

Teleconsys



TCSHIELD: DA ZERO A COMPLIANT IN 30 GIORNI

Managed Security Services a protezione delle PMI

Mirko Leanza – 22/04/2024

INDICE

- Teleconsys in a Nutshell
- Scenario
- La suite TCshield
- Evoluzioni
- Contatti



24 ml€ Ordini
20 ml€ VdP

Teleconsys
Sharing Innovation

1,4 ml€ EBITDA
115 Dipendenti (+ di 150 in
totale)

CAGR VdP 2018/23: 19%

CAGR Risorse 2018/23: 24%



Digital Innovation Company

- PMI Innovativa dal 2019
- RSI ~ 4% VdP
- ISO 56002
- Open Innovation Network

4 Business Unit

- Digital Infrastructure
- Modern Application
- Cybersecurity
- Intelligent Services

Digital Deep Tech

- Digital ledger tech.
- Artificial intelligence
- extended Reality
- Quantum

Sustainability

- Bilancio dal 2021
- Fondaz. Sost. Digitale
- ISO 14001, 45001, 31000
- UNI Pdr 125

Generation

- Talent Growing Path
- Talent Academy
- Holacracy
- Intrapreneurship



INNOVATION CENTRIC CULTURE

INDICE

Teleconsys in a Nutshell

➤ Scenario

La suite TCshield

Evoluzioni

Contatti



Teleconsys

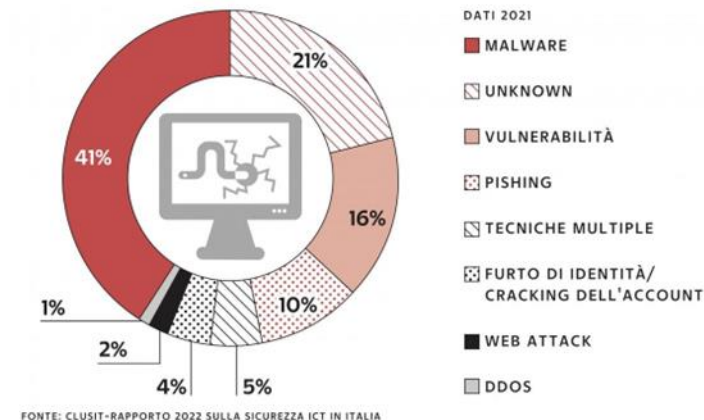
Premessa

La **sicurezza informatica** continua ad essere una fonte di preoccupazione per le imprese e non solo a causa delle crescenti tensioni internazionali e degli allarmi per l'avvio di possibili cyberwar

Negli ultimi 12 mesi molte aziende hanno subito **violazioni di reti e sistemi**, incorrendo in blocchi operativi o in sequestri di dati attraverso i famigerati ransomware, subendo pesanti richieste di riscatto

In molti casi si è trattato di violazioni che non sono state rilevate dai sistemi di sicurezza e dagli amministratori e che hanno lasciato i sistemi alla mercé dei criminali per scopi di diffusione del malware, di attacchi di Distributed Denial of Service (DDOS) o di sottrazione dei dati

LE PRINCIPALI TECNICHE DI ATTACCO INFORMatico



Le PMI nel mirino degli hacker

Uno dei principali motivi d'esposizione agli attacchi cyber è la **sottovalutazione del rischio**

Specie nelle **piccole e medie imprese** (PMI) che operano negli ambiti di produzione, in settori diversi da finanza e servizi critici, domina la falsa convinzione di non aver bisogno di protezioni, di non avere dati d'interesse per eventuali cybercriminali e, in caso di attacco, di potersi difendere con semplici backup

Al contrario, sono queste realtà a finire nel mirino dei cybercriminali, sia per il fatto d'essere **bersagli facili** sia perché sono gli anelli deboli di grandi supply chain dove condurre attacchi redditizi per le azioni criminali

Il report State of Ransomware 2022 di Sophos evidenzia come nel 2021, il 61% del campione delle PMI italiane prese in esame sia stato colpito da attacchi ransomware nell'ultimo anno

The State of Ransomware 2022

Findings from an independent, vendor-agnostic survey of 5,600 IT professionals in mid-sized organizations across 31 countries

Cyber Risk Self Assessment

Secondo lo studio Cyber Risk Self Assessment – autovalutazione del livello di sicurezza informatica delle PMI realizzato da Unindustria, Cini e Università Campus Bio-Medico di Roma (a cui ha collaborato anche Teleconsys) – l'Italia è uno dei Paesi più esposti, a livello internazionale, agli attacchi cyber per l'interesse verso il know-how e le filiere delle PMI

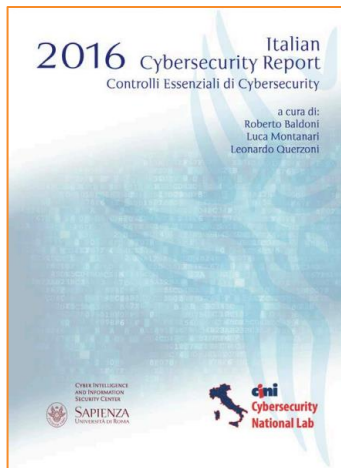
Dallo studio emerge che le principali **criticità** delle PMI nell'ambito della Cybersecurity riguardano le seguenti aree:

- **Formazione e consapevolezza:** l'inadeguata *cyber risks awareness* si traduce nella mancanza di attenzione verso il fattore umano
- **Gestione password e account:** una corretta gestione dei metodi di autenticazione è essenziale nella protezione dell'identità digitale e dei dispositivi a cui queste accedono
- **Protezione delle reti:** le reti devono essere adeguatamente protette per impedire l'accesso indiscriminato alle persone non autorizzate ai sistemi aziendali



Raccomandazioni e misure minime di sicurezza

L'esigenza di innalzare i livelli di sicurezza delle PMI, spina dorsale e prezioso humus per la crescita economica, sociale e culturale del Paese e attori imprescindibili di filiere produttive strategiche, è rappresentata in molteplici guide, sia nazionali che internazionali, contenenti raccomandazioni e misure minime di sicurezza che le stesse debbono o dovranno adottare



CINI



European DIGITAL SME Alliance



ENISA



NIS2

INDICE

Teleconsys in a Nutshell

Scenario

➤ La suite TCshield

Evoluzioni

Contatti



Teleconsys

TCshield: il servizio gestito per la sicurezza delle PMI

La suite di servizi di sicurezza **TCshield** nasce per soddisfare l'esigenza di più alti livelli di sicurezza e di rispetto delle compliance (es GDPR, HIPAA, PCI, SOX, NIS2,...) delle PMI sollevandole, nel contempo, dalla necessità di conoscere, aggiornarsi e gestire la cybersecurity

Estendendo il concetto di Servizio Gestito e focalizzandolo sulla sicurezza, Teleconsys offre un servizio innovativo che utilizza unicamente strumenti caratterizzati da:

- Zero deploy
- Zero hardware
- Subscription e/o Pay per Use

La sottoscrizione ad uno o più servizi dell'offerta TCshield porta un **beneficio immediato** a tutte quelle aziende che non possono acquistare e gestire piattaforme e strumenti in autonomia per le scarse competenze, lo staff insufficiente, la mancanza di consapevolezza dei propri dipendenti e un budget inadeguato



TCshield: disegnato per eliminare gran parte dei rischi

La suite TCshield propone, in modalità canone/pay per use, **servizi di sicurezza**, gestiti da un **team di esperti di cybersecurity** in possesso delle principali certificazioni di settore - su 4 degli aspetti fondamentali della sicurezza in ambito cyber

TCshield

SICUREZZA DELLA
AUTENTICAZIONE

SICUREZZA DELLA
NAVIGAZIONE

SICUREZZA DELLE
E-MAIL

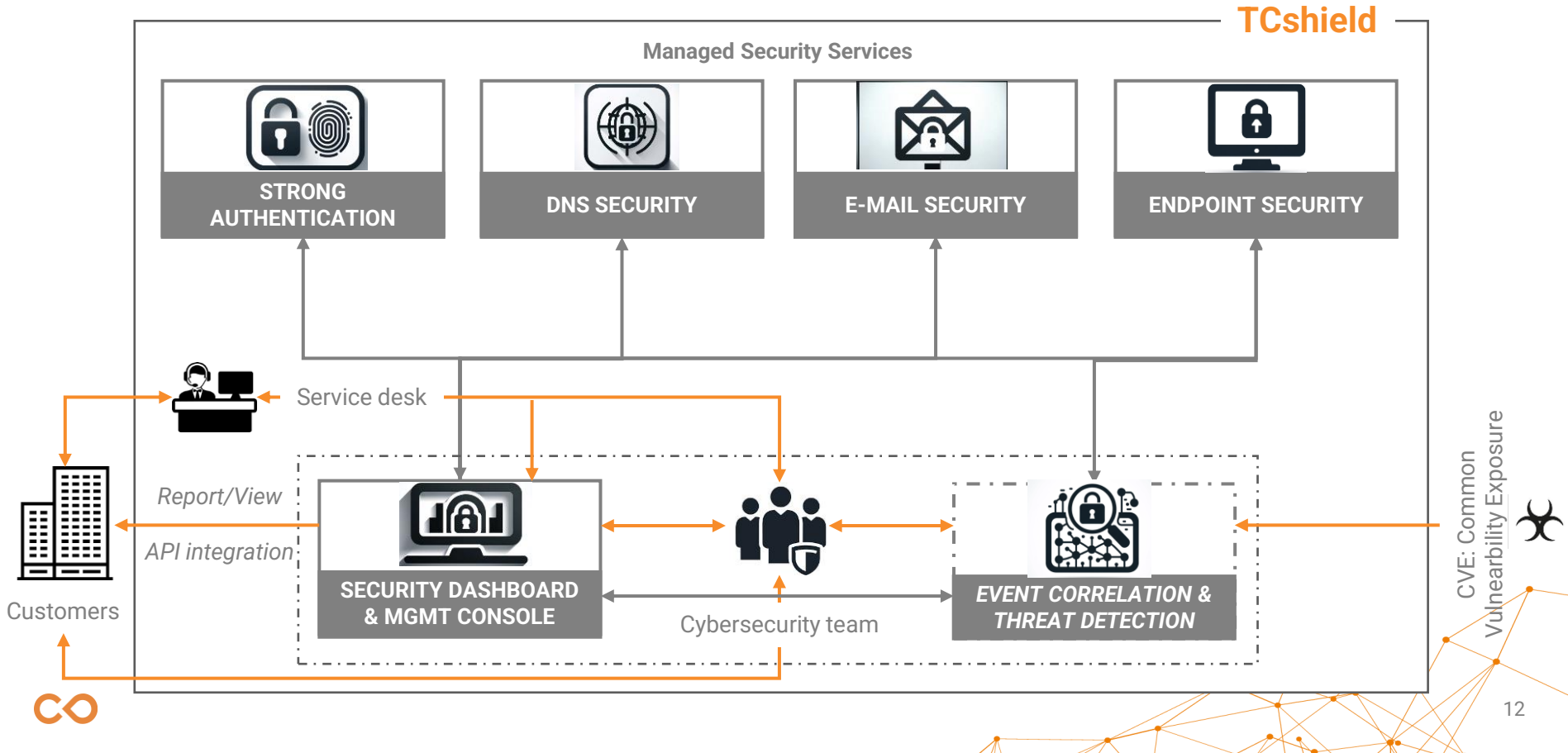
SICUREZZA SUGLI
ENDPOINT

Una organizzazione che acquista l'intero bundle di servizi riduce in maniera drastica i rischi cyber e minimizza, in caso di incidente, i tempi di risposta riducendone i potenziali danni

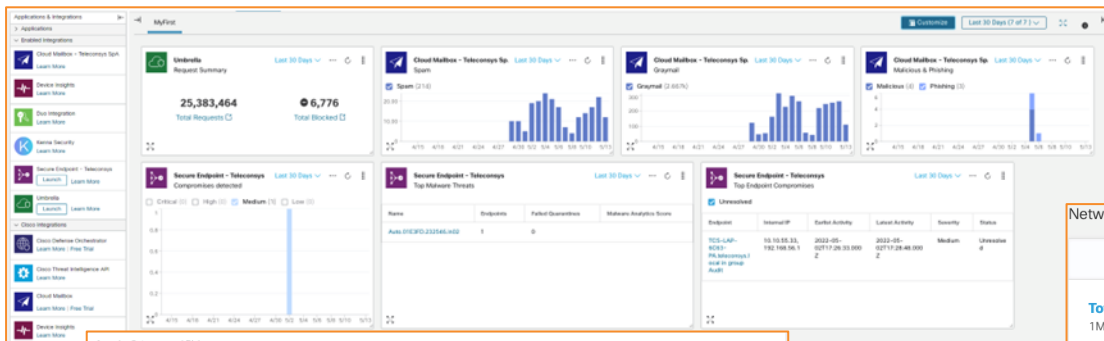
A questa offerta si aggiunge, inoltre, un servizio di **correlazione degli eventi** e **identificazione delle minacce**, potenziato da algoritmi di **intelligenza artificiale**, con cui è possibile innalzare ulteriormente i livelli di sicurezza passando ad un approccio predittivo/adattivo anziché reattivo



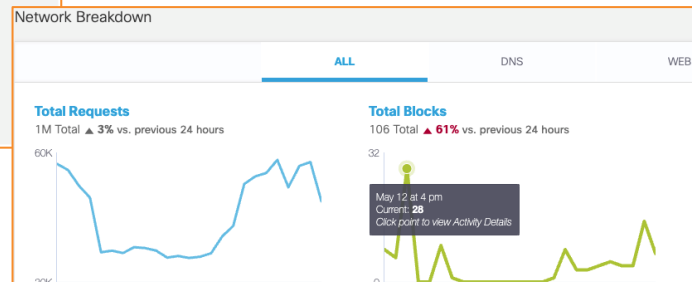
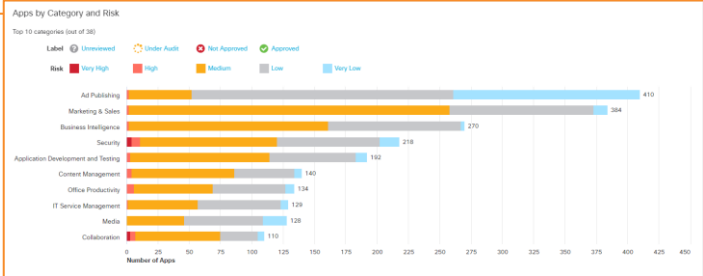
TCshield: una suite aperta, scalabile e integrabile



TCshield: Security dashboard & Management console

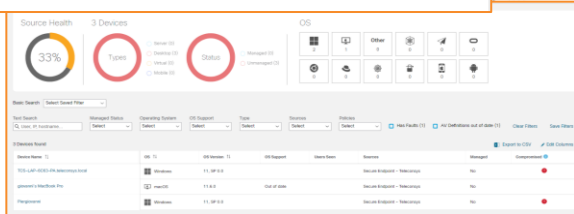


Security dashboard view (alcuni esempi)



Network Search (6 messages). Latest results as of: May 13 2022 04:54 PM GMT+2.

Verdict	Last Action	Message Rules	Received	Sender	Recipients	Subject
Malicious			May 05 2022 09:19 AM GMT+			FW: Invoice #15427
Phishing			May 05 2022 09:07 AM GMT+			FW: Invoice #15427
Spam			May 05 2022 08:52 AM GMT+			FW: Invoice #15427
Graymail			May 05 2022 08:43 AM GMT+			FW: Invoice #15427
Malicious			May 05 2022 08:43 AM GMT+			FW: Invoice #15427
Malicious			May 05 2022 08:04 AM GMT+			FW: Invoice #15427



TCshield: Cybersecurity team & Service desk

Cybersecurity team

Il gruppo di professionisti della sicurezza informatica che costituiscono il **Cybersecurity team** ha il compito di gestire i servizi di TCshield, seguendo un approccio che si fonda sul framework del NIST 2.0 (da cui quello nazionale):

- Governance
- Identificazione
- Protezione
- Rilevazione
- Risposta
- Ripristino

Il team ha anche il compito di definire con il cliente la migliore combinazione di servizi per le sue esigenze oltre a eventuali add-on custom

Service desk

Il **Service desk** ha il compito di gestire, secondo il framework ITIL 4, i clienti e i rispettivi utenti del servizio di sicurezza gestito TCshield

Tra i suoi principali compiti troviamo:

- l'attivazione/disattivazione di uno o più servizi che costituiscono l'offerta TCshield
- la gestione dell'account degli utenti che accedono alle dashboard/report e l'assistenza
- la segnalazione immediata di eventuali minacce e/o incidenti
- la ricezione di segnalazioni di malfunzionamenti e il relativo troubleshooting (TT)
- la creazione di reportistica ad-hoc
- ...

Certificazioni aziendali e del Cybersecurity team

Certificazioni aziendali

- ISO 27001:2022 - Sistema di gestione delle informazioni
- ISO 27017:2015: Controlli avanzati di sicurezza nel cloud
- ISO 27018:2016: Protezione delle informazioni personali nel cloud
- ISO 20000-1: Sistema di gestione dei servizi IT
- ISO 9001: Sistema di Gestione della qualità
- ISO 56002: Sistema di Gestione per l'innovazione
- ISO 45001 e 14001: Sistemi di Gestione della salute e sicurezza sul lavoro e l'ambiente
- ISO 31000: Sistema di Gestione del rischio
- UNI/PdR 125: parità di Genere

Certificazioni del Cybersecurity team

- Lead Auditor ISO 27001
- Lead Auditor ISO 22301
- CISA - Certified Information System Auditor
- CISM - Certified Information Security Manager ()
- CEH - Certified Etical Hacher
- CIH - Certified Incident Handler
- Certified Professionals Data Protection Officer
- CISPP
- CSX
- CC
- PMI, COBIT 5
- ITIL 4 Foundation



INDICE

Teleconsys in a Nutshell

Scenario

➤ La suite TCshield

Evoluzioni

Contatti



Teleconsys

TCshield risolve, in maniera estensiva, **i gap di sicurezza delle PMI** evidenziati dal Cyber Security Self Risk Assessment in collaborazione con Confindustria e Unindustria con tempi rapidi e a costi sostenibili, **innalzandone, immediatamente, i livelli di sicurezza** secondo le indicazioni contenute nelle principali guide nazionali ed internazionali (es. Framework nazionale, ENISA, NIS2)

Inoltre, tutti i prodotti che compongono la suite TCshield hanno caratteristiche ideali per il segmento delle PMI:

- sono prodotti di **livello enterprise**, "best of breed" nel settore della cybersecurity
- sono erogati in **modalità SaaS** e richiedono poco o nulla di attività di startup
- sono tutti a **subscription**, con una fee basata sul numero di utenti
- sono **integrabili** fra di loro e con soluzioni di terze parti
- sono **API based**, il che consente la costruzione di viste e report personalizzati, così da soddisfare le esigenze di business e regolatorie di ogni settore (es sanità, finanza, manifattura, automotive, ecc)



Esattamente come le minacce, i servizi di sicurezza gestiti che compongono la suite TCshield, come le competenze e le certificazioni del Cybersecurity team, sono in **costante sviluppo ed aggiornamento**

Ciò è indispensabile per contrastare la **continua e repentina evoluzione dei rischi** e soddisfare la revisione delle normative di settore (es la NIS), al fine di soddisfare le esigenze di quelle aziende che abbracciano processi di trasformazione digitale e di innovazione che, inevitabilmente, le costringono ad ampliare, in maniera significativa, la superficie d'attacco, rendendo sostanzialmente impossibile gestire in autonomia la cybersecurity

Affidare la propria sicurezza ai servizi gestiti TCshield significa poter disporre, costantemente, dei **migliori tool in circolazione** per la rilevazione, la risposta e la mitigazione di una minaccia o di un attacco e di un **team di professionisti della cybersecurity** in possesso delle più elevate competenze nel settore

Referenze e Vendor partnership

Referenze



Cybersecurity Establishment





Teleconsys

Sharing Innovation

Let's get started

Mirko Leanza
CISO & Responsabile BU Cyber
m.leanza@teleconsys.it
Teleconsys SpA
Via Groenlandia 31 - 00144 - Roma
+ 39 06 20396767
+ 39 06 92912491

Per informazioni e demo su TCshield
Gennaro Vuoso
Inside Sales
+39 342 852 3910
g.vuoso@teleconsys.it

www.teleconsys.it