E

HASH

IPs

DOMINIOS

E D F C Z P

ARTEFACTOS DE RED/ALOJADOS

HERRAMIENTAS

TTPs

P E Z O L C F T D

1
2
3
4
5
6
7
8
9
10
11

COACH INNOVATIVO
JUAN CARLOS PARIS

@CoachInnovativo

Modelo Snellen de Indicadores en Ciberseguridad

Introducción

El modelo "Modelo Snellen de Indicadores en Ciberseguridad" es una representación innovadora que adapta la tradicional Pirámide del Dolor de David Bianco a un formato visual inspirado en la cartilla de Snellen, utilizada en exámenes de agudeza visual. Este enfoque busca facilitar la comprensión del impacto y la dificultad de detección de distintos indicadores de compromiso (IoCs) en un contexto de ciberseguridad, utilizando una escala visual intuitiva.

Esta adaptación fue creada por Juan Carlos Paris.

Objetivo

El objetivo principal de este modelo es proporcionar una herramienta pedagógica que permita a profesionales y estudiantes de ciberseguridad entender cómo los distintos tipos de indicadores afectan las operaciones de los atacantes y la defensa de las organizaciones. La escala visual refuerza la idea de que lo más grande y visible (fácil de detectar) es también lo más sencillo de cambiar por los atacantes, mientras que lo más pequeño y difícil de ver representa lo más impactante y complejo de modificar.

Estructura del Modelo

La cartilla se organiza de forma descendente, comenzando con letras grandes y terminando con letras pequeñas, para representar la dificultad creciente en la detección de los diferentes indicadores. Cada nivel corresponde a un tipo de indicador de compromiso (IoC):

1. Letras más grandes: Hashes de archivos

- **Características:** Son los indicadores más fáciles de detectar y cambiar. Los atacantes solo necesitan recompilar o modificar ligeramente los archivos.
- **Impacto:** Mínimo.

- **Dificultad de detección:** Muy fácil de ver y reconocer.

2. Segunda fila: Direcciones IP

- **Características:** Moderadamente fáciles de cambiar. Los atacantes pueden utilizar servicios de anonimización o cambiar servidores.
- **Impacto:** Limitado.
- **Dificultad de detección:** Relativamente fácil de identificar.

3. Tercera fila: Nombres de dominio

a. **Características:** Requieren algo más de esfuerzo para cambiar, aunque los atacantes pueden emplear algoritmos de generación de dominios (DGA).

b. **Impacto:** Moderado.

c. **Dificultad de detección:** Moderada, requiere análisis especializado.

4. Fila intermedia: Artefactos de red

a. **Características:** Incluyen patrones específicos en el tráfico de red. Más difíciles de alterar porque afectan la infraestructura de los atacantes.

b. **Impacto:** Significativo.

c. **Dificultad de detección:** Más difícil de observar, requiere herramientas avanzadas de monitoreo.

5. Fila pequeña: Herramientas utilizadas para el ataque

a. **Características:** Incluyen las herramientas específicas que los atacantes emplean para llevar a cabo sus operaciones, como software de explotación, scripts personalizados o herramientas comerciales de prueba de penetración mal utilizadas.

b. **Impacto:** Alto, ya que estas herramientas son esenciales para la ejecución de los ataques y reemplazarlas puede ser complejo y

costoso para los atacantes.

c. **Dificultad de detección:** Difícil de identificar, requiere análisis forense detallado.

6. Letras más pequeñas: Tácticas, Técnicas y Procedimientos (TTPs)

a. **Características:** Reflejan el modus operandi de los atacantes. Cambiarlos requiere rediseñar partes significativas de su infraestructura o estrategias.

b. **Impacto:** Máximo, ya que cambiar estas herramientas requiere rediseñar partes significativas de su infraestructura o estrategias.

c. **Dificultad de detección:** Extremadamente difícil, involucra un entendimiento profundo del comportamiento del atacante.

Elementos Visuales del Modelo

El diseño incluye:

- **Letras grandes y pequeñas:** Simulan la escala de detección y dificultad. Lo fácil de detectar está en letras grandes (ejemplo: "HASHES"), mientras que lo más complejo aparece en letras pequeñas (ejemplo: "TTPs").
- **Colores:** Líneas verdes y rojas refuerzan la progresión de facilidad a dificultad.
- **Leyendas:** Breves explicaciones sobre cada nivel de la escala.

Beneficios

- **Pedagogía:** Simplifica conceptos técnicos mediante analogías visuales.
- **Adaptabilidad:** Puede ser utilizado en capacitaciones, presentaciones y formación académica.
- **Impacto visual:** Refuerza el mensaje a través de un diseño familiar e intuitivo.

Importancia del Modelo Snellen de Indicadores en Ciberseguridad

Este modelo es crucial porque transforma la **Pirámide del Dolor** en una representación visual más intuitiva, facilitando su comprensión y aplicación en ciberseguridad. Su importancia radica en varios aspectos clave:

1. Mejora la Pedagogía y la Enseñanza en Ciberseguridad

- Al utilizar la cartilla de Snellen como analogía, el modelo facilita el aprendizaje de los **indicadores de compromiso (IoCs)** en diferentes niveles de detección.
- Permite a estudiantes y profesionales **asimilar el concepto de detección y evasión** de amenazas de una manera más clara y estructurada.

2. Relación Directa con la Detección y Respuesta a Amenazas

- Ayuda a los equipos de seguridad a **entender qué tipos de indicadores deben priorizarse** en su detección y análisis.
- Refuerza la idea de que **bloquear hashes y direcciones IP es útil, pero no suficiente** para detener amenazas avanzadas.

3. Refuerza el Enfoque en Inteligencia de Amenazas

- Al destacar los **TTPs (Tácticas, Técnicas y Procedimientos)** como el nivel más difícil de detectar pero el más valioso para la defensa, el modelo **promueve una visión proactiva** en ciberseguridad.
- Ayuda a equipos SOC y analistas de inteligencia a **invertir más esfuerzo en el análisis de patrones de comportamiento** en lugar de depender solo de IoCs de baja durabilidad.

4. Aplicabilidad en Empresas y Estrategias de Ciberdefensa

- Este modelo puede **guiar a las organizaciones** en la construcción de estrategias de detección basadas en la madurez de su defensa.
- Sirve como una herramienta para evaluar la **efectividad de los controles de seguridad** y definir **prioridades en la inversión tecnológica**.

5. Innovación en Representación de Datos de Seguridad

- Moderniza el enfoque clásico de la **Pirámide del Dolor**, haciéndolo más accesible para audiencias no técnicas.

- Proporciona una herramienta visual poderosa para presentaciones, capacitaciones y reportes estratégicos.

Reflexiones Finales

El modelo **"Modelo Snellen de Indicadores en Ciberseguridad"** es una herramienta poderosa para enseñar y entender la relación entre la dificultad de detección de indicadores y el impacto en los atacantes. Este enfoque no solo moderniza la Pirámide del Dolor, sino que también hace que sus principios sean más accesibles y comprensibles para una audiencia amplia.

Este modelo no solo representa una innovación visual, sino que también **fortalece la comprensión y estrategia de detección de amenazas** en el mundo de la ciberseguridad. Su aplicación puede mejorar la respuesta ante incidentes, el desarrollo de inteligencia de amenazas y la educación en el campo de la seguridad informática.

Glosario de términos técnicos

- **Análisis forense:** Proceso de investigación digital para identificar, analizar y reconstruir actividades maliciosas en un sistema.
- **Artefacto de red:** Elemento dentro del tráfico de red que puede ser indicativo de actividad sospechosa o maliciosa.
- **Dirección IP:** Identificador numérico de un dispositivo en una red.
- **Hash de archivo:** Código único generado a partir del contenido de un archivo que permite identificar cambios o alteraciones.
- **Herramientas de ataque:** Software o scripts utilizados por los atacantes para comprometer sistemas.
- **IoC (Indicator of Compromise):** Indicador de compromiso, cualquier artefacto que pueda indicar una actividad maliciosa en un sistema o red.
- **Nombre de dominio:** Identificación textual de una dirección IP, utilizada en Internet.
- **Tácticas, Técnicas y Procedimientos (TTPs):** Métodos y estrategias empleadas por los atacantes para ejecutar ataques y evadir detección.

Derechos de Autor ©