Gerente de Vulnerabilidad Industrial

SIEMENS

Descuidar las vulnerabilidades significa tomar riesgos

Desafíos operativos

- Todos los días se informan nuevas vulnerabilidades de software.
- Actualmente, los fabricantes y operadores de tecnología de automatización con una multitud de diferentes componentes de software luchan por identificar si sus productos se ven afectados.
- La solución actual: Comprobación manual de diferentes páginas web de proveedores de tecnología de automatización (p. ej., en la página web de Siemens).
- El estándar de seguridad industrial IEC 62443 2-3 recomienda un amplio proceso de administración de parches.

Las vulnerabilidades de seguridad ya conocidas son uno de los principales puntos de entrada de los ciberataques. Debe mantenerse al día con las vulnerabilidades y reaccionar con prontitud.

Possible consequences

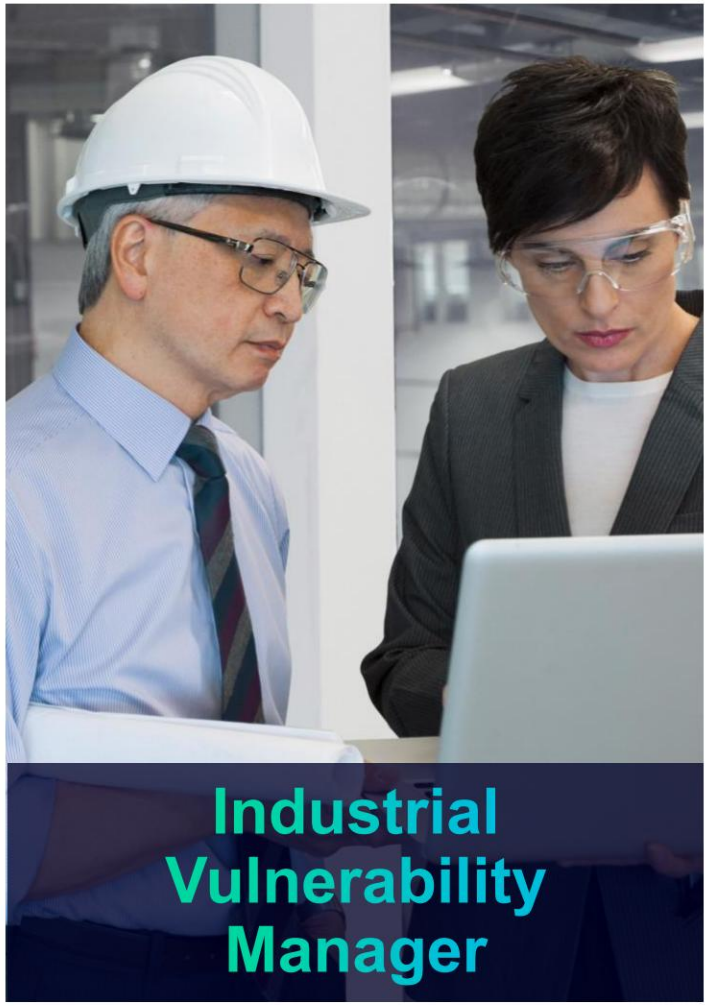
Alto esfuerzo manual y, en consecuencia, descuidar las vulnerabilidades ya informadas oficialmente

Manténgase al tanto de las amenazas reales y, en consecuencia, no active medidas proactivas (por ejemplo, parches)

Pérdida financiera significativa debido a ataques cibernéticos que explotan vulnerabilidades existentes

SIEMENS

Administre de manera eficiente las vulnerabilidades para maximizar la disponibilidad con Industrial Vulnerability Manager



Solución

Industrial Vulnerability Manager es una aplicación que proporciona información de seguridad relevante para permitir que los fabricantes y operadores de tecnología de automatización gestionen de manera proactiva sus riesgos cibernéticos, adaptados a su sistema en una ventanilla única.

¿Como funciona?

Paso 1: Definición de los componentes a monitorear

Paso 2: Monitoreo de vulnerabilidades publicadas recientemente (completamente en segundo plano)

Paso 3: Generación automática de “Boletines de Seguridad” digitales en caso de vulnerabilidades detectadas y posibles parches; descripción general a través del tablero gráfico

Varias opciones de implementación para cumplir con diferentes requisitos:

Opción A: para clientes finales, basada en AWS

Opción B: para clientes finales, en las instalaciones

Opción C: para clientes finales, basada en Siemens Industrial Edge Opción D:

para OEM, basada en una solución en la nube (incluidos los informes para los clientes de OEM)

SIEMENS

Opción A para clientes finales, basada en AWS

Paso 2: Supervise los componentes enumerados con respecto a las vulnerabilidades publicadas recientemente (ocurre completamente en segundo plano).

Paso 1: Crear y actualizar la lista de seguimiento con los componentes del cliente.

Servicio Siemens administración

Cliente final

amazon web services™

API

Paso 3: Informe al cliente sobre los componentes vulnerables con un análisis de boletín de seguridad.

Más de 80.000 componentes:

open source initiative®

ubuntu

McAfee

SIEMENS

Microsoft

¡y más!

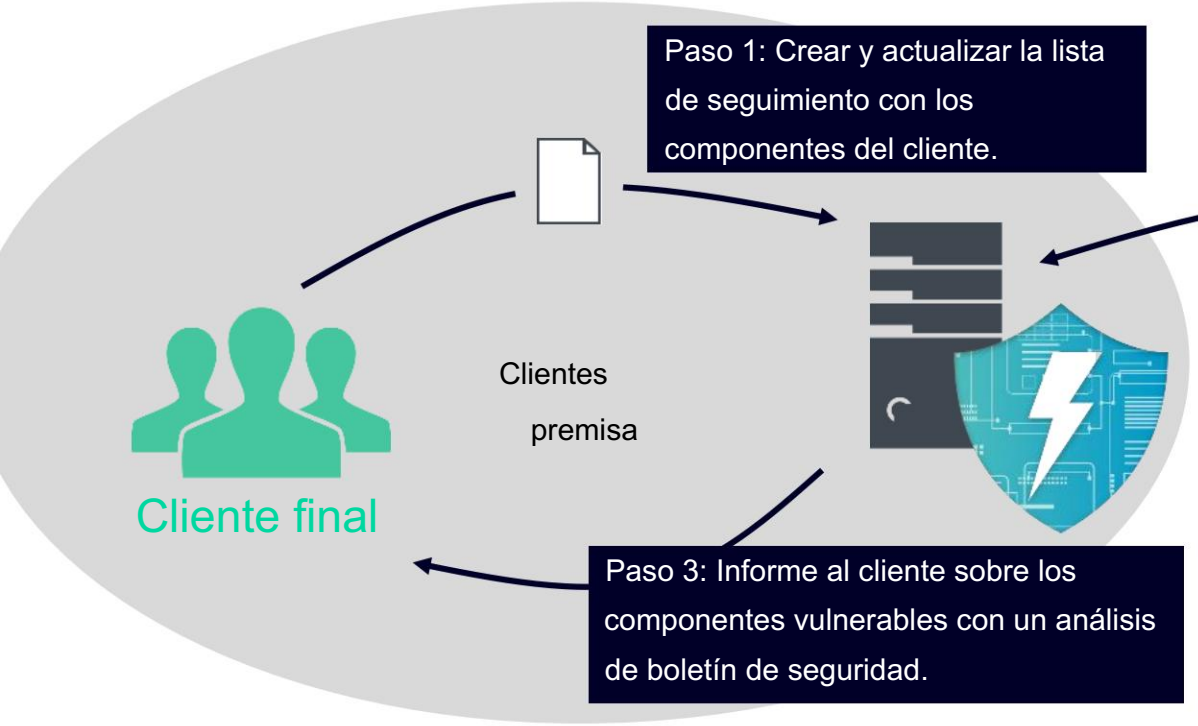
IBM

...

Condición previa: Los componentes, sus vulnerabilidades publicadas y la información de parches están disponibles.

SIEMENS

Opción B para clientes finales, en las instalaciones



Paso 2: la versión local de Industrial Vulnerability Manager sondea la información real de la base de datos del servidor central a través de puertos dedicados y entrega solo los detalles de la licencia al servidor central.

SIEMENS

Más de 80.000 componentes:

open source initiative
ubuntu
McAfee
SIEMENS
Microsoft
¡y más!
IBM
...

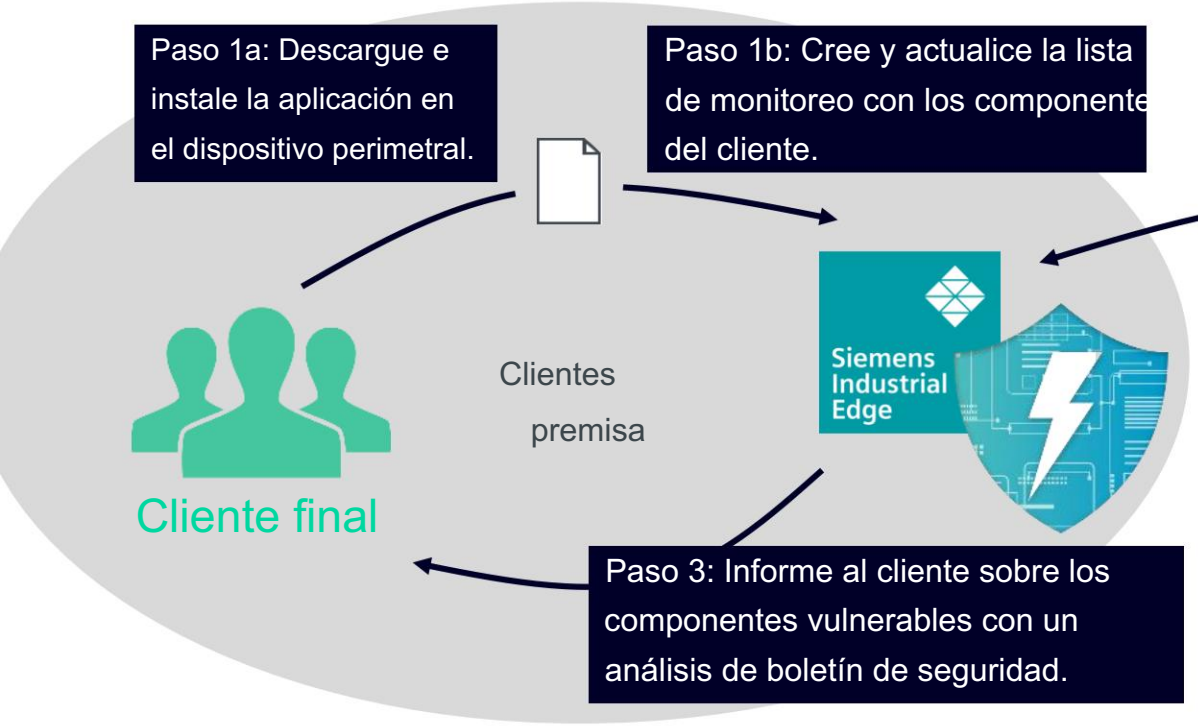
Condición previa: Los componentes, sus vulnerabilidades publicadas y la información de parches están disponibles.

Detalles:

• Industrial Vulnerability Manager está instalado en un sistema en las instalaciones del cliente (Ubuntu Linux) • Toda la comunicación se administra desde la aplicación en el sitio • Toda la información de los activos del cliente permanece en el sitio del cliente • El cliente es responsable de la administración y operación

SIEMENS

Opción C para clientes finales, basada en Siemens Industrial Edge



Paso 2: la versión perimetral de Industrial Vulnerability Manager sondea la información real de la base de datos del servidor central a través de puertos dedicados y entrega solo los detalles de la licencia al servidor central.

SIEMENS

Más de 80.000 componentes:

open source initiative
ubuntu
McAfee
SIEMENS
Microsoft
¡y más!
IBM
...

Condición previa: Los componentes, sus vulnerabilidades publicadas y la información de parches están disponibles.

Detalles:

- Industrial Vulnerability Manager se descarga de la tienda de aplicaciones Siemens Industrial Edge y se instala en el dispositivo Edge en las instalaciones del cliente.
- Toda la comunicación se administra desde el administrador de Edge
- Toda la información de los activos del cliente permanece en el sitio del cliente en el dispositivo Edge
- El cliente es responsable de la administración y operación

SIEMENS

Opción D para OEM, basada en una solución en la nube

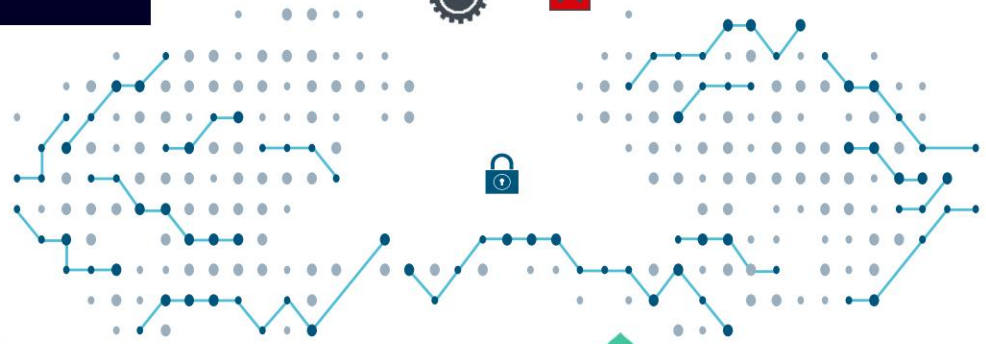
OEM

Paso 1a: Cree y actualice la lista de monitoreo con los componentes incluidos en sus máquinas.

Paso 1b: Generar cuentas de usuario para sus clientes.

Paso 2: Supervise los componentes enumerados con respecto a las vulnerabilidades publicadas recientemente (ocurre completamente en segundo plano).

Servicio Siemens administración



Más de 80.000 componentes:

open source initiative

ubuntu

McAfee

SIEMENS

Microsoft

¡y más!

IBM

...

API

cliente del OEM

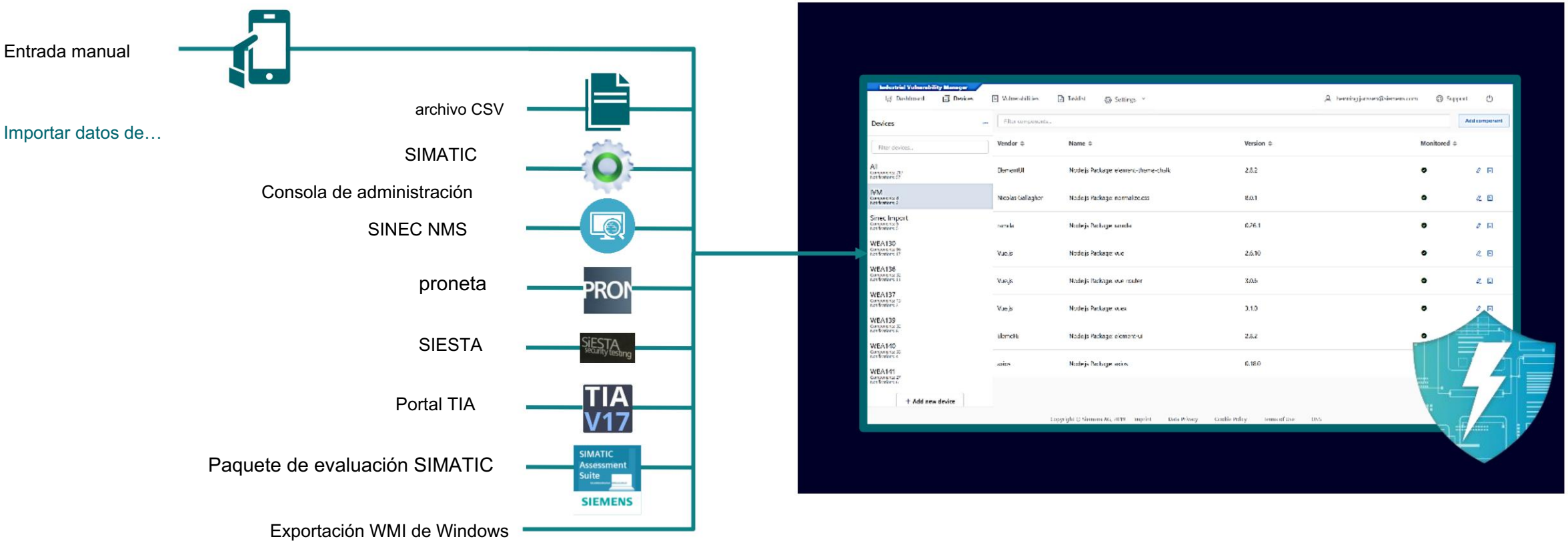
Paso 3: los clientes del OEM inician sesión en el servicio web para recibir información sobre componentes vulnerables dentro de las máquinas de los OEM, incluido un análisis de boletín de seguridad.

Condición previa: Los componentes, sus vulnerabilidades publicadas y la información de parches están disponibles.

SIEMENS

Paso 1: Definición de los componentes a monitorear

Fácil creación y actualización de la lista de componentes a través de varias opciones de importación



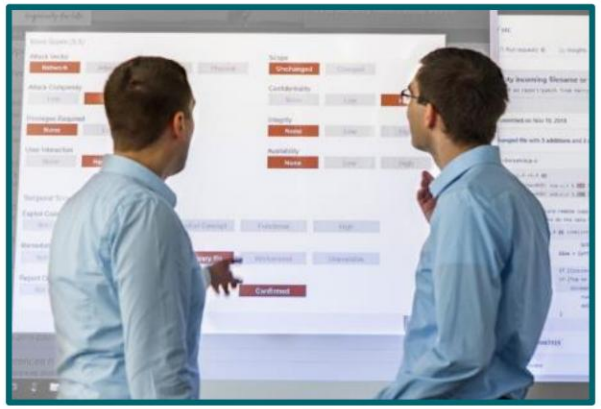
SIEMENS

Paso 2: Monitoreo de vulnerabilidades publicadas recientemente

Un sofisticado sistema como base para el Industrial Vulnerability Manager

Infraestructura de monitoreo única

- Obtener información de vulnerabilidad relevante de todo Internet, por ejemplo:
  - Avisos de seguridad oficiales
  - Páginas de soporte de proveedores
  - Comunidades de seguridad
- Cobertura de vulnerabilidades que afectan:
  - Software de código abierto
  - Software comercial
  - Componentes de hardware
  - Siemens y terceros



Equipo de expertos en seguridad

- Evalúa vulnerabilidades con el principio de los cuatro ojos con respecto a dos escalas de calificación:
  - Escala de criticidad
  - CVSS

Proceso probado

- Monitoreo de más de 80,000 componentes (en constante crecimiento)
- Más de 1,000 vulnerabilidades por mes, agrupadas en paquetes practicables

SIEMENS

Paso 3: Generación automática de “Boletines de Seguridad” digitales

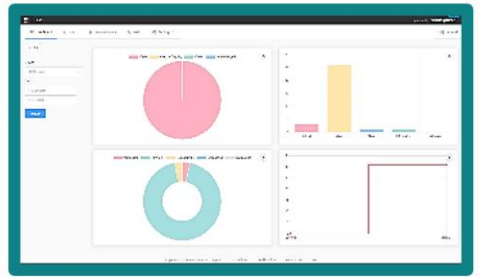
Las notificaciones y el tablero permiten una fácil gestión y reporte de riesgos cibernéticos.

Boletín de seguridad

- Descripción de la vulnerabilidad y componentes afectados
- Monitoreo en tiempo real de los parches disponibles
- Puntaje CVSS
- Prioridad
- Enlace al sitio web del proveedor

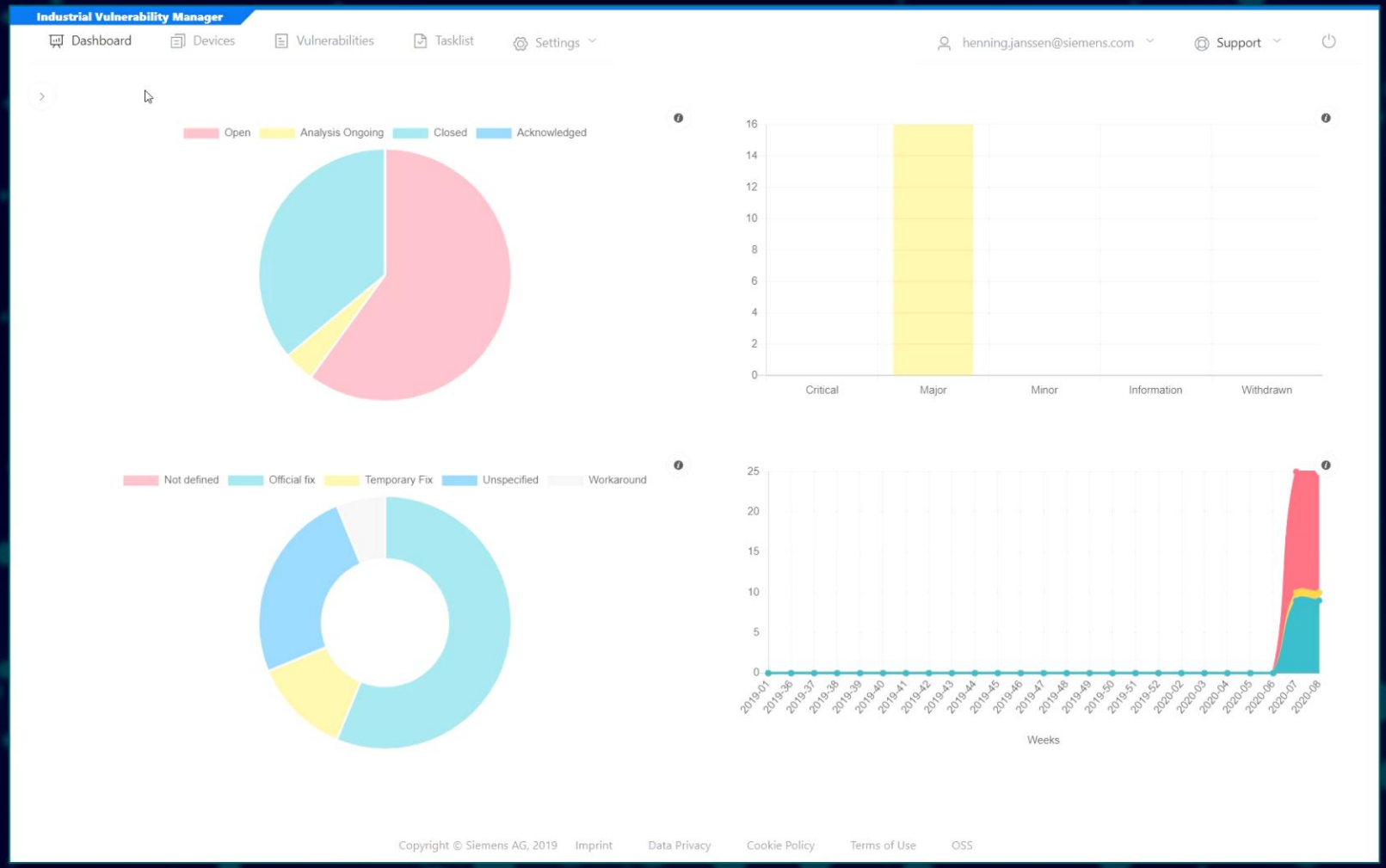
Tablero gráfico

- Resumen de vulnerabilidades incluyendo la criticidad
- Lista de tareas para verificar las correcciones vencidas y futuras
- Resumen del estado del parche para seguir y rastrear la mitigación y el cierre de las vulnerabilidades



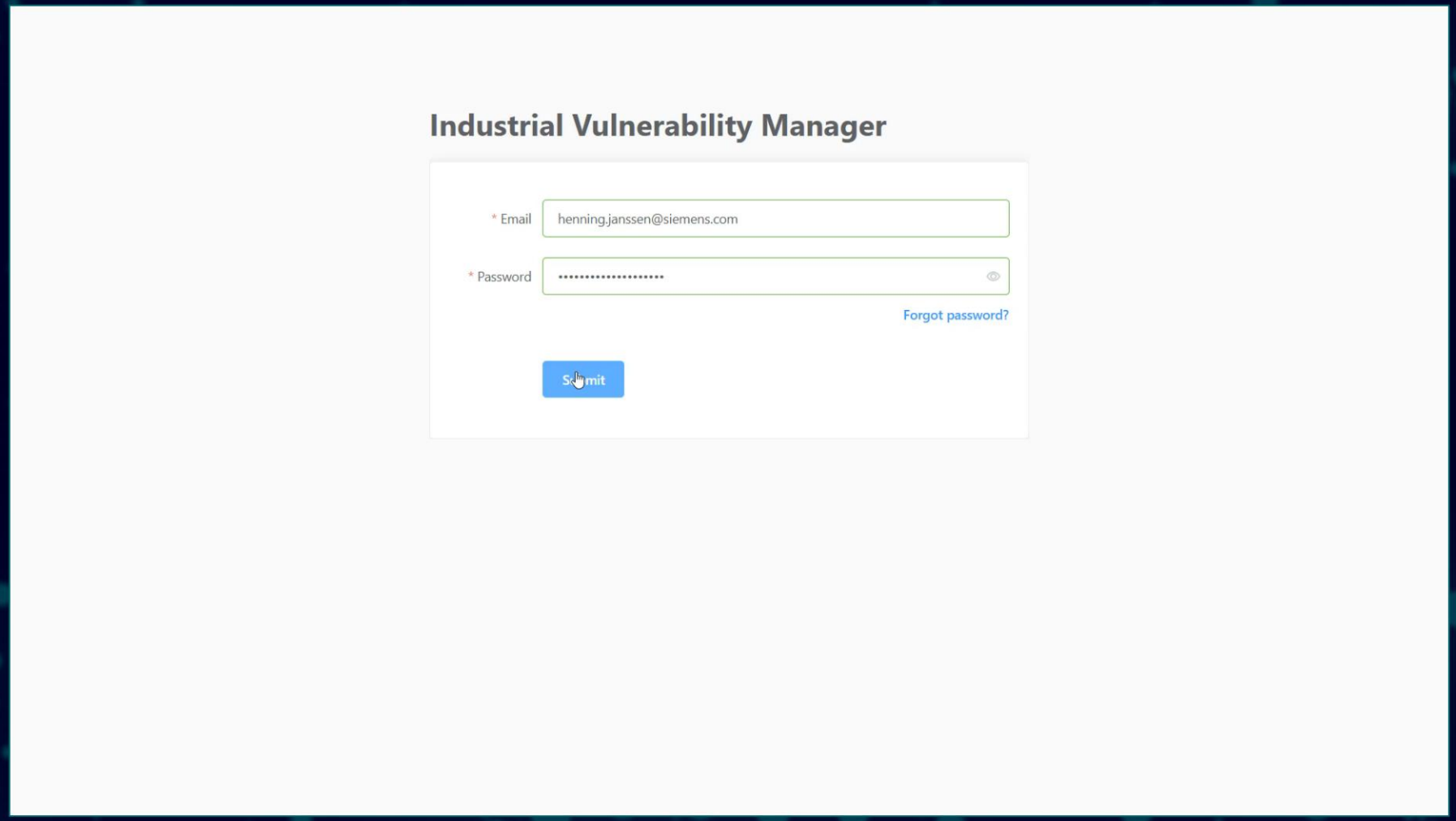
SIEMENS

Descripción general de la aplicación: versión corta



SIEMENS

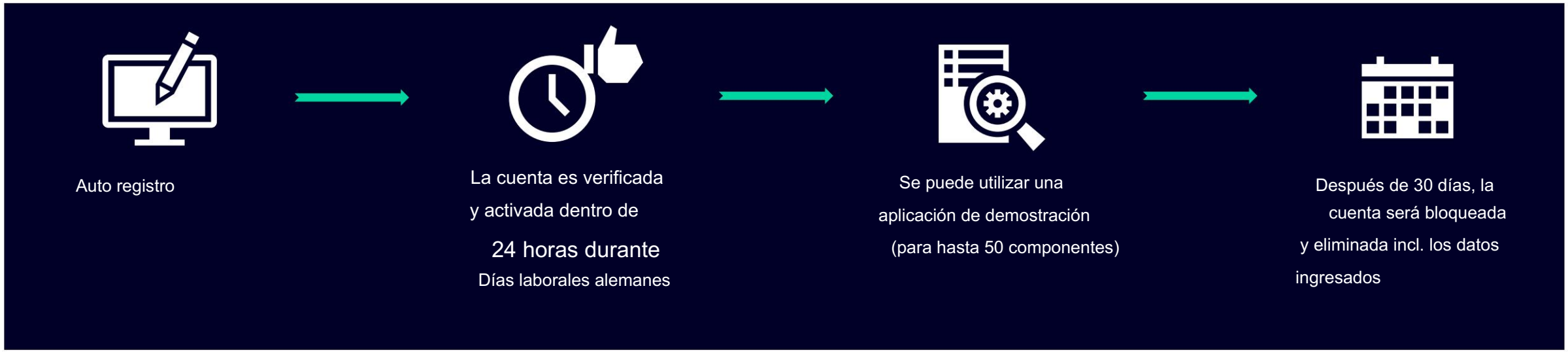
Descripción general de la aplicación: versión larga



SIEMENS

Portal de demostración: acceso, flujo de trabajo, restricciones

Se puede acceder al portal de demostración a través del siguiente enlace: siemens.com/ivm-demo



Restricciones: • El portal se puede utilizar para probar el servicio hasta por 30 días y hasta 50 componentes. No se pueden agregar nuevos componentes. • Como este es solo un portal de prueba, no garantizamos ningún nivel de servicio para la disponibilidad. • Sólo es posible registrarse una vez.

SIEMENS

Siemens como socio fiable para la seguridad industrial

Somos los expertos en automatización

Impulsamos la digitalización

Entendemos la seguridad industrial

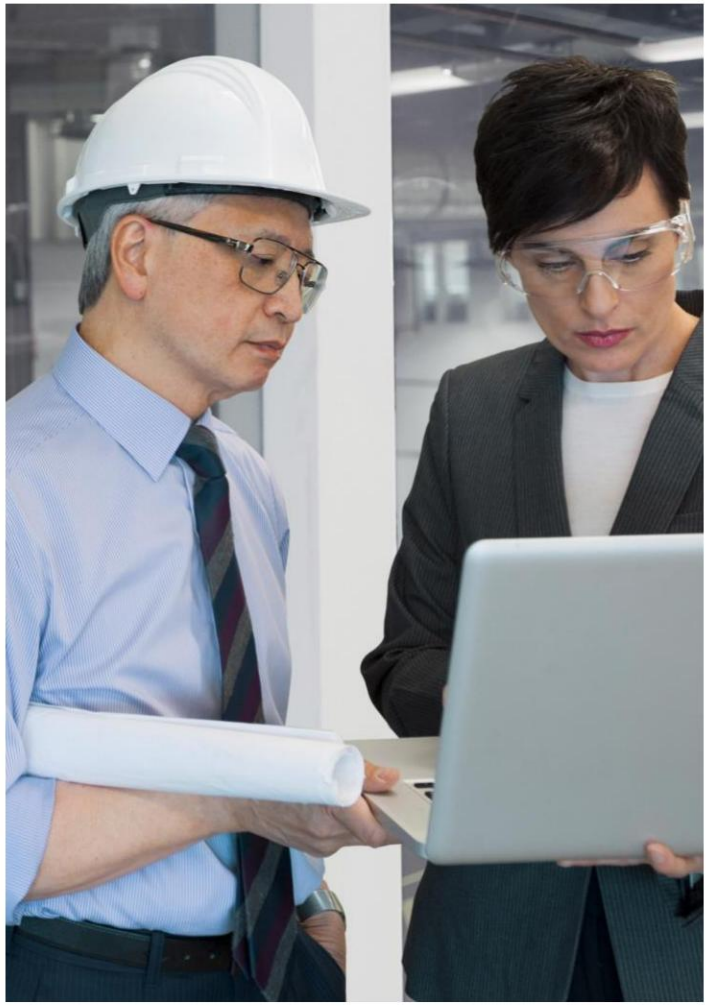
Tenemos conocimientos específicos de la industria.

Ofrecemos tecnología de punta y servicios integrales de una sola fuente

"We make sure that you can focus on your core business."

SIEMENS

¿Por qué elegir Industrial Vulnerability Manager?



Transparencia instantánea sobre vulnerabilidades y parches

Gestión proactiva de los riesgos cibernéticos

Evite el tiempo de inactividad y ahorre costos

SIEMENS

¡Háganos saber si hay algo en lo que podamos apoyarlo!

You want to find out more?

Póngase en contacto con el socio de Siemens

cerca de usted

Base de datos de contactos de Siemens

SIEMENS

Sujeto a cambios y errores. La información proporcionada en este documento solo contiene descripciones generales y/o características de rendimiento que pueden no siempre reflejar específicamente las descritas, o que pueden sufrir modificaciones en el curso del desarrollo posterior de los productos. Las características de rendimiento solicitadas son vinculantes solo cuando se acuerdan expresamente en el contrato celebrado.

SIEMENS

Informacion de seguridad

Siemens ofrece productos y soluciones con funciones de seguridad industrial que respaldan el funcionamiento seguro de plantas, sistemas, máquinas y redes.

Para proteger plantas, sistemas, máquinas y redes contra amenazas cibernéticas, es necesario implementar, y mantener continuamente, un concepto de seguridad industrial holístico y de última generación. Los productos y soluciones de Siemens constituyen un elemento de dicho concepto.

Los clientes son responsables de evitar el acceso no autorizado a sus plantas, sistemas, máquinas y redes. Dichos sistemas, máquinas y componentes solo deben conectarse a una red empresarial o a Internet si y en la medida en que dicha conexión sea necesaria y solo cuando se implementen las medidas de seguridad adecuadas (por ejemplo, firewalls y/o segmentación de la red).

Para obtener información adicional sobre las medidas de seguridad industrial que pueden implementarse, visite https://www.siemens.com/industrialsecurity

Los productos y soluciones de Siemens se someten a un desarrollo continuo para hacerlos más seguros. Siemens recomienda enfáticamente que las actualizaciones del producto se apliquen tan pronto como estén disponibles y que se utilicen las últimas versiones del producto. El uso de versiones de productos que ya no son compatibles y la falta de aplicación de las últimas actualizaciones puede aumentar la exposición del cliente a las ciberamenazas.

Para mantenerse informado sobre las actualizaciones de productos, suscríbase a la fuente RSS de Siemens Industrial Security en https://www.siemens.com/industrialsecurity

SIEMENS