ASSOCIAZIONE ITALIANA INFORMATION SYSTEMS AUDITORS

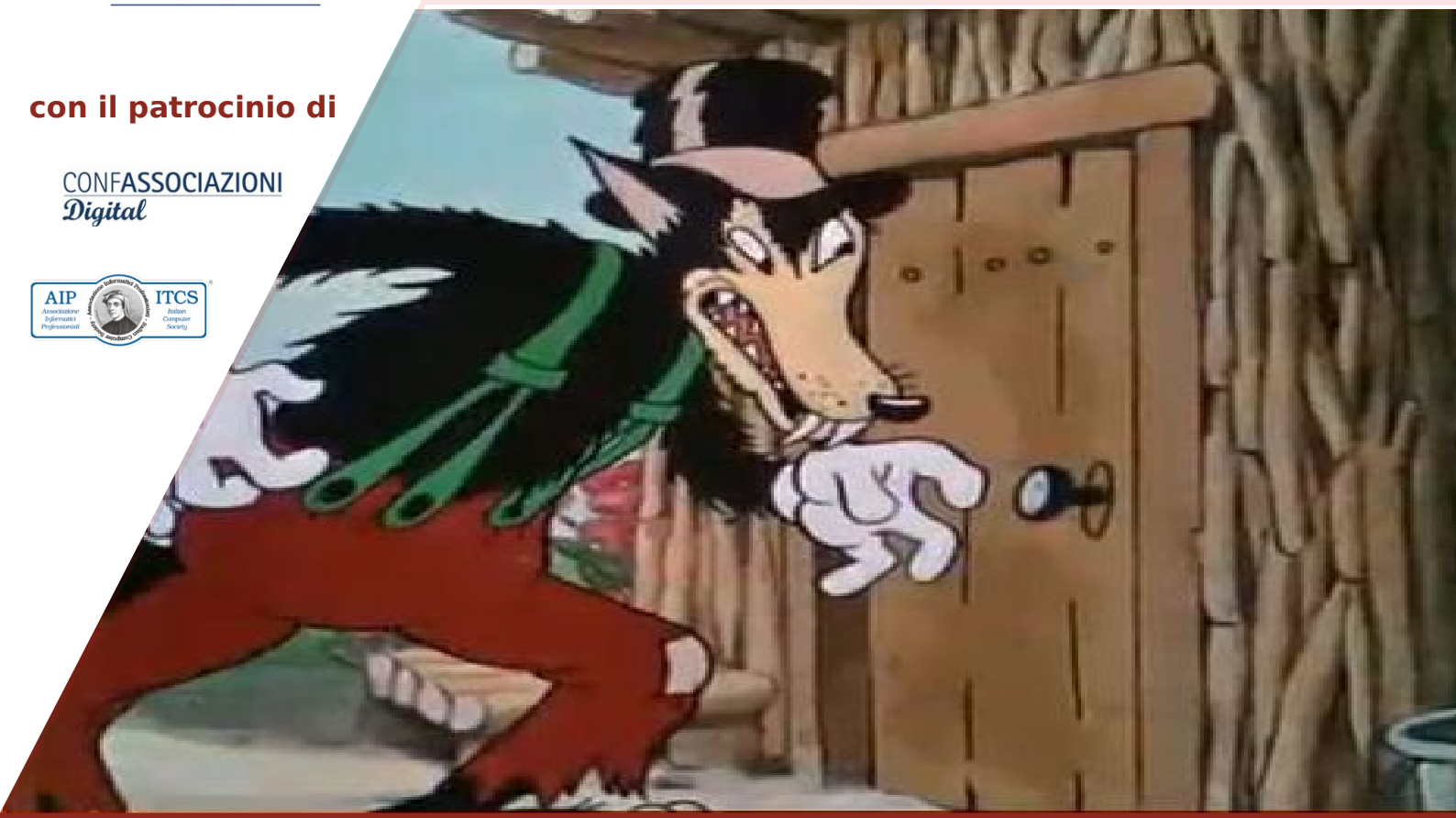
nota anche come

ISACA Milan Chapter

ORDINEdegliINGEGNERI della PROVINCIAdiSIENA

PRESENTANO

con il patrocinio di



Attenti al lupo!!

Controllo Accessi, SIEM e BEC

24 settembre 2021 14.00-18.00

Sessione di Studio in Streaming

PRESENTAZIONI

Alessandro Mecocci, Università di Siena

Intelligenza Artificiale, Edge Computing e Cloud: il futuro del controllo accessi

Controllare dove le persone sono autorizzate ad andare, quando sono autorizzate a farlo e secondo quali modalità possono permanere in determinati spazi, sono alcune delle funzionalità fondamentali dei moderni sistemi di sicurezza e certamente quelle più richieste specialmente in considerazione dell'attuale periodo pandemico. Il controllo degli accessi rappresenta oggi il settore a più alto contenuto di innovazione e con il più rapido tasso di crescita nell'ambito della sicurezza. Gli uffici, i luoghi di lavoro, i luoghi di socializzazione, che stanno finalmente riaprendo le proprie porte grazie a un allentamento delle misure restrittive legate al lockdown, impongono una profonda riflessione e l'adozione di alcuni cambiamenti nel modo di affrontare, pensare e progettare i sistemi di controllo accessi e sicurezza. In particolare, la necessità di rendere sicuri gli ambienti sia per gli impiegati che per gli utenti spinge verso una crescente adozione di tecnologie di controllo di tipo Contactless, ad un incremento delle soluzioni basate su Cloud, alla diffusione delle tecniche di Video Analytics, di analisi dei comportamenti e delle relative modalità biometriche. Con i miglioramenti derivanti dall'intelligenza artificiale e dal Machine Learning, le attività sospette potranno essere rilevate istantaneamente. Gli addetti alla sicurezza non dovranno più rimanere a fissare schermi di computer, ma potranno dedicare il loro tempo ad attività di pattugliamento e di osservazione dello spazio circostante. In caso di anomalia i corrispondenti specifici eventi saranno automaticamente notificati direttamente ai loro cellulari, rendendo possibili eventuali interventi mirati in tempo reale. Il Covid-19 ha reso più veloce il passaggio dal paradigma di controllo accessi al paradigma di controllo delle presenze. Prima del Covid-19, infatti, l'attenzione era tutta volta a conoscere l'identità di coloro che stavano entrando in una certa area mentre attualmente è altrettanto importante sapere con precisione dove si trovano le persone all'interno dei medesimi spazi per poter assicurare il corretto distanziamento oppure per supportare la diminuzione della densità nelle aree comuni. Durante la presentazione saranno illustrati alcuni risultati delle ricerche relative alle moderne tecniche di gestione dell'accesso con particolare riguardo alle problematiche di gestione di flussi ad alta densità in aree di socializzazione outdoor, nonché alcuni aspetti legati all'uso delle tecniche di Deep Learning nella rilevazione automatica di condizioni anomale. Saranno discusse brevemente anche alcune delle problematiche legate alla autenticazione e re-identificazione mediante metodi Contactless.

PRESENTAZIONI

Antonio Pusceddu, SecureWorks

E' finita l'era del Siem? I nuovi strumenti di Extended Detection & Response

Le soluzioni XDR (Extended Detection and Response) rappresentano la nuova generazione strumenti per la rilevazione e risposta di attacchi informatici mirati, di ogni tipo. Ma come queste soluzioni di nuova generazione di distinguono rispetto ai "security services" tradizionali? E che impatto puo avere una soluzione XDR nella produttivita ed efficienza delle imprese?

E' finita l'era del SIEM? I nuovi strumenti di Extended Detection & Response

- *Proteggi la superficie attaccabile, a 360 gradi*
- *Riduci il carico di lavoro: stop a "falsi positivi" e "rumore di fondo"*
- *" SOC as a service": un team di specialisti al tuo fianco per tutto il ciclo di gestione dell'incidente, inclusa la fase di incident response. Con un click*

Maurizio Spinelli, PepsiCo Europe

Business Email Compromise – Definizione, anatomia e controlli da implementare per ridurre il rischio aziendale.

Business Email Compromise (BEC) è una delle truffe più utilizzate via email per veicolare malware di ogni genere, tra cui i famigerati ransomware. In sostanza, il funzionamento ha le caratteristiche di una truffa classica, dove la tecnologia è un nuovo e rapido mezzo per portare a termine il raggiro.
La sessione di studio propone una definizione di un business email compromise. Segue l'anatomia di un potenziale attacco BEC.
La sessione prosegue con una proposta di controlli (preventive/detective) da implementare per difendersi da questo tipo di phishing.
Si conclude con un elenco di buone pratiche d'uso per una corretta gestione della sicurezza e compliance lato utente.

AGENDA

14:00 – 14:10

Avvio streaming

14:10 – 14:20

Saluti del Presidente di AIEA

14:20 – 15:10

Alessandro Mecocci, Università di Siena

Intelligenza Artificiale, Edge Computing e Cloud: il futuro del controllo accessi

15:10 – 16:00

Antonio Pusceddu, SecureWorks

E' finita l'era del Siem? I nuovi strumenti di Extended Detection & Response

16:00 – 16:30

Coffee break

16:30 – 17:20

Maurizio Spinelli, PepsiCo Europe

Business Email Compromise – Definizione, anatomia e controlli da implementare per ridurre il rischio aziendale.

17:20 – 18:00

Confronto e dibattito

18:00

Conclusione e ringraziamenti

RELATORI

Alessandro Mecocci, Università di Siena

1983 laureato con lode in Ingegneria Elettronica - Università di Firenze. 1996-2000 nominato dal MURST Delegato Nazionale a Bruxelles, Telematic Program Committeè for Environment. Curati rapporti tra Ministero e rappresentanze Europee. 1995 progettata la camera di conservazione della Mummia di Similaun (Oetzi) ed il sistema multimediale di fruizione del Nuovo Museo Archelogico di Bolzano. 1997-2005 nominato direttore del 3° polo regionale di trasferimento tecnologico. 2005 primo premio Nazionale "Federculture 2005" innovazione per sicurezza visitatori Palazzo Squarcialupi Santa Maria della Scala (mostra Hugo Pratt). 2006 membro Osservatorio Sicurezza Nazionale (OSN) del Ministero della Difesa. 2009 ad oggi, dirige VISLab sviluppo sistemi avanzati Computer Vision e sistemi di sicurezza (24 anni di cooperazione Autostrade per l'Italia S.p.A., Infoblu, Autostrade Tech). 2009 e 2011 progetta e realizza sistemi Computer Vision real-time per la protezione antivandalismo: Statua dell'Ammannati "Nettuno" P.zza della Signoria (tuttora funzionante) e monumento "Silenzio ascoltate" di Ceroli, Fortezza da basso, Firenze. 2011-2013 responsabile scientifico progettazione Performance Managements System esazione pedaggio su tutta la Francia (progetto EcoMouv). 2016 ad oggi, responsabile scientifico collaborazione RFI – R&D e Protezione Aziendale per lo sviluppo di un aeroporto mobile per Droni volanti (brevetto europeo di RFI ed UNISI) e di sistemi distribuiti di Video Analytics per la sicurezza nelle grandi stazioni, basati su Computer Vision e Deep Learning. E' detentore di 6 brevetti nell'ambito del Signal and Image Processing. E' socio fondatore di 7 start-up.

Antonio Pusceddu, SecureWorks

Antonio Pusceddu, Cyber Security Advisor in Secureworks, vanta oltre 20 anni di esperienza nel mercato IT e nel canale dei partners. Grazie alle sue competenze nell'ambito della cyber-sicurezza, Antonio e' impegnato ogni giorno ad affiancare il mondo delle imprese italiane nel miglioramento della "security posture", a partire dalla rilevazione e risposta a cyber-attacchi di ogni tipo . In Secureworks Antonio e' responsabile dello sviluppo del mercato italiano, coordina le attivita di gestione del canale dei partners e dei clienti "business".

RELATORI

Maurizio Spinelli, PepsiCo Europe

Laureato in Scienze dell'Informazione all'Università di Milano. Esperienza su compagnie internazionali nell'ambito di cybersecurity come definizione di strategie IT/OT di cybersecurity, governance risk and compliance, application risk assessment con mitigazione dei rischi, risk assessment di terze parti con relativa verifica dei contenuti dei contratti/clausole e cybersecurity awareness (ad esempio: phishing campaign, repeated clickers approach, training).
Utilizza frameworks quali COBIT, NIST, SANS, ISO, COSO, Agile, PMI and ITIL.
E' certificato ISACA CISA, CISM, CRISC, CSX and CDPSE.

ISCRIZIONE

Soci AIEA

*L'iscrizione all'evento, gratuita, deve essere completata sul Portale delle Sessioni di Studio AIEA, all'indirizzo **https://portale.aiea.jed.st/** entro e non oltre il 22 aprile 2021. La partecipazione all'evento dà diritto ad acquisire 4 CPE per mantenere le certificazioni CISA, CISM, CGEIT e CRISC.*

Ordine degli Ingegneri

*L'iscrizione all'evento deve essere completata sul portale della Formazione Continua dell'Ordine degli Ingegneri della Provincia di Siena **http://siena.ing4.it/**. La partecipazione all'evento dà diritto ad acquisire **3 CFP**.*

*La partecipazione all'evento richiede un contributo di **5 Euro**.*

Non Soci

*La partecipazione all'evento richiede un contributo di **10 Euro**. Per iscriversi contattare la Segreteria AIEA all'indirizzo email aiea@aiea.it entro e non oltre il 23 settembre 2021.*

*L'evento è **gratuito per gli studenti** e **per i soci delle associazioni patrocinanti.***

ISACA®
Milan Chapter

ORDINE degli INGEGNERI della PROVINCIA di SIENA

L'Ordine è un Ente pubblico Non Economico, ausiliario dello Stato, istituito con Legge Ordinaria.

All'Ordine sono attribuite specifiche competenze; è sottoposto al controllo ed alla vigilanza da parte del Ministero di Grazia e Giustizia, presso il quale è stabilita la sede del Consiglio Nazionale CNI

L'Ordine tiene aggiornato l'elenco degli iscritti nell'Albo Professionale.

La professione di Ingegnere, nei sui vari indirizzi, rientra tra le cosiddette professioni protette; ciò significa che per essere legittimati ad esercitare è necessaria l'iscrizione al relativo albo.
L'Ordine professionale da un lato si fa garante dell'accesso all'esercizio della professione di Ingegnere solo da parte di soggetti in possesso dei requisiti richiesti dalla legge, dall'altro lato esercita controllo sui propri iscritti, richiedendo loro che mantengano un comportamento rispondente alla deontologia professionale.

L'Ordine è totalmente sostenuto dai contributi degli iscritti, conferiti provincia per provincia

http://ording.si.it/

Ordine degli Ingegneri della Provincia di Siena
info@ording.si.it

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 alla 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 135,000 soci in 188 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