2023

Modelo Diamante

Análisis de una Intrusión

Ing. Rubén Bernardo Guzmán Mercado

2023

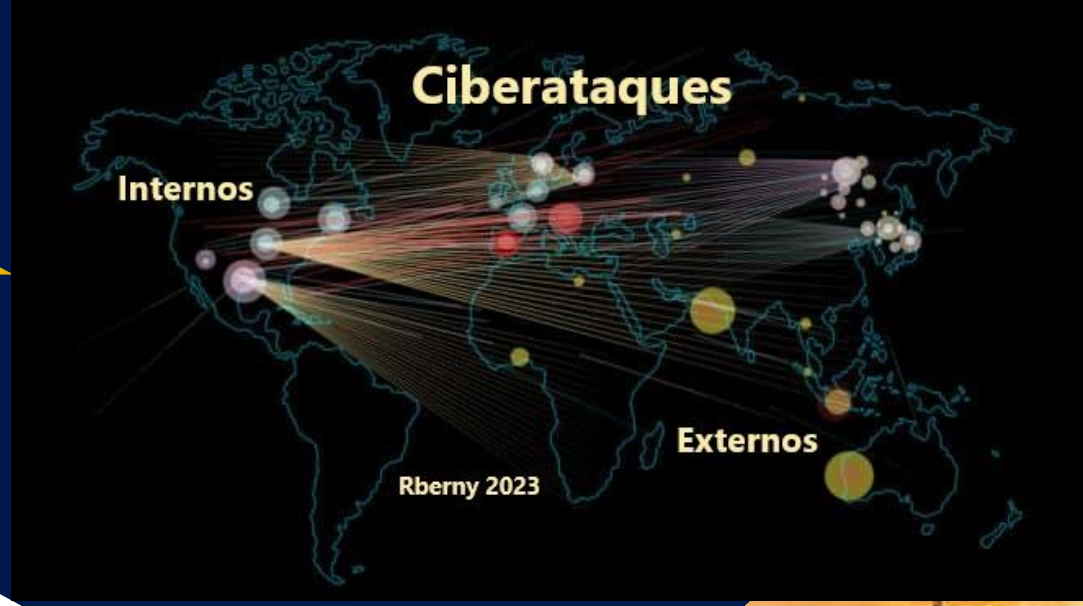
Rberny

El tema de ciberseguridad es muy amplio, cualquier intrusión en una red requiere un análisis exhaustivo para brindar a los equipos de seguridad inteligencia cibernética sobre diferentes amenazas y para ayudar a frustrar ataques futuros similares.

Ing. Rubén Bernardo Guzmán Mercado

- Hoy por hoy, las organizaciones utilizamos herramientas como SIEM, EDR, IDS, Firewall, etc. para ayudar a identificar amenazas y alertar a medida que ocurren, sin duda estas herramientas son como grandes armas en nuestro arsenal, de uso estratégico contra los malos actores, en algunas de ella hablamos de Inteligencia artificial.

- La Inteligencia de amenazas, por su parte es cierto que los ciber criminales, siguen sus propias normas y procesos para elaborar un ataque, de igual manera nosotros la utilizamos con algunos marcos para ayudar en nuestro proceso de análisis de intrusiones, no me gusta generalizar, no obstante, considero que la mayoría que estamos aquí y que esté relacionado con la ciberseguridad debe haberse topado con el término KILL CHAIN.



- Sabemos que el éxito de cualquier equipo de seguridad depende de qué tan rápido responda a las amenazas, qué tan eficientemente las detenga y también qué tan bien las prevenga en el futuro y para ello les mostraré básicamente el modelo diamante de análisis de intrusiones
- Hasta la fecha, piratas informáticos y personas internas maliciosas continúan infiltrándose y atacando a las organizaciones, mientras los equipos de seguridad trabajan arduamente para detectar y prevenir sus intenciones maliciosas, y las preguntas siguen siendo las mismas **¿quién?, ¿qué?, ¿cuándo?, ¿dónde?, ¿por qué? y ¿cómo?**

Axiomas del modelo de diamante

Incluye 7 axiomas sobre eventos de intrusión, adversarios y víctimas

1. Por cada evento de intrusión existe un adversario que da un paso hacia un objetivo previsto utilizando una capacidad de la infraestructura contra una víctima para producir un resultado.
2. Existe un conjunto de adversarios (internos, externos, individuos, grupos y organizaciones) que buscan comprometer los sistemas o redes informáticas para promover sus intenciones y satisfacer sus necesidades.
3. Cada sistema y, por extensión, cada activo de la víctima, tiene vulnerabilidades y exposiciones.
4. Cada actividad maliciosa contiene dos o más fases que deben ejecutarse exitosamente y sucesivamente para lograr el resultado deseado.
5. Cada evento de intrusión requiere que uno o más recursos externos sean satisfechos antes de tener éxito.
6. Siempre existe una relación entre el Adversario y su(s) Víctima(s), incluso si es distante, fugaz o indirecta.
7. Existe un subconjunto del conjunto de adversarios que tienen la motivación, los recursos y las capacidades para mantener efectos maliciosos durante un período de tiempo significativo contra una o más víctimas mientras se resisten a los esfuerzos de mitigación. Las relaciones entre adversario y víctima en este subconjunto se denominan relaciones de adversario persistentes.

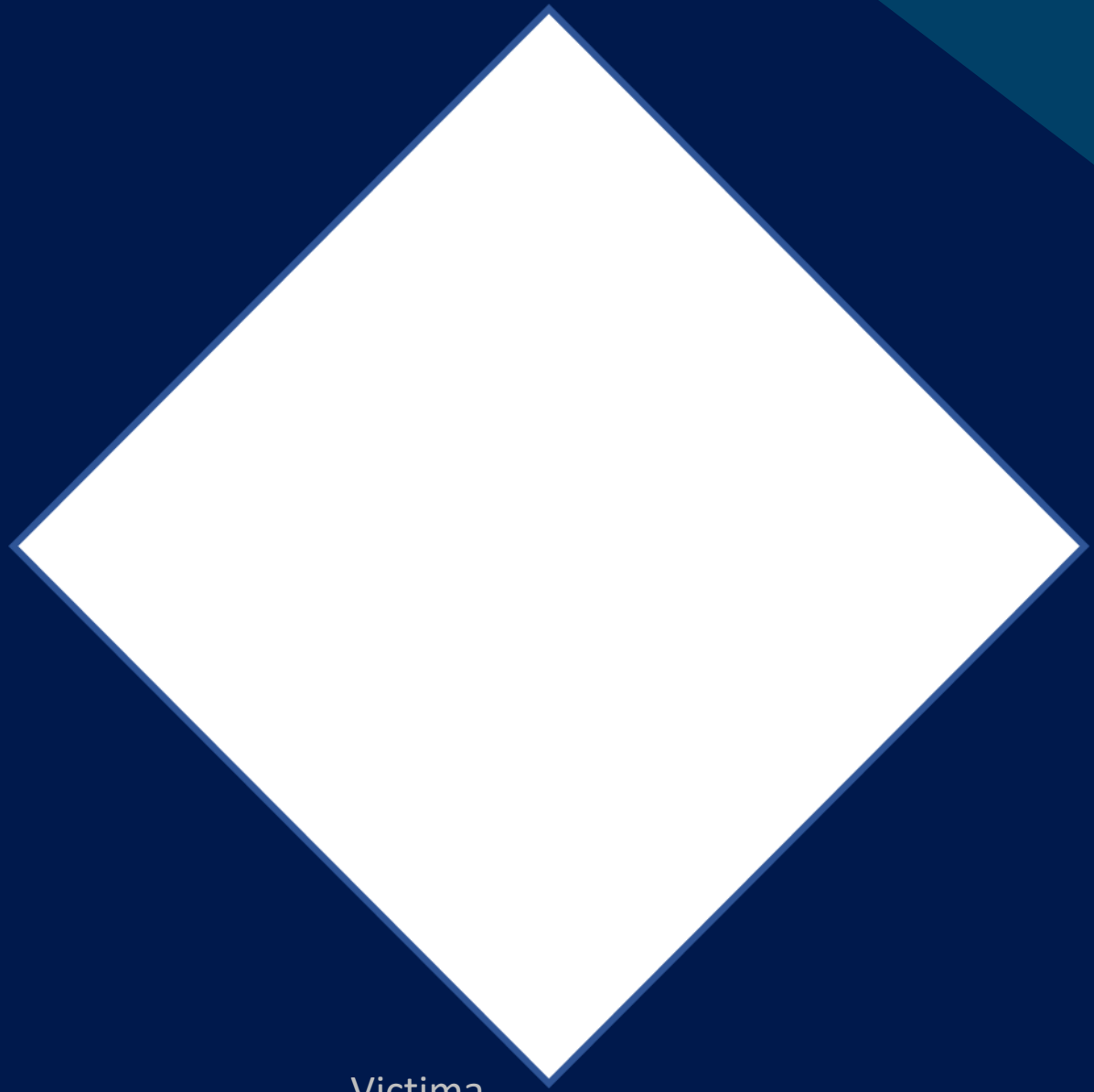
Su principio

- El modelo Diamante para el análisis de intrusiones responde a estas preguntas proporcionando información y lleva a los defensores hacia una visión más amplia de la mitigación estratégica. Se debe dar mucha atención a este modelo delicado, simple pero poderoso para el análisis de intrusiones que encaja perfectamente entre Kill chain y Att&ck, estoy seguro que este modelo les resultara peculiar porque analiza la victimología y también vincula las capacidades del atacante con la infraestructura del ataque, hace que la mitigación sea efectiva y el costo de operación para el adversario sea mayor.

Modelo Diamante

Pasos de un atacante

1. Reconocimiento
2. Armamento
3. Entrega
4. Explotación
5. Instalación
6. Comando y control
7. Acciones por Objetivo



Modelo Diamante

Adversario

Infraestructura

$$\mathbf{E_{vertices}} = \{Adversary, Infrastructure, Capability, Victim\}$$

Capacidad

Victima

Modelo Diamante

Adversario

Social y/o Política

Usos

Desarrollos

Infraestructura

Despliegue

Capacidad

Conectarse a

Tecnología

Métodos

Exploits

Victima

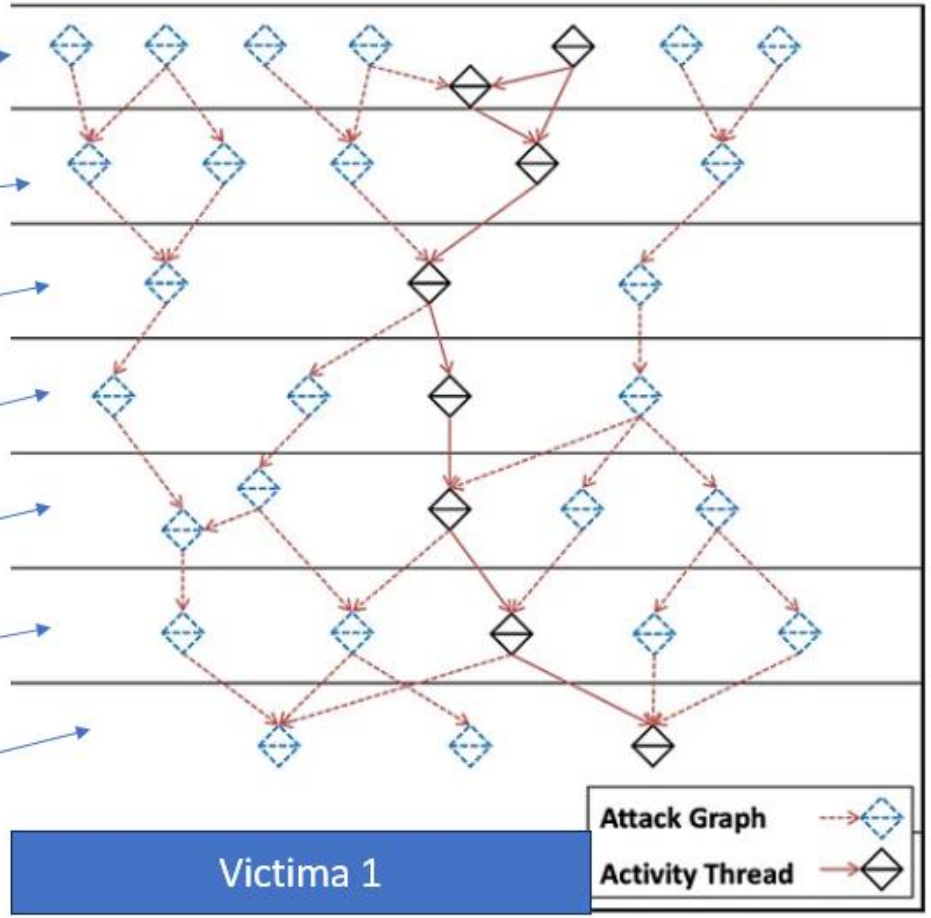
$$\mathbf{E}_{edges} = \{\{Adversary, Capability\}, \{Adversary, Infrastructure\}, \{Infrastructure, Capability\}, \{Infrastructure, Victim\}, \{Capability, Victim\}\}$$

$$\langle Victim, Confidence_{victim}\rangle = \langle\langle Organization, Confidence_{organization}\rangle, \langle HostIPAddress, Confidence_{IP}\rangle, \langle Hostname, Confidence_{Hostname}\rangle, \langle Application, Confidence_{Application}\rangle, \langle TCPPort, Confidence_{TCPPort}\rangle\rangle$$

$$\boldsymbol{E} = \langle\langle Adversary, Confidence_{adversary}\rangle, \langle Capability, Confidence_{capability}\rangle, \langle Infrastructure, Confidence_{infrastructure}\rangle, \langle Victim, Confidence_{victim}\rangle, \langle Timestamp_{start}, Confidence_{timestamp_{start}}\rangle, \langle Timestamp_{end}, Confidence_{timestamp_{end}}\rangle, \langle Phase, Confidence_{phase}\rangle, \langle Result, Confidence_{result}\rangle, \langle Direction, Confidence_{direction}\rangle, \langle Methodology, Confidence_{methodology}\rangle, \langle Resources, Confidence_{resources}\rangle\rangle$$

Modelo Diamante

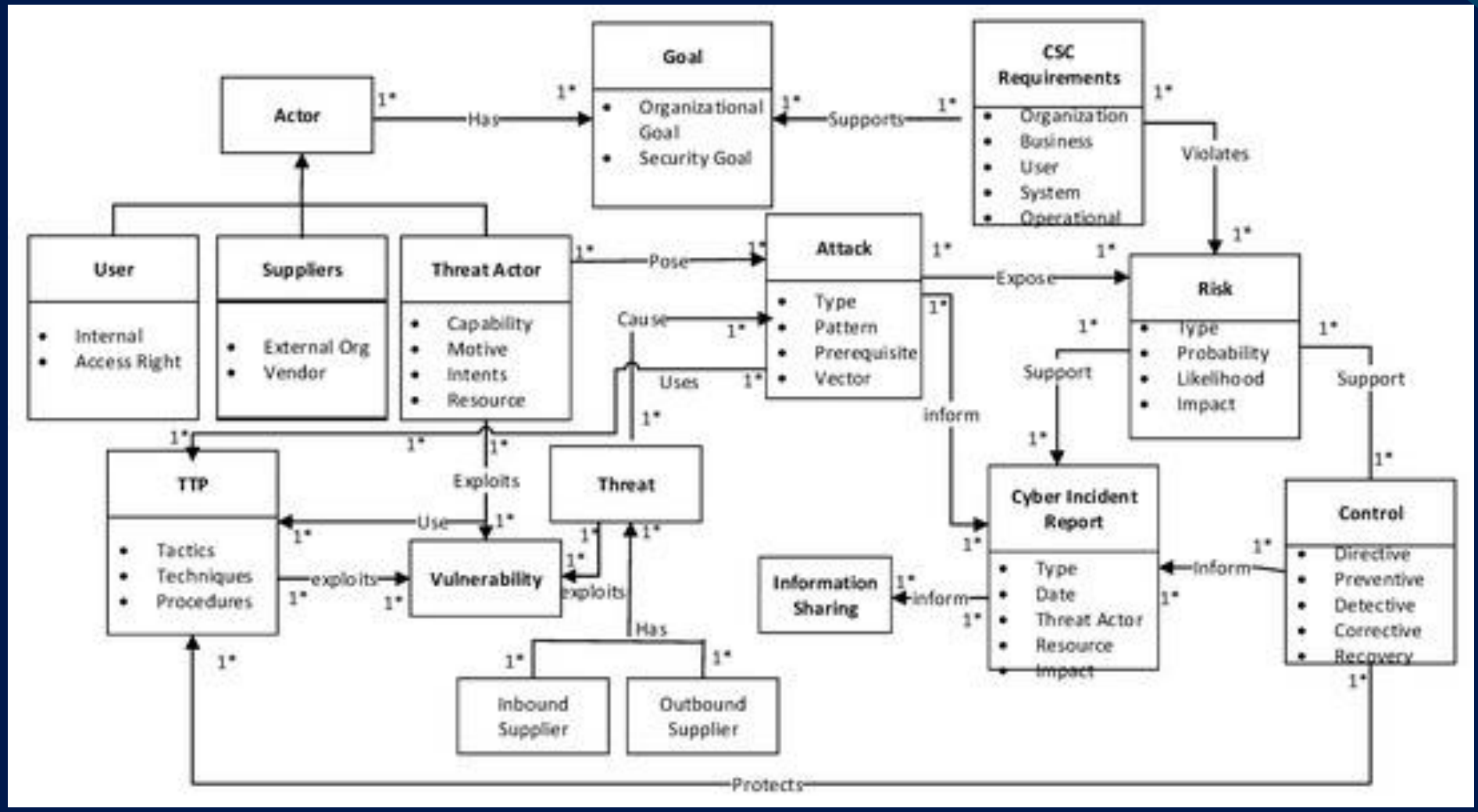
Fases de un atacante:
Reconocimiento
Armamento
Entrega
Explotación
Instalación
Comando y control (C2)
Acciones por Objetivo



Diamond Model activity-attack graph Ing. Rubén Bernardo Guzman Mercado

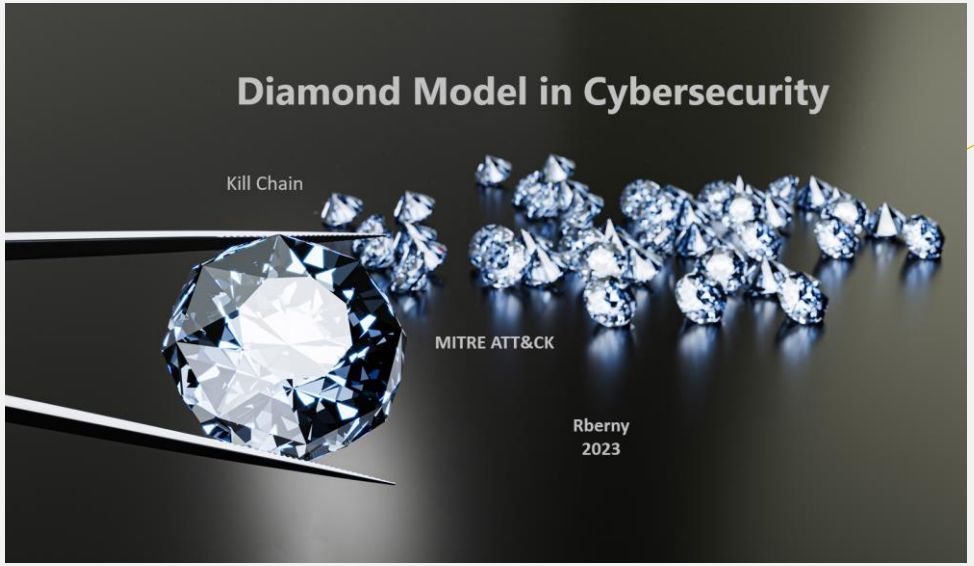
Modelo Diamante

Causa y Efecto



Muchas gracias a todos

María Carla Silveira Taboadela



Comuníquense conmigo

En LinkedIn o en mi sitio web:
Rberny.com