SCHEDA TECNICA

Cyber Physical Threat Intelligence

Zero attacchi contro sistemi fisici complessi, interconnessi e gestiti da software

CARATTERISTICHE PRINCIPALI

- Analisi e reporting sulle vulnerabilità informatico-fisiche
- Analisi tecnica dei TTP informatico-fisici degli aggressori
- Analisi dell'intelligence da tutte le fonti delle minacce informatico-fisiche
- Analisi di notizie e ricerche incentrate sulla tecnologia operativa
- Accesso a contenuti educativi per aumentare la consapevolezza della sicurezza in tutto il team

La crescente importanza delle tecnologie di comunicazione in diversi settori ha portato a una maggiore integrazione delle caratteristiche digitali che supportano il controllo e la manutenzione dei processi fisici. Questa intersezione tra il virtuale e il fisico ha portato non solo a una connettività e a una strumentazione rivoluzionaria, ma anche a rischi significativi per la sicurezza.

Sta diventando sempre più importante apprendere e condividere in modo proattivo le vulnerabilità tecniche e le possibili tattiche, tecniche e procedure (TTP) degli aggressori, in modo da poter anticipare e prevenire gli attacchi informatico-fisici.

FireEye Cyber Physical Threat Intelligence è un servizio in abbonamento che fornisce il contesto, i dati e le possibili analisi delle minacce sui sistemi ciberfisici, compresa la tecnologia operativa, i sistemi di controllo industriale, Internet delle cose e altre apparecchiature utilizzate per supportare i processi fisici, ad esempio, nel settore delle telecomunicazioni e in quello medico.

Ciò che offre il tuo abbonamento

Per le organizzazioni che hanno il compito di mantenere la sicurezza e la continuità di questi sistemi, Cyber Physical Intelligence fornisce un allarme tempestivo sulle vulnerabilità critiche, così come sulle campagne di minacce e sugli avversari che le prendono di mira. Con Cyber Physical Intelligence, i team di sicurezza possono stare al passo con gli aggressori e prendere decisioni più consapevoli sulle condizioni di sicurezza dei loro sistemi ciberfisici.

L'abbonamento a Cyber Physical Intelligence include una reportistica approfondita su malware e tattiche informatico-fisici, sulle tecniche e procedure dannose, sugli attori delle minacce, sull'attività delle minacce, sulle vulnerabilità e sulle intuizioni strategiche. La Tabella 1 elenca le aree critiche di copertura in cui FireEye fornisce informazioni approfondite ai team incaricati di difendere questi sistemi.

Tabella 1. Aree di copertura di FireEye Cyber Physical Threat Intelligence.

Area di copertura	Descrizione
Intelligence attuale	Analisi tattica e strategica dell'attività delle minacce, derivata dagli interventi di FireEye Mandiant, dalla tecnologia FireEye implementata e dalla vasta rete di sensori FireEye distribuiti in tutto il mondo.
Riferimento Cyber Physical	Revisione della terminologia, dell'architettura di rete, delle porte ICS [*Industrial Control System* (sistemi di controllo industriale)] e della sicurezza dei protocolli ICS e degli aggressori delle minacce informatico-fisiche.
Vulnerabilità Cyber Physical	Reporting tattico sulle vulnerabilità dell'ICS.
Attività della rete ICS	Analisi del traffico di rete sulle porte ICS sulla base dei dati dei log del firewall.
Ronda di sicurezza ICS	Raccolta, analisi e implicazioni delle pubblicazioni ICS nei media.
Provenienti di FireEye Mandiant	Revisione continua degli interventi di Mandiant per esaminare i dati di tendenza e le migliori pratiche di sicurezza.
Strumenti e ricerca	Ricerca e analisi di strumenti di ricognizione e di attacco focalizzati sull'ICS.

Cogli sul tempo le minacce di prossima generazione

I sistemi ciberfisici presentano una serie complessa di vantaggi e rischi. Per anticipare e bloccare le minacce che colpiscono i sistemi ciberfisici è necessario mantenere le informazioni attuali sui requisiti di sicurezza unici di queste tecnologie:

- Aumentare la consapevolezza delle vulnerabilità di sicurezza informatico-fisiche rilevanti e supportare gli sforzi di gestione delle vulnerabilità attraverso il punteggio di vulnerabilità di FireEye e l'analisi delle opzioni di rimedio.
- Acquisire consapevolezza situazionale delle minacce, delle campagne e degli attori che prendono di mira i vostri sistemi ciberfisici.
- Educare i team interni e gli stakeholder esterni con materiale di riferimento approfondito e una serie di eventi d'attualità su misura per il mondo ciberfisico.
- Prendere decisioni più consapevoli sul programma di sicurezza ciberfisica in evoluzione e sui controlli.
- Assicurarsi un'intelligenza che permetta di modificare le condizioni di gestione dei rischi informatico-fisici da reattivi a proattivi.

Per ulteriori informazioni su come FireEye Cyber Physical Intelligence può aiutare il vostro team di sicurezza a prendere decisioni di sicurezza più consapevoli, **www.FireEye.com**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

Informazioni su FireEye, Inc.
FireEye è un'azienda che offre servizi di sicurezza informatica basati sull'intelligence. Operando come estensione intuitiva e scalabile dei processi operativi di sicurezza dei clienti, FireEye offre un'unica piattaforma in grado di coniugare tecnologie di sicurezza innovative, intelligence sulle minacce a livello nazionale e servizi di consulenza Mandiant® di fama mondiale. Grazie a questo approccio, FireEye elimina la complessità e l'onere della sicurezza informatica per le aziende che hanno difficoltà a prepararsi per futuri attacchi, prevenirli e rispondere ad essi.

FIREEYE™