CASO DE ÉXITO

La implementación de Sentinel permitió a Rizobacter integrar todas sus plataformas en un solo monitor, detectando posibles ataques externos y monitoreando más de 40 servicios en una sola plataforma. Además, la compañía logró monitorear a los 800 usuarios globales que tienen en la nube, reduciendo significativamente el tiempo de investigación y análisis de posibles amenazas.

Rizobacter es una compañía argentina líder en microbiología agrícola que investiga, desarrolla y comercializa soluciones innovadoras para el mejor crecimiento de los cultivos en el mundo. Siendo parte del grupo Bioceres Crop Solutions está fuertemente posicionada en el mercado local y comercializa sus productos en más de 40 países.

Anteriormente, la compañía tenía dificultades para centralizar y monitorear todas sus plataformas de manera eficiente, lo que generaba un riesgo no adecuado para la organización en cuanto a la detección de amenazas y ataques cibernéticos. Contaban con una plataforma que no se podía integrar a cualquier otra con la velocidad y necesidad que se precisaba para el negocio. **"Se demoraba mucho tiempo en leer las alertas y esto implicaba un riesgo muy alto. El área de sistemas necesitaba más dinamismo, más velocidad y más adaptabilidad."** Señala **Augusto Zanocco, Jefe de Tecnología y Comunicaciones**. Agrega que actualmente tienen una globalización muy grande, con un dinamismo de empresas en varios países, por lo que necesitaban una herramienta que se pudiera adaptar a dicho contexto.

Además, el crecimiento de una cultura de trabajo desde cualquier lugar impone demandas intensificadas a la ciberseguridad: incluso con un dispositivo corporativo bien protegido, un empleado que usa una red no confiable o una red inalámbrica pública puede exponer datos de la empresa sin saberlo. Por lo que, evaluando constantemente su postura de ciberseguridad, el equipo de sistemas opto por la solución de Microsoft Sentinel, una herramienta nativa cloud que ayuda en la administración de eventos e información de seguridad (SIEM) y en la respuesta automatizada de orquestación de seguridad (SOAR). Proporciona análisis de seguridad y alertas sobre amenazas corporativas (que se pueden priorizar y visualizar en listas), así como para responder ante estas. También ahorra un tiempo valioso porque la IA integrada y el aprendizaje automático de Microsoft Sentinel envían alertas procesables al equipo desde Azure Log Analytics, consolidando la visibilidad..

La colaboración y el trabajo en equipo entre **Bernardo Anzoategui, Responsable de Infraestructura IT** y Prisma Soluciones Tecnológicas resultaron fundamentales para el éxito de este proyecto. De manera simple y transparente, el proceso de implementación se llevó a cabo en menos de dos meses, permitiendo que la compañía cuente con un SIEM funcional al 100%, listo para optimizar o seguir expandiéndose de acuerdo con las necesidades de la empresa.

RIZOBACTER

prisma soluciones tecnológicas

Al mismo tiempo, el equipo de seguridad pudo crear reglas analíticas personalizadas para detectar eventos de Login no autorizados con cuenta de administrador local en los servidores, lo que permitió detectar y reportar rápidamente cualquier anomalía o ataque en proceso.

Con la incorporación de Sentinel, la empresa pudo integrar todas sus plataformas en un solo monitor y empezar a ver resultados rápidamente. **Augusto Zanocco** asegura que obtuvieron beneficios de centralización, flexibilidad e integración y comenta que una de las grandes ventajas que se obtiene por medio de la solución, es la incorporación de una inteligencia que pueda detectar y relacionar los ataques con el fin de entenderlos. Sentinel les permite centralizar el control y reducir el tiempo de investigaciones de dos horas a 20-30 minutos, lo que se traduce en un ahorro de tiempo y dinero para la empresa. De modo que no hay que estar atacando problema por problema, sino que se puede hacer con una mirada global de manera centralizada. Por otra parte, el uso de inteligencia artificial agiliza la identificación de posibles amenazas. También, sus capacidades de personalización permiten customizar las formas de detección de amenazas y cómo visualizarlas en un panel de control.

Gracias a la creación de reglas inteligentes para detectar el uso indebido de permisos, ha logrado controlar a los 800 usuarios globales que tienen en la nube, reduciendo significativamente el tiempo de investigación y análisis de posibles amenazas. La plataforma ha permitido detectar posibles ataques externos y monitorear más de 40 servicios en una sola plataforma, ahorrando tiempo y recursos en comparación con las más de 10 plataformas previas utilizadas. La trazabilidad y la inteligencia de la plataforma permitió reducir el tiempo de investigación y análisis en un cuarto del tiempo anterior. Además, la implementación ha permitido detectar la correlación entre diferentes plataformas y tomar decisiones automáticas para actuar contra posibles ataques, lo que ha permitido achicar los tiempos de auditoría y reducir los costos del servicio de control, pasando de tener un servicio tercerizado a gestionarlo con su propio equipo de TI.

En definitiva, la organización ha logrado optimizar su seguridad informática y proteger sus plataformas y datos gracias a la solución de Microsoft Sentinel. La compañía ha integrado y consolidado toda su información en un solo lugar, lo que le ha permitido monitorear de manera eficiente los eventos y actuar rápidamente ante cualquier irregularidad o amenaza.

Para futuro, el área de sistemas de Rizobacter busca planificar y reforzar campañas de prevención de riesgos laborales en el lugar de trabajo. Como también realizar entrenamientos constantes de machine learning o inteligencia artificial para desarrollar reglas cada vez más inteligentes y autónomas. Ya que como sabemos cada año se duplican los incidentes de seguridad, aparecen nuevas amenazas y tipos de fraudes; siendo la información el activo más importante para las organizaciones y el usuario el eslabón más débil en la cadena de seguridad.