



ProSOC

Servicios gestionados de detección y respuesta / SOC as a Service

www.abast.es



ABAST y Proficio se han aliado para incluir los servicios Gestionados de Detección y Respuesta (MDR) de Proficio dentro de la oferta global de servicios y soluciones de Ciberseguridad ABAST CYBALL. ProSOC, la solución de SOC as a Service de Proficio, permite disfrutar de los servicios de un Centro de Operaciones de Seguridad de primer nivel de forma mucho más rentable y libre de preocupaciones que la opción de poner en marcha y mantener un SOC propio. ProSOC registra, supervisa y analiza los eventos de seguridad de su organización y proporciona notificaciones de amenazas y acciones preventivas ante posibles brechas. Gracias a un equipo de expertos en seguridad que operan 24x7 y que utilizan SIEM y las tecnologías de defensa activa líderes de la industria, ProSOC le permite abordar sus necesidades críticas de seguridad y cumplimiento, prevenir pérdidas o robo de datos y reducir sus costes operativos.

SOC as a Service / Monitorización, Detección y Respuesta 24x7

Proficio cuenta con una infraestructura multi-SOC global con centros en Barcelona, San Diego y Singapur que se turnan para ofrecer un servicio ininterrumpido "follow the sun". Esto permite ofrecer una cobertura 24x7 para la monitorización de eventos de seguridad y dar respuesta a cualquier amenaza detectada en cualquier lugar del mundo y cualquier franja horaria.

ProSOC utiliza las últimas técnicas de defensa contra amenazas para identificar las primeras etapas de estos ataques antes de que las infracciones den como resultado la pérdida de datos. Para ello utilizan tecnologías líderes y metodologías avanzadas como técnicas de correlación de eventos multivector, modelado de activos, perfilado de usuarios e inteligencia de amenazas.

Los expertos de ProSOC se encargarán también de las tareas de configuración y parcheo de sus equipos de firewalls, NGWs, IDS/IPS y WAFs, evitando que tenga que contratar personal muy especializado para tareas rutinarias de administración y gestión de su infraestructura de seguridad.

SIEM as a Service

Con ProSOC, su organización se beneficiará también de la tecnología SIEM más avanzada para registrar y correlacionar eventos de seguridad, sin los costes ni la complejidad que supone comprar y administrar un sistema SIEM propio. Los expertos detrás de ProSOC son especialistas en la configuración de sistemas SIEM y en la personalización de reglas y casos de uso para identificar alertas de seguridad críticas relevantes para su organización.



Threat Intelligence

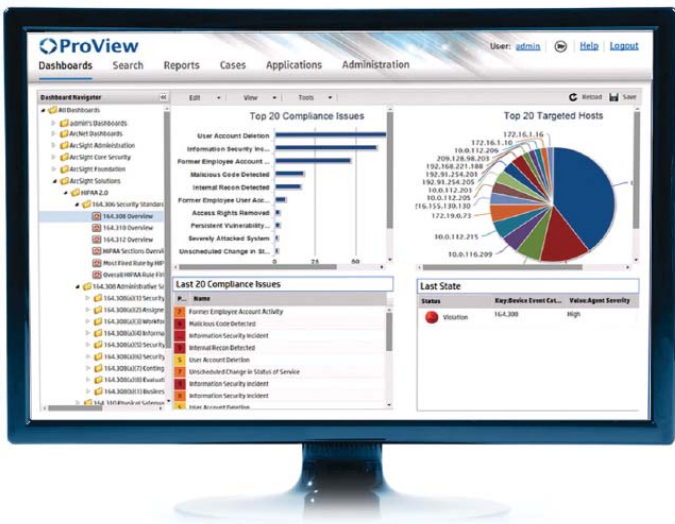
Proficio cuenta con una base de datos de información sobre amenazas de seguridad que se alimenta de una treintena de fuentes externas además de las de sus propios SOC. Esta información, combinada con el SIEM, permite ser más preciso en la detección de amenazas y minimizar los falsos positivos

Active Defense

Un valor diferencial claro de ProSOC es la posibilidad de ofrecer una respuesta automatizada a ciertas amenazas utilizando las funcionalidades de los firewalls de nueva generación (NGFW). En caso de detección de un ataque de alto riesgo se activan reglas de firewall para bloquear el tráfico sospechoso, dando tiempo a que el equipo de seguridad investigue y tome las medidas necesarias para hacer frente al incidente antes de que se produzca ningún daño. Este servicio permite dar en menos de 5 minutos una respuesta preventiva automática a un ataque potencialmente peligroso sin la necesidad de implicar recursos humanos.

ProView

Los clientes de ProSOC pueden acceder a un portal web en el que podrán encontrar toda la información sobre el tipo de amenazas a las que su organización se está enfrentando y qué está haciendo el equipo de servicios de seguridad para atajarlas. Este portal incluye cuadros de mando operacionales, informes sobre gestión de seguridad y cumplimiento, acceso total a los logs de eventos de seguridad, gestión de casos y herramientas de análisis avanzado, todo ellos con vistas basadas en roles de usuario.



Beneficios clave

- Servicios gestionados flexibles: SOC as a Service, SIEM as a Service y otras opciones híbridas.
- Monitorización 24x7 de todo tipo de eventos de seguridad por un equipo de expertos.
- Identificación precoz de los ataques y comportamientos sospechosos internos en sus primeras etapas, antes de que se produzcan pérdidas de datos.
- Inteligencia accionable que permite a los equipos de IT internos resolver eficazmente los problemas.
- Facilita el cumplimiento de los requisitos de normativas como: PCI, HIPAA, SOX, GLBA, FFIEC, NERC CIP, FISMA ...
- Visibilidad clara y completa de los eventos de seguridad gracias a un portal web de uso sencillo que incluye cuadros de mando y potentes opciones de análisis y reporting
- Despliegue escalable en la nube sin necesidad de invertir en compra de hardware o software.
- Soporta de inicio más de 350 fuentes de registro.
- Libera a los equipos de TI de las tareas de configuración, ajuste y parchado de firewalls, NGWs, IDS/IPS y WAFs.

CYBALL. Servicios de seguridad global de Abast

ABAST ofrece una amplia oferta de servicios y soluciones para dar respuesta a sus necesidades en ciberseguridad y seguridad del negocio. Las estructuramos en 4 capas:

GOBIERNO: Alineación estratégica seguridad/negocio. Tratamiento del riesgo. Análisis coste/beneficio. Medición madurez de la seguridad.

GESTIÓN: Auditorías de Seguridad. Continuidad de negocio. Cumplimiento normativo/legal. Gestión de crisis y de incidencias. Formación y concienciación.

OPERACIONES (SOC/MDR): Monitorización de la Seguridad 24x7. Detección de Amenazas e incidentes. Prevención de brechas. Respuesta a los incidentes.

INFRAESTRUCTURA: Asesoramiento e implantación de infraestructura/soluciones de seguridad TI. Administración de la seguridad TI.



Para más información:
seguridad@abast.es