Innovazione CyberSec in Webgenesys

Dr. Massimo Cristaldi
Chief Innovation Officer - Webgenesys SPA

Chief Innovation Officer

Massimo Cristaldi

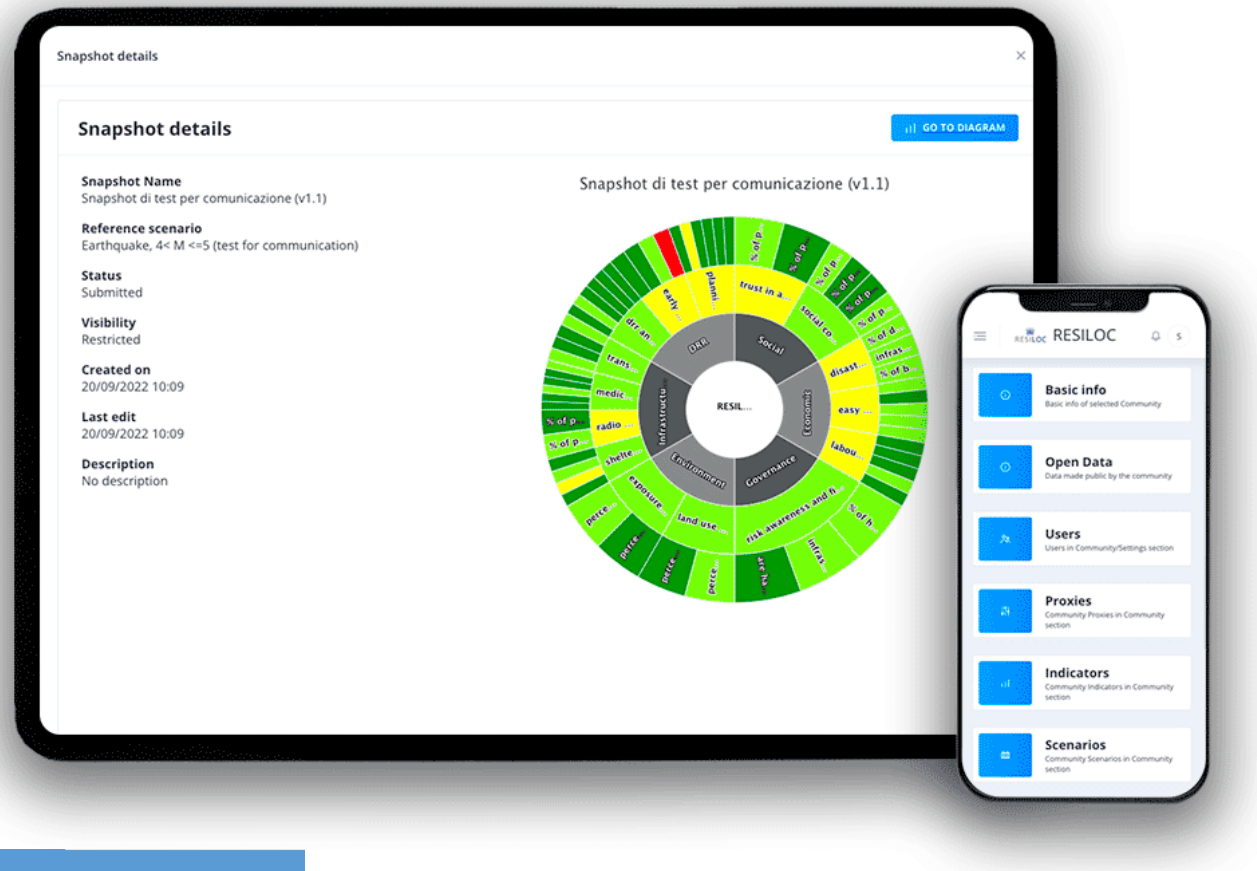
EMAIL: m.cristaldi@webgenesys.it
MOB.: 348 2816167

Resilienza e CyberSec

Resilienza: **la capacità di “Rimbalzare elasticamente” dopo un evento catastrofico per tornare velocemente alle condizioni precedenti all’evento**

Nell’ambito del progetto H2020 EU RESILOC, Webgenesys ha sviluppato una piattaforma per l’assessment della resilienza delle comunità locali

www.resiloc.it



Focus sulle Infrastrutture Critiche

*“Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, **criminal activity or malicious behaviour**, may have a significant negative impact for the security of the EU and the well-being of its citizens” - **European Union***

Il porto di Gioia Tauro, un presidio Sanitario, una ferrovia un sistema Emergency Management: tutti ASSET “danneggiabili”, tanto da disastri naturali/incidenti che da attività CyberSec related.

Se, infatti, l’ossatura info-telematica di una infrastruttura critica collassa o è compromessa, ecco che la stessa smette di operare efficacemente, con danni facilmente calcolabili all’indotto, alla Regione e, nel caso specifico, all’intero Sud Italia.

Dalla Resilienza al Rischio

PHYSICAL IMPACT OF NATURAL / ENVIRONMENTAL DISRUPTIONS ON CRITICAL DIGITAL INFRASTRUCTURE

The increased severity and frequency of environmental disasters causes several regional outages. Redundant back-up sites that maintain the availability of critical infrastructure will also be affected.

MANIPULATION OF SYSTEMS NECESSARY FOR EMERGENCY RESPONSE

Manipulation of sensors with connections to emergency services may overload services like ambulances, police, firefighters, etc. For example, call centres may be overloaded with inauthentic calls or fire alarms may be manipulated to injure specific individuals or to obscure emergency response teams' ability to locate the issue. Similarly, mass panics that overload emergency systems may also be provoked through the use of social media.

Enisa, Foresight 2030 Threats

$$R = P * V * E$$

Il **Rischio** esprime il rapporto di convoluzione tra Pericolosità, Vulnerabilità e Valore Esposto

Spesso, nelle strategie Cyber, la **Vulnerabilità** è l'elemento maggiormente considerato

Il Ruolo di un System Integrator in questo quadro

Webgenesys, che gestisce parecchi sistemi IT a livello regionale e nazionale, di concerto con le PA di riferimento, adotta un modello che, nel rispetto dei dettami ENISA, **sfrutta tecniche AI nell'ambito del SOC focalizzandosi NON solo sulla vulnerabilità ma anche sulla Pericolosità e quindi sulla PREVENZIONE/PREDIZIONE**

Pericolosità: La probabilità che un evento catastrofico accada in un determinato lasso temporale

AI nel nostro SOC 1/2

WAIX (Webgenesys AI for Cyber Security)

Un progetto che mira alla creazione di uno strumento di AI per efficientare il partenariato tra intelligenza umana ed artificiale nel SOC Webgenesys

Cosa fa?

- Scouting nel (dark) web alla ricerca di potenziali minacce per i nostri clienti. Condivide i risultati con le autorità preposte ed ACN.
- Fornisce informazioni più intellegibili di semplici LOG e migliora l'efficienza degli operatori del SOC
- Utilizza tecniche di AI per contrastare attacchi AI.

AI nel nostro SOC 2/2

- Effettua analisi del comportamento degli utenti e delle Entità (User and Entity Behavior Analytics, UEBA)
  - I tentativi di accesso ad aree riservate, l'uso di credenziali di amministratore fuori da un contesto autorizzato, sono campanelli di allarme che vengono analizzati da WAIX.
  - Ma anche senza aspettare "l'intruso" esterno, WAIX rileva comportamenti anomali anche da parte di un insider: oggi gli attacchi che arrivano da dentro le organizzazioni sono un trend in continua crescita.
- Esplora, nell'ambito di un progetto di Ricerca e sviluppo dedicato, la possibilità di sfruttare tecniche di Realtà Aumentata nei SOC
- Si integra con sistemi di Vendor diversi (Firewall Perimetrali, Web Application Firewall, NAC, SIEM, Deceptor, AD, Switch e Controller wifi)