TS-Intelligence

Cyber threat intelligence per anticipare le minacce emergenti e proteggere la tua organizzazione

Gli Advanced Persistent Threat (APT) sono tra i problemi più seri che le organizzazioni devono affrontare oggi. Il gap tra l'aumento delle capacità di attacco da parte di avversari strutturati e quelle di difesa di istituzioni e aziende è in aumento e le attività tradizionali di sicurezza sono costantemente raggirate da armi digitali spesso inedite, in un contesto informativo geopolitico estremamente complesso. Con il numero crescente di minacce non rilevate dai normali sistemi di sicurezza la maggior parte dei team si trova nella condizione di dover combattere un avversario non noto. Talvolta le minacce non vengono identificate e le misure protettive inadeguate. Ciò si traduce in una postura di sicurezza prevalentemente reattiva e inefficace contro le minacce persistenti e gli avversari strutturati. L'integrazione della **cyber threat intelligence** nei programmi di sicurezza non solo fornisce un vantaggio contro queste minacce, ma anche il contesto reale in cui esse operano, per attuare decisioni migliori in termini difensivi. **TS-WAY è pioniera in questo specifico settore in Italia**. **Esperienza decennale**, **metodologia investigativa** e un **pool di professionisti** di grande esperienza nell'ambito della cyber threat intelligence e nella risposta ad incidenti informatici, oggi sono a disposizione di organizzazioni del mondo della finanza, telecomunicazioni, governo, difesa, trasporti, e chiunque sia alle prese con problemi cogenti di sicurezza.

TS-Intelligence è la soluzione di **cyber threat intelligence** di TS-WAY per la **difesa preventiva, predittiva e di contesto da minacce informatiche inedite ed emergenti**. In TS-Intelligence c'è tutto il necessario per l'allineamento del programma di sicurezza di un'organizzazione agli obiettivi di gestione dei rischi che si è prefissata.

REPORT STRUTTURATI

Executive summary e **report strutturati in lingua italiana**, organizzati per genesi, assessment e contesto, in merito alle minacce cibernetiche inedite ed emergenti, aiutano a comprendere lo scenario globale di rischio e quello specifico per la propria organizzazione.

PROFILO DEGLI AVVERSARI

Una minuziosa analisi degli avversari censisce le loro attività, capacità e caratteristiche, le armi digitali, gli strumenti e gli impianti malware in una unica scheda tipologica. **Conoscere il proprio nemico** assume un ruolo fondamentale per migliorare ed implementare le proprie politiche di protezione ed analisi.

ACTIONABLE INTELLIGENCE

Indicatori di compromissione tecnici costantemente aggiornati e contestualizzati rispetto agli avversari ed alle loro campagne malevole, rendono possibile **l'identificazione o il blocco di minacce pubblicamente note, inedite ed emergenti**, fungendo da intelligenza tecnica per gli strumenti già presenti all'interno della propria organizzazione.

CYBER INTELLIGENCE OPERATIONS CENTER

Un **pool di esperti** che analizza costantemente le caratteristiche degli attaccanti per anticiparne intenzioni e risultati, **pronto ad intervenire in caso di attacco**.

I 4 PIANI DI TS-INTELLIGENCE

	START-UP	START-UP FOCUSED	ADVANCED	ADVANCED FOCUSED
INTELLIGENCE DASHBOARD	✓	✓	✓	✓
PROFILI DEGLI AVVERSARI	✓	✓	✓	✓
REGOLE DI DETECTION YARA, SURICATA, SNORT, BRO	✓	✓	✓	✓
REPORT ED INDICATORI SU MINACCE CIBERNETICHE EMERGENTI OSINT (TLP WHITE, GREEN)	✓	✓	✓	✓
REPORT ED INDICATORI SU MINACCE CIBERNETICHE INEDITE CLOSINT (AMBER, RED)			✓	✓
TICKET INVESTIGATIVI ON-DEMAND SPENDIBILI/ANNO			**10**	**ILLIMITATI (1 FTE)**
ACCESSO PRIORITARIO AI TICKET DI SUPPORTO INVESTIGATIVO			✓	✓
INGAGGIO PRIORITARIO DEL TEAM PER INCIDENT RESPONSE			✓	✓
MONITORAGGIO MIRATO DI MINACCE SPECIFICHE PER LA PROPRIA ORGANIZZAZIONE		**OSINT**		**OSINT E CLOSINT**
INCIDENT RESPONSE (GIORNI UOMO)			**10**	**10**
ACCESSO API ILLIMITATO			✓	✓

FEATURES

- **Executive summary** e **report strutturati in lingua italiana,** per genesi, assessment e contesto
- **Indicatori di compromissione**: malware C2, hash di malware, phishing, documenti malevoli e spear-phishing, regole yara per la detection di file malevoli, regole suricata/snort/bro per sonde di rete, domini ed URL malevoli, IPv4 malevoli, VPN e Proxy IPv4, Tor Exit Nodes IPv4
- **110+ profili di avversari** strutturati, vigilati costantemente e schedati
- **Monitoraggio** su misura dell'organizzazione cliente all'**esterno del proprio perimetro**: monitoraggio routing BGP, esposizione di vulnerabilità perimetrali, monitoraggio social media e web, ricerca di data breach (black market), domini registrati da attaccanti per sfruttare il brand per fini malevoli
- Implementazione rapida ed efficace, **non richiede formazione** o cambiamenti architetturali
- **Sincronizzazione degli indicatori di compromissione** nativa con istanze MISP
- **API** con supporto STIX / TAXII per facilitare la condivisione delle informazioni e la collaborazione con strumenti tecnologici di terze parti o custom.
- Abbonamento annuale, **numero illimitato di query**
- **Filo diretto con gli analisti** di TS-WAY per approfondimenti sui report pubblicati
- Ingaggio del Cyber Intelligence Operations Center per **analisi specifiche** su spearphishing, IPv4 o domini sospetti, attività investigative custom su fenomeni specifici e delineati
- Ingaggio del **team di risposta agli incidenti informatici** per individuare le cause, comprenderne la portata e supportare le attività di remediation

TS WAY

Indipendente, italiana, specializzata in cyber threat intelligence, TS-WAY è un'azienda che sviluppa sistemi, tecnologie e metodi di collaborazione con un approccio alla sicurezza completo a garanzia della continuità del business dei propri clienti.
Un pool di professionisti con esperienza riconosciuta in consessi internazionali, avvalorata da grandi gruppi privati nei comparti finanza, energia, telecomunicazioni e da organizzazioni governative e militari.

MEMBRI PERMANENTI DELL'ORGANIZZAZIONE TRUSTED INTRODUCER

ADERENTI ALL'EUROPEAN ELECTRONIC CRIME TASK FORCE

COMPONENTI DELLA ARMED FORCES COMMUNICATIONS AND ELECTRONICS ASSOCIATION

MEMBRI DELLA FONDAZIONE ICSA (INTELLIGENCE CULTURE AND STRATEGIC ANALYSIS)

TS-WAY srl, Piazza Monte Rosa 33 int. 6, Orvieto (TR), Italy T. +39 0763.340498 www.ts-way.com