

Cyber Threat Intelligence Platform - TS Intelligence

Managed Detection & Response - iSOC

The screenshot displays the TS Intelligence platform interface. On the left is a dark sidebar menu with sections: Dashboard, INSIGHT (Reports, Custom Reports), THREATS (Avversari, Eventi IOC), and RISORSE (Favoriti, Tickets, Documentazione, API Doc, Changelog). The main content area is titled 'Threats / Avversari' and features two threat profiles:

- ALPHV Team**: Alias: BlackCat Team, Noderus. Description: 'ALPHV Team è un gruppo di tipo Cyber Crime attivo almeno dal 2021. L'avversario prende di mira molteplici organizzazioni di diversi settori attraverso attacchi ransomware basati sull'omonima minaccia. ALPHV Team ha attivato un portale per il rilascio delle informazioni sottratte alle vittime insolventi. La minaccia utilizzata dal gruppo è un ransomware di tipo human-driven distribuito in seguito alla compromissione della rete e alla sua mappatura.'
- Anonymous Sudan**: Alias: Storm-1359. Description: 'Anonymous Sudan è un gruppo attivo dal gennaio 2023 che si definisce hacktivista e composto da membri sudanesi. In realtà, l'avversario ha quasi certamente una matrice russa e mostra vicinanza alle istanze del Cremlino. Il gruppo colpisce attraverso offensive di tipo CNA (Computer




On the right, there is a world map with red markers and a 'Reset' button. Below the map are three filter panels: 'Continenti' (Ex Unione Sovietica), 'Nazioni' (Bielorussia, Ucraina, Russia), and 'Aree' (Government, Defense/Military, Energy, Finance, Infrastructures).

Nowadays organizations operate in unpredictable scenarios and have to face more and more articulated, correlated and invasive phenomena. Providing the right tools to incident responders and cyber security decision makers is crucial.

Cyber Threat Intelligence platform allows quick access to validated relevant information, supporting security teams in deploying the best defense strategy.

TS-Intelligence Service

TS-Intelligence service is provided through the subscription to a proprietary Cyber Threat intelligence platform which delivers data useful for preventive and predictive cyber defence activities and measures. The service articulates in:

-  **Data Collection, Validation, Correlation and Contestualization of information on global threats, actors, methodologies and cyber incidents**
-  **Production and transmission of information streams (feed) Machine to Machine for interfacing with SIEM and/or similar perimeter monitoring technologies**
-  **Proprietary Dashboard which provides intuitive access to information and technical data on a global level.**

Distinctive features

- **OSINT and CLOSINT sources**
- **White, green, amber and red Reports & Feeds**
- **Full API**
- **M2M and MISP to MISP Integration**
- **Unlimited number of users**
- **More than 300 monitored APT profiles:** including general description, target industries, used tools, exploits, events, rules for detection
- **Insight report with indicators of compromise (IoC) validated and historicized in relation to APT Threats and Structured Crime**
- **Constant specialized analyst support** accessible directly from the dashboard
- **Daily news and reports** on adversaries, ongoing or emerging campaign, malware sample and detection rules

Optional add-on for a tailored offer

Brand & VIPs Tailored Monitoring

Cyber risk exposure monitoring for own brand and/or VIPs

Dark & Underground Tailored Monitoring

Active darknet monitoring to trace attacks to own infrastructure: fraud domain registration monitoring, black market check for dump and data breach

Red Line

Instant messaging hotline. A virtual meeting space for validation, further information and deep diving on technical data

Supply Chain Monitoring

Cyber risk exposure monitoring for supply chain

On Demand Investigation Ticket

Dedicated team with vertical competences and skills to analyze technological data specific of customer domain

Incident Response & Threat Hunting

Vertical professional activity for detection and response of cyber attacks for both APT or cybercrime

Executive Report

Executive (CSO/CISO) monthly report summarizing main cyber threats

Strategic Report

Geopolitical monthly report to provide both a complete scenario overview and details on the interests pursued by state or state sponsored (APT) adversaries



A TIM ENTERPRISE BRAND



telsy.com

contact@telsy.it

2024 © Telsy - All rights reserved