



# Top 5 Things To Know About Azure Active Directory Logs

Mark Morowczynski  
Principal Program Manager  
[@markmorow](#)

Who am I?

Identity Product Group, CXP Team

Premier Field Engineer

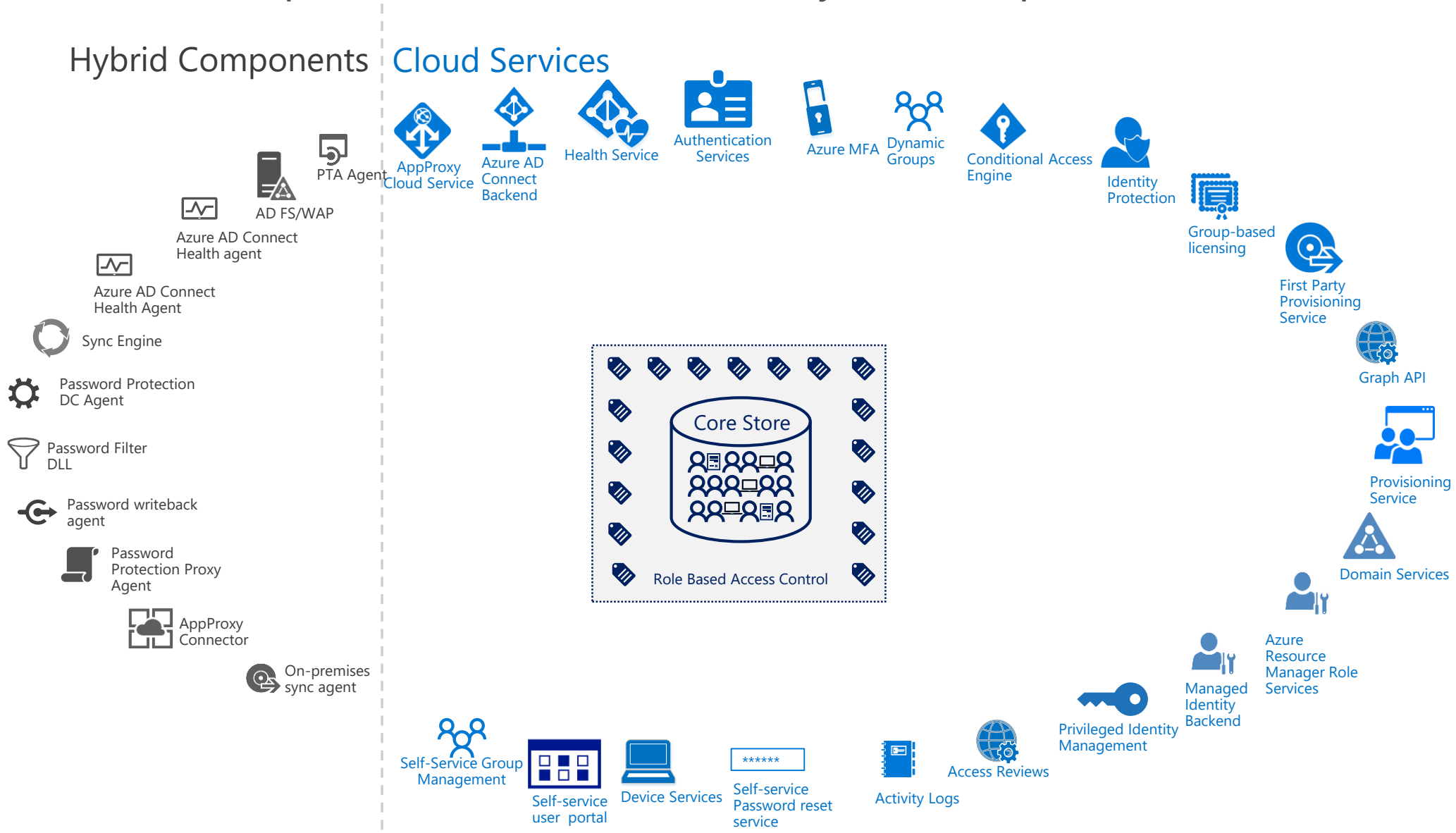
SANS STI Student

GWAPT, GCIA, GCIH, GCWN, GMOB

How Many People have Azure  
Active Directory?

# Azure AD Components

Under the hood: Multiple backend services and hybrid components



# Agenda

## What Are the Azure AD Logs

Integration with SIEM Tools

Key Events To Look For

Azure AD Logs

Sign-in logs

Interactive logins


Audit logs

Everything else

## Monitoring

---

 Sign-ins

 Audit logs

# Azure AD Sign-in Logs

Application sign-in Success/Failure

User display name and UPN

Session conditions: location, IP, Date/Time

MFA info: Required, Method, Result

Client conditions: Device ID, browser, OS

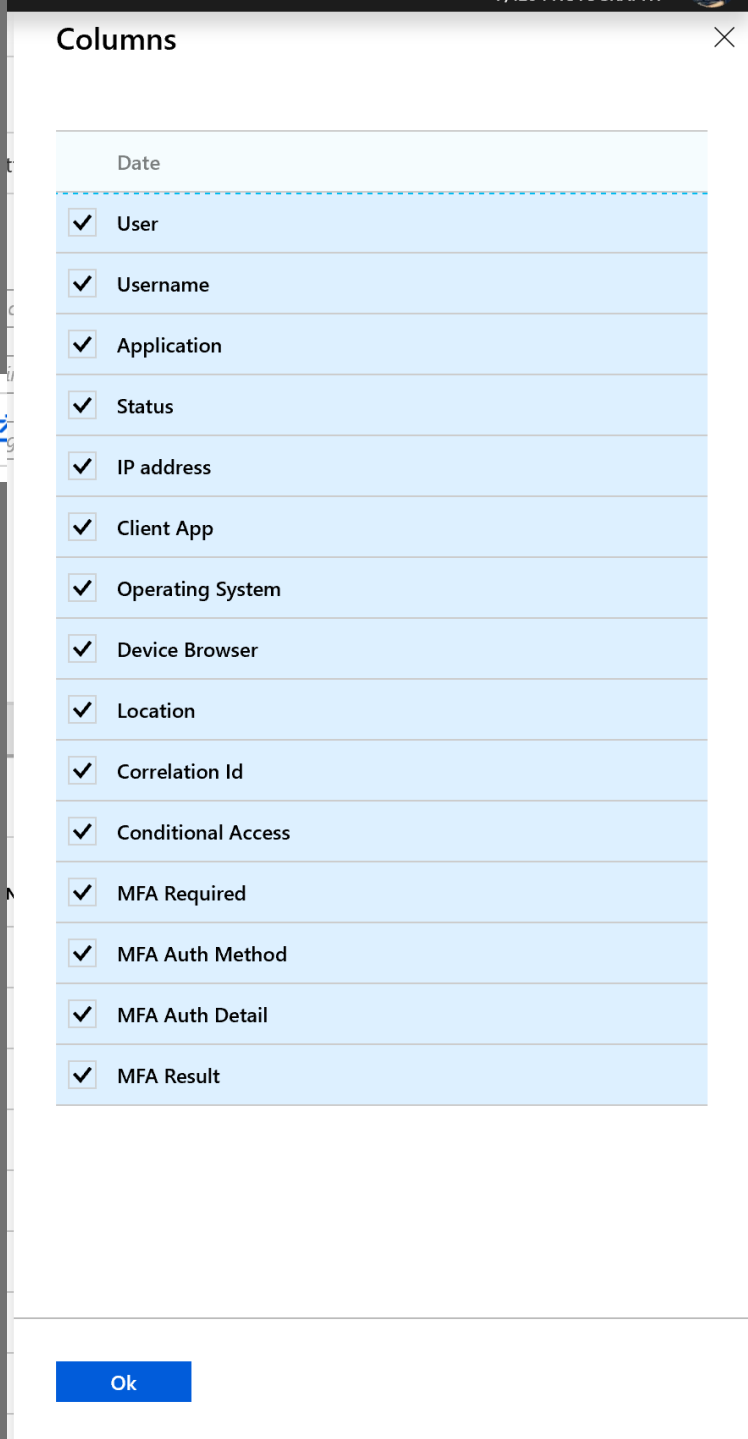
Conditional Access: Policy, Controls, Result

Correlation ID!

Latency is 5 to 10 mins



Columns Refresh Download Script



### Columns

Date
<input checked="" type="checkbox"/> User
<input checked="" type="checkbox"/> Username
<input checked="" type="checkbox"/> Application
<input checked="" type="checkbox"/> Status
<input checked="" type="checkbox"/> IP address
<input checked="" type="checkbox"/> Client App
<input checked="" type="checkbox"/> Operating System
<input checked="" type="checkbox"/> Device Browser
<input checked="" type="checkbox"/> Location
<input checked="" type="checkbox"/> Correlation Id
<input checked="" type="checkbox"/> Conditional Access
<input checked="" type="checkbox"/> MFA Required
<input checked="" type="checkbox"/> MFA Auth Method
<input checked="" type="checkbox"/> MFA Auth Detail
<input checked="" type="checkbox"/> MFA Result

Ok

# Azure AD Sign-in Logs Key Things To Know

Refresh Token Sign-ins: Only initial authentication is in the reports...today

Only successful federated logins are displayed

**Failure events are on the federated IDP**



# Azure AD Audit Logs

Actions performed that change the state of a resource, e.g.

Password Reset

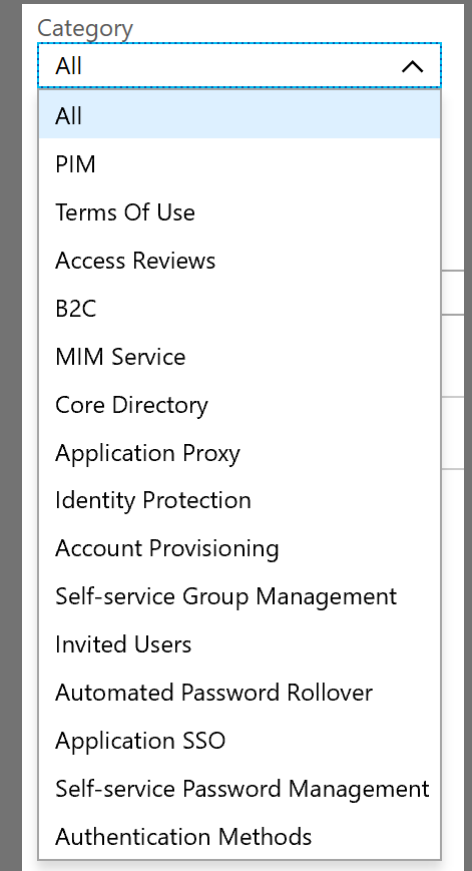
Privileged Identity Management (PIM) Elevations

Terms of Use Acceptance

B2B Redemptions

SaaS App Configuration/Provisioning

Latency is 10 to 15 mins



# Azure AD Security Logs

Users flagged for risk

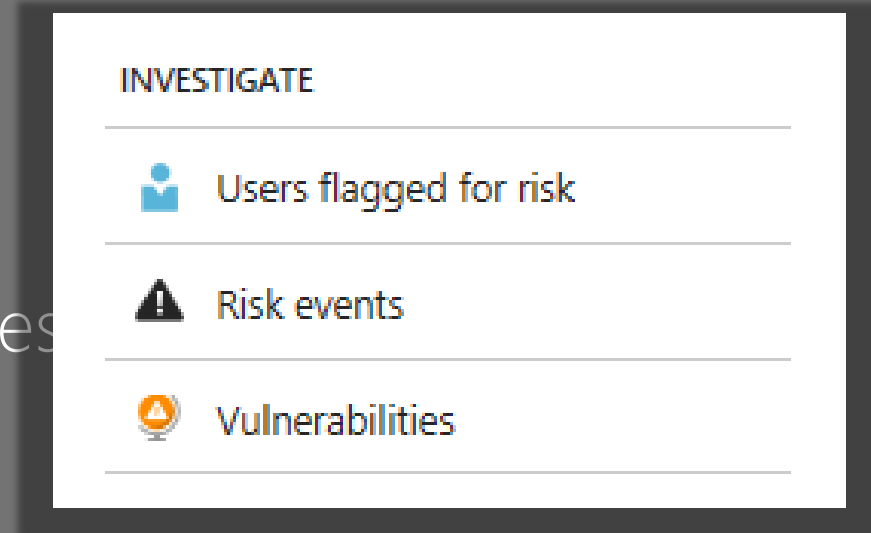
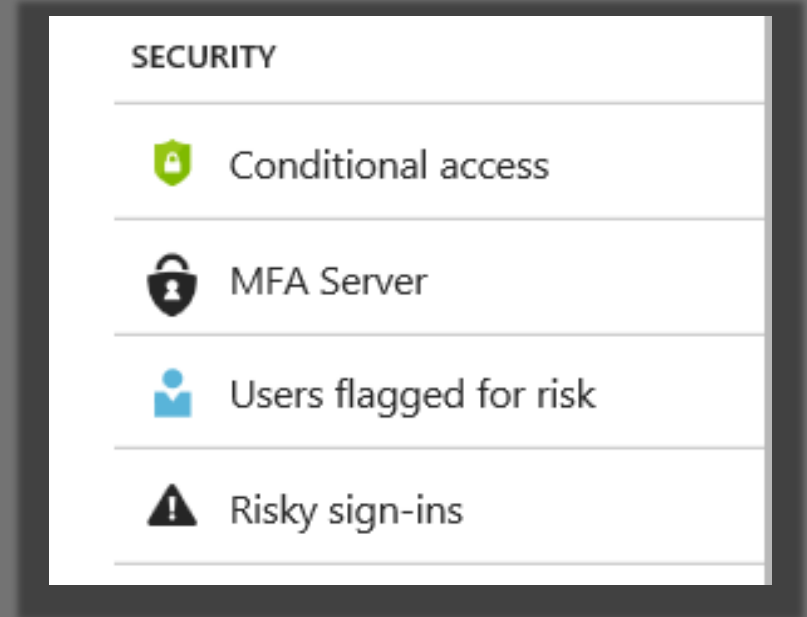
High, Medium, Low

Risk events/Risky sign-ins

leaked credentials, anonymous IPs,  
impossible travel, unfamiliar locations

Vulnerabilities

Users without MFA, Unused Admin Privileges



# Who can access logs in Azure AD

Global Administrator

Security Administrator

Security Reader

Reports Reader

No difference in data scope between roles

Users can access their own sign-in logs

# Agenda

What Are the Azure AD Logs

**Integration with SIEM Tools**

Key Events To Look For

Back in the day...Sept 2018 and earlier

The only way to programmatically access Azure AD Logs was using GraphAPI calls

Problems include but not limited to..

- Multiple end points to enumerate for different log types

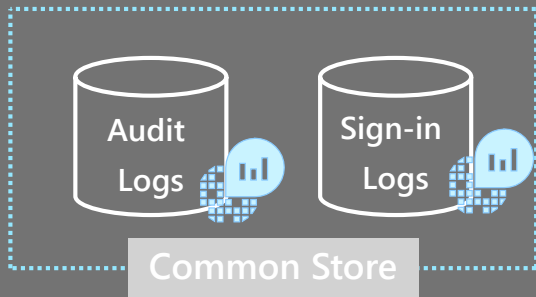
- Determining last synced event, de-duplicating events

- Using a service principal to auth with a secret stored in the script...

# Azure Monitor

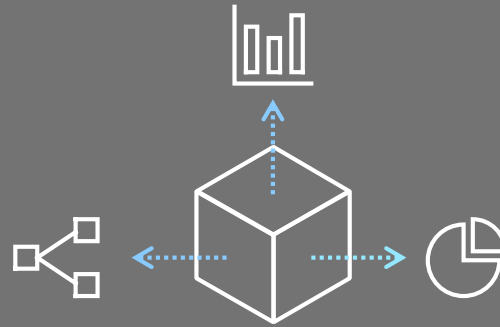


Full observability for your Azure AD Infrastructure



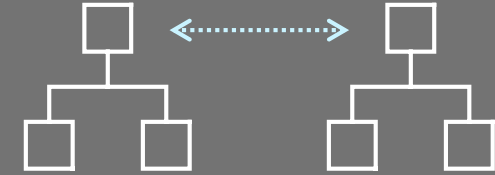
## Unified Monitoring

A common platform for all Azure AD logs



## Analyze

Rich Insights, advanced analytics and smart machine learning powered by Log Analytics



## Workflow Integrations

Rich ecosystem of popular issue management, SIEM, and ITSM tools

# Getting Started with SIEM Integration

First click on Export Settings, new Diagnostic

Give it a name, click "Stream to an Event

Optionally select storage account or Log

Select the Logs

**Diagnostics settings** [Close]

Save Discard Delete

\* Name

Archive to a storage account

Stream to an event hub

Send to Log Analytics

**LOG**

---

AuditLogs

---

SignInLogs

# SIEMs With Azure Monitor Integration

Many SIEMs have pre-built integration into Azure Monitor

Splunk ([docs](#))

Sumo Logic ([docs](#))

IBM Qradar 7.3.0 (Coming Soon)

Arcsight (Coming Soon)

Don't see your SIEM? Tell them you want this!





# Quick Win

## Azure AD Power BI Content Pack

[Download](#)

**Azure Active Directory Activity App Usage**

User Name: All Application Name: All

**19**  
Count of Unique Users

**Unique Users per App**

Application Name	Count
Azure Portal	13
Office 365	3
Azure Classic P...	4
Microsoft App ...	4
Bing	3
Graph explorer	3
O365 Suite UX	3
Identity Insights...	2
Office.com	2
AAD Onboarding	1
Azure AD Powe...	1
DocuSign	1
Dropbox	1
Facebookundef...	1
Identity Insights	1
Identity Insights...	1
Microsoft Powe...	1
Microsoft Visual...	1
Office 365 Each...	1
Protection Center	1
Skype Web Exp...	1
test-mr-app	1

**Unique Users Details**

Application Name	User Name	Unique Users
Bing	AccessTestCIO	AccessTest.CIO@wingtiptoysonline.com
Identity Insights PPE	AccessTestCIO	AccessTest.CIO@wingtiptoysonline.com
Azure Portal	Alex Weinert	alexwe@wingtiptoysonline.com
Microsoft App Access Panel	Alex Weinert	alexwe@wingtiptoysonline.com
O365 Suite UX	Alex Weinert	alexwe@wingtiptoysonline.com
Azure AD Power BI Content Pack Ap...	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Azure Classic Portal	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Azure Portal	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Bing	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
DocuSign	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Facebookundefined	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Graph explorer	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Microsoft App Access Panel	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Microsoft Power BI	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Microsoft Visual Studio Team Services	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Office 365	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Office 365 Exchange Online	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Office.com	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
Skype Web Experience On Office 365	Audrey Oliver	audrey.oliver@wingtiptoysonline.com
test-mr-app	Audrey Oliver	audrey.oliver@wingtiptoysonline.com

# Log Analytics

## Central Analytics Platform

Can utilize

Run your

Setup c

Home > f/128 Photography - Logs

Home > Log Analytics > AzureADLogsWS > Overview > Azure AD Account Provisioning Events

### Azure AD Account Provisioning Events

azureadlogs

Refresh Analytics Edit Clone

8/21/18 09:27 - 9/20/18 09:27

#### NEW USERS PROVISIONED

Successful add operations  
ACCOUNT PROVISIONING

TOTAL SUCCESSFUL ADDS  
**46.0**

APP	COUNT
Box	24
Salesforce F128	11
Workday to Active Directory Us...	11
Salesforce Managers	1
Salesforce members	1
Z Test SF	1

#### NEW USERS PROVISIONED

Failed add operations  
ACCOUNT PROVISIONING

TOTAL FAILED ADDS  
**898**

APP	COUNT
Workday to Active Directory Us...	784
Box	107
Self-Service App Access for Ser...	13
Self-Service App Access for Spl...	7
whatever you want	7
Self-Service App Access for Exp...	7
Self-Service App Access for Sal...	7
Salesforce F128	7
Self-Service App Access for Do	7

#### USERS UPDATED

Successful update operations  
ACCOUNT PROVISIONING

TOTAL SUCCESSFUL UPDATES  
**45k**

APP	COUNT
Workday to Active Directory Us...	45.1K
Box	313
Expense Managers	85
New Employees 2018	36
Socials	32
Photography Training	32
All Users	12
Salesforce members	11
Z Test SF	11

Save

ms per page

# Agenda

What Are the Azure AD Logs  
Integration with SIEM Tools

**Key Events To Look For**

# Legacy Authentication, Why You Should Care

200k accounts compromised in Aug 2018 due to password spray

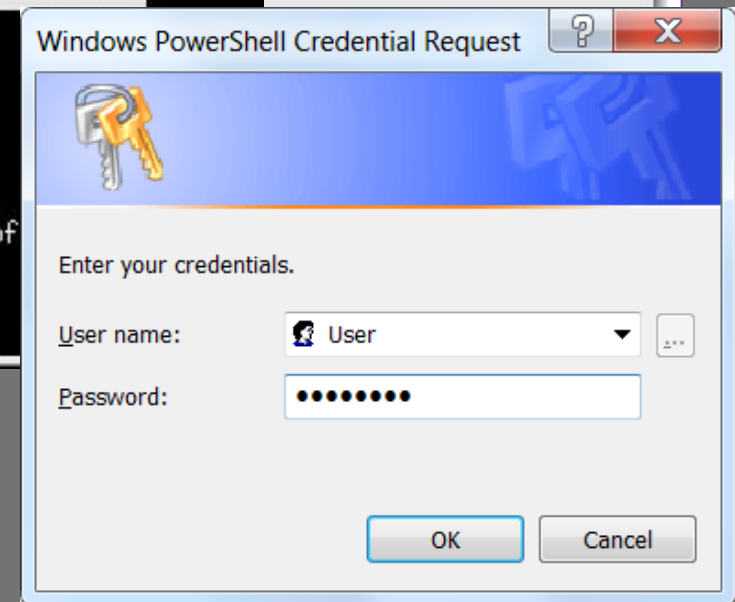
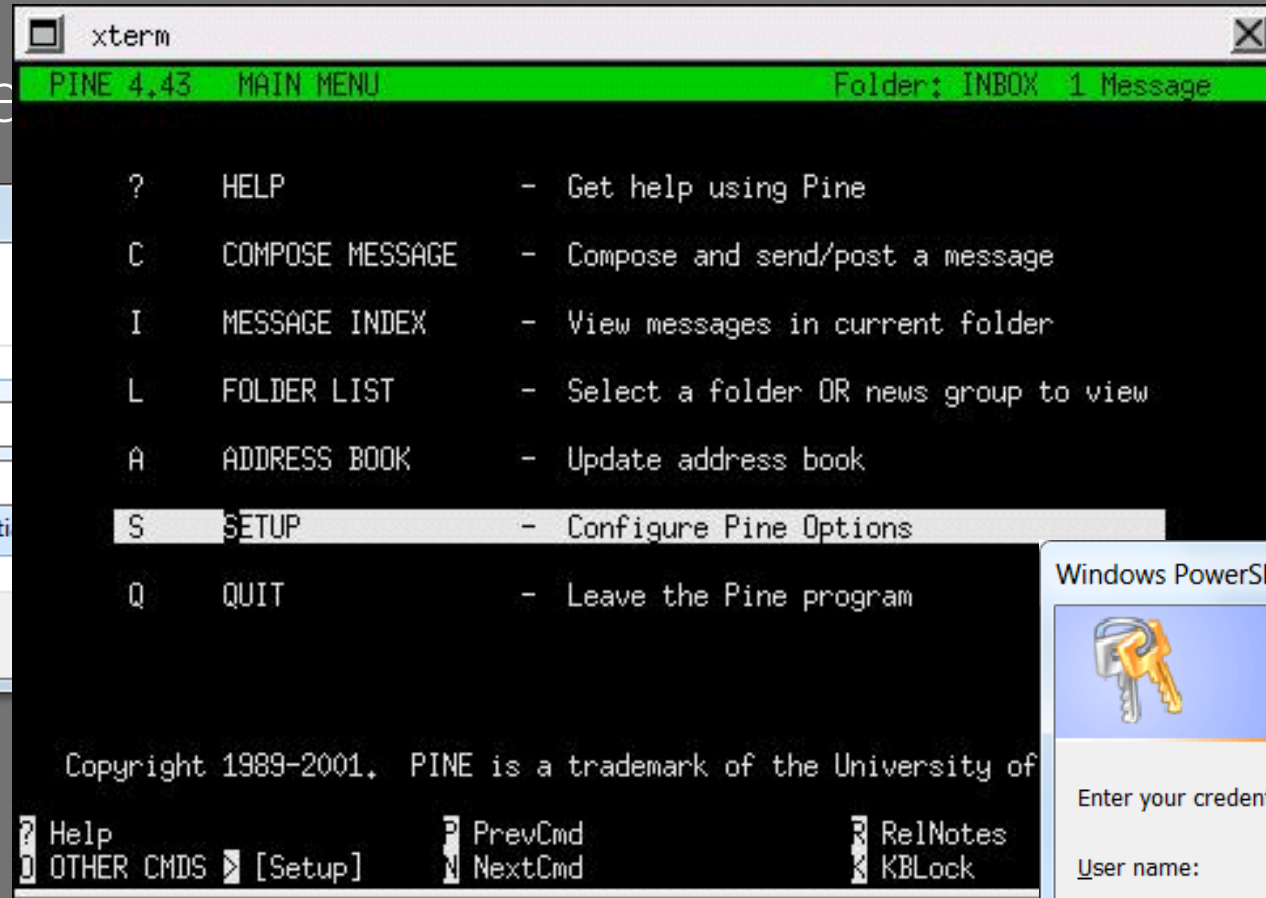
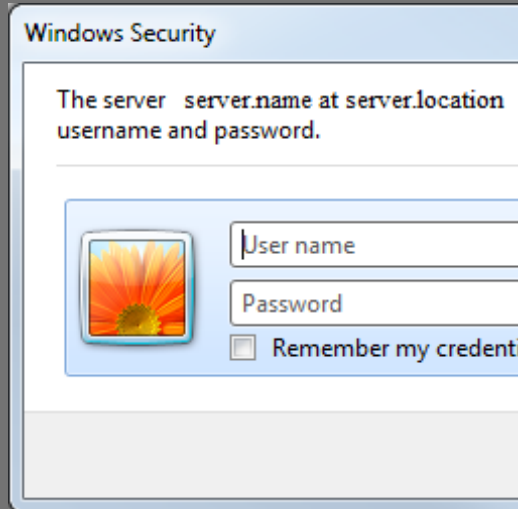
Nearly 100% of password spray attacks we see are from legacy authentication

Blocking legacy auth reduces compromise rate by 66%

<https://aka.ms>PasswordSprayBestPractices>

# Legacy Authentication, Examples

Clients that use legacy authentication



# Finding Legacy Authentication In Your Environment

Sign In Logs to examine usage

POP, IMAP, MAPI, SMTP and

ActiveSync go to EXO

“Other Clients” shows

SharePoint and EWS

Sign-In Events

Columns Refresh Download Script Power BI Troubleshoot

Search is case sensitive and supports 'starts with' operator

User:  Username:  Application:  Sign-in status:

Client App:  Conditional Access:

Show dates as:

	↑↓	USERNAME	↑↓	APPLICATION	↑↓	SIGN-IN STATUS	CLIENT APP	CONDITIONAL ACC...
		audrey.oliver@wingt...		Azure Portal		Success	Browser	Success
		audrey.oliver@wingt...		Azure Portal		Failure	Browser	Success
		audrey.oliver@wingt...		Azure Portal		Failure	Browser	Failure
		audrey.oliver@wingt...		Azure Portal		Failure	Unknown	Not Applied
7/17/2018, 1:15:08 AM		Hannah Han		hannahhanhaha@wi...		Microsoft App Acce...	Browser	Success
7/16/2018, 11:11:35 PM		Barbara Kess		barbarak@wingtpt...		Azure Portal	Browser	Not Applied
7/16/2018, 11:11:24 PM		Barbara Kess		barbarak@wingtpt...		Azure Portal	Unknown	Not Applied
7/16/2018, 11:10:58 PM		Barbara Kess		barbarak@wingtpt...		Azure Portal	Unknown	Not Applied

# Key Security Events To Take Action On

## Any High Risk Event

Leaked Credentials

Users at High Risk

## Medium Risk Events

Tor Browser Logins

Unfamiliar locations

Suspicious IP



# Key Audit Events To Investigate

Promotion of accounts to Admin Accounts

Creation of accounts that look like service accounts/high-value employees

Updates to Service Principals

Consent grants made by admins!

Removal of MFA requirements

Disablement or change of Audit configuration

## Key O365 Events To Investigate

Creation of mail forwarding rules in a mailbox or transport rule to an external domain.

Addition of mail forward permissions or mailbox delegates

Changes to external sharing policies

[More O365 events here](#)

# Questions

@markmorow  
Markmoro@Microsoft.com

Mark Morowczynski  
Principal Program Manager