FICHE PRODUIT

MANDIANT®
A FireEye® Company

Cyber Defense Center Development

Boostez la résilience de votre dispositif de sécurité

AVANTAGES

- **Amélioration du dispositif de défense :** Identifiez et comblez les failles dans vos capacités de surveillance et de réponse afin de vous protéger contre les menaces les plus avancées.
- **Mobilisation interne autour des améliorations de sécurité préconisées :** Améliorez votre collaboration et vos communications en interne à travers un meilleur partage des connaissances et une priorisation des améliorations à apporter.
- **Réduction de l'impact des incidents de sécurité :** Améliorez vos capacités de détection et de réponse afin de réduire au maximum les cyber-risques.
- **Priorisation des budgets et des ressources :** Affectez vos ressources et budgets de sécurité à une protection et des réponses plus efficaces.

La différence Mandiant

Depuis 2004, FireEye Mandiant agit en première ligne sur le front de la cybersécurité et de la Cyber Threat Intelligence (CTI). Nos experts de la réponse à incident ont opéré sur les violations de sécurité les plus complexes et les plus médiatisées que l'on ait connues. Ils possèdent une connaissance approfondie des auteurs de menaces établis et émergents, ainsi que de leurs outils, tactiques et procédures en constante évolution.

Présentation

Le service Cyber Defense Center Development est conçu pour aider les entreprises à concevoir un dispositif de sécurité capable de limiter les risques et réduire l'impact des violations de sécurité. Nos consultants proposent un modèle de sécurité directement aligné sur vos objectifs stratégiques, ainsi que des recommandations fondées sur notre expérience de terrain. Ils travaillent au contact de votre équipe pour inscrire votre dispositif de sécurité dans une stratégie de défense adaptative.

Notre approche

Les experts Mandiant ont une connaissance approfondie des tactiques, techniques et procédures (TTP) utilisées par les auteurs d'attaques avancées. Nos consultants collaboreront avec votre entreprise pour développer des technologies et processus à intégrer à votre dispositif de protection.

La détection et la neutralisation des attaques nécessitent la mise en place d'un dispositif de réponse à incident reposant sur des processus et procédures efficaces, des technologies et des compétences adaptées, ainsi que des indicateurs de fiabilité des mesures en place. Fort d'une expérience acquise sur les incidents de sécurité les plus critiques, Mandiant a développé une méthodologie basée sur les six grandes composantes d'un dispositif de sécurité résilient. Les axes de notre démarche :

- **Gouvernance —** Votre structure organisationnelle est-elle alignée sur les objectifs métiers et la mission de l'entreprise ?
- **Communication —** Avez-vous mis en place des processus favorisant un partage efficace des informations entre entités internes et externes ?
- **Visibilité —** Disposez-vous de technologies et processus visant à vous informer des activités survenant sur les systèmes et les réseaux ?
- **Cyber Threat Intelligence (CTI) —** Votre CTI parvient-elle à alimenter et améliorer vos processus de planification de la sécurité, de gestion des vulnérabilités et de réponse à incident ?
- **Indicateurs —** Vos indicateurs de performance de la réponse à incident sont-ils en phase avec les objectifs métiers de l'entreprise et conçus dans une optique d'optimisation continue des processus du département de sécurité ?
- **Réponse à incident —** Votre équipe de sécurité dispose-t-elle de processus et technologies pour l'identification, la catégorisation, l'investigation et la résolution des incidents de sécurité ?

FireEye

Nos consultants collaboreront avec votre entreprise pour développer des technologies et processus à intégrer à votre dispositif de protection. Nous vous accompagnons également dans vos activités de surveillance à court terme, ce jusqu'à ce que votre équipe soit en mesure de prendre définitivement le relais.

Tableau 1. Phases du Cyber Defense Center Development

Phase	Objectif	Tâches
Mise en place	Établir les bases d'une riposte et d'un déploiement efficaces des ressources nécessaires en cas d'incidents	• Développer une matrice d'escalade des incidents ainsi qu'un workflow de réponse • Créer des plans de gestion des stratégies et du dispositif • Définir des indicateurs de performances et concevoir un plan de reporting
Intégration	Intégrer de nouveaux processus, procédures et technologies à votre environnement opérationnel	• Concevoir et dispenser des formations • Établir des accords de niveaux de service opérationnels • Déployer et configurer les technologies
Mise en service	Mettre en œuvre les processus opérationnels et analytiques ainsi que les fonctions de surveillance	• Mettre en place la surveillance initiale • Optimiser continuellement les processus opérationnels et analytiques • Transférer les responsabilités à l'équipe de sécurité ou intervenir en appui de celle-ci

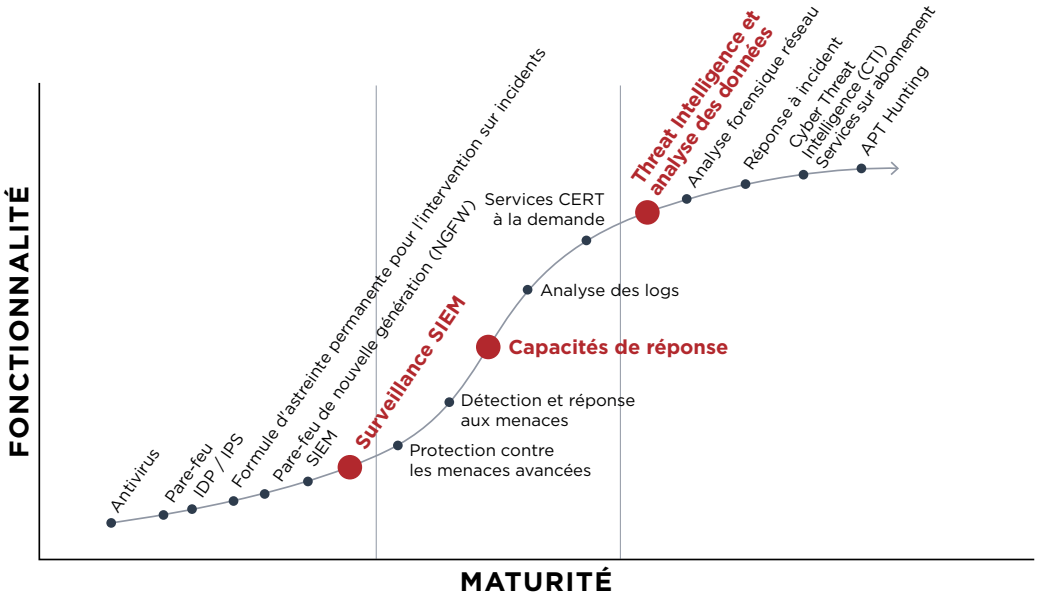

Figure 1. Modèle du Cyber Defense Center Development.

En s'appuyant sur ses six domaines de compétences fondamentales, le service Cyber Defense Center Development permet à votre entreprise d'abandonner son modèle de réponse à incident réactif au profit d'une démarche ciblée, proactive et en parfaite adéquation avec ses objectifs métiers.

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 Cyber Threat Intelligence (CTI). Prolongement naturel et évolutif des opérations de sécurité des clients, la plate-forme unique de FireEye combine des technologies de sécurité innovantes, des services de 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