Ciberseguridad
Objetivo: Datacenter

Quién soy?

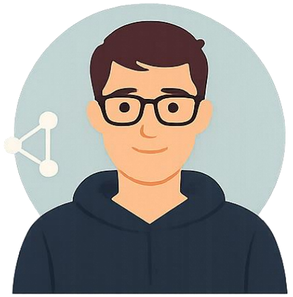
Luis Fascinetto

Director de Ciberseguridad / Datacenter / TIC

Soy un hacker

No es lo mismo?

Hacker vs. Ciberdelincuente



Hacker

Es una persona entusiasta, creativa y curiosa de la tecnologia que utiliza sus habliidades para entender y superar los limites de la techologia digital.

Ciberdelincuente

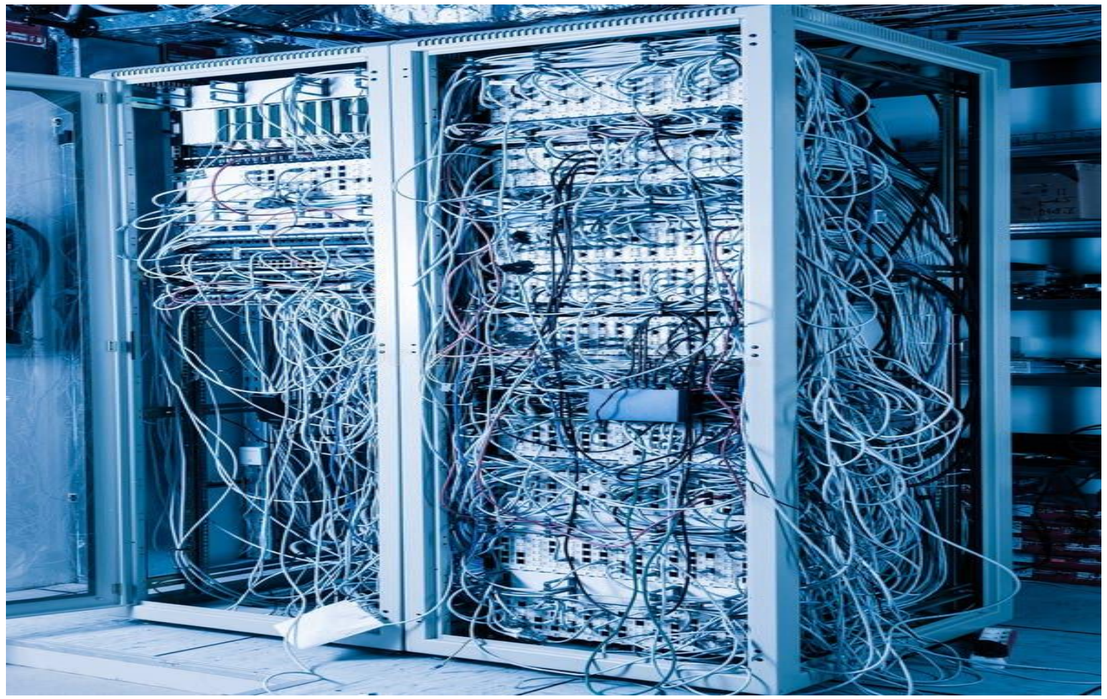
Es una persona que utiliza habilidades tecnologicas con fines maliciosos y para obtener beneficios personales

⚠️ Advertencia ⚠️

Esta presentación tiene fines exclusivamente educativos e informativos. No promovemos, incentivamos ni respaldamos el uso indebido de las herramientas, técnicas o conocimientos aquí expuestos. No nos hacemos responsables por el mal uso que terceros puedan darle a este contenido.

Next Data

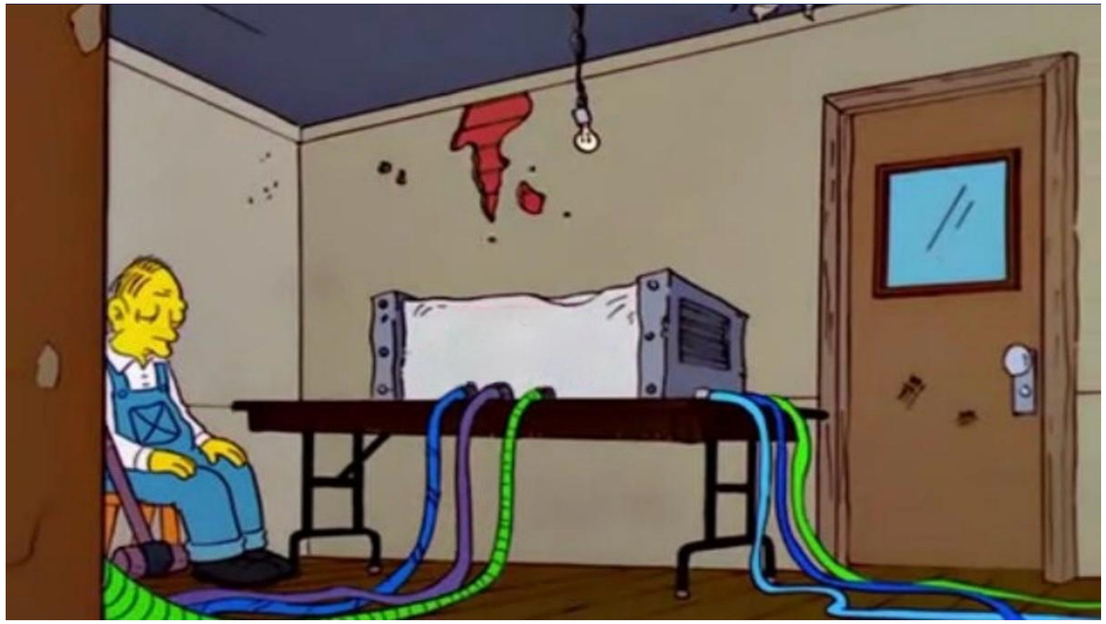
¿Qué es un DataCenter?



Datacenter

Es un espacio físico centralizado donde se encuentran servidores, sistemas de almacenamiento, sistemas de respaldo y equipos de red para procesar, distribuir y guardar grandes cantidades de información.

Nube



Es la infraestructura clave detrás de internet, los sitios web, las aplicaciones móviles y los servicios en la nube.

¿ ?

¿Por qué el Datacenter es el Objetivo?

Por que?

OnlyFans

David Ortega

Datos del DataCenter

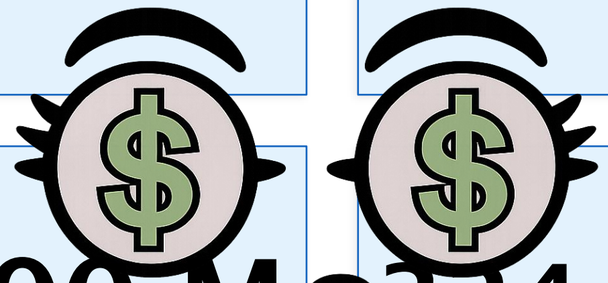
Datacenter

#2

73 nuevos DC en Mexico

5.2%

PIB Nacional (MEXDC)



$5,000 M

Inversion de AWS

$324,000 M

Ciberataques en Mexico

¿Por qué atacar a un Datacenter?

Objetivo

- Todos los servicios viven en un servidor
- Informacion financiera, clientes, credenciales, propiedad intellectual, backups
- Interrumpir un DC paralizar la operacion y la continuidad del negocio
- Obteniendo acceso al DC se pueden realizar movimientos laterales
- Un solo ataque puede valer millones en rescate o venta de datos en darkweb

Next Data

Vectores de Ataque al DC

Credenciales Comprometidas

El 80% de brechas inician con credenciales robadas. Phishing, fuerza bruta o compra en dark web. Una contraseña = acceso total al DC

Ataques DDOS

Inundan el DC con tráfico falso hasta colapsar los uplinks. Un ataque de 100 Gbps puede paralizar toda la operación en segundos

Vulnerabilidades

Sistemas legacy, hipervisores desactualizados, APIs expuestas. El atacante escanea 24/7 buscando el eslabón débil

Ransomware

No es un malware genérico — es un ataque planificado semanas antes. Cifra backups, sistemas críticos y pide rescate millonario

Acceso Fisico

Un USB en el servidor, un cable mal conectado, un técnico sin verificar. La seguridad lógica no sirve si la física falla.

Insiders

Personal con acceso privilegiado — administradores, técnicos, contratistas. El insider perfecto ya tiene las llaves del reino.

Next Data

Yo diria que... todavia no

¿Y entonces que podemos hacer?

Visibilidad y Defensa

Sauron, eres tu?

Herramientas de Monitoreo

A CCTV y Acceso Biometrico

- Monitoreo de acceso administrado y grabado para su revision
- Autorizacion de acceso administrado y protegido por identidad
- Autorizacion de acceso administrado al gabinete
- Registro el eventos

B Next Generation Firewall

- Generacion de perimetro de seguridad, en segmentos de cliente independientes (gubernamentales, peering, empresariales)
- Políticas IPS/IDS diferenciadas por perfil
- Aislamiento sin comprometer o exponer la red ni a otros clientes
- Inspeccion de trafico cifrado para evitar ocultamiento de ataques

C Anti-DDOS

- Detectar anomalías de tráfico vía análisis de comportamiento
- Automatizacion de medidas para descartar trafico malisioso
- Limpieza: se descarta tráfico malicioso, se inyectar tráfico legítimo
- Registrar el evento y genera alertas

D Control de Acceso

- Verificación de identidad y monitoreo
- Visibilidad total de dispositivos conectados
- Bloqueo de cuentas de acceso con comportamiento anomalo
- Registro de eventos

Next Data

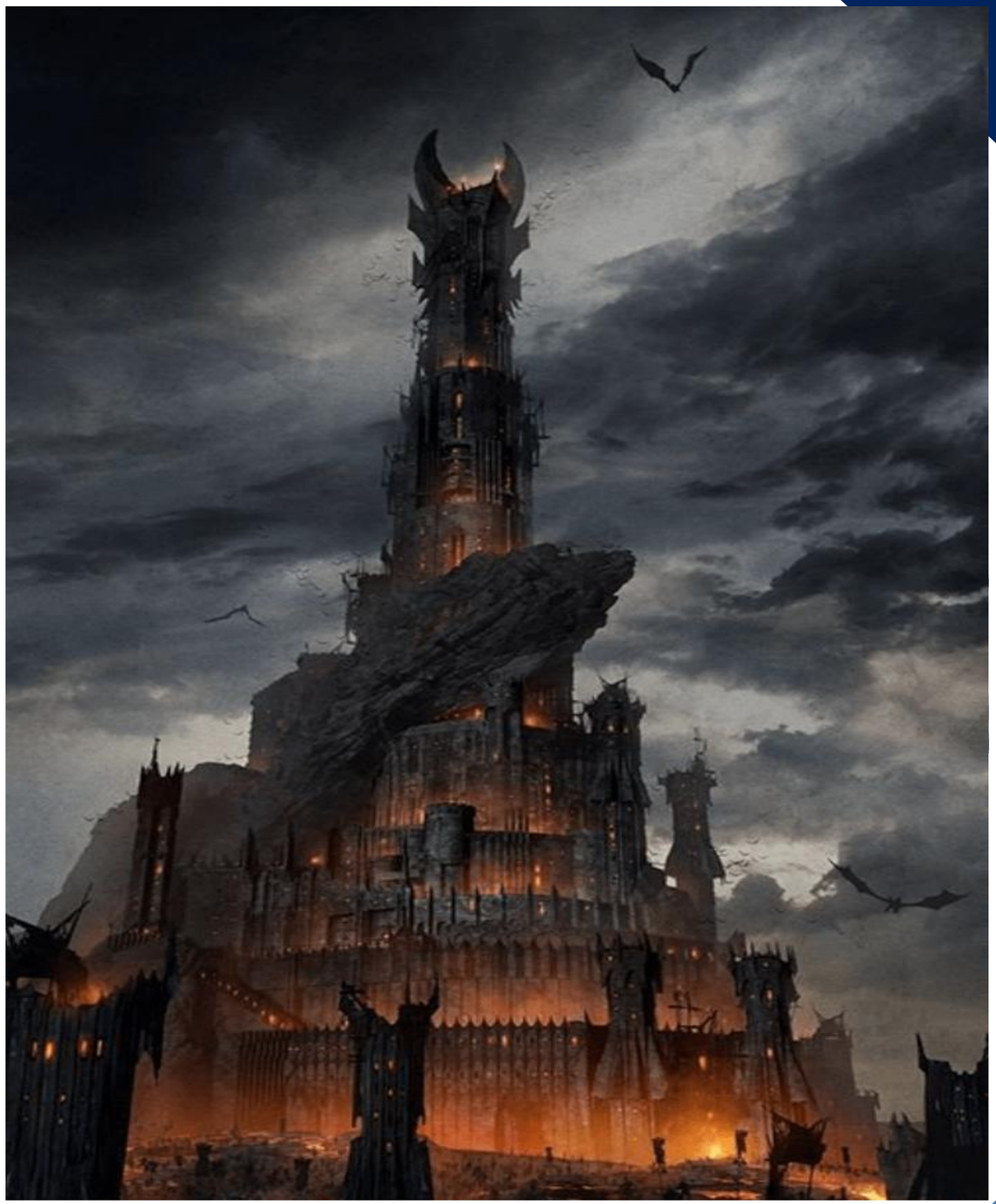
Herramientas de Monitoreo

El ojo que todo lo ve

SIEM & Analisis de Logs

- Correlación de eventos del ISP
- Detección de anomalías de tráfico en tiempo real
- Dashboards de amenazas por segmento de red
- Reportes de compliance y auditoría automatizados
- Alertas de comportamiento inusual de usuarios

Next Data



¿Entonces necesito construir una fortaleza?

NextData DC 1

La Comunidad del DataCenter

ENERGÍA

ENFRIAMIENTO

ENLACES

CIBERSEGURIDAD

Next Data

Conclusión

”El DataCenter es el Anillo Único de tu empresa — quien lo controla, controla todo”

Y Sauron sabe que no necesita un ejercito de Orcos, basta con una contraseña robada

¡Muchas Gracias!

Nuestros aliados:

Luis Fascinetto Leon

lfascinetto@nextdata.com.mx

442 437 1280

www.nextdata.com