FIREEYE™

FICHE PRODUIT

Exercices de simulation

Réalisez des exercices de mise en situation pour évaluer votre plan de réponse à incident.

AVANTAGES

- Identification des écarts entre les interventions documentées et attendues, et le comportement réel
- Recommandations basées sur les bonnes pratiques de réponse à incident issues de missions réelles
- Évaluation rapide, efficace et non invasive

« Notre capacité à répondre rapidement et efficacement aux incidents de sécurité est cruciale pour notre activité. Les exercices de simulation ont été très utiles car ils ont donné aux équipes les moyens de valider les décisions et d'entamer le dialogue. »

– RSSI, Entreprise mondiale de distribution de produits et solutions technologiques

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 compromissions de sécurité les plus complexes et les plus médiatisées au monde. Ils possèdent une connaissance approfondie des acteurs établis et émergents, ainsi que de leurs modes opératoires en constante évolution.

Les exercices de simulation s'inspirent de ce savoir-faire pour proposer des mises en situation concrètes, conçues pour couvrir vos principaux domaines de risques techniques et métiers.

Présentation

Les exercices de simulation évaluent les processus et outils mis en place par votre entreprise pour résoudre les cybercrises, ainsi que sa capacité à intervenir en cas de cyberattaques, tant au niveau de la stratégie de la direction que de l'aspect technique des réponse à incident. Lors d'une table ronde, les consultants Mandiant proposent plusieurs mises en situation basées sur leur expérience de terrain pour étudier les actions et décisions que prendrait l'entreprise en cas d'incidents.

Méthodologie

Avant de se lancer dans un exercice de simulation, les experts Mandiant déterminent le profil de menaces de l'entreprise, son environnement opérationnel et les domaines problématiques. Dans le cadre d'un atelier organisé sur site, les consultants soumettent aux principaux intervenants des scénarios basés sur les comportements, techniques et tactiques d'attaquants observés lors de leurs missions de réponse à incident.

Au cours des mises en situation, ils déterminent si les actions et décisions simulées suivent ou s'écartent des plans et processus documentés de l'entreprise, et des bonnes pratiques recommandées par les experts Mandiant en matière de réponse à incident.

PRESTATIONS ET LIVRABLES

Note de synthèse aux dirigeants [PPT]

- Débriefing sur les mises en situation :
  - Interactions des participants avec le plan de réponse à incident, le(s) plan(s) de communication et la (les) procédure(s) d'escalade
  - Enseignements tirés des exercices
  - Recommandations stratégiques

Rapport sur les exercices de simulation [PDF]

- Chronologie des événements
  - Mises en situation
  - Interventions des participants/ intervenants
- Analyse stratégique de la réponse à incident et recommandations sur les améliorations à apporter en fonction de la mise en situation :
  - Détection
  - Réponse
  - Confinement
  - Remédiation

Types d'exercices

Deux exercices de simulation s'offrent à vous : l'un portant sur **l'aspect technique de la réponse à incident** et l'autre sur **la gestion de crise à l'échelle des dirigeants**. Il est recommandé d'effectuer chacune de ces simulations une fois par an, de manière ponctuelle ou dans le cadre d'un exercice coordonné.

L'exercice portant sur l'aspect technique de la réponse à incident s'adresse idéalement aux responsables et équipes sécurité souhaitant mettre leurs capacités d'intervention à l'épreuve.

L'autre exercice, lié à la gestion de crise du point de vue de la direction, répond aux attentes des cadres dirigeants qui veulent évaluer l'efficacité de leurs stratégies de réponse en cas de crise.

À l'issue de l'atelier, nos consultants font part de leurs observations aux participants, puis remettent un rapport écrit détaillé sur les différents scénarios et réponses étape par étape.

Comparatif des exercices

Type d'exercice	Technique	Direction
Objectif	Évaluer et analyser les capacités techniques de détection, de réponse et de neutralisation des menaces avancées.	Évaluer et analyser les capacités de gestion de crise face aux menaces avancées du point de vue de l'équipe dirigeante.
Durées prévues	• Planification : 1 semaine hors site • Mise en situation : 1 à 2 jours sur site • Rapport final : 1 semaine	• Planification : 1 semaine hors site • Mise en situation : 1 à 2 jours sur site • Rapport final : 1 semaine
Participants cibles	• Équipe de réponse aux incidents de cybersécurité • Responsable de la sécurité • Équipe technique (chargée des réseaux, serveurs, boîtes de messagerie, etc.)	• Responsable de la sécurité des systèmes d'information (RSSI) • Cadres dirigeants du Comex • Relations publiques et communications d'entreprise • Directeur juridique
Compétences acquises	• Savoir quand isoler des hôtes sur un réseau • Déterminer le bon moment pour réimager un système • Définir la manière dont les analystes suivent le plan de réponse à incident, le plan de communication et la matrice d'escalade • Savoir quand et comment impliquer les fournisseurs	• Savoir quand se soumettre à une menace d'extorsion ou une demande de rançon • Prendre des décisions en fonction de l'impact des tactiques de confinement • Divulguer une compromission aux régulateurs et autres acteurs concernés • Adopter les bonnes pratiques de notifications aux clients • Adopter les bonnes pratiques de communication aux médias
Méthode de livraison	Mise en situation sur site.	Mise en situation sur site.

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.

FIREEYE™