Sentria By Netdata

Caso de Éxito

El rescate costaba diez veces más que un año de servicio.

Rescate exigido: más de 10 veces el costo anual del servicio

Ransomware contenido y erradicado en 4 días

85% de las tareas manuales de seguridad automatizadas

MTTD de 10 minutos y MTTR de 120 minutos

Desafío

Un viernes de fin de semana largo, una farmacéutica multinacional latinoamericana descubrió que estaba bajo un ataque de ransomware. Sus operaciones estaban cifradas y la nota de rescate exigía una cifra que superaba en más de diez veces el costo anual de todo su servicio de ciberseguridad.

La compañía llevaba años operando con un modelo de protección que funcionaba. Meses antes, por una decisión de estandarización tomada en su casa matriz, había sido obligada a migrar hacia una tecnología distinta a la que venía utilizando. El ataque llegó después de ese cambio.

El contexto operativo agravaba el riesgo. La organización sostiene su operación regional con un equipo de tecnología de dos personas, responsables de toda la infraestructura. En una industria donde el downtime se mide en millones de dólares y donde la cadena de distribución no admite pausas, la pregunta no era si podían pagar el rescate, sino cuántos días de operación detenida podían resistir.

Contratar especialistas en ciberseguridad en el mercado local nunca había sido una alternativa viable: el costo de un equipo interno con capacidad de respuesta 24/7 excedía por mucho el de un servicio gestionado, y la disponibilidad de ese talento es escasa.

Proceso

La compañía activó el servicio de respuesta a incidentes Sentria 911. La contención y erradicación de la amenaza tomó cuatro días, sobre un fin de semana festivo. El miércoles siguiente la operación se reanudó sin interrupciones adicionales y sin pago de rescate.

Ese resultado no fue casualidad. Detrás había casi una década de relación construida. El vínculo comenzó años antes con un diagnóstico de red: el cliente arrastraba problemas de lentitud con equipos perimetrales dimensionados por debajo de lo que exigían sus tres sedes. El análisis identificó el error de dimensionamiento y propuso un cambio de estrategia de despliegue, no solo un reemplazo de hardware.

Esa primera respuesta abrió la puerta a un hito regional: la organización fue la primera en Latinoamérica en desplegar la plataforma de protección de endpoints de Palo Alto Networks para este cliente. Con los años, la relación se amplió hacia dispositivos móviles para la fuerza de visita médica y hacia el despliegue de servidores en la nube.

Tras el incidente, la compañía consolidó su postura de seguridad sobre Cortex XDR, ampliando la cobertura de 200 a 250 endpoints, integrada al monitoreo continuo del servicio gestionado.

Sentria

Solución

El modelo combina la plataforma Cortex XDR con el servicio Sentria 911 de respuesta a incidentes, sobre una operación de seguridad gestionada. La solución integra:

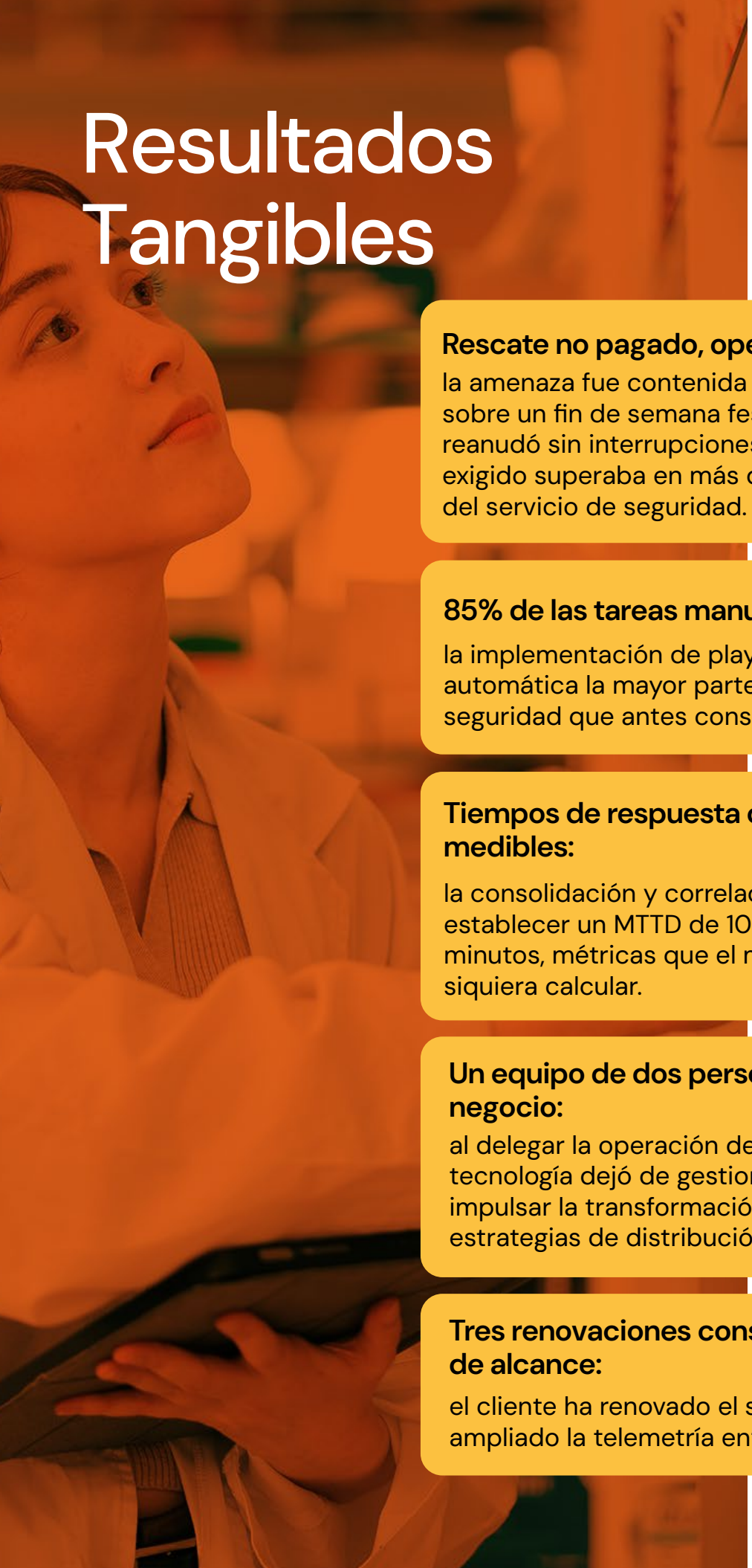
Consolidación y correlación de telemetría sobre 250 endpoints, base de las métricas comprometidas de detección y respuesta.

Automatización mediante playbooks, que hoy resuelven de forma autónoma cerca del 85% de las tareas que antes se gestionaban manualmente.

Servicio Centro 911 de contención y erradicación, disponible sin compromiso de compra previo como demostración real de capacidad de respuesta.

Postura proactiva de ciberdefensa, con cacería de amenazas e inteligencia aplicada al sector farmacéutico.

Implementación ejecutada de forma autónoma: Netdata es una de las tres entidades certificadas en Latinoamérica para desplegar sin depender de la cola de atención del fabricante, lo que reduce costos y tiempos de puesta en marcha.



Resultados Tangibles

Sentria

Rescate no pagado, operación no detenida:
la amenaza fue contenida y erradicada en cuatro días sobre un fin de semana festivo, y la operación se reanudó sin interrupciones adicionales. El monto exigido superaba en más de diez veces el costo anual del servicio de seguridad.

85% de las tareas manuales automatizadas:
la implementación de playbooks trasladó a ejecución automática la mayor parte del trabajo operativo de seguridad que antes consumía al equipo.

Tiempos de respuesta comprometidos y medibles:
la consolidación y correlación de telemetría permitió establecer un MTTD de 10 minutos y un MTTR de 120 minutos, métricas que el modelo anterior no permitía siquiera calcular.

Un equipo de dos personas enfocado en el negocio:
al delegar la operación de seguridad, el área de tecnología dejó de gestionar incidentes y pasó a impulsar la transformación digital, incluyendo nuevas estrategias de distribución y canales digitales.

Tres renovaciones consecutivas y ampliación de alcance:
el cliente ha renovado el servicio tres años seguidos y ampliado la telemetría entregada.

Testimonio del Cliente

"Credibilidad. Esa es la palabra. Cumplen siempre lo que prometen, y eso en ciberseguridad no es un detalle: es la diferencia entre un proveedor y un aliado"

Gerencia de Tecnología.

La confianza construida se ha traducido en recomendaciones activas hacia otras compañías del sector farmacéutico, canalizadas a través de redes de colaboración profesional de la industria.

Conclusión

Ningún proveedor puede prometer que un ataque no ocurrirá. Lo que sí se puede comprometer es qué pasa cuando ocurre: cuánto se tarda en contenerlo, cuánto en erradicarlo y cuánto vuelve a operar el negocio. Este caso responde esas tres preguntascon cifras.

La diferencia no estuvo solo en la tecnología. Estuvo en una relación de casi una década que permitió activar una respuesta coordinada un fin de semana festivo, y en un equipo certificado para ejecutar de forma autónoma, sin esperar la cola de atención del fabricante. Cuando el reloj corre, esa autonomía es el resultado.

Para una organización que sostiene su operación regional con dos personas en tecnología, delegar la ciberseguridad no fue una decisión de costos: fue la única forma de tener capacidad de respuesta 24/7 y, al mismo tiempo, liberar a su equipo para construir el negocio.

Sentria By Netdata