CERTs Nivel 2

Organizado por:

Gobierno de España · Ministerio de Economía y Empresa · incibe_ Instituto Nacional de Ciberseguridad · OEA OAS

Con la colaboración de:

Gobierno de España · Ministerio de Asuntos Exteriores, Unión Europea y Cooperación · universidad de león · Ayuntamiento de León · León · Santander · IDB Inter-American Development Bank · Canada · aws · EUROPOL EC3 European Cybercrime Centre · INTERPOL

PROFESORES

Manu Quintans

Alejandro Nolla

Taller 6. Inteligencia en Ciberseguridad

Introducción

Las amenazas en Internet han evolucionado de manera que ya no se producen apenas ataques desde un punto de vista considerado 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

Los talleres impartidos por Manu Quintans y Jorge Capmany no pretenden ser un manual académico sobre fundamentos de seguridad y amenazas. No buscan 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.

En estos talleres se ofrece a los asistentes acceso a una nueva mentalidad a la hora de tratar la inteligencia y hacer frente a las amenazas emergentes.

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 estos talleres es el de proporcionar metodologías prácticas y proactivas que den visibilidad sobre las nuevas amenazas sofisticadas y evasivas.

Contenidos

Durante los talleres 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 su totalidad los objetivos de cada uno de los puntos.

PROFESORES

Manu Quintans

Alejandro Nolla

Taller 6.1 - Threat Intelligence

Duración del taller: 10 horas

Temario

- 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

PROFESORES

Manu Quintans

Alejandro Nolla

Taller 6.2 - Intelligence research

Duración del taller: 10 horas

Temario

- 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

PROFESORES

Manu Quintans

Alejandro Nolla

Taller 6.3 - Intel & DFIR

Duración del taller: 10 horas

Temario

- Intel focused DFIR
- Kill Chain model
- Diamond model
- Caracterización de malware
- Consumiendo intel para detección y respuesta
  - Log washing
  - Contextualización de eventos
  - Hunting
- Generando tu propia intel
- Estructurando conocimiento de adversarios

PROFESORES

Manu Quintans

Alejandro Nolla

Taller 6.4 - CounterOPs

Duración del taller: 10 horas

Temario

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