

Nome: AI in Cybersecurity: Le nuove frontiere nelle strategie di difesa

Sessioni, date, luogo: 2-3 Luglio 2025 – 09:00-17:00 – Roma, Via Palestro 24

Competence Center: Innovazione

Prezzo: €1.000 + IVA (la quota è esente da IVA se corrisposta da Enti pubblici)

Lecturer	Mattia Siciliano
Contatti	Mail: segreteria@ceida.com
Ricevimento	Da concordare via mail

Descrizione

Questo corso offre un'esplorazione approfondita di come l'Intelligenza Artificiale stia rivoluzionando il panorama della sicurezza e della difesa. I partecipanti acquisiranno conoscenze e competenze all'avanguardia per sfruttare l'AI nella gestione delle nuove minacce informatiche, migliorare la consapevolezza situazionale e automatizzare i meccanismi di risposta agli incidenti.

Oltre alla cybersecurity, il corso approfondisce le applicazioni più ampie dell'AI nei settori governativo e pubblico. I partecipanti esamineranno scenari reali e progetti a livello aziendale, come l'uso dell'AI per ottimizzare il processo decisionale, migliorare la governance basata sui dati e sviluppare modelli predittivi per la gestione delle crisi e il soccorso in caso di calamità. Il programma evidenzia anche soluzioni innovative basate sull'AI per migliorare il coinvolgimento dei cittadini attraverso modelli di relazione con il pubblico, come l'implementazione di chatbot e sistemi intelligenti di erogazione di servizi pubblici, per comprendere meglio le esigenze delle diverse comunità.

Inoltre, il corso pone l'accento sulla cruciale intersezione tra AI, cybersecurity e reti 5G. Con la rapida diffusione della tecnologia 5G che consente una connettività e un flusso di dati senza precedenti, i partecipanti apprenderanno come utilizzare applicazioni basate sull'AI per proteggere le infrastrutture critiche.

Progettato per professionisti dell'ecosistema europeo della sicurezza e difesa, inclusi militari, forze dell'ordine, diplomatici e dirigenti del settore pubblico, il corso fornirà ai partecipanti le competenze necessarie per guidare iniziative integrate con l'AI. I partecipanti saranno in grado di progettare e implementare modelli di AI che non solo proteggano le infrastrutture critiche, ma che promuovano anche efficienza e innovazione nella pubblica amministrazione, garantendo resilienza in un mondo sempre più interconnesso e digitale.

Obiettivi

Al termine del programma, i partecipanti saranno in grado di:

- Sviluppare strategie di cybersecurity basate sull'AI**
 - Progettare e implementare sistemi basati sull'AI per rilevare, prevenire e rispondere alle nuove minacce informatiche.
- Applicare l'AI per proteggere le infrastrutture critiche**
 - Utilizzare applicazioni AI per mettere in sicurezza le reti basate su 5G e proteggere infrastrutture critiche nei settori dell'energia, trasporti, sanità e comunicazioni.
- Guidare progetti AI nei settori governativo e pubblico**
 - Progettare e gestire iniziative AI su scala aziendale per ottimizzare il processo decisionale, migliorare la governance dei dati e aumentare l'efficienza operativa.
 - Implementare soluzioni AI per la gestione delle crisi, il soccorso in caso di calamità e altre sfide della pubblica amministrazione.

4. **Migliorare l'interazione con i cittadini e i servizi pubblici tramite l'AI**
 - Sviluppare modelli basati sull'AI per la relazione con i cittadini, inclusi chatbot, sistemi intelligenti di erogazione dei servizi e strumenti di analisi dei sentimenti, per migliorare l'engagement e la soddisfazione dei cittadini.
5. **Integrare l'AI nelle strategie di sicurezza e difesa**
 - Creare framework completi che combinino AI e cybersecurity per proteggere l'ecosistema europeo della sicurezza e difesa.
 - Collaborare con team multidisciplinari per implementare soluzioni AI innovative nei contesti militari, delle forze dell'ordine e diplomatici.
6. **Navigare l'intersezione tra AI, cybersecurity e 5G**
 - Affrontare le sfide uniche poste dalla tecnologia 5G, garantendo la sicurezza dei sistemi connessi e dei flussi di dati.
 - Utilizzare l'AI per migliorare la consapevolezza situazionale e sviluppare misure proattive per la resilienza delle infrastrutture.

Alla fine del programma, i partecipanti saranno dotati di competenze tecniche, visione strategica e capacità di leadership per guidare l'innovazione e la sicurezza in un mondo sempre più digitale e interconnesso.

Programma e Contenuti

GIORNO 1

1. **Modulo 1:** *"Rivoluzionare la connettività: liberare il potenziale del 5G e dell'AI"*
2. **Modulo 2:** *"Pragmatismo dell'AI e framework agentic. Sfruttare l'innovazione per un impatto su larga scala"*
3. **Modulo 3:** *"Sfruttare l'AI per trasformare lo sviluppo urbano"*
4. **Modulo 4:** *"Navigare la diversità linguistica: sfruttare l'AI e la GenAI per un'intelligence approfondita"*

GIORNO 2

5. **Modulo 5:** *"L'AI come abilitatore per gli obiettivi strategici GPS"*
6. **Modulo 6:** *"Innovazione reinventata: come l'AI potenzia i servizi pubblici di nuova generazione"*
7. **Modulo 7:** *"Leadership attraverso l'esperienza: sfruttare CX & EX per il successo in diplomazia e difesa"*
8. **Modulo 8:** *"Fusione tra AI e cyberwar: ridefinire il futuro del conflitto digitale"*

Fonti di apprendimento

I relatori presenteranno video o libri durante il workshop.

Metodologia

Il corso "AI in Cybersecurity: La nuova frontiera nelle strategie di difesa" adotterà una metodologia di apprendimento blended per garantire ai partecipanti sia conoscenze teoriche che competenze pratiche. L'approccio includerà:

1. Lezioni tradizionali
 - I concetti fondamentali di AI, cybersecurity, 5G e le loro applicazioni nella difesa saranno introdotti attraverso lezioni strutturate tenute da istruttori esperti.
 - Queste sessioni forniranno una conoscenza di base essenziale per comprendere gli argomenti avanzati.
2. Analisi di casi di studio e scenari reali

- I partecipanti analizzeranno esempi reali di applicazioni dell'AI nella cybersecurity e nella protezione delle infrastrutture critiche.
 - I casi di studio tratteranno progetti governativi e del settore pubblico, implementazioni aziendali e sfide legate al 5G, offrendo approfondimenti sulle migliori pratiche e sulle lezioni apprese.
3. Workshop interattivi
- I workshop si concentreranno anche sulla progettazione di iniziative basate sull'AI per il settore pubblico e sull'esplorazione dell'analisi predittiva per la gestione delle crisi.
4. Speaker ospiti e panel di esperti
- Esperti rinomati nei campi della cybersecurity, dello sviluppo AI, delle infrastrutture 5G e dell'innovazione nel settore pubblico condivideranno le loro esperienze e approfondimenti.
 - I panel e le sessioni di Q&A offriranno ai partecipanti l'opportunità di interagire direttamente con leader del settore.

Valutazione

Valutazione	% sulla valutazione finale
Partecipazione e frequenza	60%
Project work	-
Test	40%
Other	-

Short bio

Mattia Siciliano

Laurea in Ingegneria TLC con lode, tesi sperimentale sull'Intelligenza Artificiale applicata alla cybersecurity, ha guidato l'implementazione di strategie digitali governative in settori quali Difesa, Finanza, Tecnologia ed Energia, operando con successo in Europa, GCC e Asia, e supportando direttamente i vertici di aziende internazionali nella gestione del rischio informatico e digitale.

Advisor strategico presso il Ministero della Difesa, è Presidente della Commissione Cyber Threat Intelligence e Cyber Warfare della Società Italiana d'Intelligence – Mattia si distingue nel mondo accademico e della ricerca.