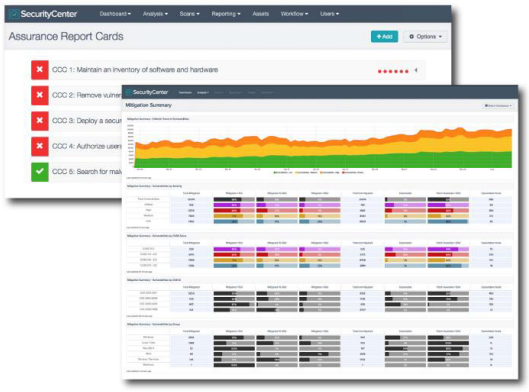
SecurityCenter CV
Continuous View

“Se ejecuta internamente con la solución integral de Tenable para priorizar los riesgos de seguridad y evaluar la posición de seguridad de la empresa según los objetivos comerciales en cualquier momento”. – Proveedor de servicios de salud

Solución líder en el mercado de monitoreo de redes continuo

Los cambiantes entornos TI (virtuales, móviles, servicios en la nube) y amenazas cibernéticas han hecho que las auditorías de cumplimiento y escaneos periódicos sean insuficientes para proteger los negocios contra los ataques cibernéticos modernos. Un monitoreo de redes continuo es un nuevo enfoque para el fortalecimiento de la seguridad de su empresa y una postura de cumplimiento permanente, ya que garantiza que sus inversiones en seguridad de TI estén configuradas y operen correctamente, además de proporcionar conocimientos prácticos sobre los riesgos de seguridad más importantes que afectan su negocio.

SecurityCenter Continuous View® (SecurityCenter CV™) es la solución líder en el mercado de monitoreo de redes continuo que provee visibilidad total de su postura de cumplimiento y seguridad en toda su infraestructura TI. También proporciona información práctica sobre las debilidades priorizadas y una garantía permanente de que la seguridad y cumplimiento están alineadas con las metas de la organización. Es la única solución que integra la detección de activos en el local y en la nube, asesoría de vulnerabilidad activa y pasiva, auditoría de configuración, detección de cambios, detección de malware, inteligencia de amenazas y análisis de redes y actividad de usuarios.



Paneles altamente personalizables, informes, políticas de seguridad y flujos de trabajo para adecuarse a sus necesidades comerciales específicas

SecurityCenter CV incluye tarjetas de informe de seguridad, que le permiten medir, analizar y visualizar de forma continua la efectividad de su programa de seguridad, con base en sus objetivos comerciales de alto nivel y políticas personalizables subyacentes que los responsables de seguridad de la información (chief information security officers, CISO) y ejecutivos consideran importantes.

Investigación de Tenable

El equipo de investigación de Tenable proporciona frecuentes actualizaciones de información sobre amenazas y vulnerabilidades, analítica avanzada, políticas de seguridad/cumplimiento, paneles/informes y tarjetas de informe de seguridad a todos los clientes de SecurityCenter CV. Este contenido listo para usar se basa en las prácticas óptimas de la industria y los clientes recopiladas por Tenable, lo que pone a su disposición el poder de nuestro equipo de investigación de seguridad. Este contenido es parte de la suscripción a SecurityCenter CV.

Beneficios clave

- Sepa siempre cuando activos nuevos o variados alteran su superficie de ataque.
- Obtenga una amplia visibilidad en toda la infraestructura TI, incluidos terminales, servidores, bases de datos, dispositivos móviles, controladores de dominio, dispositivos de redes, aplicaciones virtuales y en la nube
- Vea lo que otros dejan pasar con una visibilidad de sistemas transitorios, difíciles de acceder e inseguros de escanear
- Obtenga conocimientos detallados con el análisis automático de vulnerabilidad y datos de configuración que mejoran con el estado de parches, vulnerabilidades conocidas, inteligencia de amenazas e información de tráfico de redes sospechosas y comportamiento del usuario
- Concéntrese en lo que importa identificando rápidamente las debilidades fáciles de aprovechar
- Comunique posturas de seguridad usando tarjetas de informe de seguridad (Assurance Report Cards®, ARC)
- Documente el cumplimiento con estándares y normativas de la industria
- Manténgase al día con el contenido provisto por Tenable

Características clave

- Tarjetas de informe de seguridad (ARC): miden continuamente la efectividad de la seguridad definida por el cliente y las políticas de cumplimiento, basándose en objetivos comerciales para identificar y cerrar las brechas potenciales.
- Informes/paneles altamente personalizables: la interfaz de usuario basada en HTML5 satisface las necesidades específicas de los CISO, gestores de seguridad, analistas y profesionales/operadores.
- Amplia cobertura de activos: evalúa servidores, terminales, dispositivos de red, sistemas operativos, bases de datos y aplicaciones en infraestructuras físicas, virtuales y en la nube.
- Detección continua de activos: detecta todos los dispositivos móviles, físicos, virtuales y entornos en la nube dentro de la red, incluso los activos no autorizados.
- Clasificación dinámica de activos: agrupa los activos según las políticas que cumplan criterios específicos; por ejemplo, activos de Windows 7 con vulnerabilidades de más de 30 días.
- Gestión de vulnerabilidad: opciones de escaneo múltiple, incluidos monitoreo pasivo de redes, escaneo de vulnerabilidades no acreditadas y acreditadas para un profundo análisis y auditoría de configuración.
- Escaneo con agentes: disponible para que las organizaciones puedan escanear más fácilmente activos móviles y difíciles de acceder.
- Detección de malware: aprovecha la información de inteligencia contra amenazas integrada (indicadores de malware, listas negras) para identificar malware avanzado.
- Evaluación de salud de la red: monitorea de forma continua la red para buscar tráfico sospechoso desde o hacia sistemas o servicios vulnerables, dispositivos desconocidos, botnets o servidores de control o de comando.
- Detección de anomalías: utiliza las técnicas de análisis de comportamientos anómalos en las fuentes de registro externo, para detectar automáticamente actividades fuera de los parámetros de la línea base.
- Tendencia/analítica avanzada: proporciona conocimientos contextuales e información práctica para priorizar los temas de seguridad asociados con la postura de seguridad de todos los activos de la compañía.
- Notificaciones: dispone de alertas configurables para que los administradores tomen acciones mediante correos, notificaciones, informes de problemas o para tomar acciones automáticas mediante las interfaces de programación.
- Cumplimiento simplificado: permite realizar verificaciones predefinidas para los estándares industriales y los mandatos normativos, como CERT, DISA STIG, DHS CDM, FISMA, DSS de la PCI, HIPAA/HITECH y más.
- Integraciones: permite la utilización de integraciones listas para usar con gestión de parches, gestión de dispositivos móviles, inteligencia de amenazas y otros productos de terceros, o desarrolla integraciones personalizadas mediante las interfaces de programación del SecurityCenter.

La ventaja de SecurityCenter CV

Los clientes eligen SecurityCenter CV ya que los ayuda a:

- **Eliminar puntos ciegos** que surgen de activos no gestionados y debilidades que elevan su perfil de riesgo y que con frecuencia son el origen de problemas de seguridad.
- **Elevar la eficiencia** informada por un contexto completo para rápidamente comprender y priorizar las debilidades.
- **Garantizar la seguridad y comprobar el cumplimiento** a todos los interesados, mediante el uso de parámetros específicos que comunican el estado claramente.

Ediciones de SecurityCenter

SecurityCenter

SecurityCenter® es la solución de análisis de vulnerabilidades de última generación, que incluye múltiples escáneres Nessus, los escáneres de vulnerabilidad más implementados en todo el mundo. Provee la visibilidad más integral en la postura de seguridad de su compleja y distribuida infraestructura de TI.

SecurityCenter Continuous View

SecurityCenter Continuous View es la plataforma líder en el mercado de monitoreo continuo de redes. Integra SecurityCenter® junto con múltiples sensores de red de Passive Vulnerability Scanner® (PVS™) y Log Correlación Engine® (LCE®) para proporcionar un monitoreo de redes continuo e integral.

Para obtener más información: Visite tenable.com
Contáctenos: Escríbanos a sales@tenable.com o visite tenable.com/contact