telecom

xelere
Making IT better

Soluciones y servicios

IBM SOAR

"El desafío era buscar una solución que nos permitiera cambiar la forma de trabajar del equipo de ciberseguridad. Alternativas que aceleren la gestión, la interacción con las otras áreas y poder subirnos al mundo de la agilidad, alcanzando mayores niveles de automatización y orquestación en cada una de las herramientas. Siendo más eficientes y efectivos a la hora de actuar ante incidentes de ciberseguridad".

Adrián Judzik,
Sr. Manager CyberSecurity de Telecom Argentina

Telecom implementa la solución IBM Security SOAR como parte del proyecto CybOrg

Telecom Argentina ofrece experiencias de conectividad, entretenimiento y soluciones tecnológicas en todo el país. Potencia la vida digital de sus más de 30 millones de clientes, con un servicio flexible y dinámico, en todos sus dispositivos, mediante conexiones fijas y móviles de alta velocidad, y una plataforma de contenidos en vivo y a demanda que integra series, películas, gaming, música y programas de TV.

Sus marcas comerciales Telecom, Personal y Flow consolidan un ecosistema de plataformas, y nuevos negocios, una experiencia integral y convergente para individuos, empresas e instituciones en todo el país. Está presente en Paraguay con servicio móvil y en Uruguay, con televisión paga.

País

Argentina, Paraguay y Uruguay

Cita Telecom

"Cada vez que nos juntamos, el equipo de Xelere y Telecom, no es el equipo de Xelere y Telecom. Es el equipo que está trabajando para hacer de la herramienta IBM SOAR y de las necesidades de Telecom, un único proyecto. En cada reunión que tenemos se nota la pasión que tenemos para ir hacia adelante, como un proyecto muy desafiante de Telecom, pero aún así no hay divisiones"

Adrián Judzik,
Sr. Manager CyberSecurity de Telecom Argentina

Industria

Telecomunicaciones

Tamaño

22.5 mil empleados

Beneficios

- Mejoras del 96% en los tiempos de respuesta ante incidentes
- Detección y bloqueo automático de los posibles spams
- Reducción del 50% en intervenciones efectivas de los colaboradores fuera de horario
- Protección para los usuarios reducida de días a horas, dedicando tan sólo el 80% del equipo
- Inicio de un proceso de re skilling que empoderó en un 46% a los equipos de ciberseguridad
- Desarrollo de nuevos playbooks, integraciones y automatizaciones
- Integración de los equipos de trabajo mejorando la calidad de vida de las personas
- Gestión de incidentes desde una sola plataforma
- Centralización del seguimiento de los incidentes

"Al poder automatizar muchos de los casos de uso, nos permitió reducir horarios por fuera del trabajo normal. (...) Tareas repetitivas en las que antes intervenían personas y tardábamos horas en integrar, orquestar y llegar a la solución del tema, hoy se hacen en minutos y los equipos pueden abocarse a tareas que aportan mayor valor. Redujimos los tiempos en incidentes, siendo más eficientes; y las soluciones aplicadas más efectivas. Todas las prácticas que modelamos nos permiten reutilizar y aprovechar aquello que aprendimos en incidentes previos. Es un win constante que uno ve durante todo el proyecto."

Adrián Judzik,
Sr. Manager
CyberSecurity de
Telecom Argentina

telecom

xelere
Making IT better

Desafío

Al comienzo de la pandemia, Telecom tuvo que mudar su operatividad a la modalidad virtual, con el 70% de los colaboradores trabajando de forma deslocalizada. Gracias a las inversiones realizadas y al proceso de transformación digital, logró que cada empleado pueda conectarse desde su hogar para realizar las tareas. Sin embargo, la infraestructura de la compañía se vio más expuesta a posibles ataques informáticos.

Bajo este escenario, el principal reto se centró en reescribir todos los procesos de gestión de ciberseguridad y resolución de incidentes, modelarlos, documentarlos e implementarlos sobre una solución que permita una visión integral de la seguridad de la compañía; todo esto basándose en la automatización y orquestación de los procesos.

Solución

Para la realización de este proyecto se utilizó una metodología de trabajo ágil para su implementación y gestión del backlog mediante KanBan. Enfocándose en diseños, desarrollos e implementaciones en sprints iterativos para obtener, rápidamente, una entrega de valor, sumado a la captura de nuestra experiencia diaria para generar nuevas mejoras en las futuras versiones o ampliación del alcance de las funcionalidades de la solución.

Los ciclos fueron no mayores a dos meses, donde se dio prioridad a los procesos de incidentes y, posteriormente, la integración de los procesos operativos para su registración, orquestación y automatización. Todo gracias a la solución de IBM Security SOAR.

"Gracias a la implementación de esta metodología se pudieron realizar acciones de mejora en los procesos como, por ejemplo, el tratamiento de los post incidentes o acortar los tiempos de gestión de distintos requerimientos de horas a minutos." Adrián Judzik, Sr. Manager CyberSecurity de Telecom Argentina

telecom

xelere
Making IT better

Beneficios

"A partir de CybOrg y la implementación de IBM SOAR, desde Telecom logramos disminuir la resolución de incidentes. Hoy tenemos implementado el 100% de los procesos críticos." Adrián Judzik, Sr. Manager CyberSecurity de Telecom Argentina.

A modo de ejemplo, la infraestructura de Doble Factor de Autenticación, ha mejorado en un 96% los tiempos de respuesta ante incidentes, sin alojar recursos y automatizando el proceso y sus tareas repetitivas.

Para Spam Interno: hoy se detecta y se bloquea de manera automática los casos de posibles spams que se identifican en los correos salientes. Se redujo en un 50% las intervenciones efectivas de los colaboradores fuera de horario (durante las guardias).

En Incidentes de Phishing, una vez obtenidos los posibles indicadores de compromiso, se ingresan en el playbook correspondiente realizando los bloqueos en todos los elementos orquestados y de forma automática. De esta forma la protección para los usuarios se redujo de días a horas y en un 80% el equipo dedicado.

"A partir de aquí, incrementamos el impulso para mejorar y consolidar la metodología diagramada al inicio, escalando a más servicios y operatorias de ciberseguridad." Adrián Judzik, Sr. Manager CyberSecurity de Telecom Argentina

Próximos pasos

Telecom planea continuar con con nuevos ciclos de implementación, con hitos importantes como la integración con el SIEM para que todos los incidentes sean canalizados y gestionados a través de IBM Security SOAR.

telecom

xelere
Making IT better

Acerca de Xelere

Xelere es una empresa de servicios de consultoría de TI con más de 20 años de trayectoria. Nuestra propuesta de valor se centra en ayudar a las empresas a optimizar los servicios que provee el área de TI al negocio.

Con soluciones y servicios en más de 10 países de América Latina, contamos con un gran equipo de consultores altamente capacitados a nivel metodología, procesos y herramientas de software líderes del mercado basados en ITIL®, ISO/IEC 2000, CobIT y DevOps.

Creemos que la calidad, el liderazgo y el trabajo en equipo, junto con una visión orientada a resultados, es la estrategia ideal para optimizar la TI de una empresa.

Acerca de Telecom S.A

Telecom S.A es una empresa de soluciones de conectividad y entretenimiento, con más de 23.000 colaboradores en todo el país. Transforman la experiencia digital de sus más de 28 millones de clientes ofreciéndoles un servicio seguro, flexible y dinámico, en todos sus dispositivos, con conexiones fijas y móviles de alta velocidad, y una plataforma de contenidos en vivo y a demanda que integra series, películas, gaming, música y programas de TV. A través de sus marcas comerciales Personal, Fibertel, Flow y Telecom | Fibercorp brinda servicios de telefonía fija y móvil, transmisión de datos, televisión paga e Internet, para individuos, empresas e instituciones en todo el país. Además están presentes en Paraguay con servicio móvil y en Uruguay, con televisión paga.

Lideran una industria que constituye uno de los pilares para el desarrollo social y económico del país y participan activamente en la comunidad con prácticas sustentables e iniciativas que agregan valor al uso de la tecnología como herramienta para la formación e inclusión social.