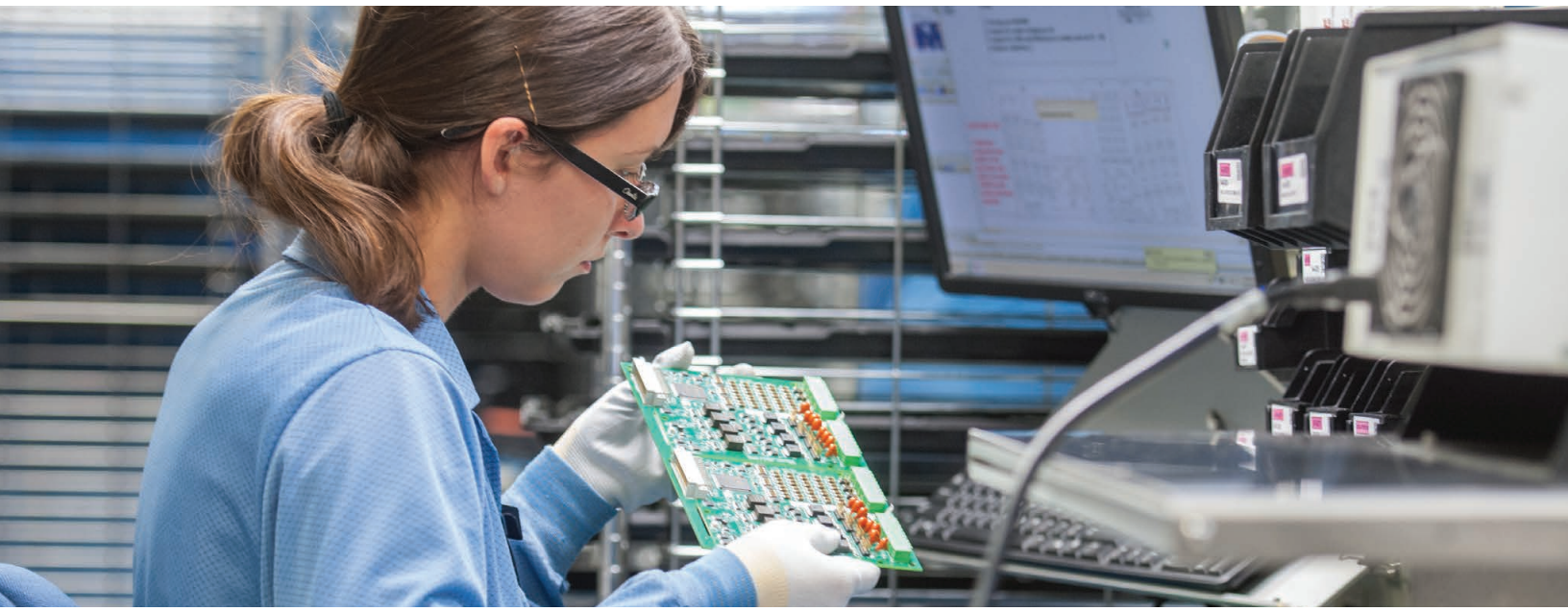
Aseguramos su cadena de suministro

Mejores prácticas de SEL



El desarrollo de planes de gestión de riesgos de seguridad cibernética en la cadena de suministro

La gestión de la cadena de suministro es un componente esencial de un programa de seguridad cibernética completo. La interconexión y la complejidad de las cadenas de suministro hacen que sea cada vez más importante la tarea de evaluar sistemáticamente los riesgos, pero este es un desafío difícil. En SEL, hemos hecho de la seguridad (que incluye la seguridad de la cadena de suministro) una de las principales prioridades durante más de 30 años, y consideramos que el manejo de los riesgos de la cadena de suministro es fundamental para garantizar la calidad de nuestros productos. Esperamos que el hecho de compartir nuestros conocimientos y mejores prácticas en esta área acelere sus iniciativas de seguridad cibernética y cumplimiento con la norma CIP-013 de NERC. Este documento destaca los procesos que sigue SEL para garantizar una cadena de suministro segura y confiable para los productos que entregamos a los clientes en todo el mundo.

SEL

CIP-013-1 de NERC, "Seguridad cibernética—Gestión de riesgos de la cadena de suministro"

Objetivo:

"Mitigar los riesgos de seguridad cibernética para la operación confiable del sistema eléctrico a gran escala (BES) implementando controles de seguridad para la gestión de riesgos de la cadena de suministro de los sistemas cibernéticos de BES".

Fecha de entrada en vigor

1 de julio de 2020

Resumen de los requisitos

- Evaluación del riesgo de los productos o servicios de los proveedores (R1.1)
- Notificación de los incidentes identificados por el proveedor (R1.2.1)
- Coordinación de la respuesta a incidentes (R1.2.2)
- Notificación por parte del proveedor cuando no se necesita acceso remoto/en el sitio (R1.2.3)
- Divulgación por parte de los proveedores de las vulnerabilidades conocidas (R1.2.4)
- Verificación de la integridad y la autenticidad del software (R1.2.5)
- Coordinación de los controles para el acceso remoto (R1.2.6)

Cómo SEL garantiza una cadena de suministro segura y confiable

La cadena de suministro de SEL es global y compleja. Adoptamos una estrategia completa de cinco partes para la evaluación de los riesgos de nuestra cadena de suministro.

Parte 1: Construir redes de suministro de confianza

Sistema de calificación de proveedores

En SEL, usamos un sistema de calificación de proveedores que evalúa a cada proveedor según su precio, calidad, características, innovación, entrega y servicio. Para llegar a esta calificación, evaluamos los siguientes riesgos del proveedor:

- Plantas de manufactura
- Plazos de entrega de los materiales
- Solvencia financiera
- Metodologías de reabastecimiento
- Tipo de tecnología
- Desempeño de entrega a tiempo

Conferencia anual de proveedores

Todos los años organizamos una conferencia para los proveedores que nos suministran componentes, equipos y servicios. Durante este evento, más de 200 empresas acuden a nuestra sede central en Pullman, Washington, donde compartimos nuestras necesidades técnicas y objetivos estratégicos para el año que sigue, e identificamos maneras de garantizar un suministro continuo de piezas de calidad.

Auditorías en las instalaciones

Construimos relaciones con nuestros proveedores al realizar auditorías continuas en sus instalaciones, a fin de verificar que sus procesos de calidad y seguridad cumplan con nuestros requisitos.

Estrategia organizativa para la selección y el monitoreo de proveedores

En SEL, la gestión de riesgos de la cadena de suministro depende de la colaboración entre las distintas funciones. El proceso comienza con la selección de proveedores, que es una tarea compartida entre nuestros grupos de desarrollo de productos, calidad y compras. De manera similar, los distintos equipos hacen sus aportes respecto de la selección de componentes, el monitoreo continuo de proveedores y piezas, y las auditorías de proveedores en el sitio. Con esta estrategia, la gestión de riesgos es responsabilidad de todos.

Privacidad

No compartimos nuestras listas de materiales (BOM). Proporcionamos pronósticos por número de parte, sin relación con el producto. A fin de evitar revelar información sobre los productos y las partes de otros proveedores, nunca enviamos esquemas de diseño.

Los proveedores de nuestros proveedores

No es suficiente conocer a nuestros proveedores de primer nivel. Les pedimos a nuestros proveedores que identifiquen sus proveedores de primer nivel, junto con los riesgos clave, las estrategias de mitigación y las metodologías de reabastecimiento.

Preferencia por proveedores nacionales

En la medida de lo posible, usamos materiales provenientes de Estados Unidos.

Calificación de proveedores de transporte y envío

A fin de ayudar a garantizar la entrega segura de nuestros productos a nuestros clientes, aplicamos los mismos procesos de calificación de proveedores a nuestros proveedores de transporte y envío.

Parte 2: Garantizar la integridad y la disponibilidad de los componentes

Proceso de calificación de los componentes

A fin de garantizar la integridad de nuestros productos, verificamos el desempeño de los componentes adquiridos en comparación con las especificaciones de los productos. Siempre que resulte posible, obtenemos los componentes directamente del fabricante o sus distribuidores oficiales. En casos en los que deben obtenerse componentes de distribuidores independientes, usamos diversos métodos para detectar productos falsificados, que incluyen pruebas funcionales e inspecciones microscópicas, de rayos X, de fluorescencia con rayos X y de decapsulación.

Pruebas continuas

Realizamos pruebas continuas de nuestros productos en todo el proceso de fabricación. Si se encuentran variaciones en el desempeño, trabajamos para comprender la causa raíz de la discrepancia.

Minimización del impacto de las interrupciones

Trabajamos con los proveedores para garantizar que tanto ellos como nosotros mantengamos un inventario suficiente de partes especializadas y en riesgo. Siempre que resulta posible, nos aseguramos de que los componentes críticos puedan obtenerse de dos proveedores aprobados como mínimo.

Parte 3. Verificar la seguridad del software y el firmware

Código fuente

No compartimos código fuente ni datos esquemáticos. Desarrollamos la mayor parte del software de manera interna, lo que proporciona una ventaja en el control de la calidad, con la posibilidad de implementar mejoras rápidas. Si usamos componentes de terceros en nuestro firmware, adquirimos el código fuente. El acceso al código se permite solo para los ingenieros de investigación y desarrollo de SEL que trabajen en esos proyectos.

Pruebas internas

Contamos con un proceso robusto que incluye revisiones por parte de desarrolladores, y pruebas positivas y negativas. También usamos herramientas automatizadas para inspeccionar el código, a fin de identificar posibles problemas que los desarrolladores puedan haber pasado por alto. Todas las pruebas se llevan a cabo en instalaciones de SEL, por parte de empleados de SEL.

Firmas digitales y hashes de firmware de SEL

El software con firma digital le permite tener la certeza de que los archivos de software y firmware son auténticos (producidos por SEL) y que no se los ha alterado ni modificado. Los usuarios de Microsoft Windows pueden consultar y verificar firmas digitales para los productos de software de SEL mediante el Explorador de Windows. Los productos de hardware de SEL realizan una comprobación transparente de la integridad de los archivos de firmware durante el proceso de actualización de firmware, utilizando datos adicionales integrados en el firmware. Si no hay coincidencia, el dispositivo de SEL rechazará el archivo de firmware e interrumpirá el proceso de actualización. Proporcionamos los hashes de firmware como una herramienta adicional para comprobar la integridad de los archivos de firmware de SEL.

Parte 4: Proteger las operaciones y el acceso de control

Seguridad física y seguridad cibernética de SEL

Nuestra infraestructura interna de seguridad física y de la información está estructurada en capas y cumple con normas reconocidas internacionalmente. Esto garantiza que todos los dispositivos y servicios de SEL se entreguen de manera segura y que todos los datos confiados a SEL estén protegidos. También nos planteamos el desafío de ir más allá de las normas para aumentar la seguridad cibernética. Por ejemplo, hemos implementado redes definidas por software en nuestra operación de fabricación, a fin de eliminar diversas vulnerabilidades de seguridad de red frecuentes.

Nuestro Sistema de Gestión de Calidad tiene certificación según la norma ISO 9001, y nuestros procesos de manufactura cumplen con la norma de mano de obra IPC-A-610 Clase 3 para productos que requieren alta fiabilidad, como los que se usan en sistemas de soporte vital y aeroespaciales.

Todos los empleados de SEL se someten a un exhaustivo proceso de averiguación de historial y antecedentes penales antes de la contratación. El acceso a los edificios de SEL y los espacios confidenciales dentro de ellos se protegen mediante controles de acceso configurables, CCTV y otros sistemas de monitoreo. Los equipos y sistemas de información de SEL se protegen de las amenazas físicas y ambientales. Los sistemas de seguridad de SEL se monitorean y cuentan con el soporte de nuestro Centro de Operaciones de Seguridad, atendido las 24 horas del día, los 7 días de la semana, por empleados de SEL. Nuestros equipos analizan diversas fuentes de amenazas y otras fuentes de inteligencia públicas y privadas a fin de detectar y analizar posibles amenazas.

Necesidad de conocimiento

La cultura de seguridad de SEL se basa en los conceptos de privilegio mínimo, necesidad de conocimiento y defensa en profundidad. Compartimentalizamos los proyectos y limitamos el acceso a la información de manera interna a las personas que necesitan acceso.

Protección de la información de los clientes

Protegemos la información del cliente en nuestros sistemas de negocios y durante las actividades de soporte. Esto incluye la protección de la información de los clientes en los productos que se envían para reparación. Cuando identificamos un incidente que afecta la información de los clientes, notificamos a los clientes y ofrecemos todo nuestro soporte para la respuesta a incidentes.

Acceso remoto

Cuando se necesita acceso remoto para el soporte técnico, usamos un sistema de seguimiento y notificación a fin de documentar y coordinar el control de ese acceso.

Parte 5: Monitorear la calidad y las vulnerabilidades de seguridad

Determinación de la causa raíz

La oferta de una garantía de diez años proporciona un incentivo para que nuestros clientes nos envíen los productos cuando fallen. Luego podemos examinar esos productos y encontrar la causa raíz de los defectos, lo que a su vez nos ayuda a identificar problemas en nuestro proceso de diseño o con nuestros proveedores, y mejorar nuestros diseños de productos. Proporcionamos una garantía de diez años sin costo para todos los productos.

Seguimiento de productos a nivel de los componentes

Mantenemos un registro detallado de todos los productos que fabricamos y los componentes integrados en ellos, a fin de saber dónde están instalados nuestros productos y poder notificar a los clientes sobre posibles problemas de calidad o seguridad.

Boletines de servicio técnico

Cuando identificamos un posible problema con un producto, organizamos un equipo multidisciplinario de expertos en diseño de productos para analizar el problema. Si esto representa un riesgo para los clientes, informamos a los clientes afectados con un boletín de servicio. Los boletines de servicio incluyen una explicación del problema identificado, así como la causa raíz, el impacto, la tasa de defectos observada, los productos afectados por cliente, las medidas correctivas y las soluciones de mantenimiento recomendadas. Un boletín de servicio técnico permite al cliente tomar una decisión informada sobre cómo solucionar el problema. Distribuimos los boletines de servicio a los clientes tanto de manera directa como a través de nuestro personal de ventas.

Vulnerabilidades de servicio

Un boletín de servicio relacionado con una vulnerabilidad en productos afectados se clasifica como una "vulnerabilidad de seguridad". Nuestro equipo desarrolla pasos correctivos sugeridos para cualquier vulnerabilidad de seguridad de productos antes de la divulgación, y los incluye en el boletín de servicio asociado.

Participación en la industria

Participamos en diversas iniciativas y actividades de desarrollo de normas dirigidas por el gobierno a fin de estar al tanto de las mejores prácticas actuales de otros, hacer aportes a las mejores prácticas de la industria y mantenernos actualizados respecto de las exigencias cambiantes que enfrentan nuestros clientes. De manera similar, hacemos aportes y usamos documentos de orientación, como el marco de seguridad cibernética del NIST, a fin de mejorar nuestros propios procesos y controles, y ayudar a dar forma a las mejores prácticas de la industria.

El compromiso continuo de SEL

En SEL, nuestra política de calidad es "comprender, crear y simplificar". Esto representa nuestra dedicación incansable al objetivo de comprender las oportunidades y los desafíos, crear soluciones innovadoras y garantizar que esas soluciones sean sencillas, robustas y seguras. Los ejecutivos de SEL incluyen la gestión de riesgos de seguridad como parte de sus actividades diarias. Se mantienen informados sobre las amenazas emergentes para la cadena de suministro y las operaciones de SEL, y hacen los ajustes correspondientes.

SEL SCHWEITZER ENGINEERING LABORATORIES

Haciendo la energía eléctrica más segura, más confiable y más económica
+1.509.332.1890 | info@selinc.com | selinc.com

20211130

WORLDWIDE 10 years WARRANTY