

SMU fortalece su estrategia de ciberseguridad con Palo Alto Networks

Marcelo Fabio

Subgerente de Op. y Proyectos de Seguridad
SMU S.A.

Fernando Carreño

Regional Sales Manager
Palo Alto Networks



Desde 2020, la decisión de SMU de incorporar tecnología Palo Alto Networks ha consolidado y fortalecido significativamente la estrategia de ciberseguridad de la compañía. La colaboración comenzó con la implementación de una plataforma de seguridad en la nube, una medida fundamental para enfrentar los desafíos de transformación digital que SMU estaba experimentando.

Debido a los excelentes resultados obtenidos, la protección se extendió al perímetro y a las redes internas, y posteriormente, se incorporó la protección de seguridad para los usuarios remotos, facilitando la movilidad segura en todo momento. Además, se implementó la plataforma de nueva generación Cortex, ofreciendo protección local a los servidores y estaciones de trabajo. Sobre este tema, así como los próximos desafíos conjuntos, conversamos con Marcelo Fabio, Subgerente de Operaciones y Proyectos de Seguridad en SMU S.A., y Fernando Carreño, Regional Sales Manager de Palo Alto Networks.

Seguridad en la Nube: El primer paso

En la estrategia de migración a la nube de una parte importante de los servicios de SMU, generó "la necesidad de contar con un socio estratégico para garantizar la se-



seguridad, visibilidad y control en este entorno fue fundamental para nuestra transformación digital”, señala Marcelo Fabio, de esta manera se comenzó con la adopción de una plataforma de seguridad para la nube, lo que permitió gestionar de manera segura sus servicios en entornos multicloud.

El éxito en la nube impulsó a SMU a expandir la protección a su red interna y perimetral con los firewalls de Palo Alto Networks. Fabio comenta que esta medida permitió asegurar “nuestras redes y proteger la información crítica de la empresa”, replicando la seguridad también para los usuarios remotos, quienes ahora disfrutan de acceso seguro y eficiente desde cualquier lugar.

La integración como ventaja competitiva

Con el tiempo, SMU amplió su estrategia incorporando Cortex, la plataforma de seguridad de nueva generación. Fernando Carreño, regional sales manager de Palo Alto Networks, destaca que “Cortex utiliza inteligencia artifi-

cial para ofrecer protección avanzada y automatizada en tiempo real, lo que permite a las empresas enfrentar amenazas informáticas de manera proactiva”.

“Ha sido un cambio fundamental para SMU”, destaca Marcelo Fabio, agregando que “ya no estamos viendo soluciones aisladas, sino una plataforma integrada que respalda nuestra estrategia a mediano y largo plazo. La ventaja de tener distintos productos del mismo fabricante es la integración y correlación de los eventos y logs generados por cada uno de ellos”. Lo cual permite que, de manera natural, las diferentes soluciones ‘conversen’ dentro de la misma plataforma, brindando mayor visibilidad e interpretación de lo que sucede en la organización. “Para los operadores del SOC, esto se traduce en una mayor eficiencia para tomar acciones rápidas y oportunas frente a las amenazas. Todos estos beneficios respaldan, sin duda, nuestra filosofía en SMU: tomamos la ciberseguridad muy en serio. El equipo de seguridad no solo es relevante, sino que un actor crítico dentro de la organización”, recalca Fabio.

Por su parte, Fernando Carreño subra-

ya que “nuestra comunicación es permanente, lo que nos permite avanzar juntos en la estrategia de seguridad, ajustando el camino a medida que enfrentamos nuevos desafíos y oportunidades”. Lo que es ratificado por el ejecutivo de SMU, quien señala que “la cercanía con Palo Alto Networks nos permite identificar de manera proactiva los problemas que surgen. Les compartimos nuestras inquietudes, lo que nos “duele”, y ellos nos ofrecen soluciones basadas en su expertise. Esta relación de confianza y colaboración es clave para el éxito de nuestra estrategia de ciberseguridad”.

Desafíos Futuros

De cara al futuro, ambos voceros coinciden en que el foco estará en la automatización. Fabio subraya que el objetivo inmediato es “maximizar el rendimiento de las tecnologías implementadas y automatizar algunos procesos de nuestro SOC”, a lo que Carreño resalta que la automatización, impulsada por inteligencia artificial, será clave en los próximos pasos de la estrategia de seguridad.

“Ya estamos trabajando en integrar modelos de IA que mejoren la automatización en la empresa, un desafío a largo plazo que requiere una alineación meticulosa de procesos, personas y tecnología,” concluye Carreño. 📍