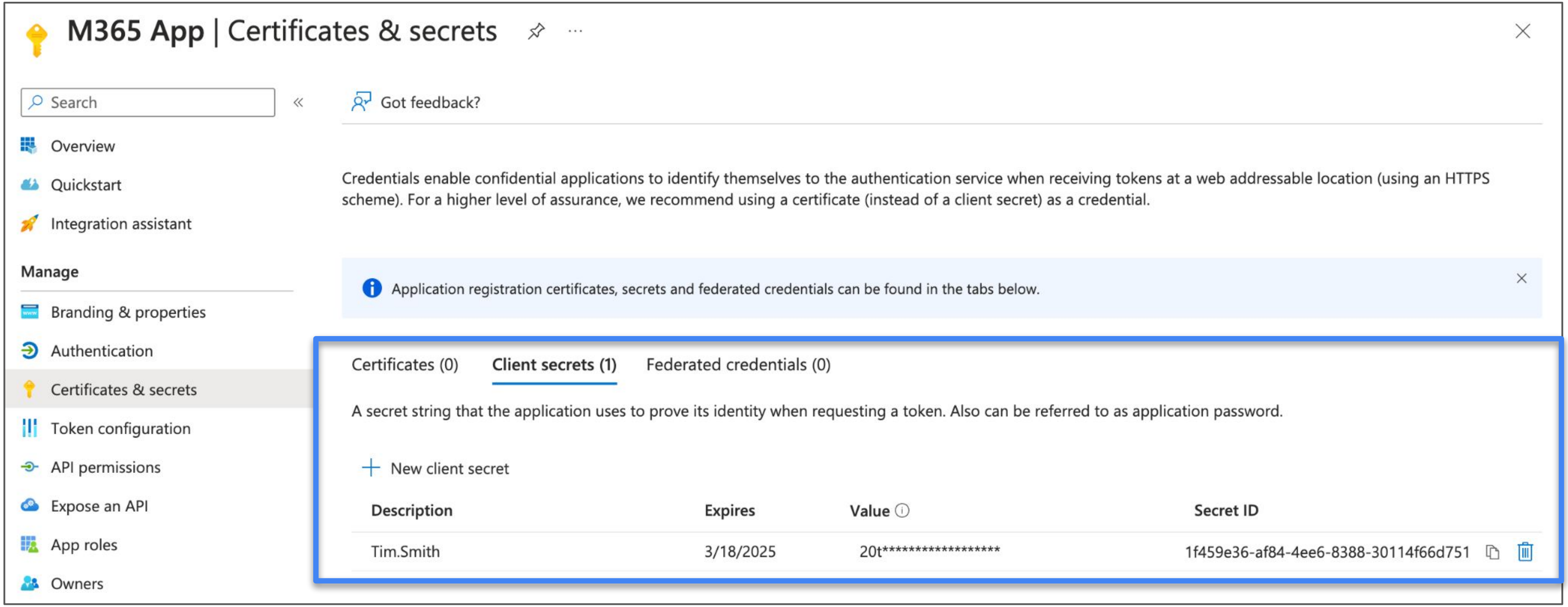
Account Manipulation: Additional Cloud Roles - Add permissions

Delete content

Update

Whatever you want!

Create a Client Secret That Could Be Used Later



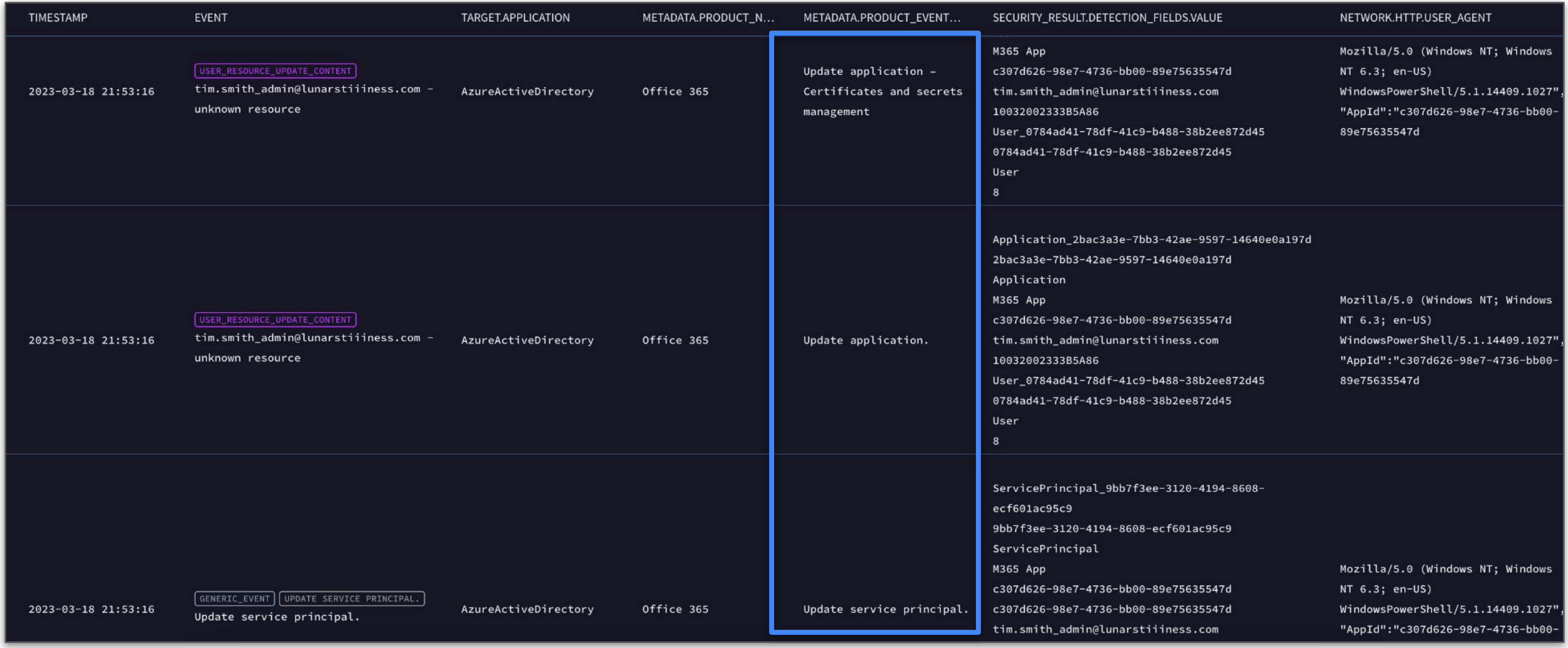
Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

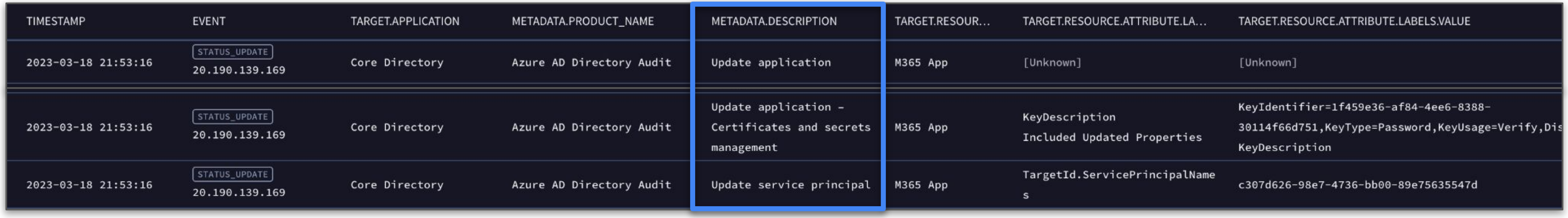
Description	Expires	Value	Secret ID
Tim.Smith	3/18/2025	20t*****************	1f459e36-af84-4ee6-8388-30114f66d751

Create a Client Secret - O365



TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODUCT_N...	METADATA.PRODUCT_EVENT...	SECURITY_RESULT.DETECTION_FIELDS.VALUE	NETWORK.HTTP.USER_AGENT
2023-03-18 21:53:16	USER_RESOURCE_UPDATE_CONTENT tim.smith_admin@lunarstiiiness.com - unknown resource	AzureActiveDirectory	Office 365	Update application – Certificates and secrets management	M365 App c307d626-98e7-4736-bb00-89e75635547d tim.smith_admin@lunarstiiiness.com 10032002333B5A86 User_0784ad41-78df-41c9-b488-38b2ee872d45 0784ad41-78df-41c9-b488-38b2ee872d45 User 8	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-89e75635547d
2023-03-18 21:53:16	USER_RESOURCE_UPDATE_CONTENT tim.smith_admin@lunarstiiiness.com - unknown resource	AzureActiveDirectory	Office 365	Update application.	Application_2bac3a3e-7bb3-42ae-9597-14640e0a197d 2bac3a3e-7bb3-42ae-9597-14640e0a197d Application M365 App c307d626-98e7-4736-bb00-89e75635547d tim.smith_admin@lunarstiiiness.com 10032002333B5A86 User_0784ad41-78df-41c9-b488-38b2ee872d45 0784ad41-78df-41c9-b488-38b2ee872d45 User 8	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-89e75635547d
2023-03-18 21:53:16	GENERIC_EVENT UPDATE SERVICE PRINCIPAL. Update service principal.	AzureActiveDirectory	Office 365	Update service principal.	ServicePrincipal_9bb7f3ee-3120-4194-8608-ecf601ac95c9 9bb7f3ee-3120-4194-8608-ecf601ac95c9 ServicePrincipal M365 App c307d626-98e7-4736-bb00-89e75635547d c307d626-98e7-4736-bb00-89e75635547d tim.smith_admin@lunarstiiiness.com	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027","AppId":"c307d626-98e7-4736-bb00-

Create a Client Secret - Azure AD

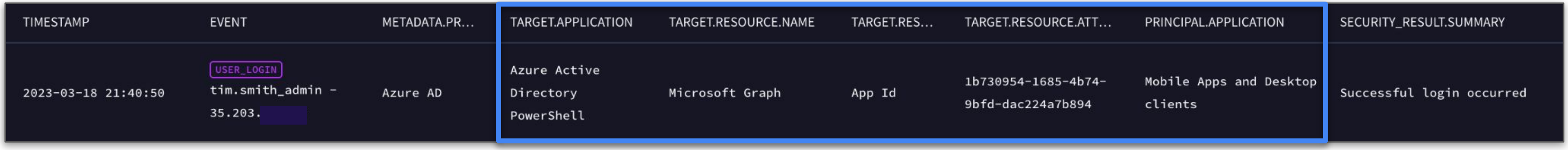


TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODUCT_NAME	METADATA.DESCRIPTION	TARGET.RESOUR...	TARGET.RESOURCE.ATTRIBUTE.LA...	TARGET.RESOURCE.ATTRIBUTE.LABELS.VALUE
2023-03-18 21:53:16	STATUS_UPDATE 20.190.139.169	Core Directory	Azure AD Directory Audit	Update application	M365 App	[Unknown]	[Unknown]
2023-03-18 21:53:16	STATUS_UPDATE 20.190.139.169	Core Directory	Azure AD Directory Audit	Update application – Certificates and secrets management	M365 App	KeyDescription Included Updated Properties	KeyIdentifier=1f459e36-af84-4ee6-8388-30114f66d751,KeyType=Password,KeyUsage=Verify,Dis KeyDescription
2023-03-18 21:53:16	STATUS_UPDATE 20.190.139.169	Core Directory	Azure AD Directory Audit	Update service principal	M365 App	TargetId.ServicePrincipalNames	c307d626-98e7-4736-bb00-89e75635547d

Create A New Access Token for App

Why? Access tokens are good for between 60-90 minutes

Once access token expires, a new one must be created



TIMESTAMP	EVENT	METADATA.PR...	TARGET.APPLICATION	TARGET.RESOURCE.NAME	TARGET.RES...	TARGET.RESOURCE.ATT...	PRINCIPAL.APPLICATION	SECURITY_RESULT.SUMMARY
2023-03-18 21:40:50	USER_LOGIN tim.smith_admin - 35.203.[redacted]	Azure AD	Azure Active Directory PowerShell	Microsoft Graph	App Id	1b730954-1685-4b74-9bfd-dac224a7b894	Mobile Apps and Desktop clients	Successful login occurred

Azure Active Directory PowerShell is a system exposed application

- Suspicious to see continual login events on this application
- AppId: 1b730954-1685-4b74-9bfd-dac224a7b894

https://learn.microsoft.com/en-us/azure/active-directory/develop/active-directory-configurable-token-lifetimes

Recharging My Token

(re)Create SAML Token

Encode SAML Token

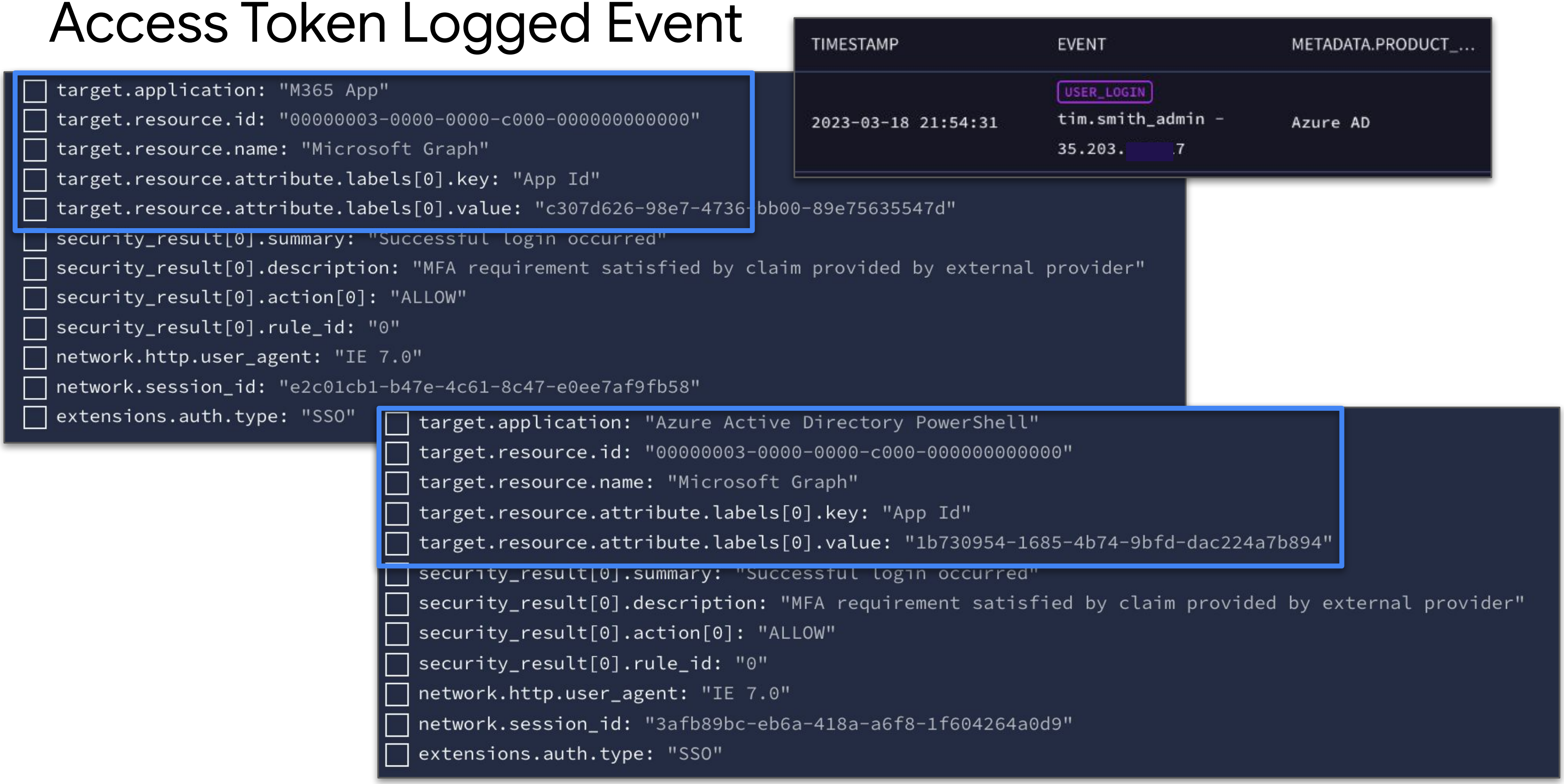
Make sure your app GUID is correct

Create request using client secret

Get new access token

Easily scripted - Could create perpetual access with a task scheduler or similar

Access Token Logged Event



TIMESTAMP	EVENT	METADATA.PRODUCT_...
2023-03-18 21:54:31	USER_LOGIN tim.smith_admin - 35.203.[redacted].7	Azure AD

```
□ target.application: "M365 App"
□ target.resource.id: "00000003-0000-0000-c000-000000000000"
□ target.resource.name: "Microsoft Graph"
□ target.resource.attribute.labels[0].key: "App Id"
□ target.resource.attribute.labels[0].value: "c307d626-98e7-4736-bb00-89e75635547d"
□ security_result[0].summary: "Successful login occurred"
□ security_result[0].description: "MFA requirement satisfied by claim provided by external provider"
□ security_result[0].action[0]: "ALLOW"
□ security_result[0].rule_id: "0"
□ network.http.user_agent: "IE 7.0"
□ network.session_id: "e2c01cb1-b47e-4c61-8c47-e0ee7af9fb58"
□ extensions.auth.type: "SSO"
```

```
□ target.application: "Azure Active Directory PowerShell"
□ target.resource.id: "00000003-0000-0000-c000-000000000000"
□ target.resource.name: "Microsoft Graph"
□ target.resource.attribute.labels[0].key: "App Id"
□ target.resource.attribute.labels[0].value: "1b730954-1685-4b74-9bfd-dac224a7b894"
□ security_result[0].summary: "Successful login occurred"
□ security_result[0].description: "MFA requirement satisfied by claim provided by external provider"
□ security_result[0].action[0]: "ALLOW"
□ security_result[0].rule_id: "0"
□ network.http.user_agent: "IE 7.0"
□ network.session_id: "3afb89bc-eb6a-418a-a6f8-1f604264a0d9"
□ extensions.auth.type: "SSO"
```

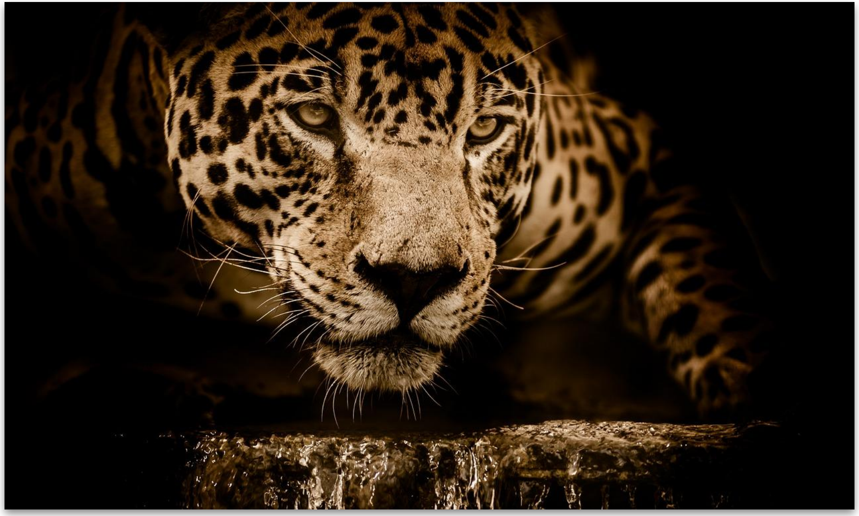
Things to Look For...

Do we need client secrets in our apps?

- Some may but others may provide alternatives
- What are the expirations on those secrets?

If you continually see Azure AD PowerShell app logins, look into it!

Baseline and understand login activities to other apps as well



Attack Path

Obtain Capabilities/ Permission Group Discovery

Gain access to ADFS signing key

Enumerate domain admins

Credential Access

Forge Web Credentials

SAML Tokens - Create a SAML Token using signing key

Craft an access token

Configure Access

Create application or use existing

Service principal creation (if creating app)

Add permissions

Add administrative consent to permissions

Establish Persistence

Create client secret in application

Create access token with client secret for future use

Actions on Objective

Enumerate users

Account Manipulation: Additional Cloud Roles - Add permissions

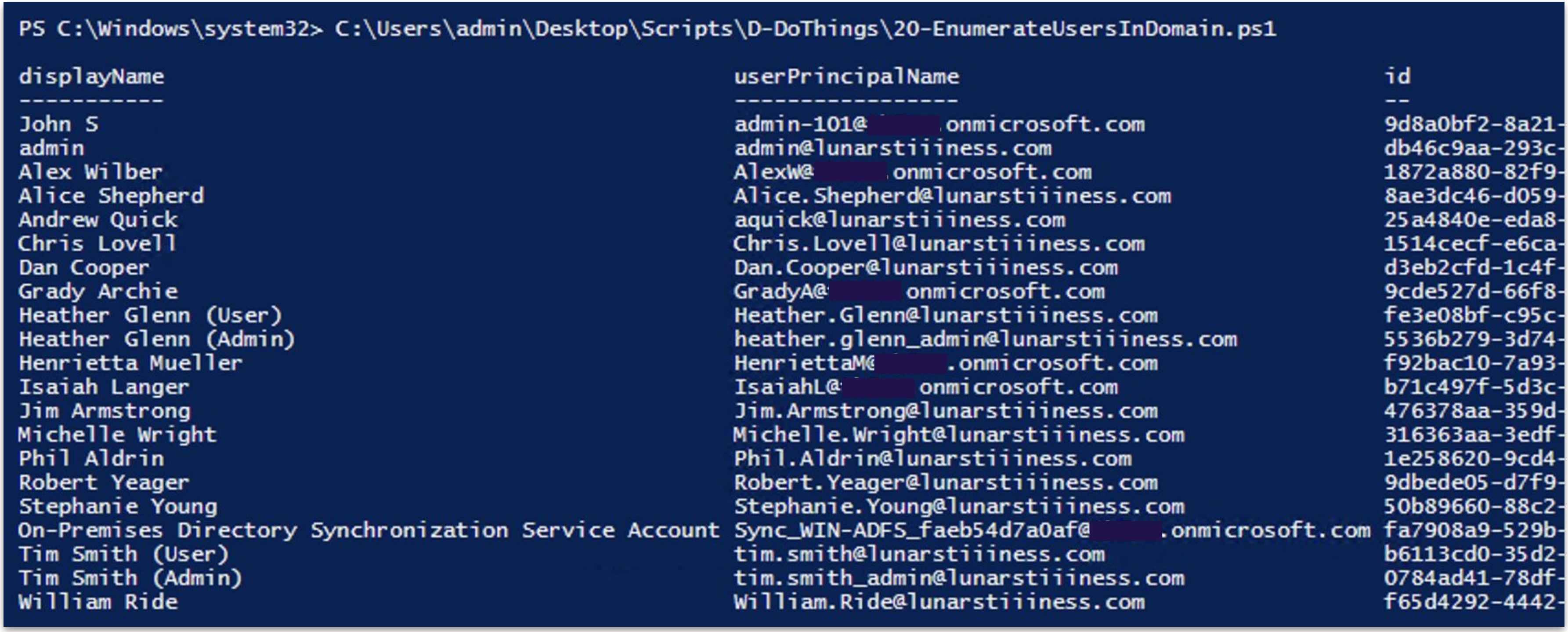
Delete content

Update

Whatever you want!

Enumerate Users

No visibility into this…

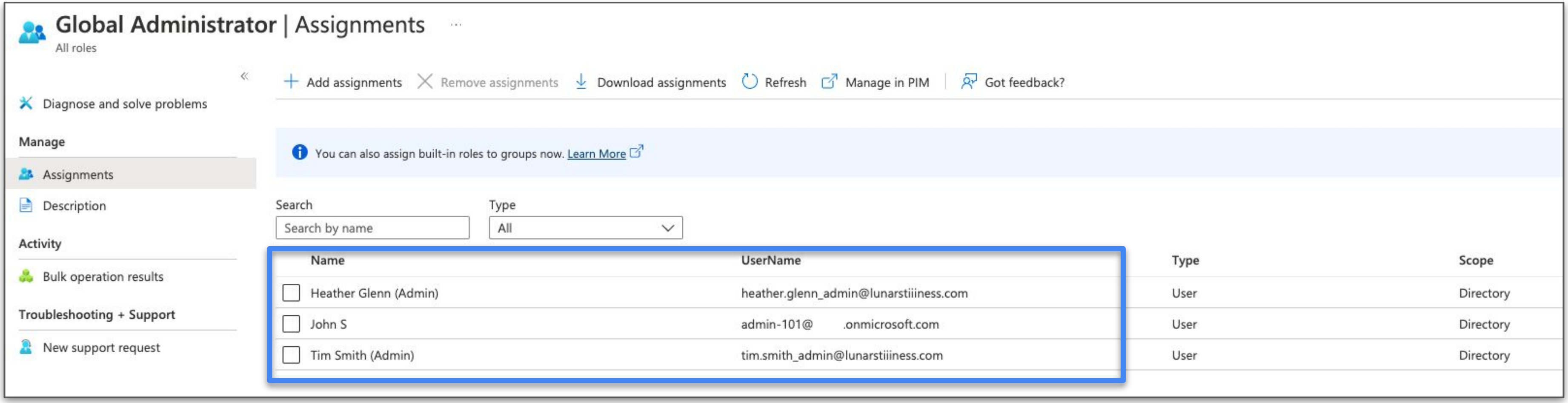


```
PS C:\Windows\system32> C:\Users\admin\Desktop\Scripts\D-DoThings\20-EnumerateUsersInDomain.ps1

displayName                                           userPrincipalName                                id
-----------                                           -----------------                                --
John S                                                admin-101@[redacted].onmicrosoft.com             9d8a0bf2-8a21-
admin                                                 admin@lunarstiiiness.com                         db46c9aa-293c-
Alex Wilber                                           AlexW@[redacted].onmicrosoft.com                 1872a880-82f9-
Alice Shepherd                                        Alice.Shepherd@lunarstiiiness.com                8ae3dc46-d059-
Andrew Quick                                          aquick@lunarstiiiness.com                        25a4840e-eda8-
Chris Lovell                                          Chris.Lovell@lunarstiiiness.com                  1514cecf-e6ca-
Dan Cooper                                            Dan.Cooper@lunarstiiiness.com                    d3eb2cfd-1c4f-
Grady Archie                                          GradyA@[redacted] onmicrosoft.com                9cde527d-66f8-
Heather Glenn (User)                                  Heather.Glenn@lunarstiiiness.com                 fe3e08bf-c95c-
Heather Glenn (Admin)                                 heather.glenn_admin@lunarstiiiness.com           5536b279-3d74-
Henrietta Mueller                                     HenriettaM@[redacted].onmicrosoft.com            f92bac10-7a93-
Isaiah Langer                                         IsaiahL@[redacted] onmicrosoft.com               b71c497f-5d3c-
Jim Armstrong                                         Jim.Armstrong@lunarstiiiness.com                 476378aa-359d-
Michelle Wright                                       Michelle.Wright@lunarstiiiness.com               316363aa-3edf-
Phil Aldrin                                           Phil.Aldrin@lunarstiiiness.com                   1e258620-9cd4-
Robert Yeager                                         Robert.Yeager@lunarstiiiness.com                 9dbede05-d7f9-
Stephanie Young                                       Stephanie.Young@lunarstiiiness.com               50b89660-88c2-
On-Premises Directory Synchronization Service Account Sync_WIN-ADFS_faeb54d7a0af@[redacted].onmicrosoft.com fa7908a9-529b-
Tim Smith (User)                                      tim.smith@lunarstiiiness.com                     b6113cd0-35d2-
Tim Smith (Admin)                                     tim.smith_admin@lunarstiiiness.com               0784ad41-78df-
William Ride                                          William.Ride@lunarstiiiness.com                  f65d4292-4442-
```

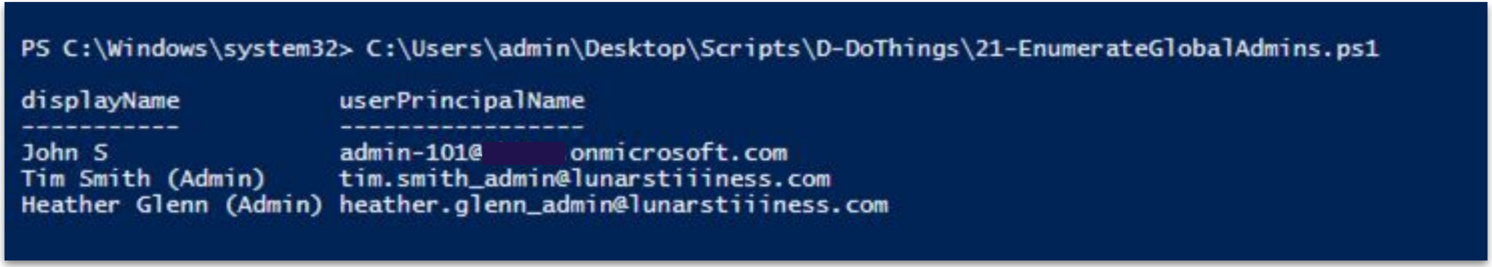
Enumerate Global Tenant Admins

The role id is a known value - 62e90394-69f5-4237-9190-012177145e10



You can also assign built-in roles to groups now. Learn More

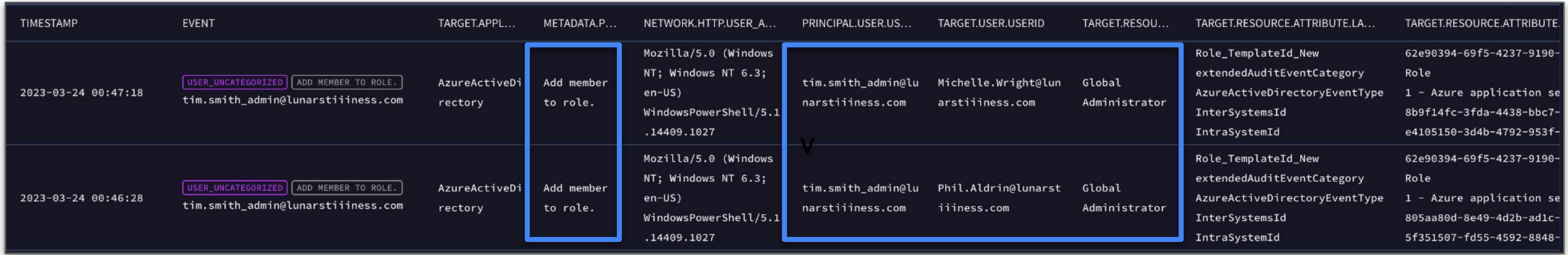
	Name	UserName	Type	Scope
□	Heather Glenn (Admin)	heather.glenn_admin@lunarstiiiness.com	User	Directory
□	John S	admin-101@ .onmicrosoft.com	User	Directory
□	Tim Smith (Admin)	tim.smith_admin@lunarstiiiness.com	User	Directory



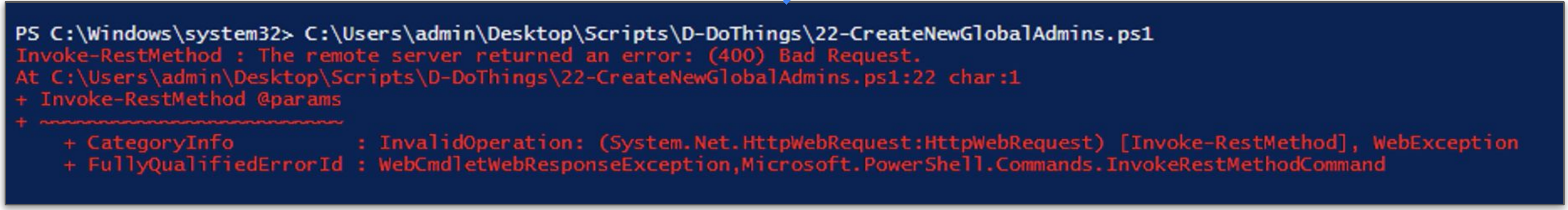
```
PS C:\Windows\system32> C:\Users\admin\Desktop\Scripts\D-DoThings\21-EnumerateGlobalAdmins.ps1

displayName           userPrincipalName
-----------           -----------------
John S                admin-101@[redacted]onmicrosoft.com
Tim Smith (Admin)     tim.smith_admin@lunarstiiiness.com
Heather Glenn (Admin) heather.glenn_admin@lunarstiiiness.com
```

Add Global Admin Role to Existing User

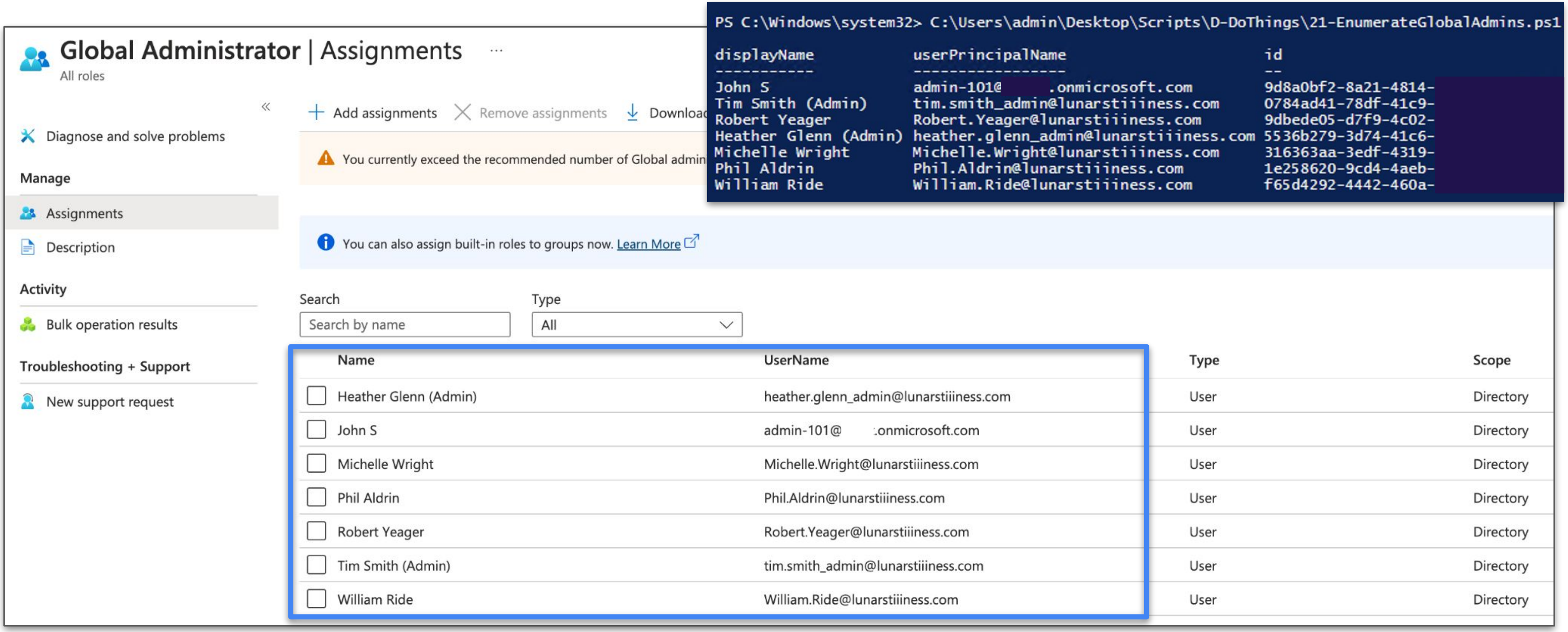


TIMESTAMP	EVENT	TARGET.APPL...	METADATA.P...	NETWORK.HTTP.USER_A...	PRINCIPAL.USER.US...	TARGET.USER.USERID	TARGET.RESOU...	TARGET.RESOURCE.ATTRIBUTE.LA...	TARGET.RESOURCE.ATTRIBUTE.
2023-03-24 00:47:18	USER_UNCATEGORIZED ADD MEMBER TO ROLE. tim.smith_admin@lunarstiiiness.com	AzureActiveDirectory	Add member to role.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027	tim.smith_admin@lunarstiiiness.com	Michelle.Wright@lunarstiiiness.com	Global Administrator	Role_TemplateId_New extendedAuditEventCategory AzureActiveDirectoryEventType InterSystemsId IntraSystemId	62e90394-69f5-4237-9190- Role 1 - Azure application se 8b9f14fc-3fda-4438-bbc7- e4105150-3d4b-4792-953f-
2023-03-24 00:46:28	USER_UNCATEGORIZED ADD MEMBER TO ROLE. tim.smith_admin@lunarstiiiness.com	AzureActiveDirectory	Add member to role.	Mozilla/5.0 (Windows NT; Windows NT 6.3; en-US) WindowsPowerShell/5.1.14409.1027	tim.smith_admin@lunarstiiiness.com	Phil.Aldrin@lunarstiiiness.com	Global Administrator	Role_TemplateId_New extendedAuditEventCategory AzureActiveDirectoryEventType InterSystemsId IntraSystemId	62e90394-69f5-4237-9190- Role 1 - Azure application se 805aa80d-8e49-4d2b-ad1c- 5f351507-fd55-4592-8848-



```
PS C:\Windows\system32> C:\Users\admin\Desktop\Scripts\D-DoThings\22-CreateNewGlobalAdmins.ps1
Invoke-RestMethod : The remote server returned an error: (400) Bad Request.
At C:\Users\admin\Desktop\Scripts\D-DoThings\22-CreateNewGlobalAdmins.ps1:22 char:1
+ Invoke-RestMethod @params
+ ~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidOperation: (System.Net.HttpWebRequest:HttpWebRequest) [Invoke-RestMethod], WebException
    + FullyQualifiedErrorId : WebCmdletWebResponseException,Microsoft.PowerShell.Commands.InvokeRestMethodCommand
```

Global Admin List



```
PS C:\Windows\system32> C:\Users\admin\Desktop\Scripts\D-DoThings\21-EnumerateGlobalAdmins.ps1

displayName           userPrincipalName                     id
-----------           -----------------                     --
John S                admin-101@[redacted].onmicrosoft.com  9d8a0bf2-8a21-4814-[redacted]
Tim Smith (Admin)     tim.smith_admin@lunarstiiiness.com    0784ad41-78df-41c9-
Robert Yeager         Robert.Yeager@lunarstiiiness.com      9dbede05-d7f9-4c02-
Heather Glenn (Admin) heather.glenn_admin@lunarstiiiness.com 5536b279-3d74-41c6-
Michelle Wright       Michelle.Wright@lunarstiiiness.com    316363aa-3edf-4319-
Phil Aldrin           Phil.Aldrin@lunarstiiiness.com        1e258620-9cd4-4aeb-
William Ride          William.Ride@lunarstiiiness.com       f65d4292-4442-460a-
```

Global Administrator | Assignments ...

All roles

⚠ You currently exceed the recommended number of Global admin

ⓘ You can also assign built-in roles to groups now. Learn More

Search: Search by name

Type: All

	Name	UserName	Type	Scope
□	Heather Glenn (Admin)	heather.glenn_admin@lunarstiiiness.com	User	Directory
□	John S	admin-101@[redacted].onmicrosoft.com	User	Directory
□	Michelle Wright	Michelle.Wright@lunarstiiiness.com	User	Directory
□	Phil Aldrin	Phil.Aldrin@lunarstiiiness.com	User	Directory
□	Robert Yeager	Robert.Yeager@lunarstiiiness.com	User	Directory
□	Tim Smith (Admin)	tim.smith_admin@lunarstiiiness.com	User	Directory
□	William Ride	William.Ride@lunarstiiiness.com	User	Directory

Things to Look For...

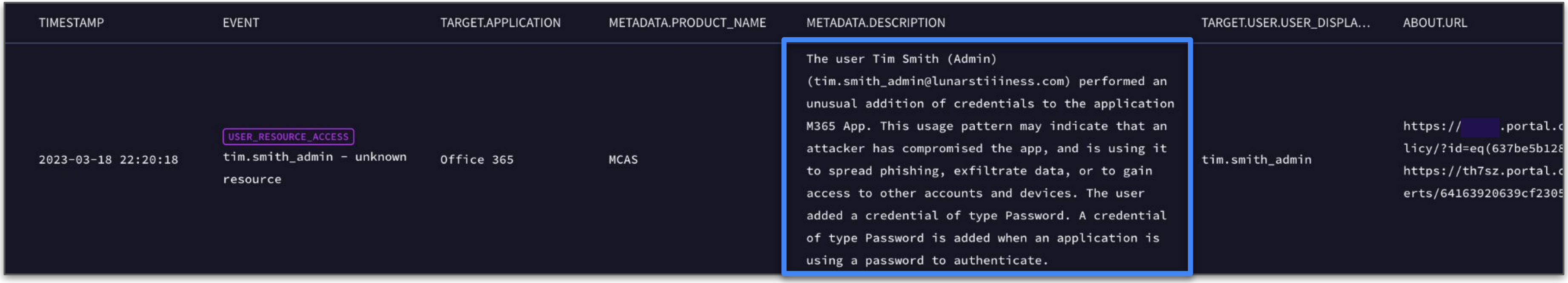
Enumeration activities are NOT logged

Roles have known GUIDs

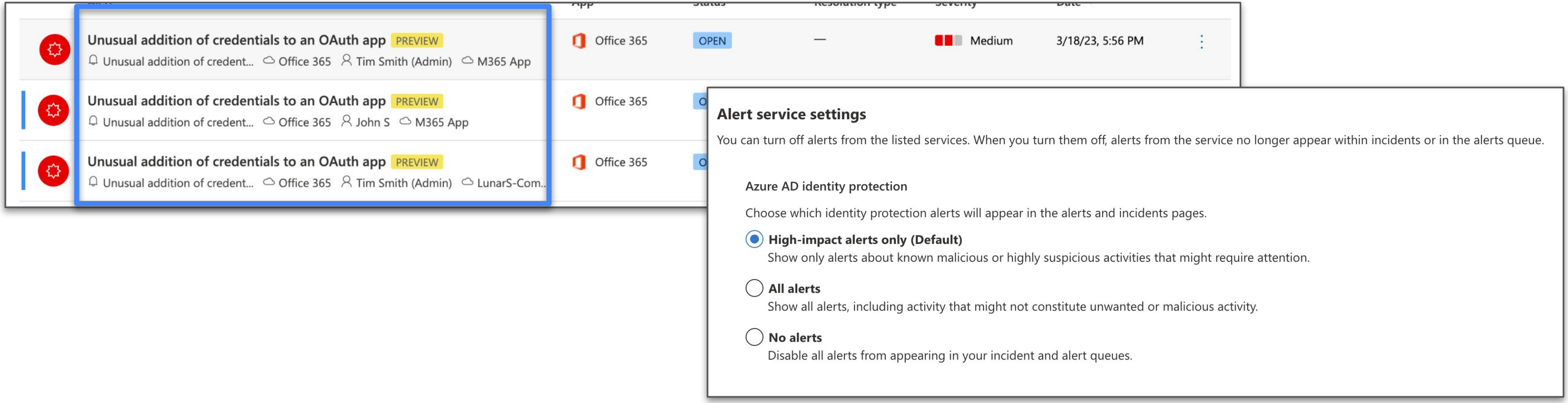
- Identify the roles of greatest interest and monitor them!

So many endpoints within the graph to monitor for, we only got to the admin role but lots more there

Graph API Alerts - Microsoft 365 Cloud Access Security



TIMESTAMP	EVENT	TARGET.APPLICATION	METADATA.PRODUCT_NAME	METADATA.DESCRIPTION	TARGET.USER.USER_DISPLA...	ABOUT.URL
2023-03-18 22:20:18	USER_RESOURCE_ACCESS tim.smith_admin - unknown resource	Office 365	MCAS	The user Tim Smith (Admin) (tim.smith_admin@lunarstiiiness.com) performed an unusual addition of credentials to the application M365 App. This usage pattern may indicate that an attacker has compromised the app, and is using it to spread phishing, exfiltrate data, or to gain access to other accounts and devices. The user added a credential of type Password. A credential of type Password is added when an application is using a password to authenticate.	tim.smith_admin	https://[redacted].portal.c licy/?id=eq(637be5b128 https://th7sz.portal.c erts/64163920639cf2305



	App	Status	Resolution type	Severity	Date	
Unusual addition of credentials to an OAuth app PREVIEW Unusual addition of credent... Office 365 Tim Smith (Admin) M365 App	Office 365	OPEN	—	Medium	3/18/23, 5:56 PM	⋮
Unusual addition of credentials to an OAuth app PREVIEW Unusual addition of credent... Office 365 John S M365 App	Office 365	O				
Unusual addition of credentials to an OAuth app PREVIEW Unusual addition of credent... Office 365 Tim Smith (Admin) LunarS-Com...	Office 365	O				

Alert service settings

You can turn off alerts from the listed services. When you turn them off, alerts from the service no longer appear within incidents or in the alerts queue.

Azure AD identity protection

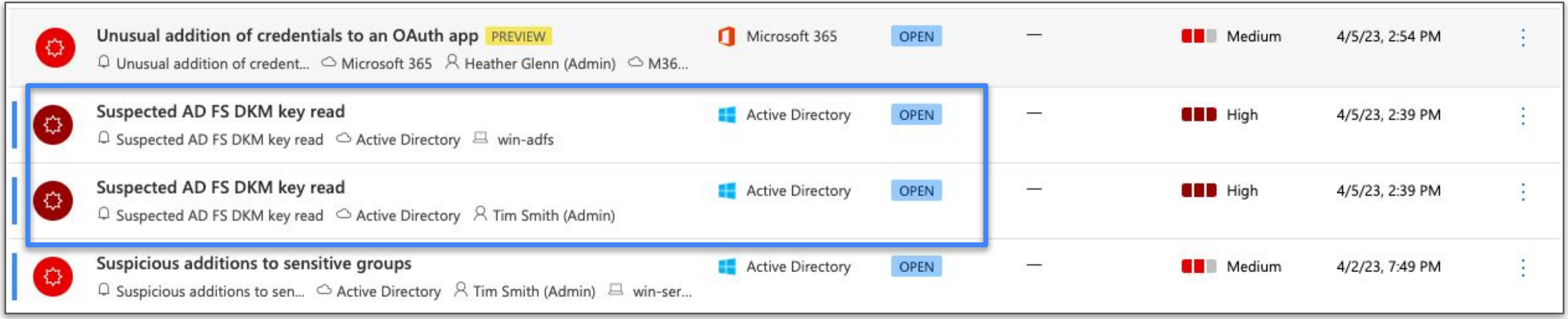
Choose which identity protection alerts will appear in the alerts and incidents pages.

● **High-impact alerts only (Default)**
Show only alerts about known malicious or highly suspicious activities that might require attention.

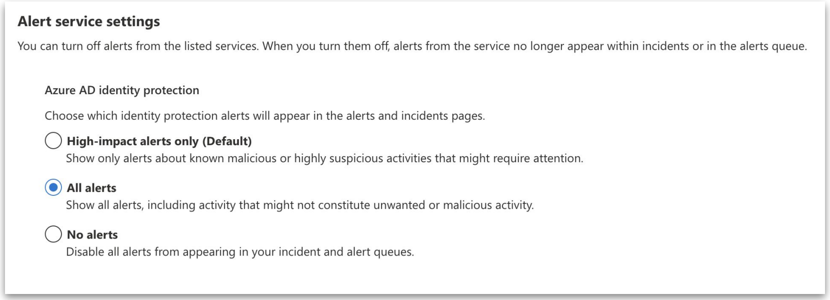
○ **All alerts**
Show all alerts, including activity that might not constitute unwanted or malicious activity.

○ **No alerts**
Disable all alerts from appearing in your incident and alert queues.

Same Attack / Different Filters



Unusual addition of credentials to an OAuth app PREVIEW Unusual addition of credent... Microsoft 365 Heather Glenn (Admin) M36...	Microsoft 365	OPEN	—	Medium	4/5/23, 2:54 PM	⋮
Suspected AD FS DKM key read Suspected AD FS DKM key read Active Directory win-adfs	Active Directory	OPEN	—	High	4/5/23, 2:39 PM	⋮
Suspected AD FS DKM key read Suspected AD FS DKM key read Active Directory Tim Smith (Admin)	Active Directory	OPEN	—	High	4/5/23, 2:39 PM	⋮
Suspicious additions to sensitive groups Suspicious additions to sen... Active Directory Tim Smith (Admin) win-ser...	Active Directory	OPEN	—	Medium	4/2/23, 7:49 PM	⋮



Alert service settings

You can turn off alerts from the listed services. When you turn them off, alerts from the service no longer appear within incidents or in the alerts queue.

Azure AD identity protection

Choose which identity protection alerts will appear in the alerts and incidents pages.

○ **High-impact alerts only (Default)**
Show only alerts about known malicious or highly suspicious activities that might require attention.

● **All alerts**
Show all alerts, including activity that might not constitute unwanted or malicious activity.

○ **No alerts**
Disable all alerts from appearing in your incident and alert queues.

What Else Could I Do?

Enumerate Users/Global Admins and Add/Modify/Delete users in those groups

Create/Update a cloud user

- Users generally are created in AD and synced to Azure AD

List/Create/Update/Delete contacts/calendar of signed in user

Read/Create mail messages

Modify Mail Rules

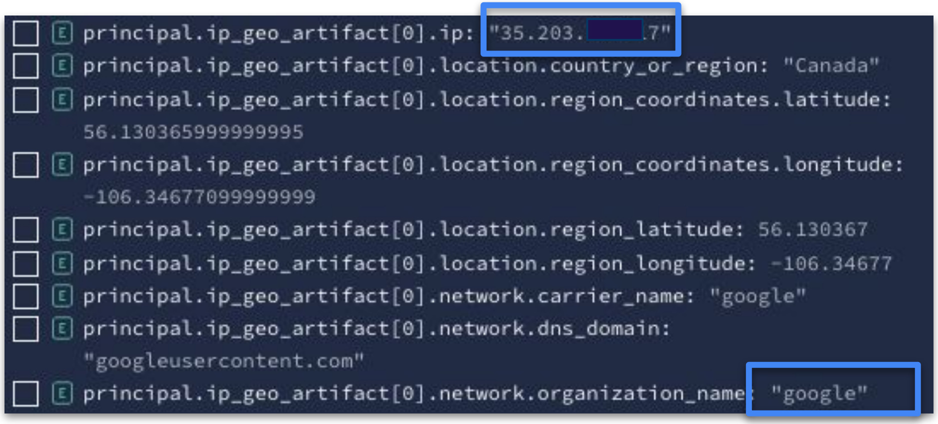
Security Alerts

IP Addressing - Azure AD

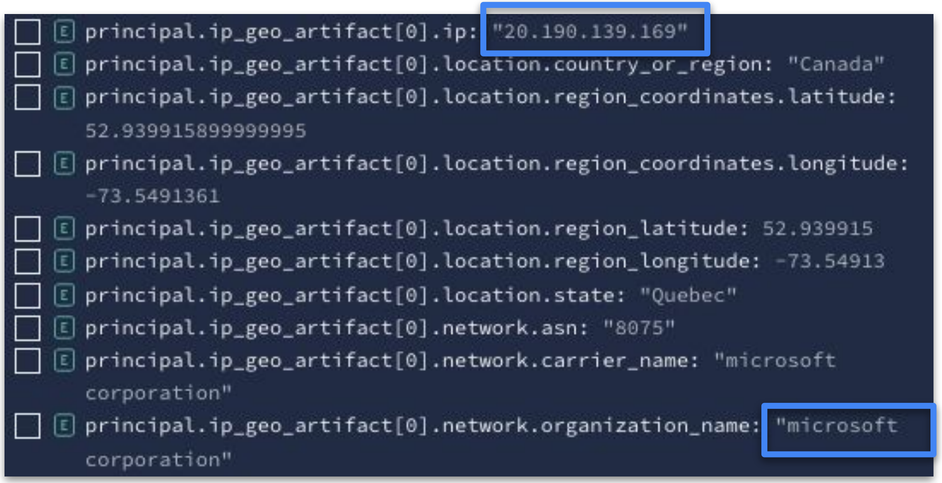
Azure AD (Sign-ins) will display user IP address

Azure AD Directory Audit is displaying Microsoft Azure IP address

- Appears to be near my adversary location (which is in GCP)
- Changed address from .169 to .170 and back during config



```
□ E principal.ip_geo_artifact[0].ip: "35.203.[redacted]7"
□ E principal.ip_geo_artifact[0].location.country_or_region: "Canada"
□ E principal.ip_geo_artifact[0].location.region_coordinates.latitude:
    56.130365999999995
□ E principal.ip_geo_artifact[0].location.region_coordinates.longitude:
    -106.34677099999999
□ E principal.ip_geo_artifact[0].location.region_latitude: 56.130367
□ E principal.ip_geo_artifact[0].location.region_longitude: -106.34677
□ E principal.ip_geo_artifact[0].network.carrier_name: "google"
□ E principal.ip_geo_artifact[0].network.dns_domain:
    "googleusercontent.com"
□ E principal.ip_geo_artifact[0].network.organization_name: "google"
```

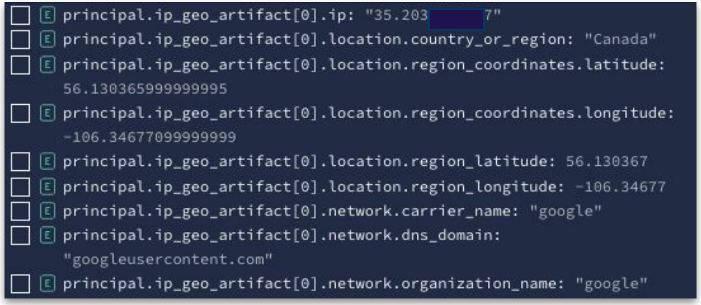


```
□ E principal.ip_geo_artifact[0].ip: "20.190.139.169"
□ E principal.ip_geo_artifact[0].location.country_or_region: "Canada"
□ E principal.ip_geo_artifact[0].location.region_coordinates.latitude:
    52.939915899999995
□ E principal.ip_geo_artifact[0].location.region_coordinates.longitude:
    -73.5491361
□ E principal.ip_geo_artifact[0].location.region_latitude: 52.939915
□ E principal.ip_geo_artifact[0].location.region_longitude: -73.54913
□ E principal.ip_geo_artifact[0].location.state: "Quebec"
□ E principal.ip_geo_artifact[0].network.asn: "8075"
□ E principal.ip_geo_artifact[0].network.carrier_name: "microsoft
    corporation"
□ E principal.ip_geo_artifact[0].network.organization_name: "microsoft
    corporation"
```

IP Addressing - O365

Office 365 events generally don’t have IP addresses

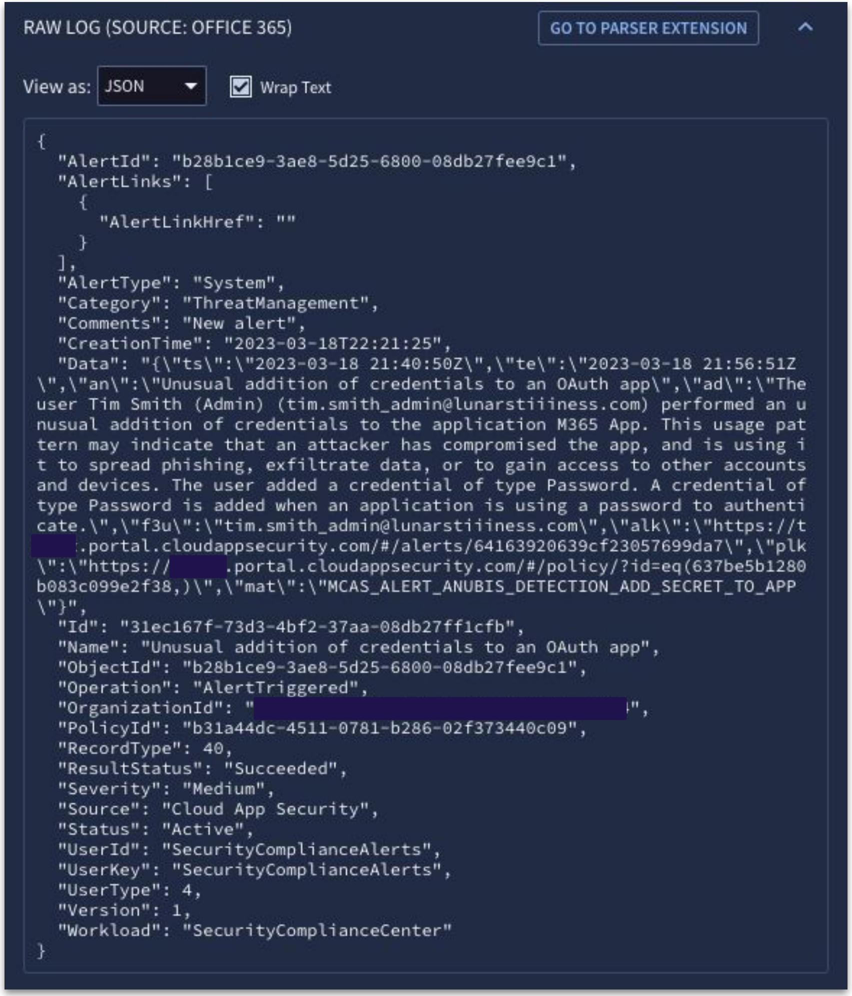
- UserLoggedIn is an exception



```
□ E principal.ip_geo_artifact[0].ip: "35.203[redacted]7"
□ E principal.ip_geo_artifact[0].location.country_or_region: "Canada"
□ E principal.ip_geo_artifact[0].location.region_coordinates.latitude:
    56.130365999999995
□ E principal.ip_geo_artifact[0].location.region_coordinates.longitude:
    -106.34677099999999
□ E principal.ip_geo_artifact[0].location.region_latitude: 56.130367
□ E principal.ip_geo_artifact[0].location.region_longitude: -106.34677
□ E principal.ip_geo_artifact[0].network.carrier_name: "google"
□ E principal.ip_geo_artifact[0].network.dns_domain:
    "googleusercontent.com"
□ E principal.ip_geo_artifact[0].network.organization_name: "google"
```

Even a threat alert doesn’t include where the behavior is originating from

Would need to pivot into the MS Defender for Cloud Apps to get Activity Log to find that IP mentioned



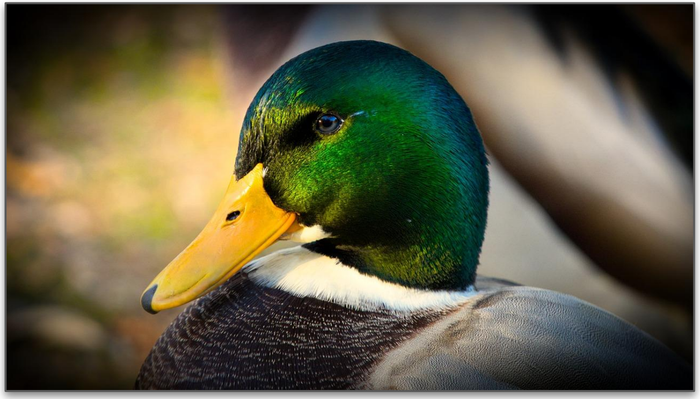
RAW LOG (SOURCE: OFFICE 365)

View as: JSON

☑ Wrap Text

```
{
  "AlertId": "b28b1ce9-3ae8-5d25-6800-08db27fee9c1",
  "AlertLinks": [
    {
      "AlertLinkHref": ""
    }
  ],
  "AlertType": "System",
  "Category": "ThreatManagement",
  "Comments": "New alert",
  "CreationTime": "2023-03-18T22:21:25",
  "Data": "{\"ts\":\"2023-03-18 21:40:50Z\",\"te\":\"2023-03-18 21:56:51Z
\",\"an\":\"Unusual addition of credentials to an OAuth app\",\"ad\":\"The
user Tim Smith (Admin) (tim.smith_admin@lunarstiiiness.com) performed an u
nusual addition of credentials to the application M365 App. This usage pat
tern may indicate that an attacker has compromised the app, and is using i
t to spread phishing, exfiltrate data, or to gain access to other accounts
and devices. The user added a credential of type Password. A credential of
type Password is added when an application is using a password to authenti
cate.\",\"f3u\":\"tim.smith_admin@lunarstiiiness.com\",\"alk\":\"https://t
[redacted].portal.cloudappsecurity.com/#/alerts/64163920639cf23057699da7\",\"plk
\":\"https://[redacted].portal.cloudappsecurity.com/#/policy/?id=eq(637be5b1280
b083c099e2f38,)\",\"mat\":\"MCAS_ALERT_ANUBIS_DETECTION_ADD_SECRET_TO_APP
\"}",
  "Id": "31ec167f-73d3-4bf2-37aa-08db27ff1cfb",
  "Name": "Unusual addition of credentials to an OAuth app",
  "ObjectId": "b28b1ce9-3ae8-5d25-6800-08db27fee9c1",
  "Operation": "AlertTriggered",
  "OrganizationId": "[redacted]",
  "PolicyId": "b31a44dc-4511-0781-b286-02f373440c09",
  "RecordType": 40,
  "ResultStatus": "Succeeded",
  "Severity": "Medium",
  "Source": "Cloud App Security",
  "Status": "Active",
  "UserId": "SecurityComplianceAlerts",
  "UserKey": "SecurityComplianceAlerts",
  "UserType": 4,
  "Version": 1,
  "Workload": "SecurityComplianceCenter"
}
```

Observations



As security practitioners, we are accustomed to having CRUD

- In this case we have DUC, no reads

The big stuff is logged

- Surprised to see contacts and calendar events and emails being created all in the GraphAPI

An adversary could use their own environment to test and script the GraphAPI calls using their choice of languages

The stumbles and hiccups and recon that we see in on-premise environments aren't there for analysts to leverage

Monitoring and hunting for this kind of attack requires particular attention because when they occur, they could be lightning quick

- Once initial access is gained, the mining of data won't be logged for an analyst to use

This also makes damage assessments difficult, the assumption must be that everything is compromised at that point

Additional Reading

Solorigate
https://www.microsoft.com/en-us/security/blog/2020/12/18/analyzing-solorigate-the-compromised-dll-file-that-started-a-sophisticated-cyberattack-and-how-microsoft-defender-helps-protect/

Remediation and Hardening Strategies for Microsoft 365 to Defend Against UNC2452
https://www.mandiant.com/resources/blog/remediation-and-hardening-strategies-for-microsoft-365-to-defend-against-unc2452

Best practice for securing and monitoring the AD FS trust with Azure AD
https://learn.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/best-practices-securing-ad-fs#best-practice-for-securing-and-monitoring-the-ad-fs-trust-with-azure-ad

AAD Internals
https://aadinternals.com/aadinternals/#introduction

Remediation and Hardening Strategies for Microsoft 365 to Defend Against APT29 (v1.3)
https://www.mandiant.com/media/17656

Thank You

@stonerpsu
https://www.linkedin.com/in/johnastoner/
@stonerpsu@infosec.exchange