FIREEYE™

FICHE PRODUIT

Diagnostic d'intégrité des systèmes de contrôle industriel

Identifiez les failles de cybersécurité de votre système de contrôle industriel et élaborez un plan réalisable pour réduire les risques

PRINCIPAUX AVANTAGES

- Méthodologie d'audit peu invasive permettant d'éviter le risque opérationnel associé à des agents logiciels et des analyses réseau dans un environnement ICS
- Identification des failles de sécurité, erreurs de configuration et irrégularités des systèmes ICS
- Analyse des activités anormales et suspectes réalisée par des experts en systèmes ICS à l'aide d'outils conçus spécifiquement pour ces systèmes
- Recommandations pragmatiques personnalisées, priorisées et contextualisées en fonction des risques et préoccupations propres à vos process industriels

Fort de plus de dix ans d'expérience dans la lutte contre les auteurs d'attaques avancées, Mandiant s'impose comme le conseiller de confiance de nombreuses entreprises à travers le monde. Nous les accompagnons pendant la période critique qui suit l'identification d'une compromission, tout en les aidant en amont à renforcer leurs dispositifs de détection, de réponse et de confinement des attaques. Le service Diagnostic d'intégrité des systèmes de contrôle industriel (ICS) de Mandiant s'appuie à la fois sur notre connaissance des cyberpirates, notre expérience en matière de réponse à incident et les compétences pointues de nos consultants spécialisés en systèmes ICS. Nous sommes ainsi parfaitement armés pour évaluer en profondeur votre efficacité réelle dans la segmentation, la protection et la surveillance de votre réseau ICS.

Présentation

Le diagnostic d'intégrité des systèmes de contrôle industriel consiste en un audit peu invasif de la sécurité globale d'une infrastructure industrielle. Il est spécialement conçu pour répondre aux besoins des entreprises soucieuses du risque opérationnel associé à des agents logiciels, analyses réseau et autres techniques de diagnostic plus perturbatrices. Le diagnostic d'intégrité des systèmes de contrôle industriel s'articule autour d'un audit de l'architecture ICS dans le cadre d'un atelier interactif, comprenant une analyse technique détaillée des configurations pare-feu et du trafic réseau en temps réel du système ICS.

Les consultants Mandiant spécialisés en systèmes ICS sont versés dans le langage des technologies opérationnelles (TO) et collaborent directement avec les ingénieurs en charge pour adapter les meilleures pratiques de cybersécurité à l'environnement ICS. Nous aidons également les responsables de la sécurité informatique (RSSI) à acquérir les connaissances et la maîtrise nécessaires à l'ouverture d'un dialogue efficace avec les équipes TO sur les questions de cybersécurité.

Notre approche

Analyse des risques inhérents à l'architecture et modélisation des menaces

Documentation du réseau existant

- Analyse des diagrammes, du flux de données et de la conception de l'architecture actuelle
- Inventaire et évaluation des protocoles de communication industrielle utilisés
- Examen des normes de sécurité en place pour le déploiement matériel et logiciel

PRESTATIONS ET LIVRABLES

- **Diagramme du modèle de menaces –**
  Un schéma représentatif de votre système de contrôle industriel qui cartographie les différents vecteurs de menaces susceptibles de perturber ou ralentir vos opérations, et propose une liste des contrôles de sécurité à mettre en place en fonction des priorités.

- **Diagnostic d'intégrité des systèmes de contrôle industriel –**
  Un rapport technique détaillant les observations de Mandiant (failles de sécurité, erreurs de configuration, faiblesses architecturales, trafic réseau suspect ou activités anormales, etc.), chaque observation étant assortie de recommandations techniques concrètes, classées par ordre de priorité. Il s'accompagne d'une synthèse des principales conclusions du diagnostic.

- **Présentation des recommandations stratégiques et techniques –**
  Un résumé de nos observations et recommandations aux principaux intervenants des équipes technique et de direction.

Modélisation des menaces

- Utilisation des diagrammes d'architecture réalisés pour établir un modèle de menaces, au cours d'un atelier interactif avec les équipes informatique, opérationnelle et technique du client
- Élaboration d'une représentation visuelle des attaques potentielles contre le système de contrôle, fondée sur notre connaissance approfondie des tactiques d'attaque sur le terrain
- Définition commune des priorités dans les contrôles de sécurité à mettre en place pour le système ICS, grâce à l'identification des vecteurs d'attaque en fonction de leur probabilité et de leur niveau de risque

Priorisation des contrôles

- Dialogue avec votre équipe technique pour identifier les contrôles de sécurité capables de répondre efficacement aux menaces identifiées
- Priorisation des contrôles potentiels en fonction de leur valeur ajoutée, calculée sur la base de facteurs tels que la réduction des risques, la rapidité d'implémentation et le rapport coût/effort

Analyse des données techniques

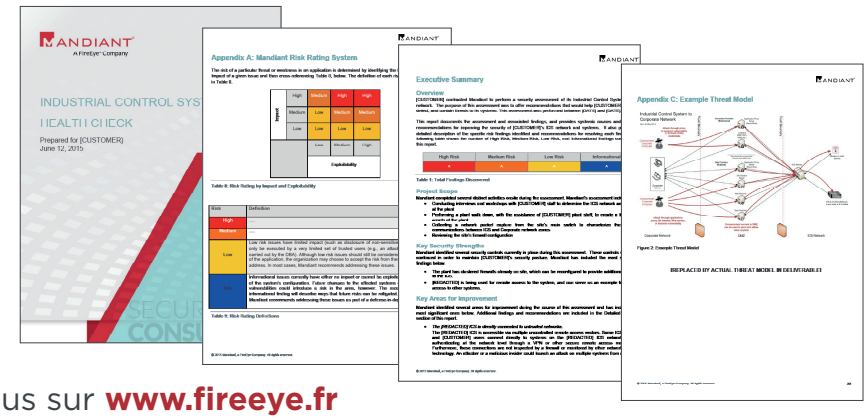
Analyse de la segmentation réseau – Nous analysons un fichier de capture de paquets réseau fourni par une solution FireEye PX déployée sur le réseau ICS du client. La capture de paquets est analysée afin d'identifier les risques tels que :

- Connexion non intentionnelle du système ICS à Internet ou au réseau de l'entreprise
- Équipements hébergés sur deux réseaux
- Protocoles ICS traversant le pare-feu ICS
- Connexions anormales d'ordinateur à ordinateur

Analyse de la configuration des équipements de sécurité – Nous analysons l'efficacité de la configuration et des règles des dispositifs de sécurité réseau tels que les pare-feux. Par exemple :

- Le trafic entrant du réseau ICS doit toujours passer par une zone démilitarisée (DMZ).
- Les réseaux ICS ne doivent pas être autorisés à accéder directement à Internet, tout comme ils ne doivent jamais y être connectés directement.

Exemple de rapport



Pour en savoir plus, rendez-vous sur **www.fireeye.fr**

FireEye, France
Nextdoor Cœur Défense
110 Esplanade du Général de Gaulle
92931 Paris La Défense Cedex 92974 +33 1 70 61 27 26
france@FireEye.com | www.FireEye.fr
FireEye, Inc.
601 McCarthy Blvd.
Milpitas, CA 95035
+1 408 321 6300 | info@FireEye.com

À propos de FireEye, Inc.

FireEye est spécialisé dans la cybersécurité axée sur la Threat Intelligence. Prolongement naturel et évolutif des opérations de sécurité des clients, la plateforme unique de FireEye combine des technologies de sécurité innovantes, des services de CTI d'envergure internationale et les services réputés de Mandiant® Consulting. FireEye simplifie ainsi la cybersécurité et son administration, devenant un allié précieux des entreprises confrontées au casse-tête que représentent la prévention et la neutralisation des cyberattaques.