



El eslabón que falta **en su** **ciberdefensa**

Realice en solo unas horas un ejercicio
realista de respuesta a incidentes

**de ciberseguridad con la participación
de todo el personal responsable.**



¿Está preparado para un ciberataque?

La dependencia de la sociedad respecto al ciberespacio aumenta constantemente. El ciberespacio se reconoce como el quinto dominio de las operaciones militares, en el que la preparación de las fuerzas armadas debe garantizarse mediante una formación adecuada. Los ciberdelincuentes son cada vez más hábiles y audaces, y sus métodos y vectores de ataque, cada vez más sofisticados.



La formación en ciberdefensa también es necesaria para las organizaciones e instituciones civiles. Además de cuantiosas pérdidas económicas, los ciberatacantes pueden causar daños que amenacen las infraestructuras críticas, los suministros básicos, los servicios e incluso vidas humanas.

Las organizaciones invierten importantes recursos económicos en medidas de prevención de ciberataques, tanto técnicas como organizativas.

La prevención es importante, pero, según los expertos, impedir el acceso de todos los ciberatacantes no debe ser el único objetivo de seguridad de una empresa.

¿Qué ocurre si, a pesar de todas las medidas adoptadas, se produce un ataque y su organización se enfrenta a un incidente de ciberseguridad?

¿Puede identificar correctamente su causa?

Numerosos estudios indican que el tiempo medio transcurrido entre el inicio de un incidente y su detección se mide en meses. Tras la detección, se analiza la causa del incidente.

¿Qué capacidad tiene para contener incidentes, eliminar sus causas raíz y restablecer los

sistemas de información y las operaciones de negocio? A diferencia de los incendios, los terremotos o incluso las pandemias, los ciberataques se dirigen a un objetivo concreto y cuentan con un atacante activo que puede adaptar sus acciones a las medidas defensivas de su organización.

¿Practica escenarios de incidentes de ciberseguridad y mejora sus tácticas, técnicas y procedimientos defensivos a partir de las lecciones aprendidas?

La tecnología desempeña sin duda un papel importante en la defensa frente a los ciberataques, pero las personas siguen siendo el elemento clave. Debe prestarse especial atención a quienes gestionan los incidentes y toman decisiones en los niveles operativo y estratégico.

Formación y ejercicios

Como ya se ha señalado, la posibilidad de que se produzca un incidente nunca puede descartarse por completo. Cuando ocurra, ¿a quién preferiría al mando: a un equipo con experiencia o a uno que se enfrenta a un incidente por primera vez? Dado que son relativamente pocas las personas que han vivido un incidente, quienes carecen de esa experiencia solo pueden adquirirla mediante ejercicios.

Muchos trabajos exigentes requieren formación. Los bomberos adquieren rapidez y eficacia mediante simulacros periódicos de emergencias. Los cirujanos comienzan asistiendo en operaciones, después trabajan bajo supervisión y, finalmente, operan de forma autónoma. Los



controladores aéreos se entrenan en simuladores en los que los «pseudopilotos» simulan el tráfico aéreo. La formación de los generales es aún más compleja y costosa. La preparación de los equipos de respuesta a incidentes de ciberseguridad plantea un reto similar.

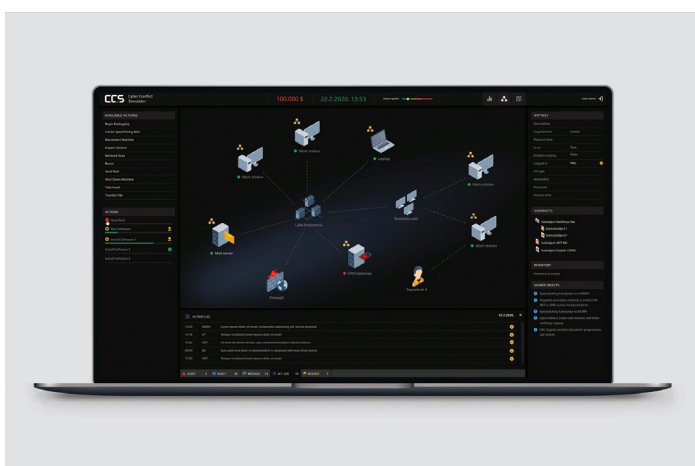
Responder a un incidente de ciberseguridad es una tarea exigente que implica gestionar a numerosas personas y coordinar múltiples actividades. Algunas de estas

actividades pueden llevar mucho tiempo, y sus resultados son importantes para decidir los siguientes pasos. Los incidentes pueden durar días, semanas o incluso más. Las decisiones necesarias suelen trascender el ámbito de TI y afectar a las operaciones de negocio, con la participación de personas que desempeñan funciones clave en la organización.

Todo ello hace que organizar y realizar ejercicios sea una tarea exigente. Resulta difícil liberar al personal clave de sus tareas habituales durante ejercicios prolongados. Por eso, es poco probable que estos ejercicios puedan realizarse con la frecuencia suficiente para adquirir experiencia en un plazo razonable.

Los organismos reguladores también han reconocido la importancia de los ejercicios. Actualmente, suelen exigirse a organizaciones de especial importancia, como los operadores de infraestructuras críticas. Las directivas NIS y NIS2 de la UE señalan los ejercicios como una de las formas de prepararse eficazmente ante un posible incidente.

Todos estos retos dieron lugar al desarrollo de Cyber Conflict Simulator, un simulador interactivo que aborda la respuesta a incidentes de ciberseguridad de una forma diferente.



Cyber Conflict Simulator (CCS) es un sistema de software diseñado para las personas responsables de gestionar incidentes de ciberseguridad en los ámbitos civil y militar.

CÓMO FUNCIONA

Cyber Landscape

Imagine que pudiera trasladar sus sistemas de TI y de negocio a un entorno virtual. Podría configurarlos para que funcionaran igual que en el mundo real. CCS permite describir cómo los servicios de negocio o los procesos de producción dependen de los sistemas de TI que son objeto de un ataque, así como las consecuencias de la interrupción de dichos sistemas.

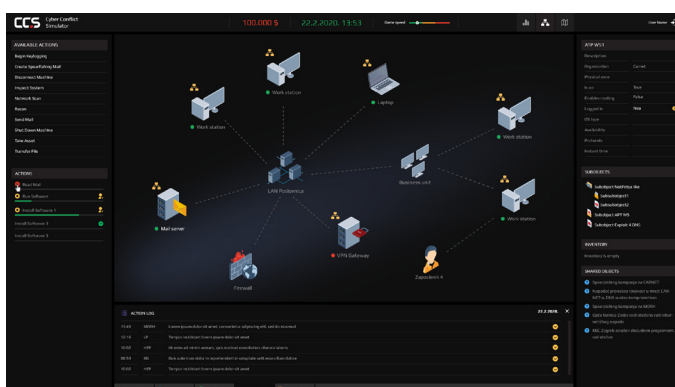
El sistema de TI se representa mediante objetos como ordenadores, servidores, dispositivos móviles, redes, sistemas operativos, software, servicios, archivos, bases de datos y sistemas SCADA. CCS también permite definir dependencias respecto a servicios externos. Estos servicios pueden verse interrumpidos por un incidente de ciberseguridad o servir como punto de entrada para un atacante.

Las personas son una parte importante de cualquier organización: administradores de sistemas, especialistas en análisis forense digital, técnicos, analistas y el resto del personal. Forman un equipo virtual que los participantes gestionan durante la simulación.

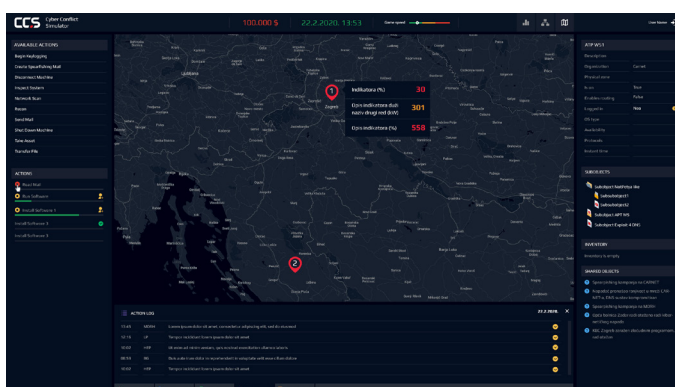
Los atacantes pueden modelarse para representar distintas fuentes de amenazas, incluidos Estados, grupos delictivos e individuos.

Simulación

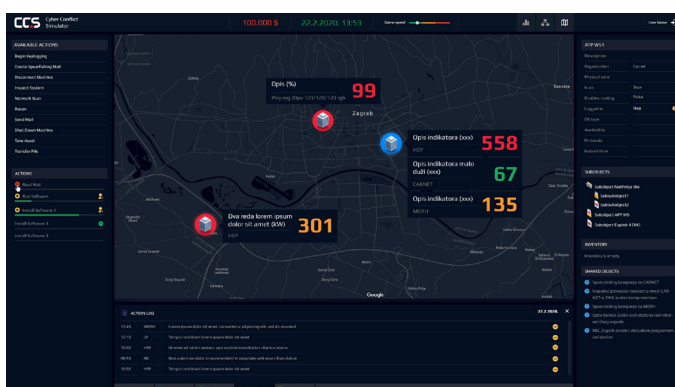
Para ser realista, un ejercicio debe modelar con precisión los eventos que tienen lugar en la infraestructura de TI, donde se origina el problema. También deben modelarse las repercusiones en el negocio, ya que reflejan los daños o las pérdidas reales que pueden producirse.



La simulación puede seguir escenarios predefinidos y pasos planificados o contar con la participación activa de un equipo de ataque (Red Team). El ejercicio puede comenzar cuando se inician las actividades ofensivas o más adelante, cuando se detecta el incidente y el atacante ya ha alcanzado algunos de sus objetivos. La persona que diseña el escenario del ejercicio decide el momento de inicio.



En la simulación pueden participar varios grupos. También pueden intervenir varias organizaciones, cada una de las cuales solo ve la información que tendría disponible en una situación real.



Los participantes asignan tareas a los miembros de su equipo virtual, a los que denominamos actores. Las habilidades de cada actor determinan qué tareas puede realizar y cuánto tiempo necesita para completarlas, igual que en la vida real. Los actores informan sobre su trabajo y sus resultados. A partir de esta información, los participantes deciden los siguientes pasos para resolver el incidente.

Durante el ejercicio, los participantes suelen tener que esperar a los resultados de las actividades de los actores. En esos momentos, la simulación puede acelerarse y volver a ralentizarse en cualquier momento. Esto permite completar el ejercicio en mucho menos tiempo del que durarían los hechos en la vida real. Con CCS, un ciberataque que duraría días o semanas puede simularse en solo unas horas.

Una vez definido el ciberespacio virtual, puede realizar un número ilimitado de ejercicios con distintos escenarios. El ejercicio depende en gran medida de los recursos de los que dispone el atacante y de las técnicas de ataque que utiliza. Esto ofrece una amplia variedad de posibilidades para crear escenarios de ejercicios.



Todos los pasos y eventos del ejercicio se registran y se incluyen en el informe de simulación. Esto permite mejorar la estrategia de defensa, las tácticas, las técnicas, los procedimientos y el sistema en su conjunto.

Hay muchas preguntas importantes para la ciberdefensa. ¿Puede detectarse un ataque de forma temprana? ¿Con qué facilidad puede un atacante desplazarse por su organización hasta alcanzar su objetivo? La lista continúa.

La mejor manera de obtener respuestas es poner a prueba sus defensas. CCS es una herramienta valiosa para evaluar su sistema de TI. Permite simular distintos ataques contra su organización y comprobar con qué facilidad puede detectar y contener un ataque y, finalmente, comprender lo que ha ocurrido realmente.

Puede introducir vulnerabilidades de día cero en cualquier componente de su sistema y comprobar cómo afectan a sus defensas en caso de ataque.

■ Funciones principales



FLEXIBILIDAD

Cree un ciberespacio virtual que se corresponda plenamente con su sistema de información real.



ESCALABILIDAD

Modele sistemas complejos incluyendo a todas las organizaciones relacionadas.



INTERACTIVIDAD

El resultado de la simulación depende por completo de las acciones de los participantes.



EXTENSIBILIDAD

Amplíe el sistema con nuevos objetos, acciones y controles mediante un mecanismo de complementos.



GESTIÓN DEL TIEMPO

Acelere la simulación siempre que quiera acortar el ejercicio y ahorrar tiempo.



LECCIONES APRENDIDAS

Analice los pasos realizados durante el ejercicio en una evaluación posterior y mejore las tácticas y técnicas defensivas de su equipo.

Convierta la práctica en preparación



CCS

**El eslabón que
falta en su
ciberdefensa**

Utilis CCS permite evaluar el grado de preparación de su organización para responder a incidentes de ciberseguridad. Le ayuda a comprobar la robustez de su sistema de TI y a preparar el elemento más importante de su defensa: las personas.

CCS está diseñado para los responsables de gestionar incidentes de ciberseguridad en los ámbitos civil y militar. Simula distintos tipos de ciberataques contra su sistema de información y permite definir un ciberespacio virtual compuesto por diferentes objetos.

CCS facilita las siguientes tareas

- Evaluar la respuesta y el rendimiento de su sistema y de su equipo de respuesta a incidentes de ciberseguridad en caso de ataque
- Probar sus procedimientos de respuesta a incidentes de ciberseguridad y sus planes de comunicación
- Ahorrar tiempo y otros recursos en la preparación para poder realizar más ejercicios con menos esfuerzo
- Simular en unas horas incidentes de ciberseguridad que durarían días o semanas

- Adquirir experiencia y habilidades mediante ejercicios con distintos escenarios de ataque
- Aumentar la concienciación sobre las amenazas a su sistema de TI

«De los errores se aprende», como dice el refrán. Los errores durante incidentes reales de ciberseguridad pueden resultar muy costosos, por lo que es mejor cometerlos primero durante los ejercicios. Hemos diseñado CCS para que sea muy fácil de usar. Además, puede ampliarse fácilmente mediante un sistema de complementos.

En su fase inicial, la Agencia Europea de Defensa (EDA) reconoció CCS como un proyecto innovador de doble uso, con aplicaciones militares y civiles, y lo seleccionó para recibir apoyo técnico.

Organice un ejercicio

Un equipo de expertos de Utilis y FER puede preparar todo lo necesario para realizar un ejercicio con una implicación mínima de su organización.

Póngase en contacto con nosotros si tiene alguna pregunta adicional, desea solicitar una presentación o quiere organizar un ejercicio adaptado a su organización.

+385 (1) 36 35 666

info@utilis.biz



Utilis Ltd.
Fallerovo šetalište 22
10000 Zagreb, Croacia
www.utilis.biz
ccs.utilis.biz



**Cofinanciado por
la Unión Europea**