

FICHE PRODUIT

Cyber Physical Threat Intelligence

Assurez la protection de vos systèmes physiques complexes, interconnectés et gérés par logiciel



EN BREF

- Analyse et reporting des vulnérabilités cyber-physiques
- Décryptage technique des modes opératoires des spécialistes d'attaques cyber-physiques
- Analyse multi-source de la Threat Intelligence spécifique aux menaces cyber-physiques
- Analyse de l'actualité et des recherches axées sur les technologies opérationnelles
- Accès aux contenus pédagogiques visant à sensibiliser votre équipe aux enjeux de la sécurité cyber-physique

Dans de nombreux secteurs, l'essor des technologies de l'information et de la communication (TIC) a conduit à une intégration accrue de fonctionnalités digitales chargées du contrôle et de la maintenance de processus physiques. Mais si cette rencontre entre virtuel et physique marque une véritable révolution en termes de connectivité et d'instrumentation, elle élargit aussi la surface de risque des entreprises.

D'où l'importance de détecter et signaler proactivement les vulnérabilités techniques et les modes opératoires des hackers pour mieux anticiper et prévenir les attaques cyber-physiques.

C'est pourquoi FireEye a lancé Cyber Physical Threat Intelligence, un service forfaitaire qui vous livre des analyses concrètes et contextualisées des menaces pesant sur les systèmes cyber-physiques (technologies opérationnelles, systèmes de contrôle industriels (ICS), Internet des objets (IoT) et tout autre équipement utilisé pour piloter des processus physiques) dans des secteurs comme les télécoms et le médical, entre autres.

Que comprend votre abonnement ?

Pour toutes les organisations chargées de maintenir la sécurité et la continuité de tels systèmes, le service Cyber Physical Threat Intelligence envoie des alertes précoces sur les vulnérabilités critiques et les campagnes cyber qui visent à les exploiter. Avec Cyber Physical Threat Intelligence, les équipes de sécurité peuvent maintenir une longueur d'avance sur les attaquants et prendre de meilleures décisions sur les orientations sécuritaires de leurs systèmes cyber-physiques.

L'abonnement Cyber Physical Threat Intelligence comprend des rapports ciblés et détaillés sur les malwares, les profils d'attaquants, leurs modes opératoires, les activités en cours, les vulnérabilités et les enjeux stratégiques. Le tableau 1 dresse un aperçu des domaines dans lesquels FireEye fournit une Threat Intelligence approfondie aux équipes chargées de défendre ces systèmes.

Tableau 1. Domaines de couverture de FireEye Cyber Physical Threat Intelligence.

Domaine de couverture	Description
Threat Intelligence actualisée	Analyses tactiques et stratégiques des activités malveillantes en cours. Le corpus d'analyse se fonde sur des données issues des missions de réponse à incident de FireEye Mandiant, des technologies FireEye déployées chez nos clients et d'un vaste réseau de capteurs FireEye dispersés dans le monde entier.
Référence cyber-physique	Examen de la terminologie, de l'architecture réseau, sécurité des ports et protocoles ICS, ainsi que des auteurs de menaces cyber-physiques.
Vulnérabilités cyber-physiques	Rapports tactiques sur les vulnérabilités ICS.
Activité du réseau ICS	Analyse du trafic réseau sur les ports ICS à partir des données des journaux du pare-feu.
Tour d'horizon de la sécurité ICS	Collecte, analyse et enjeux des publications ICS dans les médias.
Source FireEye Mandiant	Enseignements issus des interventions de Mandiant : examen des tendances et des bonnes pratiques de sécurité.
Outils et recherche	Recherche et analyse d'outils de reconnaissance et d'attaque axés sur les ICS.

Gardez une longueur d'avance sur les nouvelles menaces

Les systèmes cyber-physiques présentent une équation complexe d'avantages et de risques. Pour mieux les protéger, vous devez donc vous tenir constamment informé sur les exigences spécifiques de leur sécurité. Les avantages du service :

- Une notation des vulnérabilités et une analyse des options de remédiation pour mieux identifier et gérer les vulnérabilités cyber-physiques qui vous concernent.
- Une lecture précise de la situation sous tous ses angles – menaces, campagnes en cours et profils des attaquants ciblant vos systèmes cyber-physiques.
- Une sensibilisation de tous les acteurs internes et externes concernés grâce à des documents de référence approfondis et une couverture des événements de sécurité cyber-physique qui vous touchent directement.
- Des décisions plus éclairées pour faire évoluer votre programme et vos contrôles de sécurité cyber-physique.
- Des informations immédiatement exploitables pour passer d'une posture réactive à une gestion proactive des risques cyber-physiques.

Pour plus d'informations sur FireEye Cyber Physical Threat Intelligence et sa capacité à fiabiliser vos décisions de sécurité, rendez-vous sur www.FireEye.com

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.

