

Introducción a la inteligencia sobre amenazas cibernéticas

Tarea 1: Introducción

Introducción

En esta sala, se presentará la inteligencia de ciberamenazas (CTI) y los diversos marcos utilizados para compartir inteligencia. Como analistas de seguridad, la CTI es fundamental para investigar e informar sobre ataques de adversarios con las partes interesadas de la organización y las comunidades externas.

Objetivos de aprendizaje

- Los fundamentos de CTI y sus distintas clasificaciones.
- El ciclo de vida seguido para implementar y utilizar inteligencia durante las investigaciones de amenazas.
- Marcos y estándares utilizados en la distribución de inteligencia.

Módulo de inteligencia sobre amenazas cibernéticas

Esta es la primera sala de un nuevo módulo de Inteligencia sobre Ciberamenazas. El módulo también contendrá:

- Herramientas de inteligencia de amenazas
- YARA
- OpenCTI
- MISP

P: ¡Listo para comenzar!

R: No se necesita respuesta

Tarea 2: Inteligencia sobre amenazas cibernéticas

P1: ¿Qué significa CTI?

R1: Cyber Threat Intelligence / Inteligencia de Amenazas Cibernéticas

P2: ¿Bajo qué clasificación de inteligencia de amenazas se encontrarían direcciones IP, hashes y otros artefactos de amenazas?

R2: Technical Intel / Información técnica

Tarea 3: Ciclo de vida de CTI

P1: ¿En qué fase del ciclo de vida de CTI se convierten los datos en formatos utilizables a través de la clasificación, la organización, la correlación y la presentación?

R1: Processing / Procesamiento

P2: ¿Durante qué fase los analistas de seguridad tienen la oportunidad de definir las preguntas para investigar los incidentes?

R2: Direction / Dirección

Tarea 4: Estándares y marcos de CTI

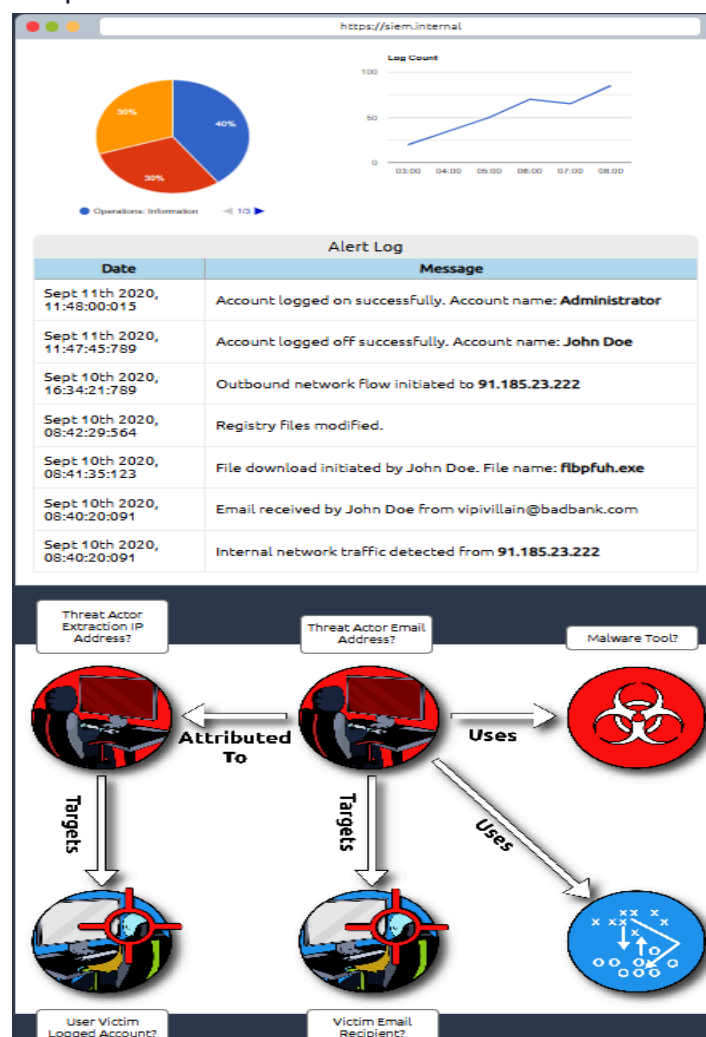
P1: ¿Qué modelos de compartición admite TAXII?

R1: Collection and Channel / Colección y Canal

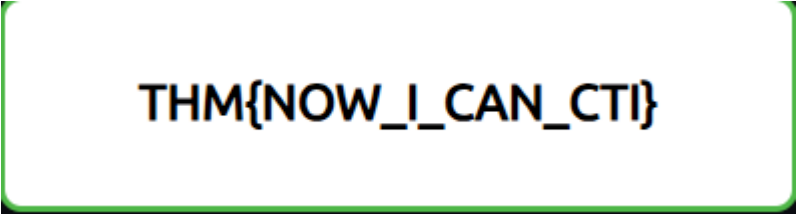
P2: Cuando un adversario ha obtenido acceso a una red y está extrayendo datos, ¿en qué fase de la cadena de ataque se encuentra?

R2: Actions on Objectives / Acciones sobre Objetivos

Tarea 5: Análisis práctico



Threat Actor Extraction IP Address: 91.185.23.222
Threat Actor Email Address: vipivillain@badbank.com
Malware Tool: flbpfeh.exe
User Victim Logged Account: Administrator
Victim Email Recipient: John Doe



THM{NOW_I_CAN_CTI}

P1: ¿Cuál era la dirección de correo electrónico de origen?

R1: vipivillain@badbank.com

P2: ¿Cuál era el nombre del archivo descargado?

R2: flbpfeh.exe

P3: Después de crear el perfil de amenaza, ¿qué mensaje recibe?

R3: THM{NOW_I_CAN_CTI}

 **LinkedIn:** <https://www.linkedin.com/in/mateo-rodr%C3%ADguez-suar-202695249/>

 **GitHub:** <https://github.com/MaateoSuar>