BASE4 SECURITY

Ayudando a construir un ecosistema digital más seguro.

Red team

DATA SHEET

Digital Footprint

A través de las técnicas avanzadas de OSINT protegemos su organización contra riesgos ocultos en Internet, realizamos la investigación, el análisis y la identificación de posibles vectores de ataque disminuyendo los riesgos cibernéticos.

Nuestro servicio Digital Footprint ofrece un análisis exhaustivo y detallado de investigación de la información de fuentes abiertas para ayudar su Organización a identificar posibles riesgos y oportunidades, mediante el uso de técnicas avanzadas y herramientas. Nuestro equipo especializado en OSINT cuenta con amplia experiencia en investigación y análisis de información de diversas fuentes, como sitios web, foros, redes sociales, repositorios de código, Deep y Dark Web. Con esta información, podemos ayudarle a su Organización a identificar posibles vectores de ataque, detectar información sensible expuesta y evaluar el riesgo de reputación, así como detectar actividad maliciosa en internet.

Con nuestro servicio Digital Footprint ustded podrá mejorar la ciberseguridad de su organización y proteger su ecosistema digital, al mismo tiempo que se mejora la capacidad de respuesta ante incidentes y amenazas, con el objetivo de garantizar la protección de sus activos digitales y minimizar los riesgos cibernéticos, por favor no dude en ponerse en contacto con nosotros, estaremos encantados de ayudarlo.

Adversarial Emulation

Realizamos una evaluación exhaustiva de los riesgos cibernéticos de su organización utilizando técnicas avanzadas como la Emulación de Ataques y la investigación de información de fuentes abiertas (OSINT). Identificamos y emulamos los posibles vectores de ataque, ayudando a su organización a detectar y mitigar vulnerabilidades críticas en sus sistemas.

Nuestra Emulación de Adversario es un servicio integral de seguridad cibernética que combina técnicas avanzadas de ataque como la Simulación de Adversarios y OSINT para evaluar el riesgo cibernético de su organización. Emulamos un ataque realista y en profundidad contra la infraestructura tecnológica, identificando posibles vectores de ataque específicos para su organización. Además, indicamos las Tácticas, Técnicas y Procedimientos (TTPs) de Mitre ATT&CK que funcionaron y evadieron los controles durante el análisis, proporcionando una comprensión detallada de los riesgos cibernéticos y ayudando a mejorar la detección y respuesta de incidentes en su servicio de SOC. Los beneficios de nuestra emulación de adversario incluyen evaluar el riesgo cibernético de su organización, identificar sus principales vectores de ataque y evaluar la resiliencia de su organización ante posibles ataques reales.

Red Team

Nuestro servicio de Red Team es un servicio especializado de ciberseguridad que combina técnicas avanzadas de ataque como OSINT, Ingeniería Social y Emulación de Adversario para evaluar la preparación de su organización ante ataques cibernéticos realistas.

Nuestro servicio de Red Team es un servicio de seguridad cibernética altamente especializado que se enfoca en la planificación y ejecución de proyectos de infiltración estratégica en la infraestructura de una Organización con el objetivo de obtener y extraer información valiosa y acceder a sistemas críticos. Nuestros expertos en seguridad utilizan y combinan técnicas avanzadas de ataque y simulaciones de comportamiento de un atacante potencial para evaluar en profundidad los controles de prevención, detección, recuperación, respuesta y resiliencia de su organización.

El objetivo es encontrar posibles brechas, fallas de seguridad y vulnerabilidades críticas, y proporcionarle recomendaciones para mejorar su plan de seguridad existente. Con nuestro servicio Red Team, su organización podrá estar mejor preparada para enfrentar incidentes y amenazas reales en el mundo digital.

Advanced Penetration Testing

Identifique posibles debilidades y vulnerabilidades de sus sistemas Web, API y Mobile así como de su Infraestructura Cibernética mediante técnicas y pruebas de Pntesting exhaustivas y en profundidad de forma controlada y segura.

Nuestros proyectos de Pentest son compuestos por técnicas avanzadas de ataque los cuales se realizan en un 70-80% de forma manual, controlada y en profundidad, los tests son exhaustivos, intentando explotar las vulnerabilidades identificadas con el objetivo de reproducir un escenario real de ataque llevado a cabo por un potencial atacante.

Realizamos los Tests de Intrusión avanzados en todo tipo de sistemas, redes y plataformas:

- Pentest Web
- Pentest API
- Pentest Android / iOs
- Pentest Wireless
- Pentest Cloud / Kubernetes
- Pentest ATM
- Pentest SCADA / OT / ICS

La metodología adoptada por BASE4 Security divide el Pentest o Test de Intrusión en fases y etapas, que siguen un estándar y las mejores prácticas de la industria como OSSTMM, OWASP, PCI-DSS, NIST SP 800-115, que acompañan las necesidades y expectativas del Cliente. A su vez, las tareas realizadas y las acciones específicas

tomadas y los exploits perseguidos se eligen en función de la oportunidad percibida y, a menudo, se aumentan con enfoques adicionales a medida que se ejecutan las diversas pruebas que siguen los estándares mencionados.

Esta alineación metodológica permitirá una administración eficaz y una gestión asertiva de resultados, planes de acción y estrategias de gestión de riesgos asociados a las vulnerabilidades que se puedan descubrir en los sistemas, plataformas y aplicaciones del cliente.

Beneficios:

En función de resultados obtenidos a través de los proyectos de Pentest nuestros clientes tendrán un ambiente tecnológico más seguro y controlado ante eventuales ataques cibernéticos, evitando de esta forma la fuga de información y la indisponibilidad de sus servicios, a su vez mitigando los riesgos, fraudes, daños económicos y exposición de la marca e imagen de la compañía.

Ingenieria Social

Nuestro servicio de Ingeniería Social consiste en simular ataques de Phishing, Smishing y Vishing para evaluar la preparación y respuesta de su Oganización a estas amenazas y mejorar la concientización en temas de seguridad de sus colaboradores.

BASE4 Security ofrece un acompañamiento anual para brindar indicadores en el grado de madurez del usuario interno y las campañas de awareness y concientización de los mismos a través de técnicas de Ingeniería Social tales como:

- Phishing & Spear Phishing
- Smishing
- Vishing
- Tailgating
- Bating
- Dumpster Diving
- Hacking WiFi

También brindamos el acompañamiento en la estrategia de Concientización y Comunicación a través de charlas presenciales y virtuales, y capacitaciones.

Beneficios:

Aumentar el nivel de madurez en ciberseguridad de los colaboradores de la compañía para reducir la superficie de ataque a gran escala en poco tiempo.

BASE4
SECURITY

www.base4sec.com