

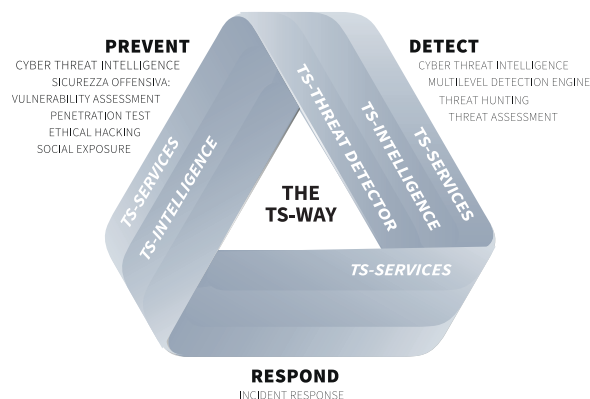
THE RIGHT

WAY

to defend your organization

Il 2017 è stato “l’anno del trionfo del malware, degli attacchi industrializzati realizzati su scala planetaria contro bersagli multipli e della definitiva discesa in campo degli Stati come attori di minaccia”. A dirlo è il rapporto Clusit che continua a dipingere uno scenario complesso, spaventoso, ormai endemico dell’era digitale. Un contesto che oggi obbliga le organizzazioni a tenerne conto prima di doverci fare i conti. Ma il gap tra l’aumento delle capacità di attacco dei criminali e quelle di difesa delle organizzazioni è in costante aumento e le attività tradizionali di cybersecurity, che fanno uso di sistemi di difesa collocati lungo il perimetro esterno delle organizzazioni, si stanno rilevando in parte inadeguate. Diventa urgente l’adozione di nuovi modelli e tecniche di difesa, nuove strade da percorrere che necessariamente partano tutte dallo stesso punto: la **sicurezza preventiva**.

In quel punto ci siamo noi. Continuiamo il percorso insieme.





DIFESA CIBERNETICA INTELLIGENCE DRIVEN

Anno di fondazione 2010, un'expertise in **cyber threat intelligence** unica nel panorama italiano, TS-WAY sviluppa sistemi, tecnologie e metodi di collaborazione per organizzazioni di medie e grandi dimensioni. Le sue soluzioni tecnologiche trasformano i dati delle minacce globali in informazioni di tipo strategico, tattico, operativo e tecnico, consentendo alle organizzazioni di risparmiare tempo e risorse, anticipare le minacce, comprenderne la portata e la natura potendo contare su un partner affidabile in caso di incidente informatico. Un approccio alla sicurezza preventivo ed estremamente completo a garanzia e tutela dei beni e della continuità del business. L'esperienza di TS-WAY è riconosciuta da grandi organizzazioni private nei comparti finanza, energia, telecomunicazioni, e da organizzazioni governative e militari che nel tempo hanno utilizzato i servizi di questa società indipendente, interamente italiana.



FONTI

TS-WAY dispone di un'ampia gamma di sorgenti informative costantemente aggiornate sulle minacce che vengono utilizzate per report (strategici, tattici, operativi e tecnici) in lingua italiana ed Indicatori di Compromissione (IOC). Questi dati consentono ai clienti l'attivazione dei propri sistemi difensivi per rendere possibile il riconoscimento delle minacce e l'eventuale blocco delle intrusioni. Le sorgenti informative di TS-WAY (OSINT, provenienti da fonti aperte, e CLOSINT, da fonti riservate, non accessibili pubblicamente) sono in larga parte esclusive e consentono di monitorare costantemente l'attività dei principali avversari strutturati che agiscono in rete.



TECNOLOGIE

TS-WAY presidia il ciclo di contrasto alle minacce cibernetiche complesse attraverso una consistente attività di ricerca e sviluppo. Questa si concretizza nella produzione di soluzioni capaci di identificare e monitorare minacce cibernetiche sia tradizionali che complesse ed inedite. Si tratta di sistemi che svolgono attività di gathering dal mondo esterno alle organizzazioni clienti, le analizzano in real time e le correlano attingendo a centinaia di fonti. I dati delle minacce globali vengono trasformati in informazioni mirate, predittive e attuabili che rilevano, identificano e aiutano a fermare le minacce persistenti.



EXPERTISE

Un pool di professionisti di altissimo profilo con skill tecnici, investigativi e di contesto. Un passato da istruttori OSCP (Offensive Security Certified Professional), responsabili e sviluppatori core della distribuzione professionale BackTrack Linux (ora Kali Linux), cofondatori del progetto "The Exploit Database". Questo è il team TS-WAY, che si configura come una effettiva estensione dell'organizzazione cliente, a supporto del team in house, sia per le attività informative e di investigazione, che per la risposta ad incidenti informatici (Incident Response) e per le attività di verifica della sicurezza tecnologica o umana (Servizi di Sicurezza Offensiva).

PERCHÉ TS-WAY

PRESIDIO

Anticipare le minacce offre un doppio vantaggio. In primo luogo, riduce al minimo i rischi fermando gli attacchi prima di un impatto significativo e in secondo luogo, elimina gli avvisi generati successivamente nel ciclo di vita dell'attacco, riducendo così il costo operativo dell'analisi. TS-WAY ha grande visibilità in tutto il ciclo di vita degli attacchi e può rilevare le minacce durante la fase di exploit, prima che l'attaccante abbia un punto d'appoggio nell'"ambiente vittima".

REPUTAZIONE

Ogni giorno operiamo a servizio dei Security Operations Center (SOC), per alert e blocco sul perimetro delle minacce. Forniamo ai Computer Emergency Response Team (CERT) una knowledge base sugli avversari per avere un quadro della situazione aggiornato in caso di incidente e orientare le attività di threat hunting e incident response. Partecipiamo nuclei di cyber threat intelligence per attività di analisi e vigilanza costante degli avversari, in relazione agli asset della propria organizzazione.

ESPERIENZA

L'esperienza di TS-WAY è riconosciuta in consessi nazionali ed internazionali a partire dalla sua fondazione. Si è ritagliata un ruolo di rilievo all'interno del panorama della cyber threat intelligence e della sicurezza offensiva da subito, coinvolta con i propri servizi e soluzioni in grandi eventi nazionali ed internazionali. TS-WAY è fornitore di importanti realtà governative, militari e law enforcement, di infrastrutture critiche nazionali e di realtà enterprise.



Membri permanenti dell'organizzazione Trusted Introducer, (CERT ed Incident Response Team Governativi Europei)



Aderenti all'European Electronic Crime Task Force (United States Secret Service, Ministero degli Interni e Poste Italiane)



Componenti della Armed Forces Communications and Electronics Association (AFCEA)



Membri della Fondazione ICSA (Intelligence culture and strategic analysis)