SECHARD

ZERO TRUST ORCHESTRATOR

PRODUCT BROCHURE

SECHARD
Complete Zero Trust

Complete Zero Trust is now possible

www.sechard.com

PRODU

INTRODUCCION

La creación de una estrategia útil y la gestión de las operaciones para garantizar la seguridad de la información suponen una gran presión y estrés para los equipos de tecnología de la información y de seguridad. Afortunadamente, los documentos de la Arquitectura de red de Confianza Cero (ACC por sus siglas) publicados por instituciones como el NIST nos guían para lograr nuestro objetivo. Nuestro producto SecHard, que ha cambiado las reglas del juego, simplifica estos procesos complejos con su enfoque integrado y le proporciona una confianza cero (ZT) completa. Además de proporcionar ventajas de tiempo y costes, también aliviar la carga de trabajo de su equipo de expertos en seguridad de la información.

> *"ZT es el término que designa el conjunto de paradigmas de ciberseguridad en evolución que hacen que las defensas pasen de los perímetros estáticos basados en la red a centrarse en los usuarios, los activos y los recursos. La ACC utiliza los principios de confianza cero para planificar la infraestructura y los flujos de trabajo industriales y empresariales. ZT asume que no hay una confianza implícita concedida a los activos o a las cuentas de los usuarios basada únicamente en su ubicación física o de red (es decir, redes de área local frente a Internet) o basada en la propiedad de los activos (de la empresa o personales). La autenticación y la autorización (tanto del sujeto como del dispositivo) son funciones discretas que se realizan antes de que se establezca una sesión a un recurso empresarial"*[1]

ACC requiere de una Protección por Control de Visibilidad (CVP por sus siglas en inglés) en cinco áreas: personas, carga de trabajo, dispositivos de red, dispositivos de usuario y datos. SecHard es la única solución integrada que proporciona CVP en estas cinco áreas.

Las organizaciones necesitan implementar prácticas integrales de seguridad de la información y resiliencia para que ZT sea efectivo. Cuando se equilibra con las políticas y orientaciones de ciberseguridad existentes, la gestión de la identidad y el acceso, la supervisión continua y el Security Hardening (mejores prácticas), la ACC puede proteger contra las amenazas comunes y mejorar la postura de seguridad de las organizaciones utilizando un enfoque de riesgo gestionado.

La importancia de la ACC en la ciberseguridad ha sido reconocida por los EE.UU. y su implementación se ha hecho obligatoria para todas las agencias federales a través de memorando publicado[2] por la Oficina Ejecutiva del presidente el 26 de enero de 2022.

La parte más difícil de la implementación y gestión de la ACC es el Hardening de seguridad. Según el Centro para la Seguridad en Internet (CIS por sus siglas), se requieren cientos de cambios de configuración en miles de dispositivos. El módulo de Security Hardening de SecHard genera informes de análisis de deficiencias en cuestión de minutos, de acuerdo con los estándares del sector, y realiza correcciones automáticas de las mismas en cuestión de segundos.

Antes de SecHard, para poner en práctica la ACC era necesario comprar y gestionar diversos productos. Esos tiempos han quedado atrás. SecHard le aporta tranquilidad gracias a su enfoque holístico y a sus funciones de corrección automática.

SecHard cumple con todos los requisitos de la arquitectura de confianza cero (ACC)en una sola plataforma.

DESCRIPCIÒN DEL PRODUCTO

SECURITY HARDENING

PRIVILEGED ACCESS MANAGER

ASSET MANAGER

RISK MANAGER

VULNERABILITY MANAGER

PERFORMANCE MONITOR

DEVICE MANAGER

TACACS+ SERVER

SYSLOG SERVER

(1): NIST Special Publication 800-207, Zero Trust Architecture, P:4

(2): https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf

SECHARD
Complete Zero Trust

SECURITY HARDENING

SecHard ofrece auditoría, puntuación y corrección automatizadas de Security Hardening para servidores, clientes, dispositivos de red, aplicaciones, bases de datos, etc.

Según el CIS, para tener un sistema operativo seguro, es necesario cambiar aproximadamente cuatrocientas configuraciones de seguridad en un servidor de Microsoft Windows que funcione con la configuración predeterminada. Lo más probable es que falten cientos de configuraciones de seguridad en el ordenador que usted tiene. En una red empresarial con cientos o miles de activos informáticos, informar y corregir todas estas deficiencias puede ser una operación que lleve años a los equipos informáticos.

Con SecHard, las empresas pueden añadir fácilmente sus propios y exclusivos controles y ejecutarlos en miles de activos diferentes. De este modo, se pueden producir auditorías especiales y remediaciones automáticas para tecnologías comunes y no comunes, como sistemas operativos, dispositivos de red, aplicaciones, IoT, SCADA, Swift, POS y muchos más.

Para el proceso de remediación se requieren especialistas de distintos sectores con experiencia y una gran cantidad de tiempo. Además, algunos cambios críticos pueden tener consecuencias inesperadas que podrían conducir a desastres. SecHard realiza automáticamente las correcciones de seguridad necesarias en segundos con un solo clic en cada vulnerabilidad que se requiera cerrar, eliminando todos los riesgos relacionados con el cambio sin necesidad de un conocimiento profundo.

SecHard es uno de los productos con mayor retorno de la inversión en el ámbito de la seguridad de la información. SecHard proporciona auditoría, puntuación y remediación de refuerzo de seguridad automatizados para servidores, clientes, dispositivos de red, aplicaciones, bases de datos y más.

EJEMPLO

Uno de nuestros clientes tiene aproximadamente 2500 activos. Tenían dificultades para gestionar sus procesos de Security Hardening para cumplir con varias regulaciones.

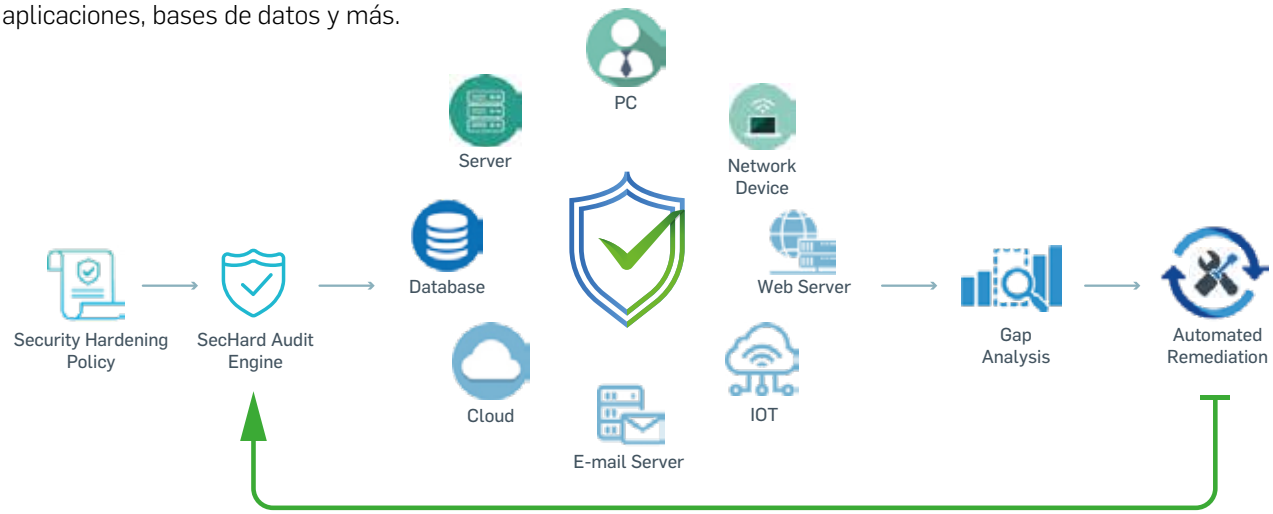
SecHard creó el informe de las deficiencias en el security hardening en tan solo una hora.

Todas las operaciones de corrección del hardening se completaron en unas pocas semanas con la función de corrección automática de SecHard.

Auditoria en tiempo real y remediación

BENEFICIOS CLAVE

- Primera auditoría de fortalecimiento de la seguridad de la industria con remediación automatizada
- Puntuación de seguridad detallada
- Amplia compatibilidad con dispositivos y plataformas
- Remediación SIN RIESGO
- Retorno de la inversión inigualable



PRIVILEGED ACCESS MANAGER

El CVP más importante de la ACC es la gente. Los estudios han probado que el 77% de las fugas de datos están causadas por el abuso de privilegios, lo que demuestra la importancia de este control. Debido a la dificultad de la gestión de identidades, pueden surgir muchos tipos diferentes de amenazas que van desde el espionaje hasta el ransomware.

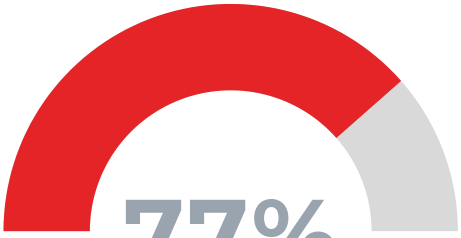
A diferencia de un producto PAM tradicional, SecHard ofrece una solución PAM que se integra con otras áreas de CVP recomendadas por la ACC. SecHard no solo da acceso a los privilegios a la persona adecuada, sino que también realiza las CVP recomendadas por la ACC en todos los dispositivos de red utilizados en la conexión, y en el ordenador que realiza la conexión. De esta manera, los ordenadores cuyo hardening o puntuaciones de seguridad producidas por SecHard están por debajo del nivel de seguridad aceptable pueden ser restringidos del acceso autorizado o se pueden generar advertencias de riesgo. SecHard puede descubrir y registrar información de nuevos activos importantes, realizar valoraciones automáticas de hardenings y remediar los ajustes de hardening predefinidos de forma totalmente automática.

Esto no significa que SecHard no tenga características PAM tradicionales. Al igual que todos los demás productos PAM, SecHard tiene una bóveda de contraseñas. Puede habilitar los accesos como RDP, VNC, SSH y Telnet sin conocer la contraseña y puede grabar todas las sesiones tanto en formato de vídeo como de texto.

¿Ya tiene un producto PAM? No se preocupe. SecHard puede integrarse con productos PAM de terceros y también puede valorar su security hardening.

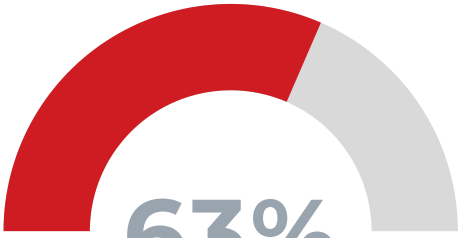
VENTAJAS PRINCIPALES

- Bóveda de contraseñas avanzada
- Grabación de sesiones RDP, VNC, SSH, Telnet y soporte OCRR
- Integración de PAM de terceros
- Autenticación de 2FA
- Reducción de costes y complejidad



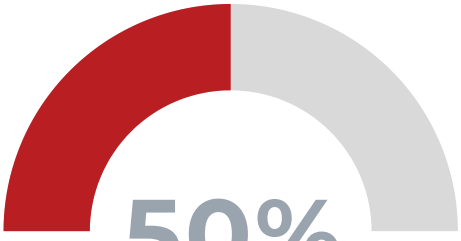
77%

filtraciones de datos causadas por el abuso de privilegios[3]



63%

filtraciones de datos causadas por el personal[4]



50%

fugas de datos causadas por el administrador del sistema[5]

(3)(4)(5): Verizon 2021 Data Breach Investigations Report, P:44

ASSET MANAGER

La gestión de activos es siempre un desafío. Los cambios se dan forma diaria en activos existentes y nuevos elementos están siendo añadidos a la infraestructura. Este tipo de actividad que ocurre constantemente, genera que las empresas pierdan fácilmente el control de sus elementos instalados, contando con información no actualizada; ocasionando que sus análisis de riesgos de seguridad, se vean impactados al no tener un inventario confiable y actualizado de su infraestructura.

SecHard resuelve el problema de la administración de equipos con una automatización total. Gracias a su función de autodescubrimiento, SecHard puede detectar bienes/activos nuevos y cambiantes, accede de forma automática y segura a los mismos utilizando las funciones del módulo PAM y genera automáticamente varias valoraciones de seguridad, incluido el Security Hardening.

El módulo SecHard Asset Manager permite la administración y reporte de hardware, componentes de hardware (CPU, RAM, disco, etc.) e inventario de software (sistemas operativos, software instalado, servicios en ejecución, etc.). Los equipos que no tienen una dirección IP, como los teclados y los monitores, pueden ser gestionados por SecHard. Todo el hardware y el software puede asignarse a personas, unidades o ubicaciones. Supervisa los períodos de garantía y de licencia del hardware y el software, los servicios en ejecución en los ordenadores, genera alarmas para los servicios críticos y puede reiniciar automáticamente un servicio que se haya detenido inesperadamente.

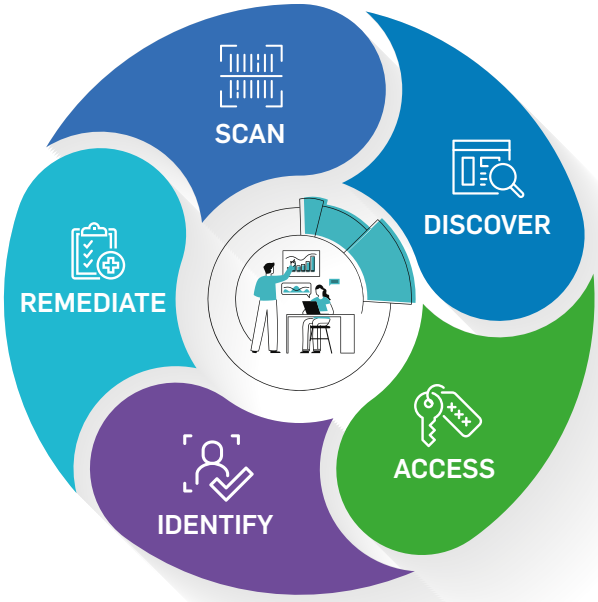
El módulo de Asset Manager también permite guardar las valoraciones de riesgo de los equipos y/o grupos de equipos, generadas por el departamento de seguridad de la información de la organización, que serán utilizadas por el módulo de gestión de riesgos. SecHard también puede importar valoraciones de riesgo de productos GRC.

El módulo Asset Manager de SecHard ha sido desarrollado de acuerdo con el Marco de Ciberseguridad del NIST y la Arquitectura de Seguridad Adaptativa de Gartner, y proporciona una potente administración de equipos en función del riesgo.

VENTAJAS PRINCIPALES

- Descubrimiento automatizado de equipos
- Valoración de seguridad automatizada para nuevos equipos
- Implementación de la referencia de seguridad
- Gestión del inventario de hardware y software
- Integración con GRC y CMDB

Proceso de Asset Manager de SecHard



RISK MANAGER

El mayor problema al que el sector no ha sabido responder, es la incapacidad de valorar y gestionar de forma holística los riesgos empresariales junto con los riesgos técnicos. En todos los análisis de cumplimiento del Sistema de Gestión de Seguridad de la Información (SGSI) de la norma ISO27001, los riesgos empresariales se valoran, pero están destinados a vivir en una celda de Excel. De hecho, estas valoraciones no se utilizan en ninguna parte.

SecHard combina los riesgos empresariales y técnicos y calcula las valoraciones de los riesgos en el mundo real. Mide y puntúa los riesgos técnicos de seguridad de los activos o grupos de activos con sus propios módulos de Security Hardening, Vulnerability Management y Asset Management.

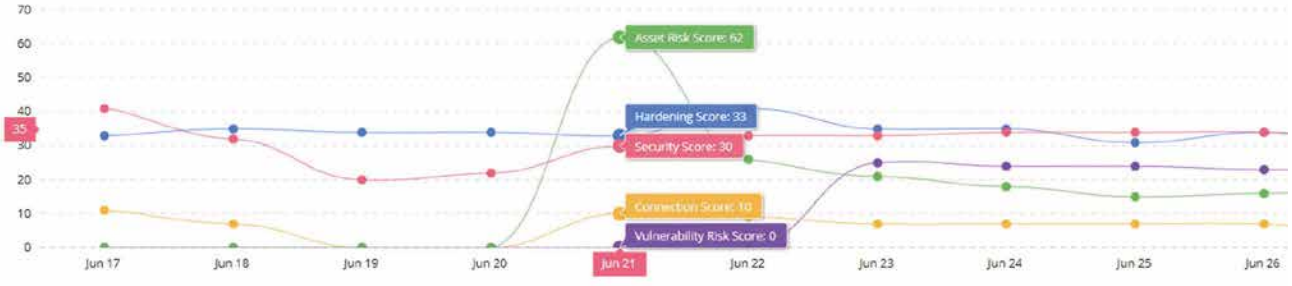
El riesgo de seguridad valorado por los equipos de seguridad de la información para la norma ISO 27001 ISMS y otras normas similares puede añadirse al módulo de gestión de activos de SecHard. Además, las valoraciones técnicas y empresariales pueden ser integradas por el algoritmo de riesgo de SecHard, que determina la calificación del riesgo en el mundo real.

SecHard cuenta con la función de remediación de Security Hardening para reducir las puntuaciones de riesgo técnico tras determinar la puntuación de riesgo real. Al mismo tiempo, gracias a la integración de Trellix (McAfee Enterprise), SecHard hace posible que el software de seguridad convencional proporcione seguridad instantánea, activando automáticamente el Hardening de las configuraciones de Endpoint Security, DLP, EDR y TIE para los dispositivos que superen el nivel de riesgo aceptable.

En las grandes empresas se utilizan soluciones de software para la Administración del riesgo y el cumplimiento (en inglés GRC), que permiten gestionar las amenazas. SecHard puede asociar los activos que descubre a nivel de los grupos ya existentes en solución GRC y recibe automáticamente las puntuaciones de riesgo de los activos o los grupos en mención. Gracias a esta integración el nivel de riesgo es recibido por SecHard de forma automáticamente para aplicar los respectivos controles de seguridad.

VENTAJAS PRINCIPALES

- Valoración de riesgos de hardening, seguridad y vulnerabilidad
- Gestión de riesgos basada en los dispositivos
- Valoración de riesgos en el mundo real
- Integración de GRC
- Seguridad inmediata con la integración de Trellix (McAfee Enterprise)



Security Graph Last 10 Days

SECHARD
Complete Zero Trust

VULNERABILITY MANAGER

Uno de los principios más importantes de la seguridad de la información es la detección y gestión de las vulnerabilidades. SecHard maneja los procesos de detección y gestión de vulnerabilidades para todos los activos de TI sin crear ningún riesgo gracias al método de escaneo pasivo.

SecHard SecHard recolecta información detallada sobre los dispositivos y su software mediante los módulos de gestión de activos y de dispositivos. Las vulnerabilidades de los sistemas operativos pueden notificarse mediante consultas enviadas a la National Vulnerability Database (NVD). Los niveles de riesgo de las vulnerabilidades detectadas se muestran en el estándar CVSS y SecHard informa de si existe un "exploit" público que utilice estas vulnerabilidades. SecHard también le redirige a artículos publicados por los proveedores para obtener información detallada sobre las vulnerabilidades.

SecHard puede importar las valoraciones generadas por herramientas de exploración de vulnerabilidades de terceros e incluirlas en el proceso de gestión de riesgos. SecHard también es capaz de enviar las calificaciones de las vulnerabilidades a terceros.

PRINCIPALES VENTAJAS

- Escaneo pasivo de vulnerabilidades
- Valoración de riesgos basada en CVSS
- Integración con terceros
- Disponibilidad pública de exploits
- Informes detallados y alarmas

PERFORMANCE MONITOR

La disponibilidad es tan importante como la privacidad y la integridad en la ecuación de la seguridad de la información. Según la ACC, el rendimiento y la disponibilidad son dos factores que deben supervisarse teniendo en cuenta los controles de seguridad y la gestión de riesgos.

SecHard proporciona monitoreo integrado de rendimiento y disponibilidad para servidores y dispositivos de red. Esta arquitectura integrada hace posible monitorear los datos de los servidores y dispositivos de red que llegan a través de los exportadores VMI, Nod y SNMP, haciendo uso de un avanzado panel de control, personalizable, el cual muestran información en tiempo real de los equipos que están siendo analizados.

Es imposible supervisar cientos de activos con el ojo humano desde las pantallas de las grandes redes. SecHard supervisa los equipos críticos en nombre del personal de supervisión. Puede generar alarmas, enviar correos electrónicos y ejecutar acciones predefinidas cuando se superan los umbrales. Además, SecHard almacena los datos de rendimiento de forma histórica y simplifica la planificación de la capacidad.

La herramienta Performance Monitor de SecHard proporciona servicios de monitoreo para todo tipo de dispositivos y software con direcciones IP, como computadoras de escritorio, servidores, bases de datos, servicios WEB, servicios SMTP, cámaras IP, impresoras de red, routers, switches, etc.

PRINCIPALES VENTAJAS

- Amplio soporte de dispositivos
- Alarmas avanzadas y acciones automáticas
- Tableros inteligentes y personalizables
- Monitoreo de ancho de banda para dispositivos de red
- Informes históricos

DEVICE MANAGER

La seguridad de la configuración es un elemento importante en la ACC. SecHard realiza comprobaciones de Security Hardening con gran éxito y rapidez. Más allá del Security Hardening, las tareas de configuración y gestión de dispositivos también son realizadas por SecHard.

Las operaciones de copia de seguridad y restauración de la configuración de los dispositivos de red, pueden realizarse de forma centralizada por SecHard. Además de las configuraciones de seguridad, SecHard puede gestionar y supervisar automáticamente todos los cambios de configuración en los equipos que gestiona. SecHard también envía los cambios de configuración en múltiples dispositivos.

En el caso de los dispositivos de red, SecHard supervisa el número de puertos y su estado, los detalles del tráfico que pasa por los puertos y el uso de la CPU y la RAM. Las alarmas pueden activarse cuando se producen eventos críticos. Las tareas operativas, como la creación de una VLAN en los dispositivos de red, pueden realizarse fácilmente a través de la interfaz de usuario de SecHard con unos pocos clics, sin necesidad de conocer los comandos de la CLI.

Para que los dispositivos de red, puedan corregir las vulnerabilidades detectadas previamente por SecHard, su firmware puede actualizarse a través de la interfaz de usuario de SecHard.

La configuración de la seguridad de los puertos es vital para prevenir ataques como ARP Spoofing, STP Manipulation y DHCP Starvation que pueden ser realizados debido a la configuración insegura de los dispositivos de red. SecHard comprueba si la configuración de seguridad de los puertos se ha realizado correctamente o no. Los dispositivos de red con configuraciones de seguridad de puertos que faltan pueden ser remediados automáticamente con SecHard. También puede desactivar los puertos que no se utilicen durante un determinado periodo de tiempo y asignarlos a una VLAN pasiva. Gracias a estas características, proporciona seguridad a los dispositivos de red incluso en áreas no afectadas por las autoridades y normativas globales de Security Hardening.

PRINCIPALES VENTAJAS

- Copia de seguridad y restauración de la configuración
- Gestión de cambios
- Gestión basada en roles
- Configuración de múltiples dispositivos
- Supervisión e informes continuos

TACACS+ SERVER

Probablemente, el más importante de los CVPs recomendados por ZTA es la gente. Microsoft Active Directory proporciona un servicio de gestión de cuentas centralizado para los sistemas Microsoft Windows, pero los sistemas *nix y los dispositivos de red no tienen tanta suerte. Estos sistemas, que no disponen de una gestión de cuentas centralizada, vienen con sus cuentas y contraseñas locales. El Centro para la Seguridad en Internet (CIS) recomienda encarecidamente restringir las cuentas locales e implementar una gestión de cuentas centralizada.

El módulo SecHard TACACS+ puede realizar la autenticación y autorización central para sistemas *nix y dispositivos de red. Proporciona una gestión eficiente de todos los dispositivos con una sola cuenta. Además, el servidor SecHard TACACS+ ofrece la posibilidad de Single Sign On (SSO) con la integración de Microsoft Active Directory.

La implementación de las configuraciones de TACACS+ en múltiples sistemas *nix y dispositivos de red es una operación difícil y que requiere mucho tiempo. SecHard proporciona una implementación automatizada para aplicar la configuración requerida en los dispositivos y servidores de red en cuestión de minutos.

SecHard TACACS+ cuenta con una autorización y supervisión detalladas más allá de la autenticación con soporte AAA. Así, es posible una gestión detallada de los roles. Todos los eventos se registran y se garantiza que estos registros permanezcan inalterados con marcas de tiempo.

PRINCIPALES VENTAJAS

- Soporta AAA
- Integración con Microsoft Active Directory
- Inicio de sesión único
- Configuración automatizada de TACACS+ en múltiples dispositivos
- Integración de SIEM y terceros

SYSLOG SERVER

En ACC es necesario monitorear continuamente, registrar eventos y activar alarmas para eventos críticos. SecHard tiene un módulo Syslog completo que puede proporcionar todas las tareas necesarias recomendadas por ACC.

SecHard Syslog Server soporta Syslog seguro (TLS) para coleccionar los registros de forma protegida de los dispositivos que soportan el envío de mensajes Syslog seguros. Además, los registros de eventos recogidos se almacenan con una marca de tiempo.

Todos los eventos Syslog pueden ser reenviados a terceros como SIEM, SOAR, software de gestión de registros en formato CEF o Syslog.

PRINCIPALES VENTAJAS

- Despliegue rápido
- Monitoreo de registros en tiempo real
- Informes y alarmas avanzadas
- Reenvío de eventos a terceros
- Tableros personalizables

RESUMEN

Con su enfoque holístico, SecHard es un cambio en el panorama actual que puede cumplir exhaustivamente los requisitos del Memorándum de la Oficina Ejecutiva del Presidente (M-22-09), la publicación NIST SP 800-207 Zero Trust Architecture y normativas ISO27001. Puede realizar automáticamente las funciones del Marco de Ciberseguridad del NIST y los procesos recomendados por la Arquitectura de Seguridad Adaptativa de Gartner, eliminando la necesidad de expertos.

Gracias a su análisis de seguridad automatizado y a su corrección, proporciona un gran ahorro de costos, ya que elimina la necesidad de contar con ingenieros experimentados en seguridad de la información. SecHard proporciona una importante rentabilidad de la inversión (ROI) decenas de veces superior a la de otros productos de seguridad de la información.

Esta increíble tecnología funciona sin agentes, sin requerir ningún cambio en su entorno, y su instalación solo lleva una hora. Tiene soporte de API bidireccional para tener una fácil integración con terceros.

Figure 1

Las Cuatro etapas de una arquitectura de seguridad adaptativa

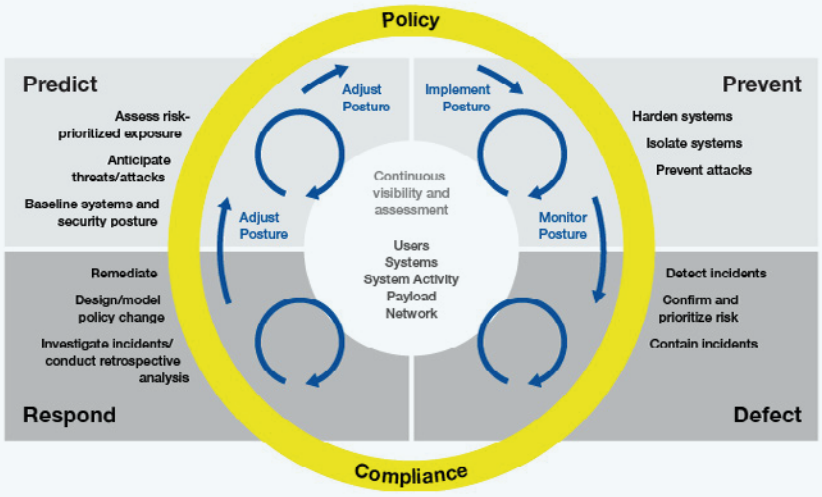


Figure 2

LICENCIAS

SecHard ofrece la confianza cero completa en una plataforma con un modelo de licencias extremadamente simplificado. Solo es necesario determinar la cantidad de servidores, dispositivos de red y equipos cliente en términos de licencias. Un número ilimitado de usuarios puede conectarse a todos los módulos, incluido PAM. SecHard, se licencia bajo la modalidad de suscripción anual, ofreciendo descuentos importantes para 2 o más años de suscripción.

Figure 1: https://www.nist.gov/cyberframework
Figure 2: https://www.gartner.com/smarterwithgartner/build-adaptive-security-architecture-into-your-organization

SECHARD

Complete Zero Trust

www.sechard.com

Distribuidor Autorizado

555 Winderley Place, Suite 300 • Maitland, FL 32751

(786) 206-6512 • (786) 513-2806

info@greenlt.com • www.greenlt.com