ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

acting also as

ISACA MILAN CHAPTER

PRESENTA

Photo by Javier Allegue Barros on Unsplash

Cloud, Cybersecurity & AI

Milano, 23 luglio 2021 14.00-18.00

online in streaming

in attesa di poter tornare nell'Auditorium UniCredit Services - Milano

IL PROGRAMMA

14:00	Avvio della connessione
14:10	Saluti e introduzione
14:20	*Daniele Catteddu* Certificate of Cloud Auditing Knowledge (CCAK): prepararsi per le nuove sfide nel cloud
15:15	*Davide Casale* Targeted attacks & active defense
16:10	Coffee Break
16:30	*Valentina Cavosi* Verso sistemi di Intelligenza Artificiale di supporto e affidabili: presentazione di uno strumento di valutazione del rischio e dell'impatto
17:20	Dibattito con i Relatori
18:00	Conclusioni e networking

LE RELAZIONI

Daniele Catteddu

Certificate of Cloud Auditing Knowledge (CCAK):prepararsi per le nuove sfide nel cloud

In questa presentazione fornirà un'introduzione al "Certificate of Cloud Auditing Knowledge" il nuovo certificato professionale frutto della collaborazione tra Cloud Security Alliance (CSA) ed ISACA e recentemente lanciato.
Verranno illustrate le ragioni che hanno portato alla creazione di CCAK, ed alcuni dei dettagli del programma.
CCAK si volge ad un ampio audience formato da auditor di sicurezza, e da tutti professionisti impegnati nella valutazione di servizi cloud.

Davide Casale

Targeted attacks & active defense

In questo intervento vedremo le metodologie con cui i «Cyber Criminals» attaccano le aziende «vittime» e procedono ad impossessarsi del loro asset informativo aziendale (scouting & fingerprinting, hacking & penetration, lateral movements, databreach, ransomware & ransom request, etc.).
Parleremo a quel punto della filosofia dell'«Active Defense» cosa propone per mitigare in modo efficace questa «Cyber War» di cui ogni azienda rischia di essere vittima.

Valentina Cavosi

Verso sistemi di Intelligenza Artificiale di supporto e affidabili: presentazione di uno strumento di valutazione del rischio e dell'impatto

Grazie alla crescente disponibilità di dati, nuovi algoritmi e all'aumento della potenza di calcolo, l'Intelligenza Artificiale (IA) di nuova generazione (basata sui dati e tecniche di machine learning) sta ottenendo risultati molto promettenti in molti settori dove classificazioni, suggerimenti e predizioni possono supportare processi decisionali con contesti di grande complessità e incertezza. I potenziali benefici sono attualmente oggetto di ricerca e dibattito sia nel settore pubblico che in quello privato, dove gli investimenti superano quello di altre tecnologie innovative così come le aspettative e la speranza di ritorni rilevanti a livello di produttività, efficienza, efficacia, sicurezza e profitto. Al tempo stesso, però, il suo utilizzo suscita alcune perplessità e timori soprattutto da un punto di vista etico, giuridico e sociale in termini di responsabilità, sicurezza, perdita della privacy, restrizioni alla libertà di espressione, pregiudizi e distorsioni nei dati, violazioni della dignità umana o discriminazione, solo per citarne alcuni. Per questo motivo va posta una particolare attenzione all'impatto che queste tecnologie possono avere sulla vita di tutti i soggetti coinvolti. Durante l'intervento verrà quindi delineato brevemente questo dibattito e presentato uno strumento di valutazione dell'impatto dell'intelligenza artificiale con lo scopo di supportare sviluppatori, distributori e coloro che desiderano utilizzare i sistemi di intelligenza artificiale ad essere consapevoli dei rischi che questi sistemi possono comportare. Lo strumento, che è il risultato di una attività di ricerca condotta presso il laboratorio MUDI (Modelling Uncertainty, Decision and Interaction) del Dipartimento di Informatica dell'Università di Milano-Bicocca, di cui è responsabile il prof. Federico Cabitza, consente di valutare qualitativamente gli aspetti legali ed etici dell'IA in modo tale da aumentare la consapevolezza su questi temi e così contribuire a mitigare tempestivamente i rischi riducendo i costi per eventuali danni, e promuovendo l'adozione e l'uso di un'IA più affidabile ed equa.

I RELATORI

Daniele Catteddu

Daniele Catteddu è un professionista della sicurezza e della gestione dei rischi ed evangelista della privacy. Ha ricoperto ruoli di responsabilità sia nel settore privato che in quello pubblico. Attualmente è il CTO di Cloud Security Alliance, dove è responsabile di guidare l'adozione della strategia tecnologica dell'organizzazione. Daniele è il co-fondatore del Programma CSA STAR. E' membro della delegazione nazionale italiana standard presso ISO/IEC SC27. È docente presso il Maastricht University Center on Privacy & Cybersecurity, membro del Comitato Scientifico della European Privacy Association e dell'Advisory Board della Kent University CyberSecurity. In passato ha lavorato presso ENISA, European Cyber Security Agency, come Esperto nelle aree della Protezione delle Infrastrutture Critiche e dei Rischi Emergenti e Futuri. Prima di entrare in ENISA, Daniele ha lavorato come consulente di Information Security nel settore bancario e finanziario. Daniele ha una laurea magistrale in Economia e Commercio presso l'Università di Parma (Italia). È un frequente relatore principale nelle principali conferenze sulla sicurezza e autore di numerosi documenti in materia di sicurezza informatica e privacy.

Davide Casale

Laureato in Ingegneria delle Telecomunicazioni al Politecnico di Torino. Senior Security Engineer esperto di Security Probing e Vulnerability Assessment, di direzione di lavori su infrastrutture perimetrali di sicurezza e sistemi di intrusion detection prima per conto di Intesis Spa e quindi dal 2000 attraverso la propria società, Shorr Kan IT Engineering, di cui è tra i soci fondatori. Docente del corso di Reti di Calcolatori, per il Politecnico di Torino, Ingegneria delle Telecomunicazioni.

Valentina Cavosi

Dopo una laurea in Teorie e Tecniche psicologiche con indirizzo in Psicologia Sociale, del Lavoro e delle Organizzazioni presso l'Università di Firenze, nel 2021 si laurea in Teorie e Tecnologie della Comunicazione all'Università degli studi di Milano-Bicocca, discutendo una tesi con titolo "Valutazione dell'impatto dell'Intelligenza Artificiale: una proposta" (relatore prof. Federico Cabitza). Durante la stesura della tesi ha svolto un tirocinio presso l'azienda RedOpen, spin-off dell'Università di Milano-Bicocca che si occupa di Data Governance e impatto di tecnologie innovative nel perimetro informativo aziendale.

LUOGO E DATA

Venerdì, 23 luglio 2021

Online sulla piattaforma di Streaming di AIEA

ISCRIZIONI

Soci AIEA

Portale delle Sessioni di Studio
https://portale.aiea.jed.st/

Se al primo accesso, recuperare la propria ISACA ID (numerica) dal sito ISACA o dalle comunicazioni di iscrizione/rinnovo e farsi inviare la password all'indirizzo preregistrato tramite la funzione
Password dimenticata

Un Socio AIEA invita un Non Socio

Ogni Socio AIEA può invitare un Non Socio, che potrà seguire lo streaming sulla pagina dedicata del Sito AIEA. Contattare Luca Pertile <luca.pertile@aiea.it> per la chiave di accesso.

Soci Associazioni patrocinanti

I Soci delle Associazioni patrocinanti possono partecipare gratuitamente seguendo le indicazioni che sono state fornite loro dalle rispettive Associazioni.

Non Soci

Contattare la segreteria AIEA per associarsi o versare il contributo organizzativo per il singolo evento
Segreteria AIEA

Associazione Italiana Information Systems Auditors

L'Associazione Italiana Information Systems Auditors è stata costituita a Milano nel 1979 con lo scopo di promuovere l'approfondimento dei problemi connessi con il controllo del processo di elaborazione automatica dei dati e di favorire lo sviluppo di metodologie e tecniche uniformi per la loro soluzione.

In particolare, gli obiettivi dell'Associazione sono:

- promuovere un processo di sensibilizzazione di tutti i livelli organizzativi aziendali alla necessità di stabilire adeguati criteri di controllo, di affidabilità dell'organizzazione, Information Systems e di sicurezza dei sistemi;
- ampliare la conoscenza ed esperienza dei suoi oltre 800 membri nel campo dell'IT Governance, IT Security, Information Systems Auditing e Risk Control, favorendo lo scambio di metodologie per lo studio e la soluzione dei problemi inerenti;
- promuovere a livello nazionale la partecipazione alle certificazioni CISA, CISM, CGEIT, CRISC, CobiT e CSX

AIEA è associata da 40 anni ad ISACA, primo Capitolo in Europa, diventando nota internazionalmente come

ISACA MILAN CHAPTER

ISACA® per i suoi oltre 145,000 soci in oltre 180 paesi e per la comunità dei professionisti IT è fonte affidabile di possibilità di networking, certificazioni professionali, conoscenza e standard negli ambiti IT Governance, Cybersecurity, IT Risk e Assurance

www.aiea.it

20123 Milano - Via privata del Gonfalone, 3 - E-mail: aiea@aiea.it
Sito web: www.aiea.it – www.isaca.mi.it - P.IVA n. 10899720154 - C.F. n. 97109000154