



ProSOC

Serveis gestionats de detecció i resposta / SOC as a Service

www.abast.es



ABAST i Proficio s'han aliat per incloure els serveis gestionats de Detecció i Resposta (MDR) de Proficio dins de l'oferta global de serveis i solucions de Ciberseguretat ABAST CYBALL. ProSOC, la solució de SOC as a Service de Proficio, permet gaudir dels serveis d'un Centre d'Operacions de Seguretat de primer nivell de forma molt més rendible i lliure de preocupacions que l'opció de posar en marxa i mantenir un SOC propi. ProSOC registra, supervisa i analitza els esdeveniments de seguretat de la seva organització i proporciona notificacions d'amenaçes i accions preventives davant de possibles bretxes. Gràcies a un equip d'experts en seguretat que operen 24x7 i que utilitzen SIEM i les tecnologies de defensa activa líders de la indústria, ProSOC li permet abordar les seves necessitats crítiques de seguretat i compliment, prevenir pèrdues o robatori de dades i reduir els seus costos operatius.

SOC as a Service / Monitorització, Detecció i Resposta 24x7

Proficio compta amb una infraestructura multi-SOC global amb centres a Barcelona, Sant Diego i Singapur que fan torns per oferir un servei ininterromput "follow the sun". Això permet oferir una cobertura 24x7 per a la monitorització d'esdeveniments de seguretat i donar resposta a qualsevol amenaça detectada en qualsevol lloc de món i a qualsevol franja horària.

ProSOC utilitza les últimes tècniques de defensa contra amenaces per identificar les primeres etapes d'aquests atacs abans que les infraccions donin com a resultat la pèrdua de dades. Per a això utilitzen tecnologies líders i metodologies avançades com tècniques de correlació d'esdeveniments multivector, modelat d'actius, perfilat d'usuaris i intel·ligència d'amenaçes.

Els experts de ProSOC s'encarregaran també de les tasques de configuració i apedaçat dels seus equips de tallafocs, NGWs, IDS / IPS i WAFs, evitant que hagi de contractar personal molt especialitzat per a tasques rutinàries d'administració i gestió de la seva infraestructura de seguretat.

SIEM as a Service

Amb ProSOC, la seva organització es beneficiarà també de la tecnologia SIEM més avançada per registrar i correlacionar esdeveniments de seguretat, sense els costos ni la complexitat que suposa comprar i administrar un sistema SIEM propi. Els experts darrere de ProSOC són especialistes en la configuració de sistemes SIEM i en la personalització de regles i casos d'ús per a identificar alertes de seguretat crítiques rellevants per a la seva organització.



Threat Intelligence

Proficio compta amb una base de dades d'informació sobre amenaces de seguretat que s'alimenta d'una trentena de fonts externes a més dels seus propis SOC. Aquesta informació, combinada amb el SIEM, permet ser més precís en la detecció d'amenaces i minimitzar els falsos positius.

Active Defense

Un valor diferencial clar de ProSOC és la possibilitat d'oferir una resposta automatitzada a certes amenaces utilitzant les funcionalitats dels tallafocs de nova generació (NGFW). En cas de detecció d'un atac d'alt risc s'activen regles de tallafocs per bloquejar el trànsit sospitós, donant temps a que l'equip de seguretat investigui i prengui les mesures necessàries per fer front a l'incident abans que es produeixi cap dany. Aquest servei permet donar en menys de 5 minuts una resposta preventiva automàtica a un atac potencialment perillós sense la necessitat d'implicar recursos humans.

ProView

Els clients de ProSOC poden accedir a un portal web en el qual podran trobar tota la informació sobre el tipus d'amenaces a les que la seva organització s'està enfrontant i què està fent l'equip de serveis de seguretat per atallar-les. Aquest portal inclou quadres de comandament operacionals, informes sobre gestió de seguretat i compliment, accés total al registre d'esdeveniments de seguretat, gestió de casos i eines d'anàlisi avançat, tots ells amb vistes basades en rols d'usuari.



Beneficis clau

- Serveis gestionats flexibles: SOC as a Service, SIEM es a Service i altres opcions híbrides.
- Monitorització 24 x 7 de tot tipus d'esdeveniments de seguretat per un equip d'experts.
- Identificació precoç dels atacs i comportaments sospitosos interns en les seves primeres etapes, abans de que es produeixin pèrdues de dades.
- Intel·ligència accionable que permet als equips d'IT interns resoldre eficaçment els problemes.
- Facilita el compliment dels requisits de normatives com: PCI, HIPAA, SOX, GLBA, FFIEC, NERC CIP, FISMA ...
- Visibilitat clara i completa dels esdeveniments de seguretat gràcies a un portal web d'ús senzill que inclou quadres de comandament i potents opcions d'anàlisi i reporting
- Desplegament escalable en el núvol sense necessitat d'invertir en compra de hardware o software.
- Suporta d'inici més de 350 fonts de registre.
- Allibera els equips de TI de les tasques de configuració, ajust i apedaçat de firewalls, NGWs, IDS / IPS i WAFs.

CYBALL. Serveis de seguretat global d'Abast

ABAST ofereix una àmplia oferta de serveis i solucions per donar resposta a les seves necessitats en ciberseguretat i seguretat del negoci. Les estructurarem en 4 capes:

- **GOVERN:** Alineació estratègica seguretat / negoci. Tractament del risc. Anàlisi cost / benefici. Mesura de la maduresa de la seguretat.
- **GESTIÓ:** Auditories de Seguretat. Continuitat de negoci. Compliment normatiu / legal. Gestió de crisi i d'incidències. Formació i conscienciació.
- **OPERACIONS (SOC / MDR):** Monitorització de la Seguretat 24x7. Detecció d'Amenaces i incidents. Prevenció de bretxes. Resposta als incidents.
- **INFRAESTRUCTURA:** Assessorament i implantació d'infraestructura / solucions de seguretat TI. Administració de la seguretat TI.



Per a més informació:
seguridad@abast.es