Quanti Solutions
SOC as a Service

¿Que es Quanti SOC as a Service?

Es un servicio que recolecta, detecta, analiza y responde ante amenazas sospechosas que evaden las soluciones de seguridad tradicionales usando plataformas avanzadas con inteligencia artificial, procesos basados en ITIL y personal altamente capacitado.

Cero adquisición de hardware/software
100% OpEx

Reducción de costos operativos ya que Quanti opera y mantiene todo

Gestor para la remediación de riesgos
Seguimiento oportuno y simplificado

Rápido y efectivo despliegue de la plataforma sin interrupción en la red

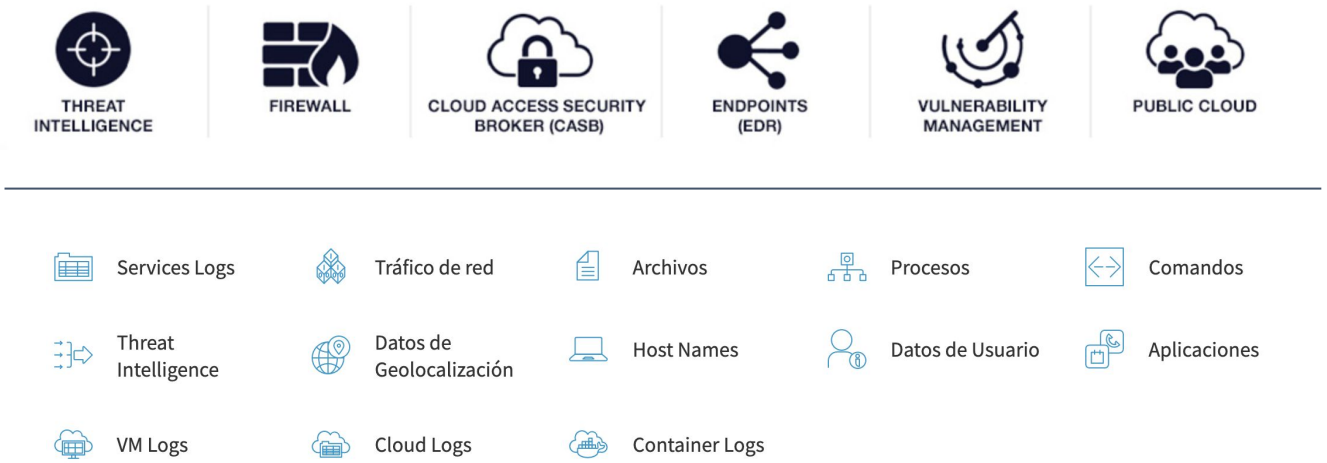
Monitoreo continuo 24x7, alertas automáticas y detección de amenazas en tiempo real

Expertos a tu disposición con alto nivel de especialización con calidad de servicio

Simplifica tu operación de seguridad

Simplificamos *la* *Tecnología para* **TI**

Quanti utiliza Stellar Cyber, una plataforma que protege de manera integral aplicaciones y usuarios, manteniendo el control de toda la infraestructura y respondiendo a las amenazas que se encuentran en constante evolución. Stellar Cyber es la primera plataforma abierta XDR, que significa Detección y Respuesta desde cualquier lugar.

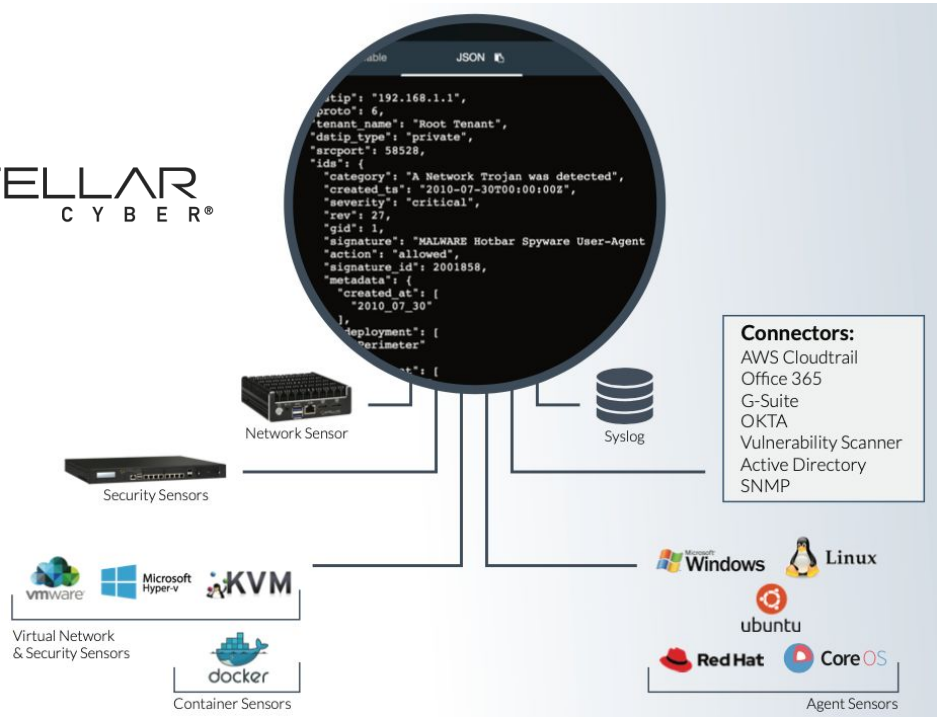


¿Qué componentes incluye?

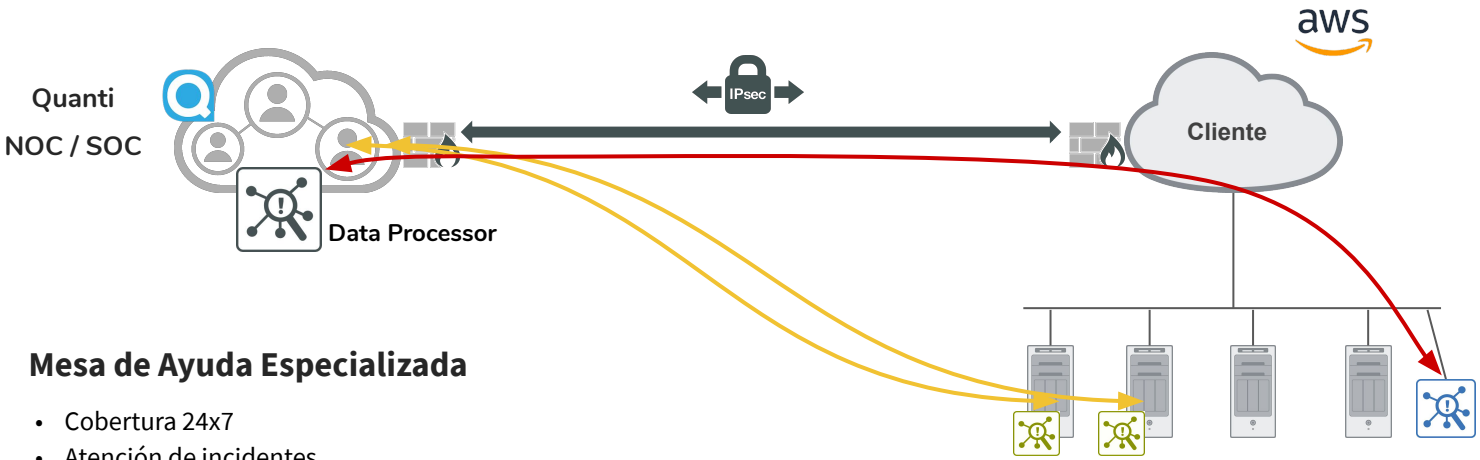
Plataforma Unificada de Seguridad

- Anti-Phishing
- Asset Manager
- SIEM
- IDS con Machine Learning
- Sandbox (File extraction & Malware detection)
- UBA (User Behavior Analytics)
- Network Analyzer
- Breach detection
- Threat Intelligence

STELLAR CYBER®



SOC as a Service ¿Cómo funciona?



Mesa de Ayuda Especializada

- Cobertura 24x7
- Atención de incidentes
- Atención de Requerimientos
- Análisis de Impactos
- Control de Cambios
- Respaldo de Configuraciones
- Reportes
- Procesos basados en ITIL

Service Powered by

STELLAR CYBER

Agentes

Server Operating System:
Windows 98 en adelante
Ubuntu, CentOS, RedHat, Debian, etc.

Sensor Físico 1/10Gbps

Port Mirror en Switch Core

Stellar Cyber *puede detectar amenazas en* ***5 minutos****, cuando al humano en promedio le toma* ***200 días***

Para resolver el problema de la falta de gente capacitada, Stellar Cyber puede responder de manera automática a amenazas, de manera que la poca gente de seguridad que tienes, se enfoque en los incidentes de seguridad más graves

Recolecta sólo la información importante

Detecta las amenazas

Investiga el problema

Automatiza la respuesta

Características SOC as a Service

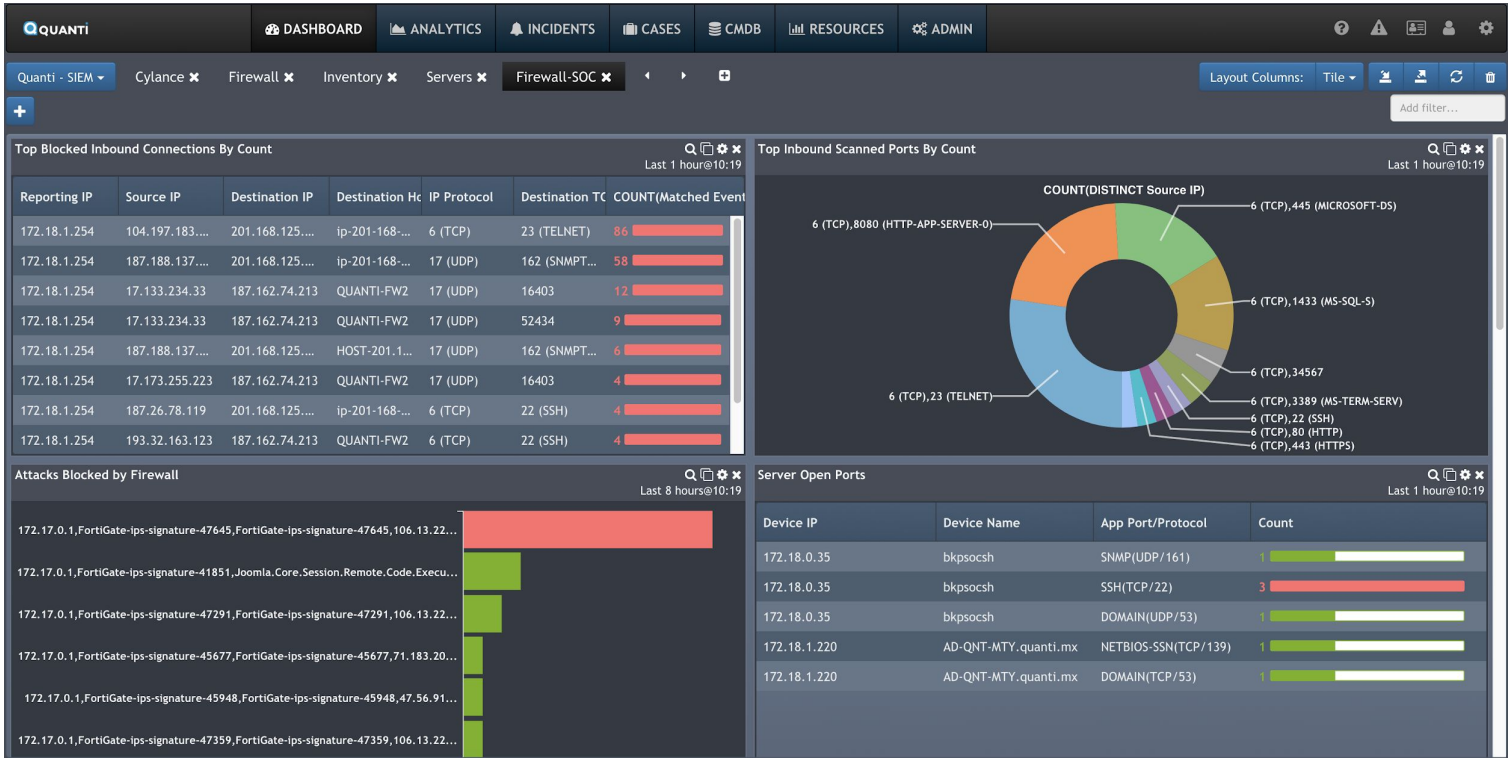
La plataforma permite una mejor operación y disponibilidad de servicio dentro del Centro de Operaciones de Quanti. Es por ello que como soluciones damos los siguientes puntos que ayudaran como servicio administrado a mejorar sus procesos actuales con su infraestructura actual y daran solucion a la misma.

- Gestión de Logs: Compatibilidad con múltiples marcas y dispositivos
- Reportes automatizados: Generación de reportes a la medida y predefinidos
- Consultas históricas y en tiempo real: Realiza consultas en el momento deseado
- Analiticos: Correlación de eventos a través del análisis NOC & SOC
- Cumplimiento: Informes predefinidos para auditoría de cumplimiento y necesidades de gestión que incluyen:

  PCI-DSS, HIPAA, SOX, NERC, FISMA, ISO, GLBA, GPG13, Controles críticos de SANS
- CMDB: Autoaprendizaje de dispositivos para inventario
- Dashboards a la medida y necesidades del cliente.

Dashboard Unificado de la Plataforma

Simplificamos *la*
Tecnología para **TI**



Sensores y Agentes

La plataforma cuenta con diversos mecanismos para recolectar la información, ya sea sin la necesidad de instalar nada en los servidores o a través de un agente que nos permite tener más detalle de los que está a pasando en los sistemas.

Algunas de las características son:

- Windows Security Logs
- Windows Application Logs
- Windows System Logs
- Windows DNS Logs
- Windows DHCP Logs
- IIS logs
- DFS logs
- File Integrity Monitoring
- Installed Software Change Monitoring
- Registry Change Monitoring
- Custom file monitoring
- WMI output Monitoring
- Power shell Output Monitoring
- Removable media (CD/DVD/USB) Monitoring

Sistemas Operativos Soportados // Windows

- Windows 7 Enterprise/Professional
- Windows 8
- Windows 10
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016

CPU: x86 or x64 (or compatible) at 2 GHz or higher
Hard Disk Free space: 10 GB (minimum)
Server Operating System
- Windows Server 2008 R2 and above (strongly recommended)
- Desktop Operating System: Windows 7, 8,10 and above

RAM
- For 32 bit OS: 2 GB for Windows 7, 8, 10 minimum
- For 64 bit OS: 4 GB for Windows 7, 8, 10, Windows Server 2008 / 2012 minimum

Acuerdos de Nivel Servicio (SLA)

CLASIFICACION DE INCIDENTES:

Crítico: Afectación mayor a equipos activos considerados de alto impacto en tus procesos de negocio (equipos Core). Se incluyen en esta categoría incidentes que afecten directamente tus procesos de negocio de 2 o más áreas, no exista una solución alternativa en el inmediato plazo y tu operación se vea afectada.

Alto: Afectación a equipos activos considerados de alto impacto en tus procesos de negocio (equipos Core). Se incluyen en esta categoría incidentes que afecten directamente tus procesos de negocio de algún área en concreto y no exista una solución alternativa en el inmediato plazo.

Medio: Afectación a equipos activos involucrados en algún proceso de negocio. Se incluyen en esta categoría incidentes que afectan parcialmente tus procesos de negocio de por lo menos algún área y para la cual exista alguna solución alternativa ("workaround").

Bajo: Afectación parcial o intermitente a equipos activos involucrados en algún proceso de negocio. Se incluyen en esta categoría incidentes que afectan a algunos usuarios o tienen intermitencia y para los cuales exista alguna solución alternativa ("workaround"). Adicionalmente esta categoría abarca todos los requerimientos (solicitudes de configuración: altas, bajas y cambios).

	Tiempos			
Tipo de Incidente	*Atención*	*Tier 1*	*Tier 2*	*Fabricante*
Crítico	15 min	4 hr	4 hr	-
Alto	20 min	6 hr	6 hr	-
Medio	40 min	12 hr	24 hr	-
Bajo	50 min	36 hr	24 hr	-

Estás en buenas manos

Simplificamos *la*
Tecnología para **TI**

MONTERREY (CORP)
Edificio Business Hub Piso 15
Blvd. Constitución 2100, Col. Santa María
Monterrey, NL, CP 64650

Tel. 811969-3800 y 800-6001380
www.quanti.mx

SIGUENOS EN LAS REDES SOCIALES