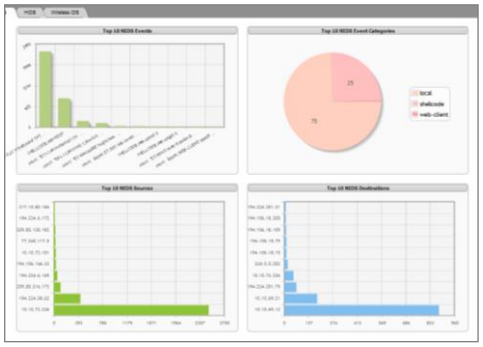
SERVICIOS SOC

servicios gestionados de seguridad

Las compañías y entidades están expuestas a un gran abanico de amenazas provenientes tanto del exterior (en especial Internet) como del interior de las organizaciones. Los dispositivos de protección habituales (Firewalls, IDS/IDP, Antivirus, etc) por sí solos no son un mecanismo suficiente para la protección.

Los elementos que conforman las redes y sistemas de las organizaciones (firewalls, proxys, IPS, switches, routers, servidores, etc) generan gran cantidad de información sobre su actividad, principalmente a través de **logs**. Esta información, correctamente analizada e interpretada puede proporcionar un gran valor sobre el estado de seguridad de la organización, permitiendo detectar además incidentes de manera temprana y actuar en tiempo real para minimizar su impacto.

6	Otros Servicios (Hardening, Auditoría Optimización, MDM, etc)
5	IDS as a Service (IDSaaS)
4	SSGG Análisis de Vulnerabilidades Remoto
3	SIEM : Gestión Eventos e Incidentes de Seguridad
2	SSGG Operación y Administración Remota
1	SSGG Monitorización Remota



Servicio SOC Global

SSGG Monitorización Remota 7x24

Detección y Gestión de **incidencias** y problemas de disponibilidad sobre los activos gestionados.

SSGG Operación y Administración Remota

Gestión de **Cambios** realizado por especialistas sobre los activos de seguridad, redes o sistemas gestionados.

SIEM (Gestión Eventos e Incidentes de Seguridad)

Consolidación y correlación de los **logs** de seguridad de los diferentes activos (firewalls, servidores, IDS/IPS, proxys, elementos de red,…) para la detección temprana de eventos e **incidentes de seguridad** y propuesta de **contramedida** en caso de ataque.

SSGG Análisis de Vulnerabilidades

Escaneos remotos para detectar **vulnerabilidades** de los sistemas (vulnerabilidad: debilidad conocida de un activo).

IDSaaS

Servicio Gestionado donde se despliega y administra uno o varios **IDS** como servicio (OPEX), con el objetivo de complementar las medidas protectoras del cliente, enriquecer la información de seguridad del servicio **SIEM** y aumentar el nivel de detección de ataques.

Cuadro de mando

El servicio incluye un Cuadro de Mando para el seguimiento en tiempo real de las métricas y KPIs de seguridad, disponibilidad, rendimiento y seguimiento de SLAs e incidentes activos.

Otros Servicios de Seguridad

Servicio Auditoría Optimización Reglas de Firewall

Optimizar las reglas de las plataformas de seguridad con el objetivo de aumentar su rendimiento y mejorar la protección.

Hardening de Sistemas

Asegurar un sistema mediante la reducción de vulnerabilidades y la eliminación de configuraciones y opciones innecesarias con el objetivo de reforzar al máximo la seguridad del equipo.

Hacking Ético y Auditoría de Seguridad

Auditorías de Seguridad externas o internas con el objetivo de analizar el nivel de seguridad de la compañías.

SSGG Cloud MDM (Mobile Device Management)

Gestionar los dispositivos móviles asegurando el cumplimiento de las políticas de seguridad corporativas desde una plataforma Cloud.

**Nota: Todos estos servicios son módulos contratables de manera conjunta o independiente según el servicio requerido.*

Beneficios para el Cliente

Previene incurrir en costes adicionales o perjuicios

Debidos a ataques malintencionados de seguridad (costes adicionales por **pérdida de imagen**, costes por **lucro cesante** por indisponibilidad de los servicios, exposición a **robo de datos confidenciales**, etc). El servicio detecta de manera temprana el incidente y proporciona una medida correctora.

Mejorar gestión de la seguridad sin inversión

Formato 100% servicio (OPEX), permite desplegar nuevas funcionalidades de seguridad sin inversión (IDSaaS, Gestión de Vulnerabilidades), prestando el servicio en remoto por personal especialista en seguridad y focalizando los recursos de seguridad de la compañía al negocio.

Cumplimiento Normativo

Facilita cumplir con las especificaciones de gestión y almacenamiento de logs incluidos en las principales leyes y normativas de seguridad nacionales y sectoriales (ISO27000, LSSI, LOPD, etc).

¿Porqué Unitronics?

Experiencia y Know-How

Unitronics lleva 50 años ofreciendo servicios de soporte especializados en IT, y **más de 10 años ofreciendo Servicios Gestionados** (NOC, SOC y VNOC) desde sus **2 CSG** (Centros de Servicios Gestionados).

Multitecnología

La capacidad multitecnología de Unitronics abarca ámbitos de especialización como redes de comunicaciones, seguridad, comunicaciones unificadas, sistemas y telepresencia le permite solventar incidentes complejos o globales que requieran de especialistas en otros entornos no sólo seguridad.

Calidad

Unitronics dispone de las certificaciones ISO20000, ISO27000 y Cisco Master Security (Únicos en España), además de adoptar procedimientos ITIL y PM-BOK en sus operaciones.