Seminarios magistrales

Cybersecurity Summer BootCamp 2017

Cybersecurity Summer BootCamp 2017

18-29 julio - León (España)

www.incibe.es/summer-bootcamp

Organizado por:

GOBIERNO DE ESPAÑA · MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

incibe_ INSTITUTO NACIONAL DE CIBERSEGURIDAD

OEA OAS

Con la colaboración de:

universidad de León

AYUNTAMIENTO DE LEÓN

León Cuna del Parlamentarismo

GOBIERNO DE ESPAÑA · MINISTERIO DE ASUNTOS EXTERIORES Y DE COOPERACIÓN

Santander

BID Banco Interamericano de Desarrollo

EUROPOL EC3 European Cybercrime Centre

INTERPOL

PONENTES

Luis Fernández

Francisco J. Rodríguez

Antonio Sepúlveda

Detección de ciberdelitos en la oscuridad...y en la claridad

Martes 18 de julio 2017
12:15 – 13:10
Auditorio Ciudad de León

Descripción

El objetivo de esta ponencia es exponer cómo desde INCIBE detectamos ciberdelitos en la oscuridad, es decir, delitos cometidos por criminales bajo el amparo del anonimato que proporcionan las redes en la DeepWeb.

Para lograr el objetivo, se unen tres factores fundamentales: el poder del desarrollo de tecnología para la automatización de tareas, la investigación aplicada en campos como la Inteligencia Artificial y la experiencia del usuario final, de las Fuerzas y Cuerpos de Seguridad del Estado.

Se describirá cómo un algoritmo de visión artificial permite etiquetar servicios dentro de la más popular de estas redes, TOR; cómo se realiza la categorización del crimen de forma automática, cómo se establece la relevancia de estos servicios ocultos o cómo se detecta e identifica automáticamente un menor en una imagen colgada de un foro.

De igual forma, se expondrá el hecho que no todos los delitos ocurren en la oscuridad del anonimato. Se describirán ejemplos de detección de ciberdelitos más cercanos, delitos que ocurren en internet y que buscan en la claridad ampliar el número de víctimas.

PONENTES

Alejandro López Parra

Javier Berciano

WannaCry y Petya: los ransom-worms más mediáticos

Martes 18 de julio 2017
13:10 – 14:05
Auditorio Ciudad de León

Descripción

Seminario sobre los recientes ciberataques de ámbito global WannaCry y Petya que son de los que más repercusión mediática han tenido en los últimos años.

Se tratarán sus antecedentes, los datos técnicos y de impacto así como la comparativa entre ambos para resaltar sus similitudes y diferencias.

Se hará especial foco en lo ocurrido en España así como la operativa desplegada por INCIBE y las acciones llevadas a cabo por el CERT.

PONENTES

Simón Roses

Software y Hardware hecho para el pentesting

Miércoles 19 de julio 2017
16:00 – 17:30
Auditorio Ciudad de León

Descripción

Esta charla introduce algunas de las herramientas software y hardware que los pentesters pueden utilizar para comprobar la seguridad de sus clientes incluyendo ataques físicos y digitales.

Raúl Siles

Desmitificando el cifrado extremo a extremo de WhatsApp

Miércoles 19 de julio 2017
17:30 – 19:00
Auditorio Ciudad de León

Descripción

WhatsApp finalmente implementó capacidades de cifrado extremo a extremo (E2E) el año pasado. En esta ponencia se proporcionará una visión global y detallada sobre las tecnologías empleadas en su implementación, y más específicamente, el protocolo Signal. El protocolo criptográfico Signal se está constituyendo de-facto en el estándar de referencia, ampliamente utilizado por soluciones seguras de mensajería (instantánea), como WhatsApp, Signal (TextSecure), Google Allo, Facebook Messenger, etc.

El objetivo de la ponencia es explicar la historia, evolución diseño, propiedades y características de seguridad, aspectos técnicos, las numerosas claves y componentes criptográficos de este complejo y moderno protocolo, junto a otros algoritmos y protocolos asociados, intentando facilitar su comprensión para los que no son criptógrafos... ;o)

PONENTES

Adolfo Rodriguez de Soto

Inteligencia artificial y ciberseguridad: una alianza ineludible

Miércoles 19 de julio 2017
19:00 – 20:00
Auditorio Ciudad de León

Descripción

La aplicación de la Inteligencia Artificial (IA) a diversos campos está viviendo una segunda juventud, especialmente gracias al desarrollo de las técnicas de aprendizaje profundo que han logrado, en poco tiempo, convertirse en las soluciones de referencia a muchos problemas en los que los resultados obtenidos por las máquinas no eran comparables al desempeño logrado por el ser humano. Este hecho ha posibilitado la ampliación de su campo de aplicación y tiene varias consecuencias sobre la Ciberseguridad.

La relación entre Inteligencia Artificial y Ciberseguridad podemos decir que es de necesidad mutua. Por una parte la ampliación de soluciones basadas en IA va a provocar el uso de muchos más sistemas automáticos en lugares antes inviables, con ello habrá más sistemas susceptibles de ser atacados con consecuencias graves. El desarrollo de la conducción automática de vehículos es un buen ejemplo. Pero en general la internet de las cosas (IoT) provocará la creación y constante uso de controles automáticos susceptibles de ser hackeados y muchos de ellos serán sistemas complejos cuya funcionalidad se conseguirá gracias a técnicas de IA. Así la Ciberseguridad debe preocuparse de la especial naturaleza de estos sistemas, algunos, cuyo mecanismo de funcionamiento e implicaciones que pueden derivarse de una modificación no deseada no son tan sencillas de analizar y explicar como lo pueden ser los sistemas de software tradicionales.

Por otra parte la Ciberseguridad debe aprovechar los métodos de IA para lograr herramientas más útiles en la resolución de sus problemas clásicos. La IA puede ayudar, y ya es una realidad en algunos casos, a detectar ataques, o a detectar intrusos, o al menos a filtrar escenarios. La capacidad de adaptación de los nuevos ataques a las medidas de seguridad establecidas puede ser limitada si esas medidas de seguridad son lo suficientemente hábiles como para transformarse o enmascararse ellas a su vez.

Esa doble relación y expectativa de ayuda mutua es lo que será expuesto en esta conferencia, mostrando casos de aplicación y líneas de trabajo futuras.

PONENTES

David Barroso

Operaciones de falsa bandera: cuando las apariencias engañan

Jueves 20 de julio 2017
16:00 - 17:30
Auditorio Centro Cívico León Oeste

Descripción

La atribución de incidentes de seguridad es realmente difícil. No solo porque muchas veces hay pocos indicios que podamos utilizar para intentar conocer el origen de un ataque, sino porque cada vez es más común utilizar pistas falsas para intentar atribuir el incidente a otro grupo. Este tipo de operaciones se han hecho desde el punto de vista militar desde el inicio de la humanidad, y ahora estamos viendo su réplica en el mundo tecnológico. Durante la presentación veremos ejemplos concretos de cómo grupos y naciones utilizan estas técnicas de bandera falsa en su beneficio.

European Cybercrime Centre
EC3 - EUROPOL

Descubriendo conexiones: Malware y criptomonedas

Jueves 20 de julio 2017
17:30 – 18:30
Auditorio Centro Cívico León Oeste

Descripción

La lucha contra el malware y el uso con fines delictivos de las criptomonedas son dos de las principales prioridades para los cuerpos policiales en todo el mundo. En esta charla se presentará el tipo de apoyo que Europol/EC3 puede proporcionar a los estados miembros en las investigaciones contra malware y monedas virtuales. Igualmente se mostrará cómo estas capacidades son utilizadas en el día a día como un instrumento útil para la investigación y persecución de los grupos criminales. Buenas prácticas, técnicas de investigación y retos futuros serán igualmente expuestos con ejemplos concretos.

PONENTES

Horacio J. Azzolin

Sigue al conejo blanco. Lecciones aprendidas en la investigación del cibercrimen

Jueves 20 de julio 2017
18:30 – 19:30
Auditorio Centro Cívico León Oeste

Descripción

Los crímenes cibernéticos presentan algunos desafíos para los investigadores, relacionados con el entorno digital en el que producen.

¿Cómo se investiga en internet? ¿Cómo se encuentran rastros en un escenario que favorece el anonimato? ¿De qué manera se obtienen evidencias cuando hay que solicitarlas a organismos ubicados en otros países? ¿Cuáles son los problemas que enfrentamos hoy y los que nos tocarán en un futuro más o menos cercano?

¿Cómo se construye un caso en esas condiciones, respetando el debido proceso?

Ésta y otras cuestiones serán tratadas desde la experiencia de trabajo de la UFECI, la unidad de cibercrimen de la Procuración General de la República Argentina.

Colin Weherill

Protegiendo el Sistema nervioso mundial – Colaboración y compartición de ciber-inteligencia

Jueves 20 de julio 2017
19:30 – 20:00
Auditorio Centro Cívico León Oeste

Descripción

Descripción pendiente.

PONENTES

Belisario Contreras

Ciberseguridad, terrorismo y delincuencia. ¿Estamos preparados en América Latina?

Viernes 21 de julio 2017
16:00 – 17:00
Auditorio Centro Cívico León Oeste

Descripción

Se presentarán generalidades sobre el concepto de ciberseguridad, así como el uso de internet con fines terroristas y criminales. Durante la presentación se hará un análisis del nivel de preparación de la región para hacer frente a estas amenazas.

Carlos Alvarez

El DNS como vector ataque

Viernes 21 de julio 2017
17:00 – 18:00
Auditorio Centro Cívico León Oeste

Descripción

Se puede decir que el Sistema de Nombres de Dominio (DNS) fue creado con el fin de facilitar a los usuarios el uso de recursos en línea sin la necesidad de memorizar complejas direcciones numéricas o alfa-numéricas. Desde una perspectiva operacional, el DNS es una infraestructura distribuida operada por miles de entidades, muchas de las que no tienen relación alguna entre sí. Desde una perspectiva eminentemente técnica, el DNS es un protocolo que hace parte de la suite de protocolos TCP/IP.

Y, aunque los recursos que hacen parte de esa inmensa infraestructura son en su enorme mayoría operados por personas o entidades con fines legítimos y legales y aunque el protocolo fue diseñado con fines más que benignos (hacer la vida más fácil para los usuarios), los delincuentes, como era de esperarse, desde hace varios años han venido dando usos creativos a vulnerabilidades existentes tanto en el protocolo como en esos recursos que hacen parte del DNS como sistema global.

La sesión cubrirá entonces temas relacionados con el DNS siendo utilizado como un vector para atacar a terceros (distribución de malware, comando y control de botnets, phishing, pharming, exfiltración o implantación de información), así como con ataques dirigidos contra el DNS mismo.

PONENTES

Javier Candau

La ciberamenaza y el reto de compartir

Lunes 24 de julio 2017
16:00 – 17:00
Edificio INCIBE

Descripción

Las ciberamenazas en 2017 están evolucionando rápidamente, se destacará al trasvase y publicación de información /exploits desconocidos por los fabricantes y con una capacidad espectacular de control de los equipos infectados y de colonización de las redes objetivos, que en un principio estaban en el dominio de los estados (eran considerados ciberarmas) y que ahora por negligencia o con intención deliberada está a disposición de cualquier atacante. Este escenario, como han demostrado WANNACRY y PETYA, ha modificado las reglas del juego. Los responsables de seguridad se enfrentan al reto de compartir para hacer frente rápidamente a estos nuevos ataques.

Las amenazas, ya sean provenientes del cibercrimen, el ciberespionaje o el cibersabotaje cada vez aprovechan más la lentitud en intercambiar entre los diferentes actores de la parte defensiva. No obstante este escenario está cambiando; los estándares de intercambio se están consolidando, se están generando cada vez más grupos de confianza para un intercambio ágil de información aunque todavía tenemos desafíos que superar como son el tratamiento de información clasificada, el intercambio de información entre gobiernos y sector privado (en especial compañías de seguridad que proporcionan servicios y convierten en dinero esa información), ganar la confianza de los responsables de seguridad privados en los diferentes sectores y definir canales automatizados basados en la confianza y en la voluntad de compartir.

PONENTESPES

Omar Cruz

Aprovechando la inteligencia de amenazas cibernéticas para los CSIRT

Martes 25 de julio 2017
16:30 – 17:30
Edificio INCIBE

Descripción

Durante el curso de la respuesta a los incidentes de seguridad cibernética, Cyber Threat Intelligence (CTI) ha permitido a los analistas de CSIRT obtener un mejor entendimiento de las Tácticas, Técnicas y Procedimientos (TTPs) del actor de amenazas cibernéticas, así como el nivel de riesgo que representan estos incidentes. Su organización. Esta presentación cubrirá cómo los analistas de CSIRT pueden aprovechar CTI durante incidentes cibernéticos importantes, así como las lecciones aprendidas y las mejores prácticas para aprovechar CTI..

José Antonio Vázquez Taín

Ciberdelincuencia y Justicia: ¿Estamos preparados?

Miércoles 26 de julio 2017
16:00 – 17:00
Edificio INCIBE

Descripción

La variadísima y cambiante fenomenología delictiva que se engloba en la denominada ciberdelincuencia, ofrece una problemática muy específica, no sólo tecnológica, sino también de enfoque legal, tanto sustantivo como procesal. Mientras los diferentes delitos que se comenten en, o a través del ciberespacio, aumentan y proliferan, la respuesta de la justicia no suele estar ni siquiera a la altura del meritorio trabajo de las fuerzas policiales. La ponencia trata de detectar las carencias de nuestro sistema judicial para dar una respuesta adecuada a estas nuevas modalidades de ataque a los derechos de los ciudadanos.

PONENTES

Prof Michael Goldsmith

Evaluando la madurez de la capacidad nacional en ciberseguridad

Jueves 27 de julio 2017
16:00 – 17:00
Edificio INCIBE

Descripción

Como centro líder a nivel internacional en materia de investigación eficiente y efectiva de capacidad en ciberseguridad, el Centro Global de Capacidad en Ciber Seguridad (GCSCC) ha creado el Modelo de Madurez de la Capacidad en Ciberseguridad para las naciones (Cybersecurity Capacity Maturity Model for Nations o CMM), el primero en su tipo, con el objetivo de analizar el nivel de madurez de la capacidad en ciberseguridad de determinado país, según el estudio de cinco dimensiones: políticas y estrategias en ciberseguridad, cultura cibernética, desarrollo del conocimiento del área, infraestructuras legales y reguladoras y control de riesgo. Junto a un grupo clave y estratégico de copartícipes internacionales, como el Banco Mundial, la Organización de Estados Americanos, la Organización de Telecomunicaciones de la Commonwealth y la Unión Internacional de las Telecomunicaciones, el Centro de Capacidad ha logrado difundir exitosamente el CMM en 18 países alrededor del mundo, y apoyado de manera significativa un estudio regional en Latinoamérica y el Caribe por medio de su colaboración con la Organización de Estados Americanos.

En este panel, el Profesor Goldsmith resumirá la amplia estrategia adoptada por el CMM, su estructura (incluidas las dimensiones, factores y sus respectivos indicadores), y su aplicación por parte del Centro de Capacidad y sus copartícipes. Asimismo, proveerá observaciones acerca de su difusión global y cómo este entendimiento contribuye al desarrollo de la capacidad nacional en ciberseguridad.

Manuel Guerra

Forense del Siglo XXI

Viernes 28 de julio 2017
16:00 – 17:00
Auditorio Ciudad de León

Descripción

El seminario presentará las nuevas técnicas en el campo de la informática forense y profundizará en los flujos de trabajo en el tratamiento de evidencias digitales, para que este tratamiento se realice de la forma más adecuada posible.

PONENTES

César Lorenzana

La transformación digital en la investigación policial

Viernes 28 de julio 2017
17:00 – 18:00
Auditorio Ciudad de León

Descripción

No cabe duda de que la sociedad en la que vivimos ha sufrido una profunda transformación y en pocos años hemos pasado de la era analógica a la digital, y nos encontramos a las puertas de una nueva era…. la era de la información. Estos cambios, patentes en el día a día han tenido su reflejo en el campo de la investigación policial. Así pues, de la misma manera que actualmente las empresas han de manejar una inmensa cantidad de datos para rentabilizar su negocio y optimizar sus procesos, las investigaciones policiales cada vez incluyen más y más datos que deben ser analizados y tratados correctamente para que éstas finalicen con éxito.
Con las capacidades actuales, el análisis de la información se realiza se realiza de forma semi-manual, lo que conlleva una lentitud y complejidad que provoca que los investigadores no puedan hacer frente a la presentación de las evidencias en sede judicial en tiempo y forma que permitan ser utilizadas en la causa, toda vez que el tiempo de la instrucción se ha visto reducido con la reciente modificación de la LeCrim. Por ello se hace necesaria una actualización tanto de dichas herramientas como de los procesos de trabajo en los que se emplean.
A lo largo de la ponencia se expondrán los actuales retos que supone al adecuado manejo de la información, y la necesidad de adaptar los estándares policiales para aprovechar las actuales tecnologías en el tratamiento de los datos para aumentar la eficacia policial.

Mikel Gastesi

Venturas y desventuras del analista de seguridad

Viernes 28 de julio 2017
18:00 – 19:00
Auditorio Ciudad de León

Descripción

En esta ponencia se mostrarán análisis de campañas de malware desde el punto de vista el analista de seguridad. Desde el análisis de una muestra hasta la extracción de información relevante, pasaremos por diferentes etapas en las que iremos viendo motivos por los que el analista sufrirá unos buenos dolores de cabeza.

PONENTES

Jaime Kindelan

Fernando Díaz

El 1%. Control de nodos de salida Tor

Sábado 29 de julio 2017
10:00 – 11:00
Auditorio Ciudad de León

Descripción

Esta ponencia/taller proporciona un punto de vista diferente sobre el control de nuestras infraestructuras desde la perspectiva de los atacantes ocultos tras las red Tor.

A lo largo de los últimos años Tor no solo ha servido para proporcionar anonimato y libertades a usuarios legítimos, sino que también ha aportado cobijo a atacantes y cibercriminales.

En esta charla tratamos de exponer los recursos necesarios para realizar una monitorización efectiva de la red con fines estadísticos, dando la posibilidad de una detección temprana de ataques que puedan influir en nuestros activos.

Ataques de Bots, Cibercriminales, Ciberguerra, Inteligencia, comportamientos sospechosos...

PONENTES

Adrián Arcoba

Elvira Tejada

Interpol y el desafío transnacional del Cibercrimen

Sábado 29 de julio 2017
11:00 – 12:30
Auditorio Ciudad de León

Descripción

Descripción pendiente de definir.

Respuesta del Estado de Derecho ante la ciberdelincuencia: La adaptación y armonización internacional de los ordenamientos jurídicos de los Estados y el reforzamiento de la cooperación internacional.

Sábado 29 de julio 2017
12:30 – 14:00
Auditorio Ciudad de León

Descripción

Es incuestionable la incidencia que el impresionante desarrollo de las tecnologías de la información y la comunicación está teniendo en el ámbito de la delincuencia. El uso generalizado de las herramientas tecnológicas ha ido determinando la aparición de nuevos comportamientos -hasta ahora difícilmente imaginables- que por afectar gravemente a los derechos de las personas o al interés general, merecen ser objeto de persecución y sanción penal. Además la posibilidad de actuar frente a estas conductas desarrolladas en el ciberespacio precisa también de herramientas tecnológicas que hagan factible la investigación de los hechos criminales y de las personas responsables de los mismos, sin que ello implique limitar o restringir los principios y valores que constituyen el fundamento del Estado de Derecho.

La respuesta ante esta situación exige de un importante esfuerzo por parte de múltiples sectores de la sociedad. Resulta imprescindible ir adaptando progresivamente las legislaciones nacionales a las necesidades que plantea la actuación frente a esos nuevos retos, siguiendo a dicho fin los parámetros asumidos internacionalmente y buscando una adecuada armonización con los ordenamientos jurídicos de los restantes Estados. Como también es esencial reforzar las herramientas de cooperación internacional, pues no en vano el carácter transnacional de estas conductas determina ineludiblemente la actuación coordinada con las autoridades competentes de otros países. Y también es imprescindible la colaboración del sector privado y de los ciudadanos, dada la naturaleza transversal de estos comportamientos y su desarrollo y expansión a través de sistemas muchas veces a disposición de organismos y entidades no públicos.

El objetivo de la intervención es analizar los nuevos desafíos que plantea la lucha contra la delincuencia que se planifica y desarrolla en el ciberespacio y los mecanismos que se están articulando desde el Estado de Derecho, tanto a nivel nacional como internacional, para ofrecer respuestas adecuadas que resulten eficaces y contribuyan a asegurar los derechos y las libertades de los ciudadanos, la seguridad de los Estados y la de la Comunidad Internacional en su conjunto.