



# Soluciones de ciberseguridad De la manera sencilla

*Nuestro Centro de Operaciones de Seguridad gestionado y Detección de Punto Terminal y Tiempo de*

Un ciberataque exitoso puede resultar en un tiempo de inactividad significativo, datos robados, pérdida de ingresos y pérdida de confianza del cliente. Esto plantea un riesgo claramente significativo para las empresas de banda ancha, que no solo tienen que preocuparse por las amenazas a su propia empresa y red, sino también por cómo un ataque podría afectar los servicios IP principales que proporcionan y el impacto potencial que puede tener en sus suscriptores.

Y, si bien un programa sólido de ciberseguridad es fundamental por derecho propio, si va a buscar fondos institucionales para el despliegue de banda ancha, existen requisitos de ciberseguridad que deben cumplirse para calificar para esos fondos.



## Centro de Operaciones de Seguridad como servicio (SOCaaS)

CyberZCurity, nuestro servicio de Centro de Operaciones de Seguridad (SOC), monitorea, previene, detecta e investiga continuamente las amenazas cibernéticas a su red, manejando el trabajo pesado necesario para una prevención y resolución efectiva de amenazas.

### Características:



#### Respuesta a la detección de amenazas

Detección de amenazas completa y actualizada al minuto, que proporciona visibilidad para asegurar eventos, incidentes en tiempo real y orientación para solucionar rápidamente los problemas.



#### Seguridad proactiva y económica

La ciberseguridad como servicio asequible reduce las costosas inversiones de capital necesarias para un equipo dedicado a los servicios de seguridad.



#### Expertos dedicados en ciberseguridad

Un equipo de operarios de seguridad que trabaja individualmente con usted para identificar y satisfacer sus necesidades de seguridad.



#### Administración de parches

Los servicios SOC se pueden combinar con Patch Management para abordar las vulnerabilidades del software y del sistema operativo sin parches con una corrección en un solo paso.

## NOC vs. SOC

Si bien tanto NOC como SOC desempeñan un papel importante en la gestión y el mantenimiento de las operaciones de una organización, difieren en términos de su enfoque, responsabilidades, tecnología y habilidades.



Un NOC se centra en el monitoreo, la administración y el mantenimiento de la red, mientras que un SOC se centra en la seguridad y la detección y respuesta ante amenazas.

Un NOC es responsable de garantizar la estabilidad y el rendimiento de la infraestructura de red de una organización, mientras que un SOC es responsable de detectar, investigar y responder a incidentes y amenazas de seguridad.

Un NOC normalmente utiliza herramientas de supervisión de red y otras herramientas de gestión de TI para supervisar la red, mientras que un SOC utiliza herramientas de seguridad como sistemas de detección de intrusiones, firewall y sistemas de gestión de eventos e información de seguridad (SIEM) para supervisar los incidentes de seguridad.

Un SOC se centra en el monitoreo, la administración y el mantenimiento de la red, mientras que un NOC se centra en la seguridad y la detección y respuesta ante amenazas.

### Características de SOC-como-Servicio:

- Clasificación de alertas
- Acciones correctivas
- Implementaciones y actualizaciones
- Caza de amenazas
- Investigación de amenazas y detecciones
- Mitigación de falsos positivos
- Monitoreo diario en vivo de amenazas
- Asistencia para la solución de problemas
- Acceso 24/7 a un especialista en seguridad
- Monitoreo de eventos 24/7
- Informes semanales y mensuales

### EDR gestionado y seguridad de puntos

Asegurar los puntos de entrada conectados a su red juega un papel capital para garantizar que los datos confidenciales estén protegidos contra ciberataques. A medida que el mundo empresarial actual ha evolucionado con el trabajo remoto y la filosofía de "traiga su propio dispositivo", el aseguramiento de puntos terminales (computadoras portátiles, computadoras de escritorio, tabletas, dispositivos móviles e impresoras) es vital para poder implementar controles de seguridad más avanzados que cubran toda su red.

CyberZCurity puede monitorear y analizar continuamente los puntos finales de su red para detectar cualquier comportamiento sospechoso que se desvíe de los patrones normales de uso y alerta a nuestro equipo si identifica un problema potencial. Administramos y monitoreamos la Detección y Respuesta de Punto Terminal (EDR) y del software de seguridad, proporcionando la visibilidad proactiva del punto terminal necesaria para detectar, contener y recuperarse de amenazas avanzadas en esos puntos.



Contact Us

ZCorum  
4501 North Point Parkway, Suite 125  
Alpharetta, GA 30022  
1-800-909-9441

ZCorum.com  
Facebook.ZCorum.com  
Twitter.com/ZCorum

© 2023