Allegato B

Avviso pubblico per la presentazione di proposte progettuali per la realizzazione di attività di ricerca industriale e sviluppo sperimentale relative al Partenariato Esteso SERICS (PE00000014), nell'ambito dello Spoke 4 "Operating Systems and Virtualization Security" (UNIVERSITA' DEGLI STUDI DI GENOVA) ammesso a finanziamento con D.D. n. 1556 dell'11 ottobre 2022, registrato dalla Corte dei Conti il 04/11/2022 n. 2783 – nell'ambito del Piano Nazionale di Ripresa e Resilienza, Missione 4 "Istruzione e ricerca" – Componente 2 "Dalla ricerca all'impresa" – Investimento 1.3 Creazione di "Partenariati estesi alle università, ai centri di ricerca, alle aziende per il finanziamento di progetti di ricerca di base", finanziato dall'Unione europea – NextGenerationEU - Codice CUP D33C22001300002

PROPOSTA DI PROGETTO

SEZIONE 1) INFORMAZIONI GENERALI E DESCRIZIONE DEL PROPONENTE

A. Informazioni Generali

Acronimo Progetto:	**POLARS**
Titolo Progetto	**POLARS - Piattaforma Open-source ad elevato Livello di sicurezza per l'automazione di Attacchi e Reportistica di Scenari di rischio**
Durata (mesi):	*12*
Costo totale progetto (€):	**405.397,55**
Contributo totale richiesto (€):	**240.440,38**
Coordinatore del Progetto:	*nome, cognome: Barbara Canesi* *e-mail: barbara.canesi@nextage-on.com* *recapito telefonico: 3477339179*

Abstract*:*

L'obiettivo del progetto POLARS è migliorare il *framework* ARTIC sviluppando un'applicazione web che permetta di accedervi in maniera *user-friendly* e sicura, utilizzando soluzioni di autenticazione e autorizzazione e protocolli standardizzati come OpenID Connect. Il progetto produrrà un ulteriore scenario simulativo di malconfigurazione IT (*cyber range*) integrato con la webapp.
La fase iniziale prevederà la raccolta e l'analisi dei requisiti, con un particolare focus sui requisiti di sicurezza, unitamente ad uno studio approfondito dei protocolli di autenticazione e autorizzazione, avvalendosi di consulenti esperti nella sicurezza di comunicazioni e reti. La progettazione coprirà architettura dell'applicazione, design dell'interfaccia utente e definizione delle funzionalità. Il prototipo dell'applicazione sarà sviluppato integrando i protocolli di sicurezza identificati.
In parallelo, verrà sviluppato uno scenario simulativo aggiuntivo che includa almeno 32 host, basato su Windows server. L'applicazione web sarà sottoposta a test di integrazione e collaudo con lo scenario creato nel progetto e con lo stesso ARTIC, nonché a test di sicurezza (*penetration test*).
L'applicazione web finale offrirà un'interfaccia grafica accessibile via *browser*, fornendo strumenti per la gestione e il monitoraggio dei *container* componenti il framework ARTIC. La UI faciliterà la configurazione e fruizione degli scenari IT di test da parte degli utenti e permetterà di lanciare anche tipologie di attacchi automatizzati sugli scenari di malconfigurazione.
Tutto il *software* sviluppato sarà *open-source*. Il progetto si pone gli obiettivi non solo di migliorare la sicurezza e l'efficacia di ARTIC, fornendo ai discenti di *cybersecurity* uno strumento che faciliti l'apprendimento aumentando le competenze nella sicurezza, ma anche a contribuire al panorama *open-source*, offrendo una

soluzione robusta che promuova trasparenza e collaborazione.	
Keywords	
Scenario, *cyber range*, autenticazione, autorizzazione, sicurezza, *cybersecurity*, applicazione web, interfaccia grafica, UI.	
TRL iniziale:	*4*
TRL finale:	*5*
Sede/i operativa/e	**Nextage Srl: Piazza della Vittoria 12/12, Genova** **Secure Network Srl: Via di Motta della Regina 6, Foggia**

B. Anagrafica dei soggetti partecipanti

B.1) Descrizione

Soggetto proponente CAPOFILA in proposte in forma associata	
Denominazione	Nextage
Forma giuridica	S.r.l.
P.IVA / C.F.	01776070995
Tipologia di soggetto (MPI, MI, GI):	MPI
Indirizzo (sede legale)	PZA DELLA VITTORIA 12/12
Indirizzo (sede operativa) *(unità dell'intervento)*	PZA DELLA VITTORIA 12/12
Rappresentante Legale	Barbara Canesi
e-mail e pec	nextage@pec.it
Codice Ateco Primario della sede di intervento	72.19.09
Core business, ramo di attività, principali attività produttive e mercato/i di riferimento	Nextage è una PMI innovativa con forti competenze nel settore biomedicale ed esperienza di partecipazione a programmi di ricerca a livello regionale, nazionale ed europeo. L'azienda è presente sul mercato ICT con servizi nell'ambito di: gestione e realizzazione di progetti software web usando le più moderne tecnologie e strumenti di programmazione; Consulenza per la Sicurezza delle Informazioni, Qualità, Erogazione Servizi IT, Continuità Operativa, *risk assessment*, sviluppo sicuro e conformità *privacy* e GDPR; Servizi di ricerca e gestione di programmi finanziati, ricerca e sviluppo conto terzi, supporto e sviluppo di iniziative di *start-up*. Nextage ha realizzato un brevetto italiano, di un applicativo software, Nx-Frame, registrato alla SIAE, e il nodo locale del fascicolo sanitario elettronico ligure per l'ospedale Galliera. Inoltre, ha recentemente depositato domanda per un altro brevetto italiano, sulla gestione dei dati criptati trattati dagli

	applicativi prodotti. L'attività di sviluppo *software* su piattaforme di tipo web *enterprise* include: un prodotto per la gestione di processi ospedalieri SurgiQ (oggi start-up innovativa); per la gestione di dati clinici, Colibri; una piattaforma di gestione delle schede di dimissione ospedaliera; un tool di *risk assessment* ERA, per la gestione del rischio in diversi *framework* a norma ISO, erogato in modalità *cloud SaaS* e certificato ISO/IEC 27001-27017-27018. Nx-Frame è un *framework* proprietario, sviluppato per avere a disposizione uno *stack* applicativo strutturato, omogeneo, testato, costantemente aggiornato e contenente tutte le caratteristiche e componenti fondamentali per la sicurezza applicativa, la progettazione e realizzazione di applicativi in maniera rapida ed efficace. Oltre all'aspetto commerciale, Nextage è socia del Polo Scienze della Vita, SIIT PMI, Confindustria, Silver Economy Network, Cluster PROSSIMO, SmartCommunitiesTech. Nextage è certificata ISO 9001:2015, ISO/IEC 27001-27017-27018, UNI/PDR 125:2022.
Ruolo del partner	Nel presente progetto Nextage si occuperà di sviluppare un'interfaccia grafica (GUI) accessibile via browser, che migliori l'accessibilità, la facilità di utilizzo e la fruizione delle informazioni presenti nei cyber range containerizzati presenti nell'iniziativa del progetto ARTIC per Spoke 4. La soluzione prenderà quindi la forma di una vera e propria applicazione web. Nextage adotterà nella GUI sviluppata soluzioni di autenticazione e autorizzazione sicura, sfruttando protocolli standardizzati come ad esempio OpenID Connect, User-Managed Access o l'architettura Zanzibar di Google, studiando la soluzione o combinazione di soluzioni ottimali per garantire sicurezza, versatilità e prestazioni ottimali al prototipo. La GUI verrà sviluppata secondo i più moderni stack tecnologici usati nelle applicazioni web, già adottati da Nextage nelle proprie soluzioni di produzione, comprendenti tecnologie come Angular, Node.Js, MongoDB, sfruttando il proprio framework proprietario brevettato per lo sviluppo di applicazioni web, Nx-Frame. Nextage collaborerà strettamente sia con il riferimento dello Spoke di Serics, sia con partner e controparti di progetto, condividendo le competenze tecniche mediante aggiornamenti periodici, e contribuendo alla revisione continua e al miglioramento delle funzionalità del progetto. I risultati del progetto saranno open-source, con l'obiettivo comune di migliorare la sicurezza informatica attraverso l'innovazione e la cooperazione.

Conoscenze e competenze apportabili dal partner	Nextage ha esperienza e competenze chiave nel campo della sicurezza informatica e dello sviluppo di applicazioni web sicure. Tra le attività e progetti rilevanti si evidenziano: 1. Sviluppo di applicazioni sicure e scalabili: Nextage, grazie all'esperienza pluriennale nell'ambito della gestione sicura e protetta del dato, in accordo con normative vigenti *Privacy* & GDPR, è in grado di realizzare soluzioni tecnologiche, come *dashboard* e console di gestione accessibili via *browser*, conformi alla protezione dei dati e alla sicurezza delle informazioni, ottimizzando processi e risorse. Ciò si riflette in prodotti come SurgiQ (ora *start-up* innovativa) e Colibri, che offrono interfacce avanzate per la gestione di dati clinici e di processi ospedalieri; e Nx-Frame, un *framework* proprietario per la sicurezza e la realizzazione rapida di applicativi. 2. Nextage ha un'intera area aziendale dedicata alla consulenza in sistemi di gestione, tra cui spicca la competenza in Sicurezza delle informazioni (famiglia ISO/IEC 27001) e sviluppo sicuro (OWASP), avvalendosi di consulenti e partner fidati per attività di VA/PT e *network security assessment*. 3. Collaborazione in Progetti di Ricerca: Nextage partecipa attivamente in consorzi di ricerca a livello regionale, nazionale ed europeo, contribuendo con competenza tecnica allo sviluppo di soluzioni innovative. Tra gli ultimi progetti finanziati ricordiamo, tra i più pertinenti: - Evergrid (Bando Competence 2023 Center Start 4.0): sicurezza informatica e ottimizzazione delle *smart grid*, piattaforma per efficientamento energetico - InventorAI (Fesr 2021-2027 - OS 1.1 - Azione 1.1.1 - Supporto allo sviluppo di progetti di innovazione nelle micro, piccole e medie imprese): applicazione AI-powered per la creazione di asset inventory per analisi del rischio per la sicurezza delle informazioni - Invictus (Cascade Funding 2023 Ecosistema RAISE): piattaforma interconnessa con dispositivi IoT per telemonitoraggio e teleassistenza.
Motivazioni, specifici vantaggi e ricadute attese dalla partecipazione al progetto	La partecipazione al progetto offre a Nextage l'opportunità di rafforzare la propria posizione nel settore della *cybersecurity*. La collaborazione con l'azienda consulente di *cybersecurity*, Gerico Lab Srl, permetterà a Nextage di migliorare le proprie competenze riguardo all'implementazione di protocolli sicuri nelle casistiche di autenticazione e autorizzazione delle applicazioni web; la collaborazione con il partner Secure

	Network e con UniGe permetterà a Nextage di incrementare le proprie competenze nel contesto della messa in sicurezza di container, e della predisposizione di *cyber range* utilizzabili nelle proprie sessioni di training e formazione, poiché Nextage è dotata di una squadra di formatori nel contesto della sicurezza delle informazioni (area aziendale "Governance"). La visibilità di partecipare al presente progetto come capofila permetterà a Nextage di instaurare nuove collaborazioni con l'Università di Genova, anche nel settore ritenuto chiave dall'azienda della sicurezza informatica. Lo sviluppo di tecnologie e metodologie permetterà di migliorare la sicurezza delle applicazioni future ed esistenti di Nextage. Inoltre, la collaborazione contribuirà allo sviluppo di soluzioni innovative e sicure che potranno essere integrate nei prodotti e servizi di cui Nextage è proprietaria. Infine, La partecipazione al progetto porterà a Nextage una maggiore visibilità nel settore della sicurezza informatica e perciò a potenziali opportunità di mercato con le aziende del settore e non.

Soggetto proponente PARTNER 1 in proposte in forma associata	
Denominazione	Secure Network
Forma giuridica	S.r.l.
P.IVA / C.F.	04205230966
Tipologia di soggetto (MPI, MI, GI)*:*	GI
Indirizzo (sede legale)	Piazza Armando Diaz 6, Milano
Indirizzo (sede operativa) *(unità dell'intervento)*	Via di Motta della Regina 6, Foggia
Rappresentante Legale	Alvise Biffi
e-mail e pec	alvise.biffi@securenetwork.it (cc antonella.caputo@securenetwork.it), securenetwork@legalmail.it
Codice Ateco Primario della sede di intervento	62.09.09
Core business, ramo di attività, principali attività produttive e mercato/i di riferimento	Secure Network è specializzata in servizi di **Offensive Cybersecurity** dal 2004. Secure Network offre, mediante un vasto catalogo di servizi altamente personalizzabili, competenze avanzate e specializzate per supportare i propri clienti nell'identificazione, la pianificazione e l'esecuzione dei percorsi che li porteranno alla miglior postura di sicurezza delle informazioni possibile. In particolare, i servizi di security assessment del nostro laboratorio certificato consentono alle organizzazioni e alle aziende di valutare la postura difensiva contro attacchi e minacce *cyber* verso le loro infrastrutture, applicazioni, linee di produzione e prodotti. Secure Network collabora a diversi progetti di ricerca insieme a vari partner accademici (e.g., Politecnico di Milano), i cui risultati sono stati presentati ed accolti alle più importanti conferenze internazionali sull'Information Security, quali *DEF CON*, *Black Hat*, *Hack in the Box*, *AppSec Europe*, *CanSecWest* e

	BlueHat. Nell'ambito della crescente richiesta di servizi *cybersecurity* di *vulnerability assessment* verso infrastrutture OT da parte dei propri clienti, Secure Network ha avviato il percorso per le certificazioni UNI CEI EN ISO/IEC 9001 – 27001 – 17025 e, nell'ampliamento dei propri uffici di Milano, ha in programma di realizzare un Laboratorio di Prova per soddisfare sia le richieste di *vulnerability assessment* e di test dei propri clienti, che per offrire supporto al CVCN rispetto alle future necessità di verifica come Laboratorio Accreditato di Prova. Con questi asset Secure Network sarà in grado di supportare sia la PA che PMI e Mid Cap, con particolare focus al settore *Manifacturing*, contribuendo in modo significativo al trasferimento delle competenze specialistiche in *cybersecurity* e al supporto operativo per la resilienza *cyber* della PA e del sistema produttivo nazionale.
Ruolo del partner	Secure Network parteciperà alla realizzazione del progetto apportando le proprie competenze in materia di *offensive cybersecurity* per lo sviluppo di scenari specifici di *testing* e *training* basati sulla simulazione di una rete aziendale moderatamente complessa e affetta dalle tipiche problematiche di configurazione e implementazione che Secure Network normalmente analizza e rileva presso i propri clienti, le quali possono permettere a un aggressore la definizione di alcuni scenari di attacco. Questi scenari verranno appositamente studiati e definiti da Secure Network sulla base delle principali Tattiche, Tecniche e Procedure (TTP) emerse dal framework ATT&CK e da fonti di Threat Intelligence. Secure Network contribuirà attivamente all'attuazione del progetto POLARS sia mediante la progettazione degli scenari che mediante l'implementazione degli stessi in una piattaforma gestita e coordinata mediante le più moderne tecniche di *infrastructure-as-code* in modo da consentirne scalabilità, portabilità e semplicità di *deployment*. Gli attacchi definiti negli scenari individuati saranno automatizzati mediante *script* ad-hoc, in modo da consentirne la riproducibilità da parte degli utenti della piattaforma. Secure Network collaborerà costantemente sia con il riferimento dello Spoke di Serics che con i partner di progetto, al fine di definire i flussi di integrazione tra le diverse componenti ed armonizzare lo sviluppo. Secure

	Network condividerà insieme agli altri partner i *task* relativi all'organizzazione e alla gestione del progetto, e interverrà con le proprie competenze di *offensive security* nell'erogazione di un *penetration test* sulla piattaforma *web* che verrà principalmente implementata dal partner capofila Nextage. I risultati delle componenti sviluppate saranno rilasciati sotto una licenza open-source scelta in fase di progetto tra quelle approvate dalla Open Source Initiative, in modo da massimizzare la fruibilità dei risultati da parte degli utenti finali.
Conoscenze e competenze apportabili dal partner	• Nel corso del 2023 è stato portato a compimento il progetto E-AR Mirror, conclusosi il 31 Dicembre 2023, che fa seguito a una intensa attività di ricerca e sviluppo sostenuta nell'ultimo triennio. A testimonianza dell'investimento di Secure Network sul tema della Sostenibilità, il progetto – promosso nel 2020 dall'allora "Ministero dello sviluppo economico" - riguarda lo sviluppo di competenze nell'area della trasformazione digitale. Il progetto di ricerca è strettamente connesso con il tema materiale della trasformazione digitale Il progetto **E-AR MIRROR** intende ricercare e studiare le nuove tecnologie interattive e mobile al fine di sviluppare una piattaforma basata sulle tecnologie della realtà aumentata, della realtà virtuale e dell'intelligenza artificiale, con l'obiettivo di migliorare ed innovare i processi di produzione e vendita di accessori personalizzabili per la moda e per la persona. • **CETMA_DIHSME:** CETMA-DIHSME è l'EDIH per la Puglia e la Basilicata, uno dei 151 europei (13 in Italia) finanziati dalla UE e dagli stati membri per accelerare la trasformazione digitale delle PMI e della PA attraverso l'implementazione di tecnologie digitali avanzate (AI | HPC | Cybersecurity) per aumentarne la competitività e la sostenibilità. Nei prossimi 3 anni fornirà più di 1400 servizi di innovazione, finanziati fino al 100%, alle PMI e alle Pubbliche Amministrazioni di Puglia e Basilicata, grazie ad un finanziamento di circa 6 milioni di euro. L'obiettivo è quello di diffondere le più avanzate tecnologie di digitalizzazione per mostrare e far conoscere i benefici che le tecnologie digitali avanzate possono offrire alle PMI e alla PA in tutti i settori. Secure Network ha messo a disposizione una vasta gamma dei suoi principali servizi, tutti finanziabili dai fondi PNRR fino al 100% a seconda della dimensione d'impresa e della

	capienza *de minimis.*
Motivazioni, specifici vantaggi e ricadute attese dalla partecipazione al progetto	La partecipazione di Secure Network al progetto permetterà di rafforzare le proprie competenze e gli strumenti utilizzati nel campo della formazione in tema di sicurezza informatica e, in particolare, in tema di formazione alla *offensive cybersecurity*. La partecipazione attiva alla definizione degli scenari implementati nella piattaforma di *training* e *testing*, nonché al loro sviluppo e implementazione, consentirà a Secure Network di avere piena familiarità e disponibilità di uno strumento che può coadiuvare in maniera interattiva i corsi di formazione erogati presso i propri clienti e aumentare la loro efficacia, oltre che permettere l'erogazione e l'inserimento a catalogo di specifici servizi volti all'installazione, all'utilizzo e al supporto relativo alla piattaforma di *training* e *testing* di POLARS e, più in generale, al *framework* ARTIC. Inoltre, quanto sviluppato congiuntamente dal consorzio verrà adottato come strumento per la formazione interna dei dipendenti tecnici di Secure Network, sia per quanto riguarda la formazione del personale che viene inserito in azienda che per quanto riguarda la formazione e l'aggiornamento continuo del proprio personale esistente in relazione alle tattiche, tecniche e procedure di attacco tempo per tempo emergenti. Infine, la partecipazione al progetto e allo sviluppo degli strumenti utilizzati, che verranno rilasciati pubblicamente secondo una licenza *open source* e verranno disseminati negli eventi e nelle modalità descritte di seguito come parte del Work Package 1, consentirà a Secure Network maggiore visibilità nel settore, portando potenziali ricadute positive a livello di *business* non solo per i servizi di formazione, ma anche per la propria linea di servizi di *assessment*.

B.2) Descrizione della partnership (in proposte in forma associata)

Il consorzio è composto da partecipanti interdisciplinari con ruoli specifici e complementari, selezionati in base al criterio basato sull'equilibrio tra le diverse competenze tecniche previste dal progetto. Tale diversificazione mira a massimizzare l'utilizzo dei risultati del progetto e il coinvolgimento attivo di diversi target chiave per garantire una diffusione ampia e duratura delle idee e prototipi. Nextage ha 15 anni di esperienza nello sviluppo software *full-stack*, sicurezza informatica, e analisi dei dati in ambito *healthcare*. Offre servizi di consulenza e formazione in tema OWASP Secure Coding, effettua attività di vulnerability assessment e penetration test, e partecipa attivamente a programmi di ricerca regionali ed internazionali. L'applicativo di POLARS sarà progettato usando il *framework* brevettato Nx-Frame TRL4, frutto delle conoscenze e competenze maturate nel corso del tempo e basato sulle tecnologie open source Angular, Node.js e MongoDB. Il *framework* Nx-Frame: 1) è progettato per consentire agli sviluppatori di creare piattaforme web *full-stack*, concentrandosi subito sulla logica applicativa e riducendo tempi e costi di sviluppo; 2) è compliant con gli standard GDPR di *privacy by design* e *privacy by default* e i requisiti di sicurezza di OWASP; 3) include una metodologia di gestione di dati criptati e metodo di ricerca di dati criptati brevettata (n. domanda di brevetto 102021000032048; data deposito 21/12/2021; Data del rapporto ricerca con esito non negativo: 20/07/2022). Secure Network, leader in Italia e in Europa per l'*offensive cybersecurity*, offre competenze avanzate e specializzate per supportare nell'identificazione, la pianificazione e l'esecuzione di percorsi in termini di sicurezza delle informazioni. Nel corso dell'ultimo anno, l'azienda ha inaugurato il suo Laboratorio di Prova, di cui ha presentato domanda di accreditamento all'Agenzia Nazionale per la Cybersicurezza (ACN) ed e' stato uno degli otto selezionati da ACN, a livello nazionale, per essere finanziato nel processo di accreditamento. I servizi di *security assessment* erogati da Secure Network consentono alle organizzazioni e alle aziende di valutare la postura difensiva contro attacchi e minacce *cyber* verso le loro infrastrutture, applicazioni, linee di produzione e prodotti.

Date le competenze descritte, Nextage si concentrerà sul miglioramento del framework ARTIC integrando soluzioni di autorizzazione e autenticazione e lo sviluppo di un'interfaccia grafica per la gestione e configurazione del framework, accessibile via *browser* e dotata di strumenti di monitoraggio (obiettivo C2 - "Authentication Mechanisms and Graphical User Interface"). D'altra parte, Secure Network provvederà all'implementazione e documentazione di uno scenario IT rappresentativo e realistico (obiettivo C3 "Training and testing scenario"), sviluppato e definito sulla base di scenari di attacco il più possibile vicini a quanto osservato da analisi reali e basato principalmente sulla simulazione di una rete moderatamente complessa in ambiente Microsoft Windows (Active Directory).

Pur prevedendo le due macroattività uno sviluppo principalmente parallelo, lo scenario sviluppato da Secure Network verrà utilizzato per testare congiuntamente l'interfaccia *software*, assicurando che le soluzioni di autenticazione e autorizzazione integrate siano efficaci, e che l'interfaccia grafica soddisfi i requisiti operativi e di sicurezza in un ambiente rilevante che simuli più accuratamente l'uso operativo reale (TRL 5). POLARS prevederà infatti nella fase di validazione l'utilizzo di un *cyber range* dell'Università di Genova o in alternativa,

in ottica di mitigazione dei rischi, di uno messo a disposizione da Secure Network e sviluppato dalla propria capogruppo BV TECH S.p.A.

Pur non avendo ancora all'attivo mutue collaborazioni passate ed in essere, la capofila Nextage annovera nel proprio curriculum partnership progettuali di successo con aziende del gruppo BV TECH, di cui Secure Network è parte, e vede nel progetto opportunità di sinergizzare le rispettive competenze per massimizzare l'efficacia delle soluzioni sviluppate, creando una solida base per future collaborazioni strategiche nel campo della sicurezza informatica.

Oltre alla *partnership* descritta, Nextage si avvarrà della consulenza di Gerico Lab Srl, già fornitore Nextage, nell'ottica della maturazione di nuove conoscenze e competenze in tema di autorizzazione e autenticazione e come mitigazione del rischio legato all'attività.

Gerico Lab è specializzato nell'erogazione di servizi e consulenze nell'ambito della *cybersecurity*. In particolare, consulenze sia in ambito IT *governance* che strategie IT con particolare riferimento ai principali standard e framework offerti, ad esempio, da NIST, ISO/IEC, COBIT, ITIL, ecc. con l'obiettivo di valutare l'approccio generale alla sicurezza, lo stato dell'arte e infine definire i punti di miglioramento per poi coordinarne e supportarne l'implementazione. Inoltre, esegue ispezioni e verifiche di sicurezza secondo standard internazionali al fine di fotografare e valutare lo stato di maturità nella gestione della sicurezza rispetto alle normative e alle *best practice* di settore. Infine, eroga servizi di *vulnerability assessment*, *penetration test* e *red team* seguendo le principali metodologie di test quali OWASP, OSSTMM, PCI DSS, ecc. con personale qualificato e specializzato munito delle principali certificazioni di settore, tra cui quelle emesse da EC-Council, eLearn Security e Offensive Security. Negli anni Gerico Lab ha partecipato a diversi importanti progetti riguardanti la progettazione di sistemi di *identity*, *authentication*, *authorization* e *single sign-on*, sia in termini architetturali che di implementazione e configurazione. Tutte queste progettazioni hanno seguito le *best practice*, gli standard e lo stato dell'arte delle tecnologie evolvendosi nel tempo da infrastrutture monolitiche a quelle a microservizi. In funzione della progettualità specifica e dei requisiti di business, le implementazioni hanno utilizzato OpenID Connect, SAML, OAuth2.0, meccanismi *role-based* (RBAC), *user-managed access* (UMA) o di *single sign-on* con le principali piattaforme di *social networking* quali Facebook, Google, Apple, Microsoft, X (Twitter), ecc.

Inoltre, il partenariato ritiene vantaggioso collaborare strettamente e in maniera complementare con i *team* interdisciplinari dell'Università degli Studi di Genova, in quanto fonte costante di stimoli innovativi - che potrebbero non emergere in un ambiente progettuale standard, chiuso e meno diversificato - oltre che del *framework* ARTIC su cui si baserà tutta l'attività progettuale.

SEZIONE 2) DESCRIZIONE DEL PROGETTO DI RICERCA

A. Coerenza con il target e le finalità programmatiche del bando

Il progetto POLARS si propone l'obiettivo di migliorare il *framework* ARTIC (Affordable, Reusable and Truly Interoperable Cyber ranges) che fornisce un'infrastruttura all'avanguardia per la simulazione e l'addestramento nel campo della *cybersecurity*. L'obiettivo principale prevede la realizzazione di un'interfaccia utente grafica (GUI) completa ed intuitiva e di meccanismi di autenticazione avanzati, nonché la progettazione e l'implementazione di uno scenario di *training* e *testing*, integrato con l'interfaccia utente e con il *framework* ARTIC. Il progetto POLARS si allinea infatti agli obiettivi C2 e C3 del bando, concentrandosi sulla creazione di un'interfaccia utente accessibile via *browser* dotata di tecnologie di autenticazione e autorizzazione.

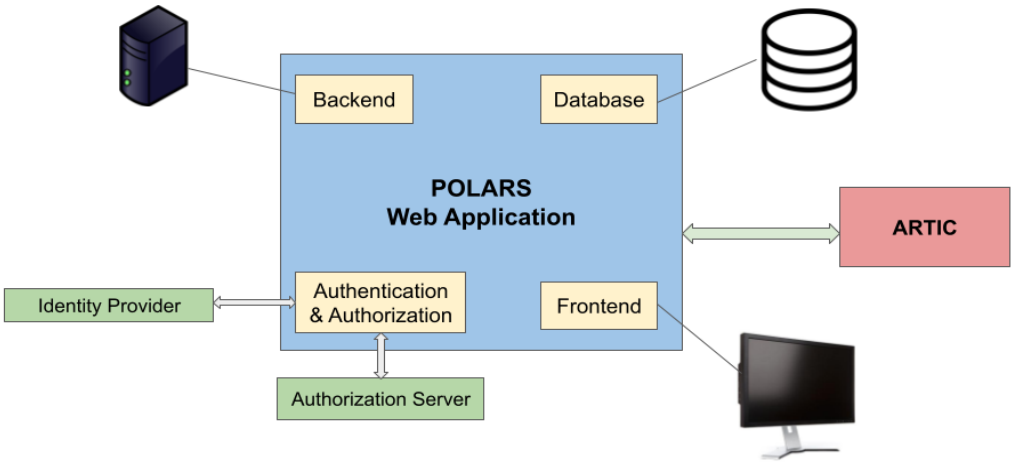

Figura 1 - Schema Architettura POLARS

La parte centrale del progetto si trova nello sviluppo di un'interfaccia utente grafica avanzata che metterà a disposizione un centro di comando del *framework* ARTIC. Questa interfaccia sarà progettata per offrire:

- Visualizzazione in tempo reale dello stato delle componenti del framework ARTIC, fornendo agli amministratori una panoramica immediata e dettagliata dell'intera infrastruttura.
- Un sistema avanzato per la configurazione, il *provisioning* e il *deprovisioning* degli scenari di *cybersecurity*, consentendo agli utenti di creare, modificare e gestire simulazioni complesse con facilità.
- *Dashboard* per la visualizzazione d'insieme delle attività e degli eventi all'interno degli scenari simulati.
- Accesso a strumenti offensivi e difensivi in base al livello di privilegio e al ruolo dell'utente nell'esercitazione.

L'interfaccia verrà progettata per essere intuitiva e *user-friendly*, garantendo al contempo la potenza e la flessibilità necessarie per gestire scenari di *cybersecurity* complessi. Particolare attenzione verrà posta

sull'implementazione di indicatori di performance (KPI), concordati con Serics, utili a fornire preziose informazioni per l'ottimizzazione continua delle simulazioni e delle strategie di difesa. Questa interfaccia non solo migliorerà significativamente l'usabilità del *framework* ARTIC, ma fornirà una piattaforma centralizzata per l'integrazione di varie funzionalità avanzate, tra cui la configurazione dell'infrastruttura IT prevista negli scenari di *cyber range*. Un elemento chiave del progetto POLARS è lo sviluppo di un sistema avanzato per la gestione degli scenari di *cybersecurity*. Questo sistema permette di:

- Implementare un formato standardizzato per gli scenari, facilitando la condivisione e il riutilizzo.
- Creare, modificare e salvare i dati relativi agli scenari simulati all'interno di un database, garantendo coerenza e affidabilità.
- Offrire agli utilizzatori la possibilità di sperimentare diverse strategie per identificare e rispondere ad attacchi all'infrastruttura simulata.

L'infrastruttura come schematizzata nella Figura 1 prevederà l'integrazione di una soluzione di autenticazione mediante l'utilizzo di un *Identity Provider* allo stato dell'arte, e di un *Authorization Server* che implementi politiche di accesso basate su principi che verranno definiti all'interno del progetto. Le soluzioni di *identity*, *authentication* e *authorization* pensate faranno uso di protocolli standard quali OpenID Connect e OAuth2.0 che consentono, laddove richiesto, la federazione con altri servizi di *identity provider*, con un modello di autorizzazione basato sull'architettura Google Zanzibar gestibile e governabile tramite accessi *user-managed* (UMA) che sarà meglio definita in base ai requisiti di Serics in fase di progettazione. Infine, tutto il software sviluppato sarà rilasciato come *open-source* sotto la licenza MIT. La natura *open-source* del progetto garantirà inoltre che possa evolversi continuamente beneficiando dei contributi della comunità e mantenendosi all'avanguardia rispetto alle sfide emergenti nel campo della cybersecurity. L'infrastruttura di cui ai precedenti paragrafi sarà integrata con uno scenario di *training* e *testing*, sviluppato in coerenza con il punto C3 del bando. Lo scenario sarà sviluppato e implementato tenendo in considerazione le più recenti tattiche, tecniche e procedure osservate in attacchi reali, anche sulla base di informazioni derivanti da threat intelligence e dall'esperienza di Secure Network in materia. Lo scenario simulerà una rete aziendale di almeno 32 host (macchine virtuali su una apposita infrastruttura *on premises*), basata principalmente ma non esclusivamente su Microsoft Windows, e includerà i servizi tipicamente presenti in una rete aziendali, quali una *directory* (Active Directory), un servizio di posta elettronica (Microsoft Exchange), oltre che un congruo numero di *client*. Questa infrastruttura conterrà vari errori di configurazione e/o di implementazione, che consentiranno la simulazione di scenari di attacco realistici. Lo scenario verrà implementato in maniera scalabile e riproducibile, e la sua installazione e configurazione sarà interamente definita sulla base di codice sorgente *infrastructure-as-code* (e.g., Ansible, Terraform) che permetterà una semplice messa in produzione in una varietà di ambienti. Il codice sviluppato sarà reso pubblicamente disponibile sotto una licenza *open-source* tra quelle approvate dalla Open Source Initiative. Lo sfruttamento degli scenari di attacco implementati sarà automatizzato mediante una serie di *script* ad-hoc sviluppati dal consorzio e resi disponibili anch'essi pubblicamente sotto una licenza open-source. La messa in opera dell'infrastruttura di *training* e *testing* sarà integrabile con l'infrastruttura schematizzata nella Figura 1 e con il framework ARTICS.

B. Obiettivi, validità tecnico-scientifica e livello di innovatività dei contenuti e delle metodologie

Nextage

Obiettivi - Gli obiettivi che si hanno intenzione di raggiungere, al termine del progetto, sono lo sviluppo di un'interfaccia grafica intuitiva, l'implementazione di meccanismi di autenticazione e autorizzazione sicura, il miglioramento dell'accessibilità e della gestione dei dati su ARTIC e il rilascio dell'applicativo *open-source*, nonché l'integrazione di uno scenario di *training* e *testing* basato su tecniche di attacco realistiche. Perciò in primo luogo si progetterà un'interfaccia utente accessibile via browser, tramite la definizione e lo sviluppo della sua architettura.

L'ambiente sviluppato dovrà fornire informazioni dettagliate sullo stato dei componenti del *framework* e dei *container*, permettendo una gestione efficace grazie a un'interfaccia a *dashboard* di controllo. La *dashboard* permetterà la visualizzazione, la gestione ed il monitoraggio degli scenari disponibili per le attività di *cyber range*: ad esempio, *log* di stato, informazioni sul consumo delle risorse e altre statistiche che verranno concordate direttamente con Serics. Le modalità di accesso degli utenti alla piattaforma web del progetto POLARS prevederà meccanismi di autenticazione e autorizzazione sicura.

Al fine di incrementare le competenze aziendali riguardo cybersecurity, protocolli sicuri di autenticazione, e *cyber range*, verranno condotte delle analisi dei protocolli presenti in letteratura al fine di implementare soluzioni adatte al caso specifico. L'infrastruttura prevede infatti l'utilizzo di un *Identity Provider* che integri su larga scala soluzioni basate su protocolli standard di autenticazione, autorizzazione e gestione degli accessi.

Obiettivo della applicazione web sviluppata sarà la facilitazione significativa dell'utilizzo del *framework* di *cybersecurity* ARTIC, permettendo all'utente di concentrarsi sulla gestione dello scenario piuttosto che sulla operatività base dello stesso *framework*. Obiettivo del progetto POLARS è anche la diffusione e l'accessibilità della sicurezza informatica in modo da promuovere la consapevolezza, l'innovazione e la collaborazione della comunità in un ambito in rapida crescita e di interesse comune: per questo motivo i risultati del progetto verranno distribuiti in formato *open-source*.

Validità tecnico-scientifica - L'applicazione web implementata verrà validata facendo utilizzo di metriche che coprano gli aspetti critici del sistema, garantendo la soluzione sicura e in linea con i requisiti. Tra loro:

- *rate* di autenticazione fallita rispetto ai tentativi totali (<2%)
- tempo di disponibilità del sistema: opportuni test di carico per verificare il tempo di operatività e accessibilità del sistema (>99.5%)
- *feedback* degli utenti: raccolta di *feedback* da parte degli utenti finali tramite sondaggi e interviste, valutando la facilità d'uso e l'intuitività dell'interfaccia utente (>80%)
- tempo medio di risposta delle comunicazioni da e verso il *framework* ARTIC e gli scenari IT (<500ms)

Ad ognuno di essi è stato associato un KPI che permettesse di valutare l'efficacia della validazione. Inoltre, la validazione permetterà di fornire una valutazione qualitativa circa l'affidabilità delle tecnologie utilizzate, i risultati delle attività di ricerca e i metodi di analisi, progettazione e sviluppo adottati.

Livello di innovatività - Il principale elemento di innovatività è il concetto di utilizzare un'interfaccia grafica con tecnologie allo stato dell'arte per garantire un'esperienza *user-friendly* agli utenti che si apprestano ad effettuare addestramenti nell'ambito della *cybersecurity*, in particolare di simulazioni di scenari di infrastruttura IT che team di attacco (*red*) o team di difesa (*blue*) debbano, rispettivamente, compromettere o difendere. In questo contesto, infatti, è difficile rimanere agnostici dagli aspetti sistemistici più tediosi che potrebbero fuorviare l'attenzione rallentando il processo di apprendimento. Infatti, invece di concentrarsi sul "far partire" il container con lo scenario di *cyber range* da affrontare, lo studente potrà concentrarsi sull'attività di *exploit* vera e propria, velocizzando l'addestramento sulle tematiche principali.

L'utilizzo di un punto unico di partenza, una dashboard per gestire organizzare e iniziare diversi scenari di *cyber range* a cui punta, in maniera semplice, ordinata e intuitiva tramite una GUI è anch'esso completamente iscrivibile ai filoni di innovatività del progetto, in quanto in commercio non sono presenti applicativi di questo tipo ascrivibili alla categoria open-source.

Dal punto di vista della complementarietà e valore aggiunto alle attività portate avanti dallo Spoke rispetto ad utilizzo di applicazioni web multipiattaforma open source per l'analisi e visualizzazione interattiva (es. Grafana, Kibana), di seguito i principali vantaggi derivanti dall'utilizzo di un *framework* dedicato, seppur sempre basato su tecnologia *open-source*:

1. Maggior grado di personalizzazione delle funzionalità e interfacce
2. Integrazione semplificata con ulteriori sistemi e database
3. Scalabilità ottimizzabile
4. Efficienza operativa nella manutenzione

L'innovazione inoltre risiede nell'utilizzo di protocolli sicuri, come OpenId, permettendo di avere un meccanismo di autenticazione degli utenti sicuro, che prevede ad esempio la gestione centralizzata degli utenti tramite un *Identity Provider* centralizzato, la conformità allo standard OAuth2.0 e l'utilizzo di HTTPS per le comunicazioni con l'IP, proteggendo da attacchi di tipo man-in-the-middle.

Secure Network

Obiettivi - Gli obiettivi che si hanno intenzione di raggiungere riguardano principalmente l'implementazione di uno scenario di *training* e *testing* basato su una serie scenari di attacco realistici così come emergono da una fase preliminare e approfondita di studio delle principali tattiche, tecniche e procedure (TTP) derivanti da attacchi effettivamente accaduti, anche in base a fonti di Threat Intelligence e all'esperienza in materia del personale di Secure Network, nonché dall'analisi dei principali framework in merito (e.g., MITRE ATT&CK).

Gli scenari saranno progettati e implementati in maniera riproducibile, simulando una rete basata sui servizi Microsoft di almeno 32 *host* e contenente i principali servizi che si ritrovano in una tipica rete aziendale, sia riferiti a *server* che riferiti a *client*. Gli scenari implementati includeranno una serie di errori di configurazione e implementazione (scelti tra quelli più comunemente riscontrati durante gli *assessment* che Secure Network effettua verso i propri clienti), che consentiranno a chi si cimenta con la piattaforma di simulare gli scenari di attacco sopra definiti. Il tutto sarà implementato tramite tecniche di *infrastructure-as-code* quali Terraform, Vagrant e Ansible, in modo da consentire la scalabilità e la riproducibilità dell'ambiente anche utilizzando piattaforme di virtualizzazione diversi, e il codice sviluppato verrà rilasciato sotto una licenza *open-source*. Gli attacchi verranno altresì automatizzati mediante la definizione di *script* ad hoc, anch'essi rilasciati sotto licenza *open source*.

Lo scenario di *training* e *testing* verrà infine validato sia in ambiente di laboratorio che in ambiente industriale, mediante la sua erogazione a supporto di uno dei corsi di formazione che Secure Network eroga nei confronti dei propri clienti.

Validità tecnico-scientifica - La validità tecnico scientifica dello scenario di *training* e *testing* implementato verrà garantita dalla presenza di una rigorosa fase di analisi e studio dello stato dell'arte e delle ultime tattiche, tecniche e procedure osservate in attacchi reali. Gli scenari verranno inoltre implementati mediante moderne tecniche di *infrastructure-as-code*, garantendone la piena riproducibilità e portabilità, e la validazione avverrà in maniera rigorosa anche mediante la raccolta strutturata di *feedback* da parte dei partecipanti agli eventi in cui avverrà la validazione, sia in ambiente di laboratorio che in ambiente industriale.

Livello di innovatività - Il principale elemento di innovatività risiede nell'utilizzo di dati e informazioni derivanti da scenari di attacco reali e da tecniche, tattiche e procedure utilizzate in attacchi reali al fine di definire tutto il ciclo di vita di progettazione e sviluppo della piattaforma. Inoltre, la piattaforma verrà interamente rilasciata pubblicamente utilizzando una licenza *open-source*, garantendo quindi la piena accessibilità dei risultati del progetto da parte della più ampia platea di utenti.

Un altro aspetto innovativo risiede proprio nella completa implementazione della piattaforma tramite tecniche di *infrastructure-as-code*, che permette la semplice modificabilità degli scenari implementati e dei relativi errori di configurazione anche in relazione a scenari di attacco che dovessero emergere nel futuro.

C. Adeguatezza dell'implementazione, idoneità e appropriatezza della partnership nonché congruità e pertinenza dei costi

Adeguatezza dell'implementazione (applicazione web) - Per la realizzazione dell'interfaccia grafica del framework ARTIC, il progetto POLARS si avvale di tecnologie web moderne e ampiamente utilizzate e validate nel settore dello sviluppo software. La selezione degli strumenti di sviluppo deve garantire inoltre robustezza, flessibilità e deve essere allineata alle tecnologie attuali. La suite di sviluppo che verrà utilizzata sarà la seguente:

- Angular: un framework di sviluppo *frontend* per applicazioni web che utilizza un'architettura a componenti, il *routing* e la *dependency injection* per consentire uno sviluppo modulare, manutenibile e scalabile.
- Bootstrap: un *framework* CSS per la progettazione di un applicazioni web *responsive* che fornisce componenti predefiniti e un sistema a griglia per interfacce coerenti su diversi dispositivi permettendo di accelerare lo sviluppo *frontend*.
- JavaScript: un linguaggio di programmazione versatile per il web che offre potenza e flessibilità per funzionalità *client-side* complesse con un vasto ecosistema di librerie.
- Node.js: un framework per lo sviluppo *backend* che consente l'esecuzione di codice JavaScript al di fuori del *browser* offrendo prestazioni elevate e scalabilità.

Sulla base di queste tecnologie Nextage ha sviluppato Nx-Frame, un *framework* che consente agli sviluppatori di realizzare un prodotto creando una piattaforma web *full-stack* concentrandosi immediatamente sulla logica applicativa in modo da riducendo così tempi e costi di sviluppo. Nx-Frame è composto da una parte *backend* e da una parte *frontend* dell'applicazione ed è stato progettato per essere *cloud-ready* e scalabile attraverso l'utilizzo dell'architettura Docker. A differenza dei tradizionali DB relazionali, grazie all'utilizzo di un *database* NoSql (MongoDB), viene garantita una forte scalabilità orizzontale, consentendo di gestire e memorizzare una grande quantità di informazioni; tuttavia, è progettato per l'utilizzo parallelo anche di database relazionali, al fine di fornire una soluzione completa e adattabile alle esigenze applicative da affrontare. Nx-Frame è stato progettato secondo i requisiti di "*secure by design*" e "*privacy by design e by default*" al fine di garantire la sicurezza della gestione delle informazioni e la conformità alla normativa GDPR. La combinazione delle tecnologie elencate precedentemente permette di creare un'interfaccia utente ad alto livello di performance, scalabile, facile da mantenere e perciò ideale per le complesse esigenze del framework ARTIC. L'utilizzo di questi strumenti ampiamente adottati nella comunità degli sviluppatori garantisce inoltre l'accesso ad una vasta base di conoscenze e risorse condivise tramite le *community* che faciliteranno sia gli sviluppi che future estensioni e miglioramenti del sistema.

Adeguatezza dell'implementazione (scenario IT di *training* e *testing*) - Per la realizzazione degli scenari di *training* e *testing*, il progetto POLARIS si avvale di tecnologie di virtualizzazione, quali Proxmox, e di *infrastructure-as-code* consolidate secondo le *best practice* attuali, quali Terraform e Ansible. Il codice (al di là dei servizi basati su Microsoft Windows al fine di simulare uno scenario il più possibile realistico) sarà basato il

più possibile su software e progetti open-source, e sarà rilasciato secondo una licenza open source, in modo da garantire l'accessibilità alla più ampia platea di utenti. Gli attacchi verranno automatizzati mediante *script* sviluppati ad-hoc utilizzando il linguaggio di programmazione Python e i suoi più diffusi *framework*, scelti a seconda dello specifico scenario e dello specifico attacco da automatizzare, così come derivante dalla prima fase di analisi e progettazione. Sulla base di queste tecnologie, il consorzio implementerà una base di codice che consentirà, in maniera integrata con la sopracitata interfaccia grafica del framework ARTIC, un semplice *deployment* degli scenari e quindi la riproducibilità degli stessi.

Idoneità e appropriatezza della partnership tra Nextage e Secure Network - Nextage in quanto esperta nello sviluppo di applicazioni web si rivela essere partner fondamentale per il progetto POLARIS, in particolare per lo sviluppo della GUI del framework ARTIC. La sua esperienza è rilevante sia dal punto di vista tecnologico per lo sviluppo sia a livello di sicurezza e conformità grazie alla progettazione del *framework* Nx-Frame, ideato secondo i principi di "*secure by design*" e "*privacy by design e by default*". Nextage si avvarrà anche della consulenza di Gerico Lab dalla fase di progettazione fino alla conclusione degli sviluppi. L'obiettivo è rispondere ai requisiti di business attraverso l'uso di soluzioni che rappresentino lo stato dell'arte nella gestione delle identità, dell'autenticazione e dell'autorizzazione con protocolli standard quali OpenID Connect sul modello architetturale di Google Zanzibar con un approccio all'accesso *user-managed* (UMA). La consulenza durante tutto il progetto garantirà anche il rispetto degli standard e delle *best practice* in termini di scelte non solo architetturali ma anche di configurazione e setup, assicurando i massimi livelli di sicurezza possibili ad oggi. Ad esempio, verrà fornito supporto anche in termini di *hardening* della soluzione, dei corretti e più sicuri meccanismi di comunicazione, dei migliori protocolli e relativa configurazione.

Congruità e pertinenza dei costi - Per quanto riguarda i costi previsti dal progetto per le attività di Nextage, essi riguardano principalmente il costo relativo alle risorse aziendali che saranno coinvolte nello svolgimento delle attività caratterizzanti il progetto. Sono previsti altresì costi di consulenza esterna per, in particolare, le attività caratterizzanti il Task 2.2. Nextage impiegherà un team misto di 11 persone - tra ingegneri, alcuni con dottorato, sviluppatori senior e junior, con comprovata esperienza nello sviluppo software full-stack, IT, e competenze di cybersecurity e sicurezza delle informazioni - per un impegno medio pari al 27% del full-time. Anche per quanto concerne Secure Network i costi riguardano principalmente l'impiego delle risorse aziendali ed i relativi costi. Non sono previsti costi per acquisti e/o consulenza esterna. Secure Network si avvarrà di un team senior composto da 4 ingegneri specializzati in attività di cyber sicurezza e comprovata esperienza internazionale. L'impegno di risorse in rapporto agli obiettivi ed ai risultati attesi del progetto risulta ben equilibrato. Ciò deriva dal fatto che in questa iniziativa convergono percorsi ed esperienze precedenti da cui i proponenti hanno ricavato sia una notevole esperienza in relazione al ruolo ed alle attività di pertinenza, sia l'incremento di *know-how* specifico, tool e procedure di lavoro idonee per assicurare la massima produttività. In tal modo, l'efficienza complessiva, in termini di capacità di ottenere i risultati prefissati utilizzando al meglio le risorse disponibili, risulta ottimizzata, e si spiega anche il limitato ricorso (<15%) a consulenti esterni, che saranno selezionati non per rafforzare numericamente il team di lavoro, ma per fornire un reale valore aggiunto in termini di conoscenze specialistiche non disponibili all'interno del partenariato.

D. Ricadute e impatti attesi

È possibile classificare ricadute e impatti attesi sia per le due aziende che per gli utenti finali dei risultati di progetto, come descritto di seguito.

Nextage **-** Il progetto POLARS permetterà a Nextage di rafforzare le proprie competenze sulle tematiche legate alla sicurezza messe già in atto nei diversi prodotti e progetti che ha sviluppato. Data la fondamentale importanza attribuita a livello aziendale nello sviluppo di applicazioni sicure e alla conoscenza delle diverse componenti di un sistema che possa essere considerato sicuro, Nextage avrà l'opportunità di espandere le sue conoscenze in ambito *cybersecurity*, e in particolare nel contesto *cyber range* che saranno alla base della formazione e della creazione di progetti che si possano ritenere sicuri e che soddisfino i più alti standard di sicurezza.

La creazione di un'applicazione web che permetta di utilizzare metodologie di autenticazione e autorizzazione sicura per accedere a un framework di addestramento per scenari cyber, con tecnologia open-source, permetterà a Nextage, utilizzandolo, di rafforzare la propria offerta di consulenza in ambito Information Security, affiancandovi dei servizi ad alta specializzazione tecnologica quali l'utilizzo dei *cyber range*. Nextage, infatti, potrà proporre ai propri clienti dell'area Governance, certificati ISO/IEC 27001 (Sicurezza delle Informazioni), questo ulteriore servizio relativo alla cyber security. Inoltre, le competenze acquisite saranno in grado di facilitare negli sviluppi futuri di Nextage l'adozione di livelli di sicurezza allo stato dell'arte.

L'opportunità di partecipare a questo bando e la stretta relazione con l'Università di Genova che si instaurerà per lo scambio di informazioni tra il *framework* ARTIC e l'app web sviluppata permetterà a Nextage di ampliare il proprio *network* e relazione con enti accademici, mantenendosi all'avanguardia rispetto agli ultimi avanzamenti scientifici e tecnologici nel campo della *cybersecurity*.

Secure Network **-** Il progetto POLARS permetterà a Secure Network di rafforzare i propri strumenti a disposizione per le attività di formazione tecnica su aspetti legati alla sicurezza informatica e, in particolare, su aspetti legati all'*offensive cybersecurity*. Data la focalizzazione delle attività aziendali, la piattaforma avrà un duplice uso: da un lato, potrà essere utilizzata come piattaforma di formazione interna per il *training* e per la validazione delle competenze del personale tecnico che viene introdotto in azienda oppure per la formazione e l'aggiornamento continuo del personale già presente in azienda.

D'altra parte, la scalabilità della piattaforma consentirà il suo utilizzo presso clienti terzi sia come servizio *stand-alone* che in maniera complementare ai corsi di formazione sul tema che già ad oggi Secure Network eroga, aumentando l'interattività e quindi l'efficacia delle sessioni formative.

End users **-** Gli utenti finali del presente progetto si inseriscono in primis nel solco del target definito nel contesto del progetto ARTIC: personale da formare nel contesto *cybersecurity* e, in particolare, nell'esercitarsi a sfruttare vulnerabilità di diverso genere, in maniera automatizzata e non, in alcuni scenari di reti simulate, sistemi ICT e altre infrastrutture critiche. Le tipologie di figure professionali impattate da attività formative

risultano vaste, dal momento che la presenza di dispositivi hardware e applicazioni software è oggi pervasiva e influenza ogni aspetto della nostra vita quotidiana, comportando implicazioni di sicurezza per aziende e individui.

Il mercato del lavoro richiede sempre più professionisti IT: esperti in tema di sicurezza informatica in grado di identificare gli attacchi e implementare contromisure efficaci, ma anche professionisti con conoscenza delle pratiche di sicurezza informatica tra sviluppatori di software, amministratori di sistema e persino il personale non tecnico. Lo sviluppo della piattaforma POLARS secondo una logica open-source consente la massima diffusione della piattaforma stessa, massimizzando la platea di possibili utilizzatori, e massimizzando l'accessibilità della piattaforma di *training* e *testing* da parte degli utenti finali.

Questo gruppo eterogeneo di stakeholder trarrebbe pertanto vantaggio dall'acquisizione di conoscenze per sviluppare *software* sicuri, configurare sistemi e aumentare la consapevolezza riguardo alle potenziali minacce.

L'obiettivo del progetto POLARS è infatti quello di andare oltre il livello di interfaccia utente previsto fornendo agli utenti un'esperienza di utilizzo più gradevole e semplificata, permettendo loro di concentrarsi sull'esercizio di *cyber range*, non dovendosi preoccupare di lanciare in modalità più di basso livello (ad es. con strumenti a linea di comando) le applicazioni per l'esecuzione degli scenari.

SEZIONE 3) PIANO DELLE ATTIVITA'

A. Work Plan e articolazione delle attività

In Figura 2 viene riportato un riepilogo del GANTT di progetto, riportato in dettaglio nell' "*Allegato D - Cronoprogramma di progetto*".

#	Work package title	Lead partic.	RI/SS	M1	M2	M3	M4	M5	M6	M7	M8	M9	M10	M11	M12
1	WP1	NXT	SS												
	Task 1.1	NXT	SS												
	Task 1.2	NXT	RI												
	Task 1.3	NXT	SS												
2	WP2	NXT	RI												
	Task 2.1	NXT	RI												
	Task 2.2	NXT	RI												
	Task 2.3	NXT	SS												
	Task 2.4	SN	SS												
3	WP3	SN	SS												
	Task 3.1	SN	RI												
	Task 3.2	SN	RI												
	Task 3.3	SN	SS												
	Task 3.4	SN	SS												

Figura 2 - Riepilogo GANTT POLARS

WP1 - Gestione, coordinamento, disseminazione: Il WP1 è trasversale all'intero progetto. Verranno organizzate riunioni di avanzamento almeno mensili di verifica del rispetto delle tempistiche e delle *milestone* previste, in previsione della rendicontazione. Verrà assicurata la massima comunicazione tra i partner per ridurre information gap e inefficienze. Verranno curate le interazioni con l'Università, assicurando l'allineamento con le specifiche durante tutta la durata del progetto. Verrà promossa la disseminazione e la diffusione dei risultati, possibilmente anche tramite convegni, presentazioni al pubblico (come, ad esempio, l'abituale appuntamento scientifico-tecnologico organizzato da Confindustria Genova, il Coffee-Tech) ed eventuali pubblicazioni su riviste scientifiche, definendo in maniera preliminare le modalità di gestione della proprietà intellettuale.

WP2 - Progettazione e sviluppo GUI e meccanismi di autenticazione: Il WP2, il cui leader è Nextage, ha durata pari all'intera durata del progetto, e si concentra su progettazione, implementazione e sviluppo dell'applicazione web. Inizialmente, da M1 a M7, verranno definite le specifiche e i requisiti necessari all'interfacciamento dell'applicazione con il framework ARTIC, tramite anche confronto con UniGe. In parallelo, da M1 a M4, verranno studiate le più adatte tecniche di autenticazione sicura, analizzando le migliori scelte in termini di protocolli da utilizzare. Successivamente, a partire da M5 e fino a M12, verrà messo in atto la fase di sviluppo dell'applicazione, di concerto sia con il programma di lavoro dello Spoke e con il partner che si occupa

di sviluppare uno scenario IT di *cyber range*. Nella parte finale del WP, a partire da M10, ci sarà spazio per la fase di test e collaudo dell'applicazione, in collaborazione con Secure Network, per verificare la corretta comunicazione tra l'applicazione, il *framework* ARTIC e lo scenario sviluppato nel WP3, nonché per uno svolgimento di un *penetration test* conclusivo sull'applicazione sviluppata.

WP3 - Progettazione e implementazione scenari di training e testing: Il WP3, il cui leader è Secure Network, ha durata pari all'intera durata del progetto e si concentra sulla progettazione e implementazione di una piattaforma di *training* e *testing* che simuli uno scenario costituito da una rete aziendale moderatamente complessa (costituita da almeno 32 host) e basata sui servizi di rete Microsoft Windows (e.g., Active Directory, Microsoft Exchange). Gli scenari saranno integrati con il framework ARTIC e l'interfaccia web implementata al WP2. La prima fase, da M1 a M2, sarà costituita da un'analisi dello stato dell'arte in termini di tattiche, tecniche e procedure (TTP) osservate in attacchi reali nonché all'analisi del framework ARTIC e alla definizione dei punti e delle interfacce di integrazione. Successivamente, da M3 a M4, verranno disegnati e definiti gli scenari da implementare nella piattaforma di *training* e *testing*, mediante la definizione dell'architettura della rete da simulare, la scelta dei servizi da implementare e la definizione degli scenari di attacco da considerare anche sulla base di quanto emerso nella fase di analisi preliminare. La terza fase, da M5 a M8, sarà invece rivolta allo sviluppo e all'implementazione degli scenari, nonché all'integrazione degli stessi con ARTIC e con l'applicazione in corso di sviluppo parallelo come parte di WP2. Da ultimo, nella fase conclusiva, da M9 a M12, gli scenari sviluppati e implementati saranno validati sia in ambiente di laboratorio (utilizzando il laboratorio operativo di Secure Network, anche in termini di parziale coinvolgimento di ARTIC e POLARS nei programmi di formazione del personale tecnico che viene introdotto in azienda) che in ambiente industriale (si prevede l'utilizzo, in forma di pilota e a titolo di *proof-of-concept*, di quanto sviluppato nel progetto come parte integrante di un corso di formazione che verrà erogato a un cliente di Secure Network). Il processo di validazione sarà iterativo: dai dati raccolti e collezionati durante l'attività di validazione potranno emergere punti di miglioramento per la piattaforma, che verranno tenuti in considerazione e integrati, a seconda della loro priorità e complessità, come parte di questo progetto o come sviluppi futuri.

Work Package (numero e titolo)	Inizio [mese]	Fine [mese]	Deliverable (numero e titolo)	Persone – mese	Budget
WP1 - Gestione, coordinamento e disseminazione	M1	M12	D1.1 – Comunicazione D1.2 - Gestione conoscenza e IPR	12,43	84.359,40€
WP2 - Progettazione e sviluppo GUI e meccanismi di autenticazione	M1	M12	D2.1 – Definizione progetto e protocolli di autenticazione D2.2 – Sviluppo e test del prototipo	29,26	187.523,15€
WP3 - Progettazione e implementazione scenari di training e testing	M1	M12	D3.1 – Analisi dello stato dell'arte D3.2 – Requisiti e Architettura D3.3 - Sorgenti IaaC, Automazione Attacchi e Manuali d'Uso D3.4 - Rapporti di Test	19,02	133.515,00€
Totale	**Durata 12 mesi**		**8 Deliverable**	**60,70**	**405.397,55€**

B. Articolazione del Progetto in Work Packages

Work Package n. 1	**Inizio attività (mese): M1**		**Fine attività (mese): M12**	
Titolo Work package: Gestione, coordinamento, disseminazione				
Tipo: Sviluppo Sperimentale				
Work Package Leader: Nextage				
n. partner coinvolti	1	2	3	**Tot.**
Nome partner	Nextage	Secure Network	-	**2**
Mesi/persona	4,90	7,53	-	**12,43**
Obiettivi: L'obiettivo principale del presente WP è quello di garantire il corretto avanzamento del progetto e il raggiungimento delle *milestone* prefissate rispondendo ai *target* definiti. Inoltre, il WP ha come obiettivi il garantire un puntuale e proficuo scambio di informazioni con lo Spoke Serics, e la corretta pianificazione ed effettuazione della *dissemination* del progetto e dei suoi risultati.				
Task 1.1 – Gestione progetto (SS) – (*Nextage, Secure Network*). Supervisione e coordinamento continuo delle attività del progetto, inclusa la pianificazione, l'allocazione delle risorse, il monitoraggio dei progressi e la comunicazione tra partner, e la definizione preliminare delle modalità di gestione della proprietà intellettuale.				
Task 1.2 – Coordinamento tecnico-scientifico con Serics (RI) – (*Nextage, Secure Network*). Interazione e confronto con l'Università di Genova (Spoke Serics) riguardo specifiche e requisiti dell'applicazione web, in modo da garantire l'integrabilità della stessa con il *framework* ARTIC, e successive riunioni in fase di sviluppo per quanto riguarda scambi di informazioni su test e collaudi degli scenari IT *cyber range*.				
Task 1.3 – Disseminazione (SS)– (*Nextage, Secure Network).* Verrà promossa la disseminazione e la diffusione dei risultati, possibilmente anche tramite convegni, presentazioni al pubblico e pubblicazioni su riviste scientifiche. Verranno messi a disposizione dell'università i canali aziendali per comunicare informazioni relative al progetto, amplificando quelli abituali.				
Descrizioni costi vivi previsti e associati al WP tra cui consulenza esterna, contratti di ricerca e acquisto di materiale: I costi previsti riguardano principalmente il costo relativo alle risorse aziendali che saranno coinvolte nello svolgimento delle attività caratterizzanti il WP. Le figure professionali previste avranno un profilo Senior sia per le attività di *management*, sia per quanto riguarda il coordinamento tecnico-scientifico. Verranno poi allocate figure specializzate in comunicazione al fine di rendere efficaci le attività di *dissemination* e valorizzazione dei risultati del progetto. Non sono previsti costi per acquisto materiali, consulenza esterna e contratti di ricerca.				
Deliverables:				
D1.1 – Comunicazione	Materiale di comunicazione: Report dell'agenda dei post *social* (es. LinkedIn) sul progetto, calendario degli eventi di *dissemination*, dettagli riguardanti strategie di pubblicazione su riviste scientifiche dedicate [consegna M12].			
D1.2 - Gestione conoscenza e IPR	Definizione preliminare delle modalità di gestione della proprietà intellettuale [consegna M12].			

Work Package n. 2	**Inizio attività (mese): M1**		**Fine attività (mese): M12**	
Titolo Work package: Progettazione e sviluppo GUI e meccanismi di autenticazione				
Tipo: Ricerca Industriale				
Work Package Leader: Nextage				
n. partner coinvolti	1	2	3	**Tot.**
Nome partner	Nextage	Secure Network	-	**2**
Mesi/persona	27,23	2,03	-	**29,26**

Obiettivi: Gli obiettivi del WP prevedono la progettazione di un'applicazione web che sfrutti metodologie di autenticazione sicura per accedere in maniera *user-friendly* ai *cyber range* previsti dal *framework* ARTIC e allo scenario IT sviluppato nel WP3.

Task 2.1 – Progettazione applicazione web (RI) – (*Nextage, Secure Network).* Definizione e sviluppo dell'architettura dell'applicazione web, comprensiva della scelta delle tecnologie, del *design* dell'interfaccia utente e della struttura delle funzionalità, con focus su esperienza utente intuitiva e integrazione dei protocolli di autenticazione e autorizzazione richiesti.

Task 2.2 – Studio di metodi di autenticazione sicuri (RI) – (*Nextage, Secure Network).* Analisi approfondita dei protocolli di autenticazione e autorizzazione sicuri, condotta con consulenza di azienda di *cybersecurity*, per identificare e implementare soluzioni avanzate e standardizzate come OpenID Connect.

Task 2.3 – Sviluppo e implementazione applicazione web (SS) – (*Nextage, Secure Network).* Realizzazione dell'applicazione web, includendo codifica, utilizzo dei protocolli di autenticazione e autorizzazione, test di funzionalità e sicurezza, e distribuzione finale, assicurando conformità ai requisiti progettuali e prestazioni.

Task 2.4 – Collaudo e test scenario (SS) – (*Secure Network, Nextage).* Esecuzione di test di integrazione e collaudo, inclusi *penetration test*, dell'applicazione web con lo scenario sviluppato nel WP3 e il *framework* ARTIC, per verificare funzionalità, sicurezza, interoperabilità e conformità agli standard richiesti.

Descrizioni costi vivi previsti e associati al WP tra cui consulenza esterna, contratti di ricerca e acquisto di materiale: i costi previsti per il WP2 riguardano i costi relativi a progettisti e sviluppatori *backend* e *frontend* di applicazioni web. Saranno coinvolti profili Senior per quanto riguarda le attività di analisi e progettazione architetturale e profili Junior per le attività di sviluppo. Inoltre, si prevede una figura Senior nel ruolo di Team Leader. Sono previsti altresì costi di consulenza esterna per, in particolare, le attività caratterizzanti il Task 2.2.

Deliverables:

D2.1 – Definizione progetto e protocolli di autenticazione	Raccoglie e specifica i requisiti funzionali e non funzionali del progetto, integrando l'analisi e la consulenza sui protocolli di autenticazione e autorizzazione sicuri [consegna M7].
D2.2 – Sviluppo e test del prototipo	Prototipo funzionante dell'applicazione web, corredato di documentazione tecnica e dei risultati dei test di integrazione e collaudo, inclusi i test con lo scenario sviluppato nel WP3 e il *framework* ARTIC [consegna M12].

Work Package n. 3	**Inizio attività (mese): M1**		**Fine attività (mese): M12**	
Titolo Work package: Progettazione e implementazione scenari di training e testing				
Tipo: Sviluppo Sperimentale				
Work Package Leader: Secure Network				
n. partner coinvolti	1	2	3	**Tot.**
Nome partner	Secure Network	-	-	**1**
Mesi/persona	19,02	-	-	**19,02**

Obiettivi: Gli obiettivi del WP prevedono la progettazione e implementazione di uno scenario di *training* che simula una rete aziendale moderatamente complessa basata principalmente sui servizi Microsoft (Active Directory, Exchange), includendo ove necessario anche altri sistemi (e.g., Linux) per una simulazione realistica.

Task 3.1 – Analisi dello stato dell'arte e contestualizzazione della piattaforma ARTIC (RI) – (*Secure Network).* Analisi delle principali tattiche, tecniche e procedure (TTP) pubbliche o derivanti da informazioni di Threat Intelligence, anche sulla base di *framework* ATT&CK ed esperienza di Secure Network. Analisi della piattaforma ARTIC e definizione dei punti e delle interfacce di integrazione con il risultato di questo WP.

Task 3.2 – Definizione e progettazione degli scenari (RI) – (*Secure Network).* Definizione dell'architettura della rete o delle reti da simulare nello scenario proposto, dei servizi da includere, nonché degli scenari di attacco da riprodurre sulla base di TTP e informazioni acquisite al Task 3.1.

Task 3.3 – Implementazione e automazione della creazione degli scenari (SS) – (*Secure Network).* Implementazione di uno o più scenari sulla base di quanto definito al Task 3.2, inclusa l'automazione del *deployment* sulla base di tecniche di *infrastructure-as-code* e l'automazione degli attacchi mediante *script* ad hoc.

Task 3.4 – Convalida della tecnologia in laboratorio e in ambiente industriale (SS) – (*Secure Network). Testing* e convalida e utilizzo dello scenario in ambiente di laboratorio e come parte di un corso di formazione presso un cliente terzo. Raffinamento della soluzione sulla base delle risultanze delle attività di convalida.

Descrizioni costi vivi previsti e associati al WP tra cui consulenza esterna, contratti di ricerca e acquisto di materiale: i costi previsti per il WP3 riguardano quelli relativi a esperti di sicurezza, progettisti e sviluppatori coinvolti nei diversi *task* che costituiscono il WP. Non sono previsti contratti di consulenza esterna.

Deliverables:

D3.1 – Analisi dello stato dell'arte	Sintetizza le risultanze dell'analisi dello stato dell'arte in termini di TTP e scenari di attacchi reali, da utilizzare come *input* per le fasi successive [consegna M2].
D3.2 – Requisiti e Architettura	Elenca i requisiti tecnici da soddisfare nelle successive fasi progettuali e schematizza l'architettura ad alto livello dello scenario [consegna M4].
D3.3 - Sorgenti IaaC, Automazione Attacchi e Manuali d'Uso	*Repository* di codice sorgente per automazione della creazione degli scenari e degli attacchi, corredato di documentazione tecnica e manuali d'uso [consegna M8].
D3.4 - Rapporti di Test	Sintesi delle attività di test svolto e delle osservazioni mosse durante le attività, anche mediante *feedback* attivo da parte dei partecipanti [consegna M12].

C. Milestone di progetto

Numero Milestone	Nome Milestone	Descrizione e obiettivi della Milestone	Data di conseguimento	Modalità di verifica (*)
1	Kickoff con UniGe	Incontro con UniGe per co-definizione e progettazione delle attività.	M1	Aver effettuato almeno un incontro con l'Università e aver redatto un documento tecnico con le linee guida progettuali derivanti.
2	Termine fase raccolta specifiche e progettazione	L'obiettivo è quello di verificare la conclusione della fase di progettazione delle varie componenti del sistema, incluse le specifiche dell'applicazione web, le metodologie di autenticazione e autorizzazione, e le caratteristiche dello scenario *cyber range* di test.	M7	Documentazione tecnica contenente le specifiche tecniche e i risultati concordati con UniGe.
3	Rilascio di software e documentazione	Lo scopo della milestone è verificare il termine dello sviluppo di tutte le componenti del sistema, e della loro interazione (applicazione e scenario di *training* e *testing* - *cyber range*).	M12	Prototipi testati e funzionanti; documentazione di sviluppo e utilizzo completati.

Allegato 1 - Requisito di sostenibilità ambientale e principio DNSH

I proponenti devono stabilire quali dei sei obiettivi ambientali, previsti all'art 17 del Reg. (UE) 2020/85217 (Danno significativo agli obiettivi ambientali), e riportati in tabella, richiedono una valutazione di fondo DNSH in relazione alla proposta progettuale.

Indicare il rispetto tra gli obiettivi ambientali in relazione alla proposta progettuale		**Si/No**	**Motivazione**
Mitigazione dei cambiamenti climatici	NON porta a significative emissioni di gas serra (GHG).	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo. *Il prototipo ottenuto nel progetto operando in ambito cyber security, potrebbe consentire in futuro di prevenire downtime significativi che potrebbero portare a inefficienze energetiche o all'utilizzo eccessivo di risorse per il ripristino.*
Adattamento ai cambiamenti climatici	NON determina un maggiore impatto negativo del clima attuale e futuro, sull'attività stessa o sulle persone, sulla natura o sui beni.	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo. *Il progetto prevede lo sviluppo di software efficiente che riduce il carico di lavoro sui server e, di conseguenza, il consumo energetico*.
Uso sostenibile e protezione delle acque e delle risorse marine	NON è dannosa per il buono stato dei corpi idrici (superficiali, sotterranei o marini) determinandone il loro deterioramento qualitativo o la riduzione del potenziale ecologico.	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo. *Non sono previste attività di smaltimento di strumentazione hardware nel corso del progetto.*

Economia circolare, compresi la prevenzione e il riciclaggio dei rifiuti	NON porta a significative inefficienze nell'utilizzo di materiali recuperati o riciclati, ad incrementi nell'uso diretto o indiretto di risorse naturali, all'incremento significativo di rifiuti, al loro incenerimento o smaltimento, causando danni ambientali significativi a lungo termine;	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo *Per il progetto non sono previsti acquisti di nuove tecnologie. Verranno invece utilizzate tecnologie già in uso.*
Prevenzione e riduzione dell'inquinamento dell'aria, dell'acqua o del suolo	NON determina un aumento delle emissioni di inquinanti nell'aria, nell'acqua o nel suolo;	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo. *Non sono previste attività di smaltimento di strumentazione hardware nel corso del progetto.*
Protezione e ripristino della biodiversità e degli ecosistemi	NON determina un aumento delle emissioni di inquinanti nell'aria, nell'acqua o nel suolo;	Sì	Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo. *Il progetto prevede lo sviluppo di software efficiente che riduce il carico di lavoro sui server e, di conseguenza, il consumo energetico e NON prevede attività di smaltimento di strumentazione hardware nel corso del progetto.*

Qualora la risposta sia «si», i proponenti sono invitati a fornire una breve giustificazione (nella colonna di destra) del motivo per cui l'obiettivo ambientale non richiede una valutazione di fondo DNSH della misura, sulla base di uno dei seguenti casi, da indicare:

A. Il progetto ha un impatto prevedibile nullo o trascurabile sull'obiettivo ambientale connesso agli effetti diretti e agli effetti indiretti primari della misura nel corso del suo ciclo di vita, data la sua natura, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo;

B. Il progetto ha un coefficiente 100 % di sostegno a un obiettivo legato ai cambiamenti climatici o all'ambiente, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo;

C. Il progetto «contribuisce in modo sostanziale» a un obiettivo ambientale, ai sensi del regolamento UE) 2020/85217, e in quanto tale è considerata conforme al principio DNSH per il pertinente obiettivo.

Qualora la risposta sia «no», i proponenti sono invitati ad indicare nella motivazione:

D. Il progetto richiede una valutazione DNSH complessiva.

e saranno invitati a procedere alla fase 2 della lista di controllo per gli obiettivi ambientali corrispondenti.

BARBARA
CANESI
25.07.2024
14:11:51
GMT+01:00