COATL
CYBER DEFENSE

COATL EN ACCIÓN

Análisis de Ciberseguridad

www.nsk.com.mx/coatl

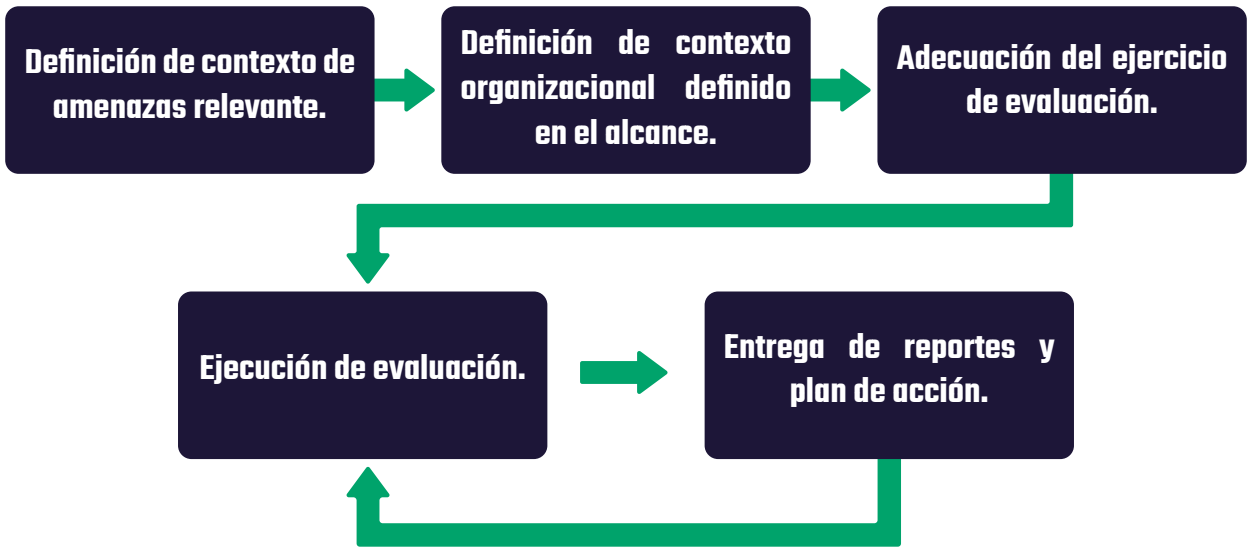
Análisis de Seguridad de COATL: Maximiza la Protección de tu Empresa

En **COATL**, nuestro enfoque de análisis de seguridad no solo identifica las vulnerabilidades presentes en tu infraestructura, sino que también proporciona recomendaciones precisas para mejorar la resiliencia de tu empresa ante ciberataques. A continuación, te mostramos cómo nuestras herramientas y metodologías pueden ayudarte a optimizar la seguridad y minimizar riesgos de manera eficiente.

Así lo hacemos

Análisis de Vulnerabilidades

En **COATL**, el análisis de vulnerabilidades es un proceso continuo que desafía la capacidad de una empresa para enfrentar amenazas latentes. Utilizando **muestras** e **indicadores de compromiso (IOC)**, identificamos en tiempo real los puntos fuertes y débiles de las medidas de seguridad, optimizando así las inversiones en ciberseguridad. Gracias a la visibilidad que obtenemos con este enfoque, es posible dirigir esfuerzos para maximizar el uso de la infraestructura de seguridad existente y aumentar la eficiencia operativa al reducir los riesgos de ataque.



Ejecución de Ataques como Servicio (On-demand)

Nuestro servicio de **Pentest as a Service** está diseñado para simular amenazas internas. Imagina a un atacante que logra evadir tus controles de seguridad; en ese momento, comienza la verdadera prueba. Desde dentro de la red, replicamos cómo un atacante se movería lateralmente, buscando vulnerabilidades y objetivos de alto valor como **bases de datos, credenciales, accesos y información confidencial**. El objetivo es identificar cualquier brecha que pueda comprometer tu empresa.

Métricas de Evaluación

Para guiar la remediación de vulnerabilidades, utilizamos **métricas de evaluación** basadas en diferentes parámetros que nos permiten priorizar acciones de seguridad:

1. **Estándares**: Utilizamos el sistema de puntuación **CVSS (Common Vulnerability Scoring System) versión 3** para calificar las vulnerabilidades de manera objetiva.
2. **Contexto organizacional**: Tomamos en cuenta la prioridad de los activos informáticos involucrados, así como el nivel de exposición de cada activo.
3. **Contexto de amenazas**: Evaluamos si la amenaza es un riesgo activo para la organización utilizando inteligencia de amenazas, casos de uso, vulnerabilidades explotadas, malware utilizado, y tácticas y procedimientos de ataque.

Análisis basado en Mitre Attack: Nuestro enfoque en el **Framework Mitre Attack** permite no solo evaluar la criticidad de una vulnerabilidad, sino también enfocar los esfuerzos donde tendrán un mayor impacto inmediato, dificultando la ejecución de ataques futuros.

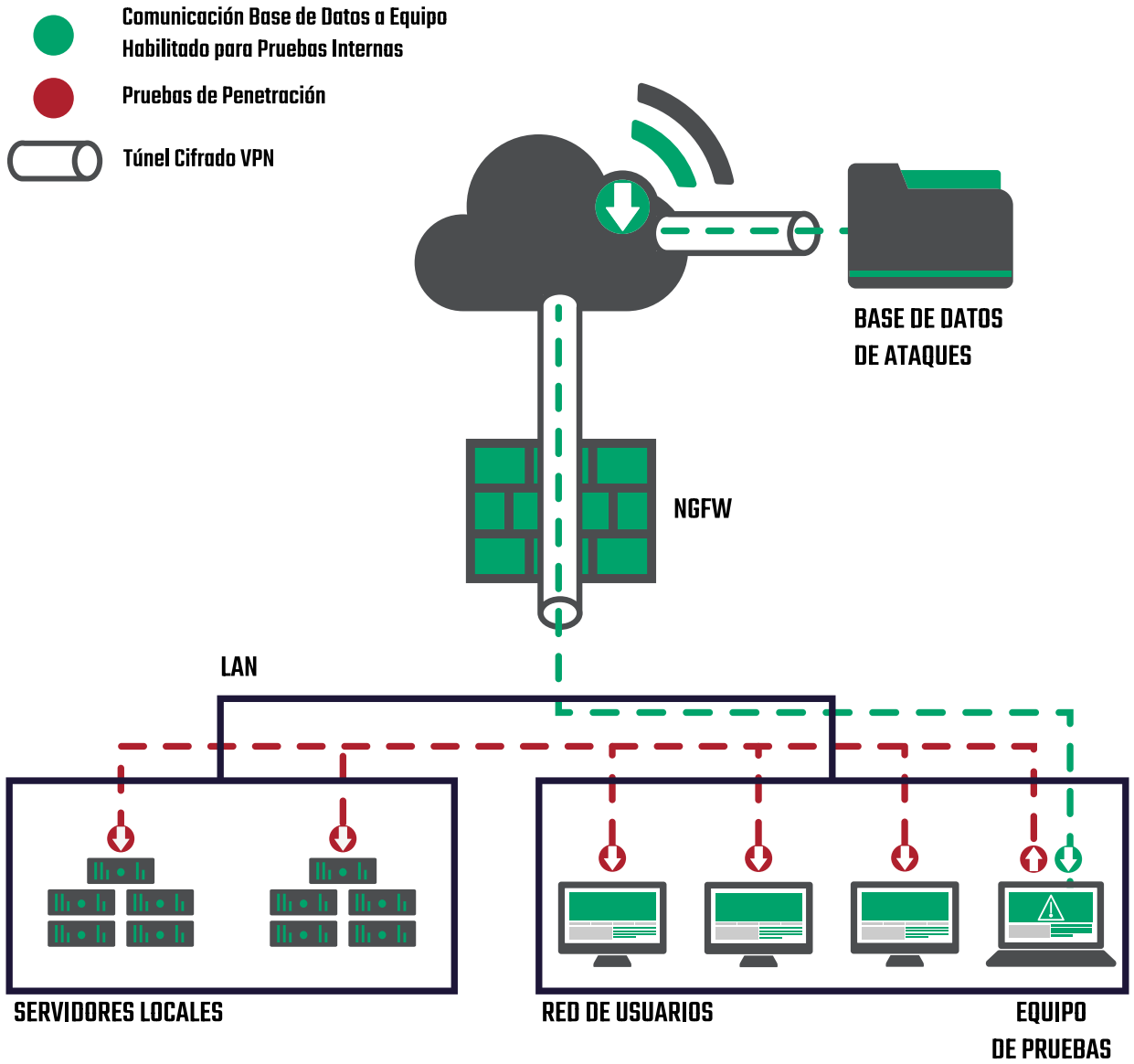
Severidad	Definición
Crítica	Ataques con un CVSS mayor a 9.0 y que el contexto organizacional y de amenazas priorice la remedación del riesgo.
Alta	Ataques con un CVSS entre 7.5 a 9.0 y que el contexto organizacional y de amenzas priorice la remediación del riesgo.
Media	Ataques con un CVSS entre 5.0 a 7.5 y cuya ejecución exitosa presente multiples condiciones de vulnerabilidad.
Baja	Técnicas que forman parte de la estructura de un ataque y puedan dar pie a amenazas, pero no causen daño por sí mismas.

Metodología de Evaluación

En **COATL**, nuestra metodología es aplicable tanto para **simulaciones de ataques y brechas** como para pruebas de intrusión en servicios. Esta flexibilidad nos permite adaptarnos a diferentes escenarios, siempre buscando los puntos de entrada más vulnerables en las redes de nuestros clientes.

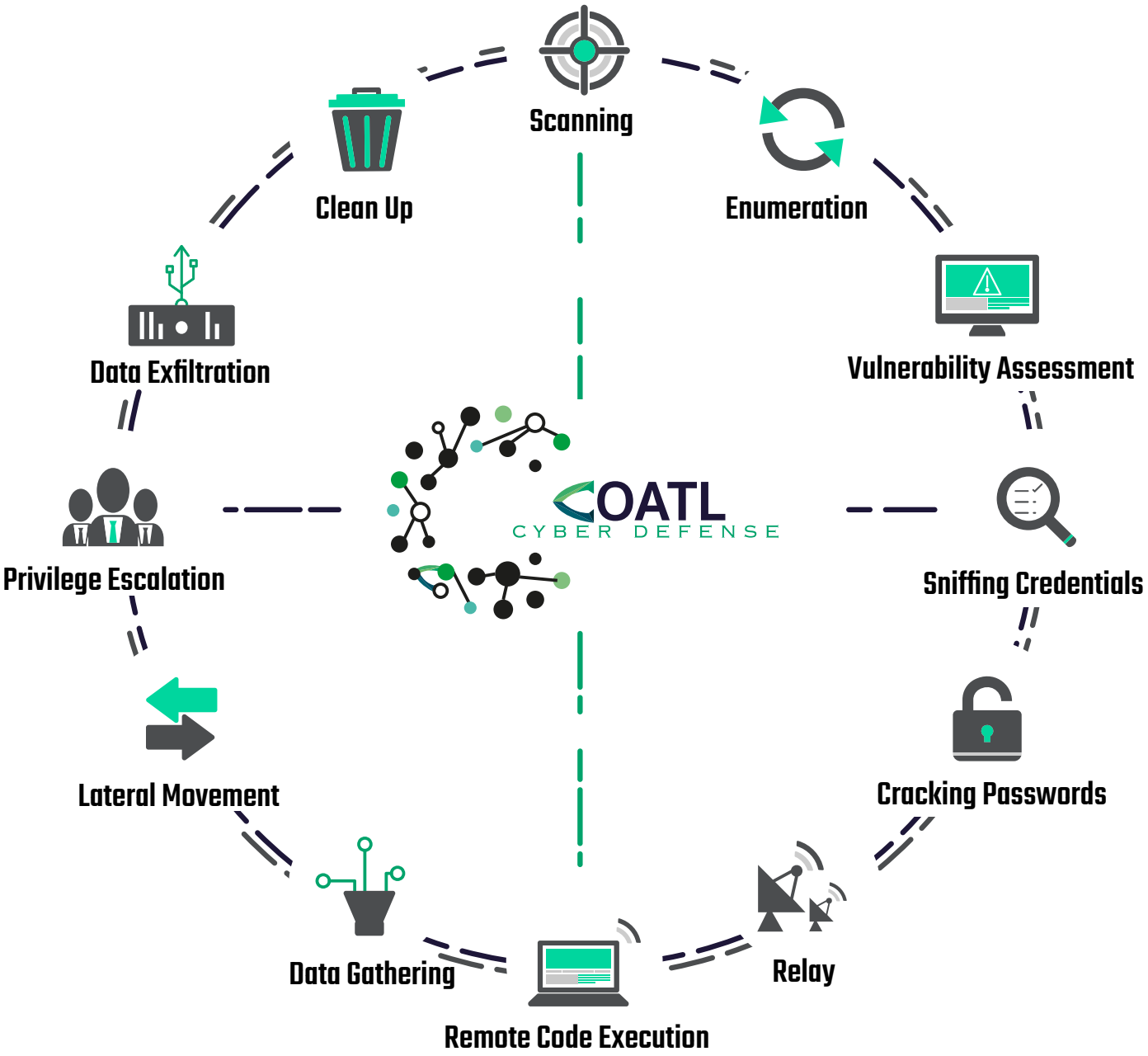
Metodología de Pentest como servicio

Con COATL podemos evaluar tanto tu superficie externa ante los ataques en internet así como podemos brindar la visibilidad interna ante escenarios de riesgo organizacional mediante los sensores de COATL simulando que somos un atacante dentro de tus premisas.



Metodología de Pentest como servicio

Apóyate en COATL y ve más allá de identificar vulnerabilidades en componentes y obtén la visibilidad del ciclo de ataque por la cual la amenaza tiene que cruzar para materializar el riesgo de dañar a la organización. Una vez que vemos el ciclo completo, es mucho más fácil lograr romper la cadena del ciber ataque.



COATL
CYBER DEFENSE

COATL EN ACCIÓN

Un análisis de ciberseguridad salvando a una empresa

Nota: Los datos aquí presentados son una representación real ejecutada como ejercicio sin ningún cliente real involucrado, cualquier parecido con la realidad es mera coincidencia.

COATL en Acción: El Análisis de Seguridad que Salva Empresas de Ataques Cibernéticos

En **COATL**, nos especializamos en detectar vulnerabilidades y áreas de oportunidad críticas en las infraestructuras de nuestros clientes, y hemos ayudado a empresas a evitar ataques cibernéticos devastadores. Este reporte que te presentamos es el resultado de un análisis real que realizamos para uno de nuestros clientes, donde identificamos fallos de seguridad que podrían haber llevado a un compromiso total del dominio. A través de este caso, queremos mostrarte cómo nuestro enfoque puede generar valor para tu organización al mejorar su resiliencia frente a ataques cibernéticos.

Nuestro análisis reveló varias vulnerabilidades críticas que podían haber sido explotadas para comprometer completamente el entorno de red y dominio del cliente. A continuación, te presentamos un resumen de los hallazgos más importantes y enfocado a un vector de ataque mediante como 1 sola vulnerabilidad puede desencadenar todo el camino de ataque hasta la toma de control de Hosts o servidores:

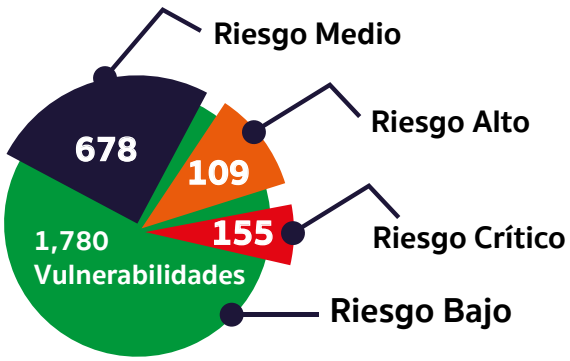
Started	Sep 13, 2024, 7:38 PM UTC	Initiated by	José Madero	Hosts Assessed	6.5K
Completed	Sep 17, 2024, 2:50 AM UTC	For client	Producciones S.A De C.V		
Duration	3d 7h 11m				

332
Vías de ataque explotadas

1,780
Vulnerabilidades encontradas

628
Credenciales comprometidas

98
Hosts comprometidos



1. Explotación de Vulnerabilidad Crítica en librería vulnerable en Apache Webserver

El análisis de COATL identificó y explotó debilidades que permitieron comprometer el dominio del cliente. La vulnerabilidad más grave fue en librería vulnerable en Apache Webserver, que afectaba a **261 aplicaciones**, lo que exponía datos sensibles. Esta vulnerabilidad fue explotada en **262 rutas de ataque** que llevaron a una exposición de ransomware y otros impactos graves.

2. Filtrado de base de datos con hashes de credenciales y Pass the Hash

Detectamos la vulnerabilidad **base de datos con hashes de credenciales. (Acceso critico a recursos confidenciales de sistemas Windows)** en **45 hosts**. Esta vulnerabilidad permitía a los atacantes acceder a credenciales almacenadas localmente en memoria y archivos de sistemas Windows y extraer dicha información aun "protegida" por mecanismos de Hash NTLM.

3. Credenciales Locales y de Dominio Compartidas

Una debilidad más permitía a los atacantes pivotar desde una única máquina hacia todo el dominio. COATL detectó que la **credencial del administrador del dominio** fue reutilizada en **25 sistemas** diferentes, lo que exponía toda la infraestructura al compromiso del directorio activo.

Impacto de las Vulnerabilidades Conocidas y la Falta de Seguridad en Endpoints

COATL identificó que 72 hosts fueron comprometidos a través de vulnerabilidades explotadas, reconocidas por organismos internacionales que auditan controles de ciberseguridad, incluidas controladoras de dominio. Además, logramos adquirir 160 credenciales utilizando métodos de volcado de credenciales, lo que revela una falta significativa de controles de seguridad en los dispositivos finales.

Para proteger la infraestructura de manera efectiva y evitar futuras brechas, estas son las acciones clave que recomendamos al cliente tomar:

1. **Mitigar la reutilización de credenciales:** COATL comprometió a 136 usuarios distintos del dominio debido a la reutilización de contraseñas. Para prevenir esto, recomendamos actualizar tu política de contraseñas según la NIST Special Publication 800-63b, asegurando contraseñas con una longitud mínima de 12 caracteres y fomentando la rotación regular de las mismas.

2. **Parches de vulnerabilidades críticas:** COATL explotó vulnerabilidades conocidas por organismos internacionales que auditan controles de ciberseguridad en 72 hosts, incluidos controladores de dominio. Es fundamental corregir o mitigar rápidamente estas vulnerabilidades conocidas para dificultar que los atacantes obtengan acceso inicial o se muevan lateralmente dentro de tu red.

3. **Fortalecer la seguridad en los endpoints:** COATL recolectó 160 credenciales mediante el ataque a base de datos con hashes de credenciales (volcado de credenciales del sistema operativo), lo que expone fallos en la protección de los endpoints. Implementar una solución de EDR (Endpoint Detection and Response) en cada endpoint y configurarla adecuadamente es esencial para evitar que los atacantes utilicen métodos comunes de recolección de credenciales, como el volcado de LSASS, LSA y SAM (los explotados en el presente ejercicio de COATL).

¿Qué tan segura es tu ciberseguridad?

Este análisis real demuestra cómo una empresa puede quedar expuesta a ataques cibernéticos si no se toman las medidas correctas a tiempo. Si quieres mejorar tu postura de seguridad y proteger tus credenciales, contacta a COATL para realizar un análisis exhaustivo de seguridad. No dejes que las vulnerabilidades te sorprendan, actúa antes de que sea demasiado tarde!

COATL
CYBER DEFENSE

Contacta a COATL hoy mismo para proteger tu empresa:

Correo electrónico: contacto@nsk.com.mx

Visita nuestro sitio web: www.nsk.com.mx/coatl