

Caratteristiche	Silver	Gold	Advanced
Cyber Threat Intelligence Tattica	●	●	●
Cyber Threat Intelligence Tattica e operativa	●	●	●
Daily CTI Report	●	●	●
Tactical CTI Report		●	●
Operational & Strategic CTI Report		●	●
Utilizzo di CTI Feed legati a specifici settori industriali	●	●	●
Cyber Threat Intelligence Operativa e strategica		●	●
Supporto on-demand			●

Che tipo di informazioni/ intelligence vengono fornite?

Tipo di subscription	Caratteristiche	Settori Industriali			
		Government	Finance & Banking	Energy	Telco
SILVER	Adversary Network Infrastructure	●	●	●	●
	Malware Campaigns	●	●	●	●
	DDoS Campaigns	●	●	●	●
	Security Vulnerability	●	●	●	●
	Torear Actions	●	●	●	●
	Tools, Techniques, & Procedures (TTP)	●	●	●	●
	Incidents & Campaigns	●	●	●	●
GOLD	Vulnerability & Incident per sistemi ICS/SCADA			●	●
	Domain Abuse	●	●	●	●
	Phishing (Kits e URLs)	●	●	●	●
	Compromised Account (Data Leak e Data Breach)	●	●	●	●
	Brand Reputation	●	●	●	●
	Analisi Mention & Information in DarkWeb	●	●	●	●
ADVANCED	Intelligence on-demand di 50 giornate specialistiche di Secondo Livello per custom report e analisi personalizzate	●	●	●	●
ADD ON	Compromised Credit Card		●		

Nota: il servizio include ulteriori vertical di mercato oltre a quelli indicati

Cyber Threat Intelligence

Servizio FUSION

Cyber Threat Intelligence

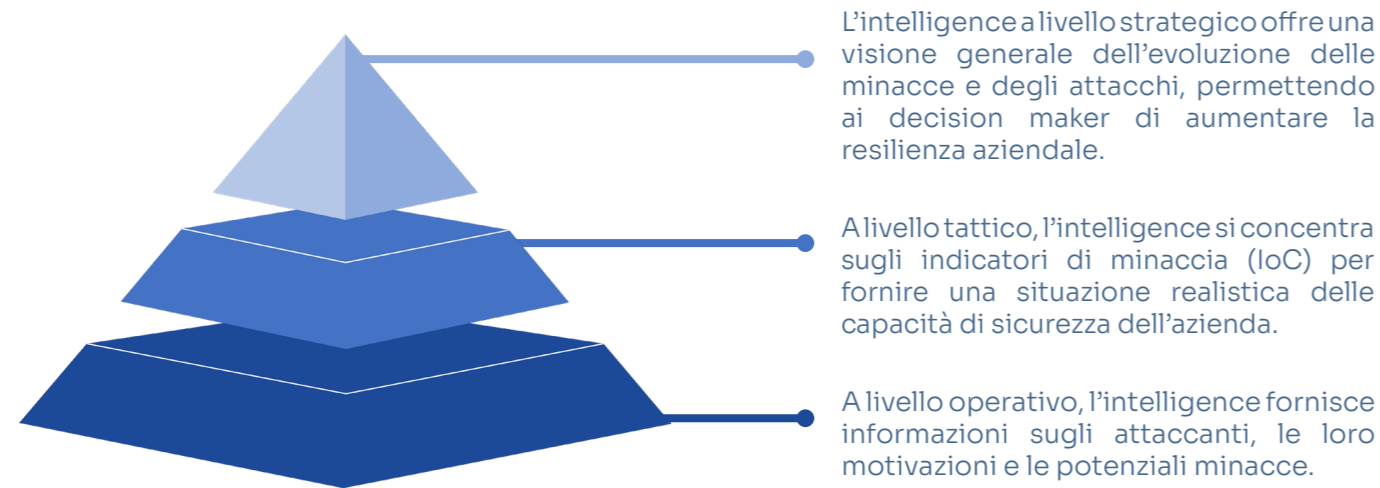
Uno strumento potente per massimizzare l'efficacia della tua difesa proattiva

La Cyber Threat Intelligence (CTI) consiste nel raccogliere, analizzare e utilizzare informazioni sulle minacce di cyber security. Le fonti variegata forniscono dati sulle cyber threats e le TTP, permettendo da subito

l'identificazione, il monitoraggio e il blocco delle minacce. Ciò si traduce in una difesa proattiva e preventiva, proteggendo i sistemi prima che questi vengano attaccati.

L'unicità del nostro modello

Con l'obiettivo di migliorare la prevenzione degli attacchi e definire più complete strategie di mitigazione e risposta al rischio cyber, il servizio FUSION di cyber threat intelligence proposto da DeepCyber e Cy4gate risponde all'esigenza di fornire i tre livelli di informazioni della CTI:



L'esigenza

Potenziare i livelli di difesa cyber a partire da quella proattiva

Il crescente numero e l'intensità degli attacchi informatici sta spingendo verso il miglioramento dei sistemi di difesa, in particolare attraverso l'uso di strumenti di difesa proattiva e preventiva in grado di neutralizzare le minacce prima che queste possano creare impatti.

La soluzione

Cyber Threat Intelligence

Combinando l'intelligence con il monitoraggio e l'analisi delle minacce cyber, è possibile creare una vincente strategia di contenimento per gestirle. Un'efficace strategia difensiva si basa sull'intelligence tattica tempestiva e costante, utilizzabile attraverso il centro operativo di sicurezza (SOC). Le informazioni fornite sono

contestualizzate verticalmente rispetto alla destinazione d'uso di riferimento, ovvero sono relative al solo contesto tecnologico e al settore merceologico del cliente. Oltre ai feed di CTI, i clienti ricevono dal servizio i principali actionable insights sotto forma di report anche questi verticali su settore/industry di riferimento.

Un servizio avanzato di intelligence

In cosa è diversa questa soluzione: benefici ed elementi differenzianti

Il servizio FUSION di cyber threat intelligence (CTI) fornisce un valore aggiunto che può essere sintetizzato con questi vantaggi immediati:

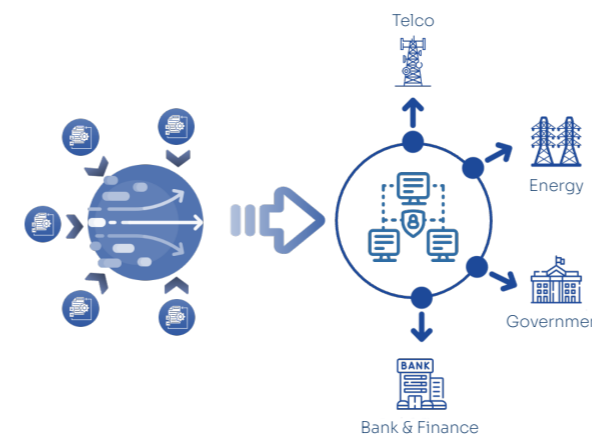
1. Permette all'azienda di impiegare in modo efficace la CTI evitando alti costi di investimento per piattaforme e competenze specialistiche.
2. Fornisce giornalmente l'acquisizione di fonti dati CTI qualificate sia commerciali (Mandiant, Group-IB, ecc.) sia open source.
3. Propone una intelligence immediatamente utilizzabile grazie alla contestualizzazione sull'ambito tecnologico di riferimento, in aggiunta a tutte le campagne maggiormente significative trasversali.
4. Fornisce periodicamente (anche su base giornaliera) report personalizzati sulla base dei settori industriali dei clienti.

Come funziona?

Il servizio è erogato attraverso la condivisione dei CTI Feed già aggregati, normalizzati e correlati, pronti all'uso sui sistemi di cybersecurity, raccolti giornalmente da fonti qualificate (commerciali e open source) e specificatamente legate al settore

industriale di riferimento. Questo permette di ricevere in maniera flessibile un'intelligence tattica già processata e immediatamente utilizzabile sui sistemi di sicurezza aziendali (Firewall, AV/AM, Web App Security/Web Filtering, etc.).

Analisi, gestione ed invio dei Feed



Creazione, update e dissemination dei report



Il servizio prevede tre livelli di erogazione:

- nella **versione Silver** il cliente riceve una completa intelligence tattica
- nella **versione Gold** l'intelligence fornita con la versione Silver è arricchita con informazioni sugli attaccanti e sulle modalità operative utilizzate per realizzare gli attacchi
- nella **versione Advanced** il cliente riceve l'intelligence operativa della versione Gold, ma può usufruire di un livello di supporto on-demand dedicato