FIREEYE™

FICHE PRODUIT

Intelligence Capability Development

Optimisez vos capacités de Threat Intelligence

EN BREF

- Améliorez votre capacité à utiliser, analyser et appliquer la Threat Intelligence à vos opérations de cybersécurité
- Misez sur plus de 12 ans d'expérience dans le développement de solutions de Threat Intelligence pour les organisations publiques et privées
- Évaluez vos capacités de Threat Intelligence existantes et planifiez des améliorations
- Établissez le profil de cyber-risque de votre organisation, les informations nécessaires pour réduire ce risque et les personnes habilitées à utiliser ces données
- Structurez l'application de la Threat Intelligence autour des cas d'usage tactiques, stratégiques et opérationnels
- Participez à des ateliers qui vous aideront à améliorer vos capacités et à mieux exploiter la CTI au quotidien

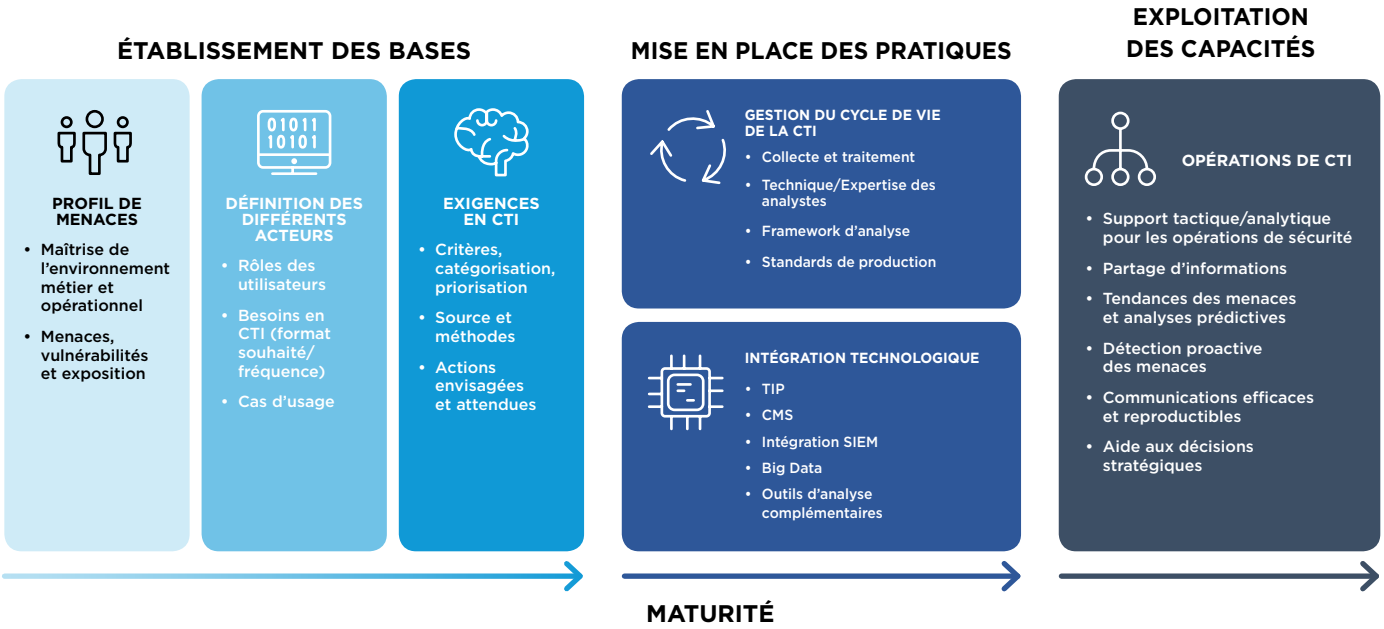
Aujourd'hui, les cybercriminels sont mieux formés, financés et équipés qu'un grand nombre d'équipes de sécurité. Les cyberattaques en deviennent par conséquent plus complexes et plus destructrices que jamais. Dans le monde de la sécurité, les entreprises peinent à attirer et fidéliser les talents, sans compter qu'elles ne peuvent généralement pas se permettre toutes les compétences dont elles auraient besoin.

C'est pourquoi un nombre croissant d'organisations se tournent vers des services externes de Cyber Threat Intelligence (CTI) pour réduire leur risque et renforcer leur sécurité. Cependant, beaucoup d'entre elles ne savent pas par où commencer. D'autres foncent tête baissée sans vraiment cerner leurs besoins en CTI ni quel usage en faire. Or, cela se révèle généralement aussi coûteux que contre-productif. D'où l'importance pour elles de mieux rentabiliser leurs investissements CTI.

Les services FireEye Intelligence Capability Development (ICD) ont été spécialement conçus pour aider les entreprises à libérer le potentiel réel de leur CTI. Au cours de la dernière décennie, des centaines d'organisations ont suivi les conseils des consultants ICD de FireEye pour mieux utiliser, analyser et mettre en application leur CTI. Elles ont ainsi pu renforcer l'efficacité de leurs programmes de sécurité.

Le principe
Basés sur un framework standardisé, les services CTI développés par l'équipe ICD se déroulent en trois temps : 1) **bilan** du programme CTI en place et des menaces en présence ; 2) **conception** d'un programme de sécurité en phase avec vos exigences réglementaires et organisationnelles ; et 3) **formation** de votre équipe à l'analyse et à l'application de la CTI à des cas d'usage spécifiques.

Ce framework définit les éléments les plus indispensables à un programme CTI efficace.



Des projets ciblés sur des cas d'usage spécifiques jusqu'aux déploiements à très grande échelle, les services ICD s'adaptent à tous les besoins. Quelle que soit la configuration, l'objectif reste le même, à savoir renforcer la capacité d'une entreprise à rentabiliser au maximum sa Cyber Threat Intelligence externe. Au menu :

- **Threat Intelligence Foundations (TIF)**
  Cette étape vise à poser les bases du développement de vos capacités de Threat Intelligence. Il s'agira entre autres d'identifier les menaces qui vous concernent, les différents acteurs qui bénéficieront de la Threat Intelligence et les actions à mettre en place pour un déploiement et un usage efficaces. [Bilan]
- **Cyber Threat Diagnostic (CTD)**
  CTD analyse votre environnement actuel pour identifier et documenter les menaces auxquelles votre entreprise fait face. Bien connaître la physionomie de la menace, c'est mieux adapter vos défenses et prioriser vos actions en fonction des motivations et des intentions des cybercriminels ciblant votre entreprise. [Bilan]
- **Intelligence Capability Assessment (ICA)**
  L'ICA évalue l'efficacité de vos systèmes actuels de Threat Intelligence et leur intégration à votre programme de sécurité. Une analyse détaillée des écarts sert de base à une feuille de route destinée à corriger ces lacunes sur les plans humains, technologiques et méthodologiques. [Bilan]
- **Intelligence Capability Uplift (ICU)**
  ICU crée un plan de mise en place d'une Cyber Threat Intelligence basée sur des processus évolutifs et reproductibles de collecte, d'analyse et de diffusion de l'information dans toute l'entreprise. [Conception]
- **Intelligence Jumpstart (IJ)**
  IJ est une introduction aux nombreux sujets abordés en détail par les services de consulting. Cet atelier interactif d'une journée s'appuie sur l'expertise de nos professionnels de la Threat Intelligence tactique et stratégique pour définir les cas d'usage techniques et opérationnels adaptés à votre organisation. [Conception]
- **Analytic Tradecraft Workshop (ATW)**
  Cet atelier d'une journée aide votre équipe à affiner ses capacités d'analyse pour gérer les activités de Threat Intelligence interne. Au programme : concepts de base de la CTI, techniques d'analyse structurée, communication et gestion des menaces et des risques. [Formation]
- **Hunt Mission Workshop (HMW)**
  HMW introduit votre équipe à un framework permettant de standardiser la traque des menaces dans votre entreprise. Une analyse de vos méthodes actuelles vous aidera à identifier un ensemble de processus reproductibles définis comme bonnes pratiques. Cet atelier s'adresse aux équipes du SOC, aux experts de la réponse à incident et aux spécialistes de la veille tactique chargés de détecter les menaces. [Formation]

L'avantage FireEye

Avec FireEye à vos côtés, vous pouvez préparer vos collaborateurs, processus et procédures aux rigueurs d'un champ des menaces en constante évolution et en perpétuelle expansion.

L'équipe FireEye Intelligence Capability Development (ICD) possède plus de 10 ans d'expérience dans le développement des capacités CTI de ses clients. Cette expérience est le fruit des leçons et bonnes pratiques acquises au contact du pôle FireEye Threat Intelligence. Ce n'est donc pas un hasard si FireEye est le seul fournisseur de services de Threat Intelligence classé dans la catégorie « Leader » du rapport « The Forrester New Wave™: External Threat Intelligence (3ème trimestre 2018) » du cabinet Forrester Research.

FireEye a passé ces dix dernières années à aider des entreprises de divers secteurs à adopter et intégrer des services de CTI à leurs opérations de sécurité. Ces missions ont contribué à la création et l'affinement de services adaptés aux objectifs et besoins de n'importe quelle organisation. Acteurs des médias, pouvoirs publics, entreprises du privé… des organisations du monde entier font confiance au leadership et aux solutions FireEye.

Ensemble ou séparément, les services ICD ont pour but de faciliter le développement et la gestion d'un programme de Threat Intelligence complet.

Pour en savoir plus, rendez-vous sur **https://www.fireeye.com/solutions/cyber-threat-intelligence/intelligence-capability-development.html** et consultez le **rapport Forrester**.

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 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.