Seekurity

STATE OF INFORMATION SECURITY

Contáctanos en +(52) 55-8195-8834 o envíanos un correo electrónico a Info@Seekurity.com o a 911@Seekurity.com si tu compañía se encuentra bajo ataque y necesitas una cotización urgente.

Seekurity for Information Security Cybersecurity SAS de C.V. es una firma de consultoría de Seguridad de la Información con base en el corazón de la Ciudad de México, México.

Ofrecemos una completa consultoría de servicios de Seguridad de la Información para empresas Industriales, Gubernamentales y no-Gubernamentales.
Entregamos un detallado, exhaustivo y personalizado reporte al finalizar cada servicio proporcionado. Nuestros reportes típicamente incluyen un resumen ejecutivo, hallazgos técnicos detallados con pruebas de concepto claras y bien definidas, así como recomendaciones de los pasos a seguir para su remediación.

NUESTROS SERVICIOS

[-] PRUEBAS DE PENETRACIÓN DE SEGURIDAD

[-] PRUEBAS FÍSICAS DE PENETRACIÓN DE SEGURIDAD

[-] HARDENING DE SEGURIDAD PARA SISTEMAS GESTORES DE CONTENIDO (CMS)

[-] ANÁLISIS DE VULNERABILIDADES

[-] INVESTIGADORES DE SEGURIDAD

[-] ANÁLISIS DE MALWARE

[-] PRIVACIDAD Y CUMPLIMIENTO DE LA SEGURIDAD DE LOS DATOS E INFORMACIÓN

[-] GESTIÓN DE INCIDENTES

[-] GESTIÓN DE RIESGOS

[-] INTELIGENCIA DE FUENTES ABIERTAS (OSINT)

[-] ANÁLISIS DE PHISHING

[-] SOLUCIONES ANTI-FRAUDE

[-] ATAQUES DE INGENIERÍA SOCIAL

[-] MONITOREO DE CIBERSEGURIDAD

[-] SEGURIDAD DE SISTEMAS DE VOZ SOBRE IP Y SOLUCIONES

[-] INTERNET DE LAS COSAS (IOT)

[-] ORGULLOSAMENTE APOYANDO AL FLOSS

PRUEBAS DE PENETRACIÓN DE SEGURIDAD

Ofrecemos pruebas de penetración de seguridad de Caja-Blanca (White-Box), Caja-Negra (Black-Box) y auditorías a código fuente para aplicaciones de escritorio, móviles y aplicaciones web basadas en vulnerabilidades recientemente descubiertas, Top 10 de OWASP y nuestras propias vulnerabilidades Día-Zero basadas en nuestra gran experiencia dentro del campo de la Seguridad de la Información. Al finalizar cada prueba, entregamos un reporte detallado que incluye típicamente un resumen ejecutivo con las amenazas identificadas y con pruebas de concepto bien definidas, así como los pasos de remediación para cada una.

PRUEBAS FÍSICAS DE PENETRACIÓN DE SEGURIDAD

El objetivo principal para una prueba física de penetración de seguridad es medir la eficiencia y efectividad de los controles de seguridad existentes y descubrir sus debilidades antes de que un atacante tenga la oportunidad de descubrirlas y explotarlas. Las pruebas físicas de seguridad o pruebas físicas de intrusión, revelan las oportunidades reales que tiene un atacante o un actor interno para comprometer los controles físicos (por ejemplo: candados, sensores, cámaras, trampas.) de tal manera que al ser vulnerados dichos controles permitan el acceso físico no autorizado a áreas sensibles que conducen a brechas de datos y al compromiso del sistema y/o red.

HARDENING DE SEGURIDAD PARA SISTEMAS GESTORES DE CONTENIDO (CMS)

Los Sistemas Gestores de Contenido como Wordpress, Drupal, Joomla, entre otros. Permiten que el proceso de iniciar un negocio sea fácil, pero los SGC no son seguros por si mismos. Nosotros ofrecemos pruebas de seguridad y hardening dedicados para asegurar que su negocio se encuentre a salvo y seguro, por lo cual ofrecemos tips de mejores prácticas de seguridad y tips de remediación de problemas en sus plataformas.

EVALUACIÓN DE VULNERABILIDADES

Una evaluación de vulnerabilidades es el proceso de identificar, cuantificar y priorizar/valorar las vulnerabilidades existentes en un sistema. Algunos ejemplos de sistemas a los que se realizan evaluaciones de vulnerabilidades incluyen, pero no se limitan a sistemas de tecnologías de la información, sistemas de suministro de energía, sistemas de suministro de agua, sistemas de transporte y sistemas de comunicación. Ofrecemos dichas evaluaciones las cuales pueden realizarse a una gran variedad de organizaciones, desde pequeñas empresas hasta grandes infraestructuras regionales.

INVESTIGADORES DE SEGURIDAD

Nuestros investigadores expertos en seguridad trabajan continuamente para desarrollar, descubrir e identificar nuevos ataques antes que algún actor malicioso lo haga. Nuestros descubrimientos son dirigidos responsable y apropiadamente a los dueños de los sistemas, a quienes se les otorga el tiempo suficiente para asegurarse de que las vulnerabilidades descubiertas sean corregidas exitosamente. Después de asegurarnos que las vulnerabilidades reportadas se han corregido correctamente, realizamos la publicación de los hallazgos en conjunto con una asesoría y procedimientos de conciencia de seguridad públicos, para prevenir incidentes y abusos generalizados. Nos fascinan las investigaciones de seguridad y siempre mantenemos nuestra base de conocimientos al día.

ANÁLISIS DE MALWARE

El análisis de malware es el estudio o proceso de determinar la funcionalidad y el impacto potencial de una muestra de malware dada, como virus, caballos de Troya, Rootkits, ransomware o puertas traseras. Este servicio es perfecto para usted, si nota actividad inusual en sus sistemas o experimenta extraños comportamientos funcionales en su infraestructura. Nuestros expertos pueden detectar, analizar y limpiar su activos infectados, así como remover cualquier infección de Amenazas Persistentes Avanzadas (APT por sus siglas en inglés: Advanced Persistent Threat).

PRIVACIDAD Y CUMPLIMIENTO DE LA SEGURIDAD DE LOS DATOS E INFORMACIÓN

Nuestros expertos pueden implementar todo tipo de tecnologías de seguridad de datos como cifrado de discos, Mecanismos basados en software vs hardware para proteger los datos, respaldos de información, enmascaramiento de datos, eliminación segura de datos, propiedad intelectual, protección y privacidad de datos basados en lineamientos o leyes nacionales e internacionales como LFPDPPP, evaluaciones de privacidad basadas en estándares internacionales como ISO 27000 y en estándares de seguridad de datos de la industria de tarjetas de pago PCI-DSS por sus siglas en inglés: Payment Card Industry DataSecurity Standard).

Ayudamos a su compañía a cumplir con el proceso de certificación apropiadamente.

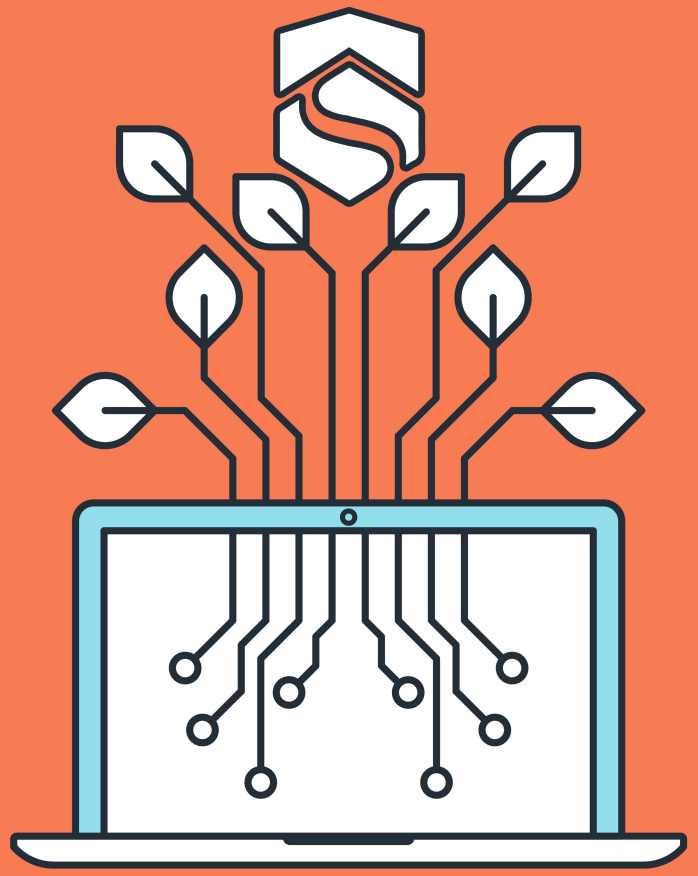
GESTIÓN DE INCIDENTES

Nuestro servicio de Gestión de Incidentes describe actividades de la organización para identificar, analizar y corregir amenazas, previniendo futuras re-currencias.

Ayudamos a gestionar, controlar y prevenir incidentes que afectan a la compañía severamente, a sus clientes y daños a la reputación de su compañía.

GESTIÓN DE RIESGOS

La gestión de riesgos es un proceso que permite a los administradores de TI, equilibrar los costos operativos y económicos de las medidas de protección y lograr mejoras mediante la protección de los sistemas de TI y los datos que respaldan la misión de su compañía.



Inteligencia De Fuentes Abiertas (OSINT)

Inteligencia De Fuentes Abiertas (OSINT por sus siglas en inglés: Open-Source Intelligence), es todo lo relacionado a la inteligencia de la Información que es recolectada de fuentes abiertas.

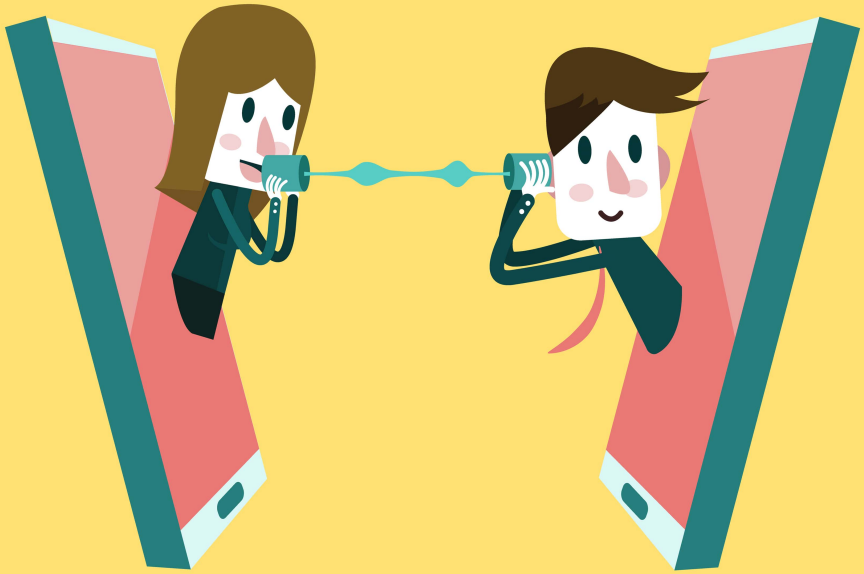
En la comunidad de inteligencia (IC), el término “abierto” se refiere a fuentes abiertas públicamente (en contraposición a fuentes secretas o clandestinas); No está relacionado con el software de código abierto o con la inteligencia pública. Ofrecemos una exhaustiva investigación basada en la recopilación de información para satisfacer todas sus necesidades, porque una pieza de información significa mucho.

ANÁLISIS DE PHISHING

Phishing es el intento de obtener información confidencial como nombres de usuario, contraseñas y detalles de tarjetas de crédito (indirectamente dinero), a menudo por razones maliciosas, disfrazándose como una entidad confiable en una comunicación electrónica y es uno de los muchos ejemplos de técnicas de ingeniería social utilizadas para engañar a los usuarios y explotar las debilidades de seguridad web actuales.

Ofrecemos servicios para casos de robo de identidad, generalmente o comúnmente para empresas cuyos clientes podrían ser afectados por correos electrónicos de phishing, pérdidas financieras y robo de identidad para empresas.

Los servicios de Internet pueden utilizarse para presentar solicitudes fraudulentas a posibles víctimas, para realizar transacciones fraudulentas o para transmitir el producto del fraude a instituciones financieras o a otras personas relacionadas con el sistema. La investigación sugiere que las estafas en línea pueden ocurrir a través de la ingeniería social y la influencia social. Puede ocurrir en salas de chat, medios de comunicación social, correo electrónico, tableros de mensajes o en sitios web. Nuestros expertos altamente capacitados analizan, eliminan y controlan las amenazas internas, diseñan y personalizan controles de seguridad para prevenir cualquier aparición de viejas o nuevas amenazas a través de nuestras incomparables soluciones anti-fraude construidas con amor en **Seekurity**.



ATAQUES
DE INGENIERÍA SOCIAL

La ingeniería social se refiere a la manipulación psicológica de las personas para realizar acciones o divulgar información confidencial.

Ofrecemos pruebas de Ingeniería Social en sitio y remotos que incluyen pero no limitado a campañas de ingeniería social, phishing, spear-phishing, llamadas a números telefónicos clonados y engaño físico.

MONITOREO DE CIBERSEGURIDAD

Es la protección de los sistemas informáticos contra el robo o daño al hardware, software o la información almacenada en ellos, así como de la interrupción o mala gestión de los servicios que prestan. Incluye el control del acceso físico al hardware, así como la protección contra los daños que pueden ocurrir a través del acceso a la red, la inyección de datos y código y debido a la negligencia de los operadores, ya sean intencionales, accidentales o debido a que se desvían de los procedimientos seguros.

Ofrecemos un servicio de supervisión contra ataques recientes y nuevas amenazas del mundo real.

SEGURIDAD DE SISTEMAS DE VOZ SOBRE IP Y SOLUCIONES

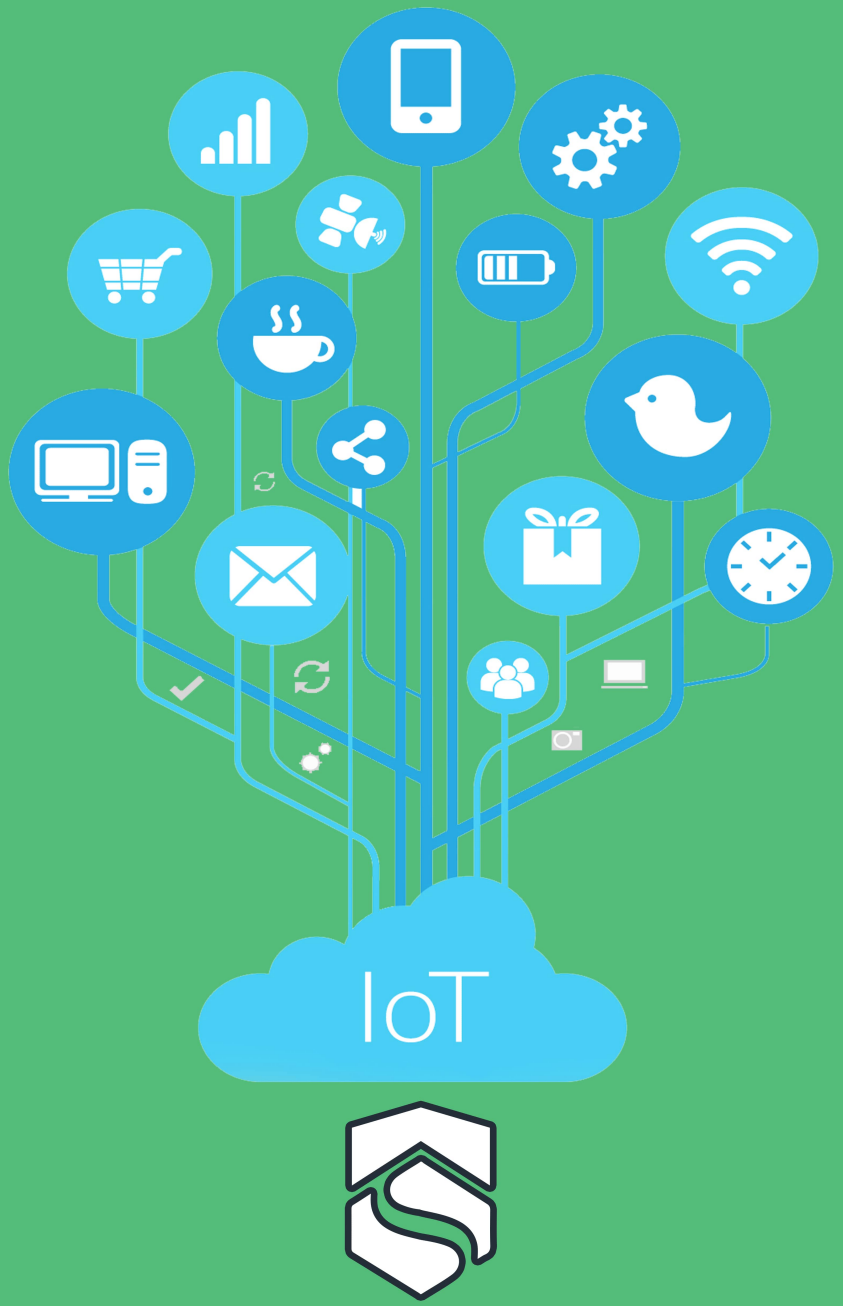
¿Qué es VoIP?

La Voz sobre Protocolo de Internet (Voz sobre IP, VoIP y telefonía IP) es una metodología y un grupo de tecnologías para la entrega de comunicaciones de voz y sesiones multimedia a través de redes IP, como Internet. Los términos telefonía por Internet, telefonía de banda ancha y servicio telefónico de banda ancha se refieren específicamente al suministro de servicios de comunicaciones (voz, fax, SMS, mensajes de voz) a través de la Internet pública, en lugar de la red telefónica pública conmutada (RTPC).

Para asegurarse de que los servicios de VoIP y de telefonía por Internet no pueden ser atacados, ponemos a prueba la seguridad de sus sistemas VoIP frente a muchas vulnerabilidades, por ejemplo, pero no limitado a:

- Intercepción de llamadas.
- Ataques de denegación de servicio.
- Robo del servicio.
- Exfiltración de datos a través de la sesión de medios.
- Malware incorporado en la sesión de señalización y medios de comunicación.

También diseñamos e implementamos medidas de seguridad para todo tipo de soluciones VoIP.



Internet de las Cosas (IoT)

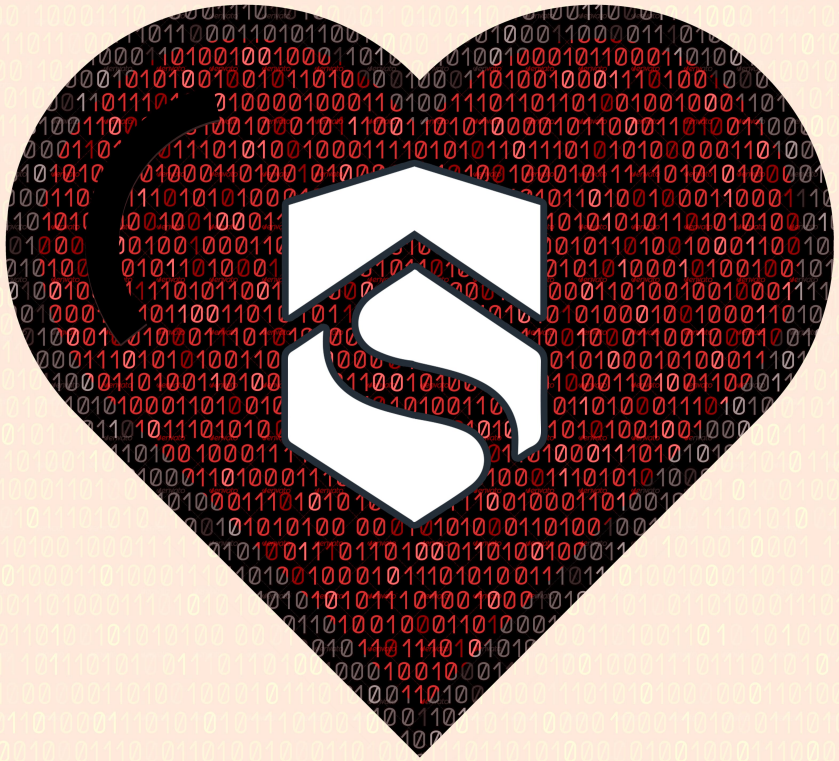
El Internet de las cosas (Internet of Things por sus siglas en inglés: IoT) es la interconexión de dispositivos físicos, vehículos (también conocidos como "dispositivos conectados" y "dispositivos inteligentes"), edificios y otros elementos-integrados con la electrónica, el software, sensores, actuadores y conectividad de red que permiten a estos objetos recopilar e intercambiar datos.

En el 2013, la Iniciativa de Normas Globales sobre Internet de las Cosas (IoT-GSI) definió el IoT como "la infraestructura de la sociedad de la información". El IoT permite que los objetos sean detectados o controlados remotamente a través de la infraestructura de red existente, creando oportunidades para una integración más directa del mundo físico en sistemas basados en computadoras, y resultando en una mayor eficiencia, precisión y beneficio económico además de una intervención humana reducida. - "Wikipedia"

Recientemente IoT se convirtió en la industria más importante (si no crítica) debido a su naturaleza sensible y la participación en la vida humana estas "cosas conectadas" tienen que ser probados periódicamente contra errores de seguridad y vulnerabilidades.

En **Seekurity** estamos realizando muchas investigaciones sobre IoT y dispositivos incrustados. También ofrecemos servicios de pruebas de seguridad a proyectos basados en Arduino, Raspberry PI y otras placas lógicas.

¡Contáctenos para más información!



FLOSS

Free/Libre Open Source Software

ORGULLOSAMENTE APOYANDO EL FLOSS

Debido a que en Seekurity adoramos los proyectos basados en Free Source Software y Creative Commons (CC), estamos ofreciendo gratuitamente pruebas de seguridad, evaluaciones de vulnerabilidades y un soporte de seguridad a largo plazo (LTSS) a cualquier proyecto libre y de código abierto elegible.

Visite nuestro sitio web para obtener más información o envíenos un correo electrónico a: Info@Seekurity.com.

¡En **Seekurity** deseamos ser parte de su proyecto!

RECONOCIMIENTOS

Seekurity es orgullosamente reconocido y recompensado por cientos de empresas de alto perfil.