Retos específicos de empresas

Retos propuestos por empresas comprometiéndose a validar las soluciones propuestas por los equipos promotores.

Generación de mecanismos de impacto de concienciación en Ciberseguridad

Plataforma que integre diferentes elementos que permitan evaluar el nivel de conciencia en términos de Ciberseguridad de una organización así como hacer un seguimiento de dicho nivel tras diversas acciones de concienciación.

La plataforma debería ser capaz de simular campañas, extremo a extremo, con los ataques más comunes enfocados hacia el usuario interno, como puede ser el phishing o malware, empleando técnicas y herramientas de ingeniería social y generando patrones de evasión contra los principales controles de seguridad con los que las compañías cuentan. Así mismo, debe medir la efectividad de dichas campañas, proponer modelos de concienciación basados en el resultado obtenido y establecer un modelo de seguimiento que mida la evolución en términos de concienciación de la organización a través de distintas oleadas/campañas.

Nuevas herramientas, sistemas y servicios basados en la normativa PSD2

Herramientas o aplicaciones que permitan iniciar pagos, basadas en la normativa PSD2. Sistemas de autenticación que puedan cumplir con PSD2 para firmar transacciones.

Nuevos métodos de pago y ticketing basados en movilidad y/o geolocalización

Nuevos servicios de pago y ticketing, en base a la ubicación del usuario, distancia recorrida, etc. considerando los requerimientos de seguridad en las transacciones y privacidad de los usuarios.

Protección y securización de Sistemas de Control Industrial (ICS) empleados en infraestructuras críticas del sector eléctrico

Adaptación de técnicas y herramientas de Ciberseguridad provenientes de sistemas IT sobre sistemas OT, definición de casos de pruebas específicos para estos equipos industriales y pentesting sobre equipos reales bajo un entorno de test.

Prevención de ataques DDos sobre los servidores DNS de las empresas con servicios abiertos al público

Las empresas que tratan datos sensibles y ofrecen servicios públicos en Internet, están expuestas a ataques DoS (Denial of Service). Si bien se hace hincapié en la protección de las entradas de servicios de las aplicaciones, los servidores DNS también están expuestos y son un objetivo de dichos ataques.

Seguridad en Internet of Things (IoT)

Medidas de seguridad para la securización de los dispositivos y las comunicaciones del Internet de las cosas (IoT): Soluciones perimetrales, mejora de los actuales estándares y protocolos, así como la creación de nuevos estándares específicos.

Copia cifrada de datos en la nube, manteniendo los datos críticos de los clientes a salvo de cualquier tipo de ataque / pérdida

Mecanismo que permita realizar copias de datos en la nube, de forma asíncrona y utilizando métodos que aseguren la seguridad y autenticidad de la información. Se debe indicar los requisitos de comunicaciones, ancho de banda o velocidad de transferencia que aseguren que la información ha sido copiada/transferida correctamente y que la copia se mantiene inalterada. Los datos deben estar encriptados desde el origen y las claves de encriptado deben ser conocidas sólo por el Cliente final.

Robot de Ciberseguridad, dando al CISO de las empresas información en tiempo real y de forma continuada de lo que está pasando en su landscape de TI

Aplicación basada en Inteligencia Artificial que permita gestionar la información/eventos/logs generados por los diferentes sistemas de seguridad y puestos de trabajo, cuyo motor sea capaz de analizar y tomar decisiones de manera preventiva, generando, además, informes y estadísticas precisas sobre las vulnerabilidades detectadas en tiempo real y las acciones tomadas con carácter preventivo. La aplicación debería contar con:

Motor de lógica preventiva basada en IA; detectar ataques de forma temprana, lanzar acciones correctivas (i.e. cerrar puertos) y emitir informes de actividades de remediación

Mecanismo de consolidación, normalización y carga de eventos de seguridad (logs, SIEM, etc..) para alimentar la bbdd de eventos de seguridad.

Identificación de las amenazas de la compañía

Al estilo de los threat map o cyber attack como los que los fabricantes de antimalware o elementos de seguridad perimetral tienen publicados en Internet, pero con un ámbito diferente; en este caso el de la empresa donde se instale. Se debe identificar y representar de una forma visual los eventos de seguridad que se estén produciendo en la compañía, pudiéndose seleccionar tipos de ataques (malware, DDoS, inyección de código, etc..), por localizaciones (país, sede,..) u otros criterios.

Identificación y gestión continúa de la exposición a vulnerabilidades de los sistemas en producción

Los sistemas en producción, son difíciles de analizar y más cuando tienen que estar 24 horas operativos. La compañía requiere simular mediante un "equipo victima virtual" si los ataques de explotación de vulnerabilidades podrían atravesar las defensas y tener éxito. El sistema de gestión realizará en la fase de exploración de la superficie de ataque, identificando puertos y servicios. Esta información puede ser alimentada con información concreta de parches y versiones. En la fase de ejecución realizará el ataque y caso de ser positivo recibirá desde la sonda el resultado del mismo.

Amenazas Ciber-físicas en infraestructuras críticas

Identificar si una instalación está sufriendo ataques combinados e identificar qué ataques físicos pueden suponer un incremento de la amenaza de Ciberseguridad.