iPhalanx
CYBER RANGE SOLUTION

Solución avanzada para la formación práctica, entrenamiento, experimentación, pruebas e investigación en ciberseguridad

INTRODUCCIÓN

Para una implementación eficaz de la ciberseguridad las organizaciones deben contar con personal altamente cualificado así como disponer de entornos adecuados donde experimentar y probar nueva tecnología que posteriormente desplegar en producción.

Los campos de maniobra cibernéticos (cyber range) se han erigido como la aproximación ideal para que usuarios del sector tanto civil como militar formen a sus profesionales y adquieran el nivel de preparación necesario para responder eficazmente a las ciberamenazas actuales y futuras.

MÚLTIPLES PROPÓSITOS

La solución de Indra está diseñada para satisfacer de forma integral un amplio abanico de necesidades:

- Formación práctica intensiva a nivel individual y grupal en técnicas y tácticas de forense de sistemas informáticos, ciberdefensa y ciberataque.
- Ciberejercicios cooperativos y competitivos en ciberdefensa (CDX).
- Simulación y experimentación segura de nueva tecnología, malware y ciberarmas.
- Pruebas de ciberseguridad en un entorno controlado.

MODOS DE USO

iPhalanx puede usarse en modo servicio (SaaS). El cliente se despreocupa de cualquier cuestión relativa a la instalación, configuración y mantenimiento, accediendo únicamente de forma remota a la plataforma de Indra.

En modo despliegue, Indra instala y pone a punto la solución en la instalación del cliente, que pasa a ser gestionada por él mismo.

Adicionalmente Indra ofrece una serie de servicios de alto valor añadido como complemento a la solución tecnológica, tales como cursos de formación a medida, diseño de ejercicios personalizados, etc.

FORMACIÓN Y ENTRENAMIENTO

iPhalanx ha sido diseñado para mejorar cinco **habilidades** esenciales:

- **PREVENCIÓN**: análisis de vulnerabilidades; bastionado, optimización y parcheo; SSDLC.
- **DETECCIÓN y REACCIÓN**: configuración segura de redes y sistemas; monitorización y gestión de la seguridad (SIEM, Firewall, IDS/IPS, network probing, ...).
- **ATAQUE**: exploración e identificación de objetivos; análisis de vulnerabilidades; explotación y consolidación.
- **ANÁLISIS FORENSE**: análisis de sistemas de fichero (FAT, NTFS, ext2/3/4, UFS, HFS, ISO 9660, YAFFS) y nivel aplicación de S.O. Windows y Linux; obtención y gestión centralizada de evidencias; generación de informes forense.

Tipos de **ejercicios de entrenamiento**:

- **CIBERDEFENSA**: El alumno debe defender un sistema ante ataques automatizados, impidiendo que logren su objetivo.
- **CIBERATAQUE**: El alumno debe atacar un sistema objetivo dado a partir de cierta información de partida y debiendo cumplir unos objetivos predeterminados.
- **CIBERGUERRA**: Escenario cooperativo / competitivo donde dos o más grupos de alumnos se enfrentan entre sí, debiendo cada grupo defender su propio sistema y atacar el de los adversarios.
- **ANÁLISIS FORENSE**: El alumno debe llevar a cabo un análisis forense metodológico sobre cierto sistema comprometido, y recuperar las evidencias y generar el informe que apoyen la hipótesis planteada.

CIBEREJERCICIOS (CDX)

Construcción, planificación, conducción, y análisis de resultados de ciberejercicios colaborativos y competitivos orientados a concienciar, evaluar y mejorar las habilidades técnicas, de comunicación y cooperación en las organizaciones para responder a ciberataques.

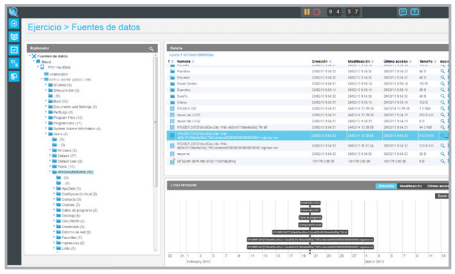
Características principales:

- **Herramientas de apoyo** al equipo blanco en la monitorización de la evolución y rendimiento de los participantes y del ciberejercicio.
- Soporta **equipos distribuidos** geográficamente.
- **Role playing**, coaliciones de equipos, canales de comunicación entre participantes.
- Reutilización, restauración y lanzamiento **automáticos** de ciberejercicios.

EXPERIMENTACIÓN, PRUEBAS E INVESTIGACIÓN

Entorno virtual seguro en el que realizar experimentaciones de nuevas tecnologías y herramientas para propósitos de estudio, homologación, análisis comparativo, etc.

Las características del entorno posibilitan el análisis de comportamiento y eficacia de malware y ciberarmas en escenarios diseñados a medida.



PRODUCTOS DE LA SUITE iPhalanx

CAPACIDADES	Solución para entrenamiento y ciberejercicios CDX **iPhalanx CTER** (Cyber Training & Exercise Range)	Solución para la experimentación, pruebas e investigación **iPhalanx CSTR** (Cyber Simulation & Test Range)	Solución para diseñar y crear nuevos escenarios para **CTER** y **CSTR** **iPhalanx SGT** (Scenario Generation Tool)
MaCyR - Malware & Cyber attacks Repository	●	●	
NetTraf - Network Traffic Generator	●	●	
DVS - Deep Vulnerability Scanner		●	●
SIAS - Static Intelligent Attack Scheduler		●	●
DIAS - Dynamic Intelligent Attack Scheduler	●	●	
CAP - Cyber Attack Platform	●	●	
Automated Monitoring & Guidance	●		
Life Cycle Management	●	●	

● Control absoluto por el usuario ● Capacidad incluida pero transparente al usuario ● Para propósitos de configuración

indra

Avda. de Bruselas, 35.
28108 Alcobendas.
Madrid (Spain)
T +34 91 480 60 00
F +34 91 480 60 31
indracompany.com
security@indracompany.com