ETP TECNOLOGÍA

Smart SOAR para MSSP

D3 SECURITY

Orquestación, Automatización y Respuesta de Seguridad

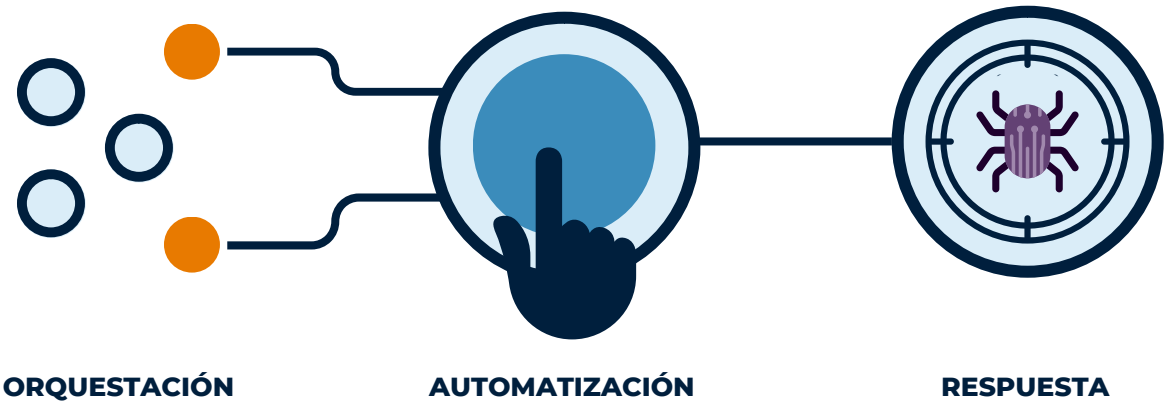
Las plataformas de orquestación, automatización y respuesta de seguridad (SOAR) se han convertido en un elemento básico del centro de operaciones de seguridad (SOC) empresarial moderno, debido a su gran capacidad de reducir la complejidad, acelerar las operaciones y unir tecnologías dispares y silos de datos. Sin embargo, a pesar del surgimiento de SOAR en la empresa, es particularmente adecuado para los proveedores de servicios de seguridad administrados (MSSP), tanto en términos de mejorar sus operaciones como de habilitar nuevas fuentes de ingresos. Al finalizar este documento podrá entender el valor que nuestro Smart SOAR le puede brindar a su MSSP a diferencia de SOAR Tradicionales.

ETP TECNOLOGÍA

D3 SECURITY

¿QUÉ ES UNA PLATAFORMA SOAR?

La orquestación, automatización y respuesta de seguridad (SOAR) es una tecnología importante para la seguridad de TI, el centro de operaciones de seguridad (SOC) y los equipos de respuesta a incidentes (IR) que desean mejorar la velocidad, la calidad y la eficiencia de sus operaciones. SOAR ayuda a las empresas a recopilar alertas de seguridad e inteligencia de amenazas, optimizar el análisis y la clasificación, y orquestar acciones entre herramientas y personal dispares. Juntas, estas capacidades aumentan la velocidad de la toma de decisiones y la remediación, lo que reduce significativamente el riesgo para la organización.



GARTNER DEFINE SOAR COMO LA COMBINACIÓN PERFECTA DE TRES TECNOLOGÍAS DISTINTAS:

Respuesta a Incidentes de Seguridad: Incluye documentación de incidentes, asignación de tareas e investigación / gestión de casos.

Orquestación y Automatización: Automatiza el flujo del trabajo de herramienta a herramienta, principalmente para clasificación y remediación simple pero carece de gestión de casos, informes y otras características a nivel ejecutivo.

Inteligencia contra Amenazas: Reúne múltiples fuentes de inteligencia de amenazas externas en un sólo lugar con algunas capacidades de correlación. Requiere soluciones adicionales para actuar sobre la inteligencia.

CÓMO UN MSSP SE BENEFICIA DE SOAR

La tecnología de orquestación, automatización y respuesta a incidentes de seguridad (SOAR) de D3 Security es un componente crítico de los SOC MSSP en todo el mundo. Dicho esto, contar con la tecnología de D3 MSSP es mucho más que solo el software. Trabajamos con nuestros clientes MSSP para ayudarles a optimizar su uso de D3 Smart SOAR y alcanzar sus objetivos comerciales.

Mejorar los márgenes de utilidad a través de la automatización, introduciendo nuevos servicios de alto valor y diferenciar las ofertas de los competidores son solo algunos de los resultados observados por nuestros clientes MSSP. Lo que le permite ir más lejos y más rápido.

USOS DE SOAR PARA MSSP

1. Agregar valor y aumentar las ganancias al mejorar los servicios brindados.
2. Escalar las operaciones sin necesidad de un equipo de trabajo grande, aumentando así los márgenes.
3. Integrar el stack de seguridad de su cliente de manera eficiente.
4. Usar los flujos de trabajo guiados y la automatización para incorporar más rápido al nuevo personal.
5. Proporcionar una mejor visibilidad a sus clientes.

ETP TECNOLOGÍA

D3 SECURITY

TECNOLOGÍA SMART SOAR PARA MSSP

La tecnología de orquestación, automatización y respuesta a incidentes de seguridad (SOAR) de D3 Security es un componente crítico de los SOC MSSP en todo el mundo. Dicho esto, contar con la tecnología de D3 MSSP es mucho más que solo el software. Trabajamos con nuestros clientes MSSP para ayudarles a optimizar su uso de D3 Smart SOAR y alcanzar sus objetivos comerciales.

Mejorar los márgenes de utilidad a través de la automatización, introduciendo nuevos servicios de alto valor y diferenciar las ofertas de los competidores son solo algunos de los resultados observados por nuestros clientes MSSP. Lo que le permite ir más lejos y más rápido.

BENEFICIOS TECNOLÓGICOS DE SMART SOAR

Los MSSP podrán ofrecer servicios de clase mundial a sus clientes, impulsados por la única plataforma SOAR que está diseñada específicamente para las necesidades de los MSSP: **D3 SMART SOAR**

ETP TECNOLOGÍA

D3 SECURITY

PORTAL DE CLIENTES DE MSSP

Los MSSP tendrán una ventaja única cuando se trate de atraer y retener clientes con el Portal de Clientes de Smart SOAR. Este portal es una ventanilla única para administrar las interacciones con los clientes y compartir información. En lugar de enviar correos electrónicos y esperar respuestas, toda la comunicación puede ocurrir en un entorno seguro que se encuentra conectado a Smart SOAR. Los beneficios clave incluyen:

- Mantener a sus analistas enfocados en la seguridad. No más perseguir clientes para obtener aprobaciones y entradas.
- Respuesta más rápida a incidentes de seguridad. Las aprobaciones de clientes pueden desencadenar tareas pendientes automáticamente.
- Demostrar valor a los clientes. Los dashboards del portal mantienen a los clientes informados del trabajo que como MSSP está haciendo, sin necesidad de realizar informes manuales.

ETP TECNOLOGÍA

D3 SECURITY

FUNCIONES	SMART SOAR	SOAR TRADICIONAL
Integraciones ilimitadas	Integración sencilla de cualquier producto con el soporte de D3	Las integraciones pueden requerir codificación lo que puede limitar la calidad de éstas según los intereses del proveedor
Diseño experto de integración	El equipo de D3 estudia diversas herramientas para diseñar integraciones que cierren las brechas de detección y mitigación de cada herramienta	La mayoría de las integraciones se basan en APIs públicas con funcionalidades básicas
Incorporación de clientes / tenant	Incorporación de nuevos clientes / tenants rápidamente con un flujo de trabajo de incorporación automatizado	Incorporación manual
Solución multinivel y multinenant	Administración de todos los clientes desde una única interfaz, mientras mantiene los datos, sitios y configuraciones segregadas de forma segura	El Multitenant limitado puede causar ineficiencia, seguridad deficiente e incumplimiento normativo
Controles de acceso basados en roles (RBAC)	Controles de acceso robustos y personalizables para garantizar la seguridad de la información	La granularidad de los controles de accesos variará entre plataformas

FUNCIONES	SMART SOAR	SOAR TRADICIONAL
Triaje autónomo basado en el riesgo (RBAT)	Clasificación de alertas más rápidamente con mayor confianza para filtrar los falsos positivos y priorizar amenazas reales	La correlación y automatización limitadas implican mayor trabajo manual sin asegurar un triaje confiable
Pipeline de eventos	Normalización, correlación y priorización automática de alertas	Automatización limitada a incidentes, no incluye alertas
Playbooks sin código	Construcción, prueba e implementación de playbooks a través de una interfaz sencilla de arrastar y soltar, no code o low code	Creación de playbooks requiere codificación de un programador especializado
Correlación entre dimensiones	Búsqueda de patrones e incidentes pasados, presentes, TTPs y artefactos	Correlación limitada a coincidencia de artefactos entre alertas
Memoria de alertas y artefactos	90 días de almacenamiento para enriquecer y clasificar alertas	Muchas plataformas SOAR no tienen almacenamiento por lo que las alertas pasadas no se pueden utillzar en el análisis
Respuesta basada en identidad	Incorporación de datos de identidad para un mejor análisis	No utiliza datos de identidad
Portal Cliente	Colabore y comparta información con sus clientes en un portal seguro e integrado	Comunicación fuera de plataforma SOAR como email y tickets

> La conciencia del peligro es ya la mitad de la seguridad
>
> Ramón J. Sénder

ETP Tecnología es una empresa mexicana con consultores con más de 30 años de experiencia especializados en mejores prácticas de Administración de Activos y Ciberseguridad.

Nuestro enfoque se basa en la optimización de la inversión en TI, contribuyendo a la reducción del gasto no planeado o no identificado; a su vez, contribuimos a la habilitación óptima de la tecnología con el apoyo de Servicios Profesionales y de Consultoría.

Contáctanos

José Luis García
(55) 5415 7355
joseluis.garcia@grupoetp.mx

Zesergio Mendoza
(55) 7845 0122
zesergio.mendoza@grupoetp.mx

ETP TECNOLOGÍA

D3 SECURITY