CYBER THREAT INTELLIGENCE · BROCHURE

Il servizio che ti mette un passo avanti agli hacker.

Individua le minacce prima che diventino problemi.

Cyber Threat Intelligence

CYBERFERO

Cos'è la Cyber Threat Intelligence?

La *Cyber Threat Intelligence* è la conoscenza riguardo una minaccia o un rischio per le proprie risorse.

Il servizio parte dal presupposto che una **minaccia sia presente**, prima ancora di averne le prove. Questo approccio proattivo permette di intercettare gli attacchi sul nascere, anziché difendersi solo quando sono già in corso.

L'obiettivo è trasformare i dati grezzi disponibili sulla rete in informazioni **azionabili**, su cui i team di sicurezza possono basare decisioni operative.

I vantaggi sono numerosi

+34%

Maggiore efficienza del team

Di tempo risparmiato nella stesura di report e nella gestione delle priorità.

10×

Localizzazione veloce delle minacce

Più rapidi nell'identificazione di una minaccia rispetto a un approccio tradizionale.

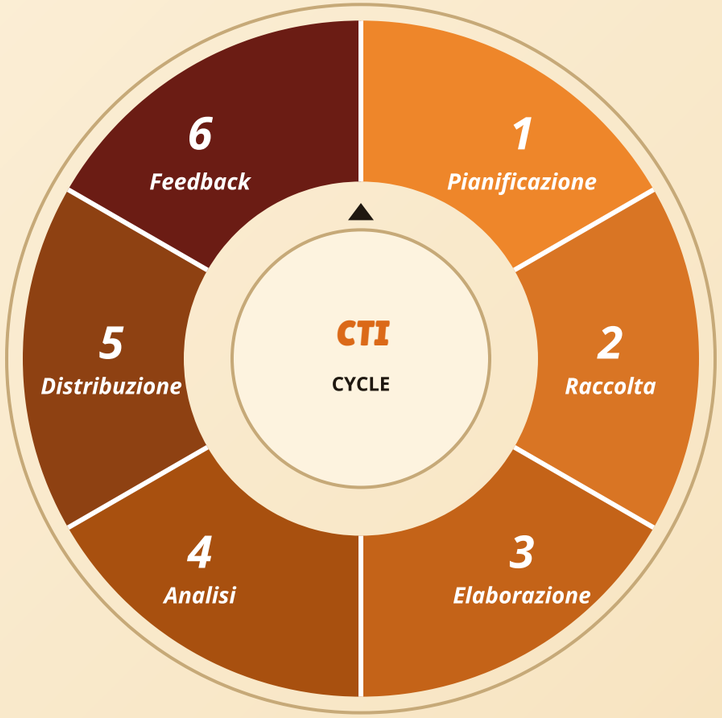
Mitigazione tempestiva

Le minacce individuate vengono soppresse molto più velocemente, riducendo l'impatto.

Il ciclo della Cyber Threat Intelligence

La **CTI** *è il prodotto finito di un ciclo in* **sei parti** *che comprende raccolta, elaborazione e analisi dei dati.*

Il processo è un ciclo perché nuove domande e lacune vengono identificate nel corso dello sviluppo dell'intelligence, portando alla definizione di nuovi requisiti di raccolta. Un programma di intelligence efficace è iterativo e diventa più **raffinato ed efficiente** *con il tempo.*



1. Pianificazione e direzione

Il primo passo è porre la **domanda giusta** per guidare la creazione delle informazioni attuabili sulle potenziali minacce.

2. Raccolta

Si raccolgono **dati grezzi** che soddisfino i requisiti stabiliti nella prima fase.

3. Elaborazione

I dati raccolti vengono organizzati con metadati, filtrando informazioni ridondanti, falsi positivi e falsi negativi.

4. Analisi

Si cercano potenziali **problemi di sicurezza** e si notificano ai team pertinenti nel modo definito in fase di pianificazione.

5. Distribuzione

Affinché l'*intelligence* sulle minacce sia utilizzabile, deve arrivare alle **persone giuste**.

6. Feedback

Chi ha fatto la richiesta iniziale rivede il prodotto di intelligence finito e determina se le domande hanno trovato risposta.

Il segreto? Pensare come un hacker

L'**analisi continua** dei dati che si possono trovare nel *Deep Web* e nel *Dark Web* fornisce importanti indizi su quali potrebbero essere le **nuove tecniche di attacco** degli hacker.

Vengono inoltre tenute sotto controllo le **fonti fraudolente** rintracciabili sotto la superficie del web mainstream.

Partendo dal presupposto che si potrebbe essere sotto attacco **inconsapevolmente**, la ricerca non è influenzata da alcun bias. Verifiche e controlli continui assicurano che l'intelligence raccolta non si applichi alla propria azienda.

Web di superficie	Tutto ciò che è indicizzato dai motori di ricerca pubblici.
Deep Web	Contenuti non indicizzati: portali aziendali, database privati, area riservate.
Dark Web	Reti accessibili solo con software dedicati, dove circolano spesso dati trafugati.

Monitoriamo costantemente

20B+
credenziali rubate

250+
fonti di threat intelligence

100M+
nomi di dominio

50+
fonti legali ufficiali

Cosa comprende il servizio nella pratica

Grazie a tecniche **OSINT** (*Open Source Intelligence*), siamo in grado di **setacciare tutto il web** in cerca di informazioni e dati che potrebbero essere stati trafugati.

Non è raro che i dati aziendali vengano sottratti e utilizzati per pianificare un colpo, ad esempio un *ransomware*. Questi dati sono spesso condivisi nelle aree del web chiamate **Deep Web** e **Dark Web**.

Grazie ai nostri **Cyber Threat Hunter** siamo in grado di cercare e recuperare quelle informazioni. Sapere cos'è stato trafugato rende molto più semplice organizzare una **difesa mirata**.

Cosa potrebbe già essere nelle mani sbagliate

- **Credenziali rubate**
- **Documenti esposti**
- **Leak di codice sorgente**
- Sistemi che hanno subito **Data Breach**
- Siti di **phishing** collegati al nome dell'azienda
- Account falsi nei **Social Network**
- Rapporti sulle **vulnerabilità** non richiesti
- Violazioni del **marchio**
- Nomi di **dominio** occupati

Dal **2011** ci occupiamo di tecnologia Cloud e di sicurezza, affidati a professionisti esperti.

Scegli la sicurezza per la tua azienda

Scopri il servizio sul sito

CYBERFERO

Per ulteriori informazioni, i nostri contatti sono:

Via Statuto 3,
42121 Reggio Emilia (RE)
www.cyberfero.com

Tel. +39 0522 1685330
E-mail: info@cyberfero.com
Pec: cyberfero@pec.it
P. IVA: 03058120357