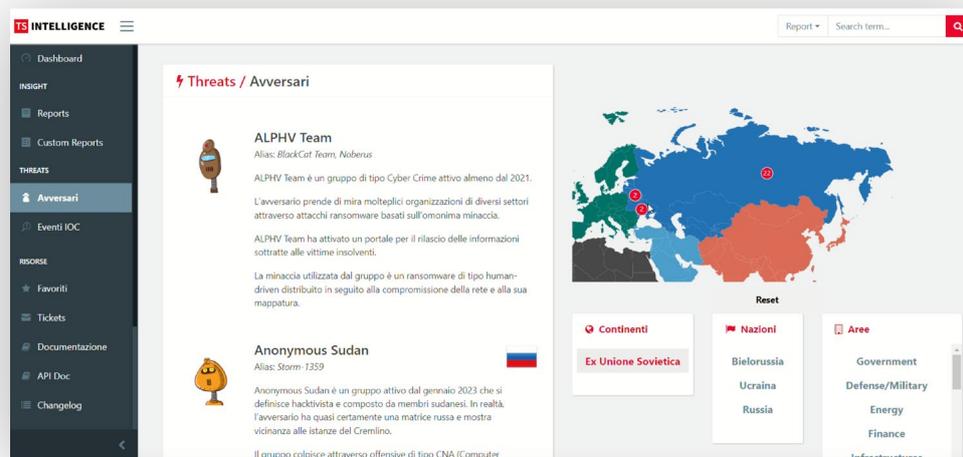


Cyber Threat Intelligence Platform - TS Intelligence

Managed Detection & Response - iSOC



Oggi le organizzazioni operano in ambienti imprevedibili e devono affrontare fenomeni sempre più articolati, correlati ed invasivi. È fondamentale dotarsi di strumenti in grado di valorizzare i dati interni ed esterni mettendoli al servizio degli incident responder e dei decisori di cyber sicurezza. La Cyber Threat Intelligence consente di analizzare e validare tempestivamente le informazioni rilevanti, supportando i team di sicurezza nell'attuazione delle strategie di difesa più efficaci.

Il servizio di TS-Intelligence

Il servizio fornisce una piattaforma di Cyber Threat Intelligence chiamata TS-Intelligence utile a supportare le attività e le decisioni di cyber-difesa preventiva e predittiva.



Attività di raccolta, validazione, correlazione e contestualizzazione delle informazioni in ambito globale su minacce, attori, metodologie ed incidenti cyber



Produzione ed invio di flussi informativi (feed): stream di dati (Machine to Machine) da caricare sul SIEM e/o tecnologie perimetrali



Dashboard proprietaria che mostra in maniera intuitiva le informazioni e i dati tecnici a livello globale

Caratteristiche distintive

- Fonti **OSINT** e **CLOSINT**
- **Report & Feed white, green, amber e red**
- **Full API**
- Integrazione **M2M** e **MISP to MISP**
- **Utenze illimitate**
- Più di **300 profili di APT monitorati**: descrizione, settori target, tools utilizzati, exploits, eventi, regole per la detection
- **Insight report** con **indicatori di compromissione (IoC)** validati e storicizzati rispetto alle **minacce APT** e **StructuredCrime**
- La possibilità di usufruire del **supporto costante di analisti specializzati** attivabile direttamente dalla dashboard
- **News e report quotidiani** in lingua italiana su avversari, campagne in corso o emergenti, malware sample e regole di detection

Optional add-on per offerta custom

Brand & VIPs Tailored Monitoring

Monitoraggio dell'esposizione a rischi cyber in riferimento al proprio brand e/o VIPs

Dark & Underground Tailored Monitoring

Monitoraggio attivo della darknet per rintracciare attacchi alle proprie infrastrutture: monitoraggio della registrazione di domini fraudolenti, controllo di Dump e Data Breach nei black market

Red Line

Filo diretto in instant messaging. È uno spazio virtuale di confronto per validazione, arricchimento ed approfondimento di dati tecnici

Supply Chain Monitoring

Monitoraggio dell'esposizione a minacce cyber dei propri fornitori e del proprio brand

Investigation Ticket on Demand

Disponibilità di un team con verticalità specifiche per analizzare dati tecnologici specifici all'interno del proprio dominio

Incident Response & Threat Hunting

Attività professionale verticale per la detection e la risposta ad attacchi informatici sia di tipo cybercrime che di tipo APT

Executive Report

Report mensile per gli executive (CSO/CISO) che riassume le principali minacce cibernetiche

Strategic Report

Report mensile di tipo geopolitico finalizzato a fornire uno scenario completo e di dettaglio degli interessi perseguiti da avversari statuali o sponsorizzati da stati (APT)



A TIM ENTERPRISE BRAND



telsy.com

contact@telsy.it

2023 © Telsy - Tutti i diritti riservati