

¿Por qué CCS?

La ciberresiliencia no es solo una cuestión de tecnología: también depende de las personas, los procesos y las decisiones que se toman bajo presión. CCS ofrece un entorno seguro y realista para practicar la respuesta a incidentes, validar procedimientos y reforzar la confianza de la organización en su capacidad de respuesta.

Ventajas principales



ESCENARIOS REALISTAS

Adaptados a su infraestructura, sus riesgos y su panorama de amenazas.



PARTICIPACIÓN DE TODO EL EQUIPO

Desde el personal de TI hasta la dirección, cada participante se entrena en su función real.



FORMACIÓN EFICIENTE

Los incidentes que duran varios días pueden simularse en solo unas horas.



MAYORES CAPACIDADES

Los equipos ganan rapidez, coordinación y resiliencia.



VALOR A LARGO PLAZO

Un entorno cibernético reutilizable permite una formación continua con una amplia variedad de escenarios.



CONOCIMIENTO DEL ATACANTE

Comprenda las tácticas, técnicas y procedimientos (TTP) de los adversarios.

Conviértase en socio de CCS

Estamos creando una red de socios de confianza - consultores, integradores de sistemas y proveedores de formación - que quieran ofrecer ejercicios avanzados de ciberseguridad con CCS.

QUÉ OFRECEMOS

- Formación para socios: aprenda a diseñar entornos cibernéticos y escenarios, y a realizar ejercicios.
- Soporte continuo: asistencia para adaptar los ejercicios a las necesidades y los requisitos de los usuarios finales.
- Colaboración escalable: utilice CCS en proyectos o como parte de sus servicios.

POR QUÉ COLABORAR CON NOSOTROS

- Incorpore servicios de alto valor
- Diferencie su oferta
- Refuerce las relaciones con sus clientes
- Amplíe sus capacidades
- Ofrezca formación de vanguardia en respuesta a incidentes de ciberseguridad

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd. | www.utilis.biz | ccs.utilis.biz



Cofinanciado por
la Unión Europea

Escanee para
otros idiomas



CCS Cyber Conflict
Simulator

Prepare a su organización para gestionar una cibercrisis

Una plataforma de simulación de
ciberconflictos para reforzar la
ciberresiliencia de su organización.

Contexto de ciberseguridad

En el mundo hiperconectado de hoy, la ciberseguridad se ha convertido en una preocupación fundamental para las personas, las empresas y los gobiernos. Los ataques patrocinados por Estados, la delincuencia con fines económicos y los movimientos hacktivistas evolucionan más rápido que las defensas.

Marcos normativos de la UE como DORA y NIS2 exigen una mayor ciberresiliencia. Las organizaciones deben garantizar no solo la protección de los datos, sino también la continuidad de los servicios esenciales durante y después de los incidentes.



INCIDENTES DE CIBERSEGURIDAD

Desde hace varios años consecutivos, los incidentes de ciberseguridad son el principal riesgo empresarial a escala mundial. Las organizaciones invierten recursos considerables en medidas de prevención, tanto técnicas como organizativas. Es igualmente importante invertir en la preparación.

POR QUÉ ES IMPORTANTE LA PREPARACIÓN

Según un estudio de IBM, los planes de respuesta a incidentes probados y un equipo de respuesta bien formado pueden reducir significativamente los costes de las brechas de datos.

Estar preparado significa contar con:

- **Un plan sólido:** los planes de respuesta a incidentes (IR) adaptados a cada organización y probados en escenarios realistas permiten detectar carencias y definir funciones.
- **Un equipo formado:** la práctica bajo presión mejora la coordinación.



CCS Cyber Conflict Simulator

CCS es una plataforma de simulación de ciberconflictos que reproduce escenarios realistas de ataque y defensa. Permite modelar un gemelo digital de los sistemas IT/OT, los procesos de negocio y las personas, y ayuda a las organizaciones a mejorar su preparación para responder a incidentes y su capacidad para tomar decisiones bajo presión.

Cómo funciona

CYBER LANDSCAPE

CCS Cyber Landscape (CL) es un gemelo digital que refleja sus sistemas IT/OT y sus procesos de negocio tal como existen en el mundo real. Los procesos de negocio dependen de los sistemas IT/OT que los sustentan, por lo que los eventos técnicos pueden interrumpir las operaciones y provocar pérdidas económicas, daños a la reputación o incluso poner en peligro vidas humanas.

Las personas también forman parte del modelo: administradores, analistas, técnicos y otros perfiles, cada uno representado con sus habilidades, su concienciación en materia de seguridad y sus hábitos. Es posible simular adversarios y comportamientos de ataque realistas que representan una amplia variedad de fuentes de amenazas, desde actores patrocinados por Estados y grupos de ciberdelincuentes hasta atacantes individuales. Sus acciones se basan en tácticas, técnicas y procedimientos (TTP) derivados de la inteligencia sobre amenazas. Una vez configurado Cyber Landscape, puede realizar un número ilimitado de ejercicios con diversos escenarios de ataque.

ESCENARIO

Cada escenario de ejercicio se adapta a sus objetivos y puede basarse en inteligencia sobre amenazas o en evaluaciones de riesgos. CCS admite una amplia variedad de ataques y puede simular vulnerabilidades tanto en el hardware como en el software. Los escenarios pueden grabarse y reproducirse de nuevo o guardarse como punto de partida para futuros ejercicios.

Se asignan a los participantes funciones realistas: responsable de la gestión del incidente, responsable técnico, personal de operaciones de TI y administradores de redes, dirección, responsables de negocio, CISO, expertos en distintas áreas, responsable de relaciones públicas, asesoría jurídica y recursos humanos. De este modo, se reproducen las responsabilidades reales y la coordinación entre áreas.

SIMULACIÓN

CCS simula tanto los eventos técnicos como sus repercusiones en el negocio. Los ejercicios pueden seguir secuencias de ataque predefinidas o incorporar la actividad en directo de un equipo de ataque (Red Team), y comenzar en una fase temprana de detección o en una fase posterior de escalada.

Los participantes interactúan con miembros virtuales del equipo cuyas acciones reflejan sus habilidades y capacidades. La compresión del tiempo permite condensar días de actividad en horas y realizar ejercicios realistas y eficientes.

EVALUACIÓN POSTERIOR AL EJERCICIO

ECada acción, decisión y mensaje se registra de forma detallada. Tras el ejercicio, CCS genera informes exhaustivos para evaluar la eficacia, la coordinación y los procedimientos de respuesta a incidentes (IR), lo que ayuda a los equipos a aprender, adaptarse y mejorar continuamente sus procesos de respuesta.

Resultados de la evaluación

- Eficacia de las acciones de detección, verificación y priorización de incidentes, determinación de su alcance, contención, erradicación de amenazas y recuperación
- Comunicación y colaboración entre los distintos roles y las partes implicadas bajo presión
- Puntos fuertes y carencias en los procedimientos y las guías operativas de respuesta a incidentes existentes
- Eficacia de los cortafuegos, EPP, EDR, DLP y otros controles de seguridad
- Tácticas, técnicas y procedimientos (TTP) de ataque observados
- Áreas prioritarias para mejorar las defensas técnicas y los procedimientos organizativos