
NEW THREATS EVOLVE, READY TO GO DEEP
DEEPCYBER

Summary

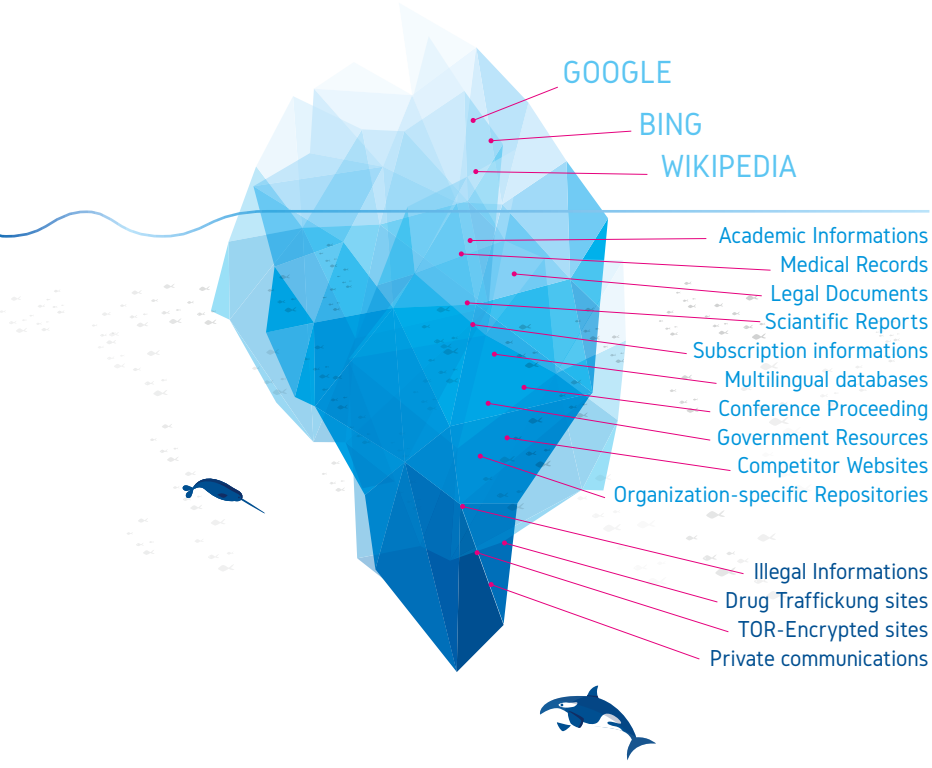
Lo scenario delle minacce è in continua evoluzione e la natura transnazionale delle stesse necessita di un approccio integrato, tattico e strategico, attivando tutti i possibili canali di ascolto, compreso l'ambito web ed in particolare il Deepweb e il Darkweb.

Un approccio «Intelligence Driven», è quello più efficace per ridurre i tempi e più in generale per avere un'ottima «Situational Awareness» su quanto avviene in ambito internazionale.

Che cosa è la Cyber Threat Intelligence

Esiste una differenza sostanziale tra (Cyber) Threat Data (es. dump con dati su compromissione generica di ATM e 20.000 BIN carte) e Threat Intelligence (es. di questi dati, alcuni riguardano la versione specifica degli ATM in uso presso il proprio istituto e dei 20.000 PIN, il 10% riguarda proprie carte) , rappresentata principalmente dalla capacità di quest'ultima di fornire un'informazione **analizzata, contestualizzata, tempestiva, accurata, rilevante e predittiva**, rispetto ad avere singole informazioni "atomiche".

Threat intelligence is evidence-based knowledge (e.g.,context, mechanisms, indicators, implications and action-oriented advice) about existing or emerging menaces or hazards to assets. - Gartner 2016



AMBITI DI UTILIZZO

Security Operation Center (SOC)
Informazioni (con o senza piattaforma) tra cui: warning per attacchi targettizzati, IoC, blacklist, data breach noti, vulnerabilità recenti, etc

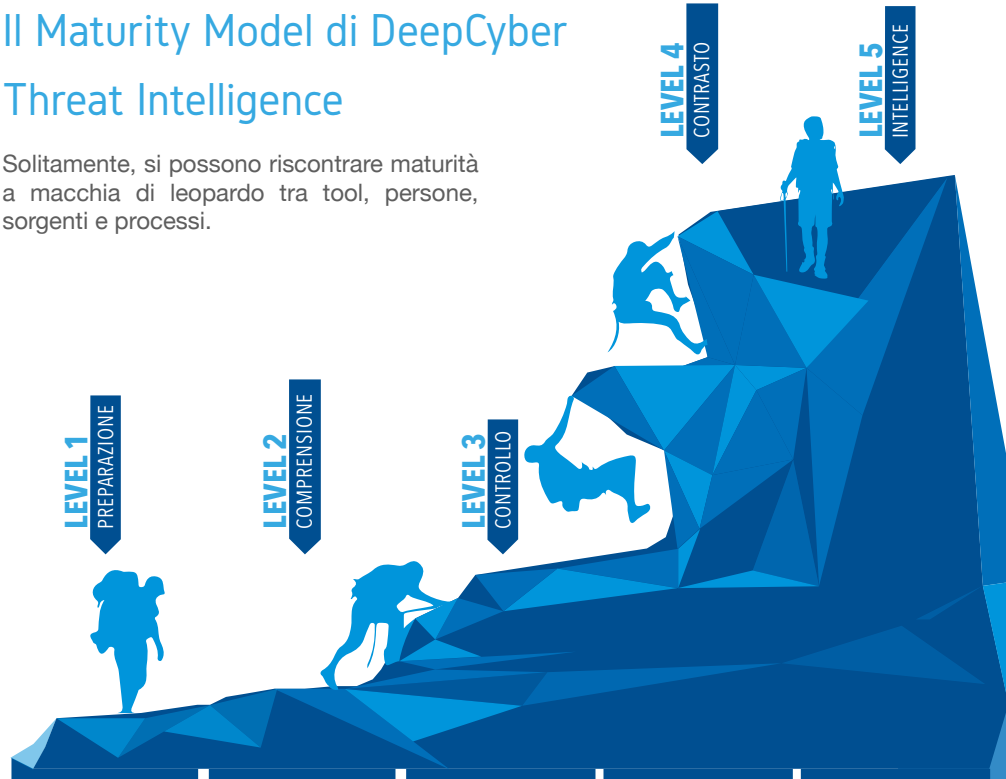
Anti-Fraud
Informazioni (con o senza piattaforma) legate al phishing, monitoraggio sul mercato nero di carte di credito clonate, e-commerce fraud, atm skimming etc.

AML
Informazioni (con o senza piattaforma) legate ai soggetti utilizzati come «muli» per il riciclaggio.

Reputation
Informazioni (con o senza piattaforma) su «sentiment» negativi in termini di sicurezza e frodi sui social network e web, report customizzati per gli «executive», alert via sms/email.

Il Maturity Model di DeepCyber Threat Intelligence

Solitamente, si possono riscontrare maturità a macchia di leopardo tra tool, persone, sorgenti e processi.

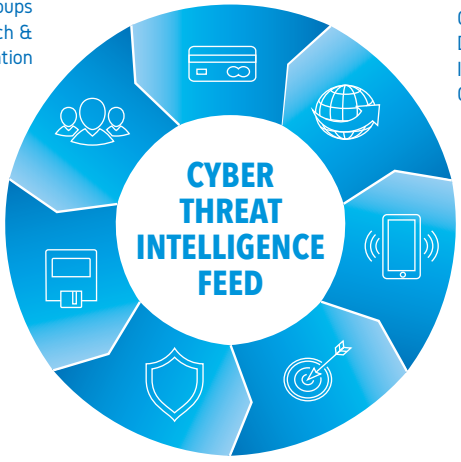


	LEVEL 1 PREPARAZIONE	LEVEL 2 COMPRENSIONE	LEVEL 3 CONTROLLO	LEVEL 4 CONTRASTO	LEVEL 5 INTELLIGENCE
TOOL	SIEM	SIEM	Security Analytics	Portali di threat intelligence	Threat Intelligence Platform
PERSONE		Analista di Cyber Threat	Team di Cyber Threat	Team esperto di Cyber Threat	Team esperto di Cyber Threat
SORGENTI	Uso di IoC	OSINT	Feeds e Componente di TI Tattica	Feeds e Componente di TI Tattica	Componente di TI Tattica e Strategica e fonti interne
PROCESSI	Assenza di correlazione	Security Monitoring e Incident Response	Security Monitoring, IR, Security Engineering	Security Monitoring, IR, Security Engineering e data fusion	Programma di TI, Predisposizione di un I-SOC

Fraud Analysis & AML
Leaked Corporate Accounts
Compromised Customer Accounts
Compromised Bank Cards
Money Mule Information
Compromised IMEI
AML Information

Social Networks
Social Networks Profiles
Search for People or Groups
Email Address Search & Correlation

Network Infrastructure
ICS-SCADA Vulns
Compromised SSL Certificate
Compromised or Infected Host
Data Heatmap
IP Addresses History
Geolocation Info



Physical Security
Critical Infrastructure
Geo-political conflict
ATM Infrastructure
IoT Threat & Weakness

SYSTEM & MOBILE MALWARE
CVE - Zero Day
Malware Details
Suspicius IP Addresses
Malware Components
Hashes' Payload
Exploited Vulnerability

BRAND REPUTATION
Domain Info & Reputation
Brand Reputation
Counterfeitting
Digital Piracy
Site Forgery
Cybersquatting

BAD ACTORS
Bad Actors Attributes
Attack's Target
Adversary Tactics, Tools & Procedures
Espionage Campaign

I Feed nella Cyber Threat Intelligence

I feed sono il primo valore della Threat Intelligence, sono le informazioni di base, disponibili in formato «grezzo» o più «strutturato».


DEEPCYBER
ADVANCED INTELLIGENCE PROTECTION ANTIFRAUD.
Offerta di Cyber Threat Intelligence

I nostri servizi di Cyber Threat Intelligence

ADVANCED INTELLIGENCE

- Supporto nell'individuazione delle fonti informative e reporting sulle potenziali minacce in ambito government, defence, financial services e critical infrastructure (data breaches account, carte di credito su deep e dark web, AML account, etc).
- Monitoraggio del deep e dark web dei domini, classi IP, informazioni di interesse a tutela del brand del cliente.
- Malware intelligence su minacce targettizzate per il mondo government, defence, financial services e critical infrastructure, con focus specifico sul cliente.

TECHNOLOGY

- Selezione, progettazione e realizzazione di piattaforme di Cyber Threat Intelligence (TIP) per la prevenzione e identificazione «intelligence driven» delle minacce interne e esterne, ad integrazione rispetto alle tecnologie esistenti.

PROACTIVE HUNTING

- Supporto all'identificazione ed al contrasto delle cyber minacce, in modalità Knowledge as a services.
- Integrazione di knowledge di secondo livello nel SOC, Anti-Fraud Center o in altre strutture di analisi e risposta agli eventi e/o incidenti. Con l'ausilio di partner trusted, outsourcing end to end di I-SOC e/o I-Anti-Fraud Center.

ADVANCED LEARNING

- Formazione avanzata per la prevenzione, identificazione e gestione delle minacce Cyber, anche mediante l'ausilio di «simulatori» di ultima generazione, per cyber-attacchi o campagne di phishing supervisionate.

Servizio di reporting su base mensile o trimestrale sulle principali minacce sul surface, deep e dark web

Servizio di monitoring personalizzato sulle principali minacce sul surface, deep, dark web e livello reputazionale del cliente

Servizio di supporto per l'acquisizione e l'utilizzo di Feed e piattaforme di Cyber Threat Intelligence.

Chi siamo

DeepCyber aiuta i propri clienti nell'accrescere l'efficacia al contrasto delle «Cyber threat», con un approccio «intelligence driven».

DeepCyber ed il suo team di esperti supporta i propri clienti in un processo di sviluppo delle proprie «capability» di proactive detection & response su Cyber Threat Intelligence, Protection e Antifraud.

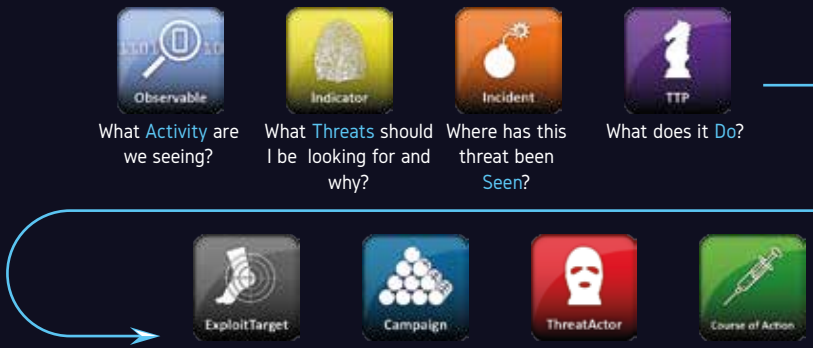
Per quanto concerne la Cyber Threat Intelligence, DeepCyber propone una metodologia finalizzata al «data fusion» attraverso l'utilizzo delle diverse fonti informative, interne ed esterne, derivanti altresì da un network specializzato, a livello mondiale su USA, Cina, Russia, Israele oltre che Italia.

Contattaci

DeepCyber S.r.l - Piazzale Sturzo nr. 15 – 00144 Rome - Italy
info@deepcyber.it - www.deepcyber.it

Gli standard internazionali di cyber threat intelligence: l'uso di STIX/TAXII

DeepCyber incoraggia l'utilizzo del linguaggio STIX, che è stato progettato per fornire maggiore contesto alla minaccia cyber , attraverso l'integrazione di modelli osservabili, in grado di coprire l'intera gamma di informazioni necessarie. Il linguaggio utilizza l'XML per definire il contesto relativi alla minaccia ed utilizza diversi costrutti :



Il protocollo di comunicazione TAXII fornisce un meccanismo di trasporto per lo scambio nell'ambito della cyber Intelligence in modo sicuro e automatizzato.