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

Hybrid Components

Cloud Services

- AppProxy Cloud Service
- Azure AD Connect Backend
- Health Service
- Authentication Services
- Azure MFA
- Dynamic Groups
- Conditional Access Engine
- Identity Protection
- Group-based licensing
- First Party Provisioning Service
- Graph API
- Provisioning Service
- Domain Services
- Azure Resource Manager Role Services
- Managed Identity Backend
- Privileged Identity Management

Core Store

Role Based Access Control

- Role Based Access Control
- Dynamic Groups
- Self-Service Group Management
- Self-service user portal
- Device Services
- Self-service Password reset service
- Activity Logs
- Access Reviews

On-premises sync agent

Privileged Identity Management
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
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
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 Setting
Give it a name, click “Stream to an Event Hub”
Optionally select storage account or Log Analytics
Select the Logs
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!
What About Security Events?
These come from the Intelligent Security Graph and lots of other security alerts

http://aka.ms/GraphSecuritySIEM

Setup Azure Monitor to send alerts to the same Event Hub
Quick Win

Azure AD Power BI Content Pack

Download
Log Analytics

Central Analytics Platform

Can utilize ML algorithms for clustering and anomaly detection

Run your own queries natively in Azure Portal

Setup custom alerts and actions
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:

- Office 2010 and older
- Office 2013 by default (can use modern auth with reg key)
- Clients using older mail protocols (POP, IMAP, SMTP, etc.)
- Older PowerShell Modules
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.
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 ServicePrincipals

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