

# I servizi alla cybersecurity



## I servizi alla cybersecurity

La piattaforma della *cybersecurity* e protezione dei dati Pragmemma POC, dispone di diversi *tool* dedicati ad aspetti differenti della *cybersecurity* quali:

- vocabolari semantici controllati
- *risk assessment*
- *risk evaluation*
- *remediation techniques*
- *standardization references*
- application tools

## A chi si rivolge

Stakeholder privilegiati: CERT, CSIRT, SIEM, SOC e clienti infrastrutture critiche e servizi essenziali come da Direttiva NIS.

## Funzionalità

Le funzionalità offerte dai vari servizi sono:

- il vocabolario semantico controllato della *cybersecurity* (VSC) (e i vocabolari generici) è il servizio di definizione delle informazioni e dei dati utili per gestire univocamente le attività di *cybersecurity*
- *risk assessment*: il servizio consente di verificare lo stato dell'arte preliminare e *in progress* del sistema e nel tempo l'andamento ovvero il check di sistema di sicurezza inerente dati e tecnologie delle aziende e delle istituzioni. Il modello è il *fra-*



*mework* NIST. Disponibili altri modelli. Su richiesta del cliente il modello *check* può essere personalizzato e interrelato ai sistemi tecnologici di *cybersecurity* aziendali/istituzionali. Il servizio copre la PIA prevista dal GDPR



- *risk evaluation*: il servizio consente di valutare il rischio dell'azienda in caso di attacchi cyber. Può essere customizzato
- *remediation techniques*: il servizio consente di definire le attività di resilienza in caso di attacchi. Può essere customizzato
- *standardization references*: il servizio offre la gamma di standard internazionali richiesti per la cybersecurity. E' connesso ai form/application tools
- gli *application tools* sono form/schemi da compilare e memorizzare sul *data base* dell'azienda o dell'istituzione correlandosi ai servizi di sicurezza presenti nel sistema informativo informatico ed effettuare le seguenti attività: reportistica eventi ed incidenti, statistiche, valutazione del rischio, *assessment*, ecc. Consente l'automazione del servizio e dei segnali di rischio.

I dati aziendali inseriti nel database customizzato consentono di analizzare le evoluzioni del sistema di sicurezza nella logica della *big data analytics*. La correlazione dei dati consente di pervenire a una interpretazione preventiva e, in prospettiva, predittiva degli attacchi.

## Casi di utilizzo

Pubbliche amministrazioni, aziende e organizzazioni che adottino questi servizi saranno in grado di avere una comprensione a livello manageriale dei concetti e delle relazioni logico semantiche della *cybersecurity*. Mentre, a livello operativo si avranno a disposizione degli strumenti che permettono l'acquisizione e la gestione controllata di dati correlati all'ontologia.

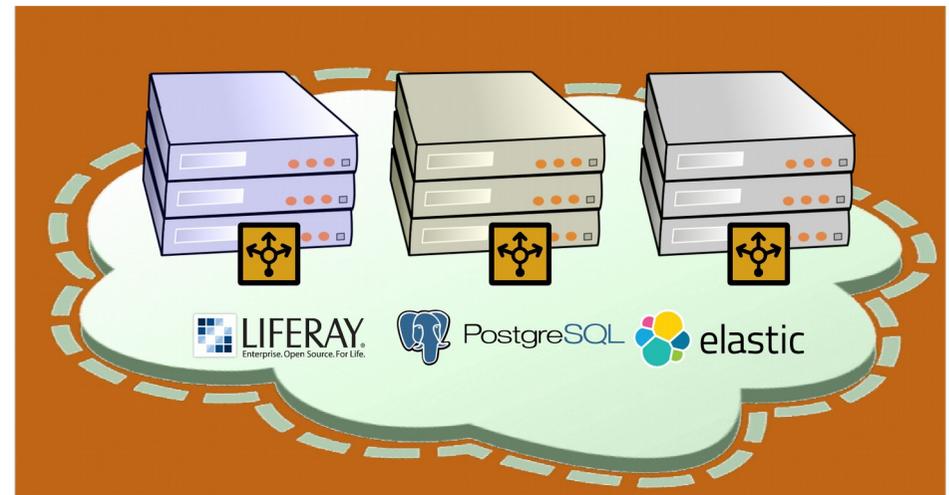
## Descrizione tecnica

Il supporto tecnologico dei servizi è un portale Liferay che utilizza un *database* Postgres e un motore di ricerca Elastic Search.

L'installazione del portale è disponibile su:

- computer del cliente
- *appliance* fornita da Pragmema in *cloud*

È anche possibile attivare un differente portale per ogni singolo servizio.



# L'azienda

## **Pragmema srl**

sede sociale e sede operativa piazza della

cancelleria 85 - 00186 Roma

tel. 06/68392146 fax 06/68211644

REA 1078363 P.I. 01224680551

[www.pragmema.it](http://www.pragmema.it)

