SECURITY OPERATION CENTER

DETECCIÓN Y RESPUESTA ADMINISTRADA

"protección avanzada contra amenazas internas y perimetrales"

NUVOL
Cybersecurity services

El auge de la ciberseguridad como servicio

Crear un SOC interno es complejo, lento y costoso. Los estudios han demostrado que el costo de construir un SOC interno puede ser cinco veces más caro que la subcontratación. Según nuestro análisis de la industria, el punto de equilibrio en el que un SOC interno tiene sentido económico comienza en las organizaciones con más de 500 dispositivos de seguridad y más de 10 000 empleados.

75%

Empresas del sector bancario, telecomunicaciones e industria están optando cada vez más por contratar los servicios de centros de operaciones de seguridad en modalidad de contrato mensual, principalmente porque les reporta ahorros en hardware, software y profesionales especialistas.

Clientes del sector bancario, por ejemplo, han reportado ahorros anuales de hasta 32% en equipamiento, 35% en licencias de software y 25% en profesionales especialistas en seguridad. Transferir el riesgo de seguridad de la operación interna de las empresas, a especialistas de seguridad, es un buen negocio y garantiza máximos niveles de seguridad en la operación.

Y tú, ¿Qué estrategia has pensado para tu organización para estos tiempos?

Acerca de Nosotros

Nuvol cuenta con varios partners de las marcas más reconocidas a nivel mundial en ciberseguridad. Una de esas alianzas es la que hay con **Proficio**. La empresa fue fundada con el objetivo de proporcionar capacidades de operaciones de seguridad de clase mundial entregados como un servicio asequible. Nuestra estrategia de negocio se centra en nuestra capacidad de proporcionar un servicio de seguridad 24x7, el cual llamamos **PROSOC**, con el objetivo que nos vean como si fuéramos una extensión de su propio equipo de seguridad.

FOLLOW THE SUN
SOC EN SAN DIEGO | BARCELONA | SINGAPUR

CERTIFICACIÓN SOC TIPO II
RIGUROSOS CONTROLES DE SEGURIDAD

+ DE 200 ESPECIALISTAS
CERTIFICADOS EN SEGURIDAD INFORMÁTICA

Nuvol www.cybernuvol.com

Protege tu organización las 24 horas al día

CONTAMOS CON TRES SOC´S: SAN DIEGO, SINGAPUR Y BARCELONA

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

PROVIEW PORTAL

- Visibilidad de gestión y amenazas en ProView Portal
- Gestión de casos de ITSM
- Investigador y búsqueda de registros

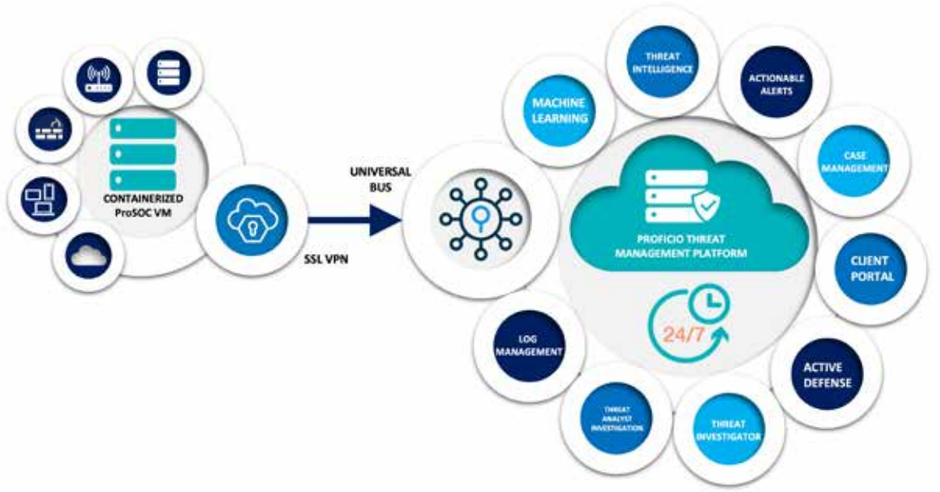
Nuvol www.cybernuvol.com

PROSOC aprovecha un Log Collector in situ para recopilar y transmitir registros de una manera segura y encriptada a nuestros SOCs

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

SERVICIO REMOTO
MAQUINA VIRTUAL | LOG COLLECTOR

CUMPLIMIENTO
ALINEADOS NIST Y GDPR



PROSOC MDR
MANAGED DETECTION AND RESPONSE

ProSOC MDR es nuestra solución principal de detección y respuesta administrada que aprovecha la plataforma de administración de amenazas nativa de la nube, que es una plataforma Open XDR que se puede implementar rápidamente para la recopilación de logs, la búsqueda de amenazas, la respuesta automatizada y la remediación, a través de Active Defense.

INTELIGENCIA DE AMENAZAS
THREAT INTELIGENCE PROFILER (TIP)

Nuestro Threat Intelligence Profiler (TIP) patentado agrega indicadores de compromiso en tiempo real, detección y enriquecimiento contextual de eventos de seguridad para una detección y alerta precisas. Estos eventos se investigan y notifican, y se escalan como incidentes con recomendaciones para acciones de remediación y respuesta automática opcional.

CAZA DE AMENAZAS
THREAT HUNTING

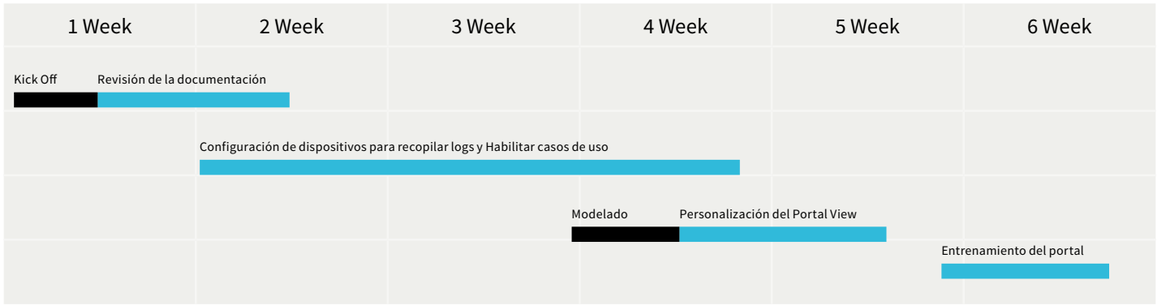
Threat Hunting comienza recopilando los logs hacia la plataforma, clasificándolos y aplicando una biblioteca de contenido de amenazas certificada por el proveedor. Threat Monitoring hace uso de la plataforma para aumentar la investigación de amenazas humanas a través de una extensa biblioteca de casos de usos.

> Utilizamos una combinación de herramientas propias y tecnologías de seguridad líderes en la industria para detectar amenazas y contener ataques antes de que puedan causar daños.

Nuvol www.cybernuvol.com

ProSOC en 30 días

El proceso de incorporación está diseñado para tomar aproximadamente 30 días



1 Week

REVISIÓN DE LA DOCUMENTACIÓN

El proceso comienza con la comprensión y documentación de la red y las políticas de un cliente y continúa hasta la capacitación y la ejecución del servicio.

2 Week

CONFIGURACIÓN Y RECOPILACIÓN DE LOGS

Una vez recibido el evento, ProSOC Collector analiza, agrega y normaliza los eventos y luego los transmite a nuestro SIEM a través de una conexión segura.

3 Week

HABILITAR CASOS DE USO

Bibiloteca de casos de uso: aprovecha cientos de casos de uso que abarcan casos de seguridad, cumplimiento, industria y tecnología, y también proporciona una gran cantidad de reglas de correlación y casos de uso listos para usar que incluyen reglas, filtros, tendencias, paneles e informes.

4 Week

MODELADO DE ACTIVOS

El Runbook documentado se asigna al Plan de respuesta a incidentes y está automatizado para proporcionar alertas de escalamiento a los equipos operativos con las acciones requeridas para la respuesta.

5 Week

PERSONALIZACIÓN DEL PORTAL VIEW

Los informes del SIEM se pueden enviar a petición del cliente. Estos informes pueden ser generados en un horario estándar o ad-hoc por el cliente en el Portal ProView.

6 Week

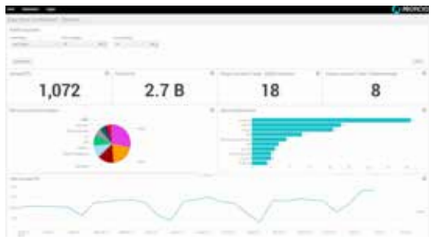
ENTRENAMIENTO DEL PORTAL

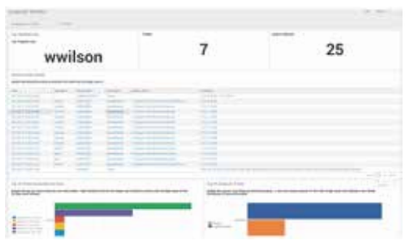
Los clientes pueden revisar tableros, informes, casos y buscar eventos en el Portal ProView, utilizando tecnología Splunk para un manejo más eficiente de los datos.

MONITOREO Y PREVENCIÓN
Y RESPUESTA ANTE INCIDENTES

RESPUESTA Y REMEDIACIÓN
PERSONAS, PROCESOS Y TECNOLOGÍA

Somos el único MSSP en la región con certificación SOC 2 que garantizan los principios de confianza de seguridad, disponibilidad y confidencialidad, lo cual, muestra que nuestros controles cumplen plenamente con las normas.





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

Nuvol Example 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

SOLICITE UNA DEMOSTRACIÓN

cfarfan@cybernuvol.com

www.cybernuvol.com

NUVOL

The right people, for the best service

México | *Panamá* | *Colombia*