Agedos Business Datacenter

Mohammed Lakhouaja
C/Central, 10 1ª Planta – Ed. Azor
968 000 777
https://www.age2.es/

MODELO DE MADUREZ

Es un sistema de evaluación que acaba ofreciendo un indicador del grado en el que determinados criterios o condiciones se están teniendo en cuenta.

Es un sistema de evaluación que acaba ofreciendo un indicador del grado en el que determinados criterios o condiciones se están teniendo en cuenta. Permiten a una organización conocer cuál es su grado de madurez en ciberseguridad.

TEST DE INTRUSIÓN AVANZADO IT OT

una prueba de seguridad ofensiva que simula un ciberataque real OT IT

Consiste en una prueba de seguridad ofensiva que simula un ciberataque real en un entorno controlado. El objetivo es identificar las debilidades que podrían ser aprovechadas por un atacante respecto a activos importantes determinados por el cliente (ejemplo AD , ERP...) y si es posible explotarlos.

DISEÑO IMPLANTACIÓN DE SOLUCIONES DE SEGURIDAD IT/OT

Ofrecemos a nuestros clientes, soluciones avanzados de seguridad (IT/OT) :EDR, anti phishing , monitorización y seguridad (IT/OT).

Ofrecemos a nuestros clientes, soluciones avanzados de seguridad (IT/OT) :EDR, anti phishing , monitorización y seguridad (IT/OT), gestión de parches ,gestión de credenciales ,gestión de copias de seguridad ,gestión de vulnerabilidades , Seguridad del active Directory...

PENTESTING IOT, API, APLICACIÓN WEB Y MÓVIL

Pentesting

- De Aplicación Mobile aplicando la metodología de OWASP (MSTG), que consiste al análisis de seguridad de aplicaciones Mobile Android IOS usando como referente la lista de pruebas de aplicaciones Mobile aplicando el Pentesting manual y semiautomático .SAST Y DAST con niveles L1,L2,R.
- De Aplicación Web aplicando la metodología de OWASP (WSTG).que consiste al análisis de seguridad de aplicaciones Web usando como referente la lista de pruebas de aplicaciones web, aplicando el Pentesting manual y semiautomático Con metodologías de Caja Negra y Gris(DAST).
- De API aplicando la metodologías de OWASP que consiste al análisis de seguridad de APIs usando como referente La metodología OWSP , aplicando el Pentesting manual y semiautomático Con metodologías de Negra y Gris(DAST).
- Prueba de Penetración detección con técnicas utilizadas por hackers éticos, tiene como objetivo encontrar potenciales vulnerabilidades en un sistema, servidor ,redes. en entornos IT o OT.

PRUEBA DE SEGURIDAD DE APLICACIONES ESTÁTICAS (SAST)

Prueba de seguridad de aplicaciones estáticas (SAST) ,metodología de prueba de caja blanca.

Prueba de seguridad de aplicaciones estáticas (SAST) ,metodología de prueba de caja blanca, consiste al análisis de seguridad de aplicaciones al nivel de código Fuente .

SIMULACIÓN DEL PHISHING

El objetivo de esta prueba es el aprendizaje a través de la experiencia, Enfrentarse al propio peligro con ataques controlados de simulaciones de phishing

El objetivo de esta prueba es el aprendizaje a través de la experiencia. Enfrentarse al propio peligro con ataques controlados de simulaciones de phishing aumentará la capacidad del empleado para responder con precisión a los ataques reales del phishing y de la ingeniera social.

VIGILANCIA DIGITAL

Consiste en encontrar, analizar y rastrear cualquier información perjudicial para evitar que la amenaza se convierta en un problema real

Consiste en encontrar, analizar y rastrear cualquier información perjudicial para evitar que la amenaza se convierta en un problema real.(Leaks,datos expuestos ..) Así minimizaríamos el impacto sobre la reputación corporativa y anticipar al atacante.