grupo analytiko

Inteligencia y Tecnología contra el fraude

Casos de Estudio

Banca y Finanzas I

Un alto ejecutivo de un Banco Latinoamericano tenía la sospecha que en la Gerencia de Investigaciones estaban siendo manipulados los indicadores de productividad y las estadísticas generales referentes a los procesos de resolución de casos.

Luego de iniciar un proceso de Auditoría Interna minucioso, la Gerencia encontró que los casos a investigar se anotaban manualmente en una lista, según un orden de aparición y los investigadores decidían que casos tomaban para analizarlos, sin tener en cuenta ningún criterio de asignación o selección. Lo cual generaba:

- ***Daño reputacional a la Institución:*** *Al encontrarse casos sin haber sido procesados o investigados o con largos tiempos de desatención, por no haber sido registrados en el inventario.*
- ***Pérdidas financieras:*** *Por reintegros de reclamos debido al vencimiento de los lapsos máximos de respuesta al cliente ante fraudes dados por la normativa.*
- ***Violación de Código de Conducta y Antifraude de la Institución:*** *Algunos investigadores aprovechaban las oportunidades para seleccionar los clientes a los que investigar y solicitar comisiones para tramitar su caso y reintegrar sus saldos defraudados.*

La Alta Gerencia tomó la decisión de desechar el proceso manual y contratar a *Grupo Analytiko* para gestionar eficientemente los equipos de investigadores. Los resultados fueron inmediatos al establecimiento de controles en el proceso:

- *Los tiempos de resolución y los índices de productividad fueron confiables.*
- *La asignación de casos supervisada y la carga equilibrada de trabajo entre el personal, produjo un incremento en la productividad de los equipos.*
- *Los índices confiables arrojados por las estadísticas produjeron una mejora en la Gestión de Riesgo de Fraude.*
- *Mejoró la opinión de los clientes al momento de verificar su experiencia con los resultados del nuevo proceso.*

Banca y Finanzas II

El vicepresidente de Seguridad de un banco en Latinoamérica nos plantea la siguiente problemática:

La Unidad de Monitoreo de Fraudes (Capa de Detección y Respuesta Inmediata), encargada de recibir, gestionar y procesar las alertas generadas por el aplicativo de Detección de Fraude en Tiempo Real, posee un proceso manual de análisis resultando en tiempos de respuesta lentos para descubrir la ruta del dinero defraudado, también para analizar la validación de usuario ante el canal e iniciar el proceso de recuperación de fondos.

Este problema le ha generado al banco:

- ***Pérdidas financieras:*** *Al no lograr procesar rápidamente todos los datos asociados al fraude, la institución pierde un tiempo de reacción valioso que no permite la inmediata contención y recuperación de fondos defraudados, debiendo recurrir a provisiones o seguros para afrontar el reclamo del cliente.*

continúa:

Banca y Finanzas II *continuación*

- ***Posibles hechos de colusión de empleados y agentes externos en los fraudes:*** *Una amenaza interna que es realmente preocupante y que posee un alto riesgo de ocurrencia si no existen tanto controles como bitácoras del proceso que puedan ser auditadas.*
- ***Alta rotación de empleados:*** *Gestionar manualmente procesos de respuesta inmediata a fraudes agrega altos componentes de presión sobre los equipos de analistas, generando bajos resultados de recuperaciones de fondos y altos niveles de frustración en el personal.*
- ***Gestión ineficiente del riesgo de fraude:*** *El registro ineficiente de datos de fraudes, genera estadísticas e indicadores poco confiables impactando directamente en la retroalimentación y ajuste de las reglas o modelos de las soluciones de detección.*

Para cumplir con el requerimiento, *Grupo Analytiko* ofreció la Solución *Analytiko®* junto con el componente *Skuld®*, dotando a la Unidad de Monitoreo de una herramienta integrada al software de detección de fraudes en tiempo real que ya poseía el banco, agilizando la adquisición y asignación de las alertas a los analistas.

Los analistas e investigadores cuentan además con herramientas de análisis visual ofrecidas por *Immersion®*, como Analisis de Redes Sociales y Líneas de Tiempo, que les ayudan a comprender y ubicar rápidamente el flujo de dinero defraudado.

Nuestra Solución ayudó a:

- *Mejorar los tiempos de respuesta en la Gestión de Alertas.*
- *Ayudar a mejorar los indicadores de contención y recuperaciones de fondos defraudados.*
- *Mejorar la gestión de trabajo dentro de los equipos de analistas.*
- *Permitir a Gerentes y Supervisores a obtener indicadores de gestión confiables.*

Telecomunicaciones

La Vicepresidencia de seguridad de una empresa de Telecom en Latinoamérica requirió de nuestros servicios para dotar a su Unidad de Ciberinteligencia adscrita a su SOC (Centro de Operaciones de Seguridad) de una herramienta con la capacidad de:

- *Integración de los procesos operativos de estas Unidades.*
- *Generar y mantener una base de conocimiento de actores, tácticas y puntos de compromiso.*
- *Tener a disposición una trazabilidad de los procesos de detección, investigación y respuesta de contra amenazas y vulnerabilidades de la corporación.*
- *Contar con herramientas de análisis y adquisición, conectada tanto a fuentes de datos internas de información (logs y bases de datos), como a fuentes externas y que ayude a visualizar la interconexión de las diferentes capas de datos para convertirlos en inteligencia.*

Nuestro equipo de desarrollo integró la Solución *Skuld®* y *Analytiko®* junto con un software de Análisis Visual y OSINT conectados al SIEM (que ya poseía la corporación) para la gestión de alertas en el SOC. Para potenciar el proceso de análisis se integraron todas las aplicaciones que en forma conjunta apoyan a los investigadores y analistas en el proceso de adquisición, procesamiento y análisis de datos.

Los equipos de ciberseguridad generan resultados acertados y de gran valor, ya que, cuentan con una solución de generación de Inteligencia sobre Amenazas, la cual está focalizada en la protección de los activos críticos de la corporación, aportando a los analistas las siguientes ventajas competitivas:

- *Obtención de Alertas desde dispositivos de monitoreo para la asignación a los ciberanalistas.*
- *Obtención rápida y eficiente de datos de fuentes internas.*
- *Entorno de análisis con énfasis en colección de evidencia e informes individuales.*
- *Base de conocimiento de amenazas, actores y tácticas a disposición de los analistas.*
- *Integración entre los equipos de Ciberseguridad y Ciberinteligencia bajo un mismo entorno.*