La empresa mexicana de logística que predice los futuros ciberataques

La clave: visibilidad total

El aumento de la digitalización, el uso de la tecnología de la información y las comunicaciones para cumplir funciones críticas en la industria de la logística trajeron nuevos aspectos de riesgo que deben gestionarse, pues cuando alguna de las partes involucradas es vulnerada, es solo cuestión de tiempo antes de que suceda algo gravemente negativo.

Bajo esta realidad, Onest Logistics, compañía 3PL logística, líder en México que provee soluciones integrales en la cadena de suministro, buscó una solución que le diera una visibilidad completa de los eventos de riesgo de ciberseguridad, tanto en la infraestructura de aplicaciones como los equipos de los usuarios, con el objetivo de reducir el número de incidentes, así como el impacto asociado a las aplicaciones y usuarios.

Ver el ataque antes de que suceda

Al ser reconocida en el país por otorgar a sus clientes una flexibilidad total, amplio conocimiento logístico, capacidad de innovación y procesos de alta calidad, Onest Logistics no podía permanecer indiferente ante los nuevos riesgos, así que buscó una solución que identificara oportunamente anomalías para estar un paso adelante de los atacantes. Pero, sobre todo, un socio tecnológico que la acompañara en todo el viaje: desde la consultoría y el dimensionamiento del proyecto, hasta el apoyo de expertos y el suministro de tecnología de última generación que brinde mayor confianza a sus clientes.

Datos Onest Logistics

- Operador logístico 3PL, 100% mexicano fundado hace 18 años, apasionado por sus clientes y su gente.
- Reconocido por su flexibilidad, amplio conocimiento logístico, capacidad de innovación y procesos de alta calidad.
- Considerado como la mejor opción en servicios integrales de logística en el país.

Retos a enfrentar

- Descripción del proceso y áreas donde fue implantado, así como entender el papel de los empleados y directivos ante cada probable circunstancia.
- Comunicación de datos y la opción de bloquear información en caso de algún evento de riesgo, además de evitar el uso de agentes para recolectar los datos y enviar la información a **Prophecy** mediante una conexión segura.
- Personalización de indicadores, alertas, modelo de predicción, tableros y diseño de una interface de visualización a medida.
- Reportes ejecutivos, añadiendo la posibilidad de elegir las fechas de ejecución.

"Puedo dedicarme a otras actividades con la confianza de que mis sistemas informáticos se encuentran protegidos y, si algo sucede, tengo la certeza de que Prophecy me alertará en mi móvil".

Yael López
Gerente de Seguridad Informática en Onest Logistics

Así fue como se optó por la implementación de **Prophecy,** una solución que se desplegó en un modelo de Software as a Service, la cual permite conectar los logs de operación de cada uno de los firewalls que atienden, tanto a las oficinas corporativas como a los almacenes de operaciones, para detectar los problemas a medida que surgen (idealmente antes de que interrumpan la experiencia del cliente), responder rápidamente y resolverlos lo antes posible.

El grado de personalización que obtuvo Onest Logistics con la solución de KIO Networks, a partir del uso de Prophecy, así como las funcionalidades analíticas para el modelado y alertamiento de los índices de compromiso, fue determinante en su elección.

Ahora la compañía cuenta con indicadores en aplicaciones, usuarios, protocolos, VPN, email, vulnerabilidades, IPS y antivirus, así como en las funcionalidades de Alerta de IoC's basadas en reglas de operación y Alerta de predicción de caídas de VPN. Como complemento, se sumó a la plataforma un módulo de reporteo que permite al cliente enviar a dirección los indicadores más relevantes dentro de la operación. Se sabe que un sorprendente 97% de las empresas se han visto afectadas por una brecha de seguridad cibernética en su cadena de suministro, mientras que los ataques en el primer trimestre de 2021 en este sector en los EE. UU. afectaron a siete millones de personas[1].

Los desafíos

Al ir configurando una solución a la medida del cliente, un reto relevante fue la descripción del proceso y áreas en dónde se implantaron.

Otros aspectos importantes fueron detallar las áreas de la empresa involucradas y el papel de los empleados o directivos en cada circunstancia, así como diseñar un esquema de comunicación que permitiera al cliente contar con la opción de cerrar la comunicación en caso de algún evento de riesgo, además de evitar el uso de agentes para colectar los datos que impactaran al performance de los dispositivos.

Para solucionarlo, se contó con el apoyo del cliente para desplegar un colector dentro de su infraestructura que permitiera recaudar en sitio los datos para enviarlos posteriormente a Prophecy, mediante una conexión segura. En tanto que la consulta de datos se realizó a través de un protocolo nativo en los dispositivos que envían la información al colector antes mencionado.

Cada proyecto es un traje a la medida, en este caso se personalizaron los indicadores, alertas y modelos de predicción, así que los tableros publicados para el cliente fueron diseñados desde cero con el fin de mostrar solo aquellos indicadores de su interés, además de elegir las visualizaciones y gráficos adecuados para cada Indicator of Compromise (IoC). Y lo mismo se llevó a cabo tanto para el motor de alertas como el motor analítico, ya que ambos responden a aquellos casos considerados por el cliente como relevantes.

En cuanto a los indicadores dentro del dashboard, los resultados son analizados con el equipo directivo de Onest Logistics, por lo que resultó imperativo añadir un módulo que permitiera concentrar en un reporte ejecutivo la operación mensual, añadiendo la posibilidad de elegir las fechas de ejecución.

[1]BlueVoyant Research (2021). BlueVoyant Research Reveals Rise in Supply Chain Cybersecurity Breaches as Firms Struggle to Effectively Monitor Third-Party Cyber Riskconsultadoenenero de 2022.

Onest Logistics redujo en un **30%** los **costos de software**

El futuro

Onest Logistics ve a Prophecy como su SOC automatizado, ya que puede confiar en que las alertas recibidas son las que realmente pueden afectar a su operación, además de que accede no solo a los datos que puede consultar a partir de la plataforma, sino con el respaldo del equipo de especialistas certificados.

De esta forma es como Onest Logistics se toma la seguridad como un aspecto crítico, ya que una brecha en el sistema podría dañar o interrumpir las operaciones de todos sus clientes y generar costos innecesarios o cronogramas de entrega ineficientes.

La cadena de suministro global enfrenta grandes desafíos y KIO Networks tiene la experiencia de más de dos décadas y más de 400 especialistas dispuestos a combinar estrategias audaces y tecnologías transformadoras para ayudar a las organizaciones a innovar de manera más sostenible y lograr ganancias duraderas.

Hoy Onest Logistics tiene en Prophecy un diferenciador en la entrega del servicio a sus clientes, que contribuye a un movimiento de mercancías más seguro y eficiente que se recupera rápidamente ante las interrupciones.

El éxito es notorio

- Se redujeron en un 30% los costos de software.
- El tiempo invertido en el análisis de la operación de Firewall disminuyó de 72 horas a una hora, aunado a que ahora se hace de manera automatizada, evitando el costo del pago a un especialista.
- El proceso de las funciones de reporteo tomaba al menos 3 días y personal dedicado, ahora es parte de la solución y se puede llevar a cabo en el momento en que se necesite.
- La reducción del número de eventos de parches de seguridad y los eventos de antivirus e IPS disminuyó a 90% menos incidentes en equipos infectados.
- Los clientes nacionales e internacionales tienen la confianza de que mientras su información pase por Onest Logistics está protegida y, por lo tanto, sus inversiones. Algo que pocos proveedores locales pueden garantizar.

Tecnología implementada

- **Prophecy:** analítica avanzada como servicio.
- Solución de Inteligencia Artificial que predice anomalías para minimizar la indisponibilidad de los sistemas de misión crítica de tu negocio. Aporta visibilidad completa de tu ecosistema, como redes, aplicaciones y amenazas de seguridad.
- Predice posibles problemas, reduce el tiempo de revisión exhaustiva de 7 horas a solo 20 minutos y agiliza la identificación de la causa raíz del problema.