FIREEYE™

FICHA TÉCNICA

Diagnóstico de fallos del sistema de control industrial

Comprender las vulnerabilidades expuestas del sistema de control industrial y establecer un plan viable para reducir los riesgos de ciberseguridad del sistema

VENTAJAS PRINCIPALES

- El método de la evaluación mínimamente invasiva evita los riesgos operativos que se asocian con los agentes de software y el análisis de la red en un entorno de ICS
- Identifica las vulnerabilidades, los errores de configuración y los fallos de seguridad del ICS
- Análisis humano de las actividades anómalas y sospechosas, que los expertos en ICS llevan a cabo mediante la utilización de herramientas especiales para el ICS
- Recomendaciones viables que se priorizan, personalizan y colocan en el contexto apropiado en función de riesgos y preocupaciones que son específicos para su proceso industrial

Mandiant es asesor de confianza de organizaciones del mundo entero con más de 10 años de experiencia en la lucha contra amenazas avanzadas en todo el planeta. Ayudamos a las organizaciones en los momentos más difíciles que siguen a la identificación de vulneraciones de seguridad y contribuimos preventivamente a que mejoren su capacidad de detección, respuesta y contención. El diagnóstico de fallos del sistema de control industrial (*Industrial Control Systems*, ICS) combina el conocimiento que Mandiant tiene con respecto a los perpetradores y la experiencia de responder a los incidentes de seguridad mediante la experiencia de dominio de nuestros consultores en ICS a fin de brindar una evaluación completa del nivel de segmentación, protección y supervisión real de su red de ICS.

Descripción general

El diagnóstico de fallos del ICS es una evaluación mínimamente invasiva del nivel de seguridad cibernética general de una instalación industrial. Esta evaluación se diseñó específicamente para satisfacer las necesidades de las organizaciones a las que les preocupa el riesgo operativo asociado con los agentes basados en software, el análisis de la red u otras técnicas de evaluación de seguridad más agresivas. El diagnóstico de fallos del ICS combina una revisión de la arquitectura del ICS basada en talleres con un análisis técnico detallado de la configuración del firewall y tráfico de red activo del ICS.

Los especialistas en ICS de Mandiant son expertos en tecnología operativa (*Operational Technology*, OT) y trabajan directamente con los ingenieros responsables de la misma a fin de adaptar las mejores prácticas de ciberseguridad de forma apropiada con respecto al entorno del ICS. También trabajamos con los líderes en seguridad de TI para proporcionarles el conocimiento de dominio y la credibilidad que se requieren para que los equipos de OT participen de discusiones de ciberseguridad eficaces.

Nuestro método

Analizar los riesgos de la arquitectura y modelado de amenazas

Documentar la comprensión actual de la red

- Revisar los diagramas de la arquitectura, el flujo de datos y los diseños existentes.
- Realizar un inventario y evaluar los protocolos de comunicaciones industriales que se utilizan.
- Revisar cualquier norma de seguridad existente para detectar implementaciones de hardware y software.

LO QUE OBTIENE

- **Diagrama de modelos de amenazas:** diagrama representativo de su ICS que define los distintos vectores de amenazas que pueden utilizar los agresores para interrumpir o impedir sus operaciones, y un análisis de cómo establecer prioridades entre los controles de seguridad apropiados.
- **Informe del diagnóstico de fallos de seguridad del ICS:** informe técnico detallado que describe las observaciones de Mandiant, como vulnerabilidades de seguridad, errores de configuración, puntos débiles de la arquitectura, tráfico de red sospechoso o actividades anómalas, junto con recomendaciones viables y priorizadas para cada observación y un resumen de los aspectos principales resultantes de la evaluación.
- **Presentación de recomendaciones estratégicas y técnicas:** resumen de nuestras observaciones y recomendaciones dirigidas al personal técnico y directivo interesado.

Desarrollo de modelos de amenazas

- Tomar los diagramas de arquitectura resultantes y generar la base para un modelo de amenazas durante un taller interactivo con el personal de TI y operaciones/ingeniería del cliente.
- Generar presentaciones visuales de los ataques probables al sistema de control, en función de nuestro amplio conocimiento de las tácticas de los agresores del mundo real.
- Brindar ayuda para la priorización de la implementación del control de seguridad para el ICS, identificar los vectores del agresor que presentan el mayor nivel de riesgo y exposición.

Priorizar los controles

- Facilitar un análisis con su equipo técnico a fin de identificar los controles de seguridad que aborden de manera apropiada las amenazas que se identificaron.
- Brindar una priorización basada en valores de los controles potenciales, tomando en cuenta factores como reducción de riesgos, costo/esfuerzo y velocidad de la implementación.

Análisis de datos técnicos

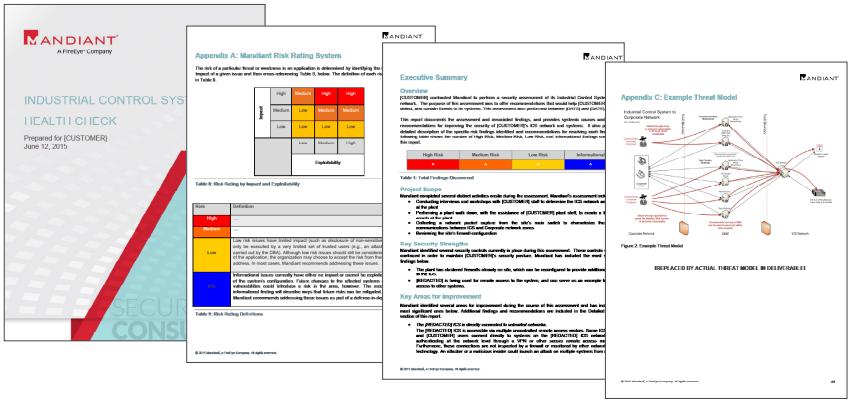
Revisión de la segmentación de la red: Analizamos un archivo de captura de paquetes de red a partir de un dispositivo FireEye PX que se implementa en la red del ICS del cliente. La captura de paquetes se revisa para detectar riesgos de seguridad como los siguientes:

- Conectividad imprevista desde el ICS a Internet o la red empresarial
- Dispositivos con doble vinculación
- Protocolos del ICS que atraviesan el firewall del ICS
- Conexiones anómalas entre computadoras

Revisión de la configuración de dispositivos de seguridad: Revisamos la eficacia de la configuración y los conjuntos de reglas de los dispositivos de seguridad de la red, como los firewalls. Por ejemplo:

- El tráfico entrante a la red del ICS siempre debe canalizarse a través de una DMZ.
- Las redes del ICS no deben contar con acceso directo, y tampoco deben estar conectadas directamente, a Internet.

Muestra del informe



Para obtener más información sobre FireEye, visite: **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Acerca de FireEye, Inc.

FireEye es una empresa de seguridad basada en información. FireEye, que funciona como una extensión escalable y flexible de las operaciones de seguridad del cliente, ofrece una sola plataforma que combina tecnologías innovadoras de seguridad, información sobre amenazas a nivel de nación-estado y los servicios de consultoría de Mandiant® de fama mundial. Gracias a este método, FireEye elimina la complejidad y la carga de la ciberseguridad para las organizaciones que desean estar preparadas y responder ante los ataques cibernéticos, además de prevenirlos.