INFOCERT
TINEXTA GROUP

TINEXTA CYBER

DEFENSYO

La protezione cyber per le PMI, senza complicazioni

INFOCERT
TINEXTA GROUP

PERCHÉ DEFENSYO?

Con l'entrata in vigore della **nuova normativa NIS 2**, l'adeguamento alla sicurezza informatica diventa una **necessità regolamentata.**

NIS 2 estende i suoi effetti non solo ai fornitori di servizi essenziali e digitali, ma anche a **tutte le realtà imprenditoriali che**, anche in minima parte, **fanno parte delle catene di fornitura.**

Oltre ai risvolti di carattere organizzativo, esistono **una serie di attività tecniche che le aziende devono garantire**, come:

- Anomaly Detection,
- Cyber Threat Intelligence,
- Monitoraggio dello stato di sicurezza

INFOCERT
TINEXTA GROUP

LA PROTEZIONE CYBER ACCESSIBILE IN LINEA CON LE ESIGENZE DI BUSINESS E NORMATIVE

DEFENSYO

Plug & play di facile utilizzo
DefensYo, frutto della tecnologia italiana, garantisce massima protezione cyber senza la necessità di personale specializzato, è un sistema plug and play pronto per essere utilizzato appena collegato

Sicurezza continua e predittiva
Aggiornamenti automatici in tempo reale tramite la Threat Intelligence di Tinexta Cyber, senza impattare la velocità dell'infrastruttura digitale.

Supporto proattivo
Unisce le funzionalità avanzate di Network Detection and Response (NDR) con le competenze ed eccellenze del Security Operation Center di Tinexta Cyber

1 Monitora la rete aziendale

2 Identifica le minacce

3 Blocca i rischi cyber

4 Protegge la tua azienda

INFOCERT
TINEXTA GROUP

COME FUNZIONA

DEFENSYO

Sonda NDR

Servizio di tipo Security Operation Center 5x8, in lingua italiana

Aggiornamenti applicativi e software [3 anni]

Accesso al portale di gestione e monitoraggio CSDC

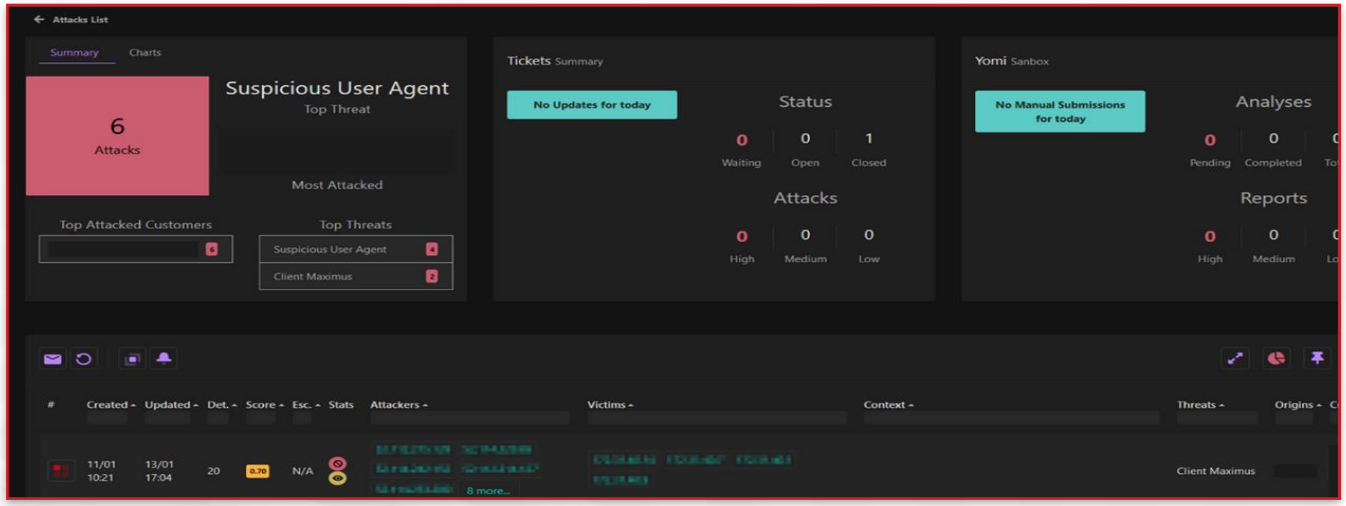
Software Defensyo per l'analisi del traffico e blocco automatico delle minacce

Utenze per l'accesso alla dashboard cloud di controllo e gestione della soluzione

Corso di Formazione

Defensyo ogni 15 minuti aggiorna in automatico le minacce in corso da monitorare attingendo alla Threat Intelligence del Polo Tinexta Cyber, con continuità senza interruzione del servizio.

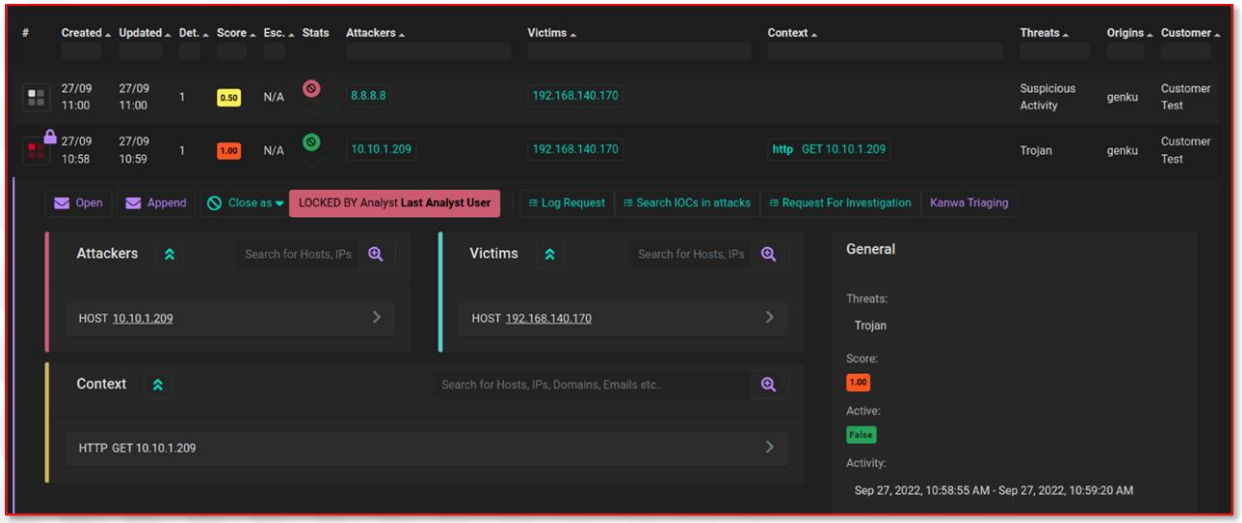
INFOCERT
TINEXTA GROUP



Schermata Defensyo:
Attack and Ticket summary

Schermata Defensyo:
Dashboard attacchi in corso

Schermata Defensyo:
Attack list



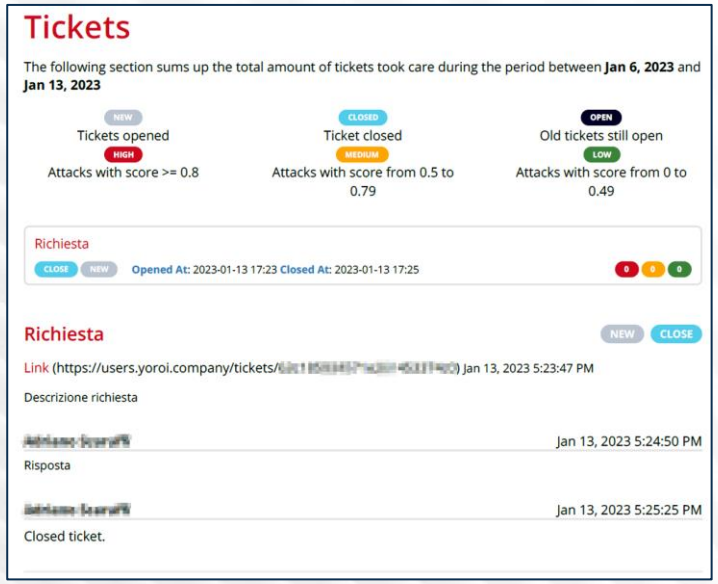
DEFENSYO

INFOCERT
TINEXTA GROUP

REPORT SETTIMANALI

Sintetizza le informazioni principali su:

- Indicatori di compromissione (IoC)
- Eventi analizzati ed attacchi bloccati
- Tickets Statics



Tickets

The following section sums up the total amount of tickets took care during the period between **Jan 6, 2023** and **Jan 13, 2023**

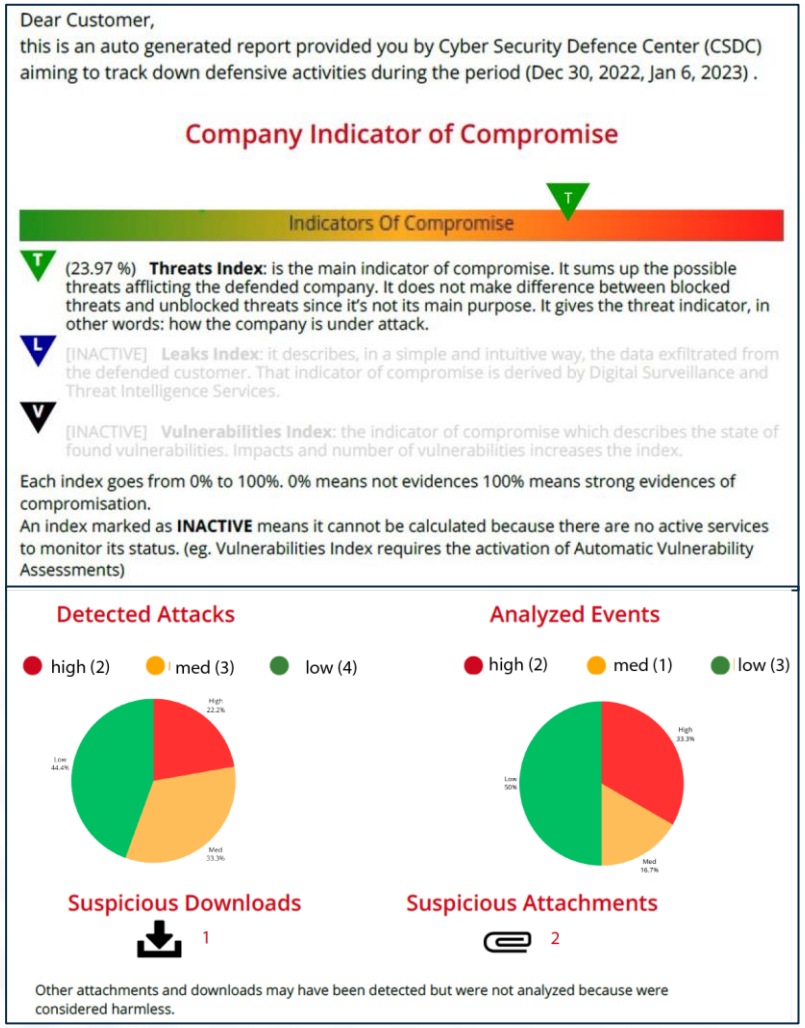
NEW — Tickets opened
HIGH — Attacks with score >= 0.8

CLOSED — Ticket closed
MEDIUM — Attacks with score from 0.5 to 0.79

OPEN — Old tickets still open
LOW — Attacks with score from 0 to 0.49

Richiesta
CLOSE NEW **Opened At:** 2023-01-13 17:23 **Closed At:** 2023-01-13 17:25 0 0 0

Richiesta NEW CLOSE
Link (https://users.yoroi.company/tickets/[redacted]) Jan 13, 2023 5:23:47 PM
Descrizione richiesta
[redacted] Jan 13, 2023 5:24:50 PM
Risposta
[redacted] Jan 13, 2023 5:25:25 PM
Closed ticket.



Dear Customer,
this is an auto generated report provided you by Cyber Security Defence Center (CSDC) aiming to track down defensive activities during the period (Dec 30, 2022, Jan 6, 2023) .

Company Indicator of Compromise

Indicators Of Compromise

(23.97 %) **Threats Index**: is the main indicator of compromise. It sums up the possible threats afflicting the defended company. It does not make difference between blocked threats and unblocked threats since it's not its main purpose. It gives the threat indicator, in other words: how the company is under attack.

[INACTIVE] **Leaks Index**: it describes, in a simple and intuitive way, the data exfiltrated from the defended customer. That indicator of compromise is derived by Digital Surveillance and Threat Intelligence Services.

[INACTIVE] **Vulnerabilities Index**: the indicator of compromise which describes the state of found vulnerabilities. Impacts and number of vulnerabilities increases the index.

Each index goes from 0% to 100%. 0% means not evidences 100% means strong evidences of compromisation.
An index marked as **INACTIVE** means it cannot be calculated because there are no active services to monitor its status. (eg. Vulnerabilities Index requires the activation of Automatic Vulnerability Assessments)

Detected Attacks

high (2) med (3) low (4)

Analyzed Events

high (2) med (1) low (3)

Suspicious Downloads

1

Suspicious Attachments

2

Other attachments and downloads may have been detected but were not analyzed because were considered harmless.

DEFENSYO

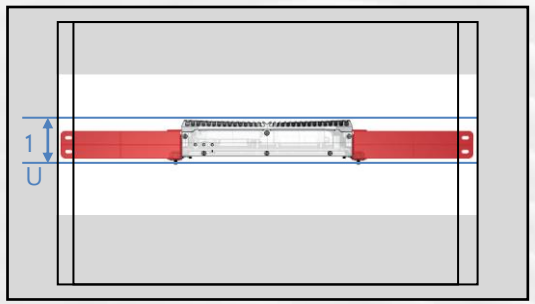
INFOCERT
TINEXTA GROUP

DEFENSYO È SEMPLICE DA INSTALLARE

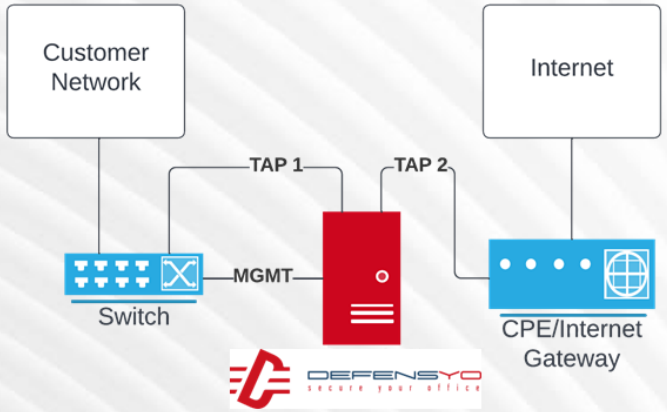
1) Basta collegare Defensyo alla rete della tua azienda per mettere in sicurezza la tua rete aziendale

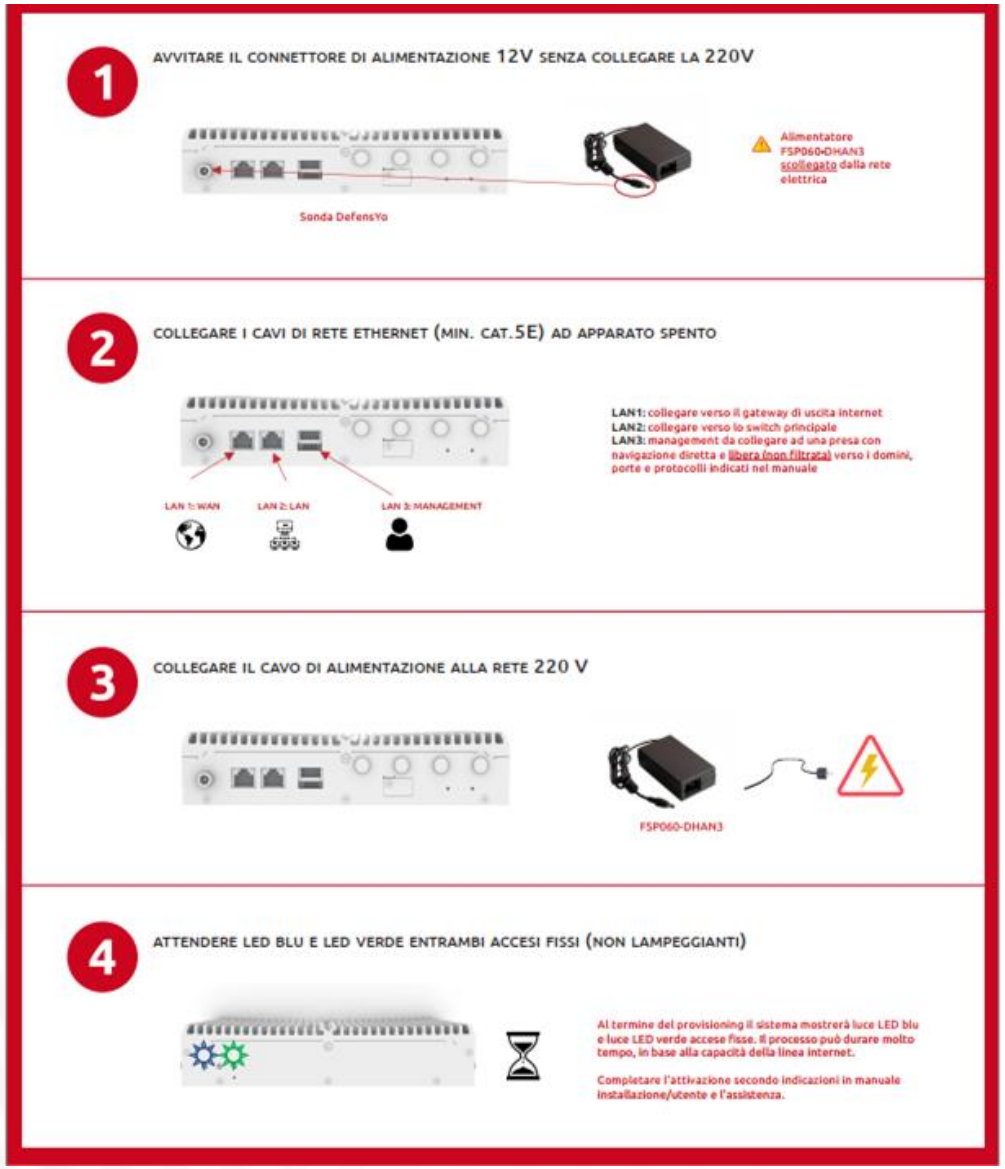
2) Nessun software da scaricare, nessuna configurazione da fare

3) La soluzione è plug and play e non ha impatti sulle configurazioni di rete esistenti.



Installabile anche in Rack 19”





INFOCERT
TINEXTA GROUP

AFFIDABILITÀ MADE IN ITALY

Soluzione proprietaria sviluppata in Italia

Qualificato su Cloud Marketplace dell'Agenzia per la Cybersicurezza Nazionale

Compliance Italiana ed europea su GDPR, data residency, Privacy

Certificata secondo gli standard di settore dalle Regulation Authority

ISO/IEC 27017:2015
ISO/IEC 27018:2019
ISO/IEC 27001:2022
CE certified EU Directive 1999/5/CE
RoHS
Directive 2014/30/EU
Directive 2014/35/EU
Directive 2011/65/EU
EN 55032:2015 + A11:2020
EN 55035:2017 + A11:2020
EN 62368-1:2020 + A11:2020
EN 62311:2008

INFOCERT
TINEXTA GROUP

TINEXTA CYBER

PER MAGGIORI INFORMAZIONI CONTATTA IL TUO ACCOUNT DI RIFERIMENTO!

SIXTEMA
TINEXTA GROUP

Camerfirma
AN INFOCERT COMPANY

CERTEUROPE
AN INFOCERT COMPANY

ICTECHLAB
AN INFOCERT COMPANY