



UNIONE EUROPEA
Fondo Sociale Europeo



PROGRAMMA OPERATIVO NAZIONALE RICERCA E INNOVAZIONE 2014-2020

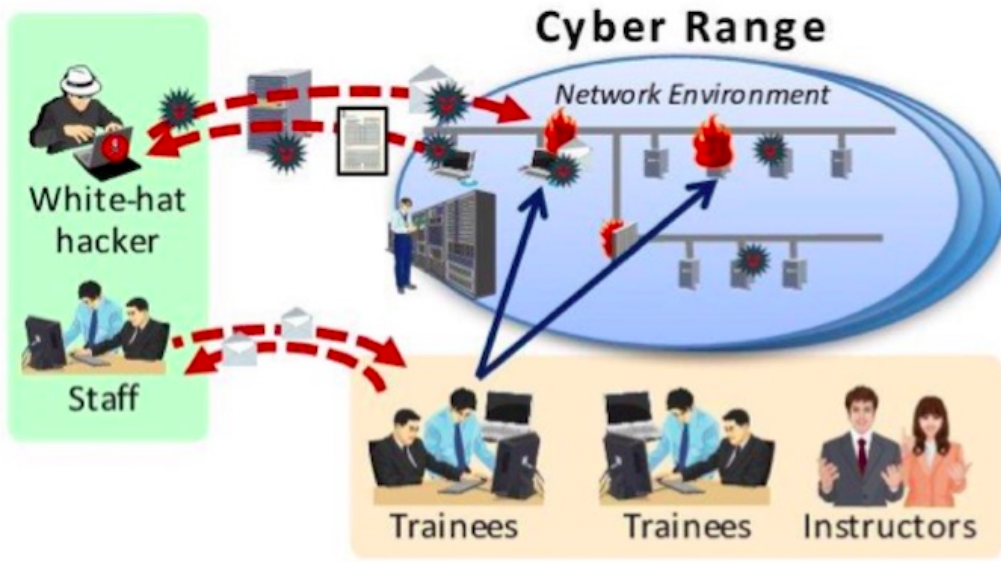
Dottorati Innovativi con caratterizzazione industriale

a.a. 2020/2021 - CICLO XXXVI

aggiornato il 24/09/20 alle ore 11:58

Borse richieste

BORSA n. 2

A. RICERCA PROPOSTA	
<p>a. Tema della ricerca, evidenziandone la coerenza con la Strategia Nazionale di Specializzazione Intelligente (SNSI)</p>	<p>Next-generation CyberRange-as-a-Service</p> <p>I Cyber Range ("Poligoni Virtuali") sono ambienti esercitativi per il potenziamento delle capacità di difesa dei sistemi ICT dalle minacce cibernetiche. I Cyber Range supportano la formazione del personale sui vari aspetti della cybersecurity; l'addestramento di operatori preposti alla difesa dei sistemi ICT; il testing e valutazione degli strumenti di difesa; lo sviluppo di strategie, tattiche e tecniche per contrastare le minacce.</p>  <p>La ricerca mira a sviluppare una piattaforma di Cyber Range di nuova generazione, che si integri con le moderne tecnologie di cloud computing e con il paradigma "as-a-service", per creare ambienti esercitativi di elevata complessità (per quantità e diversità di servizi, elementi di rete, etc.), che simulino in maniera realistica i sistemi ICT utilizzati nelle grandi organizzazioni.</p> <p>Il tema è trasversale a molte delle aree tematiche della Strategia Nazionale di Specializzazione Intelligente (SNSI). Le infrastrutture di cloud computing sono la tecnologia abilitante alla base dei servizi innovativi per la fabbrica intelligente, per la mobilità sostenibile, per la distribuzione dell'energia, per la telemedicina. Ad esempio, sia l'università proponente sia l'azienda partner hanno progetti sull'utilizzo di tecnologie cloud con grandi aziende nei settori dell'energia, del trasporto ferroviario, delle telemedicina, e della industria 4.0. Tali servizi innovativi richiederanno algoritmi complessi su grosse moli di dati, da distribuire su cloud. Inoltre, la SNSI evidenzia la criticità dell'uso delle infrastrutture di calcolo nell'Aerospazio e Difesa (es., veicoli unmanned, air traffic management). Si pone quindi il problema di garantire la cybersecurity di tali infrastrutture, al fine di</p>

	<p>fronteggiare attacchi che potrebbero causare conseguenze catastrofiche sugli utenti e sull'ambiente. La proposta mira a simulare scenari di attacco su una controparte virtuale di tali infrastrutture, consentendo al personale di migliorare capacità e responsività agli attacchi, e di identificare in anticipo le debolezze dei propri sistemi.</p> <p>La ricerca sarà svolta in collaborazione con la System Management SpA (SM). SM è un fornitore di soluzioni ICT che opera nei settori telecomunicazioni, sicurezza informatica, new media, system integration e analisi dei dati. L'azienda, localizzata a Napoli con sedi operative a Roma e Milano, è coinvolta nella pianificazione e nello sviluppo di sistemi e soluzioni che integrano l'ICT con l'automazione industriale, le soluzioni high tech, la sicurezza informatica, e la gestione e l'analisi dati. Nel settore sicurezza informatica, l'azienda è impegnata nello sviluppo di una piattaforma per governare attività di addestramento e esercitazioni della cyber-security (Sistema C2 nato in seno al progetto UNAVOX), di sistemi per intercettazioni telematiche multi-canale (Sistema ELISA), e di sistemi per l'analisi intelligente del traffico dati di rete.</p>
<p>b. Attività di ricerca proposta, metodologie e contenuti</p>	<p>La ricerca svilupperà nuove tecniche di Cyber Range, integrandole in una piattaforma di nuova generazione, dotata delle seguenti capacità innovative:</p> <ul style="list-style-type: none"> ● Istanziare scenari di reti virtuali su larga scala, mettendo in cloud le risorse di calcolo di datacenter privati dell'organizzazione. ● Clonare una infrastruttura aziendale all'interno dello scenario virtuale ("digital twin"), per emulare utenti, risorse, processi, e traffico di rete della infrastruttura aziendale, senza interferire con la infrastruttura reale. ● Facilitare la gestione di scenari esercitativi complessi, fornendo un linguaggio ad alto livello (domain-specific) e dashboard visuali per interagire con la piattaforma. ● Monitorare le attività dei partecipanti in maniera invisibile agli stessi e automatica, sfruttando tecnologie di virtual machine introspection a livello hypervisor, in modo da fornire un feedback dettagliato agli organizzatori. ● Affiancare il personale impegnato nelle esercitazioni con attori (attaccanti/difensori) simulati tramite tecniche di intelligenza artificiale, in modo da consentire le esercitazioni anche a gruppi ristretti di persone. <p>La piattaforma agevererà la creazione di scenari esercitativi complessi, tramite un linguaggio ad alto livello con cui descrivere servizi, dati, utenti e vulnerabilità di interesse. La piattaforma consentirà di creare un modello statistico delle infrastrutture aziendali esistenti; in questo modo, gli organizzatori dei CyberRange potranno progettare esercitazioni realistiche, senza dover modellare i dettagli della infrastruttura virtuale. Il modello statistico garantirà la riservatezza dei dati sensibili aziendali, poiché la simulazione genererà una versione diversa e anonimizzata della infrastruttura e di utenti, risorse e traffico.</p> <p>Saranno sviluppate tecniche di monitoraggio per tracciare le attività dei "red" e "blue team" non tradizionali (a livello di host e di rete), bensì a livello di hypervisor, in modo da essere invisibili ai team e per ridurre l'onere di gestione degli host. I dati di monitoraggio saranno utilizzati per analizzare in modo automatico il comportamento dei partecipanti all'esercitazione, evitando l'onere manuale dei "white team".</p> <p>Saranno studiate tecniche di intelligenza artificiale per emulare le azioni degli attori, difensori e attaccanti. In questo modo, l'esercitazione di un team difensore non richiederà un team di attaccanti (e viceversa): la controparte sarà simulata da agenti intelligenti. Questa soluzione renderà le esercitazioni meno costose. Inoltre, saranno possibili esercitazioni con soli agenti intelligenti, permettendo ai "white team" di valutare se l'infrastruttura ha punti deboli. Tale paradigma è simile a quello utilizzato dai sistemi di IA per apprendere come vincere una competizione (es., AlphaGo di Google DeepMind); in questo caso, il sistema apprende come difendere al meglio l'infrastruttura.</p>
<p>c. Grado di innovazione della ricerca proposta per il settore di intervento</p>	<p>Il grado di innovazione della ricerca proposta può considerarsi estremamente elevato, dal punto di vista sia tecnologico, poiché saranno sviluppati nuovi sistemi basati su tecnologie hypervisor e di cloud computing, sia metodologico, poiché le soluzioni utilizzeranno tecniche statistiche e di intelligenza artificiale per migliorare il realismo delle esercitazioni.</p> <p>I sistemi di cyber-range esistenti hanno elevati costi di gestione e scarsa flessibilità, richiedendo un significativo intervento manuale da parte dei gestori per: (1) creare le macchine e le reti da utilizzare nella esercitazione; (2) configurare l'ambiente per simulare in maniera realistica l'infrastruttura aziendale; (3) analizzare le attività dei partecipanti per fornire loro un feedback; (4) coinvolgere un alto numero di unità di personale per ricoprire i vari ruoli della esercitazione (con relativi costi di ore-uomo).</p> <p>La proposta mira a ridurre il costo e la difficoltà per gestire esercitazioni efficaci, attraverso: (1) tecnologie di cloud computing per rendere automatica, veloce e scalabile la creazione degli scenari; (2) modelli statistici per profilare una infrastruttura aziendale e crearne una controparte virtuale che sia realistica ma senza violare la riservatezza dei dati aziendali; (3) monitoraggio, in maniera non intrusiva ed automatica, delle attività dei partecipanti; (4) affiancamento con partecipanti simulati, basati su agenti intelligenti.</p> <p>I seguenti Key Performance Indicators (KPI) verranno utilizzati per valutare l'impatto della ricerca</p>

	<p>nel conseguire cyber-range efficienti, realistici, e in grado di preservare la riservatezza dei dati. Tempo di creazione di nuovi scenari esercitativi</p> <p>ESISTENTE: Da alcune ore, fino ad alcuni giorni (uso di molti tool a livello di rete e di host, senza il supporto di astrazioni ad alto livello).</p> <p>PROPOSTA: Decine di minuti (supporto dato da un nuovo linguaggio ad alto livello, e da API e dashboard visuali user-friendly, pieno automatismo end-to-end).</p> <p>Valutare e fornire feedback ai partecipanti</p> <p>ESISTENTE: Da alcune ore, fino ad alcuni giorni (monitoraggio fai-da-te e intrusivo, analisi manuale di tracce e log).</p> <p>PROPOSTA: Decine di minuti (monitoraggio incorporato a livello hypervisor, tecniche di correlazione dei dati da più fonti).</p> <p>Realismo della infrastruttura simulata dal cyber-range</p> <p>ESISTENTE: Basso/moderato (è richiesto un grosso sforzo manuale per configurare reti e macchine)</p> <p>PROPOSTA: Moderato/alto (Possibilità di combinare e personalizzare un catalogo di configurazioni e di vulnerabilità. Uso di modelli data-driven per generare topologie e configurazioni realistiche)</p> <p>Protezione delle informazioni sensibili</p> <p>ESISTENTE: A rischio di fuoriuscita (eseguono i cyberrange su infrastrutture esterne. Lo scenario può accidentalmente contenere info riservate)</p> <p>PROPOSTA: Pienamente protette (I dati non lasciano mai il data center privato. Gli scenari sono repliche anonimizzate della infrastruttura aziendale)</p>
<p>d. Coerenza del tema di ricerca con l'ambito disciplinare del dottorato e con la composizione del Collegio dei docenti</p>	<p>Il programma affronta diversi problemi aperti nell'ambito della cybersecurity da una prospettiva interdisciplinare. A differenza dell'attuale didattica rivolta all'alta formazione nell'ambito della ricerca, il progetto propone un alto livello di interazione tra esperti di sicurezza e i ricercatori di diverse discipline. Infatti, da un punto di vista intellettuale, la proposta riunisce connessioni interdisciplinari tra diversi di temi di ricerca, cercando di unire il campo della Intelligenza Artificiale con quelli della Software Security e dell'Ingegneria dei Sistemi di Elaborazione.</p> <p>In tal senso il programma di ricerca e di formazione prevede la più ampia partecipazione della comunità scientifica del DIETI e del suo Collegio di Dottorato nell'ambito di discipline della cybersecurity e del machine learning. Tutte queste aree di competenza, fondamentali per la definizione del programma di dottorato in Ingegneria Elettrica e Tecnologia dell'Informazione, trovano naturale espressione grazie ad una significativa esperienza da parte dei diversi membri che costituiscono il comitato e il collegio di dottorato. In sintesi, i membri dell'ITEE, composti da docenti e ricercatori con comprovate capacità in campi complementari, fortemente integrati dalle collaborazioni strategiche con il mondo industriale, garantiscono la fattibilità e l'appropriatezza della proposta.</p> <p>La formazione permetterà la costituzione di una nuova generazione di ingegneri esperti in grado di applicare le più avanzate tecnologie di machine learning e di avere un'ampia conoscenza degli attacchi software più conosciuti. Ciò sarà realizzato, nell'ambito del corso di dottorato ITEE, con una ampia formazione di ricerca, attingendo sia da corsi specificatamente attivati dal corso di dottorato ITEE e dedicati ai dottorandi, quali ad esempio i corsi "Virtualization technologies and their applications" e "Advanced techniques for software robustness and security testing" già esistenti, ed ulteriori corsi di prossima attivazione; sia dai corsi della laurea magistrale in ingegneria informatica incardinati nei due curriculum "Ingegneria dei Dati e dell'Intelligenza Artificiale" e "Cyber-Security", che includono entrambi corsi verticali ad elevata specializzazione quali "Software Security", "Network Security", "Big Data Engineering", "Information Systems and Business Intelligence" e "Advanced Machine Learning".</p>
<p>e. Fattibilità tecnica della proposta e cronoprogramma di attuazione</p>	<p>La proposta si articola su 36 mesi, durante cui il dottorando studierà lo stato dell'arte, per poi progettare e sperimentare le soluzioni innovative.</p> <p>La ricerca è articolata nei seguenti workpackages.</p> <p>WP1 - Engine per la virtualizzazione di cyber-range</p> <p>Nel primo anno sarà realizzato un "engine", base degli studi del progetto. La sua caratteristica sarà la possibilità di modellare scenari esercitativi complessi, tramite un linguaggio domain-specific, che permetterà agli organizzatori di definire ad alto livello servizi, risorse (es., utenti e dati da</p>

	<p>proteggere), comportamenti (leciti e malevoli) e vulnerabilità.</p> <p>Lo engine convertirà la descrizione (ad alto livello) degli scenari in operazioni (a basso livello) sulla infrastruttura, con tecnologie di Infrastructure-as-a-Service ed Infrastructure-as-code. Esso sarà basato sulla piattaforma standard di cloud computing OpenStack, e dotato di un repository di configurazioni host di server e client, e di dashboard visuali per gli organizzatori (es. "white teams", "yellow teams"), con vulnerabilità combinabili per realizzare nuovi scenari esercitativi.</p> <p>WP2 - Tecniche di simulazione degli scenari e di monitoraggio Nel secondo anno la piattaforma sarà estesa con una tecnica avanzata per la simulazione realistica di utenti, risorse, processi e traffico di rete della infrastruttura aziendale. La tecnica si baserà su dati raccolti dalla infrastruttura esistente, utilizzati per creare un modello statistico del comportamento degli utenti e della distribuzione delle risorse e del traffico. Il modello sarà poi utilizzato per generare scenari esercitativi sulla infrastruttura virtualizzata, rappresentativa di quella reale e anonimizzata da dati sensibili dell'azienda.</p> <p>Sarà inoltre realizzato un sistema di monitoraggio hypervisor-based per tracciare le attività dei team (es. tentativi di connettersi a un nodo, esecuzione di codice malevolo). Si utilizzeranno tecniche di "virtual machine introspection" invisibili ai team, per maggiore realismo e per ridurre l'onere di gestione degli host (es., non richiedendo di installare nuovi processi). Il monitoraggio sarà implementato come moduli dell'hypervisor (Linux/KVM o altro hypervisor di interesse per l'azienda). I dati di monitoraggio saranno utilizzati per analizzare il comportamento dei partecipanti all'esercitazione.</p> <p>WP3 - Simulazione di attori basati su intelligenza artificiale L'ultima parte riguarderà l'uso di tecniche di IA nelle esercitazioni. Saranno sviluppati agenti software in grado di effettuare le azioni degli attori, sia offensive sia difensive. Gli agenti, basati su tecniche di "reinforcement learning", effettueranno, in base a politiche configurate in fase di addestramento, sequenze di azioni per portare il sistema in uno stato desiderato (es., violare una risorsa protetta o respingere un attacco). I dati di monitoraggio (raccolti con gli strumenti sviluppati nel WP2) saranno utilizzati per fornire feedback ("reward") agli agenti.</p>
<p>f. Sinergie rispetto all'eventuale successivo impiego dei dottori di ricerca (in rapporto al mondo del lavoro)</p>	<p>Il programma di ricerca e di formazione è stato progettato in risposta all'esigenza di avere infrastrutture informatiche sempre più sicure. Secondo l'Osservatorio Cybersecurity & Data Protection, promosso dalla School of Management del politecnico di Milano, il mercato dell'Information Security del 2019 ha raggiunto un valore di 1,317 miliardi di euro, in crescita di poco meno dell'11% rispetto all'anno precedente (dopo aver registrato un +9% nel 2018 e un +12% nel 2017). La spesa in sicurezza si concentra soprattutto in soluzioni di security, che raccolgono il 52% degli investimenti (in particolare per componenti di sicurezza più tradizionali), a fronte del 48% nei servizi che però crescono maggiormente (in crescita per il 45% delle aziende). La tecnologia al centro dell'attenzione è l'Artificial Intelligence, già impiegata per la gestione della sicurezza dal 45% delle grandi imprese. Un siffatto andamento scatena una forte richiesta di "ingegneri della cybersecurity" che oggigiorno il paese non è in grado di soddisfare.</p> <p>Il programma di ricerca soddisferà le attuali esigenze di formazione degli ingegneri in relazione alle richieste di una nuova generazione di metodi di cybersecurity. Pertanto, lo studente del dottorato avrà un'opportunità unica di acquisire un ampio spettro di nozioni, che vanno dagli aspetti puramente scientifici/teorici fino agli aspetti orientati all'implementazione, nonché altamente specializzati, dei problemi oggetto della proposta. Avrà anche la possibilità di confrontarsi continuamente con il lavoro di gruppo.</p> <p>Alla fine del periodo di dottorato, è ragionevole ritenere che lo studente di dottorato avrà acquisito oltre una competenza specifica sia nel campo dell'intelligenza artificiale che nel campo della cybersecurity. Lo studente al conseguimento del titolo si proporrà nel mondo del lavoro come un "problem solver" con alta qualificazione scientifica in grado di ricoprire profili professionali di elevato livello grazie alla capacità di affrontare in modo autonomo i problemi ed alla predisposizione a lavorare in team, spesso in contesti di carattere internazionale. Ciò permetterà al mondo industriale di assorbire un ingegnere nella propria forza lavoro e includerlo nel proprio team di innovazione.</p>
<p>B. ATTIVITA' DA SVOLGERE PRESSO L'IMPRESA con sede nell'intero territorio nazionale</p>	
<p>a. Attività di ricerca da svolgere presso l'impresa</p>	<p>System Management è impegnata nella realizzazione della piattaforma UNAVOX - poligono virtuale per l'addestramento di utenti civili e militari all'interno di un ambiente di simulazione votato alla creazione di contesti realistici di cyber-warfare. Il progetto è sviluppato nell'ambito del Programma Nazionale di Ricerca Militare per il Segretariato Generale della Difesa.</p> <p>L'attività di System Management prevede lo sviluppo del sistema centrale di coordinamento e controllo delle attività di gioco - il Sistema Comando e Controllo (C2) il cui scopo è governare e monitorare i processi all'interno di un Battle-Lab. Caratteristica innovativa del sistema C2 è la capacità di gestire i processi di gioco in modo completo, governandone tutte le fasi dalla progettazione degli scenari, alla pianificazione, briefing, esecuzione e finalizzazione. C2 consente di</p>

	<p>disegnare e rappresentare un'intera infrastruttura ICT composta da nodi, reti, sistemi, dipartimenti, apparati di rete, componenti software, etc. Nella fase di pianificazione si possono definire le caratteristiche dei gruppi di gioco, le fasi di gioco e il materiale necessario a condurre correttamente le attività esercitative. Nelle fasi attive di gioco (esecuzione) la piattaforma C2 dispiega in modo automatico l'intera infrastruttura di gioco insieme a sistemi di supporto necessari a raccogliere dati e valutare lo stato e l'andamento delle operazioni. Durante il gioco il sistema fornisce interfacce di supporto a tutti i diversi giocatori impegnati (attaccanti, difensori, valutatori, ops, testers, analisti, etc).</p> <p>La ricerca promuoverà sinergie con l'azienda nello sviluppo di nuovi elementi della piattaforma, legati ad un modello avanzato di rappresentazione delle infrastrutture ICT per attività CyberRange (vulnerabilità, comportamenti, prescrizioni, regole di controllo, etc) e per la progettazione e prototipazione di un sistema automatico che simuli il comportamento dei team di gioco (con particolare riferimento ai red team e blue team).</p> <p>L'azienda ospiterà il dottorando nel corso della terza spira del progetto UNAVOX - fase essenziale in cui posizionare le componenti innovative sulla piattaforma - in modo da favorire l'identificazione dei requisiti e della definizione di una roadmap tecnica per la realizzazione delle componenti innovative che saranno inserite all'interno del progetto.</p> <p>L'attività in azienda permetterà al dottorando di collaborare con i suoi ingegneri nella integrazione della soluzione e nella sua validazione con casi di studio aziendali. La co-supervisione contribuirà inoltre alla realizzazione di soluzioni adatte ad essere applicate in contesti reali, identificando in anticipo le difficoltà tecniche (es., legate alla modellazione degli utenti, traffico e risorse delle infrastrutture aziendali, alla definizione di scenari e di vulnerabilità realistiche) che determinano il successo della transizione da prototipo di ricerca a innovazione utilizzabile in contesti industriali.</p>
b. Denominazione dell'impresa presso cui verrà svolta l'attività relativa al tema di ricerca	System Management SpA
c. Sede legale dell'impresa (Città, Provincia, indirizzo)	Città: NAPOLI Provincia: NA Indirizzo: Via G. Porzio, 4 Centro Direzionale - Is. E7, 80143 Napoli
d. Sede operativa principale (e se pertinente unità organizzativa) presso cui è svolta l'attività di ricerca del dottorando	Città: NAPOLI Provincia: NA Indirizzo: Via G. Porzio, 4 Centro Direzionale - Is. E7, 80143 Napoli
e. Nome, cognome e riferimenti del tutor aziendale;	Nome: Giuseppe Cognome: Lieto Ruolo: Chief Executive Officer (CEO) Email: glieto@sysmanagement.it Telefono: +390816581584, +393936165059
f. Modalità di supervisione tutoriale dei dottorandi	<p>Le attività di ricerca dello studente saranno svolte sotto la supervisione di due tutor, uno universitario e l'altro aziendale. I tutor svolgeranno, inoltre, la supervisione dell'attività formativa dello studente, accertando l'adempimento delle attività di formazione e di ricerca assegnate e informando il Collegio su specifiche esigenze che dovessero presentarsi.</p> <p>Lo studente, con cadenza periodica, relazionerà ai tutor sulle attività svolte nel periodo di riferimento attraverso la presentazione di documenti scritti (relazioni, mappe, schemi) e concorderà le attività da svolgere nel prosieguo.</p> <p>Durante il periodo di formazione in azienda, lo studente sarà indirizzato e seguito dal tutor aziendale principalmente e da ingegneri e tecnici specializzati che, a seconda delle attività di ricerca e/o sperimentali di laboratorio nelle quali sarà coinvolto, contribuiranno alla formazione dello studente supportando lo sviluppo delle attività.</p>

g. Durata di permanenza in impresa del dottorando titolare della borsa aggiuntiva PON (minimo 6 mesi, massimo 18)	(mesi) 10
h. Impiego dei risultati e delle ricadute dell'attività di ricerca per l'accrescimento delle abilità del dottorando con riferimento al settore di intervento	<p>Negli ultimi anni, il settore della sicurezza informatica sta vivendo una evoluzione tecnologica legata alla crescente richiesta di sicurezza dal mondo dell'industria ICT. In questo contesto le attività di ricerca e risultati conseguiti, renderanno lo studente una figura professionale di notevole interesse applicativo per le aziende operanti nel settore dell'ICT.</p> <p>Tuttavia, gli argomenti affrontati dal progetto sono tutti associati a una domanda di mercato in costante aumento. Per questo motivo, il profilo del potenziale studente sarà decisamente interessante sia per le aziende che erogano servizi in diversi settori, quali la distribuzione energetica, le tecnologie per l'Industria 4.0 e la telemedicina, e la gestione delle infrastrutture di trasporto (es., infrastrutture ferroviarie intelligenti). Nel suo iter formativo lo studente, inoltre, si arricchirà nel dialogo con la comunità scientifica internazionale sulle tematiche più attuali della Ricerca e Sviluppo (R&D), maturando familiarità verso le nuove tecnologie e la loro ricaduta sul sistema produttivo, delineandosi come una figura strategica capace di coniugare sinergicamente Accademia e Impresa. Lo studente sarà guidato lungo un percorso di alta formazione tecnico-scientifica che gli garantiranno strumenti metodologici e competenze tali da delineare una professionalità altamente qualificata nell'ambito della ricerca e dell'innovazione tecnologica.</p> <p>La capacità di gestire l'innovazione e l'originalità creativa nell'elaborazione e nella realizzazione di progetti e servizi acquisite dallo studente saranno aspetti strategici che risulteranno particolarmente utili all'interno delle PMI che intendano investire in R&D. Lo studente al conseguimento del titolo si proporrà nel mondo del lavoro come un "problem solver" con alta qualificazione scientifica in grado di ricoprire profili professionali di elevato livello grazie alla capacità di affrontare in modo autonomo i problemi ed alla predisposizione a lavorare in team, spesso in contesti di carattere internazionale.</p>
C. ATTIVITA' ALL'ESTERO	
a. Attività di ricerca da svolgere all'estero	<p>Il progetto vedrà attività di ricerca svolte all'estero presso l'Università di Coimbra, in collaborazione con il gruppo di ricerca "Software and Systems Engineering research group (SSE)" diretto dal prof. Marco Vieira. Il gruppo SSE svolge da oltre 20 anni attività sui temi legati alla cybersecurity, tra cui Security Assessment and Benchmarking, Fault Injection and Vulnerability & Attack Injection, Robustness and Security Testing, e Software Verification & Validation. L'attività di ricerca presso SSE approfondirà le tecniche di security testing ed offensive security oggetto della ricerca del gruppo SSE, e la loro integrazione all'interno della piattaforma di CyberRange. Le tecniche di security testing saranno rese disponibili ai partecipanti dei CyberRange sotto forma di strumenti riusabili, in modo da favorire l'apprendimento da parte dei red e blue team delle soluzioni allo stato dell'arte. Inoltre, le tecniche di security testing saranno parte integrante degli agenti intelligenti, permettendo di automatizzare tali attività durante le esercitazioni. Infine, l'attività di ricerca si avvarrà della expertise del gruppo SSE, in particolare nelle tecnologie hypervisor e cloud computing, per la progettazione di soluzioni hypervisor-based per il monitoraggio dei CyberRange.</p>
b. Denominazione del soggetto ospitante all'estero (università, ente di ricerca pubblico o privato, impresa)	Università di Coimbra
c. Sede legale del soggetto ospitante all'estero	<p>Città: Coimbra</p> <p>Portogallo</p> <p>Indirizzo: 3004-531 Coimbra, Portogallo</p>
d. Sede operativa principale (e se pertinente unità organizzativa) presso cui è svolta l'attività di ricerca all'estero	<p>Città: Coimbra</p> <p>Portogallo</p> <p>Indirizzo: Departamento de Engenharia Informática Polo II - Pinhal de Marrocos 3030-290 Coimbra - Portugal</p>
e. Nome, cognome,	Nome: Marco

ruolo e contatti del tutor del soggetto ospitante	Cognome: Vieira Ruolo: Full Professor Email: mvieira@dei.uc.pt
f. Modalità di supervisione tutoriale dei dottorandi	<p>Sfruttando la possibilità di internazionalizzazione mediante dottorato in co-tutela prevista dal Regolamento di dottorato dell'Ateneo Federico II, lo studente sarà co-tutorato da un docente del Dottorato di Ricerca in Information Science and Technology dell'Università di Coimbra. Il tutore accademico presso l'università ospitante seguirà le sue attività scientifiche con incontri settimanali e fornirà indicazioni e suggerimenti per il migliore prosieguo del lavoro. Il tutore accademico presso la Federico II parteciperà agli incontri periodici di supervisione del dottorando mediante teleconferenza e strumenti on-line per la condivisione del materiale di lavoro, assicurando che le attività siano coerenti con gli obiettivi del programma di ricerca e di formazione. Oltre all'interazione con i tutor, il dottorando lavorerà a stretto contatto con gli altri membri del gruppo di ricerca dell'università ospitante, interagendovi in base alle necessità ed alle competenze specifiche di ciascuno.</p>
g. Durata della permanenza all'estero (minimo 6 mesi, massimo 18 mesi)	(mesi) 8
h. Impiego dei risultati e delle ricadute dell'attività di ricerca per l'accrescimento delle abilità del dottorando con riferimento al settore di intervento	<p>Il periodo all'estero consentirà allo studente di raggiungere un livello avanzato di esperienza nel campo dell'applicazione di tecniche di security testing e di cloud computing. Lo studente avrà l'opportunità di partecipare a seminari, conferenze e incontri organizzati regolarmente dall'università ospitante, incrementando le proprie capacità di esposizione dei risultati scientifici raggiunti con i propri pari e con il personale docente. Inoltre, lo studente avrà l'opportunità di apprendere l'uso degli strumenti di security testing sviluppati dall'Università di Coimbra e applicarli a casi di studio pratici, effettuando la sperimentazione sul testbed disponibile presso l'università ospitante. Tale sperimentazione pratica permetterà dottorando di sviluppare le sue capacità nel trasferimento tecnologico delle soluzioni di ricerca su sistemi reali di elevata complessità.</p>
D. ATTIVITA' FORMATIVA PRESSO L'UNIVERSITA'	
a. Modalità di svolgimento e contenuti delle attività integrative di formazione destinate al dottorando (oltre a quelle già previste dal corso di dottorato) rilevanti per il percorso individuato	<p>Il programma di formazione comprende corsi specialistici, eventi di formazione di gruppo focalizzati, supporto per lo sviluppo delle competenze, impegno nella comunità di ricerca con particolare attenzione allo scambio tra industria e accademia. La formazione sarà svolta in conformità con la "Carta europea dei ricercatori".</p> <p>Il programma sarà incentrato su:</p> <ul style="list-style-type: none"> ● Conoscenza scientifica, attraverso l'esposizione delle attività di ricerca. ● Capacità di ricerca, attraverso discussioni e tutoraggio con i supervisori. ● Capacità di comunicazione, attraverso la partecipazione a corsi di impegno pubblico, presentazioni, conferenze, seminari e workshop internazionali. ● Sfruttamento dei risultati della ricerca (gestione dei diritti di proprietà intellettuale, brevetti, segretezza e pubblicazione dei risultati della ricerca). ● Capacità di gestione e networking, attraverso incontri di progetto e impegno con i partner. <p>La formazione sarà supportata da corsi sulle conoscenze di base necessarie per la ricerca di livello internazionale in ambito cybersecurity. I corsi saranno strutturati con un buon equilibrio tra contenuto accademico, applicazione delle conoscenze con laboratori pratici, interazione con i docenti e i ricercatori senior dei partner, studio individuale e attività di gruppo. Ogni corso partirà da una rassegna dei principi della materia, per passare all'interpretazione critica dei risultati di ricerca con l'obiettivo di promuovere la capacità di pianificare la ricerca e presentare idee innovative. Alcuni dei corsi di formazione previsti sono:</p> <ul style="list-style-type: none"> ● C1 - Progettazione di servizi avanzati di cloud computing, basati sulla piattaforma OpenStack; ● C2 - Metodologie didattiche e gamification nel contesto della formazione in cybersecurity; ● C3 - Tecniche di data science applicate all'analisi dei dati degli eventi e del traffico all'interno delle infrastrutture informatiche; ● C4 - Algoritmi di reinforcement learning; ● C5 - Requisiti operativi e standard di riferimento in ambito cybersecurity. <p>Le competenze pratiche sull'uso delle tecnologie avanzate saranno arricchite da workshop tecnici. Alcuni dei workshop proposti sono:</p> <ul style="list-style-type: none"> ● W1: prototipazione, sviluppo e testing di servizi di cloud computing; ● W2: framework di programmazione per algoritmi di reinforcement learning; ● W3: realizzazione e conduzione pratica di esercitazioni di CyberRange. <p>Il dottorando avrà la possibilità, tramite l'azienda System Management, di partecipare a veri eventi CyberRange organizzati in collaborazione con i suoi partner commerciali (in particolare, il gruppo</p>

	<p>industriale Leonardo), ove potrà apprendere con un approccio hands-on e sperimentare le soluzioni innovative.</p> <p>Saranno inoltre organizzati periodicamente workshop in cui studenti afferenti al curriculum "cybersecurity" della laurea magistrale in Ingegneria Informatica utilizzeranno la piattaforma innovativa di CyberRange, ai fini della validazione e della sperimentazione della soluzione.</p>
b. Elementi di co-progettazione o intervento diretto da parte dell'impresa	<p>L'azienda System Management svolge un ruolo diretto di supervisione, di condivisione e programmazione delle attività formative e di ricerca dello studente sia in ambito aziendale che accademico con particolare riferimento alla progettazione tecnica della piattaforma innovativa di CyberRange. L'azienda System Management supporterà inoltre la formazione del dottorando coinvolgendo esperti, sia al suo interno sia nell'ambito esteso dei suoi partner di progetto a livello nazionale (es., il gruppo industriale Leonardo) e internazionale (es., NATO), per la organizzazione di seminari dedicati all'approfondimento delle problematiche di cybersecurity in ambito aziendale e della difesa, e all'utilizzo delle piattaforme di CyberRange.</p>
c. Grado di rispondenza della proposta rispetto alla domanda di alta formazione per garantire le adeguate competenze richieste dal tessuto produttivo	<p>La proposta è un programma di formazione unico che riunisce le competenze in materia di alta formazione di dottorato da parte di istituzioni accademiche di fama internazionale e la formazione di ricerca industriale di una impresa industriale impegnata a livello internazionale nell'ambito della cybersecurity. L'impatto tecnico della proposta di progetto e le relative competenze da formare sono in termini di:</p> <ul style="list-style-type: none"> • Riduzione dei rischi di cybersecurity all'interno delle infrastrutture informatiche; • Riduzione, in termini di ore/uomo, dello sforzo di organizzazione, di conduzione, e di esecuzione di attività di CyberRange; • Maggiore protezione di informazioni sensibili nella creazione di scenari esercitativi realistici. <p>L'impatto socio/economico della proposta di progetti di ricerca è in termini di:</p> <ul style="list-style-type: none"> • Supporto al lifelong learning nell'ambito della cybersecurity, in continua evoluzione; • Nuovi metodi di formazione di maggior qualità, in termini di realismo degli scenari e delle vulnerabilità; • Applicazione del paradigma del CyberRange in nuovi settori critici. <p>L'impatto della formazione è, invece, in termini di:</p> <ul style="list-style-type: none"> • Miglioramento della formazione del dottorando in ambito di cybersecurity, fornendogli un ventaglio completo di competenze sulle vulnerabilità a diversi livelli delle infrastrutture informatiche (hardware, reti, software, a livello sia applicativo sia di sistema operativo, etc.) e sulle tecniche di difesa ed attacco (es., tecniche di security testing sia statiche sia dinamiche). • Miglioramento della formazione del dottorando su aspetti verticali dell'intelligenza artificiale e delle sue applicazioni nell'ambito della cybersecurity. Ciò migliorerà la prospettiva di carriera dello studente rispetto a programmi di formazione tradizionali forniti da una singola istituzione, in quanto lo studente acquisirà competenze interdisciplinari e utili in tutta l'Unione Europea.
E. CONTRIBUTO AL PERSEGUIMENTO DEI PRINCIPI ORIZZONTALI	
a. Eventuali iniziative che si intende mettere in atto per assicurare i principi di pari opportunità, antidiscriminazione, parità di genere ed accessibilità per le persone disabili sia in fase di accesso che di attuazione dei percorsi di dottorato	<p>Tutte i soggetti coinvolti condividono l'impegno alla lotta contro tutte le forme di discriminazione - genere, età, disabilità, etnia, fede religiosa, orientamento sessuale - e l'impegno a valorizzare le diversità - in particolare, le due università coinvolte hanno tali principi nel proprio codice etico.</p> <p>Quindi, nell'ambito del progetto:</p> <ul style="list-style-type: none"> • tutti condividono l'obiettivo etico di creare e preservare un ambiente di studio, ricerca e lavoro libero da discriminazioni, in cui tutti vengano trattati con dignità e rispetto; • il Dottorato ITEE è vincolato a non discriminare alcun candidato o dottorando sulla base di sesso, colore, razza, etnia, nazione di origine, religione, età, stato civile, disabilità, stato di gravidanza, e appartenenza politica, e a prendere come unico fattore distintivo il merito. <p>In virtù di questo, i tre soggetti si impegnano a contribuire al raggiungimento degli obiettivi condivisi attraverso alcune azioni concrete:</p> <ul style="list-style-type: none"> • integrare il principio di parità di trattamento nei processi che regolano tutte le fasi del percorso di progetto proposto, affinché le decisioni relative alla formazione e sviluppo di competenze vengano prese unicamente in base alle competenze, all'esperienza, al potenziale delle persone; • sensibilizzare e formare il dottorando sul valore della diversità e sulle modalità di gestione delle stesse; • monitorare il rispetto dei principi condivisi; • informare il dottorando dell'impegno assunto - da studente dell'Ateneo - a favore di una cultura Universitaria ed aziendale delle pari opportunità; • informare il dottorando dei servizi che l'Ateneo offre attraverso il proprio apposito centro SInAPSi (Servizi per l'Inclusione Attiva e Partecipata degli Studenti) a tutti gli studenti che si sentono esclusi dalla vita universitaria a causa di disabilità, disturbi specifici dell'apprendimento (dislessia, disgrafia, disortografia, discalculia) o difficoltà temporanee, ivi incluso il servizio di Counselling Psicologico. Il centro offre servizi e promuove iniziative per favorire la partecipazione di tutti gli studenti alla vita universitaria, collabora con le strutture dell'Ateneo per assicurare l'accessibilità degli ambienti,

	<p>promuove e svolge attività di studio e ricerca per migliorare l'inclusione degli studenti, promuove dibattiti sull'inclusione di studenti disabili, segnala offerte di lavoro per categorie protette.</p>
<p>b. Presenza di soluzioni ecocompatibili nella realizzazione e gestione dei percorsi di dottorato, includendo ad esempio la presenza di moduli specifici o contenuti formativi nel campo della green e/o blue economy</p>	<p>Il percorso formativo prevede in primo luogo la frequenza di un corso interdisciplinare comune a più dottorati concernente gli argomenti:</p> <ul style="list-style-type: none"> • sviluppo sostenibile; • green economy; • blue economy. <p>In particolare, il corso intende formare il dottorando sulla Green Economy, da considerare come un nuovo modello economico tout court e non semplicemente la parte verde dell'economia.</p> <p>Il corso delinea le caratteristiche di un'economia il cui impatto ambientale sia contenuto entro dei limiti accettabili, in cui tecnologia e conoscenza scientifica svolgono un ruolo di primaria importanza, ed evidenzia che un'Economia è Green se porta ad un miglioramento del benessere umano e dell'equità sociale, riducendo in modo significativo i rischi ambientali e i limiti ecologici legati allo sfruttamento delle risorse.</p> <p>Particolare attenzione è rivolta alla Blue Economy ed al ruolo che essa riveste nell'ambito dello sviluppo sostenibile, in tema di risultati più soddisfacenti dal punto di vista ambientale, con il passaggio dalla tutela degli ambienti al concetto di rigenerazione degli ecosistemi, dalla eco-efficienza alla biomimesi.</p> <p>Nel corso è illustrato il concetto di Blue Economy come inteso da Gunter Pauli: modello di business dedicato alla creazione di un ecosistema sostenibile grazie alla trasformazione in risorse di valore di sostanze precedentemente sprecate.</p> <p>La presenza di soluzioni ecocompatibili nella realizzazione e gestione dei percorsi di Dottorato in area ingegneristica verrà soddisfatta attraverso l'organizzazione di corsi e/o seminari che includono la presenza di moduli specifici e contenuti formativi nel campo della green e/o blue economy. Nello specifico, gli studenti di dottorato verranno introdotti alla green economy e al suo impatto sul management dei progetti ingegneristici e sullo sviluppo di prodotti e soluzioni eco-compatibili attraverso una serie di seminari e/o corsi che verranno organizzati all'interno del percorso formativo del dottorato. Nello specifico si introdurranno gli studenti alle tematiche ambientali e sociali legate ai cambiamenti climatici e all'adozione di Corporate Social Responsibility da parte di grandi e piccole aziende. Nell'ambito dei corsi e seminari che verranno organizzati le sfide poste dalla green economy e dal project management verranno analizzati usando approcci teorici differenti ispirati alla teoria dei Complex Systems, Resilience, e Collective Intelligence. Verranno forniti esempi ed applicazioni in campi diversi che includono lo sviluppo di Carbon Free Economy, Smart Cities, Green Design di nuovi prodotti, Green Supply chain e Zero Waste Factory. Gli studenti di dottorato verranno anche introdotti alla valutazione di progetti e prodotti sulla base di criteri legati all'impatto ambientale usando metodologie tradizionali e non, come Cost/Benefit Analysis, Network Analysis, fuzzy multi attribute decision making e Agent-Based Simulation.</p>



Corso di Dottorato



Borse richieste (Indicare per ciascuna borsa le seguenti informazioni)



Autorizzazione