
NEW THREATS EVOLVE, READY TO GO DEEP
DEEPCYBER

Summary

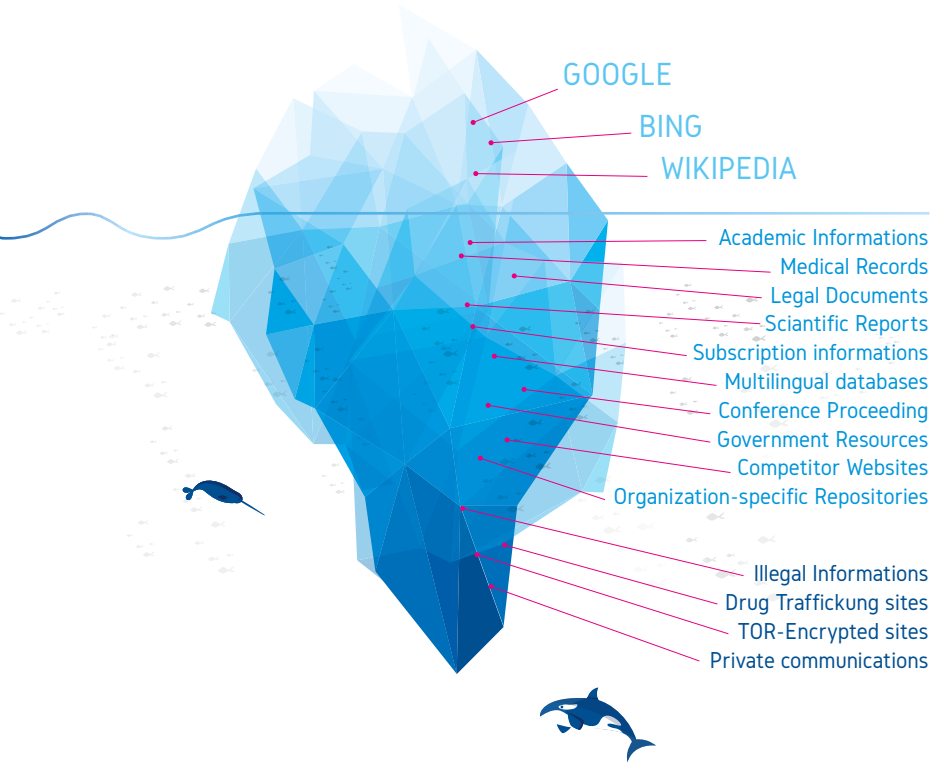
The threat landscape is constantly evolving and the transboundary nature of attack requires an integrated approach, tactical and strategic, enabling all possible channels, including the Web environment and in particular the Deepweb and Darkweb.

“Intelligence Driven” approach is the most effective way to reduce the time and more generally to have a good "Situational Awareness" about what is happening in cyber international scenario.

What is the Cyber Threat Intelligence

There is a substantial difference between (Cyber) Threat Data (i.e dump of data of ATMs compromised and 20,000 BIN cards) and Threat Intelligence (i.e these data, some related to specific version of ATMs in a financial institute and 20,000 PINs are related to 10% of their cards), represented mainly the ability of provide an **analyzed, contextualized, timely, accurate, relevant and predictive** information, than to have a single "atomic“ information.

> *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*



USE CASES

Security Operation Center (SOC)
Information (with or without platform) about warning on custom attack, IoC, Blacklist, mains data breach, recently vulnerability, etc.

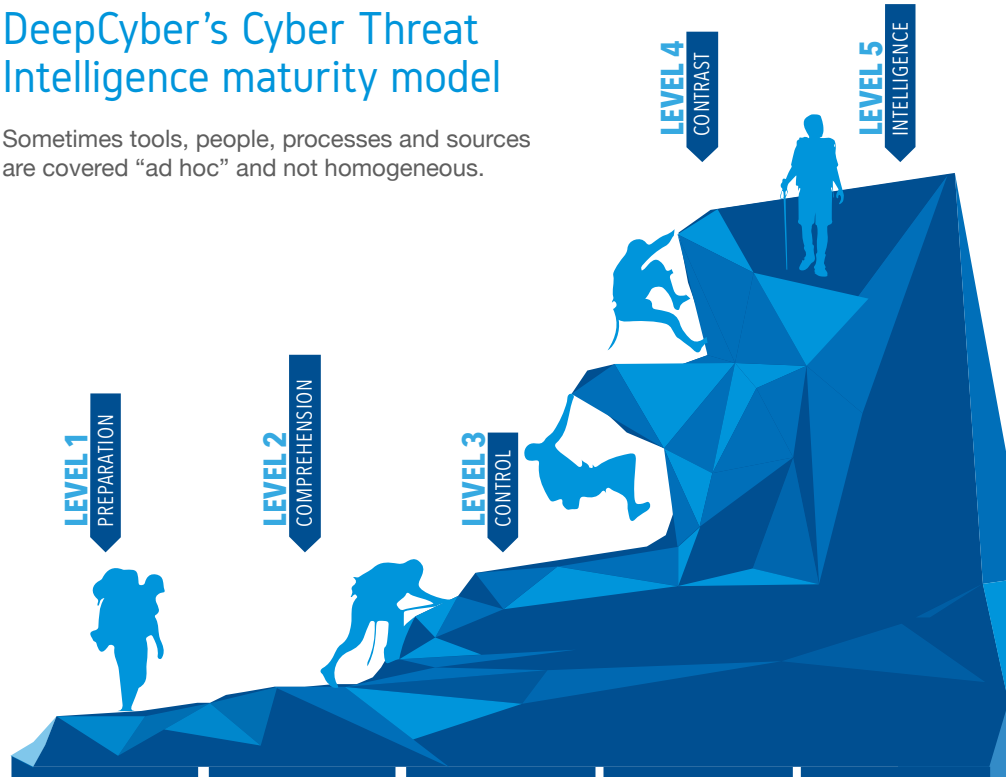
Anti-Fraud
Information (with or without platform) about phishing, monitoring of credit cards on black market, commercial fraud, atm skimming, etc.

AML
Information (with or without platform) about «money mules» for antimoneylaundering.

Reputation
Information (with or without platform) about negative «sentiment» in terms of security and fraud on social networks and web, custom reports for «executive», alert by sms / e-mail.

DeepCyber's Cyber Threat Intelligence maturity model

Sometimes tools, people, processes and sources are covered "ad hoc" and not homogeneous.

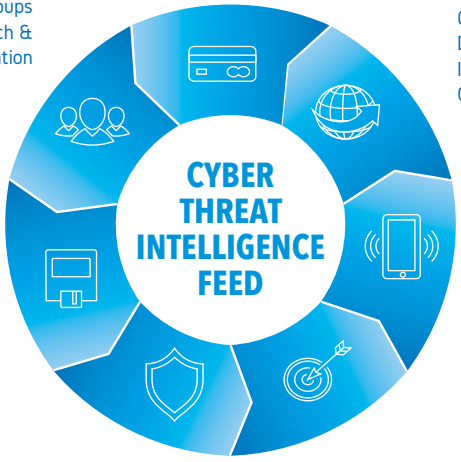


	LEVEL 1 PREPARATION	LEVEL 2 COMPREHENSION	LEVEL 3 CONTROL	LEVEL 4 CONTRAST	LEVEL 5 INTELLIGENCE
TOOL	SIEM	SIEM	Security Analytics	Threat intelligence Portal	Threat Intelligence Platform
PERSON		Threat Data Analyst	Threat Data Analyst team	Threat Data Analyst team	Threat Data Analyst team
SOURCE	Use of IoxC	OSINT	Feeds and Component of tactic TI	Feeds and Component of tactic TI	TI componentl Tactic and strategic Internal info
PROCESS	Without correlation	Security Monitoring , Incident Response	Security Monitoring, IR, Security Engineering	Security Monitoring, IR, Security Engineering data fusion	TI programme, ISOC

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

Feed on Cyber Threat Intelligence

Feeds are the first value of threat intelligence, they are the basic information, available in “raw" or "structured" format.


DEEPCYBER
ADVANCED INTELLIGENCE PROTECTION ANTIFRAUD.
Cyber Threat Intelligence Services

Our cyber threats intelligence

ADVANCED INTELLIGENCE

- Support in identifying sources of information and reporting on potential threats in government, defense, financial services and critical infrastructure environment (data breaches accounts, credit cards in deep and dark web, AML accounts, etc.).
- Domain/IP intelligence in deep and dark web, antiphishing, brand intelligence.
- Malware intelligence, Indicators of compromise, bad actors, etc.

TECHNOLOGY

- Selection, designing and implementation of Cyber Threat Intelligence platforms for prevention and identification of internal and external threats “intelligence driven”, to integration with existing technologies.

PROACTIVE HUNTING

- Support for identifying and fighting Cyber Threats, with Knowledge as a Services, for Integration in the SOC, Anti-Fraud Center or in other Analysis and Response organization for Events/incidents. Also with trusted partner is possible to offer end-to-end outsourcing of I-SOC and/or I-Anti-Fraud Center.

ADVANCED LEARNING

- Advanced training for Cyber threat prevention, identification and management, also with the help of ”last-generation” simulators, cyber-attacks environment or phishing supervised campaigns.

Monthly or quarterly reporting service for the major surface, deep & dark web threats

Custom monitoring service for the major threats on surface, deep, dark web and reputable customer level

Support for selecting, customizing and using the Feed and Threat Intelligence Platform

Who we are

DeepCyber helps its customers to increase the effectiveness of cyber threat defense, with an "intelligence driven" approach.

DeepCyber and his expert team, supports its customers trough a process development of their proactive, detection and response "capability" of Cyber Threat Intelligence, Protection and Antifraud.

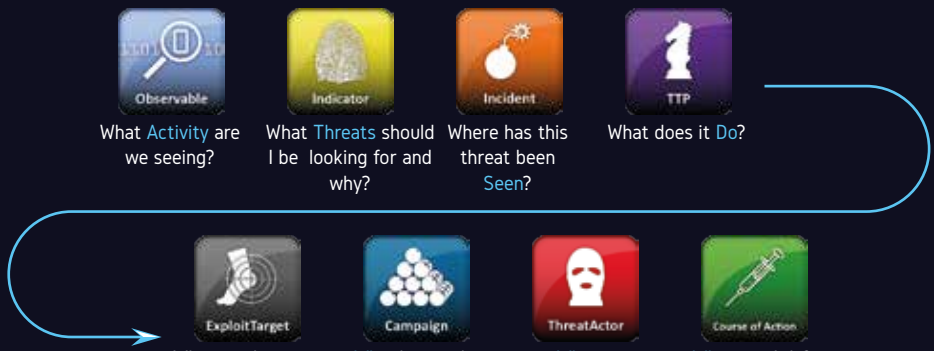
Regarding the Cyber Threat Intelligence, Deep Cyber use a methodology aimed to "data fusion", able to use different information sources, internal and external, to get from a world network, such as USA, China, Russia, Israel and Italy.

Contact us

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

Cyber Threat Intelligence International Standard : STIX/TAXII

DeepCyber encourages the use of the STIX language, which is designed to provide major contexts to cyber threats, through the integration of observable models in order to cover all range of necessary information. Language uses is XML to define the context related to threat :



The TAXII communication protocol provides a secure and automated exchange mechanism for Cyber Intelligence.