



General Protec CiberCompleet Plus

Protección Integral y Adaptativa frente a Amenazas Avanzadas

CiberCompleet Plus es una solución de seguridad diseñada con una arquitectura de defensa profunda que aborda el ciclo completo de las amenazas, desde la prevención de ataques de día cero hasta la remediación automatizada y la gestión del riesgo. Esta plataforma combina tecnologías de Inteligencia Artificial y heurísticas avanzadas para garantizar la resiliencia operativa de su infraestructura.

El conjunto de tecnologías descritas ofrece una protección integral y adaptativa frente a amenazas avanzadas, abarcando desde la detección proactiva hasta la remediación automatizada. Al integrar capas como Anti-Exploit, ATC, EDR, HyperDetect, Sandbox y EASM, las organizaciones logran una visibilidad total y una reducción efectiva del riesgo de seguridad.

Principales beneficios de CiberCompleet Plus:

1 Neutraliza los Ataques de Día Cero y Exploits
·Descripción: La combinación de Anti-Exploit Avanzado y HyperDetect utiliza IA y heurísticas para detener amenazas antes de que sean conocidas o se ejecuten.
·Ventaja Clave: Elimina la vulnerabilidad asociada a parches faltantes o a la lentitud en la reacción,

2 Garantiza la Continuidad del Negocio frente a Ransomware
·Descripción: La capa de Mitigación de Ransomware (ATS) crea copias de seguridad de datos en tiempo real al detectar actividad sospechosa.
·Ventaja Clave: Permite la recuperación inmediata de archivos cifrados o alterados.

3. Proporciona Visibilidad Total y Control Centralizado del Riesgo
·Descripción: Las funciones de Gestión de Riesgos (ERA) y EASM evalúan continuamente las configuraciones y los activos expuestos (internos y externos).
·Ventaja Clave: Otorga un dominio total sobre la postura de seguridad, permitiendo identificar y corregir configuraciones erróneas y vulnerabilidades críticas.

4. Acelera la Detección y Respuesta a Incidentes (EDR)
·Descripción: El Control de Amenazas Avanzado (ATC) y las herramientas EDR rastrean la cadena de ataque y permiten acciones remotas de cuarentena y bloqueo.
·Ventaja Clave: Facilita una respuesta de seguridad inmediata minimizando el impacto de un ataque exitoso.



Aprendizaje Automático Híbrido: Local y en la Nube

El enfoque híbrido ofrece una defensa multicapa, rápida y eficiente, con mínima carga para el usuario. Combina la inteligencia global en la nube con análisis local basado en IA para detectar amenazas desconocidas y de día cero sin afectar el rendimiento del sistema.



Visibilidad, Detección y Respuesta (EDR)

La visibilidad completa de la cadena del ataque es primordial. Tecnologías como el Control de Amenazas Avanzado (ATC) y la Mitigación de Ransomware (ATS) trabajan en conjunto para rastrear, detener y recuperar datos, ofreciendo opciones de cuarentena, bloqueo y una visión consolidada del estado de seguridad de la red.



Gestión Proactiva de Vulnerabilidades y Cumplimiento

Las vulnerabilidades de software y las configuraciones erróneas son el punto de entrada más común para los ciberatacantes. El sistema escanea continuamente los endpoints para identificar parches faltantes, desviaciones de las políticas de seguridad y riesgos de usuario, como cuentas sin autenticación multifactor. Esta capa transforma la gestión del riesgo en un proceso automatizado, asegurando que la infraestructura siempre cumpla con los estándares de seguridad más rigurosos.

Qué Capas de Defensa Incluye CiberCompleto Plus

Requisitos CiberCompleto Plus:

- Gestión Centralizada: Plataforma ERA para la gestión de riesgos y parches.
- Recuperación: Mecanismos de mitigación local y remota (ATS).
- Superficie de Ataque: Requiere escaneo continuo (EASM) para activos expuestos a Internet.

Qué incluye CiberCompleto Plus (como parte de CiberSteps):

- Gestión y monitorización por parte del Técnico Dedicado.
- Anti-Exploit Avanzado
- Control de Dispositivos
- Control de Amenazas Avanzado (ATC),
- Gestión de Riesgos (ERA)
- HyperDetect,
- Gestión de Parches,
- Sandbox Analyzer
- Mitigación de Ransomware (ATS)
- Gestión de Superficie de Ataque Externa (EASM)
- Protección de Red
- Aprendizaje Automático Híbrido
- Visibilidad, Detección y Respuesta (EDR)
- Gestión Proactiva de Vulnerabilidades

Características	Acción	Cómo protege
Anti-Exploit Avanzado	Utiliza aprendizaje automático para monitorizar procesos del sistema y evitar el secuestro de ejecución.	Bloquea ataques de día cero y exploits que aprovechan vulnerabilidades de memoria en aplicaciones comunes (Office, navegadores).
Control de Dispositivos	Aplica políticas de bloqueo y excepciones controladas de forma centralizada.	Previene la entrada de malware y la fuga de datos a través de dispositivos externos (USB, Bluetooth, CD/DVD).
Control de Amenazas Avanzado (ATC)	Supervisa continuamente los procesos en ejecución para detectar comportamientos sospechosos (escalada de privilegios, inyección de código).	Genera alertas automáticas si el nivel de sospecha supera un umbral, identificando amenazas complejas.
Gestión de Riesgos (ERA)	Escanea y evalúa vulnerabilidades en endpoints y configuraciones incorrectas.	Ofrece recomendaciones automatizadas de remediación y una visión consolidada del estado de seguridad de la red.
HyperDetect	Utiliza heurísticas avanzadas e IA para una capa de detección previa a la ejecución.	Identifica amenazas persistentes avanzadas (APT) y malware antes de que puedan iniciarse.
Gestión de Parches	Realiza escaneos y aplicación automatizada de parches de seguridad para sistemas y aplicaciones.	Mantiene actualizados Windows y Linux, cerrando las vulnerabilidades explotadas en la mayoría de los ciberataques.
Sandbox Analyzer	Analiza archivos sospechosos en un entorno virtual seguro, observando su comportamiento.	Detiene amenazas de archivo desconocido en un entorno aislado, permitiendo bloqueo o monitoreo según políticas.s.
Mitigación de Ransomware (ATS)	Crea copias de seguridad en tiempo real antes de que un proceso modifique archivos.	Permite recuperar datos cifrados, ofreciendo mitigación local, remota y con visibilidad completa de la cadena de ataque.
Gestión de Sup. de Ataque Ext. (EASM)	Descubre y analiza activos y vulnerabilidades expuestos a Internet.	Ayuda a reducir la superficie de ataque y a mejorar la seguridad perimetral de la organización.
Protección de Red	Incluye filtrado de contenido, escaneo de tráfico, control de aplicaciones y detección de ataques de red.	Permite configurar políticas de acceso y protección de datos, defendiendo el perímetro.
Aprendizaje Automático Local/Nube	Combina inteligencia global con análisis local basado en IA.	Detecta amenazas desconocidas y de día cero con mínima carga para el usuario, gracias a un enfoque híbrido rápido.



www.generalprotec.com/cibercompletoplus

EL SOFTWARE Y LOS SERVICIOS DE GENERAL PROTEC ESTÁN SUJETOS A LAS LEYES Y NORMATIVAS DE EXPORTACIÓN APLICABLES DE LA UNIÓN EUROPEA Y OTRAS JURISDICIONES. SE PROHÍBE CUALQUIER USO CONTRARIO A DICHAS NORMAS.

El uso de este servicio y su software asociado está sujeto a un acuerdo de licencia entre usted y General Protec Ciberseguridad S.L.

General Protec, el logotipo de General Protec, CiberSafe, CiberSafe Plus, CiberCompleto, CiberCompleto Plus, CiberControl, CiberCopy, CiberAuditWeb y CiberTraining son marcas comerciales o marcas comerciales registradas de General Protec Ciberseguridad S.L. en España y/o en otros países. Los demás nombres y marcas pueden ser reclamados como propiedad de otros.

Copyright © 2025 General Protec Ciberseguridad S.L. Todos los derechos reservados.