



Individua le *minacce* prima
che diventino *problemi*

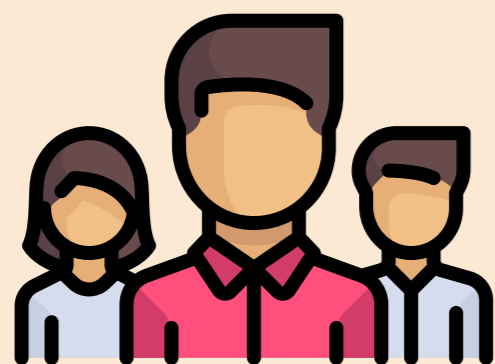
Il servizio che ti mette
un passo avanti agli hacker:

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 di avere le prove.

I vantaggi sono numerosi



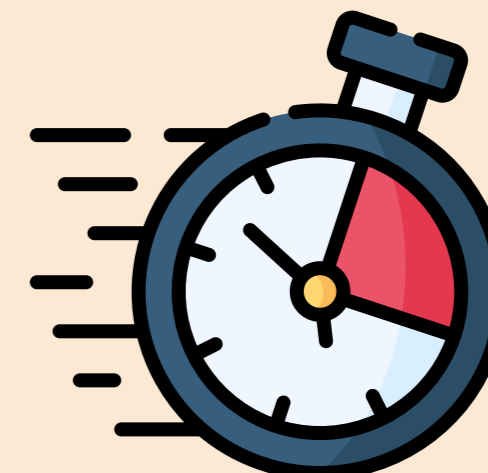
Maggiore efficienza del team

34% di tempo risparmiato nella stesura di report



Localizzazione veloce delle minacce

Fino a 10 volte più veloci nell'identificazione di una minaccia



Mitigazione tempestiva

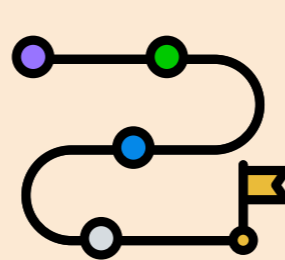
Le minacce individuate sono **sopresse più velocemente**

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.



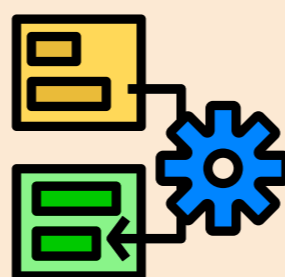
2. Raccolta

Il passo successivo è quello di raccogliere dati grezzi che soddisfino i requisiti stabiliti nella prima fase.



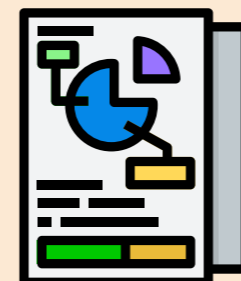
3. Elaborazione

Una volta che tutti i dati grezzi sono stati raccolti, è necessario organizzarli con metadati, filtrando le informazioni ridondanti o i falsi positivi e negativi.



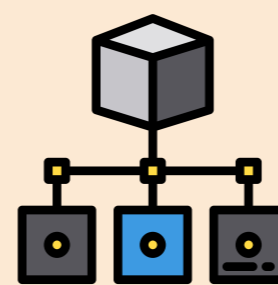
4. Analisi

L'obiettivo dell'analisi è la ricerca di potenziali problemi di sicurezza e la notifica ai team pertinenti nel modo definito nella prima fase di pianificazione.



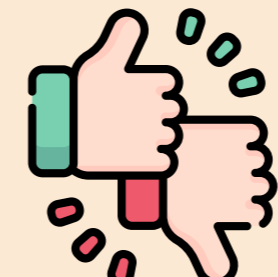
5. Distribuzione

Affinché l'intelligence sulle minacce siano utilizzabili, devono arrivare alle persone giuste.

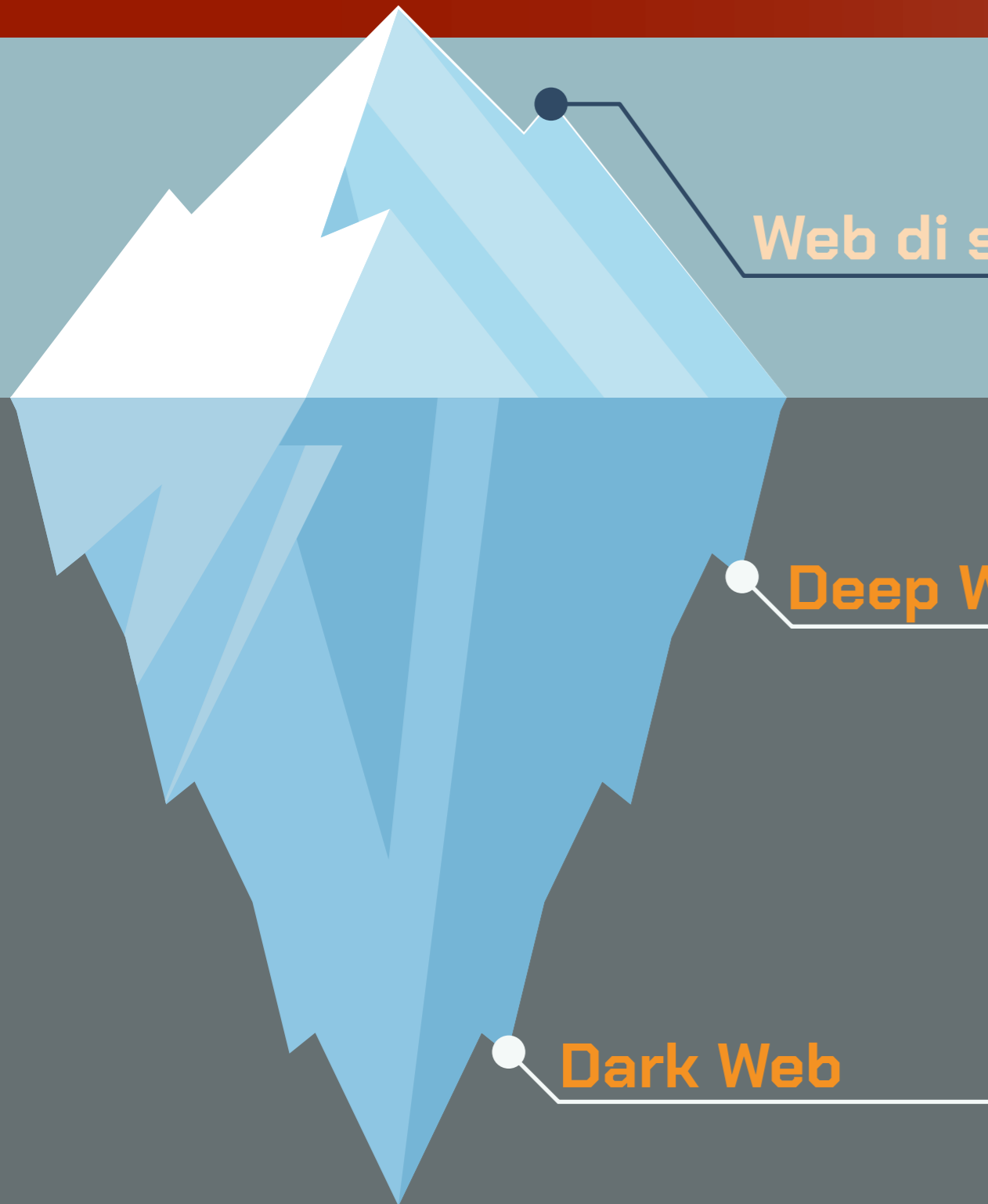


6. Feedback

Dopo aver ricevuto il prodotto di intelligence finito, chi ha fatto la richiesta iniziale lo rivede e determina se le sue domande hanno trovato risposta.



Il segreto è pensare come un hacker



Web di superficie

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

Inoltre, vengono tenute sotto controllo le fonti fraudolente rintracciabili sotto la superficie del web *mainstream*.

Vengono monitorate continuamente:

20+ miliardi
di credenziali rubate

100+ milioni
di nomi di dominio

250+
fonti di threat intelligence

50+
fonti legali ufficiali

Partendo dal presupposto che si potrebbe essere sotto attacco inconsapevolmente, la ricerca non è influenzata da alcun *bias*. **Vengono eseguite continue verifiche e controlli** per assicurarsi che le *intelligence* recuperate nelle fasi di ricerca e analisi non si applichino alla propria azienda.

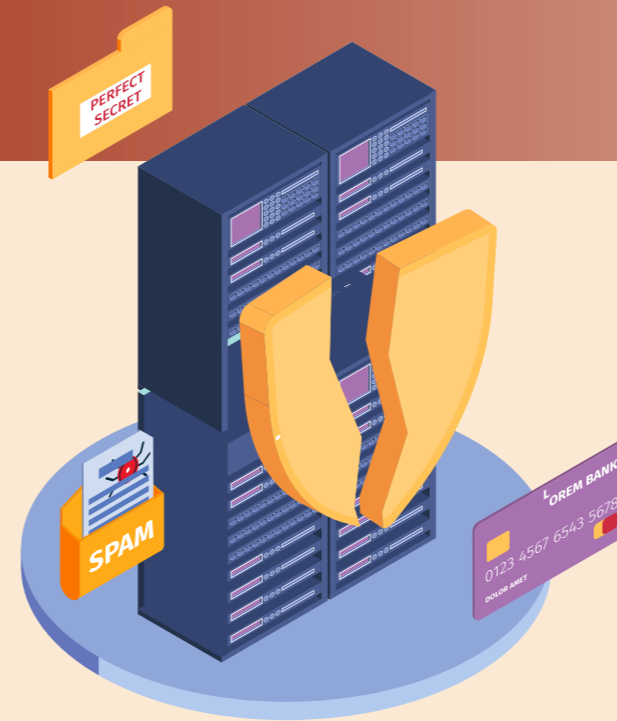
Cosa comprende il servizio nella pratica

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 trafugati e utilizzati per pianificare un colpo, per esempio un ransomware. Questi dati sono spesso condivisi in quelle aree del web chiamate *Deep Web e Dark Web*.

Alleghiamo una lista *non esaustiva*, delle **informazioni che potrebbero già essere nelle mani sbagliate**.

Grazie ai nostri Cyber Threat Hunter siamo in grado di cercare e recuperare quelle informazioni. *Allo stesso tempo, sapendo cos'è stato trafugato, è molto più semplice organizzare una difesa.*



- **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 Networks**
- **Rapporti sulle vulnerabilità non richiesti**
- **Violazioni del marchio**
- **Nomi di dominio occupati**

Scegli la sicurezza per la tua azienda

Dal 2011 ci occupiamo di tecnologia Cloud e di sicurezza, affidati a dei professionisti esperti!

Scopri il servizio sul sito

Per ulteriori informazioni, i nostri contatti sono:

Via Zacchetti 6, 42124 - Reggio nell'Emilia (RE)

www.secure-od.com

Tel. +39 0522 1685330

Fax. +39 0522 015371

E-mail: info@secure-od.com

Pec: secure-od@pec.it

