PROFICIO™

Centro de Operaciones SOC as a Service

Proficio es un servicio del tipo "Managed Detection and Response (MDF) de clase mundial, ofrece monitoreo de seguridad y detección de amenazas 24/7 con servicio de respuesta a incidentes automatizados.

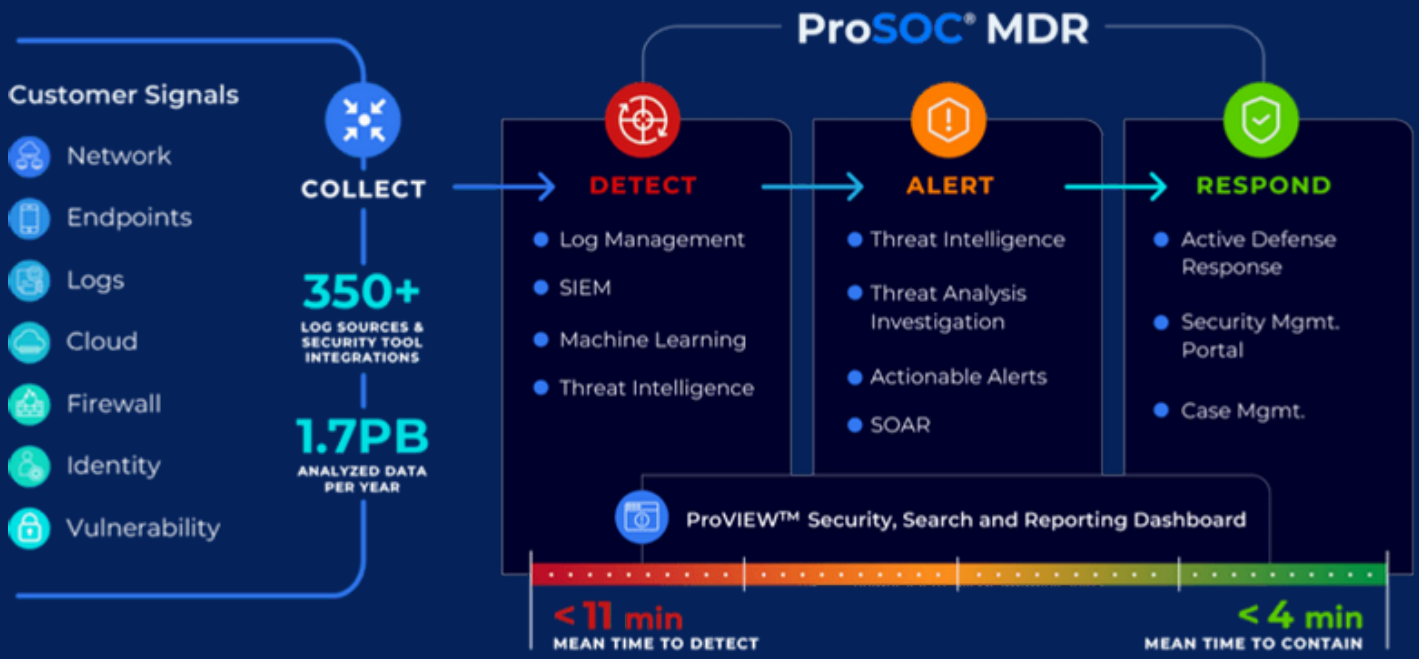
- Expertos 24 × 7 de seguimiento y análisis continúo.
- 3 SOC´s a nivel mundial: Singapur, San Diego y Barcelona, "follow the sun"
- Threat Intelligence
- Threat Hunting e investigación de amenazas
- Defensa activa (SOAR).
- Protección avanzada contra amenazas, internas y perimetrales.
- Experto de seguridad, reunión mensual de seguimiento
- Certificación SOC Tipo II e ISO 27001:2013

Servicios Detección y respuesta gestionadas:

1. **ProSOC MDR:** SOC como servicio 24/7 con tecnología SIEM alojada en Proficio
2. **ProSOC MDR para Microsoft**: Gestión de plataformas y SOC como servicio 24/7 con tecnología de Microsoft Sentinel
3. **ProSOC MDR para endpoint:** Protección contra amenazas en todos sus endpoints
4. **ProSOC MDR para Splunk:** Gestión de plataformas y SOC como servicio 24/7 con tecnología de Splunk
5. **ProSOC XDR:** Potente monitorización 24/7 SOC-as-a-Service impulsado por la plataforma SIEM

Servicio Monitoreo y Detección de Amenazas

El servicio administrado de Nuvol/Proficio proporciona un servicio SOC, llamado ProSOC, completamente gestionado utilizando el conjunto de herramientas más avanzado de la industria, administrado por un equipo de expertos en SIEM y SOC



Especificaciones técnicas del servicio

Servicio PROSOC			
THREAT MANAGEMENT / GESTIÓN DE AMENAZAS			
Threat Monitoring	*	Investigación de analistas de amenazas	*
Caza de amenazas basada en machine Learning	*	Biblioteca de contenido de amenazas	*
Threat Hunting	*	**Notificación de amenazas**	*
THREAT DEFENSE / DEFENSA DE LA AMENAZA			
Threat Intelligence Profiler	*	**Active Defense**	*
Tipos de inteligencia de amenazas	*	Seguridad perimetral	*
Alcance de la amenaza	*	Endpoint Security	*
Fuentes de amenazas principales	*	Matriz de tecnología compatible	*
Puntuación de reputación de amenazas	*		
GESTIÓN DE REGISTROS			
Hot Log Storage (1 año)	*		*
Instancia Dedicada Elastic	*		
SERVICIOS PRINCIPALES			
Portal de clientes		**Gestión del éxito del cliente**	*
ProView	*	**Expert on Call**	*
ITSM	*		
Investigador de Amenazas	*		

En esencia, PROSOC MDR de Proficio es un SOC como servicio gestionado por expertos, con tecnología incluida, que proporciona detección proactiva y respuesta rápida a incidentes de seguridad.

¿Qué se requiere?, requisitos técnicos

Nuvol/Proficio sigue un enfoque minucioso y metódico para implementar servicios para nuevos clientes. 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.

PASOS	DESCRIPCIÓN
Event Collection	El cliente configura dispositivos dentro del entorno para transmitir datos a un colector ProSOC y configurarlos para que el recopilador ProSOC recupere datos. Los tipos de recopilación más comunes son la transmisión de syslog, el sondeo de WMI para orígenes de datos de Windows y las conexiones de bases de datos a tipos especiales de productos, como los servidores de antivirus. Las características de dicho colector son: 6 GB RAM, 4 VCPUs, 40 GB HD, Una interfase de red, HyperV o VMWare
Collector Event Processing	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.
SIEM Event Processing	El ProSOC/ SIEM recibe los eventos y realiza la gestión de correlación e incidentes a través del SIEM. Es en este momento cuando los eventos están disponibles para revisión y escalamiento.
Analyst Review	Los analistas de Proficio en línea 24x7 realizan varios análisis de datos de alto nivel con paneles, visores de consultas y canales activos para evaluar las tendencias que se deben escalar a los clientes de ProSOC como posibles incidentes de seguridad.
Automated Notifications	Pueden ocurrir varios tipos de incidentes que no requieren revisión adicional por parte de Proficio y necesita ser escalado inmediatamente al cliente. Las notificaciones automáticas se envían al cliente y el caso correspondiente con los eventos que desencadenaron el caso se guardan en el Portal de ProView.
ProSOC Reports	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
Analyst Action Notifications	Muchas alertas no se pueden enviar directamente al cliente y requieren una revisión de analistas para evaluar si se ha producido un incidente de seguridad. Para los eventos considerados por el analista como una seguridad potencial, estos casos se derivan al cliente como una notificación.
ProView Portal Access	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.
ProView Reports	Los clientes recibirán un resumen de los servicios, como un resumen mensual de notificaciones, un informe TIP diario u otros tipos de informes personalizados que detallan un resumen de los servicios.

Proceso de toma del servicio en 6 semanas

Implementación PROSOC	semanas					
	1	2	3	4	5	6
Reunión Inicial - Kick off Revisión de la documentación Recopilación de datos Diagrama de Red Bienes Contacto Escalada Políticas de seguridad						
Implementación VM Collector y acceso a la red Cuenta de servicio de dominio						
Configuración de registros y casos de usos Configurar el dispositivo para la recopilación de registros Habilitar casos de uso y reglas de correlación para fuentes de registro						
Modelado de activos Configurar dispositivos avanzados para la recopilación de registros						
Personalización Personalización del tablero Usar la personalización de casos Personalización de informes						

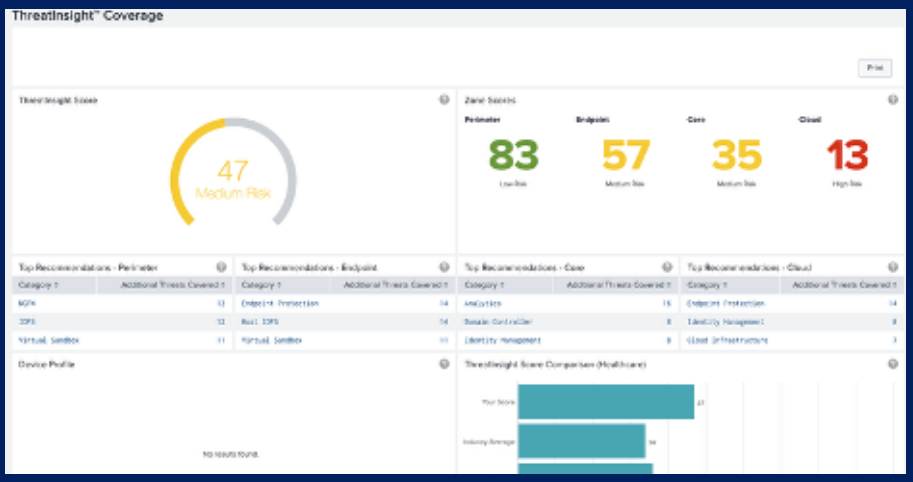
Dashboard e informes

El portal ProView de Nuvol/Proficio se desarrolló para brindar a los equipos de seguridad una visión más profunda de la postura de seguridad de su organización.

El dashboard ejecutivo presenta resúmenes de alto nivel que le permiten ver los detalles, las tendencias y podrá tener una visión completa de su entorno de seguridad. A continuación, se muestran unos ejemplos del portal ejecutivo

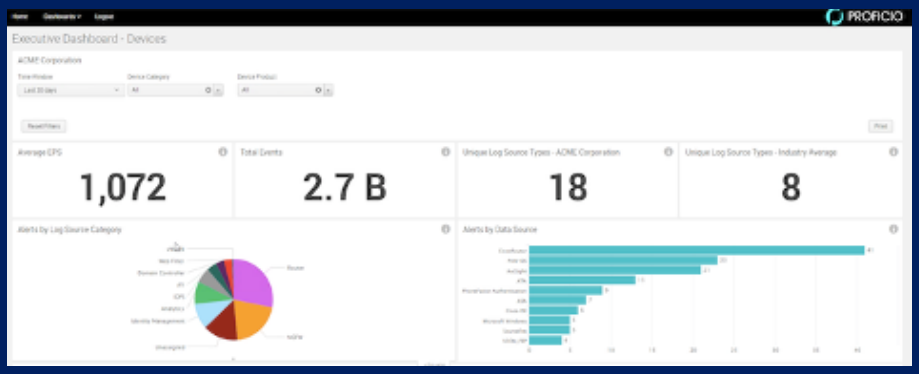
Portal ProView Portal

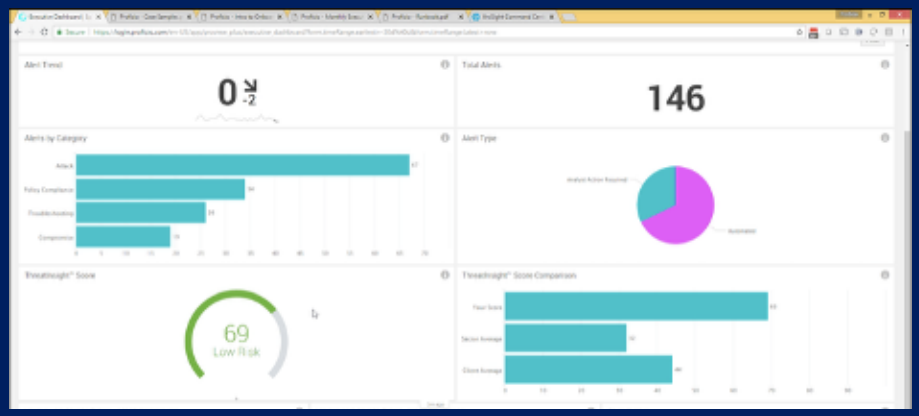
El portal ejecutivo provee un análisis detallado del estado de salud para las diferentes zonas (core, perímetro, end users y cloud), como la tendencia de alertas, casos de uso para análisis de causa- raíz y una calificación del riesgo comparándolo con otros clientes de Proficio o bien, con el promedio de la industria.



Alertas de alta calidad

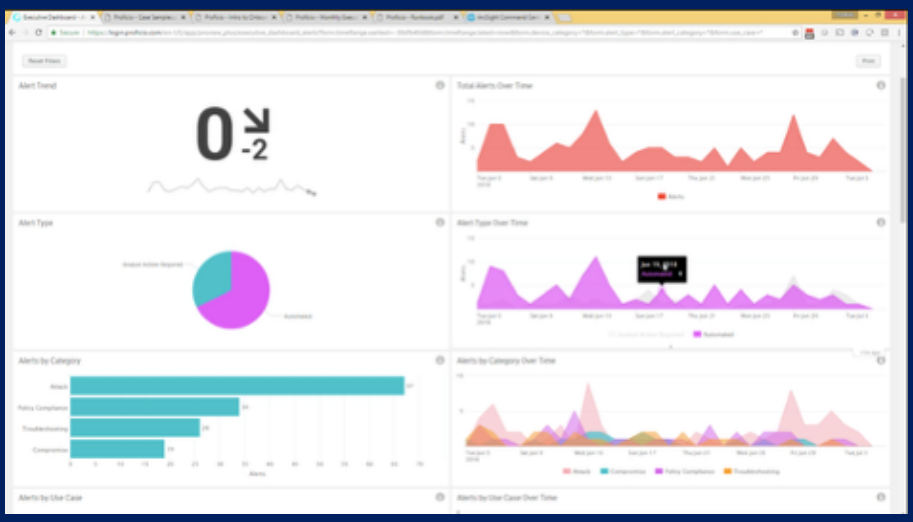
El objetivo de Nuvol/Proficio es proporcionar a los clientes alertas accionables a los pocos minutos de un evento desencadenante. Como se muestra en el ejemplo anterior, las alertas útiles incluyen información suficiente para ayudar al destinatario a comprender el contexto de la alerta y las recomendaciones que permiten una acción inmediata.





Informes predefinidos, parametrizables o a solicitud

Nuvol/Proficio monitorea activamente cada elemento de SIEM en busca de salud y rendimiento, monitorea cada fuente de registro crítica y alerta si una fuente de registro deja de enviar registros durante un período de tiempo específico. Nuvol/Proficio proveerán al cliente un Dashboard con los KPIs y métricas del servicio.



¿Quién es Proficio?

Proficio fue fundado en el año 2010, es un galardonado proveedor de servicios de seguridad administrados (MSSP), que brinda servicios de monitoreo de seguridad y detección y respuesta administrada (MDR) las 24 horas del día, los 7 días de la semana a través de su red global de Centros de operaciones de seguridad modernos, los cuales se encuentran en San Diego, Barcelona y Singapur, monitoreando eventos de seguridad y buscando ataques dirigidos.

@proficio.com

Beneficios

- Presencia global con 3 SOC´s ubicados en Singapur, Barcelona y San Diego en un esquema "Follow the sun", monitoreo 24x7
- Contamos con más de 50 personas certificadas en tecnología SIEM
- Contamos con más de 100 ingenieros certificados en otras tecnologías, desde firewalls, CEH, CISM, CISSP, etc.
- MMSP con certificación SOC 2, así como en el framework NIST e ISO 27001:2013
- Servicio integrado de Threat Intelligence profiles y threat hunting, tanto para los servicios web, dark web y redes sociales.
- Ofrecemos un SLA de notificación y tiempo de respuesta sumamente agresivo: 30 minutos para los incidentes de prioridad 1.
- Nuestro portal web permite al usuario profundizar y pivotar sobre un activo, incidente o usuario para comprender mejor la naturaleza.
- Implementación en 30 días, sin agentes, logs ilimitados.

Cumplimiento y Certificaciones