
Microsoft
Microsoft Security Envisioning
white Hat
CONSULTORES

Perfil de WHC

• Somos una empresa mexicana con 12 años en el mercado de la consultoría. Contamos con **alta especialización en Servicios de Ciberseguridad** con importante presencia en las principales verticales reguladas.

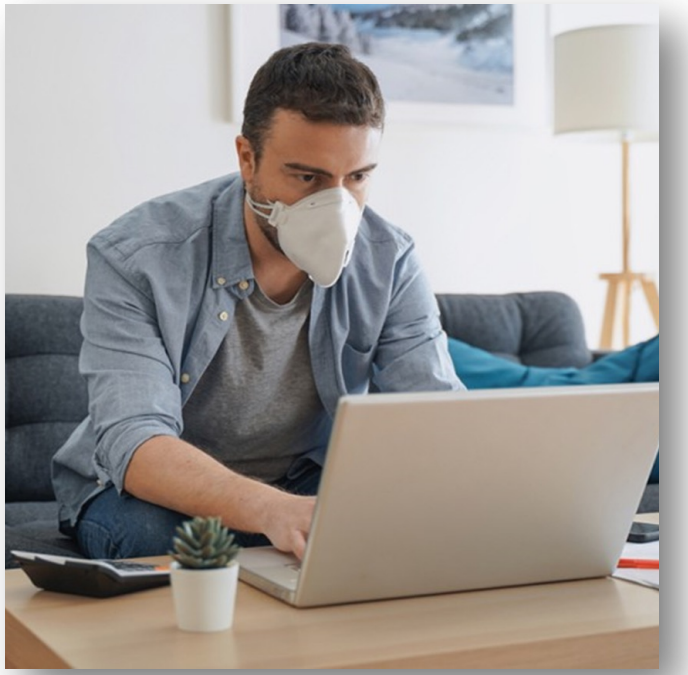
- **De nuestros principales valores agregados es que somos una empresa que cuenta con la certificación internacional ISO 27001:2013 en nuestros procesos de Ciberseguridad**

- **Partners de Microsoft en Servicios de Seguridad**

El trabajo remoto – Home Office

Aumento en el uso de dispositivos móviles y acceso remoto a sistemas de la organización.

- Migración a plataformas de nube.
- VPNs
- Mecanismos de autenticación.
- Integración de más equipos al ecosistema.



Los dispositivos y sistemas que no cuenten con protección podrían provocar la perdida de datos, afectaciones a los servicios, divulgación de información confidencial y contagio por malware.

Microsoft

La seguridad en tiempos del COVID-19: Retos

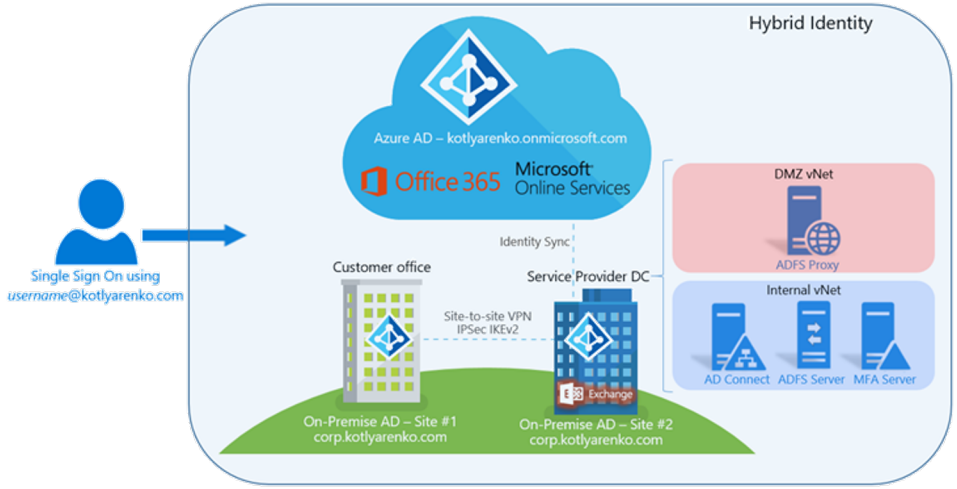
- Una repentina carrera por trabajar de forma remota ha dejado a las organizaciones luchando por implementar tecnología, actualizar políticas y capacitar a los empleados.

- Los atacantes se están aprovechando de la confusión y las brechas en la cobertura para atacar, enviando malware y contenido malicioso a sus correos electrónicos buscando algún acceso.

- Una modalidad actual es atacar directamente a los sistemas en la Nube y posteriormente acceder a sistemas críticos.

- Sistemas Críticos de seguridad:

✓ Sistemas VPNs.
✓ Sistemas Cloud.
✓ Sistemas de Colaboración.

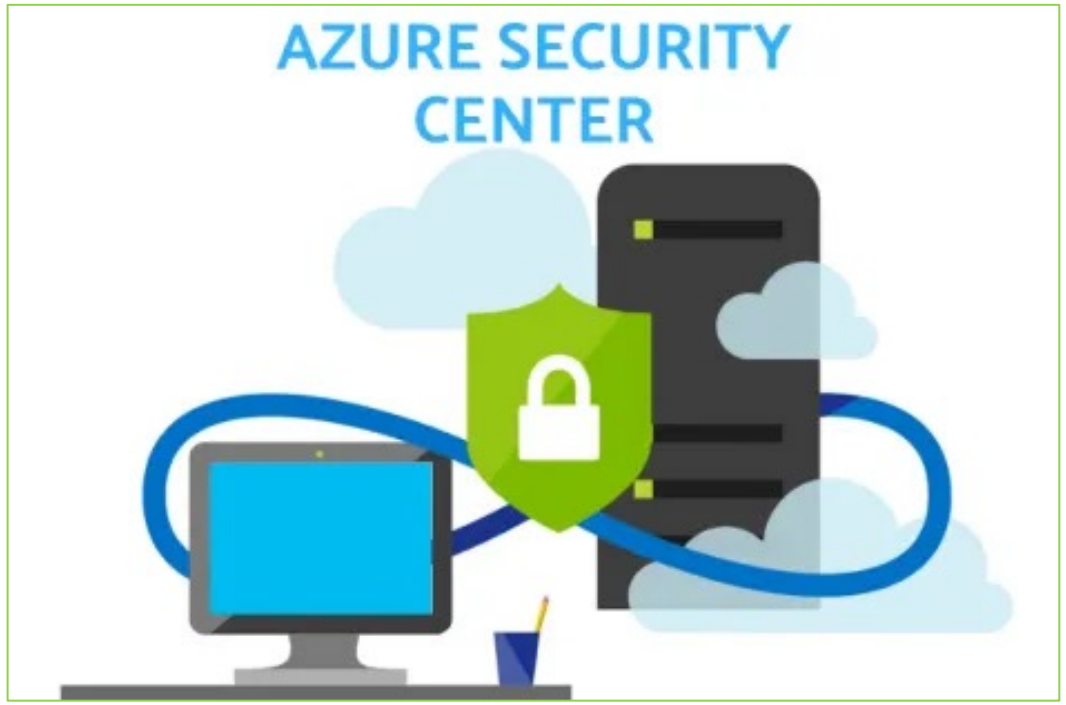


Alcance del servicio

White Hat
CONSULTORES

Alcance

Dar demostración en vivo de las funcionalidades de seguridad avanzada en el *tenant* del cliente a través de las soluciones:



Microsoft

Puntos Relevantes

Security Center

Una solución integral la cual da una mayor visibilidad de cuales son las vulnerabilidades de nuestros entornos, nos ayuda a dar cumplimiento a los estándares mas reconocidos globalmente, como PCI, ISO, SOC, además de contar un un EDR como Azure Defender el cual dará una mayor seguridad a nuestros endpoints.

Azure Sentinel

Es una de las mejores soluciones con las que podamos contar hoy en día, es un SIEM, que tiene un universo de conectores que nos ayudaran a que ese monitoreo sea mas ágil, para una contención, así como levantar incidentes para su erradicación.

Ambas soluciones tienen la versatilidad de poder integrarse a cualquier ambiente sea hibrido o en cualquier cloud.

Attackers Know Microsoft 365 Better Than You Do

Users have taken to Microsoft Office 365's tools, but many are unaware of free features that come with their accounts -- features that would keep them safe.

Organizations have quickly adopted the full-featured set of productivity and collaboration tools offered by Office 365 (O365), which was moved under the Microsoft 365 umbrella this spring. They're leveraging Microsoft Teams, SharePoint, OneDrive, and other file storage systems to store and collaborate on sensitive documents and data. However, with the exponential increase of usage in the last few months, the platform has become an enticing and fruitful target for attackers of all types.

In 2019, 85% of all incident response investigations conducted by the Kudelski Security Incident Response team started with a compromised Office 365 account. While reviewing the results of those investigations, one thing quickly became apparent: Attackers know the productivity suite better than most IT administrators and defenders.

How Attackers Are Attacking

This year, we saw attackers leverage a multitude of attack techniques, most of which could have been easily prevented by turning on features included with most Office 365 Enterprise plans. As organizations strategize for 2021, it is paramount to know and understand how malicious actors are capitalizing on their knowledge of these environments to compromise, persist in, and exfiltrate data.

https://www.darkreading.com/cloud/attackers-know-microsoft-365-better-than-you-do/a/d-id/1339404

Requerimientos

- ✓ Envío presentación (Alcances)
- ✓ Go-ahead del cliente para inicio

- ✓ Una sesión para configuración inicial (2 h)
- ✓ Máximo 10 servidores para la demostración
- ✓ Sesión de la demostración (2h)



- ✓ Firma de carta de cierre del servicio (al final del servicio)

Dudas o comentarios

Servicios:

Fernando Garay:
Fernando.garay@whitehatconsultores.com

Dudas & asesoría ténicas:

José Antonio Morales:
Antonio.morales@whitehatconsultores.com

INSURGENTES 586, INT 401, COL. DEL VALLE, BENITO JUAREZ, CIUDAD DE MEXICO, C.P. 03100

Gracias!