Silent for Business

Servicio de Protección de correo

(anti-phishing)

El **Servicio de Protección contra Phishing con Microsoft Defender para Office 365** es una solución avanzada de seguridad diseñada para proteger a los usuarios de Microsoft 365 contra amenazas sofisticadas como el phishing, la suplantación de identidad (spoofing), y otros ataques basados en correo electrónico.

Entorno

¿Qué es el anti-phishing en Defender para Office 365?

Es una solución avanzada de seguridad que analiza los correos electrónicos entrantes para detectar y bloquear intentos de phishing antes de que lleguen a los buzones de los usuarios. Utiliza inteligencia artificial, aprendizaje automático y señales de seguridad de Microsoft para identificar patrones sospechosos.

La Protección contra Phishing con **Microsoft Defender para Office 365** funciona en diversos entornos y plataformas dentro del ecosistema de Microsoft 365, lo que permite una cobertura integral contra amenazas basadas en correo electrónico.

Principales entornos compatibles:

- Exchange Online y Outlook de escritorio
- Microsoft Teams
- SharePoint Online y OneDrive

Las capacidades de respuesta de Microsoft Defender para Office 365 son una parte fundamental de su enfoque de seguridad, ya que no solo detecta amenazas como el phishing, sino que también permite responder de forma rápida, automatizada y eficaz para minimizar el impacto en la organización.

Características

- Protección avanzada contra amenazas (ATP Anti-Phishing)
- Políticas personalizadas
- Análisis de enlaces (Safe Links).
- Protección contra suplantación de usuarios y dominios
- Integración con Microsoft Sentinel y otras soluciones SIEM/SOAR
- Análisis de comportamiento.
- Investigación automatizada y respuesta (AIR)
- Cuarentena avanzada y portal de revisión

Tecnologías

- Microsoft Defender for 365

Beneficios

- Reducción significativa del riesgo de ataques de phishing.
- Mayor visibilidad y control sobre amenazas dirigidas.
- Entrenamiento proactivo para los usuarios.

Casos de uso

1. **1. Protección de ejecutivos (CEO/CFO).** - Defender detecta la suplantación del dominio o del nombre del remitente y bloquea el mensaje antes de que llegue al destinatario.
2. **Prevención de fraudes de facturación. -** Defender analiza el comportamiento del remitente y detecta anomalías en el contenido o en los enlaces, marcando el correo como sospechoso.
3. **Simulación de ataques para concientización. -** Se utiliza el **Attack Simulator** para enviar correos simulados y medir quién hace clic, quién reporta, y quién desconoce de los riesgos.
4. **Protección contra enlaces maliciosos (phishing de credenciales). - Safe Links** reescribe y analiza el enlace en tiempo real, bloqueando el acceso si se detecta como malicioso.

ARQUITECTURA