Counter Threat Intelligence BOOTCAMP

/RootedCON 2018

/Rooted®

Introducción

Las amenazas en Internet han evolucionado de manera que ya no se producen apenas ataques desde un punto de vista clásico hoy en día, es decir atacando directamente la infraestructura expuesta a internet.

Las amenazas actuales utilizan capas de infraestructura, productos y servicios capaces de evadir los controles de seguridad tradicionales, como los productos basados en firmas o en heurísticas clásicas.

El enfoque actual de seguridad de la información debe evolucionar hacia un modelo más agresivo y dinámico basado en el conocimiento profundo de este tipo de amenazas para defender nuestra infraestructura e información.

Objetivos

El bootcamp impartido por el equipo de **CounterThreat.IO** no pretende ser un manual académico sobre fundamentos de seguridad y amenazas. No busca ceñirse a una estructura rígida, sino ir evolucionando desde una visión básica, hacia un entendimiento más profundo de las amenazas y presentar distintas técnicas que permitan a los asistentes estar un paso por delante sobre las amenazas en Internet.

CounterThreat.IO ofrece a los asistentes acceso a una nueva mentalidad a la hora de tratar la inteligencia y hacer frente a las amenazas emergentes.

Objetivos

Esta visión analítica proporciona a los analistas y responders de la capacidad de detectar y defenderse contra las nuevas amenazas en Internet, mientras que todavía están madurando.

Finalmente el objetivo de **CounterThreat.IO** es el de proporcionar metodologías prácticas y proactivas que den visibilidad sobre las nuevas amenazas sofisticadas y evasivas.

Contenido

Contenidos

Durante el Bootcamp se trabajará sobre una misma metodología pero con diferentes entornos de trabajo.

Los siguientes puntos pueden variar en función de la dinámica del grupo de trabajo.

Todos los asistentes irán al mismo ritmo y no se avanzará en los temas hasta que el grupo haya cumplido en sus totalidad los objetivos de cada uno de los puntos.

Contenidos

Durante el Bootcamp se trabajará sobre una misma metodología pero con diferentes entornos de trabajo.

Los siguientes puntos pueden variar en función de la dinámica del grupo de trabajo.

Todos los asistentes irán al mismo ritmo y no se avanzará en los temas hasta que el grupo haya cumplido en sus totalidad los objetivos de cada uno de los puntos.

Contenidos

Threat Intelligence

- Conoce a tu enemigo
- Teoría de las amenazas
- Tipos de amenazas
- Evolución de las amenazas
- Estado actual de las amenazas
- Modelado de amenazas
- Ciclo de vida de las amenazas
- Malware Research
- Intelligence Research
- Prevención de fraude, IR, APT's

Intelligence Research

- Introducción al mundo Underground
- Open Source Intelligence
- Intelligence Crawling
- Malware Crawling
- Monitorización de actores
- Análisis con grafos
- Monitorización de campañas
- Monitorización de Botnets
- Extracción de indicadores IOC's
- Del periódico a virustotal

Contenidos

Intell & DFIR

- Intel focused DFIR
- Kill Chain model
- Diamond model
- Caracterización de malware
- Generando tu propia intel
- Estructurando conocimiento de adversarios

CounterOPs

- Conceptos básicos
- Metodología
- Offensive Tracking
- Atacando infraestructuras de amenazas
- Workshops y evaluación final°

Sobre los formadores

Jorge Capmany

Jorge es líder técnico de un equipo de detección y respuesta en una organización centroeuropea, donde desempeña labores relacionadas con la respuesta a incidentes, threat intelligence y detección de intrusiones.

En sus ratos libres, Jorge se involucra con la comunidad DFIR y de analistas de malware, a distintos niveles, ya sea organizando eventos, o contribuyendo a otras conferencias y/o comunidades (DFRWS, ROOTEDCON, Malcon, etc.).

Es miembro fundador de MLW.RE, una organización sin ánimo de lucro que busca promover el talento español como referente en temas de análisis de malware, y tiene como objetivo principal, investigar y compartir el conocimiento sobre amenazas emergentes en Internet con otras organizaciones, usuarios y fuerzas de seguridad de diversos países.

Manu Quintans

Manu es Malware Researcher vinculado desde hace muchos años a la escena como colaborador de grupos DC4420-Defcon (UK), Hacktimes.com o Malware Intelligence, entre otros

.

Durante su carrera, ha tenido la oportunidad de trabajar en equipos de respuesta a incidentes en zonas como Oriente Medio, Estados Unidos y Europa, siempre centrado en reversing y el análisis de amenazas.

En la actualidad se dedica a investigar amenazas relacionadas con Malware e Intelligence. Manu también es miembro fundador de MLW.RE.

Requisitos

Requisitos Técnicos

Para el correcto funcionamiento de los labs será necesario que los alumnos dispongan de equipos con las siguientes características técnicas o similares.

- Equipo portátil con VMWARE.
- 4GB de RAM mínimo
- Sistema operativo con arquitectura de 64bits.
- Sistema operativo Linux like

Conociminetos y aptitudes

Conocimientos básicos de:

- Análisis de Malware
- Reversing
- Exploiting
- Redes
- Sistemas Operativos
- Programación (scripting/c/asm)

*No se requieren conocimientos avanzados los puntos enumerados anteriormente. Como ya se ha comentado se empezarán todas las temáticas desde 0 y se avanzará según el ritmo general de la clase

Costes

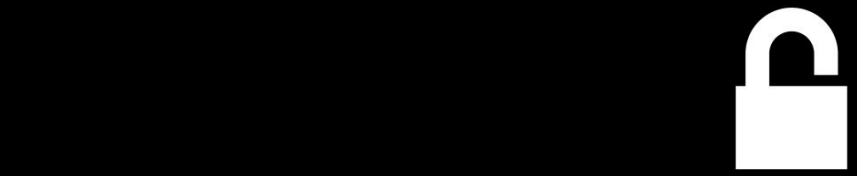
Coste

- El coste del curso es de 1100€
- Si tienes tu entrada para RootedCON2018 el coste de este curso es de 990€
- **IMPORTANTE**: se requiere un mínimo de diez (10) asistentes para que el curso tenga lugar.

Contact

General information:	info@rootedcon.com
Registration form:	
https://reg.rootedcon.es/training/.../	
Hashtag:	**#RC18**
Manu twitter:	@shakethemalware
Facebook, LinkedIn:	*Rooted CON*
Twitter:	*@rootedcon* *Tags:* *#rootedcon #rooted2018*

/Rooted®



Muchas gracias