TDIR

PREPARACIÓN ACTIVA

Devel
CYBERSECURITY REDEFINED

- Web: www.deve.group
- Email: info@develsecurity.com
- Guatemala - El Salvador - Honduras - Rep. Dominicana

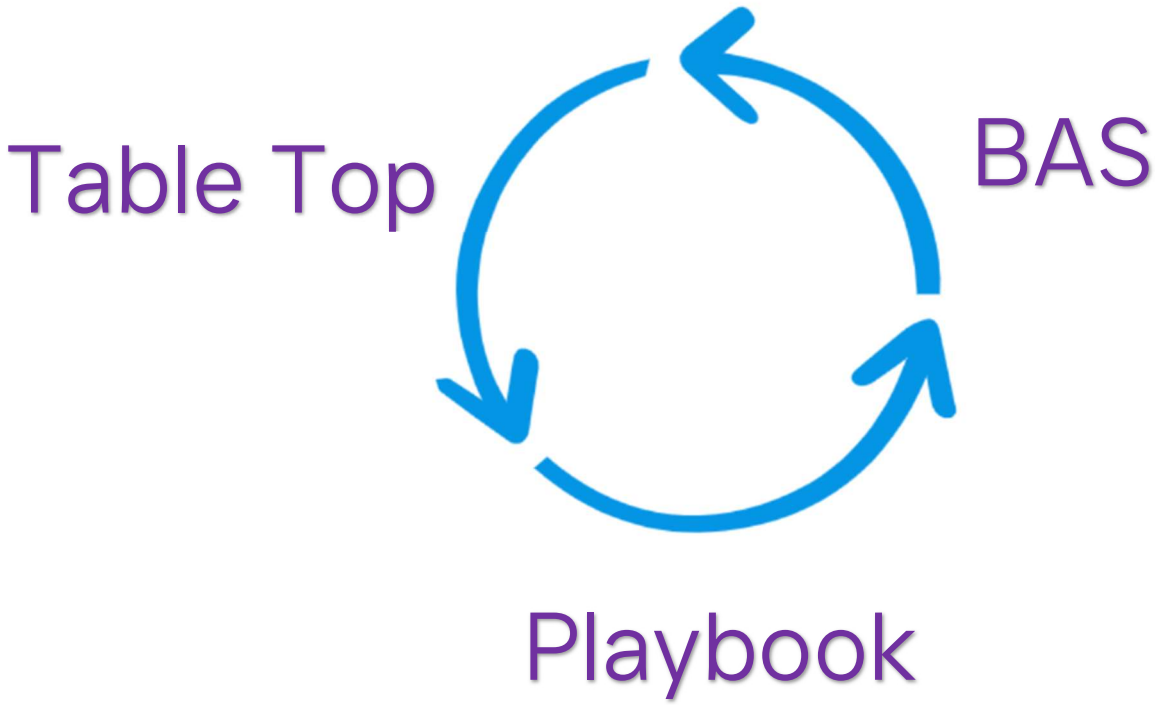
Índice

¿Qué es Preparación Activa?

La preparación activa es el conjunto de prácticas, metodologías y simulaciones que permiten a una organización anticiparse a incidentes de seguridad, estas ya están incluidas por el servicio SOC contratado con Devel Security, fortaleciendo de forma proactiva sus capacidades de respuesta. A diferencia de un enfoque meramente reactivo, la preparación activa busca validar la efectividad de los procesos, entrenar al personal y comprobar la eficiencia de los controles técnicos antes de enfrentar un ataque real cada año, durante la vigencia del servicio.

Servicios

Ofrecemos un ciclo integral de preparación frente a incidentes de seguridad que combina Playbooks, Table Top y Breach and Attack Simulation (BAS). Los Playbooks definen procedimientos claros de respuesta, los Table Tops validan su aplicación en escenarios simulados y colaborativos, y el BAS pone a prueba la eficacia técnica mediante ataques controlados en tiempo real. En conjunto, garantizan procesos sólidos, equipos entrenados y controles de seguridad verificados para enfrentar amenazas actuales y emergentes.



Playbooks

Nuestro servicio está diseñado para evaluar y optimizar la postura de ciberseguridad de su organización, con un enfoque en la mejora continua y en la alineación con las mejores prácticas internacionales. A través de una sesión estructurada, se lleva a cabo un diagnóstico integral, una evaluación detallada y un proceso de fortalecimiento de sus capacidades de respuesta ante incidentes, poniendo especial atención en la fase de preparación mediante el uso de cinco playbooks de referencia.

Playbooks de referencia

- Ransomware
- Ataque de red
- Sitio de phishing
- Correo de phishing
- Malware

Cronograma de actividades

Fase 1 – Diagnostico:

En esta fase se llevará a cabo la aplicación de un checklist de los controles actualmente implementados en la organización, con el propósito de evaluar de manera precisa la postura de seguridad existente. Una vez completado, el checklist será compartido para su posterior traslado a la plataforma. Cualquier duda o detalle adicional será revisado y validado de forma conjunta con el equipo correspondiente.

Fase 2 – Seguimiento de Preparación:

En esta etapa se revisará el resumen de los controles actualmente implementados en la organización, con el objetivo de evaluar su alcance y efectividad. Se validará el estado de aquellos controles que no estén completamente aplicados, determinando si se encuentran en proceso de implementación, aplicados parcialmente o si se han presentado dificultades en su ejecución. Al finalizar, se entregará un enlace con las herramientas recomendadas para optimizar la aplicación de estos controles.

Fase 3 - Aseguramiento del Uso Correcto de herramientas:

En esta fase se presentará un escenario común que sea aplicable a los playbooks, explicando paso a paso cómo se implementaría cada uno en dicha situación. Se realizará una demostración de herramientas recomendadas, detallando su propósito y el valor que aporta dentro del flujo de los playbooks, con el objetivo de garantizar una comprensión clara y práctica de su funcionamiento en el contexto de la organización.

Fase 4 – Cierre y Retroalimentación

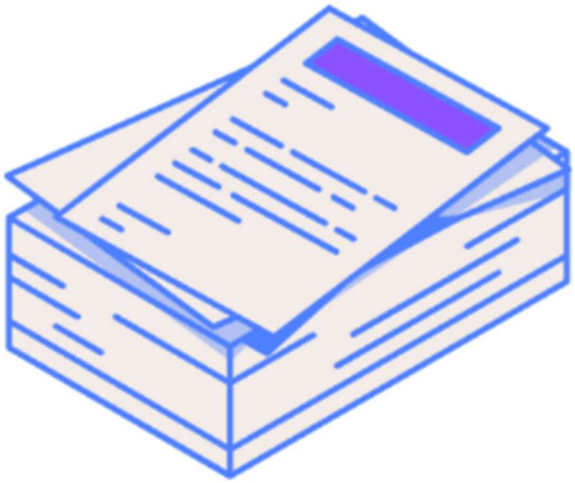
En esta etapa se realizará un repaso de la evolución del proceso, presentando un resumen general y mostrando el progreso por fase, incluyendo los puntos cumplidos, en progreso y pendientes. Se presentará un gráfico o tabla que resuma la situación por cada playbook, seguido de la validación final del cumplimiento del checklist, revisando el estado actual de cada control y clasificándolo como “implementado”, “en progreso” o “no implementado”.

Table Top

Los ejercicios Table Top son una dinámica de simulación diseñada para fortalecer la preparación organizacional en ciberseguridad, continuidad de negocios y gestión de crisis. A través de esta metodología, los equipos conformados por representantes de distintas áreas analizan y discuten, de manera guiada, la forma en que responderían ante un escenario hipotético de incidente o crisis.

A diferencia de un simulacro práctico, nuestro enfoque Table Top se desarrolla en un entorno teórico y conversacional, sin impacto sobre los sistemas ni la infraestructura de la organización. Durante la sesión, se revisan y evalúan los roles, responsabilidades, procesos y decisiones críticas, facilitando la identificación de fortalezas, brechas y oportunidades de mejora en la capacidad de respuesta.

Los ejercicios Table Top permiten evaluar de forma realista la efectividad de los planes de respuesta a incidentes, fortaleciendo la preparación de los equipos, mejorando la comunicación entre áreas y detectando oportunidades de mejora. Además, impulsan el compromiso de la alta dirección y validan que los procedimientos existentes respondan adecuadamente ante una crisis.



Cronograma de actividades

Fase 1 - Kickoff (Cliente/Devel):

La fase inicial del ejercicio comienza con la sesión de Kickoff, que constituye el punto de partida oficial de la actividad. En este espacio se busca alinear a todos los participantes en torno a los objetivos estratégicos, el alcance y la metodología del ejercicio. También se presentan los requerimientos necesarios y se detallan los lineamientos que guiarán su desarrollo.

Fase 2 - Ejecución (Cliente/Devel):

La segunda fase corresponde a la ejecución del ejercicio de Tabletop, desarrollada en una sesión de 1 hora y 30 minutos, de los cuales al menos 60 minutos se destinan de manera efectiva a la simulación. En esta etapa participan los integrantes designados por el cliente que forman parte del proceso de respuesta ante incidentes, con el objetivo de validar la coordinación entre equipos, evaluar la efectividad de los procedimientos y detectar oportunidades de mejora frente a situaciones críticas.

Fase 3 - Evidencias (Cliente):

La tercera fase contempla la recopilación de evidencias durante y después del ejercicio, donde se solicita al cliente la entrega de procedimientos, políticas y playbooks internos u otra documentación que hayan sido mencionados en la simulación. Este material permite validar la veracidad y efectividad de los documentos, asegurando que los controles y lineamientos establecidos estén correctamente formalizados y sean aplicables en la práctica.

Fase 4 - Informe de resultados (Cliente/Devel):

La cuarta y última fase corresponde a la presentación del informe de resultados, una sesión de aproximadamente 30 minutos en la que se exponen los hallazgos, conclusiones y principales aprendizajes derivados del ejercicio. Este espacio permite al cliente conocer de manera clara las fortalezas identificadas, así como las áreas de mejora necesarias para fortalecer su proceso de respuesta ante incidentes.

Breach & Attack Simulation (BAS)

Servicio de Simulación de Brechas y Ataques (BAS) proporciona a su organización una visión clara y en tiempo real de su capacidad para enfrentar ciberamenazas. Mediante la recreación controlada de tácticas, técnicas y procedimientos empleados por atacantes reales, este servicio permite evaluar efectividad de los controles implementados y fortalecer los procesos de detección, contención y respuesta ante incidentes.

A diferencia de un ejercicio de Red Team que busca evadir controles de seguridad como AppLocker y soluciones AV/EDR/XDR durante semanas, los ejercicios de BAS se realizan típicamente en 1 a 2 horas y parten de la hipótesis de que el atacante ya se encuentra dentro y ha ejecutado acciones maliciosas. A partir de ese punto evaluamos tres aspectos: la visibilidad (si la telemetría captura las actividades maliciosas), la generación de alertas (si el sistema notifica al equipo correspondiente) y la capacidad operativa (qué tan efectivos son los procesos actuales para contener y remediar la amenaza).

Para la ejecución de las pruebas de Breach and Attack Simulation (BAS) se emplean herramientas especializadas como Scythe, las cuales permiten emular tácticas y técnicas de ataque de manera controlada, evaluando la capacidad de detección, respuesta y contención de la organización.

Preguntas Clave que Resuelve el Servicio BAS

Contactos

IT Project Manager II - Karla Hernandez

Correo: khernandez@devel.group

Adversarial Simulation, IR & Detection Engineer Coordinator - Sergio Mazariego

Correo: smazariego@devel.group