FICHA TÉCNICA

MANDIANT®
A FireEye® Company

Verificação das condições de sistemas de controle industrial

Compreenda que o seu sistema de controle industrial está exposto a vulnerabilidades e estabeleça um plano viável para reduzir o risco de segurança cibernética do seu sistema

PRINCIPAIS VANTAGENS

- Abordagem de avaliação minimamente invasiva, que evita os riscos operacionais associados a agentes de software e varredura de rede em um ambiente ICS
- Identificação de vulnerabilidades, má configuração e falhas na segurança de ICS
- Análise humana de atividade anômala ou suspeita, realizada por especialistas em ICS utilizando ferramentas adequadas para ICS
- Recomendações decisivas priorizadas, personalizadas e colocadas no devido contexto, com base nos riscos e preocupações específicos para o seu processo industrial

FireEye

A Mandiant é uma consultora confiável para organizações globais, com mais de dez anos de experiência lidando com agentes de ameaças avançadas do mundo todo. Oferecemos suporte para as organizações nos momentos mais críticos, após a identificação de uma violação de segurança, e as ajudamos proativamente a melhorar suas capacidades de detecção, resposta e contenção. A verificação das condições de sistemas de controle industrial (ICS, Industrial Control Systems) combina o conhecimento da Mandiant sobre perpetradores de ameaças e sua experiência em responder a incidentes de segurança com o conhecimento sobre domínios de nossos consultores de ICS para oferecer uma avaliação detalhada do quão bem segmentada, protegida e monitorada está a sua rede ICS na prática.

Visão geral

A verificação das condições de ICS é uma avaliação minimamente invasiva da postura de segurança cibernética geral de uma instalação industrial. Essa avaliação é realizada especificamente de maneira a satisfazer as necessidades de organizações preocupadas com o risco operacional associado a agentes com base em software, varredura de rede ou outras técnicas de avaliação de segurança mais agressivas. A verificação das condições de ICS combina um exame da arquitetura de ICS baseado em workshop com uma análise técnica detalhada das configurações de firewall e tráfego de rede de ICS em tempo real.

Os especialistas em ICS da Mandiant são versados em tecnologia operacional (TO) e trabalham diretamente com os engenheiros responsáveis pela TO para adaptar devidamente as melhores práticas de segurança cibernética ao ambiente de ICS. Também trabalhamos com os líderes de segurança de TI para equipá-los com o conhecimento sobre domínios e a credibilidade necessários para que possam interagir com suas equipes de TO em discussões produtivas sobre segurança cibernética.

Nossa abordagem

Análise de riscos à arquitetura e modelagem de ameaças

Documente o conhecimento atual sobre a rede

- Examine os projetos, fluxogramas e diagramas de arquitetura existentes.
- Faça inventários e avaliações dos protocolos de comunicações industriais utilizados.
- Examine quaisquer padrões de segurança existentes referentes a desenvolvimento de hardware e software.

O QUE VOCÊ RECEBE

- **Diagrama do modelo de ameaças:** um diagrama representativo do seu ICS que mapeia os diversos vetores de ameaça que podem ser utilizados por atacantes para interromper ou prejudicar as suas operações e uma discussão sobre como priorizar os controles de segurança apropriados.
- **Relatório de verificação das condições do ICS:** um relatório técnico detalhado que descreve as observações da Mandiant, incluindo quaisquer vulnerabilidades de segurança, más configurações, pontos fracos na arquitetura, tráfego de rede suspeito ou atividade anômala com recomendações técnicas decisivas e priorizadas para cada observação, juntamente com um resumo dos principais temas levantados pela avaliação.
- **Apresentação de recomendações estratégicas e técnicas:** um resumo de nossas observações e recomendações para as partes interessadas dos níveis técnico e administrativo.

Desenvolva um modelo de ameaça

- Reúna os diagramas de arquitetura resultantes e crie a base para um modelo de ameaça durante um workshop interativo com as equipes de operações/engenharia e TI do cliente.
- Construa uma representação visual dos ataques possíveis contra o sistema de controle, com base em nosso amplo conhecimento sobre táticas de atacantes da vida real.
- Ajude a priorizar a implementação do controle de segurança do ICS, identificando os vetores de ataque que representem mais exposição e risco.

Priorize os controles

- Propicie uma discussão com a sua equipe técnica para identificar controles de segurança que lidem de maneira apropriada com as ameaças identificadas.
- Ofereça uma priorização dos controles potenciais com base em valor, considerando fatores como redução de risco, custo/trabalho e velocidade de implementação.

Análise técnica dos dados

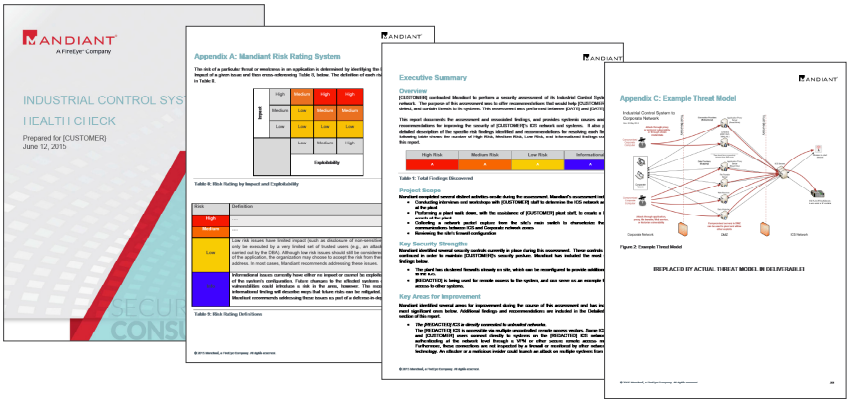
Revisão da segmentação da rede: Analisamos um arquivo de captura de pacotes de rede obtido de um dispositivo FireEye PX distribuído na rede ICS do cliente. O pacote de captura é examinado quanto a riscos de segurança, como:

- Conectividade indevida do ICS com a Internet ou com uma rede de negócios
- Dispositivos com mais de uma interface de rede
- Protocolos de ICS atravessando o firewall de ICS
- Conexões anômalas entre computadores

Revisão da configuração do dispositivo de segurança: Examinamos a eficácia da configuração e dos conjuntos de regras dos dispositivos de segurança de rede, como firewalls. Por exemplo:

- O tráfego recebido na rede ICS deve ser sempre roteado através de uma DMZ.
- As redes ICS não devem acessar diretamente e nunca devem ser conectadas diretamente à Internet.

Exemplo de relatório



Para saber mais sobre a FireEye, visite: **www.FireEye.com**

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

Sobre a FireEye, Inc.

A FireEye é a empresa líder em segurança orientada por inteligência. Atuando harmoniosamente como extensão expansível das operações de segurança dos clientes, a FireEye oferece uma plataforma única que mescla tecnologias de segurança inovadoras, inteligência sobre ameaças em nível de país e a consultoria mundialmente reconhecida da Mandiant®. Com essa abordagem, a FireEye elimina a complexidade e o fardo da segurança cibernética para organizações empenhadas em se preparar, prevenir e responder a ataques cibernéticos. A FireEye tem mais de 6.600 clientes em 67 países, incluindo mais de 45 por cento das empresas da Forbes Global 2000.