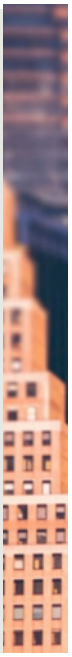
Nuvol

www.cybernuvol.com

Casos de éxito

CENTRO DE OPERACIONES SOC AS A SERVICE



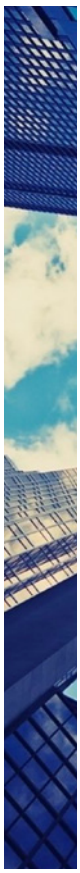
RETAIL

AMERICA LATINA

Desafio: Dado el crecimiento y expansión del grupo, la ciberseguridad se convirtio en una prioridad clave para el equipo de TI, el equipo tenía proveedores locales de seguridad, pero sentían que no estaban satisfaciendo sus necesidades; no tenían mecanismos adecuados de seguimiento a incidentes, por lo cual, el equipo decidió buscar tiempos de respuesta más rápidos y un monitoreo más avanzado para toda su infraestructura.

Durante una busqueda de varios meses encontramos a Nuvol quien nos ofrecio un servicio de Managed Detection and Response (MDR) con monitoreo y respuesta 24x7 con la garantía de contar con una visibilidad de seguridad en tiempo real. El inicio fue sencillo, una vez configurado y recopilado los logs a través de una conexión segura, habilitamos los casos de uso, mientras se nos asigno un equipo consultor de seguridad.

Resultados: No solo hemos disfrutado de tener acceso a los expertos de Proficio y Nuvol, sino hemos encontrado información de gran valor, hemos aumentado la visibilidad de seguridad de la organización y hemos podido identificar los puntos ciegos.



BANCARIO

AMERICA LATINA

Desafio: Anteriormente la organización dependía de varios sistemas de seguridad diferentes de una variedad de proveedores y no se contaba con un equipo centralizado para contactar cuando surgían alertas.

Con oficinas en diferentes regiones, el equipo requería de una visión holísitca de la seguridad con mecanismos de seguimiento de incidentes constantes, el equipo recibia un alto volumen de alertas y se requería una mejor manera de priorizar incidentes críticos.

Resultados: No más fatiga de alertas. Al aplicar casos de uso relevantes, se priorizaron los incidentes proporcionando alivio a la fatiga de alertas, con Proficio se agilizaron los procesos y se redujeron las redundancias. Al contar con un proveedor de SOC global tenemos la facilidad de contar con equipo especializado las 24 horas del día, los 7 días de la semana. Hemos sentido la confianza para saber que cuando surge un problema crítico, se está abordando rápidamente.

Nuvol

www.cybernuvol.com

IMPLEMENTACIÓN EN 30 DIAS
RUN BOOK | PLAN DE RESPUESTA A INCIDENTES

SERVICIO REMOTO
MAQUINA VIRTUAL | LOG COLLECTOR

CUMPLIMIENTO
ALINEADOS NIST Y GDPR

GOBIERNO
ESTADOS UNIDOS

Desafio: Esta gran organización de servicios públicos ofrece tecnologías y servicios de agua, gas y electricidad. Normalmente utilizaba aplicaciones con centros de datos locales, pero a medida que su negocio evolucionaba, buscaban comenzar a migrar varias aplicaciones de servicios públicos a AWS, después de la migración, comenzaron a experimentar un alto volumen de ataques a su infraestructura en la nube.

Resultados: Para garantizar que todos sus datos en la nube estuvieran seguros, Proficio creó casos de uso de monitoreo que se alinearon con los requisitos de referencias CIS que aprovecha AWS Cloudtrail, VPC flow & AWS WAF. Esto llevo al cliente examinar sus configuraciones utilizando las recomendaciones de Proficio para crear una estrategia de seguridad en la nube junto con un monitoreo en tiempo real.

FARMACEUTICO
EUROPA

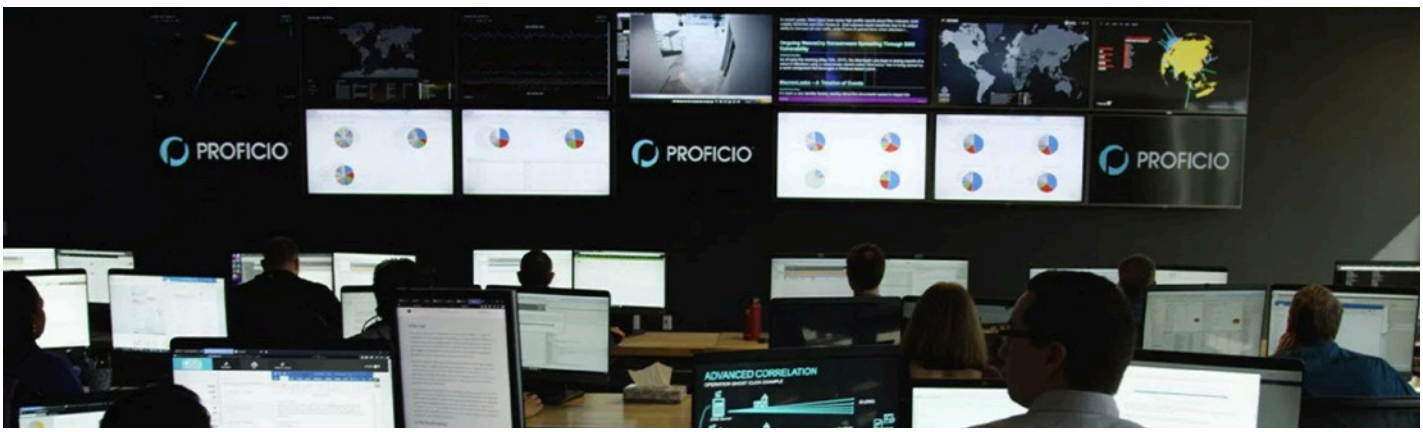
Desafio: Después de reunirse con varios proveedores, nos decidimos asociar con Proficio debido a su capacidad para brindar monitoreo, detección avanzada de amenazas y respuesta a incidentes. El equipo de seguridad señala poder accesar y aprovechar la amplia variedad de casos de uso ya desarrollados, nos ha ayudado a identificar amenazas potenciales que anteriormente podrían haber pasado desapercibidas.

Resultados: La entrega de los servicios de Proficio ha sido confiable y eficiente, el equipo ha sido receptivo, tanto que parece que pertenecen al departamento de seguridad de TI. ProviewPortal nos brinda una visión más profunda de la postura de seguridad de la organización, nos proporciona detalles, tendencias y comparaciones entre peers.

LEGAL
ASIA

Desafio: El grupo se formó en 2014 y es una de las firmas de abogados más grandes registradas en la Bolsa de Valores de Australia, desde entonces el grupo ha crecido significativamente. Requerian aliviar la limitación de recursos internos que conlleva la investigación de incidentes de seguridad.

Resultados: Proficio se ha convertido en una extensión del equipo, es un socio confiable, proporciona recomendaciones para mejorar la seguridad. Sin duda ha demostrado ser una solución mucho más rentable que construir un SOC interno, libera tiempo a nuestro equipo interno para enfocarse en otras prioridades.



Nuvol

www.cybernuvol.com

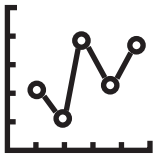
Protege tu organización las 24 horas al día

PROSOC OFRECE A LOS CLIENTES UN NÚMERO MANEJABLE DE ALERTAS DE ALTA CALIDAD

PROSOC es un servicio del tipo "Managed Detection and Response" (MDR) de clase mundial, que ofrece monitoreo de seguridad y detección de amenazas 24 horas al día, 7 días a la semana, con servicios de respuesta a incidentes automatizados.

ADMINISTRACIÓN DE LOGS

- Recolección de logs
- Almacenamiento de logs
- Log Archiving



GESTIÓN DE AMENAZAS

- Supervisión de SOC 24x7 y alertas de incidentes
- Analyst Investigation
- Notificaciones de alerta procesables
- Biblioteca de casos de uso de amenazas
- Búsqueda de amenazas verificada por analistas

DEFENSA CONTRA AMENAZAS

- Visibilidad de la postura de seguridad en tiempo real
- Threat Intelligence Profiler
- Se asigna un consultor como asesor de seguridad
- Defensa activa perimetral y de endpoints

RESPUESTA AUTOMATIZADA (SOAR)

- Equipos perimetrales
- Getión de identidades (AD)
- Seguridad de EndPoint

Nuvol

www.cybernuvol.com

¿Qué ofrecemos?

ProSOC SMB, está diseñado para organizaciones que tengan un volumen de logs por dia, entre 10 a 50 GB. La siguiente tabla muestra los entregables de la solución de respuesta y detección administrada.

"La capacidad de una organización para responder rápidamente a un incidente de seguridad, es esencial para limitar el impacto de un ataque"

PROSOC MDR for SMB	
Client Data Volume	10GB - 50GB
Service Name	
24x7 Threat Monitoring	✓
Threat Hunting	✓
Analyst Investigation	✓
Machine Learning Models	✓
Threat Content Library	✓
Threat Intelligence Profiler	✓
Active Defense Threat Response	✓
Perimeter & Endpoint Containment	✓
Threat Investigator & Search	✓
Log Management	✓
Expert on Call	✓
Security Advisor	✓
Proview Portal	✓

✓ INCLUDED ✓ OPTIONAL

10 a 50GB

CLIENT LOG VOLUME / PER DAY

* Para un volumen más alto de logs se ofrece un diseño a medida

SOLICITE UNA DEMOSTRACIÓN

cfarfan@cybernuvol.com