Servicios Gestionados de Seguridad

Centro de Operaciones de Seguridad como un Servicio

El escenario de amenazas está en constante evolución, causando aumento de los costos y complejidades en seguridad. SOCaaS de NTT aprovecha las inversiones realizadas en su plataforma SIEM para vencer esa batalla

Habilidades en seguridad

Montar un equipo de operaciones de seguridad es un gran desafío. La operación de una plataforma SIEM en régimen 24x7 requiere de conocimientos profundos en diversas áreas. La gestión de la plataforma, investigación de amenazas e informes de conformidad son sectores en que la mayoría de las empresas están descubriendo que poseen pocos conocimientos para garantizar una seguridad consistente.

Los recursos existentes tienden a analizar un gran volumen de alertas, pero queda la incertidumbre de si están encontrando los verdaderos ataques.

Las plataformas SIEM líderes de mercado, poseen excelentes recursos para analizar todos los eventos y entregar los respectivos informes de conformidad. Sin embargo, pocas empresas poseen la capacidad de direccionar sus inversiones en herramientas de seguridad e integrarlas de forma correcta en la plataforma SIEM.

SOCaaS (por sus siglas en inglés para Security Operation Center as a Service) de NTT ofrece un servicio 100% gestionado. Además de ofrecer la implementación de SIEM, brinda también toda la gestión de la plataforma, detección de las amenazas cibernéticas, informes de conformidad, personalización de casos de uso, creación de dashboards y desarrollo de playbooks para escalamiento de los incidentes.

Demandas además del tradicional MSSP

Las compañías necesitan acceso instantáneo a grandes cantidades y variedades de información, al mismo tiempo que las aplicaciones y los datos que generan se están moviendo por varios ambientes en la nube. Esas son las tendencias en el desarrollo de negocios, permitiendo que la empresa crezca, se adapte y se vuelva cada vez más competitiva.

Desafortunadamente, también son los vectores de ataques para las nuevas amenazas cibernéticas avanzadas, trayendo un gran riesgo a los negocios, ya que pocas empresas poseen los recursos para un combate efectivo contra esas amenazas. Al mismo tiempo que los requisitos de seguridad son cada vez más altos, es necesario superar la lista de obstáculos provenientes de la transformación digital. La definición de una estrategia para la detección de amenazas, y la capacidad de implementarla en la práctica, se vuelve esencial.

Las fuentes de datos necesarias para los informes de conformidad y de negocios están en constante actualización. A medida que las aplicaciones de negocio se transforman, los orígenes también cambian y los casos de uso para detectar los incidentes de conformidad necesitan estar siempre actualizados. Una vez que un patrón de conformidad es implementado, los informes necesitan ser constantemente ajustados para que estén actualizados con los cambios en los procesos de negocios, las nuevas aplicaciones y los cambios en la infraestructura.

SOCaaS combina los recursos nativos de las plataformas SIEM del mercado con una metodología y experiencia comprobada de NTT para la detección efectiva de ataques cibernéticos. Un servicio gestionado que incluye gestión total de la plataforma SIEM, detección y validación de los ataques cibernéticos (evitando falsos positivos), personalización de casos de uso, creación de dashboards e informes de conformidad. Como parte del servicio de **SOCaaS**, nuestros especialistas de seguridad ofrecen atención 24 horas por día, 7 días por semana, ritmo que normalmente las empresas tienen dificultad de mantener utilizando sólo recursos internos.

Principales beneficios de SOCaaS de NTT

- **Reducir los riesgos relacionados con el negocio, encargos administrativos y costos.**
- **Cumplir con las conformidades regulatorias requeridas por cada industria.**
- **Maximizar el uso funcional de la plataforma SIEM.**
- **Hacer que la operación de SIEM sea más escalable y flexible con especialistas certificados.**

Nuevo ambiente o gestión del actual

Si el cliente ya posee una plataforma SIEM en operación, podemos gestionar el ambiente actual. En caso contrario, podemos implementar un nuevo ambiente, utilizando las mejores prácticas de mercado y nuestros conocimientos técnicos en las mejores tecnologías de SIEM.

SOCaaS ofrece:

- Todo el equipo de SOC 24x7 con especialistas certificados en seguridad.
- Gestión de la plataforma de SIEM, incluyendo estado y disponibilidad, aplicación de parches y respaldo de las configuraciones.
- Configuración de la plataforma de SIEM, incluyendo la sintonización de las reglas.
- Creación de casos de uso personalizados, dashboards e informes.
- Monitoreo de eventos y alertas de incidentes de seguridad 24x7.
- Monitoreo de conformidad, informes y notificaciones personalizadas, basadas en playbooks.
- Playbooks personalizados y acompañamiento de todo el ciclo de vida del incidente.

Cómo funciona SOCaaS

SOCaaS es un servicio a medida para gestión de SIEM y análisis de alertas de seguridad. El servicio ofrece productos de seguridad líderes de mercado, utilizando procesos conocidos para la entrega a través de funcionarios certificados. Provee visibilidad del ambiente, acelerando la identificación de las alertas para el escalamiento necesario, mientras proporciona modelos de riesgos de forma proactiva y con soporte para toda la mitigación. **SOCaaS** maximiza el valor de las inversiones en otras tecnologías de seguridad, aumentando el nivel de madurez en ésta. Posibilita la concentración de los esfuerzos en el negocio, sin una sobrecarga para mantener, monitorear y operar la plataforma de SIEM con recursos internos.

La configuración de SIEM está personalizada para los requisitos de negocio de cada cliente. NTT inicialmente realiza una evaluación del ambiente identificando todos los elementos-clave, como topología de red, equipamientos generadores de los registros, localización de los centros de datos y análisis del ambiente de red para desarrollar el plano de entrega del servicio.

La detección, el análisis y los informes detallados de los incidentes relativos a los ataques cibernéticos son entregados a través de una metodología comprobada por NTT a través de las capacidades de las plataformas de SIEM líderes del mercado. Los eventos más importantes son analizados por analistas de seguridad con procesos de escalamiento bien definidos, con el fin de garantizar el recibimiento de los informes de incidentes de forma precisa y en tiempo hábil para que se tome una acción correcta de forma rápida.

Cómo funciona SOCaaS

Los informes con las conformidades regulatorias requeridas por las industrias son generados a través de funcionalidades existentes en las plataformas de SIEM. NTT configura el conjunto de reglas necesarias para el correcto monitoreo y la detección de las violaciones de las políticas de conformidad. La adherencia al cumplimiento de las políticas de negocios se puede lograr a través de casos de uso personalizados. Las notificaciones de eventos pueden ser configuradas de forma selectiva, para ser enviadas apenas se accione una regla.

Con **SOCaaS**, establecemos un punto de consolidación, mejorando la organización de la seguridad y colaborando con la visibilidad en tiempo real de todo el ambiente, permitiendo la realización del monitoreo correcto de seguridad.

Contáctenos

Si quiere saber más sobre nuestro servicio de **SOCaaS**, o está interesado en una evaluación, comuníquese con su Client Manager o contáctenos aquí:

Leader IDC MarketScape:
Worldwide Managed Security Services (MSS) 2020 Vendor Assessment

Leader IDC MarketScape:
Asia Pacific Managed Security Services (MSS) 2020 Vendor Assessment

2020 Asia Pacific Managed Security Services Provider of the Year

Certified for Cyber Security Incident Response and Penetration Testing, Audited for SOC Certification

Conversemos

¿Por qué **NTT**?

EXTENSO HISTÓRICO DE EVENTOS
Mitigamos 2 mil millones de eventos por año.

RECURSOS DE AUTOMATIZACIÓN DE LA PRÓXIMA GENERACIÓN Acceso a análisis, entrega de los servicios y desarrollo de procesos exhaustivos.

CICLO DE VIDA COMPLETO
Transformamos metas en resultados a través de un ciclo de vida completo de servicios.

ESCALA GLOBAL
Prestamos servicios en más de 200 países en los 5 continentes.

Everything is i**NTT**erconnected