

Работни книги на Azure AD

Даниел Ууд

Програмен мениджър

Защита на самоличности на Azure AD

18 февруари 2021 г.

Важността да се използва работната книга на Azure AD, за да се разберат често срещани модели на атаки

- 01.** Как да получите достъп до работната книга на Azure AD
- 02.** Част 1: Променени идентификационни данни на приложения и услуги и методи за удостоверяване
- 03.** Част 2: Променени настройки за федерации
- 04.** Част 3: Нови разрешения, дадени на главните субекти на услуги
- 05.** Част 4: Общ преглед на промените, направени в членството на главните субекти на услуги

01.

Влезте в **портала на Azure**.

02.

Отидете на **Azure Active Directory > Наблюдение > Работни книги**

03.

В секцията „Отстраняване на неизправности“ отворете **Отчет за чувствителните операции**

01.

Променени идентификационни данни на главни субекти на приложения и услуги/методи за удостоверяване

01.

Променени идентификационни данни на приложения и услуги и методи за удостоверяване

Всички нови
идентификационни данни,
добавени към главните
субекти на приложения и
услуги, включително типа
идентификационни данни

Най-активни действащи лица
и количеството промени в
идентификационните данни,
които са извършили

Времева линия за всички
промени в
идентификационните данни

02.

Променени настройки за федерации

Woodgrove | Workbooks | Sensitive Operations Report

Azure Active Directory

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
 - Sign-ins
 - Audit logs
 - Provisioning logs (Preview)
 - Logs
 - Diagnostic settings
 - Workbooks
 - Usage & insights
- Troubleshooting + Support
 - Virtual assistant (Preview)
 - New support request

Workbooks

Edit

- Modified application and service principal credentials/authentication methods
- New permissions granted to service principals
- Directory role and group membership updates to service principals

Modified federation settings

This section monitors when a user or application modifies the federation settings on the domain. For example, this alert will trigger when a new Active Directory Federated Service (ADFS) TrustedRealm object, such as a signing certificate, is added to the domain. Modification to domain federation settings should be rare. Confirm the added or modified target domain/URL is legitimate administrator behavior.

- To understand why an authorized user may update settings for a federated domain in Office 365, Azure, or Intune, see: <https://docs.microsoft.com/office365/troubleshoot/active-directory/update-federated-domain-office-365>.
- For details on security realms that accept security tokens, see the ADFS Proxy Protocol (MS-ADFSPP) specification: https://docs.microsoft.com/openspecs/windows_protocols/ms-adfspp/e7b9ea73-1980-4318-96a6-da559486664b.

TimeRange: Last 60 days

Operation: All

InitiatingUserOrApp: All

TimeGenerated	OperationName	InitiatingUserOrApp	AADOperationType	targetDisplayName	TargetResources	Result	UserAgent
12/18/2020, 8:59:57 PM	Set federation settings on domain	jeffs@woodgrove.ms	Update	woodgrove.net	[{"displayName":"woodgrove.net","administrativeUnits":[],...	success	
12/7/2020, 3:37:54 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
12/7/2020, 3:12:05 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
12/7/2020, 3:11:40 PM	Add unverified domain	joeyc@woodgrove.ms	Add	pre2.woodgrove.ms	[{"displayName":"pre2.woodgrove.ms","administrativeUnits":...	success	Mozilla/5.0 (Windows NT 10.0.17134.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0
12/7/2020, 3:10:58 PM	Add verified domain	joeyc@woodgrove.ms	Add	Unknown	[{"displayName":"Unknown","administrativeUnits":[],"mod...	failure	Mozilla/5.0 (Windows NT 10.0.17134.0; Win64; x64; rv:60.0) Gecko/20100101 Firefox/60.0

02.

Променени настройки за федерации

Промени, извършени в
съществуващи гаранتي за
федерации на домейни

Добавяне на нови домейни и
гаранти

03.

Нови разрешения, дадени на
главните субекти на услуги

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights
- Troubleshooting + Support
- Virtual assistant (Preview)
- New support request

Workbooks

Edit

New permissions granted to service principals

This section monitors for changes to OAuth 2.0 permissions granted to Service Principals. For example, this alert will trigger when a Service Principal is granted Application (AppOnly) permissions to read mail through the Microsoft Graph API. When this occurs, the Service Principal is added to an App Role with a value of Mail.Read.

An attacker could elevate their privileges by using a compromised account to grant new permissions to a Service Principal they control, or by tricking a user into granting permissions. Investigations should focus on high privilege permissions that either grant access to sensitive data, or represent opportunities for lateral movement by attackers.

The first view in this section focuses specifically on Application permissions, which generally (but not always) represent higher risk. The second view is broader- it includes Delegated (App+User) permissions grants and additional audit events.

TimeRange: Last 60 days

ClientApp: All

Resource: All

New Application (AppOnly) permissions added to service principals

Search

Resource	↑↓	ClientApp	↑↓	Role_Added	↑↓	Explanation	↑↓	InitiatingUserOrApp	↑↓	TimeGenerated	↑↓
Office 365 Exchange Online (4)											
JeffTestCreds2" (4)											
Microsoft Graph (4)											
JeffTestCreds2" (3)											
		JeffTestCreds2"		Application.Read.All"		"Read all applications"		jeffs@woodgrove.ms		12/20/2020, 1:54:46 PM	
		JeffTestCreds2"		"Mail.Send"		"Send mail as any user"		jeffs@woodgrove.ms		12/22/2020, 11:56:24 AM	
		JeffTestCreds2"		"Mail.ReadWrite"		"Read and write mail in all mailboxes"		jeffs@woodgrove.ms		12/22/2020, 11:56:24 AM	
Mimorony AuthTS API" (1)											
Office 365 SharePoint Online (1)											
JeffTestCreds2" (1)											

TimeRange: Last 48 hours

Operation: All

InitiatingUserOrApp: All

Recent app permissions activity

TimeGenerated	↑↓	InitiatingUserOrApp	↑↓	OperationName	↑↓	ClientApp	↑↓	Resource	↑↓	Result	↑↓
1/26/2021, 4:25:23 PM		jerryw@woodgrove.ms		Consent to application		CCE Test		Not logged		success	

04.

Общ преглед на промените, направени в
членството на главните субекти на услуги

- External Identities
- Roles and administrators
- Administrative units
- Enterprise applications
- Devices
- App registrations
- Identity Governance
- Application proxy
- Licenses
- Azure AD Connect
- Custom domain names
- Mobility (MDM and MAM)
- Password reset
- Company branding
- User settings
- Properties
- Security
- Monitoring
- Sign-ins
- Audit logs
- Provisioning logs (Preview)
- Logs
- Diagnostic settings
- Workbooks
- Usage & insights
- Troubleshooting + Support
- Virtual assistant (Preview)
- New support request

Workbooks

Edit

Sensitive Operations Report - Apps, Service Principals and Federation Settings

Workspace: All

This workbook is intended to help identify suspicious application and service principal activity that may indicate compromises in your environment. [Learn more](#) about best practices to protect M365 from attacks.

- Modified application and service principal credentials/authentication methods
- New permissions granted to service principals

Directory role and group membership updates to service principals

Directory role and group membership updates to service principals

This section monitors for Service Principals being as members of Directory Roles (admin roles) or Groups. For example, this alert will trigger when a Service Principal is added to the Company Administrator or Application Administrator role.

An attacker could elevate their privileges by adding a Service Principal they control to a high privileged role or a group that is used to protect access to sensitive resources. Investigations should focus on administrator rules and Groups that either grant access to sensitive data or represent opportunities for lateral movement by attackers.

TimeRange: Last 60 days

Operation: Add member to role

InitiatingUserOrApp: All

TimeGenerated	InitiatingUserOrApp	ServicePrincipalDisplayName	GroupOrRoleNameAddedTo
12/22/2020, 11:49:13 AM	jeffs@woodgrove.com	JeffTestCreds2	"Application Administrator"
12/22/2020, 11:52:28 AM	jeffs@woodgrove.com	Risky App	"Global Administrator"
12/20/2020, 7:46:25 PM	jeffs@woodgrove.com	JeffTestCreds2	"Security Operator"

Select

All

Add member to role

Add eligible member to role

Add scoped member to role

Add member to group

Общ преглед на Solorigate

Следващи СТЪПКИ

01 Гледайте Solorigate Поредица от видеоклипове в това местоположение

02 Посетете Microsoft Security за още актуализации: www.microsoft.com/en-us/security/business

03 Прочетете публикациите в блога на адрес: www.microsoft.com/security/blog/

<https://aka.ms/solorigate>

