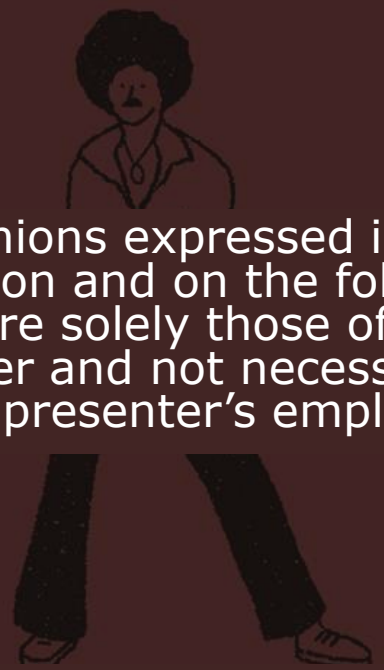
Knocking on ~~Heavens~~ Clouds Door

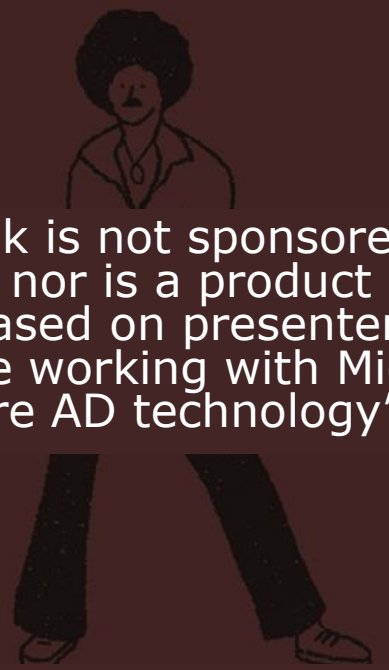
Threat Hunting in Azure AD using Azula

@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

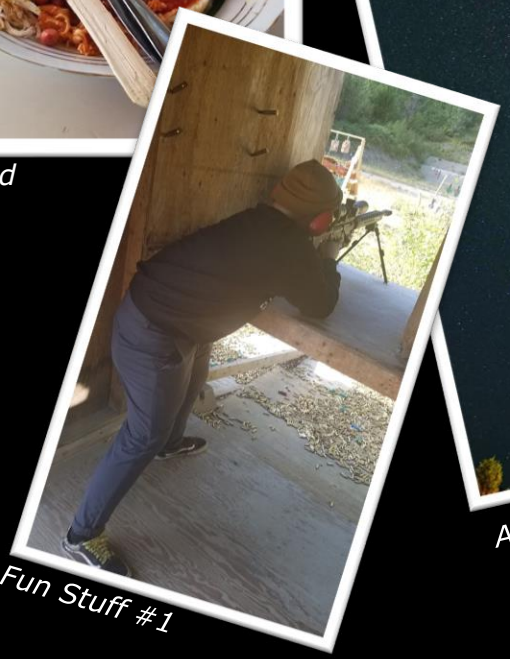
Communities:
- The DFIR Report contributor
- OSCD contributor
- CDEF.ID member
- Sheridan College’s ISSessions member
- Presented in numerous international conferences

Who am I?

Good Food

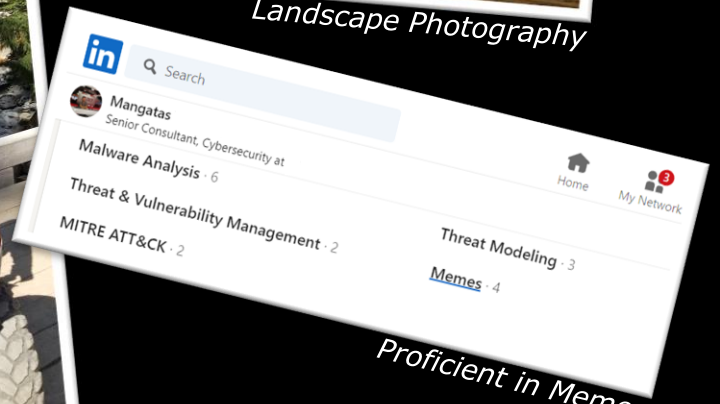
Astrophotography

Landscape Photography



Fun Stuff #1

Fun Stuff #2



Proficient in Memes

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

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® Navi

Version Permalink

layout: side | show sub-techniques | hide sub-techniques | help

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

VS

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

PS: THIS OFC OVERSIMPLIFICATION

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

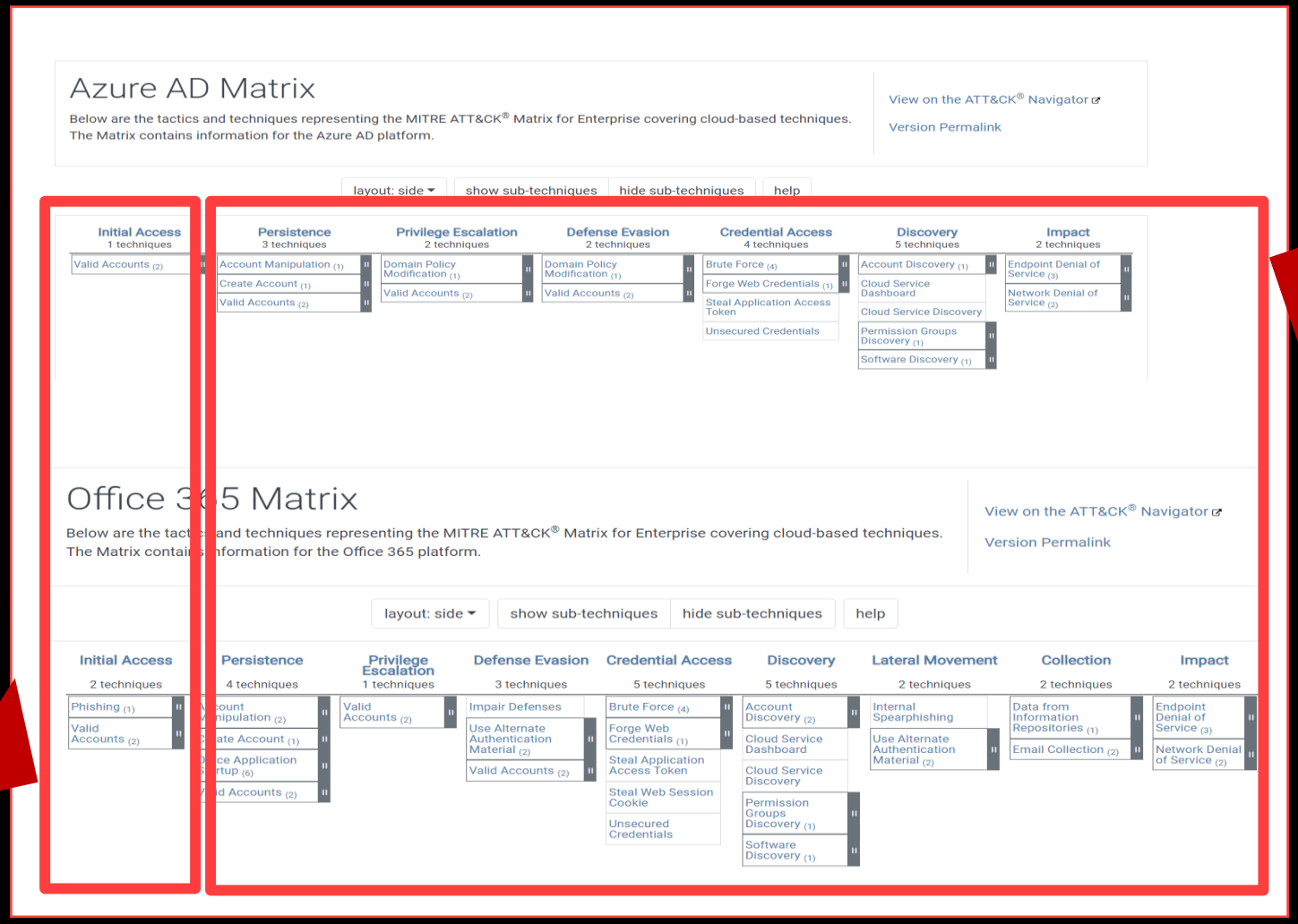
VP

- 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



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

Strong multi-factor authentication safeguards user credentials

Context-based adaptive policies grant, limit or block access

Real-time machine learning guards against use of leaked or stolen credentials and blocks suspicious login attempts

Identity governance controls access to apps and data for all users, including privileged users, across hybrid environments

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

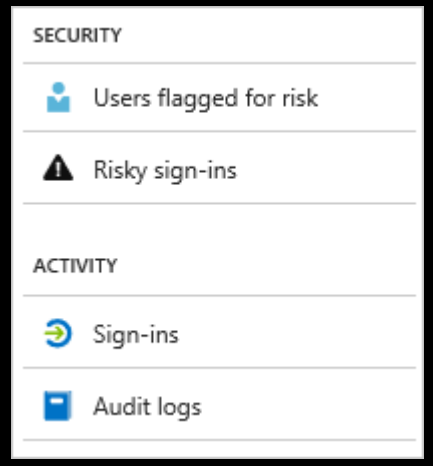
Introduction to “Azure AD Reports”

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

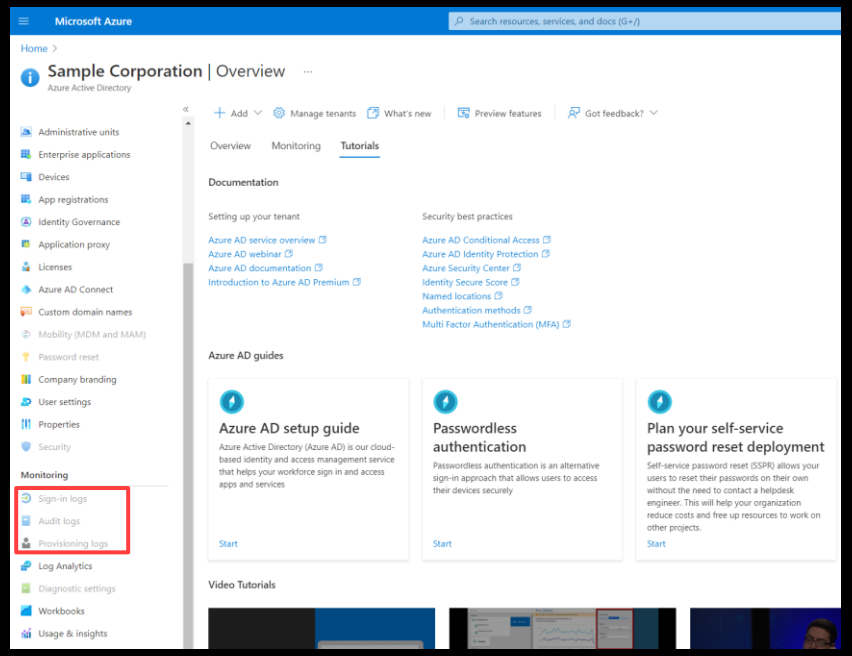
- All report types interconnected and can help give complete story!
  - Even with additional logs from other sources (e.g., O365 Logs)



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

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

Audit Logs

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

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.)

User Information

properties.userDisplayName	Tas
properties.userId	12312312-46c1-4f10-bd7b-11111111111
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

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.

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"
},
```


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

properties.authenticationProcessingDetails


```
{
  "key": "Domain Hint Present",
  "value": "True"
},
{
  "key": "IsCAEToken",
  "value": "False"
}
```


properties.authenticationRequirement: multiFactorAuthentication

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

<table>
<tr><th>Attack</th><th colspan="2">Detection</th><th>Response</th></tr>
<tr><td>Password Spray
• Legacy Application
• Single Factor Account</td><td>• High number of failed Single Factor, some success possible
• Unusual IPs
• Multi Users
• Legacy/Single Factir Application used (ex. BAV2ROPC)</td><td rowspan="2">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</td><td rowspan="3">• Collect the attacker IP address
• Look for Error Code 0 (Success) from all the involved IP address, check if other users are compromised
• If any success in Single Factor, it means Password compromised
  • Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts
  • Revoke session, reset password, enable MFA when possible
• If any success in Multi Factor, it means Password + MFA compromised
  • Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts
  • Attacker may reset user password or add new MFA device
  • Revoke session, reset password, undo all the changes made, restore MFA
• Depending the company policy, block or report the attacker IP address</td></tr>
<tr><td>Password Brute Force</td><td>• High number of failed Single Factor, some success possible
• Unusual IPs
• Unusual User Agent or Device
• Single or Multi Users</td></tr>
<tr><td>MFA Brute Force
• Attacker spamming user with MFA requests until user accepts the MFA request</td><td>• Successful Single Factor
• High number of Failed MFA, some success possible
• Usually using Mobile App Notifications or Phone Call MFA
• Unusual IPs, possibly Hosting, VPN or Tor
• Possibly unusual User Agent or Device
• Single or Multi Users</td><td>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</td></tr>
</table>

Attack, Detection and Response – Cont.

<table>
<tr><th>Attack</th><th>Detection</th><th>Response</th></tr>
<tr><td>Compromised Password
Saved by MFA
• Credential Harvesting Victim
• Credential Stuffing</td><td>• Successful Single Factor, BF/PS might happen earlier
• Failed MFA
• Unusual IPs
• IP possibly Hosting, VPN or Tor
• Unusual User Agent or Device
• Single or Multi Users</td><td rowspan="3">• Collect the attacker IP address
• Look for Error Code 0 (Success) from all the involved IP address, check if other users are compromised
• If any success in Single Factor, it means Password compromised
  • Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts
  • Revoke session, reset password, enable MFA when possible
• If any success in Multi Factor, it means Password + MFA compromised
  • Review Azure AD Audit logs and O365 logs on the IP address for each compromised accounts
  • Attacker may reset user password or add new MFA device
  • Revoke session, reset password, undo all the changes made, restore MFA
• Depending the company policy, block or report the attacker IP address
• Add information to intel platform (such as MISP)</td></tr>
<tr><td>Compromised Password
Compromised MFA
• User Accepting MFA initiated by attacker</td><td>• Successful Single Factor, BF/PS might happen earlier
• High number of Failed MFA, some success possible
• Usually using Mobile App Notifications or Phone Call MFA
• Unusual IPs
• IP possibly Hosting, VPN or Tor
• Unusual User Agent or Device
• Single or Multi Users</td></tr>
<tr><td>Username Recon</td><td>• High number of failed Single Factor, some success possible
• Unusual IPs
• Unusual User Agent or Device
• Single or Multi Users
• Error code - 50,126 - Invalid username or password</td></tr>
</table>

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","bav2ropc", "cabprod", "microsoft office", "macoutlook", "apple-ipad", "appleexchangewebservices", "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_mserror.py | module_ipinfo.py | module_logic.py

```
107.152.24.197 - N/A - San Jose (US) | AS33011 Box.com | No Hostname Found
52.173.134.115 - Datacenter - Des Moines (US) | AS8075 Microsoft Corporation | No Hostname Found
162.125.7.20 - N/A - San Jose (US) | AS19679 Dropbox, Inc. | No Hostname Found
162.125.6.20 - N/A - Washington (US) | AS19679 Dropbox, Inc. | No Hostname Found
162.125.8.20 - N/A - Dallas (US) | AS19679 Dropbox, Inc. | No Hostname Found
72.21.91.29 - N/A - Ashburn (US) | AS15133 MCI Communications Services, Inc. d/b/a Verizon Business | No Hostname
64.62.208.12 - Datacenter - Fremont (US) | AS6939 Hurricane Electric LLC | No Hostname Found
99.84.214.93 - Datacenter - Washington (US) | AS16509 Amazon.com, Inc. | server-99-84-214-93.iad79.r.cloudfront.n
23.67.200.172 - Datacenter - Miami (US) | AS16625 Akamai Technologies, Inc. | a23-67-200-172.deploy.static.akamai
151.139.128.14 - Datacenter - Dallas (US) | AS20446 Highwinds Network Group, Inc. | No Hostname Found
52.252.20.242 - Datacenter - Boydton (US) | AS8075 Microsoft Corporation | No Hostname Found
23.54.187.27 - Datacenter - New York City (US) | AS16625 Akamai Technologies, Inc. | a23-54-187-27.deploy.static.
204.141.43.95 - Datacenter - Corvallis (US) | AS2639 ZOHO | No Hostname Found
13.33.165.78 - Datacenter - Fostoria (US) | AS16509 Amazon.com, Inc. | server-13-33-165-78.yto50.r.cloudfront.net
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	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	Office 365 Exchange Online	50074	User did not pass the MFA challenge.	unfamiliarFeatur	2
4	jean_d@companya.com	154.21.252.77	Mozilla/5.0 (iPhone; CPU iPhone OS 14_4_2 like Mac	Outlook Mobile	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	Outlook Mobile	50127	User needs to install a broker app to gain a	__missing__	1
6	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac O	Microsoft Teams	50074	User did not pass the MFA challenge.	unfamiliarFeatur	1
7	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac O	Microsoft Teams	50097	Device Authentication Required - DeviceId	unfamiliarFeatur	1
8	user2@company1.com	72.143.236.215	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac O	Microsoft Teams	500121	Other	__missing__	1
9	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	50097	Device Authentication Required - DeviceId	__missing__	1
10	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	50097	Device Authentication Required - DeviceId	unfamiliarFeatur	1
11	jake_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	501291	Other	__missing__	2
12	contr_rahul01@companya.com	157.48.155.22	Mozilla/5.0 (Linux; Android 11; Mi A3 Build/RKQ1.20	Microsoft Teams	501291	Other	__missing__	2
13	contr_rahul01@companya.com	157.48.155.22	Mozilla/5.0 (Linux; Android 11; Mi A3 Build/RKQ1.20	Microsoft Teams	50097	Device Authentication Required - DeviceId	__missing__	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__	unfamiliarFeatur	1
16	jean_d@companya.com	207.134.39.101	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1	OneDrive	0	__missing__	__missing__	1
17	jean_d@companya.com	207.134.39.101	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1	OneDrive	0	__missing__	unfamiliarFeatur	1
18	conttr_chen02@companya.com	104.200.138.69	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	__missing__	__missing__	1
19	conttr_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 O	Microsoft Authentication Broker	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	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	Office 365 Exchange Online	50074	User did not pass the MFA challenge.	unfamiliarFeatur	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	Outlook Mobile	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	Outlook Mobile	50127	User needs to install a broker app to gain a	__missing__	1
6	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No	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 O	Microsoft Teams	50074	User did not pass the MFA challenge.	unfamiliarFeatur	1
7	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No	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 O	Microsoft Teams	50097	Device Authentication Required - DeviceId	unfamiliarFeatur	1
8	user2@company1.com	72.143.236.215	Vancouver (CA) - AS812 Rogers Communications Canada Inc. - No	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 O	Microsoft Teams	500121	Other	__missing__	1
9	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemedia Services - te	Bharti Airtel Ltd., Telemedia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applic	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	50097	Device Authentication Required - DeviceId	__missing__	1
10	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemedia Services - te	Bharti Airtel Ltd., Telemedia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applic	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	50097	Device Authentication Required - DeviceId	unfamiliarFeatur	1
11	jake_p@company2.com	122.183.51.23	Hyderabad (IN) - AS24560 Bharti Airtel Ltd., Telemedia Services - te	Bharti Airtel Ltd., Telemedia Services Datacenter	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applic	Mozilla/5.0 (Linux; Android 11; IN2011 Build/RP1A.2	Microsoft Teams	501291	Other	__missing__	2
12	contr_rahul01@companya.com	157.48.155.22	Hyderabad (IN) - AS55836 Reliance Jio Infocomm Limited - No Host	N/A	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applic	Mozilla/5.0 (Linux; Android 11; Mi A3 Build/RKQ1.20	Microsoft Teams	501291	Other	__missing__	2
13	contr_rahul01@companya.com	157.48.155.22	Hyderabad (IN) - AS55836 Reliance Jio Infocomm Limited - No Host	N/A	Benign Indian ISP provider, observed regularly used by Indian contractor/consultant. From phone accessing microsoft teams applic	Mozilla/5.0 (Linux; Android 11; Mi A3 Build/RKQ1.20	Microsoft Teams	50097	Device Authentication Required - DeviceId	__missing__	1
14	carol_p@company2.com	199.167.24.147	Calgary (CA) - AS54182 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) - AS54182 Axia Connect Limited - No Hostname Found	AXIA-CONNECT Datacenter	From phone.	Apple-iPhone13C2/1806.72	Office 365 Exchange Online	0	__missing__	unfamiliarFeatur	1
16	jean_d@companya.com	207.134.39.101	Sainte-Anne-des-Monts (CA) - AS852 TELUS Communications Inc. -	TELUS Communications Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone.	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1	OneDrive	0	__missing__	__missing__	1
17	jean_d@companya.com	207.134.39.101	Sainte-Anne-des-Monts (CA) - AS852 TELUS Communications Inc. -	TELUS Communications Datacenter	Benign Canadian ISP provider, observed regularly by local employees. From phone.	Mozilla/5.0 (Linux; Android 11; SM-G781W Build/RP1	OneDrive	0	__missing__	unfamiliarFeatur	1
18	conttr_chen02@companya.com	104.200.138.69	Toronto (CA) - AS46562 Performive LLC - No Hostname Found	PERFORMIVE Datacenter | Hotspot VPN	VPN, historical user	Microsoft ASP.NET Core OpenIdConnect handler	Citrix Cloud	0	__missing__	__missing__	1
19	conttr_chen02@companya.com	104.200.138.69	Toronto (CA) - AS46562 Performive LLC - No Hostname Found	PERFORMIVE 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) - AS40808 Vancouver International Airport Authori	YVRAA Datacenter	From phone. Possibly from Airport WIFI	Mozilla/5.0 (iPhone; CPU iPhone OS 14_6 like Mac O	Microsoft Authentication Broker	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

File Edit View Navigate Code Refactor Run Tools VCS Window Help PySINT

PySINT azula.py

Project

azula.bat

azula.py

Run: azula

AutoSave Off [DEV] AzureAD Risky Users Reporting Visual.csv Mangatas Tondang MT

File Home Insert Page Layout Formulas Data Review View Help Share Comments

Paste Clipboard Calibri 11 Font Alignment General Number Conditional Formatting Format as Table Cell Styles Styles Insert Delete Format Cells 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@compunyu.com	154.21.252.77	Mozilla/5.0 (iPhone	Office 365 Excha	530021	Other	__missing__	3		
3	jeun_d@compunyu.com	154.21.252.77	Mozilla/5.0 (iPhone	Office 365 Excha	50074	User did not pass the	unfamiliarFeatu	2		
4	jeun_d@compunyu.com	154.21.252.77	Mozilla/5.0 (iPhone	Outlook Mobile	50097	Device Authenticatior	__missing__	1		
5	jeun_d@compunyu.com	154.21.252.77	Mozilla/5.0 (iPhone	Outlook Mobile	50127	User needs to install a	__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 Authenticatior	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 Authenticatior	__missing__	1		
10	juke_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; /	Microsoft Teams	50097	Device Authenticatior	unfamiliarFeatu	1		
11	juke_p@company2.com	122.183.51.23	Mozilla/5.0 (Linux; /	Microsoft Teams	501291	Other	__missing__	2		
12	contr_rahul01@compunyu.con	157.48.155.22	Mozilla/5.0 (Linux; /	Microsoft Teams	501291	Other	__missing__	2		
13	contr_rahul01@compunyu.con	157.48.155.22	Mozilla/5.0 (Linux; /	Microsoft Teams	50097	Device Authenticatior	__missing__	1		
14	curol_p@company2.com	199.167.24.147	Apple-iPhone13C2/	Office 365 Excha	0	__missing__	__missing__	1		
15	curol_p@company2.com	199.167.24.147	Apple-iPhone13C2/	Office 365 Excha	0	__missing__	unfamiliarFeatu	1		
16	jeun_d@compunyu.com	207.134.39.101	Mozilla/5.0 (Linux; /	OneDrive	0	__missing__	__missing__	1		
17	jeun_d@compunyu.com	207.134.39.101	Mozilla/5.0 (Linux; /	OneDrive	0	__missing__	unfamiliarFeatu	1		
18	conttr_chen02@compunyu.cor	104.200.138.69	Microsoft ASP.NET	Citrix Cloud	0	__missing__	__missing__	1		
19	conttr_chen02@compunyu.cor	104.200.138.69	Microsoft ASP.NET	Citrix Cloud	0	__missing__	__missing__	1		
20	ramos_admin@company2.com	204.239.251.5	Mozilla/5.0 (iPhone	Microsoft Authe	0	__missing__	__missing__	1		
21	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	50053	Sign-in was blocked b	__missing__	5		
22	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	50053	Sign-in was blocked b	__missing__	10		
23	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	50053	Sign-in was blocked b	__missing__	5		
24	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	50053	Sign-in was blocked b	__missing__	10		
25	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	50053	Sign-in was blocked b	__missing__	10		
26	store_20Avenue@bestretail.co	23.106.160.123	BAV2ROPC	Office 365 Excha	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 Event Log

PyCharm 2020.3.5 available // Update... (today 8:59 AM) 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.
2. UserLoginFailed.
3. Update user.
4. Update device.
5. Update group.
6. Add contact.
7. Add member to group.
8. Update StsRefreshTokenValidFrom Timestamp.
9. Change user license.
10. Add group.
11. Add user.
12. Change user password.
13. Add owner to group.
14. Add device.
15. Add registered owner to device.
16. Add registered users to device.
17. Remove owner from group.
18. Remove member from group.
19. Device no longer compliant.
20. Delete group.
21. Disable account.
22. Add member to role.
23. Add delegated permission grant.
24. Update service principal.
25. Add app role assignment grant to user.
26. Consent to application.
27. Delete user.
28. Delete device.
29. Restore user.
30. Enable account.
31. Hard Delete group.
32. Add service principal.
33. Device no longer managed.
34. Delete contact.
35. Remove member from role.
36. Set Company Information.
37. Add service principal credentials.
38. Update application.
39. Update contact.
40. Enable Strong Authentication.
41. Update policy.
42. Hard Delete user.
43. Reset user password.
44. Create application password for user.
45. Remove user strong authentication phone app detail.
46. Remove service principal credentials.
47. Update application – Certificates and secrets management
48. Add app role assignment to service principal.
49. Add application.
50. Add app role assignment to group.
51. Add owner to application.
52. Remove registered owner from device.
53. Add policy.
54. Delete application password for user.
55. Disable Strong Authentication.
56. Remove registered users from device.
57. Set group license.
58. Remove delegated permission grant.
59. Finish applying group-based license to users.
60. Remove app role assignment from user.
61. Start applying group-based license to users.
62. Add a deletion-marked app role assignment grant to user as part of link removal.
63. Add policy to service principal.
64. Set user manager.
65. Add owner to service principal.
66. Remove service principal.
67. Add a deletion-marked app role assignment grant to group as part of link removal.
68. Add eligible member to role.
69. Add owner to policy.
70. Hard Delete application.
71. Remove app role assignment from group.
72. Revoke consent.
73. Trigger group license recalculation.
74. Update external secrets
75. Add partner to company.
76. Set Partnership
77. Delete application.
78. Update company settings
79. Update domain.

*Ranked based on commonly observed event types
*List might miss rarely observed event types, more can be found here