Microsoft

Azure AD アイデンティティ IOC

Daniel Wood

プログラム マネージャー

Azure AD Identity Security

2021 年 2 月 18 日

Solorigate ビデオ シリーズ

Azure Active Directory に対する攻撃の 4 つのパターン

01 パターン 1:盗まれた SAML トークン署名マテリアルを使用して偽造された SAML トークン

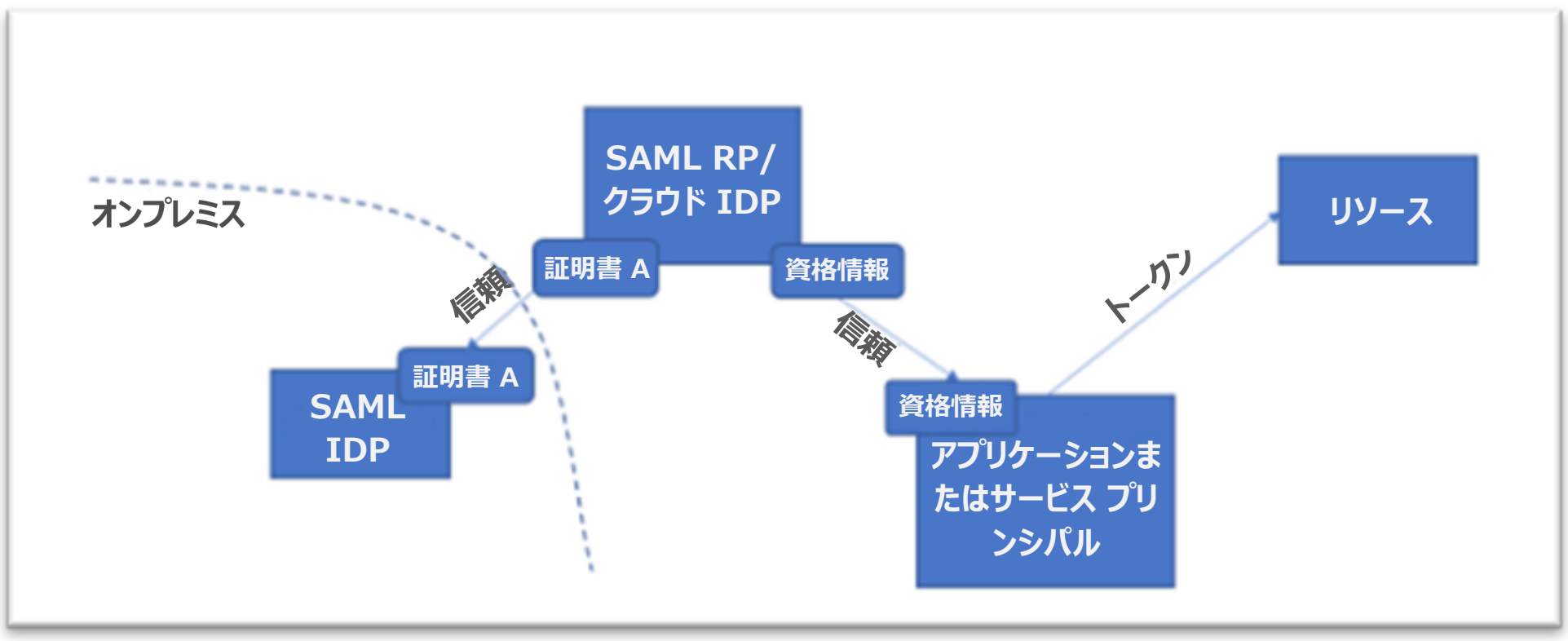
02 パターン 2:SAML 信頼関係の不正登録

03 パターン 3:既存アプリケーションへの資格情報追加

04 パターン 4:既存アプリケーションを偽装するクエリ

Microsoft Security

Solorigate ビデオ シリーズ



01. パターン

盗まれた SAML トークン署名マテリアルを使用して偽造されたSAML トークン

これらを探します:

- SP が受領した SAML トークンの構成が IDP の構成済み行動から逸脱している。
- SP が受領した SAML トークンに対応する発行ログが IDP に存在しない。
- SP が受領した SAML トークンに MFA クレームがあるが、対応する MFA アクティビティ ログが IDP にない。
- 受領した SAML トークンの送信元の IP アドレス、エージェント、時刻、対象のサービスが、そのトークンが示す要求側アイデンティティにとって変則的である。
- 未承認の管理者アクティビティの証拠。

すべきこと:

1. 証明書盗み出しのメカニズムを特定し、修復します。
2. すべての SAML トークン署名証明書をローリングします。
3. オンプレミス SAML 信頼への依存を、可能であれば減らすことを検討します。
4. HSM を SAML トークン署名証明書の管理に使うことを検討します。

02. パターン

SAML 信頼リレーションシップの不正登録

これらを探します：

フェデレーション信頼関係の改変を伴う変則的な管理者セッション。

すべきこと:

1. フェデレーション信頼関係をすべて見直し、正当であることを確認します。
2. 管理者アカウント偽装のメカニズムを特定します。
3. 管理者アカウントの資格情報をローリングします。

03. パターン

既存アプリケーションへの資格情報追加

これらを探します:

- フェデレーション信頼関係の改変を伴う変則的な管理者セッション。
- 予期しないサービス プリンシパルの追加がクラウド環境内の特権ロールに対して行われている。

すべきこと

1. すべてのアプリケーションとサービス プリンシパルを見直して、資格情報の改変活動を見つけます。
2. すべてのアプリケーションとサービス プリンシパルを見直して、過剰なアクセス許可が付与されていないことを確認します。
3. 環境内にある、非アクティブのサービス プリンシパルをすべて削除します。
4. すべてのアプリケーションとサービス プリンシパルの資格情報を定期的にローリングします。

04. パターン

既存アプリケーションを偽装するクエリ

これらを探します:

- 信頼しているアプリケーションやサービス プリンシパルからの変則的なリソース要求。
- サービス プリンシパルからの要求でグループ、ユーザー、アプリケーション、サービス プリンシパル、または信頼関係が追加または変更されている。

すべきこと:

1. フェデレーション信頼関係をすべて見直し、正当であることを確認します。
2. 管理者アカウント偽装のメカニズムを特定します。
3. 管理者アカウントの資格情報をローリングします。

Solorigate ビデオ シリーズ

次のステップ

01 この場所にある Solorigate ビデオ シリーズを見る

02 Microsoft Security にアクセスして最新情報を入手する: www.microsoft.com/ja-jp/security/business

03 ブログを読む: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft

© Copyright Microsoft Corporation. All rights reserved.