FICHE PRODUIT

MANDIANT®
A FireEye® Company

Bilan de sécurité des équipements embarqués

AVANTAGES

- Décelez les risques sur vos produits avant leur mise sur le marché
- Préservez la sécurité de vos clients et votre réputation
- Sensibilisez vos ingénieurs à l'importance de la sécurité

La différence Mandiant

Mandiant, une entreprise FireEye, possède plus de 14 ans d'expérience de première ligne dans le domaine de la cybersécurité et de la Threat Intelligence. Nos experts de la réponse à incident traitent les compromissions de sécurité les plus complexes et les plus médiatisées du monde. Ils possèdent une connaissance approfondie des acteurs établis et émergents, ainsi que de leurs modes opératoires en constante évolution.

Présentation

Notre bilan de sécurité des équipements embarqués (Embedded Device Assessment) mesure les forces et faiblesses de l'appareil lui-même, mais aussi de son processus de développement. Comprendre les défauts systémiques dans vos processus permet d'améliorer la sécurité de vos équipements de A à Z.

Le bilan fait le point sur des aspects de sécurité spécifiques de l'appareil en fonction du stade de son cycle de vie, de son utilisation prévue et des mesures de sécurité existantes. Les experts Mandiant sont à vos côtés pour identifier et réaliser ensemble vos objectifs de sécurité.

Objectifs de sécurité tout au long du cycle de vie d'un équipement

	Étapes du cycle de vie d'un équipement			
	Conception et implémentation	**Preuve de concept (POC)**	**Disponibilité sur le marché**	**Fin de vie**
Problématiques	• Architecture du processeur • Mode de distribution du noyau • Protection anti-altération suffisamment forte • Outils disponibles	• Validation des choix de conception • Adéquation des fonctionnalités de sécurité • Utilisation d'outils, de bibliothèques et de logiciels à jour • Pratiques de développement sécurisées	• Sécurité du produit pour la protection et la confidentialité du consommateur • Validation des arguments de sécurité	• Sécurité robuste pendant toute la durée du contrat de support
Exemples d'objectifs de sécurité	• Validation des décisions avant d'entamer la production coûteuse du prototype	• Évaluation des pratiques de développement • Identification des risques associés aux fonctionnalités de l'équipement • Identification des risques avant production pour réduire les coûts	• Réplication d'actes malveillants visant à exploiter le produit	• Mise en place de tests de sécurité en continu

FireEye®

Options du service

Le bilan peut se dérouler de deux manières :

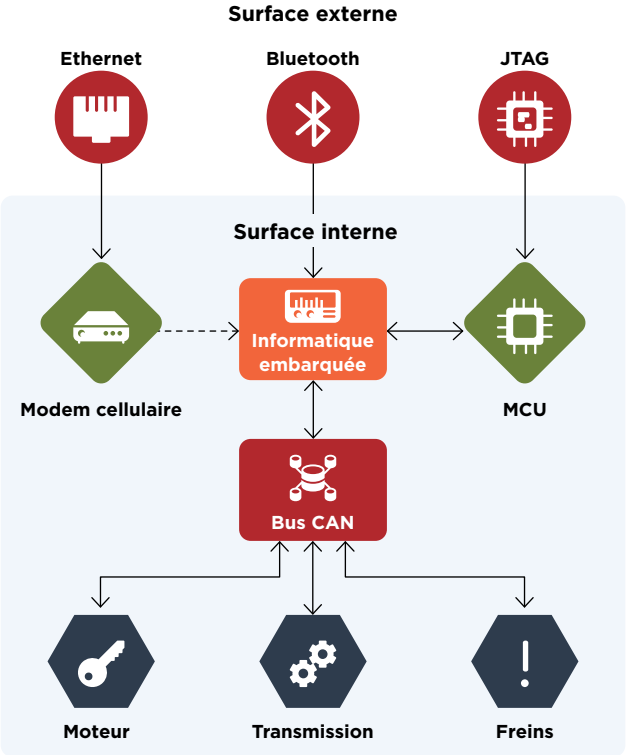
- Test en mode « black box » où les consultants Mandiant ne reçoivent aucune information préalable concernant votre équipement
- Test en mode « white box » où vos équipes et nos experts discutent ensemble de la conception de votre appareil pendant la mission

À l'issue du bilan, nos consultants vous livrent des recommandations documentées pour renforcer la sécurité de l'équipement testé.

Le principe

Avant de commencer le bilan de sécurité, les experts Mandiant procèdent à une modélisation des menaces sur le système de déploiement type d'un équipement spécifique. L'objectif : déterminer les risques réels liés aux vulnérabilités détectées.

Cette modélisation permet d'identifier tous les points d'entrée externes pour déterminer l'accessibilité de chaque interface d'entrée et le niveau de connectivité interne. Elle recense également les vecteurs d'attaque et détaille l'impact de compromissions potentielles.



Exemple de modélisation des menaces sur une voiture connectée.

Une fois la modélisation effectuée, les experts Mandiant analysent chaque interface d'entrée et de sortie identifiée pour mesurer les niveaux potentiels d'interactivité et la surface d'attaque externe. Les interfaces recensées peuvent faciliter l'accès à différents protocoles :

- Standards réseau courants de type Ethernet ou sans fil IEEE 802.11
- Standards réseau personnels de type Bluetooth/ Bluetooth Low Energy ou IEEE 802.15.4 et stacks applicatives associées telles que ZigBee ou Z-Wave
- Protocoles périphériques de type USB, RS-232, RS-423, SPI ou I^2C
- Interfaces de programmation et de débogage telles que JTAG ou ICSP

Les experts Mandiant tentent de collecter des informations sur la configuration et les programmes sous-jacents de l'équipement. Pour ce faire, ils en extraient et dissèquent divers éléments : firmware, noyau et toute donnée stockée dans la mémoire non volatile. Les informations ainsi obtenues peuvent permettre de prendre le contrôle de l'appareil et d'installer des backdoors, de compromettre l'efficacité de son chiffrement ou encore d'exploiter son statut de confiance au sein d'un système plus vaste.

En outre, les objets connectés (IoT) s'accompagnent généralement d'une application mobile ou de services web. Nos consultants peuvent détecter les faiblesses de ces services associés, telles que des mises à jour non sécurisées du firmware. Ils exploitent alors ces vulnérabilités pour étendre leur emprise sur l'équipement testé.

Une fois l'appareil compromis, les experts Mandiant mettent au point des outils pour démontrer l'impact des vulnérabilités identifiées. Par exemple, ils peuvent compiler des outils d'accès via un backdoor, conçus spécialement pour l'architecture de cet équipement.

Livrables

- Document de synthèse destiné aux managers et équipes dirigeantes
- Documentation technique présentant une procédure détaillée pour vous permettre d'établir une reconstitution
- Bilan-risque factuel pour vous aider à déterminer la pertinence de l'analyse au regard de votre équipement
- Recommandations de long terme pour améliorer la sécurité de votre appareil tout au long de son cycle de vie

Pour en savoir plus sur Mandiant, rendez-vous sur : **www.fireeye.fr/services.html**

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

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 Cyber Threat Intelligence 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. FireEye compte plus de 6 600 clients dans 67 pays, dont plus de 45 % figurent au classement Forbes Global 2000.

FireEye