Microsoft

Azure AD Identity IOC

Daniel Wood

Administrador de programa

Seguridad de identidad Azure AD

18 de febrero de 2021

Serie de videos sobre Solorigate

4 patrones de ataques en Azure Active Directory

01 Patrón 1: Tokens SAML falsificados utilizando material robado de inicio de sesión con token SALM

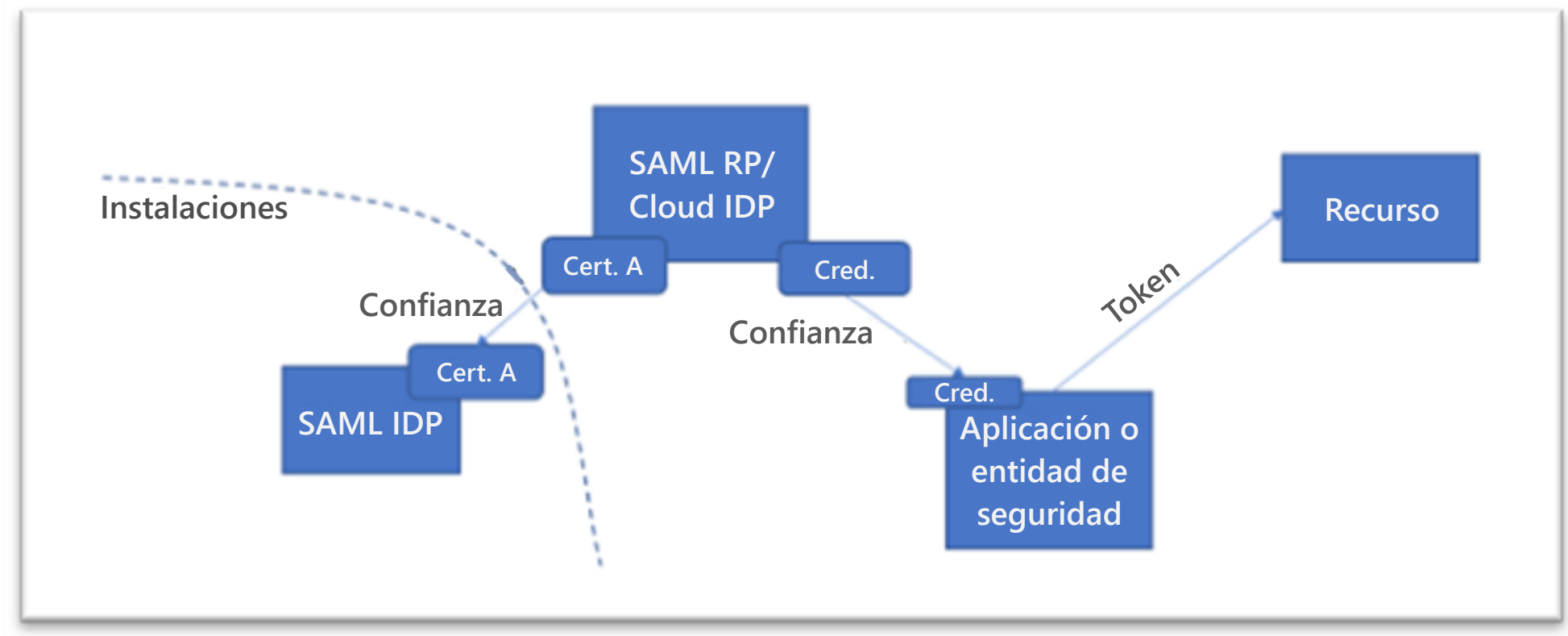
02 Patrón 2: Registros ilícitos de las relaciones de confianza SAML.

03 Patrón 3: Agregar credenciales a aplicaciones existentes

04 Patrón 4: Consultas que suplantan aplicaciones existentes

Microsoft Security

Serie de videos sobre Solorigate



01. Patrón

Tokens SAML falsificados utilizando material de inicio de sesión de token SALM robado

Qué buscar:

- Tokens SALM recibidos por SP con configuraciones que se desvían del comportamiento configurado de IDP.
- Tokens SAML recibidos por SP sin que se correspondan con el registro emitido por IDP.
- Tokens SAML recibidos por SP con solicitudes de MFA pero sin registros que se correspondan con la actividad de MFA en IDP.
- Tokens SAML que se reciben de direcciones IP, agentes, tiempos o para servicios que son anómalos debido a la identidad de solicitud representada en el token.
- Prueba de una actividad administrativa no autorizada.

Qué hacer:

1	Determina el mecanismo de filtraciones certificadas y corrígelo.
2	Rota todos los certificados de firma de token SAML.
3	Considera reducir tu confianza en la trust SAML en el entorno local cuando sea posible.
4	Considera utilizar un HSM para gestionar tus certificados de firma de tokens SAML (TSC).

02. Patrón

Registros ilícitos de las relaciones de confianza SAML

Qué buscar:

Sesión administrativa anómala asociada con la modificación de relaciones de confianza.

Qué hacer:

1	Revisa todas las relaciones de confianza y asegúrate de que sean válidas.
2	Determina el mecanismo de suplantación de la cuenta administrativa.
3	Rota las credenciales de cuentas administrativas.

03. Patrón

Agregar credenciales a una aplicación existente

Qué buscar:

- Sesión administrativa anómala asociada con la modificación de relaciones de confianza.
- Entidades de seguridad inesperadas agregadas a roles con privilegios en entornos en la nube.

Qué hacer

1	Revisa todas las aplicaciones y entidades de seguridad en busca de una actividad de modificación de credenciales.
2	Revisa todas las aplicaciones y las entidades de seguridad en busca de excesos de permisos.
3	Quita todas las entidades de seguridad inactivas de tu entorno.
4	Rota de forma habitual las credenciales de todas las aplicaciones y entidades de seguridad.

04. Patrón

Consultas que suplantan aplicaciones existentes

Qué buscar:

- Solicitudes anómalas a tus recursos de aplicaciones de confianza o entidades de seguridad.
- Solicitudes de entidades de seguridad que agregaron o modificaron grupos, usuarios, aplicaciones, entidades de seguridad o relaciones de confianza

Qué hacer:

1	Revisa todas las relaciones de confianza y asegúrate de que sean válidas.
2	Determina el mecanismo de suplantación de la cuenta administrativa.
3	Rota las credenciales de cuentas administrativas.

Serie de videos sobre Solorigate

Siguientes pasos

01 Ver la serie de videos de Solorigate en esta ubicación

02 Visita Seguridad de Microsoft para más actualizaciones: www.microsoft.com/es-mx/security/business

03 Lee las publicaciones en el blog en: www.microsoft.com/security/blog

https://aka.ms/solorigate

Microsoft Security

Microsoft