FIREEYE™

FICHE PRODUIT

Diagnostic du degré de préparation à un incident

Évaluez votre capacité à détecter, réagir et neutraliser les menaces avancées

Pourquoi choisir FireEye 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 opèrent sur les violations de sécurité les plus complexes et les plus médiatisées qui soient. Ils possèdent une connaissance approfondie des auteurs de menaces établis et émergents, ainsi que de leurs outils, tactiques et procédures en constante évolution.

Présentation

Que vous souhaitiez élaborer un plan de réponse à incident de A à Z, renforcer votre dispositif existant ou investir dans les technologies sous-jacentes, Mandiant vous aide à renforcer vos défenses face aux menaces persistantes d'aujourd'hui. Le diagnostic FireEye Mandiant évalue les capacités de cyberdéfense d'une entreprise en général, et de ses équipes SOC et de réponse à incident (IR) en particulier. Lors de leurs missions, les consultants Mandiant mettent dans la balance des pratiques d'excellence et toute leur expérience acquise à répondre à des intrusions dans des entreprises de divers secteurs et zones géographiques. À l'issue du diagnostic, nos experts produisent un rapport comprenant une feuille de route détaillée et des recommandations sur les actions prioritaires à engager.

Même dans les entreprises qui ont investi massivement dans leur cyberdéfense, il n'est pas rare que le doute plane quant à l'efficacité de leurs capacités d'identification, d'évaluation et de neutralisation de menaces ciblées. Les consultants Mandiant sont là pour clarifier la situation. Des malwares courants aux menaces APT de groupes étatiques, en passant par les ransomwares et toutes les formes de cybercriminalité, ils possèdent une expérience de terrain acquise au contact direct de tous les types d'attaque. Ils vous aident ainsi à mesurer votre faculté à gérer des menaces spécifiques à votre entreprise et vous proposent des axes concrets d'amélioration.

Notre méthodologie

Les experts Mandiant analysent votre documentation et les configurations de vos systèmes de journalisation, organisent des ateliers, dirigent des mises en situation et conduisent des tests d'efficacité de vos contrôles de détection des menaces. Vos capacités de cyberdéfense et de réponse sont alors évaluées au regard de six grands domaines de compétences :

- **Gouvernance.** Cadre de référence visant à aligner les pratiques de cyberdéfense sur les objectifs plus stratégiques de l'entreprise.
- **Communication.** Transfert d'informations entre les principaux intervenants internes et externes avant, pendant et après un incident.
- **Visibilité.** Personnes, processus et technologies déployés pour détecter les menaces dans toute l'infrastructure d'une entreprise.
- **Threat Intelligence.** Identification des modes opératoires des attaquants et création de stratégies de détection et d'intervention efficaces.
- **Réponse.** Capacité d'une organisation à vérifier et catégoriser les incidents, évaluer leur gravité et y apporter une réponse appropriée.
- **Métriques.** Mesure et développement des stratégies de renforcement des capacités de cyberdéfense à long terme.

À l'issue du diagnostic, les consultants Mandiant produisent un rapport détaillé assorti d'un plan d'amélioration de vos lignes de défense.

Différentes formules : Chaque structure varie en termes de taille, de maturité et d'objectifs. C'est pourquoi le diagnostic du degré de préparation à incident est adapté aux spécificités de votre entreprise. Vos principaux domaines de compétences IR sont évalués et renforcés par diverses activités d'accompagnement.

Tableau 1. Formules du diagnostic du degré de préparation à un incident.

Formules et prestations comprises dans le diagnostic	NIVEAU I Diagnostic	NIVEAU II Diagnostic Exercices	NIVEAU III Diagnostic Exercices Validation technique
Durée habituelle (semaines)	4	5	6
Revue de la documentation	X	X	X
Ateliers portant sur les six domaines de compétences de la préparation à incident	X	X	X
Examen des configurations de vos systèmes de journalisation	X	X	X
Rapport détaillant le degré de préparation à incident	X	X	X
Débrief pour vos équipes techniques (présentation du rapport)	X	X	X
Débrief pour vos dirigeants (PowerPoint personnalisé)		X	X
Exercices portant sur la matrice des compétences de l'équipe IR		X	X
Comparaison du degré de préparation d'une entreprise par rapport aux acteurs de son secteur		X	X
Plan d'amélioration de la préparation à incident		X	X
Threat Intelligence sectorielle		X	X
Exercices de simulation pour les équipes techniques		X	X
Exercices de simulation pour les équipes dirigeantes			X
Tests d'efficacité des contrôles de détection des menaces (réalisés par FireEye Verodin)			X

Déroulement du diagnostic

Selon la formule sélectionnée, le diagnostic comprend quatre à six étapes et se déroule généralement sur une période allant de quatre à six semaines.

Revue de la documentation (1 semaine)

Analyse hors site de la documentation relative à votre cyberdéfense (plans de réponse à incident, guide tactiques, plans de communication et de gestion de crise, etc.).

Ateliers sur site et exercices portant sur la matrice des compétences (1 semaine)

Ateliers sur site couvrant chacun des grands domaines de compétences de la préparation à incident, en collaboration avec vos intervenants internes, et exercices visant à évaluer la matrice des compétences avec l'équipe IR (jusqu'à sept ateliers au total)

Examen des configurations de vos systèmes de journalisation (0,5 semaine)

Analyse d'échantillons de logs critiques pour valider les configurations nécessaires à une détection et une réponse efficaces.

Exercices de simulation (0,5 semaine)

Exercices de simulation reposant sur des discussions avec vos collaborateurs techniques et vos dirigeants pour évaluer le processus de réponse à incident de bout en bout (jusqu'à deux exercices).

Tests d'efficacité des contrôles de détection des menaces (1 semaine)

Simulation d'attaque sur votre réseau dans un environnement cloisonné et sans risque pour mesurer l'efficacité de vos contrôles de détection des menaces.

Création d'un rapport et bilan (2 semaines)

Rapport détaillant les recommandations stratégiques et tactiques par ordre de priorité, assorti d'une feuille de route concrète pour optimiser les capacités de cyberdéfense de l'entreprise.

LIVRABLES

Une fois le diagnostic effectué, les consultants Mandiant vous remettent un rapport incluant les livrables suivants :

- Évaluation détaillée des capacités actuelles de cyberdéfense de votre organisation
- Recommandations détaillées pour bâtir ou améliorer votre système de défense
- Débrief pour vos équipes techniques
- Plan de mise en application des axes d'amélioration recommandés (Niveau II et Niveau III)
- Débrief pour vos dirigeants (Niveau II et Niveau III)

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 cyberveille. 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.