
16 Ore CPE
RESILIENZA
INNOVAZIONE
SICUREZZA
l'ICT ai tempi della guerra pandemica
20 -21 OTTOBRE 2020
IT
RISK
AUDITING
SECURITY
GOVERNANCE
Organizzato da
AIEA
also known as
ISACA
Milan Chapter
XXXIV CONVEGNO NAZIONALE
In conferenza virtuale su internet dal sito www.aiea.it

Organizzato in collaborazione con

Ordine Ingegneri della Provincia di Siena

ORDINE degli INGEGNERI della PROVINCIA di SIENA

con il patrocinio dell'Ordine degli Ingegneri della Provincia di Napoli

INGEGNERI ORDINE NAPOLI

also known as ISACA Milan Chapter

XXXIV CONVEGNO NAZIONALE AIEA

RESILIENZA INNOVAZIONE SICUREZZA

l'ICT ai tempi della guerra pandemica

Milano, 20 - 21 Ottobre 2020

In conferenza virtuale sul sito www.aiea.it

L'anno scorso avevamo chiuso il Convegno con il consueto arrivederci, fiduciosi di poter riproporre l'evento secondo uno schema ormai consolidato. Ricordo che ci eravamo ripromessi di vederci nelle stesse date del 2019.

Non è stato facile, stiamo ancora lavorando, ma vi scrivo per comunicarvi che con certezza manterremo quell'impegno e il XXXIV Convegno AIEA si svolgerà nelle giornate del 20 e 21 ottobre esclusivamente via streaming, secondo un format fortemente rinnovato

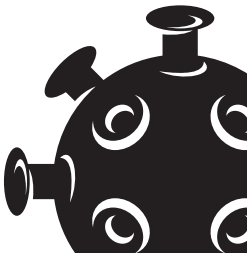
Il collegamento sarà gratuito per i Soci e istruzioni per la "partecipazione" saranno divulgate in tempi utili.

Come ogni anno abbiamo lavorato, e stiamo ancora lavorando intensamente, per portare al nostro evento ospiti con esperienze e competenze di prima grandezza.

Trovate in allegato, allo stato dell'arte, la scaletta delle due giornate che frutteranno complessivamente 16 ore CPE.

Save the date! Ci vediamo in ottobre.

Stefano Niccolini



also known as ISACA Milan Chapter

XXXIV CONVEGNO NAZIONALE AIEA

RESILIENZA INNOVAZIONE SICUREZZA

l'ICT ai tempi della guerra pandemica

Milano, 20 - 21 Ottobre 2020

In conferenza virtuale sul sito www.aiea.it

Quota partecipazione

30 Euro IVA inclusa entrambe le giornate

Per i Soci AIEA la partecipazione è gratuita

I Soci delle Associazioni Patrocinanti hanno diritto a sconti dedicati

Per le iscrizioni contattare la Segreteria AIEA all'indirizzo aiea@aiea.it

AIEA

also known as ISACA Milan Chapter

Martedì 20 Ottobre mattino — Tavole rotonde

9:30 - Digital Transformation

Ettore Turra — Tommaso Dradi

Luca Gastaldi — Martina Pugliese

10:30 - Intelligenza Artificiale

Antonio Mauro — Marco Gori

Alex Orlowski — Paolo Poto

12:00 - Security & Cybersecurity

Luca Bechelli — Daniele Ali

Alessio Pennasilico

Stefano Zanero — Claudio Telmon

Martedì 20 Ottobre pomeriggio — Tavole rotonde

14:00 – Dove va la tecnologia

Marella Folgori — David Neumarker
Valentina Frediani — Pietro Lanza

15:00 – L'innovazione e le paure

Alfonso Fuggetta — Daniela Clerici
Alex Orlowski — Alessandro Garofalo

16:30 – Smartworking e Controlli interni

Paola Rocco — Mariano Corso
Andrea Garulli — Alessandro Garofalo

Mercoledì 21 Ottobre — Le presentazioni

09:00	*Apertura collegamento*
09:15	Introduzione
09:30	**Dance Band on the Titanic: The Data Loss Iceberg Principle** **Richard Hollis**, *Director Risk Crew*
	break out & surveys
10:30	IoT magic gadgets for bad people in enterprise environments, **Davide Casale**, *Shorr Kan*
	break out & surveys
11:20	Supply-chain attack ed insider threat, tecnologie per il threat hunting, **Marco Zonta**, *Cyber Armor*
	break out & surveys
12:10	Incident Response e Digital Forensics Readiness in azienda, **Mattia Epifani**, *RE@LITY NET*
13:00	*pausa pranzo*
14:00	La Cybersecurity nell'IoT e nel dominio Automotive, **Filippo Capocasale**, *NTTDATA*
	break out & surveys
15:00	Intelligenza artificiale e sicurezza: le sfide oltre le opportunità, **Mauro Barni**, *Università di Siena*
	break out & surveys
16:00	Il Cybercrime scopre IoT, **Fabrizio Sensibile**, *@Mediaservice.net*
	break out & surveys
17:00	Panel Session e discussione
17:30	*Conclusioni,* ***Stefano Niccolini***

KEYNOTE SPEECH IN ENGLISH

also known as ISACA Milan Chapter

09:30

DANCE BAND ON THE TITANIC: THE DATA LOSS ICEBERG PRINCIPLE

What if everything we're doing to secure our data is for naught? Have you stopped and thought that perhaps this data has already been compromised and the efforts we continually make to protect it are – too little too late?

This presentation assesses the current threat landscape and explores the idea that the vast majority of the sensitive data processed stored and transmitted every day by governments, NGO's, businesses and private individuals has already been breached and we are wasting our time and money trying to protect it. Are the information technology systems we currently use even capable of this role? The presentation compares the data losses publicly acknowledged to date through mandatory disclosure laws against the widely held principle that they are only a small percentage of the actually losses incurred. If this is true then a new security paradigm is required but what would this look like?

Richard Hollis

Cyber Security & Privacy Expert, Risk Crew

Richard Hollis is the Chief Executive Officer for a London-based, European cyber security consultancy firm called Risk Crew specialising in data security risk management and testing services.

Richard possesses over 30 years of "hands on" skills and experience in designing, implementing, managing and auditing information security risk management programs.

Over the course of his career Richard has served as Director of Security for Phillips, Paris, and Deputy Director of Security for the US Embassy Moscow Reconstruction Project as well as a variety of sensitive security positions within the US government and military. In addition to his work with the Risk Crew, Richard serves on several security technology company boards and security industry advisory councils. Richard is a celebrated public speaker and seasoned ISACA CISM, CRISC, CSX and Cybersecurity Audit certifications trainer. Richard has presented to hundreds of audiences across the world on a wide variety of

information risk management topics and techniques. As a recognised industry authority, he has published numerous articles and white papers and appeared on national and international broadcast news shows as well as being cited in a wide range of press including the BBC, MSNBC, Radio 4, the Financial Times, Time magazine and various others.

also known as ISACA Milan Chapter

9:30

TAVOLA ROTONDA: DIGITAL TRANSFORMATION

Ettore Turra

Direttore Dipartimento Tecnologie, APSS Trento

Ettore Turra è laureato in economia aziendale all'Università Bocconi di Milano. Prima di occuparsi di sanità ha svolto esperienze nel settore della consulenza aziendale e nel High Tech (J.D. Edwards, Arthur Andersen, Siebel Systems). Lavora nell'Azienda Provinciale per i Servizi Sanitari (APSS) dal 2003 dove ha svolto funzioni di pianificazione e controllo strategico, governo dell'IT, sviluppo dell'organizzazione e dei sistemi e direzione del Project management office (PMO). Nel 2011 è stato nominato alla guida della tecnostruttura Area sistemi di gestione con responsabilità dei sistemi informativi, del controllo di gestione, dei progetti e programmi aziendali di cambiamento tecnologico e organizzativo. Dall'agosto 2017 è Direttore del Dipartimento Tecnologie e da marzo 2018 riveste anche il ruolo di Responsabile della Transizione al Digitale. Ha realizzato in APSS i maggiori progetti di automazione dei processi e di sanità digitale. È senior project manager certificato IPMA e Agile Certified Scrum Product Owner (CSPO). Inserito nell'Elenco nazionale del Ministero della Salute dei soggetti idonei alla nomina di direttore generale delle aziende sanitarie locali, delle aziende ospedaliere e degli altri enti del servizio sanitario nazionale.

9:30

TAVOLA ROTONDA: DIGITAL TRANSFORMATION

Tommaso Dradi

Responsabile dell'Unità di Gestione Architettura d'impresa, Direzione Sistemi Informativi e Agenda Digitale, Comune di Milano

Tommaso Dradi si occupa di sviluppare la pratica di Enterprise Architecture per contribuire ai progetti di trasformazione digitale del Comune di Milano. In precedenza ha intrapreso progetti di sicurezza informatica nell'ambito di startup del settore bancario.

9:30

TAVOLA ROTONDA: DIGITAL TRANSFORMATION

Luca Gastaldi

Direttore dell'Osservatorio Agenda Digitale, Politecnico di Milano

Luca Gastaldi, è direttore dell'Osservatorio Agenda Digitale, un gruppo di ricerca del Politecnico di Milano che offre modelli interpretativi, strumenti fondati su solide evidenze empiriche e spazi di confronto per attuare le opportunità offerte dall'Innovazione Digitale nell'ambito della Pubblica Amministrazione italiana.

9:30

TAVOLA ROTONDA: DIGITAL TRANSFORMATION

Martina Pugliese

Neolaureata in Ingegneria Gestionale al Politecnico di Milano

Martina Pugliese si è recentemente laureata in ingegneria gestionale al Politecnico di Milano con specializzazione in Digital Business and Market Innovation. Ha svolto uno stage presso il Comune di Milano in collaborazione con AIEA dove ha sviluppato la ricerca della sua Tesi di laurea. In particolare, ha approfondito il tema della Trasformazione Digitale nella Pubblica Amministrazione presentando il caso del Comune di Milano e studiando come l'implementazione di un framework come COBIT possa supportare il cambiamento e incrementare il livello di maturità dell'IT Governance.

10:30

TAVOLA ROTONDA: INTELLIGENZA ARTIFICIALE

Marco Gori

Università di Siena

Marco Gori received the Ph.D. degree in 1990 from Università di Bologna, Italy, working partly at the School of Computer Science (McGill University, Montreal). In 1992, he became an Associate Professor of Computer Science at Università di Firenze and, in November 1995, he joint the Università di Siena, where he is currently full professor of computer science, where he is leading the Siena Artificial Intelligence Lab (SAILAB) http://sailab.diism.unisi.it/ Professor Gori is primarily interests in machine learning with applications to pattern recognition, Web mining, game playing, and bioinformatics. He has recently published the monograph “Machine Learning: A constraint-based approach,” (MK, 560 pp., 2018), which contains a unified view of his approach. His pioneering role in neural networks has been emerging especially from the recent interest in Graph Neural Networks, that he contributed to introduce in the seminal paper “Graph Neural Networks,” IEEE-TNN, 2009, which received nearly 500 citations in 2019. Professor Gori has been the chair of the Italian Chapter of the IEEE Computation Intelligence Society and the President of the Italian Association for Artificial Intelligence. He is a Fellow of IEEE, a Fellow of EurAI, and a Fellow of IAPR. He was one the first people involved in European project on Artificial Intelligence CLAIRE, and he is currently a Fellow of Machine Learning association ELLIS. He is in the scientific committee of ICAR-CNR and is the President of the Scientific Committee of FBK-ICT. He has been recently invited by the Agence Nationale de la Recherche of France to be a member of the pool of experts for the French national research plan on AI. Dr. Gori is currently holding the 3IA Chair position at the Université Cote d’Azur.

10:30

TAVOLA ROTONDA: INTELLIGENZA ARTIFICIALE

15:00

TAVOLA ROTONDA: L'INNOVAZIONE E LE PAURE

Alex Orlowski

Waters On Mars

Fin da giovanissimo si appassiona alla informatica e cinema da 30 anni lavora nel campo della comunicazione prima come regista e pubblicitario a Londra per poi concentrarsi sulla comunicazione internet come esperto di propaganda online e OSINT (open source intelligence). Scrive per Rolling Stone Italia ed ha collaborato a varie inchieste sul mondo della disinformazione ed estremismi online con Fanpage e Sandro Ruotolo, Report Rai3, Piazza Pulita LA7, Le Iene Mediaset. Ha al suo attivo, numerose inchieste che hanno scoperchiato il problema dei finti account e della manipolazione del consenso attraverso le reti sociali. Ha fondato la Start-Up innovativa WOM, con cui ha creato un tool di analisi dei social e internet che permette la identificazione di casi di **information disorder** e account automatizzati (**BOTnet**)

10:30

TAVOLA ROTONDA: INTELLIGENZA ARTIFICIALE

Paolo Poto

Expert System

Alcune applicazioni dell'informatica sono per me una vera e propria passione, fin dai tempi dell'Università: il primo "social" che quotidianamente frequentavo richiedeva un terminale a caratteri e un lentissimo modem telefonico, il primo chatbot riconosceva una decina di parole chiave per azzardare una risposta.
Sono passati molti anni ma sono riuscito a seguire questa mia passione: lavoro nel campo dell'intelligenza artificiale specializzata nella comprensione del linguaggio. Ho avuto così la possibilità di imparare sul campo cosa vuol dire applicare efficacemente l'intelligenza artificiale nelle Banche, nelle Assicurazioni e negli altri settori.

10:30

TAVOLA ROTONDA: INTELLIGENZA ARTIFICIALE

Antonio Mauro

Chief Cyber Protection, Innovation and IoT Officer, DeepCyber

My responsibility and focus also include the IoT world (included ICS and SCADA) in particular my team manage high technology to improve the cybersecurity aspects in our customers. Innovation, Cyber Protection, Design and Architecture, Security R&D, Digital Investigation, Computer Forensics and Compliance is my top activities. I was Captain (reserve force) in The Carabinieri Corps (Department of Defense). I have worked in Government Agencies, Department of Defense, Department of Homeland Security and NATO in preempting, investigating and remediating government cyber espionage, cyber security and cyber terrorism. Furthermore, I have worked with high Government/Defense managers to improve the organization chart and technology aspects. I'm permanent member at The National Security Observatory - Italy MoD - and also member at the New York/New Jersey Electronic Crimes Task Force (NYECTF)-U.S. Secret Service. I'm also member and expert of the Cybersecurity Task Force of the Strategic Forum for Important Projects of Common European Interest (IPCEI) and I am a speaker and member for the San Francisco Bay Area Chapter of InfraGard (InfraGard is a partnership between the Federal Bureau of Investigation (FBI) and members of the private sector to the protection of Critical Infrastructure). Doctor of Philosophy (PhD) graduated in Electronic Communications, Cybercrime Security Governance, focus on Cloud Computing for the U.S. Government from the University of Northwest, US, in more than 20 years of international career (Compaq - Cisco Systems Inc. – ZTE Corporation Octo Group SpA, etc.), I have accumulated various executive experiences across some key high technology sectors. My career track combines operational and strategic leadership roles, leading cyber security, digital forensics, business model in global industries impacted by cyber security and high technology, I have also establish operational security frameworks and adhering to compliance and regulatory requirements. Furthermore also I have managed Information e Cyber Security, Security Audit and Risk Analysis project engagements for a number of clients throughout Europe and U.S. with industry expertise in Public Sector, Financial Institutions, Retail, Energy and Telecommunications. I have developed research projects and prototypes of innovative technologies for Government's crypto communications, information security and computer forensics investigation. I have also two important patent pending: forensics investigations in the Internet of Things (IoT) devices and Method and System for vulnerability assessment of IoT devices. I'm a member of the Scientific Committee for the UNI 11506 as certifier and examiner and Adjunct Professor in many University, Military and Government organizations, I'm also Professor and member of the Academic Board at The University of Northwest in U.S.A. I'm co-authored several books on Information Security and Intelligence, Computer Forensics, Digital Investigations, Cloud Computing, IoT and I also a Consultant for Judge in the Court in the computer forensics and digital forensics area. I'm a spokesman and chairman in many international conferences like to NIST, IEEE, AFCEA Europe, NATO NC3A, Cloud Security Alliance, Mobile World Congress, InfoTech, etc. Complete my profile strong knowledge of information security best practices, standards, frameworks, risk analysis and compliance, such as ISO/IEC 27001, ISO/IEC 27037, ISO 20000-1, ISO 37001, ISO 22301, NIST 800-53, ENISA, PCI DSS, SAE, JFLT, FedRAMP, etc.

12:00

TAVOLA ROTONDA: SECURITY & CYBERSECURITY

Luca Bechelli

Partner P4I

Luca Bechelli, Information & Cyber Security Advisor svolge da più di 20 anni attività di consulenza su temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie.
All'interno di P4I, coordina un team di esperti su tematiche di Cybersecurity, IT Compliance, IT Security Governance, Risk Management, che svolge consulenza rivolta a aziende e pubbliche amministrazioni di varie dimensioni e settori, da quello bancario e assicurativo, al manifatturiero, passando dalla GDO, Oil & Gas, infrastrutture e trasporti.
É membro del Comitato Scientifico Clusit, coopera con l'Osservatorio Cybesecurity e Data Protection del Politecnico di Milano -nell'ambito del quale supporta il coordinamento di gruppi di lavoro, è Direttore Didattico del Master Experis in CyberSecurity, docente presso il master DPO presso Cefriel. Da anni svolge attività di formazione e sensibilizzazioni sulle tematiche di innovazione nell'ambito della sicurezza delle informazioni, in collaborazione con aziende del settore, centri di ricerca e in ambito associativo.

12:00

TAVOLA ROTONDA: SECURITY & CYBERSECURITY

Stefano Zanero

Politecnico di Milano

Stefano Zanero ha ricevuto un dottorato di ricerca in Ingegneria dell'Informazione presso il Dipartimento di Elettronica, Informazione e Bioingegneria del Politecnico di Milano, dove è attualmente professore associato di “Advanced Cybersecurity Topics” e “Computer Forensics and Cybercrime”. Tra i suoi interessi di ricerca figurano la virologia informatica, la sicurezza dei sistemi cyber-fisici, e la cybersecurity in genere. Oltre all'attività didattica presso varie strutture universitarie italiane ed estere, ha partecipato come relatore a numerosissimi convegni internazionali, ed è autore di oltre 90 articoli scientifici pubblicati su riviste e conferenze. È Senior Member dello IEEE (Institute of Electrical and Electronics Engineers) e siede nel Board of Governors internazionale della IEEE Computer Society. È inoltre lifetime senior member della ACM (Association for Computing Machinery), e fellow di ISSA (Information System Security Association). È inoltre fondatore e presidente di Secure Network, una società di consulenza, formazione e servizi alle imprese in tema di sicurezza dell’informazione; co-fondatore di 18Months S.r.l., azienda che sviluppa soluzioni di cloud-based ticketing; co-fondatore di BankSealer, spinoff universitaria nel settore FinTech dedicata all’analisi delle frodi.

12:00

TAVOLA ROTONDA: SECURITY & CYBERSECURITY

Alessio Pennasilico

Partner P4I

Alessio L.R. Pennasilico, Information & Cyber Security Advisor, Security Evangelist, noto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto dei temi legati alla gestione della sicurezza delle informazioni e delle nuove tecnologie. Per questa ragione partecipa da anni come relatore ai più rilevanti eventi di security italiani ed internazionali ed è stato intervistato dalle più prestigiose testate giornalistiche, radio e televisioni nazionali ed internazionali.

All'interno di P4I, per importanti Clienti operanti nei più diversi settori di attività, sviluppa progetti mirati alla riduzione dell'impatto del rischio informatico/cyber sul business aziendale, tenendo conto di compliance a norme e standard, della gestione del cambiamento nell'introduzione di nuovi processi ed eventuali tecnologie correlate.

Credendo che il cyber risk sia un problema organizzativo e non un mero problema tecnologico, Alessio da anni aiuta il top management, lo staff tecnico e l'organizzazione nel suo complesso a sviluppare la corretta sensibilità in merito al problema, tramite sessioni di awareness, formazione e coaching.

Alessio è inoltre membro del Comitato Tecnico Scientifico di Clusit, Presidente di Associazione informatici Professionisti - AIP, membro del Comitato di Schema UNI 11506 di Kiwa Cermet e Vice Presidente del Comitato di Salvaguardia per l'Imparzialità di LRQA, l'ente di certificazione dei Lloyd's.

14:00

TAVOLA ROTONDA: DOVE VA LA TECNOLOGIA

David Neumarker

Head of Cybersecurity, SIA Spa

David Neumarker nasce a Novara nel 1968 e ha conseguito lauree in Scienze dell'Informazione, Scienze Politiche e Scienze Marittime e Navali. Nel 1987 inizia la sua carriera come Ufficiale della Marina Militare dove presta servizio per 10 anni nel corpo dello Stato Maggiore.
Entra successivamente nel Credito Cooperativo con ruoli di responsabilità nell'ambito dei sistemi informativi e networking. Nel 2001 passa in SSB inizialmente in qualità di IT Auditor, poi come Responsabile della funzione IT Security. Nel 2007 David Neumarker viene nominato Responsabile della funzione Security di SIA, occupandosi principalmente di tematiche di protezione dei servizi erogati in favore di istituzioni Finanziarie e Centrali europee, sicurezza dei servizi di monetica e sistemi di pagamento, ICT Security Governance e Compliance, Security Operation Centre, Identity and Access Management.
Dal gennaio 2016 è nominato Responsabile della funzione Cybersecurity.

15:00

TAVOLA ROTONDA: L'INNOVAZIONE E LE PAURE

16:30

TAVOLA ROTONDA: SMARTWORKING E CONTROLLI INTERNI

Alessandro Garofalo

Garofalo & Idee Associate

Fondatore (nel 1995) e titolare di "Garofalo & Idee Associate" (www.garofalo.it), laboratorio per aziende nell'area dello sviluppo di nuovi product concept e nella formazione manageriale innovativa. Nella sua esperienza professionale sono presenti collaborazioni con Ferrari auto, Lavazza, Pirelli, Geox, Technogym, ecc. Dal 2005 al 2012 è stato presidente e poi membro del direttivo di Trentino Sviluppo S.p.A. È docente e responsabile del laboratorio creatività del Master Innovazione della Fondazione Cuoa di Vicenza e professore a contratto presso la Facoltà di Economia dell'Università di Verona nel corso di Leadership e Innovation Management. È docente presso l'Istituto di Studi Militari Marittimi della Marina Militare all'Arsenale di Venezia su innovazione e creatività, docente di innovazione interdisciplinare presso la Scuola Holden di Torino e adjunct faculty member alla Luiss Business School. Negli anni 2016/17 è stato membro del gruppo di lavoro scientifico della Camera di Commercio di Trento per la definizione delle linee di indirizzo per la crescita economica del Trentino. Nel 2019 fa parte della Commissione tecnica per la valutazione dell'assetto delle società pubbliche della Provincia Autonoma di Trento. Ha esperienze lavorative nell'area ricerca e sviluppo in industrie del settore meccanico e energia.

16:30

TAVOLA ROTONDA: SMARTWORKING E CONTROLLI INTERNI

Andrea Garulli

Università di Siena

Andrea Garulli e' nato a Bologna nel 1968. Ha conseguito la Laurea in Ingegneria Elettronica presso l'Università di Firenze nel 1993, e il titolo di Dottore di Ricerca in Ingegneria dei Sistemi presso l'Università di Bologna nel 1997. Nel 1996 ha afferito al Dipartimento di Ingegneria dell'Informazione dell'Università di Siena, presso il quale è Professore Ordinario di Automatica dal 2006. È stato preside della Facoltà di ingegneria e dal 2015 è direttore del Dipartimento di Ingegneria dell'Informazione e Scienze Matematiche.

Ha ricoperto la posizione di visiting scientist presso il Department of Mechanical and Environmental Engineering, University of California at Santa Barbara, USA, e il Department of Electrical Engineering, University of Linkoping, Svezia. E' autore di oltre 200 pubblicazioni su riviste e atti di conferenze internazionali. I suoi principali interessi di ricerca riguardano: identificazione di sistemi dinamici; teoria della stima e del filtraggio; tecniche di ottimizzazione per il controllo robusto; sistemi multi-agente; applicazioni di tecniche di stima e controllo alla robotica mobile e ai sistemi aerospaziali.

16:30

TAVOLA ROTONDA: SMARTWORKING E CONTROLLI INTERNI

Paola Rocco

Intrum Italy

Laureata in Ingegneria Informatica, attualmente ricopre il ruolo di Responsabile della Sicurezza per Intrum Italy SpA ed è anche il LISO di Intrum, il Local information Security Officer del Gruppo per l'italia. Dal 2003 si occupa di sicurezza Informatica e ha lavorato presso le principali aziende di consulenza, occupandosi dei clienti nei principali segmenti di mercato: Telco, Energy&Utilities, Banking e nelle Pubbliche Amministrazioni. Ha gestito progetti relativi sia alla sicurezza logica che alla sicurezza fisica, in particolare ha lavorato nell'ambito del controllo accessi e sistemi di raccolta log, sicurezza perimetrale e DDoS mitigation, networking, policy e procedure di sicurezza, progettazione di sistemi antifrode e antispam per il traffico sms, sistemi integrati di videosorveglianza, Internal Auditing e gli adeguamenti al nuovo regolamento Europeo UE 2016/679.
Lead Auditor ISO 27001, ISO 22301, DPO UNI 11697, Valutatore Privacy 11697, inoltre ha conseguito l'abilitazione come R.S.P.P. e certificazioni tecniche di prodotto. Dal 2013 è Presidente della Commissione Sicurezza Informatica presso l'Ordine degli Ingegneri della provincia di Roma, dove ha tenuto interventi tecnici in Seminari e Corsi. Ha partecipato a conferenze internazionali e pubblicato diversi articoli sul tema della sicurezza informatica ed è docente nel Master "Competenze digitali per la protezione dei dati, la cybersecurity e la privacy" di Tor Vergata, membro del consiglio Direttivo e docente del Master «La cybersecurity per la protezione dei sistemi di controllo nell'industria 4.0 e nelle infrastrutture critiche».

16:30

TAVOLA ROTONDA: SMARTWORKING E CONTROLLI INTERNI

Mariano Corso

Politecnico di Milano

I'm Professor of “Leadership and Innovation” at the School of Management of Politecnico di Milano.
I co-founded the Digital Innovation Observatories, and I'm responsible for many Observatories including Smart Working, HR Innovation Practice, Digital Agenda, Digital Innovation in Healthcare, Cloud and ICT as a Service and the Digital Business-Innovation Academy.
I'm founder and Scientific Director at P4I - Partners4Innovation, the Advisory r Company of the Digital360 group. As senior advisor in management and Digital Transformation, I manage projects for companies, Local Governments and Public Administrations. I promoted and co-ordinated national and international research projects, authored many scientific publications of which more than 180 at the international level.
My specialties are: Digital Innovation, Smart Working, Digital Transformation, Knowledge Management, Enterprise 2.0, Communities of Practice, Outsourcing, ICT Governance, Change Management.

10:30

IOT MAGIC GADGETS FOR BAD PEOPLE IN ENTERPRISE ENVIRONMENTS

In questo intervento si effettuerà una carrellata di strumenti hardware, embedded, ioT utilizzati nelle attività di “Red Teaming” e dai “cattivi” (bad people) per violare infrastrutture telematiche di varia tipologia nel mondo enterprise. L’evoluzione di schede programmabili potenti ed a basso costo (come le Raspberry Pi o altre) ha portato alla realizzazione di strumenti di attacco piccoli ed efficaci sia per attività di ‘intelligence’, che per attività di hacking vero e proprio. Inoltre l’evoluzione delle schede SDR (Software Defined Radio) ha permesso di costruire attacchi anche attraverso i vari canali radio ad oggi utilizzati dai dispositivi ioT (radio DAB, GPS, GSM, ZigBee, Bluetooth, etc.), ampliando ancora di più la superficie di attacco dall’esterno delle aziende (condizionatori, termostati, smartwatch e molto altro). E tale trend con l’avvento pervasivo del 5G sarà sempre maggiore. Si discuterà anche di casi reali, avvenuti negli ultimi tempi, di intrusioni realizzate grazie a piccoli ‘magic gadget’.

Davide Casale

Shorr Kan IT Engineering

Laureato in Ingegneria delle Telecomunicazioni al Politecnico di Torino con una tesi dal titolo: "Progetto di un sistema di telecomunicazione per l'accesso remoto in reti geografiche". Fin da studente svolge attività formativa verso i propri colleghi, attraverso una Borsa di Studio per assistenza nei corsi di Sistemi Informativi I, Fondamenti di Informatica II e Sistemi Informativi II del Politecnico di Torino. Contemporaneamente fornisce un determinante supporto tecnico alle esigenze dell'Associazione degli Studenti Informatici ed inizia la propria opera di consulente per software house ed internet service provider e l'attività di System Administrator ed esperto di sicurezza informatica per reti di server internet, nonchè la docenza per innumerevoli corsi di carattere universitario od aziendale relativamente all'Information Technology. Docente del corso di Reti di Calcolatori, per il Politecnico di Torino, Ingegneria delle Telecomunicazioni. Svolge attività di Security Engineer ed in questo ambito è relatore in svariate conferenze e presente in interviste radiofoniche e giornalistiche come esperto di problematiche di hacking e virus informatici.è esperto di Security Probing e Vulnerability Assessment, di direzione di lavori su infrastrutture perimetrali di sicurezza e sistemi di intrusion detection presso carrier telefonici, banche, assicurazioni, strutture pubbliche, gruppi industriali, 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. Si occupa inoltre di problematiche di Information Technology innovative, di network security, di sistemi di votazione elettronica, di motori di ricerca mirati ad intelligenza artificiale su tecnologie in Fuzzy Logic, di sistemi di desktop videoconference su reti IP su canale satellitare.

11:20

SUPPLY-CHAIN ATTACK ED INSIDER THREAT, TECNOLOGIE PER IL THREAT HUNTING

Gli attacchi informatici basati sull'abuso della catena di fiducia sono in assoluto i più complessi da rilevare. Rientrano in questa categoria sia gli attacchi supply-chain (sfrutto un fornitore), sia quelli portati avanti da membri interni dell'organizzazione. Per rilevare gli stadi iniziali di questi attacchi è fondamentale scomporli in fasi specifiche, conoscere le tecniche e le tattiche utilizzabili in ogni fase ed aver predisposto un sistema di rilevazione di questi comportamenti.
Introdurremo la teoria e vedremo degli esempi pratici di la rilevazione precoce (prima che l'attacco sia stato completato)

Marco Zonta

Cyber Armor

IIngegnere Elettronico (Università di Padova) con un master in telecomunicazioni.
Per 20 anni consulente e docente in ambito IT ed ICT su tecnologie di nicchia in progetti nazionali ed internazionali come UN, NATO e clienti istituzionali.
Grazie alla profonda conoscenza delle tecnologie unita alla capacità di analizzare il mercato, supporta le aziende disegnando con loro strategie innovative per sviluppare mercati e realizzare prodotti/servizi IT ed OT.
Consigliere all'interno dell'associazione APM-Ticino, fotografo, viaggiatore e velista per passione.

12:10

INCIDENT RESPONSE E DIGITAL FORENSICS READINESS IN AZIENDA

Le fasi di gestione e risposta ad un incidente informatico sono critiche poichè hanno il duplice obiettivo di limitare il danno subito, riducendo i tempi e i costi di recupero, e raccogliere i dati utili per una indagine di quanto accaduto al fine di implementare una politica di remediation. Obiettivo del talk è quello di fornire una introduzione al tema, illustrando i concetti di Digital Forensics Readiness, ovvero la capacità di implementare proattivamente sistemi che consentano la raccolte dei dati utili in fase di investigation.

Mattia Epifani

RE@LITY NET - System Solutions

Nato nel 1977 a Genova, è socio e fondatore di REALITY NET – System Solutions, dove si occupa di Digital Forensics, Forensic Readiness, Mobile Security e Incident Response. Laureato in Informatica nel 2002 presso il Dipartimento di Informatica e Scienze dell'Informazione dell'Università degli Studi di Genova, ha conseguito un Master in Controllo di Gestione Aziendale nell'Impresa Moderna presso SOGEA (2004) e un corso di Perfezionamento in Computer Forensics ed Investigazioni Digitali presso l'Università degli Studi di Milano (2009). Ha ottenuto diverse certificazione in materia di sicurezza informatica e digital forensics riconosciute in ambito internazionale e conseguite presso SANS, IISFA International, EC Council, ISFCE, AccessData e Cybex. E' relatore in seminari e corsi in materia di Computer Forensics e Ethical Hacking presso università italiane e straniere, convegni nazionali e internazionali, associazioni, enti pubblici e privati.

14:00

LA CYBERSECURITY NELL'IOT E NEL DOMINIO AUTOMOTIVE

Con la diffusione pervasiva di device IoT e con l'avvento delle auto connesse (e presto a guida autonoma), la Cybersecurity assume una nuova, rilevante importanza in settori che prima trascuravano il rischio dei cyber-attack. Il rigore di alcuni standard emergenti e l'applicazione della "Security by Design" sono la chiave per mitigare i rischi e costituiscono un fattore abilitante per la diffusione delle nuove tecnologie in questi settori.

Filippo Capocasale

NTTDATA

Manager della Security Service Line di NTT DATA Italia, con responsabilità sulla practice "Security Architecture & Innovation", membro del Center of Excellence "Connected Cars" della struttura "Global Automotive" di NTT DATA Corporation. Esperienza quasi ventennale nel mondo della Cybersecurity, svolta principalmente presso clienti del mondo TelCo su tematiche di Identity and Access Management, Enterprise Architectures, Datacenter, ecc.

Da alcuni anni si occupa di tecnologie di sicurezza applicate al mondo IoT ed in particolare al contesto Automotive.

15:00

INTELLIGENZA ARTIFICIALE E SICUREZZA: LE SFIDE OLTRE LE OPPORTUNITÀ

Oltre a offrire nuove opportunità, impensabili fino a pochi anni fa, l'utilizzo delle tecniche di IA per applicazioni di sicurezza pone una serie di sfide legate alla facilità con cui un avversario può sfruttare le peculiarità di tali tecniche per sviluppare nuovi attacchi, sia fisici che digitali. Per evitare che l'utilizzo dell'IA finisca per diminuire, anziché aumentare, la sicurezza dei sistemi da proteggere, è necessario che le problematiche di sicurezza legate all'IA siano studiate attentamente, sia per evitare di trascurarne la pericolosità, sia perevitare che la loro stessa esistenza mini la fiducia in questo tipo di tecniche. L'obiettivo di questo intervento è illustrare le nuove sfide di sicurezza poste dall'utilizzo sempre più diffuso delle tecniche di intelligenza artificiale e i tentativi in atto da parte dei ricercatori per rendere i sistemi basati su IA veramente sicuri.

Mauro Barni

Università di Siena

Oltre a offrire nuove opportunità, impensabili fino a pochi anni fa, l'utilizzo delle tecniche di IA per applicazioni di sicurezza pone una serie di sfide legate alla facilità con cui un avversario può sfruttare le peculiarità di tali tecniche per sviluppare nuovi attacchi, sia fisici che digitali. Per evitare che l'utilizzo dell'IA finisca per diminuire, anziché aumentare, la sicurezza dei sistemi da proteggere, è necessario che le problematiche di sicurezza legate all'IA siano studiate attentamente, sia per evitare di trascurarne la pericolosità, sia per evitare che la loro stessa esistenza mini la fiducia in questo tipo di tecniche. L'obiettivo di questo intervento è illustrare le nuove sfide di sicurezza poste dall'utilizzo sempre più diffuso delle tecniche di intelligenza artificiale e i tentativi in atto da parte dei ricercatori per rendere i sistemi basati su IA veramente sicuri.
Nel 2004 è stato il general chairman dell'IEEE Multimedia Signal Processing Workshop e nel, 2005 il general chairman della IV edizione dell'International Workshop on Digital Watermarking. Nel 2008 ha ricevuto il premio per il miglior articolo dell'IEEE Signal Processing Magazine, e nel 2010 il premio per il miglior paper apparso su IEEE Transactions on Geoscience and Remote Sensing. Ha fondato l'EURASIP Journal on Information Security ed ha ricoperto la posizione di Editor in Chief dell'IEEE Transactions on Information Forensics and Security deal 2014 al 2017. Dal 2010 al 2011, è stato il chairman dell'IEEE Information Forensics and Security Technical Committee (IFS-TC) della IEEE Signal Processing Society. In precedenza è stato membro dell'IEEE Multimedia Signal Processing technical committee e parte del Conference Board della IEEE Signal Processing Society. Attualmente è il presidente del chapter italiano della società per l'elaborazione dei segnali dell'IEEE. Mauro Barni è fellow dell'IEEE e senior member dell'EURASIP. È stato nominato distinguished lecturer dalla IEEE Signal Processing Society per gli anni 2013 e 2014.

16:00

IL CYBERCRIME SCOPRE IOT

Durante questo incontro verrà presentata una panoramica relativa all'evoluzione degli attacchi che hanno "rincorso" in questi anni il progresso della domotica, e in generale dei sistemi smart, che ormai pervadono la quotidianità delle case intelligenti. Si affronteranno casi reali del recente passato e verranno inoltre presentati i trend e le ipotesi della comunità internazionale su possibili tipologie di attacco future.

Fabrizio Sensibile

@Mediaservice.net

Opera professionalmente nel settore della IT Security dal 1997. E' impiegato dal 2000 come Senior Security Tester nella Divisione Sicurezza Dati per la società @ Mediaservice.net S.r.l. Former Contributor della metodologia OSSTMM e Team Member di ISECOM (Institute of Security and Open Methodologies), Fabrizio è stato il primo ad essere certificato da ISECOM come Authorized International Trainer nel 2002 tenendo negli anni corsi di certificazione in Italia cosi come in Ungheria, Turchia e Sud Africa; in seguito ha conseguito le certificazioni OPSA, HHST, OWSE, OPSE, LA27001 e OSCP. Dal 2010 Fabrizio ha ideato e tenuto diverse sessioni formative per l'Arma dei Carabinieri, agenzie governative e per lo Stato Maggiore della Difesa.

CHAIRMAN

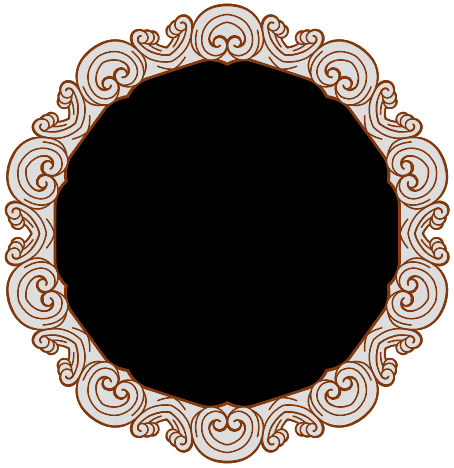
Andrea Chiappetta

autore di Italia.NEXT

Andrea Chiappetta, ha un dottorato in Diritto ed Economia presso l'Università degli Studi di Roma Tor Vergata. Si occupa di cybersicurezza e open innovation. E' consigliere di amministrazione del Centro Studi Americani, Autore di ITALIA.NEXT edito da Rubbettino.
Docente del Master in Sicurezza e Geopolitica presso l'Università Niccolò Cusano

also known as ISACA Milan Chapter

CHAIRMAN



Roberto Rossi

Banca Monte dei Paschi di Siena

Laurea in Scienze Economiche e specializzazioni su temi di sicurezza, geopolitica e guerra economica. Giornalista, ha lavorato per oltre tre lustri per testate della carta stampata e in televisioni locali, nazionali ed estere in Italia e Europa occupandosi di cronaca ed economia reale, soprattutto in ambito agroalimentare, nonché in Africa e nei Balcani in aree interessate da crisi internazionali in fase bellica e post bellica. Da 15 anni lavora in Banca Monte dei Paschi di Siena, prima nella comunicazione, oggi nel comparto sicurezza.

also known as ISACA Milan Chapter

CHAIRMAN

Stefano Niccolini

Presidente AIEA

Stefano Niccolini, CISA, CISM, laurea in fisica, dal 1983 attivo nell'ICT, reti, mainframe, sistemistica, organizzazione. Sono "approdato" all'auditing nel 1999 e all' ICT Auditing dal 2002. Dopo la certificazione CISA (2003) ho collaborato costantemente con AIEA, in particolare in ambito della formazione (COBIT). Mi interesso di innovazione, intelligenza artificiale, big data, big computing, organizzazione, ecc. Sono Presidente di AIEA –ISACA Milan Chapter dal 2013.

also known as ISACA Milan Chapter

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 900 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, CDPSE, 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

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