



# Knocking on ~~Heavens~~ Clouds Door

Threat Hunting in Azure AD using Azula

@tas\_kmanager



"The opinions expressed in this presentation and on the following slides are solely those of the presenter and not necessarily those of presenter's employer"



# Disclaimer




"This talk is not sponsored by  
Microsoft nor is a product pitch;  
This is based on presenter own  
experience working with Microsoft  
Azure AD technology"



# Disclaimer

# Who am I?

Tas - @tas\_kmanager 

Senior Consultant, Big 4's MDR

## Experience:

- Detection Engineering
- Threat Hunting and Threat Research
- DFIR
- Automation

## Communities:

- The DFIR Report contributor
- OSCP contributor
- CDEF.ID member
- Sheridan College's ISSessions member
- Presented in numerous international conferences





# Who am I?



Good Food



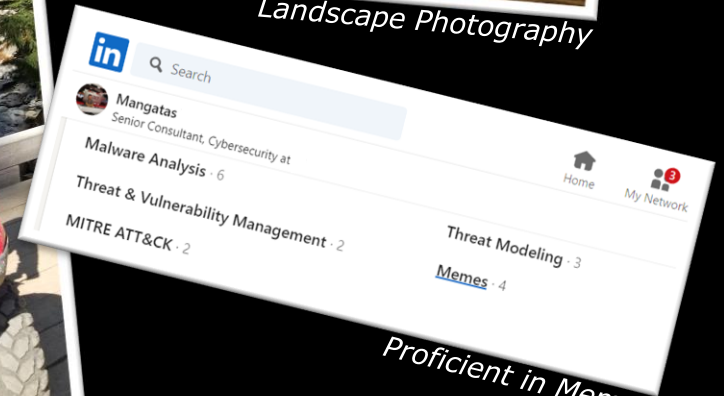
Astrophotography



Landscape Photography



Fun Stuff #2



Proficient in Memes



Fun Stuff #1

## *Who are You?*

- ...are a defender and wants to protect your cloud assets
- ...are a red teamer and wants to avoid being detected
- ...are a detection engineer and wants to build new detections
- ...are thinking this presentation is good to know
- ...are being told to go to this presentation by your boss
- ...are a Guns and Roses fan and works in Security
- ...are a ATLA fan and works in Security
- ...are lost and can't find your way out (plz stay ☹)

# Why are you here?

## Introduction

- Who am I?
- Who are you?
- Why are you here?

## Understanding Azure AD

- Azure AD vs Traditional Windows AD
- Risk Assessment of Azure AD
- Azure AD protection mechanisms

## Introduction to "Azure AD Reports"

- What is Azure AD Reports
- How to Access Azure AD Reports
- Types of Azure AD Reports

## Threat Hunting with "Azure AD Reports"

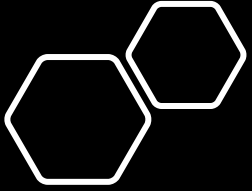
- Prerequisites
- Attack, Detection and Response
- Threat Hunting at Scale
- Reducing False Positives

## "Azula"

- Azula Details
- Demonstration

## Closing

- Blind Spots
- Improvement Ideas



# *Understanding Azure AD*





## Traditional AD vs Azure AD – Key Differences

### Traditional AD

- On premise, old-school
- Need some effort to integrate with other services
- Rely on on-premise components (DNS, DHCP, *bla-bla-bla*)
- Natively only support Windows OS devices

### Azure AD

- Cloud stuff
- Connected to other AZ services (HR systems, IAM, etc.)
- Apps are the future! (aka virtual this and virtual that)
- Mobile Devices? Computers? Servers? VMs? Kubernetes? Dockers? Apps? YES!

## *Traditional AD vs Azure AD – Access and Security*

### Traditional AD

- Internal, more secure?
- Domain, Org Unit, Groups
- Passwords ( + policy), Certs, Smartcard auth
- Auth Options
  - Kerberos
  - NTLM
- Policy
- External Users as Trusts

### Azure AD

- Internet facing, less secure?
- Roles (AZ AD RBAC) + PIM
- (Intelligent) password, and fancy MFA and Password-less auth
- Auth Options
  - SAML 2.0
  - OpenID
  - OAuth 2.0
  - WS Federation
- Microsoft Graph or Azure AD Graph
- External Users as Guests

# Risk Assessment of Azure AD

### Azure AD Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Azure AD platform.

[View on the ATT&CK® Navigator](#)  
Version Permalink

layout: side ▾

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
1 techniques	3 techniques	2 techniques	2 techniques	4 techniques	5 techniques	2 techniques
Valid Accounts (2)	Account Manipulation (1) Create Account (1) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (1) Steal Application Access Token Unsecured Credentials	Account Discovery (1) Cloud Service Dashboard Cloud Service Discovery Permission Groups Discovery (1) Software Discovery (1)	Endpoint Denial of Service (3) Network Denial of Service (2)

### Office 365 Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Office 365 platform.

[View on the ATT&CK® Navigator](#)  
Version Permalink

layout: side ▾

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
2 techniques	4 techniques	1 techniques	3 techniques	5 techniques	5 techniques	2 techniques	2 techniques	2 techniques
Phishing (1) Valid Accounts (2)	Account Manipulation (2) Create Account (1) Office Application Startup (6) Valid Accounts (2)	Valid Accounts (2)	Impair Defenses Use Alternate Authentication Material (2) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (1) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials	Account Discovery (2) Cloud Service Dashboard Cloud Service Discovery Permission Groups Discovery (1) Software Discovery (1)	Internal Spearphishing Use Alternate Authentication Material (2) Cloud Service Discovery	Data from Information Repositories (1) Email Collection (2) Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Man-in-the-Middle (2) Screen Capture Video Capture	Endpoint Denial of Service (3) Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

PS: THIS OFC OVERSIMPLIFICATION

## Windows Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise. The Matrix contains information for the Windows platform.

[View on the ATT&CK® Navigator](#)

[Version Permalink](#)

layout: side ▾

show sub-techniques

hide sub-techniques

help

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
9 techniques	10 techniques	18 techniques	13 techniques	32 techniques	14 techniques	23 techniques	9 techniques	15 techniques	16 techniques	8 techniques	13 techniques
Drive-by Compromise Exploit Public-Facing Application External Remote Services Hardware Additions Phishing (2) Trojan Valid Accounts (3)	Command and Scripting Interpreter (5) Exploitation for Client Execution Inter-Process Communication (2) Native API Scheduled Task/Job (2) Trojan Modules Trojan System Services (1) User Execution (2)	Account Manipulation (1) BITS Jobs Boot or Logon Autostart Execution (16) Boot or Logon Initialization Scripts (2) Browser Extensions Compromise Client Software Binary Create Account (2) Create or Modify System Process (1) Event Triggered Execution (11) External Remote Services Hijack Execution Flow (9) Modify Authentication Process (2) Office Application Startup (6) Pre-OS Boot (3) Scheduled Task/Job (2) Server Software Component (3) Traffic Signaling (1) Valid Accounts (3)	Abuse Elevation Control Mechanism (1) Access Token Manipulation (5) BITS Jobs Deobfuscate/Decode Files or Information Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (1) Hide Artifacts (6) Hijack Execution Flow (9) Impair Defenses (5) Indirect Command Execution Masquerading (3) Modify Authentication Process (2) Modify Registry Obfuscated Files or Information (5) Pre-OS Boot (3) Process Injection (8) Rogue Domain Controller Rootkit Signed Binary Proxy Execution (11) Signed Script Proxy Execution (1) Subvert Trust Controls (3) Template Injection Traffic Signaling (1) Trusted Developer Utilities Proxy Execution (1) Use Alternate Authentication Material (2) Valid Accounts (3) Virtualization/Sandbox Evasion (3)	Abuse Elevation Control Mechanism (1) Access Token Manipulation (5) BITS Jobs Deobfuscate/Decode Files or Information Domain Policy Modification (2) Execution Guardrails (1) Exploitation for Defense Evasion File and Directory Permissions Modification (1) Hide Artifacts (6) Hijack Execution Flow (9) Impair Defenses (5) Indirect Command Execution Masquerading (3) Modify Authentication Process (2) Modify Registry Obfuscated Files or Information (5) Pre-OS Boot (3) Process Injection (8) Rogue Domain Controller Rootkit Signed Binary Proxy Execution (11) Signed Script Proxy Execution (1) Subvert Trust Controls (3) Template Injection Traffic Signaling (1) Trusted Developer Utilities Proxy Execution (1) Use Alternate Authentication Material (2) Valid Accounts (3) Virtualization/Sandbox Evasion (3)	Brute Force (4) Credentials from Password Stores (3) Exploitation for Credential Access Forced Authentication Forge Web Credentials (2) Input Capture (4) Man-in-the-Middle (2) Modify Authentication Process (2) Network Sniffing OS Credential Dumping (6) Steal or Forge Kerberos Tickets (4) Steal Web Session Cookie Two-Factor Authentication Interception Unsecured Credentials (4)	Account Discovery (3) Application Window Discovery Browser Bookmark Discovery Domain Trust Discovery File and Directory Discovery Network Service Scanning Network Share Discovery Network Sniffing Password Policy Discovery Peripheral Device Discovery Permission Groups Discovery (2) Process Discovery Query Registry Remote System Discovery Software Discovery (1) System Information Discovery System Location Discovery System Network Configuration Discovery (1) System Network Connections Discovery System Owner/User Discovery System Service Discovery System Time Discovery Virtualization/Sandbox Evasion (3)	Exploitation of Remote Services Internal Spearphishing Lateral Tool Transfer Remote Service Session Hijacking (1) Remote Services (3) Replication Through Removable Media Software Deployment Tools Taint Shared Content Use Alternate Authentication Material (2)	Archive Collected Data (3) Audio Capture Automated Collection Clipboard Data Data from Information Repositories (1) Data from Local System Data from Network Shared Drive Data from Removable Media Data Staged (2) Email Collection (3) Input Capture (4) Man in the Browser Man-in-the-Middle (2) Screen Capture Video Capture	Application Layer Protocol (4) Communication Through Removable Media Automated Collection Clipboard Data Data Encoding (2) Data Obfuscation (3) Dynamic Resolution (3) Encrypted Channel (2) Fallback Channels Ingress Tool Transfer Multi-Stage Channels Non-Application Layer Protocol Non-Standard Port Protocol Tunneling Proxy (4) Remote Access Software Traffic Signaling (1) Web Service (3)	Automated Exfiltration Data Transfer Size Limits Exfiltration Over Alternative Protocol (3) Exfiltration Over C2 Channel Exfiltration Over Other Network Medium (1) Exfiltration Over Physical Channel Exfiltration Over Web Service (2) Scheduled Transfer	Account Access Removal Data Destruction Data Encrypted for Impact Data Manipulation (3) Defacement (2) Disk Wipe (2) Endpoint Denial of Service (4) Firmware Corruption Inhibit System Recovery Network Denial of Service (2) Resource Hijacking Service Stop System Shutdown/Reboot

“Defenders think in lists.  
Attackers think in graphs. As  
long as this is true, attackers  
win.”

VP

- John Lambert, ~~General Manager~~, Microsoft Threat Intelligence Center

# DEFENDERS HAVE TO THINK IN GRAPH TOO!

*initial access connects the rest of the (tactics) graph with the attackers*

**STOP  
THEM  
HERE**

# Azure AD Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Azure AD platform.

View on the ATT&CK® Navigator

Version Permalink

layout: side

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Impact
1 techniques	3 techniques	2 techniques	2 techniques	4 techniques	5 techniques	2 techniques
Valid Accounts (2)	Account Manipulation (1) Create Account (1) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Domain Policy Modification (1) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (1) Steal Application Access Token Unsecured Credentials	Account Discovery (1) Cloud Service Dashboard Cloud Service Discovery Permission Groups Discovery (1) Software Discovery (1)	Endpoint Denial of Service (3) Network Denial of Service (2)

# Office 365 Matrix

Below are the tactics and techniques representing the MITRE ATT&CK® Matrix for Enterprise covering cloud-based techniques. The Matrix contains information for the Office 365 platform.

View on the ATT&CK® Navigator

Version Permalink

layout: side

show sub-techniques

hide sub-techniques

help

Initial Access	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Impact
2 techniques	4 techniques	1 techniques	3 techniques	5 techniques	5 techniques	2 techniques	2 techniques	2 techniques
Phishing (1) Valid Accounts (2)	Account Manipulation (2) Create Account (1) Steal Application Access Token (6) Valid Accounts (2)	Valid Accounts (2)	Impair Defenses Use Alternate Authentication Material (2) Valid Accounts (2)	Brute Force (4) Forge Web Credentials (1) Steal Application Access Token Steal Web Session Cookie Unsecured Credentials	Account Discovery (2) Cloud Service Dashboard Cloud Service Discovery Permission Groups Discovery (1) Software Discovery (1)	Internal Spearphishing Use Alternate Authentication Material (2)	Data from Information Repositories (1) Email Collection (2)	Endpoint Denial of Service (3) Network Denial of Service (2)

**WORRY  
LESS  
HERE**

# Attack Vectors

## *BEFORE Initial Access*

Lots of negligence and misconfiguration-based vectors

- **Non-MFA and Legacy user compromise (related to Brute Force)**
- **MFA user negligence**
- MFA compromise
- **Neglected Risky Users alerts**
- **Ignoring Azure AD Reports and O365 Logs**
- Custom integration containing misconfigurations (e.g., Identity Provider)
- Unsecured Cloud apps and objects
- **Credential Stuffing**

Brute Force based vectors

- **Regular Brute Force**
- **Password Spray attacks**
- Username Brute force or recon
- MFA Brute force or recon

Default Configuration and Naming

- Following Azure naming convention to the teeth (Federation recon)

## *AFTER Initial Access*

Hybrid AD vectors

- PHS exploit
- Golden SAML exploit

Azure LOLBAS style vectors

- Add users, resources, groups, etc.
- Modify access, policy, roles, etc.

Resources vectors (VMs, Kubernetes, etc.)

Others







## Azure AD Protection Mechanisms

- MFA, yes, the Multi Factor Authentication
- Conditional Access policy
  - E.g., no access except from these IPs, no access except from accepted devices
- Attack surface reduction
  - Just In Time Access
- Blocking Legacy Authentication
  - Old MS Office Apps
  - IMAP, POP3, etc.
- Go Passwordless (Whenever you are ready!)
- All-in-one Security Portal + others security solutions
- Risk Detection (Azure AD Identity Protection Automation)
- Reporting AKA Logs
  - Audit Logs
  - Sign-in Logs
  - Risky Users (from ML Risk Detection)

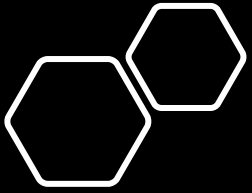


# Azure AD Protection Summarized

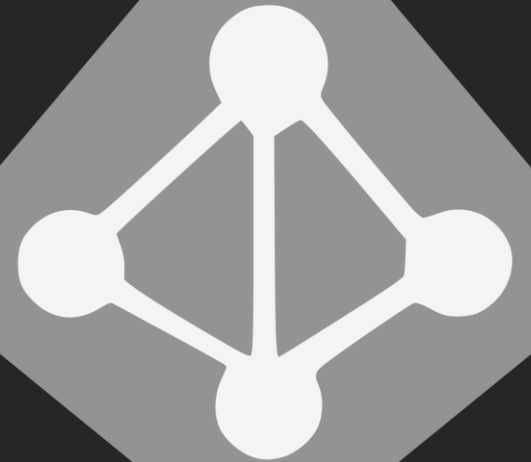
 <p>Strong multi-factor authentication safeguards user credentials</p>	 <p>Context-based adaptive policies grant, limit or block access</p>	 <p>Real-time machine learning guards against use of leaked or stolen credentials and blocks suspicious login attempts</p>	 <p>Identity governance controls access to apps and data for all users, including privileged users, across hybrid environments</p>
---	---	---	---

# Azure AD ML Risk Detection

Name	Description	Timing	Linked to	Detection source	Status
Anonymous IP address	Tor or anonymizer VPNs	Real-time	Azure AD login	Identity Protection	GA
Atypical travel	Travel distance > Travel time	Offline	Azure AD login	Identity Protection	GA
Leaked credentials	Valid credentials compromised	Offline	User	Identity Protection	GA
Malware linked IP address	Botnet linked IP address	Offline	Azure AD login	Identity Protection	GA
Unfamiliar sign-in properties	Periodicity based unfamiliar properties.	Real-time	Azure AD login	Identity Protection	GA (New)
Unfamiliar sign-in properties	Multiple failed sign-ins in a short time period	Real-time	Azure AD login	Identity Protection	GA
Azure AD threat intelligence	ISP investigations intel	Offline	User	ISP investigations	GA
Admin confirmed user compromised	Admin feedback	Offline	User	Admin	GA
Malicious IP address	Valid creds, blocked IP (Sharkfin, etc.)	Offline	Azure AD login	Identity Protection	GA (New)
Impossible travel	Inter / intra session travel (MCAS)	Offline	Azure AD login	MS Cloud App Security	Preview
Suspicious inbox manipulation rules	Mailbox manipulation (MCAS)	Offline	Azure AD login	MS Cloud App Security	Preview
Malicious IP address (ADFS)	ADFS login from high failure IP	Offline	ADFS login	Identity Protection	Preview
Malware linked IP address (ADFS)	Botnet detection on ADFS logins	Offline	ADFS login	Identity Protection	Preview
Additional risk detected	Premium detection(s)	-	-	-	GA

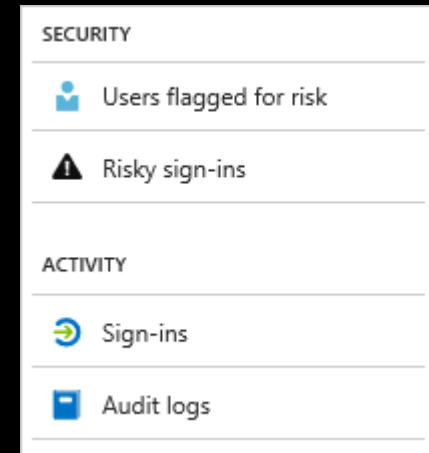


# *Introduction to “Azure AD Reports”*



# What is Azure AD Reports

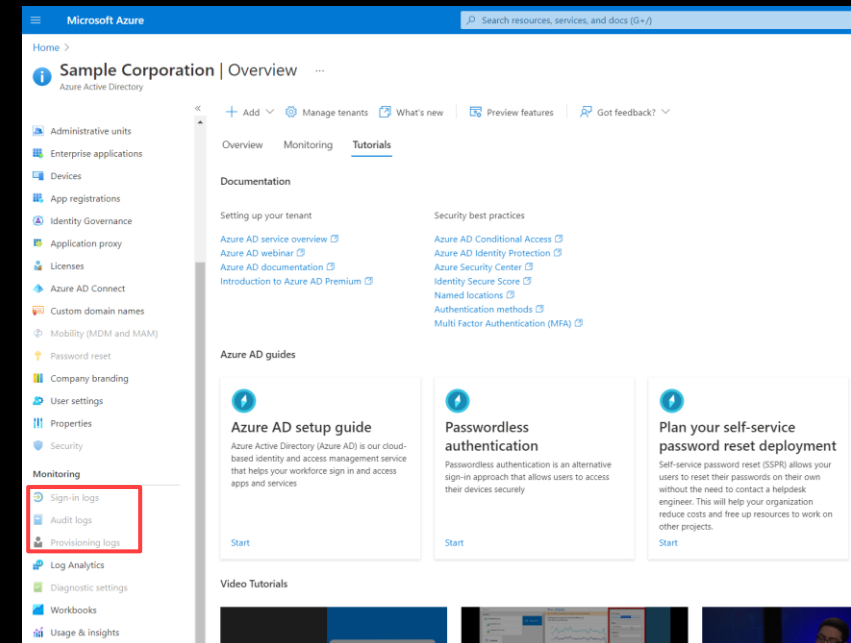
- Provide comprehensive view of activity in your environment
- Different type of reports, such as
  - Users flagged for Risk report (part of Azure AD Identity Protection Automation)
  - Risky Sign-ins report (part of Azure AD Identity Protection Automation)
  - Audit logs report
  - Sign-ins report
- All report types interconnected and can help give complete story!
  - Even with additional logs from other sources (e.g., O365 Logs)



*Types of Azure AD Reports*

# How to Access Azure AD Reports

- Quick view from Azure Active Directory menu > [Monitoring](#) section
- Analyze using [Graph API](#), instruction is [here](#)
- Integrate and analyze with SIEM
  - [Azure Monitor Logs](#)
  - [ArcSight](#)
  - [Splunk](#)
  - [Elastic/ODFE \(Filebeat\)\\*](#)



Azure AD Monitoring section

\* Data presented in this presentation is imported to Elastic/ODFE

# *Types of Azure AD Reports*

## **Users Flagged For Risk**

- Contains information if a user is Risky, based on activities or user's parameter on Azure AD via Risk model
- Sources are from MS Threat Intel and leaked credentials
- Either Real Time or Offline (2hr - 24hr delay)
- We won't talk too much about this here

## **Audit Logs**

- Contains all management activities (or as configured) performed by users and admins
- Available for all licenses

## **Risky Sign-Ins**

- Coming from their Risk model, flags sign-in as suspicious based on several conditions.
- Either Real Time or Offline (2hr - 24hr delay)
- Low (P2 License), Medium and High



## **Sign-Ins**

- Contains all sign-ins (or as configured) performed by users and admins
- Interactive or Non-Interactive, Failed or Success, MFA or Single Factor
- Can be used to track sign in pattern, create statistic, baselining, etc.




# Sign-Ins Important Attributes

## IP Address and Enrichment Information

properties.ipAddress	123.123.123.123
properties.isInteractive	true
properties.isTenantRestricted	 false
properties.location.city	Beijing
properties.location.countryOrRegion	CN
properties.location.geoCoordinates.latitude	56.695
properties.location.geoCoordinates.longitude	-111.337
properties.location.state	Beijing
properties.networkLocationDetails	

Geo Information sometimes inaccurate, double check with additional OSINT sources  
(Different city name, 1 IP with 2 cities, etc.)

## Application and Device Information

properties.clientAppUsed	Browser
properties.userAgent	Mozilla/5.0 (iPhone; CPU iPhone OS 14_7_1 like Mac OS X) AppleWebKit/605.1.15
properties.appDisplayName	Microsoft App Access Panel
properties.crossTenantAccessType	 none
properties.deviceDetail.browser	Mobile Safari 14.1.2
properties.deviceDetail.deviceId	
properties.deviceDetail.operatingSystem	iOS 14

If device is registered, there will be more information here such as device name, device ID, etc.

## User Information

properties.userDisplayName	Tas
properties.userId	12312312-46c1-4f10-bd7b-111111111111
properties.userPrincipalName	tas@samplecorporation.com
properties.userType	Member

## Error/Failure Information

resultDescription	User did not pass the MFA challenge.
resultSignature	None
resultType	50074

If result description is “Others”, you must look it up at [login.microsoftonline.com/error](https://login.microsoftonline.com/error)

## Time Information

properties.createdDateTime	2021-09-03T04:37:30.555222+00:00
azure.enqueued_time	Sep 3, 2021 @ 00:41:18.506

Created Date Time is when the sign-ins event is created (aka happened) - UTC

Enqueued Time is when the sign-ins event completed the Risk Model process - Local Time

## Sign-Ins Important Attributes

## MFA and Conditional Access

```

    properties.appliedConditionalAccessPolicies {
      "enforcedGrantControls": [
        "Mfa"
      ],
      "id": "1231231123-0d8c-4ca2-8773-12314415122512",
      "conditionsSatisfied": 287,
      "enforcedSessionControls": [],
      "result": "failure",
      "conditionsNotSatisfied": 0,
      "displayName": "Windows-MacOS-Conditional-Access-with-MFA"
    },
  ],
  "id": "1231231123-0d8c-4ca2-8773-12314415122512",
  "conditionsSatisfied": 287,
  "enforcedSessionControls": [],
  "result": "failure",
  "conditionsNotSatisfied": 0,
  "displayName": "Windows-MacOS-Conditional-Access-with-MFA"
}

```

Above will be listed all the Conditional Access policies applied to the user, default and custom e.g., MFA for admin accounts, block legacy auth or allow managed devices only

Conditional Access policy is available on certain Azure AD license

```

    properties.authenticationDetails
    {
      "authenticationMethod": "Password",
      "RequestSequence": 1,
      "succeeded": true,
      "StatusSequence": 0,
      "authenticationMethodDetail": "Pass-through Authentication; PTA AgentId",
      "authenticationStepRequirement": "Multi-factor authentication",
      "authenticationStepDateTime": "2021-09-02T22:40:09.9435008+00:00"
    },
    {
      "authenticationStepRequirement": "Multi-factor authentication",
      "authenticationStepDateTime": "2021-09-02T22:40:09.9435008+00:00",
      "authenticationStepResultDetail": "MFA required in Azure AD",
      "succeeded": false
    }
  ]
}

```

Above will tell you the details of authentication completed (or denied)  
First factor (PTA, PHS) and their status  
Multi factor (MFA method; Mobile App, Phone, Text) and their status

```

① properties.authenticationProcessingDetails {
    "key": "Domain Hint Present",
    "value": "True"
  },
  {
    "key": "IsCAEToken",
    "value": "False"
  }
}

! properties.authenticationRequirement multiFactorAuthentication

② properties.authenticationRequirementPolicies {
  "detail": "Conditional Access",
  "requirementProvider": "multiConditionalAccess"
}

! properties.conditionalAccessStatus failure

```

Above shows summary of authentication requirement, overall conditional (sign in) status, and processing details

## *Risky Sign-Ins Important Attributes*

### Risk Information

properties.riskDetail	none
properties.riskEventTypes	unfamiliarFeatures
properties.riskEventTypes_v2	unfamiliarFeatures
properties.riskLevelAggregated	low
properties.riskLevelDuringSignIn	medium
properties.riskState	atRisk

Risk Detail available on certain Event Types

Risk Level Aggregated generated after aggregating user's data, might be different from Risk Level During Sign In

Risk State indicate if the sign in event is marked Risky or not



## *Risky Sign-Ins Event Types (Risk Model)*

### Location Based Risk

- Atypical travel
- Impossible travel
- New country

### IP Address Based Risk

- Malicious IP address
- Anonymous IP address
- Malware linked IP address
- Activity from anonymous IP address

### Anomaly Based Risk

- Anomalous Token
- Token Issuer Anomaly
- Suspicious browser
- Unfamiliar sign-in properties
  - Such as User Agent, Application, etc.
- Suspicious inbox manipulation rules
- Suspicious inbox forwarding

### Other Risk

- Azure AD threat intelligence
- Admin confirmed user compromised
- Password spray
- Additional risk detected



## *Audit Logs*

### User Management

- New user creation
- Add/edit role, device and memberships

### Group Management

- Reset/Restore group password
- Get policies

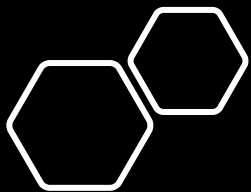
### Application Management

- Set MFA registration policy
- Update conditional access policy
- Issuing Token, OAuth2 and Auth code

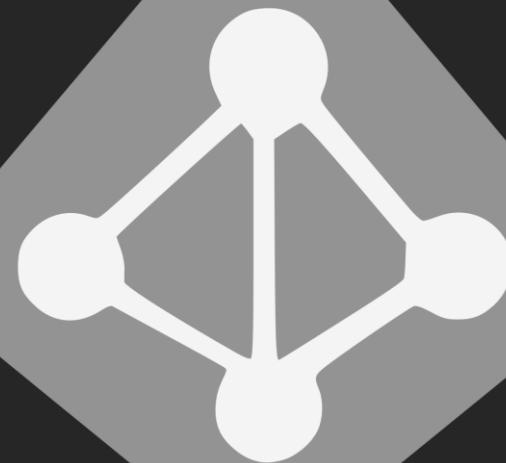
### Role Management

- Add device, add/remove user to device
- Update conditional access policy





# *Threat Hunting with “Azure AD Reports”*





# *Prerequisites*

- Understanding of your organization user behaviors, mature security and compliance policies
  - Where are my employees? My contractors? My subsidiaries? My vendors?
  - Do we have VPN technology? Proxy? Do we use cloud for applications?
  - Are users allowed to use VPN? Is it against our policy?
  - Are users allowed to bring their own devices?
  - Did we “translate” our policy to Conditional Access policy in Azure?
- Understanding of Azure Security operation to follow up on suspicious/malicious activity
  - How do I revoke session?
  - How do I prompt user to perform additional MFA?
  - How do I prompt user password reset?
- Understanding of the attack concepts
  - How SAML/OAuth/cloud-lingo-here work?
  - What about ADFS?
- Appropriate access to the Azure AD to access these logs
- SIEM is recommended for better visibility

# Attacks That Can Be Detected via Azure AD Report

## Password Spray

- Legacy Application
- Single Factor Account

## Brute Force

- Password Brute Force (Single Factor)
- MFA Brute Force (User Approving MFA)
- Password + MFA Brute Force

## Recon

- Username Recon

## Compromised Account (Phished, Leaked, Breached, Reused)

- Compromised Password (Credential Stuffing)
- Compromised MFA (+ User Approving MFA)

## Unusual/Suspicious Signals

AKA investigate when these appeared

- Single Factor in MFA environment
- Malicious IP Address (from MISP or TI sources)
  - Sibling IPs
- Suspicious ASN
  - TOR Exit Node
  - VPN, VPS
  - Datacenter, Hosting
- Suspicious Application
  - Legacy Application
- Suspicious User Agent
  - Scanner User Agent
  - Legacy User Agent
    - "cbainprod"
    - "bav2ropc"
    - "cabprod"
    - more in appendix
- Unusual User Agent



# Attack, Detection and Response

Attack	Detection		Response
Password Spray <ul style="list-style-type: none"> <li>• Legacy Application</li> <li>• Single Factor Account</li> </ul>	<ul style="list-style-type: none"> <li>• High number of failed Single Factor, some success possible</li> <li>• Unusual IPs</li> <li>• Multi Users</li> <li>• Legacy/Single Factor Application used (ex. BAV2ROPC)</li> </ul>	Error Codes 50,053 - Account is locked because user try to sign in too many times with failed creds 50,126 - Invalid username or password 53,003 - Access has been blocked due to conditional access policy 50,057 - User account is disabled. The account has been disabled by an administrator. 0 - Success	<ul style="list-style-type: none"> <li>• Collect the attacker IP address</li> <li>• Look for Error Code 0 (Success) from all the involved IP address, check if other users are compromised</li> <li>• If any success in Single Factor, it means Password compromised               <ul style="list-style-type: none"> <li>• Review Azure AD Audit logs and 0365 logs on the IP address for each compromised accounts</li> <li>• Revoke session, reset password, enable MFA when possible</li> </ul> </li> <li>• If any success in Multi Factor, it means Password + MFA compromised               <ul style="list-style-type: none"> <li>• Review Azure AD Audit logs and 0365 logs on the IP address for each compromised accounts</li> <li>• Attacker may reset user password or add new MFA device</li> <li>• Revoke session, reset password, undo all the changes made, restore MFA</li> </ul> </li> <li>• Depending the company policy, block or report the attacker IP address</li> </ul>
Password Brute Force	<ul style="list-style-type: none"> <li>• High number of failed Single Factor, some success possible</li> <li>• Unusual IPs</li> <li>• Unusual User Agent or Device</li> <li>• Single or Multi Users</li> </ul>		
MFA Brute Force <ul style="list-style-type: none"> <li>• Attacker spamming user with MFA requests until user accepts the MFA request</li> </ul>	<ul style="list-style-type: none"> <li>• Successful Single Factor</li> <li>• High number of Failed MFA, some success possible</li> <li>• Usually using Mobile App Notifications or Phone Call MFA</li> <li>• Unusual IPs, possibly Hosting, VPN or Tor</li> <li>• Possibly unusual User Agent or Device</li> <li>• Single or Multi Users</li> </ul>	Error Codes 50,076 - User did not pass the MFA challenge (non interactive). 50,074 - User did not pass the MFA challenge. 500,121 - The user didn't complete the MFA prompt. They may have decided not to authenticate, timed out while doing other work, or has an issue with their authentication setup. 50,088 - Limit on telecom MFA calls reached. Please try again in a few minutes. 500,881 - Limit on telecom MFA calls reached. Please retry with PhoneAppNotification or try again in a few minutes. 500,882 - Limit on telecom MFA calls reached. Please retry with PhoneAppCode or try again in a few minutes. 0 - Success	

# Attack, Detection and Response – Cont.

Attack	Detection	Response
Compromised Password Saved by MFA <ul style="list-style-type: none"><li>• Credential Harvesting Victim</li><li>• Credential Stuffing</li></ul>	<ul style="list-style-type: none"><li>• Successful Single Factor, BF/PS might happen earlier</li><li>• Failed MFA</li><li>• Unusual IPs</li><li>• IP possibly Hosting, VPN or Tor</li><li>• Unusual User Agent or Device</li><li>• Single or Multi Users</li></ul>	<ul style="list-style-type: none"><li>• Collect the attacker IP address</li><li>• Look for Error Code 0 (Success) from all the involved IP address, check if other users are compromised</li><li>• If any success in Single Factor, it means Password compromised<ul style="list-style-type: none"><li>• Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts</li><li>• Revoke session, reset password, enable MFA when possible</li></ul></li><li>• If any success in Multi Factor, it means Password + MFA compromised<ul style="list-style-type: none"><li>• Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts</li><li>• Attacker may reset user password or add new MFA device</li><li>• Revoke session, reset password, undo all the changes made, restore MFA</li></ul></li><li>• Depending the company policy, block or report the attacker IP address</li><li>• Add information to intel platform (such as MISP)</li></ul>
Compromised Password Compromised MFA <ul style="list-style-type: none"><li>• User Accepting MFA initiated by attacker</li></ul>	<ul style="list-style-type: none"><li>• Successful Single Factor, BF/PS might happen earlier</li><li>• High number of Failed MFA, some success possible</li><li>• Usually using Mobile App Notifications or Phone Call MFA</li><li>• Unusual IPs</li><li>• IP possibly Hosting, VPN or Tor</li><li>• Unusual User Agent or Device</li><li>• Single or Multi Users</li></ul>	
Username Recon	<ul style="list-style-type: none"><li>• High number of failed Single Factor, some success possible</li><li>• Unusual IPs</li><li>• Unusual User Agent or Device</li><li>• Single or Multi Users</li><li>• Error code - 50,126 - Invalid username or password</li></ul>	

## *Threat Hunting at Scale*

When you are a large company or multi-national company, Threat Hunting can be hard!

(Based on experience) False Positive could occurs on every Azure AD Risk Event Types, such as:

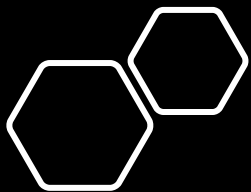
- Atypical travel, Impossible travel, New country
  - Business Travel
  - Vacation
  - External consultant on VPN
- Malicious IP address, Malware linked IP address
  - Stale Threat Intel
  - Hosting/Datacenter IP Address
- Anonymous IP address, Activity from anonymous IP address
  - User using VPN for privacy
- Suspicious browser, Unfamiliar sign-in properties
  - User using VPN for privacy

Start from the Risky Users first (aka Risk State is atRisk), to reduce the amount of data to work with

## *Reducing False Positives*

- List of Known ASN
  - Telecom company
  - Vendor
  - Consultant/Contractor
- List of Known VPN and TOR User
- List of Known Country or City
  - External User
- List of Known User with Legacy Application
- List of Known User with Single Factor Authentication
- List of Approved Application
- List of Approved Device Type
- List of Approved User Agent
- Comparing a user behavior with their past behavior via Azure Sign-ins log





*AzuLa*





"This tool is still in development  
and will be released as POC.  
Modifications required for  
operational use."



# Disclaimer

*Azula, when almost is not good enough*

Attack, Detection and Response



Threat Hunting at Scale



Reducing False Positives



The Threat Hunting process above is great but still take lot of time to do (based on experience)  
It is almost perfect.....

# Azula Details

## Azure (AD) Unified Lightweight Automated (AZULA)

Python based automation, with some data analytics and historical reference systems.

Rely mainly on Sign-Ins and Risky Sign-Ins Reports, Audit logs will be used for investigation.

5 main components:

### OSINT Enrichment

- Check if it is VPN, Tor, or Datacenter
- Check hostname
  - Check Geo Information
  - Check ASN

python

### Logic Engine

Add as per your requirement  
Example:

- North American Contractor
- If VPN, in North America, and account start with CONTR\*

Recent Scanner Success Login

- If IP is in Scanner IP DB, and Error code is 0

python

### Reference DB Known

Used to reduce FPs,  
Known Signals

Example:

- Known Benign ASN
  - Vendor ASN
- Known VPN/Tor

.txt file + inline

### Reference DB Bad

Used for  
Unusual/Suspicious  
Signals

- Bad User Agent
- Suspicious ASN
- Legacy User Agent
- Legacy Application

.txt file + inline

### Reports I/O Engine

Process the data  
received from Azure AD  
Reports

Add "Comment" where the  
verdict will be written  
into

.csv files

## *Azula, Step by Step*

Prepare CSV with the right information



Transform Data from CSV to Pandas



Enrich IP address information



Apply logic, compare with Reference DB (Bad and Known)



Add the comments and enrichment



Analyst/Threat Hunter review and complete the result

# Azula Screenshots

```
##### START OF LOGIC #####

# User Agent is a phone
is_phone = ("iphone".."android")
# User Agent is suspicious, commonly used in attack
is_sus = ("cbainprod".."bav2rope", "cabprod", "microsoft office", "macoutlook", "apple-ipad", "appleexchangelwebmail", "outlook", "mowahost"..)
is_phoneapp = ("microsoft teams", "workday", "outlook mobile", "employee wellness program")

if any(ua in UserAgent for ua in is_phone..):
    df.at[row, 'Comments'] = df.at[row, 'Comments'] + "From phone. "
    for app in is_phoneapp:
        if app in AppAccessed:
            comment = ("From phone accessing " + app + " application, often triggering alert. Check Error Code. ")
            df.at[row, 'Comments'] = comment

if any(ua in UserAgent for ua in is_sus):
    df.at[row, 'Comments'] = "[SUSPICIOUS] Suspicious User Agent used, possibly an attack. " + df.at[row, 'Comments']

# Known Benign Telco and ISP Company
for kg in known_org:
    kg = kg.lower()
    if kg in IPInfo and "(ca)" in IPInfo:
        df.at[row, 'Comments'] = "Benign Canadian ISP provider, observed regularly by local employees. " + df.at[row, 'Comments']
    elif kg in IPInfo and "(in)" in IPInfo:
        df.at[row, 'Comments'] = "Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. " + df.at[row, 'Comments']
    elif kg in IPInfo and "(us)" in IPInfo:
        df.at[row, 'Comments'] = "Benign US ISP provider, observed regularly used by American employees. " + df.at[row, 'Comments']
```

*Part of Azula's Logic Engine*

## Azula Screenshots

```
module_pandas.py × enriched_ip.txt × core_azula.py × core_ipenrich.py × modue_merror.py × module_ipinfo.py × module_logic.py ×
1 107.152.24.197 - N/A - San Jose (US) | AS33011 Box.com | No Hostname Found
2 52.173.134.115 - Datacenter - Des Moines (US) | AS8075 Microsoft Corporation | No Hostname Found
3 162.125.7.20 - N/A - San Jose (US) | AS19679 Dropbox, Inc. | No Hostname Found
4 162.125.6.20 - N/A - Washington (US) | AS19679 Dropbox, Inc. | No Hostname Found
5 162.125.8.20 - N/A - Dallas (US) | AS19679 Dropbox, Inc. | No Hostname Found
6 72.21.91.29 - N/A - Ashburn (US) | AS15133 MCI Communications Services, Inc. d/b/a Verizon Business | No Hostname
7 64.62.208.12 - Datacenter - Fremont (US) | AS6939 Hurricane Electric LLC | No Hostname Found
8 99.84.214.93 - Datacenter - Washington (US) | AS16509 Amazon.com, Inc. | server-99-84-214-93.iad79.r.cloudfront.n
9 23.67.200.172 - Datacenter - Miami (US) | AS16625 Akamai Technologies, Inc. | a23-67-200-172.deploy.static.akamai
10 151.139.128.14 - Datacenter - Dallas (US) | AS20446 Highwinds Network Group, Inc. | No Hostname Found
11 52.252.20.242 - Datacenter - Boydton (US) | AS8075 Microsoft Corporation | No Hostname Found
12 23.54.187.27 - Datacenter - New York City (US) | AS16625 Akamai Technologies, Inc. | a23-54-187-27.deploy.static.
13 204.141.43.95 - Datacenter - Corvallis (US) | AS2639 ZOH0 | No Hostname Found
14 13.33.165.78 - Datacenter - Fostoria (US) | AS16509 Amazon.com, Inc. | server-13-33-165-78.yto50.r.cloudfront.net
15 99.84.214.59 - Datacenter - Washington (US) | AS16509 Amazon.com, Inc. | server-99-84-214-59.iad79.r.cloudfront.n
```

IP Reference DB

# Azula Screenshots

	A	B	C	D	E	F	G	H
1	User Name	IP Address	User Agent	App Accessed	Error Code	Failure Reason	Risk Reason	Count
2	jean_d@companya.com	154.21.252.77	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	530021	Other	missing	3
3	jean_d@companya.com	154.21.252.77	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50074	User did not pass the MFA challenge.	unfamiliarFeature	2
4	jean_d@companya.com	154.21.252.77	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	missing	1
5	jean_d@companya.com	154.21.252.77	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50127	User needs to install a broker app to gain access	missing	1
6	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50074	User did not pass the MFA challenge.	unfamiliarFeature	1
7	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
8	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	500121	Other	missing	1
9	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
10	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
11	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	501291	Other	missing	2
12	contr_rahul01@companya.com	157.48.155.22	Mozilla/5.0 (Linux; Android 11; MI A3 Build/RKQ1.20) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	501291	Other	missing	2
13	contr_rahul01@companya.com	157.48.155.22	Mozilla/5.0 (Linux; Android 11; MI A3 Build/RKQ1.20) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
14	carol_p@company2.com	199.167.24.147	Apple-iPhone13C2/1806.72	Office 365 Exchange Online	0	missing	missing	1
15	carol_p@company2.com	199.167.24.147	Apple-iPhone13C2/1806.72	Office 365 Exchange Online	0	missing	unfamiliarFeature	1
16	jean_d@companya.com	207.134.39.101	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	0	missing	missing	1
17	jean_d@companya.com	207.134.39.101	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	0	missing	unfamiliarFeature	1
18	contr_chen02@companya.com	104.200.138.69	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	missing	missing	1
19	contr_chen02@companya.com	104.200.138.69	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	missing	missing	1
20	ramos_admin@company2.com	204.239.251.5	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	0	missing	missing	1
21	store_20Avenue@bestretail.com	23.106.160.123	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	5
22	store_20Avenue@bestretail.com	23.106.160.123	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10
23	store_20Avenue@bestretail.com	23.106.160.123	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	5
24	store_20Avenue@bestretail.com	23.106.160.123	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10
25	store_20Avenue@bestretail.com	23.106.160.123	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10

Sample Input File

	A	B	C	D	E	F	G	H	I	J	K
1	User Name	IP Address	IPInfo	Spur.us	Comments	User Agent	App Accessed	Error Code	Failure Reason	Risk Reason	Count
2	jean_d@companya.com	154.21.252.77	QuÃ©bec (CA) - AS26932 BRAVO TELECOM - No Hostname Found	BRAVO-TELECOM Datacenter	From phone. Smaller ISP OK	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	530021	Other	missing	3
3	jean_d@companya.com	154.21.252.77	QuÃ©bec (CA) - AS26932 BRAVO TELECOM - No Hostname Found	BRAVO-TELECOM Datacenter	From phone. Smaller ISP OK	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50074	User did not pass the MFA challenge.	unfamiliarFeature	2
4	jean_d@companya.com	154.21.252.77	QuÃ©bec (CA) - AS26932 BRAVO TELECOM - No Hostname Found	BRAVO-TELECOM Datacenter	From phone. Smaller ISP OK	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	missing	1
5	jean_d@companya.com	154.21.252.77	QuÃ©bec (CA) - AS26932 BRAVO TELECOM - No Hostname Found	BRAVO-TELECOM Datacenter	From phone. Smaller ISP OK	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50127	User needs to install a broker app to gain access	missing	1
6	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No I	ROGERS-COMMUNICATIONS Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone accessing microsoft teams application, often tri	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
7	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No I	ROGERS-COMMUNICATIONS Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone accessing microsoft teams application, often tri	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
8	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No I	ROGERS-COMMUNICATIONS Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone accessing microsoft teams application, often tri	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	500121	Other	missing	1
9	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applica	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
10	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applica	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
11	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemidia Services - te Bharti Airtel Ltd., Telemidia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applica	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	501291	Other	missing	2
12	contr_rahul01@companya.com	157.48.155.22	Hyderabad (IN) - ASS5836 Reliance Jio Infocomm Limited - No Host/N/A	Hyderabad (IN) - ASS5836 Reliance Jio Infocomm Limited - No Host/N/A	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applica	Mozilla/5.0 (Linux; Android 11; MI A3 Build/RKQ1.20) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	501291	Other	missing	2
13	contr_rahul01@companya.com	157.48.155.22	Hyderabad (IN) - ASS5836 Reliance Jio Infocomm Limited - No Host/N/A	Hyderabad (IN) - ASS5836 Reliance Jio Infocomm Limited - No Host/N/A	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applica	Mozilla/5.0 (Linux; Android 11; MI A3 Build/RKQ1.20) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	50097	Device Authentication Required - DeviceId	unfamiliarFeature	1
14	carol_p@company2.com	199.167.24.147	Calgary (CA) - ASS4182 Axia Connect Limited - No Hostname Found	AXIA-CONNECT Datacenter	From phone.	Apple-iPhone13C2/1806.72	Office 365 Exchange Online	0	missing	missing	1
15	carol_p@company2.com	199.167.24.147	Calgary (CA) - ASS4182 Axia Connect Limited - No Hostname Found	AXIA-CONNECT Datacenter	From phone.	Apple-iPhone13C2/1806.72	Office 365 Exchange Online	0	missing	unfamiliarFeature	1
16	jean_d@companya.com	207.134.39.101	Sainte-Anne-des-Monts (CA) - ASS82 TELUS Communications Inc. - TELUS Communications Datacenter	TELUS Communications Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone.	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	0	missing	missing	1
17	jean_d@companya.com	207.134.39.101	Sainte-Anne-des-Monts (CA) - ASS82 TELUS Communications Inc. - TELUS Communications Datacenter	TELUS Communications Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone.	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/89.0.4389.105 Mobile Safari/537.36	Office 365 Exchange Online	0	missing	unfamiliarFeature	1
18	contr_chen02@companya.com	104.200.138.69	Toronto (CA) - AS46562 Performix LLC - No Hostname Found	PERFORMIX Datacenter   Hotspot VPN	VPN, historical user	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	missing	missing	1
19	contr_chen02@companya.com	104.200.138.69	Toronto (CA) - AS46562 Performix LLC - No Hostname Found	PERFORMIX Datacenter   Hotspot VPN	VPN, historical user	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	missing	missing	1
20	ramos_admin@company2.com	204.239.251.5	Vancouver (CA) - AS48088 Vancouver International Airport Authority VYRAA Datacenter	VYRAA Datacenter	From phone. Possibly from Airport WiFi	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac OS X) AppleWebKit/605.1.15 (KHTML, like Gecko) Version/14.0 Mobile/15E148 Safari/604.1	Office 365 Exchange Online	0	missing	missing	1
21	store_20Avenue@bestretail.com	23.106.160.123	San Francisco (US) - AS7203 Leaseweb USA, Inc. - No Hostname Fo	LEASEWEB-USA-SFO-12 Datacenter	[SUSPICIOUS] Suspicious User Agent used, possibly an attack. All Failed	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	5
22	store_20Avenue@bestretail.com	23.106.160.123	San Francisco (US) - AS7203 Leaseweb USA, Inc. - No Hostname Fo	LEASEWEB-USA-SFO-12 Datacenter	[SUSPICIOUS] Suspicious User Agent used, possibly an attack. All Failed	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10
23	store_20Avenue@bestretail.com	23.106.160.123	San Francisco (US) - AS7203 Leaseweb USA, Inc. - No Hostname Fo	LEASEWEB-USA-SFO-12 Datacenter	[SUSPICIOUS] Suspicious User Agent used, possibly an attack. All Failed	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	5
24	store_20Avenue@bestretail.com	23.106.160.123	San Francisco (US) - AS7203 Leaseweb USA, Inc. - No Hostname Fo	LEASEWEB-USA-SFO-12 Datacenter	[SUSPICIOUS] Suspicious User Agent used, possibly an attack. All Failed	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10
25	store_20Avenue@bestretail.com	23.106.160.123	San Francisco (US) - AS7203 Leaseweb USA, Inc. - No Hostname Fo	LEASEWEB-USA-SFO-12 Datacenter	[SUSPICIOUS] Suspicious User Agent used, possibly an attack. All Failed	BAV2ROPC	Office 365 Exchange Online	50053	Sign-in was blocked because it came from	missing	10

Sample Output File



# *Demonstration*



PySINT

File Edit View Navigato Code Refactor Run Tools VCS Window Help

azula.py

Project

azula.bat

azula.py

Run: azula

azula

Run

Structure

Favorites

AutoSave OFF

[DEV] AzureAD Risky Users Reporting Visual.csv

Mangatas Tondang MT

File Home Insert Page Layout Formulas Data Review View Help

Paste

Clipboard

Calibri 11

B I U

Font

General

Alignment

Conditional Formatting

Format as Table

Cell Styles

Styles

Insert

Delete

Format

Cells

Σ

Editing

Analyze Data

Analysis

G9

\_\_missing\_\_

	A	B	C	D	E	F	G	H	I	J
1	User Name	IP Address	User Agent	App Accessed	Error Code	Failure Reason	Risk Reason	Count		
2	jeun_d@companyu.com	154.21.252.77	Mozilla/5.0 (iPhone Office 365 Exch		530021 Other		__missing__	3		
3	jeun_d@companyu.com	154.21.252.77	Mozilla/5.0 (iPhone Office 365 Exch		50074 User did not pass the	unfamiliarFeatu		2		
4	jeun_d@companyu.com	154.21.252.77	Mozilla/5.0 (iPhone Outlook Mobile		50097 Device Authentication	__missing__		1		
5	jeun_d@companyu.com	154.21.252.77	Mozilla/5.0 (iPhone Outlook Mobile		50127 User needs to install	__missing__		1		
6	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone Microsoft Teams		50074 User did not pass the	unfamiliarFeatu		1		
7	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone Microsoft Teams		50097 Device Authentication	unfamiliarFeatu		1		
8	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone Microsoft Teams		500121 Other	__missing__		1		
9	juke_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; # Microsoft Teams		50097 Device Authentication	__missing__		1		
10	juke_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; # Microsoft Teams		50097 Device Authentication	unfamiliarFeatu		1		
11	juke_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; # Microsoft Teams		501291 Other	__missing__		2		
12	contr_rahul01@companyu.com	157.48.155.22	Mozilla/5.0 (Linux; # Microsoft Teams		501291 Other	__missing__		2		
13	contr_rahul01@companyu.com	157.48.155.22	Mozilla/5.0 (Linux; # Microsoft Teams		50097 Device Authentication	__missing__		1		
14	curol_p@company2.com	199.167.24.147	Apple-iPhone13C2/ Office 365 Exch		0 __missing__	__missing__		1		
15	curol_p@company2.com	199.167.24.147	Apple-iPhone13C2/ Office 365 Exch		0 __missing__	unfamiliarFeatu		1		
16	jeun_d@companyu.com	207.134.39.101	Mozilla/5.0 (Linux; # OneDrive		0 __missing__	__missing__		1		
17	jeun_d@companyu.com	207.134.39.101	Mozilla/5.0 (Linux; # OneDrive		0 __missing__	unfamiliarFeatu		1		
18	contrr_chen02@companyu.com	104.200.138.69	Microsoft ASP.NET Citrix Cloud		0 __missing__	__missing__		1		
19	contrr_chen02@companyu.com	104.200.138.69	Microsoft ASP.NET Citrix Cloud		0 __missing__	__missing__		1		
20	rumos_admin@company2.com	204.239.251.5	Mozilla/5.0 (iPhone Microsoft Auth		0 __missing__	__missing__		1		
21	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		5		
22	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		10		
23	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		5		
24	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		10		
25	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		10		
26	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC Office 365 Exch		50053 Sign-in was blocked b	__missing__		100		
27										
28										
29										

(DEV) AzureAD Risky Users Repor

Ready

Display Settings

100%

Run

TODO

Problems

Terminal

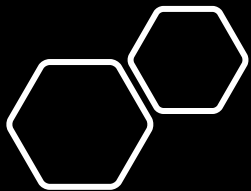
Python Console

PyCharm 2020.3.5 available // Update... (today 8:59 AM)

Event Log

1:1 Python 3.9 (PySINT)

11:38 PM



## *Closing Remarks*

## *Blind Spots*

- Azure Risk Model can miss some of the attacks, always a good idea to review all Sign-ins logs
- Threat Intel information can be misleading sometimes, even from different sources
- Creating a known list based on Signals might create blind spots, thread carefully

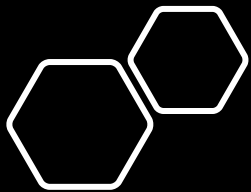
## *Improvement Ideas*

- Correlation with Historical Data (live stream of data) using the SIEM API
- Additional Enrichment such as “Others” error code, IP Abuse DB, etc.
- Connection to HR system to pull user role in the organization
- Connection to Audit logs for possibly compromised user to find changes made after compromise
- Connection to O365 logs for possibly compromised user to find changes made after compromise
- Using proper database such as MongoDB instead of .txt file

# Thank You!



Scan for slides and POC code (soon)



# *Appendix*

## *List of Legacy/Suspicious User Agent*

- Cbainprod
- Bav2ropc
- Cabprod
- Microsoft office
- Macoutlook
- Apple-ipad
- Appleexchangewebservices
- Outlook
- Mowahost



## *List of Azure AD Audit Logs Category*

- AdministrativeUnit
- ApplicationManagement
- Authentication
- Authorization
- Contact
- Device
- DeviceConfiguration
- DirectoryManagement
- EntitlementManagement
- GroupManagement
- KerberosDomain
- KeyManagement
- Label
- Other
- PermissionGrantPolicy
- Policy
- ResourceManagement
- RoleManagement
- UserManagement

# List of Azure AD Audit Logs Event Types

- |   |  |   |
|---|--|---|
| 1. UserLoggedIn.                              | 28. Delete device.   | 55. Disable Strong Authentication.  |
| 2. UserLoginFailed.                           | 29. Restore user.  | 56. Remove registered users from device.  |
| 3. Update user.                               | 30. Enable account.  | 57. Set group license.  |
| 4. Update device.                             | 31. Hard Delete group.                                       | 58. Remove delegated permission grant.  |
| 5. Update group.                              | 32. Add service principal.                                   | 59. Finish applying group-based license to users.                                     |
| 6. Add contact.                               | 33. Device no longer managed.                                | 60. Remove app role assignment from user.   |
| 7. Add member to group.                       | 34. Delete contact.  | 61. Start applying group-based license to users.                                      |
| 8. Update StsRefreshTokenValidFrom Timestamp. | 35. Remove member from role.                                 | 62. Add a deletion-marked app role assignment grant to user as part of link removal.  |
| 9. Change user license.                       | 36. Set Company Information.                                 | 63. Add policy to service principal.  |
| 10. Add group.                                | 37. Add service principal credentials.                       | 64. Set user manager.   |
| 11. Add user.                                 | 38. Update application.                                      | 65. Add owner to service principal.   |
| 12. Change user password.                     | 39. Update contact.  | 66. Remove service principal.   |
| 13. Add owner to group.                       | 40. Enable Strong Authentication.                            | 67. Add a deletion-marked app role assignment grant to group as part of link removal. |
| 14. Add device.                               | 41. Update policy.   | 68. Add eligible member to role.  |
| 15. Add registered owner to device.           | 42. Hard Delete user.  | 69. Add owner to policy.  |
| 16. Add registered users to device.           | 43. Reset user password.                                     | 70. Hard Delete application.  |
| 17. Remove owner from group.                  | 44. Create application password for user.                    | 71. Remove app role assignment from group.  |
| 18. Remove member from group.                 | 45. Remove user strong authentication phone app detail.      | 72. Revoke consent.   |
| 19. Device no longer compliant.               | 46. Remove service principal credentials.                    | 73. Trigger group license recalculation.  |
| 20. Delete group.                             | 47. Update application – Certificates and secrets management | 74. Update external secrets   |
| 21. Disable account.                          | 48. Add app role assignment to service principal.            | 75. Add partner to company.   |
| 22. Add member to role.                       | 49. Add application.   | 76. Set Partnership   |
| 23. Add delegated permission grant.           | 50. Add app role assignment to group.                        | 77. Delete application.   |
| 24. Update service principal.                 | 51. Add owner to application.                                | 78. Update company settings   |
| 25. Add app role assignment grant to user.    | 52. Remove registered owner from device.                     | 79. Update domain.  |
| 26. Consent to application.                   | 53. Add policy.  |   |
| 27. Delete user.                              | 54. Delete application password for user.                    |   |

*\*Ranked based on commonly observed event types*

*\*List might miss rarely observed event types, more can be found [here](#)*