SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

ROMA 2015

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma https://www.securitysummit.it/roma-2015, che si terrà nei giorni 10 e 11 giugno presso lo Sheraton Parco de' Medici Rome Hotel https://www.securitysummit.it/roma-2015/location

La partecipazione al Security Summit e a tutti gli eventi che lo compongono è libera e gratuita, con il solo obbligo di iscriversi online su https://www.securitysummit.it/roma-2015/registrazione-eventi

2. PROGRAMMA DEL 10 GIUGNO

09:00 Registrazione

09:30-11:00 – Sala Loggia dei Signori – Sessione plenaria

Introduzione: Gabriele Faggioli, Presidente Clusit

"Presentazione del Rapporto Clusit 2015"

Oltre alla consueta analisi degli attacchi ed incidenti del 2014 in Italia, in Europa e nel mondo, il Rapporto 2015 contiene un contributo inedito della Polizia Postale e delle Comunicazioni ed un altro del Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza. Completano il Rapporto nove Focus On: Internet of (Hacked) Things; M-Commerce; Bitcoin, aspetti tecnici e legali della criptovaluta; Doppia autenticazione per l'accesso ai servizi di posta elettronica; Lo stato della sicurezza dei siti web della pubblica amministrazione; Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni; Cloud e sicurezza: profili legali; Return on Security Investment; L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario.

Modera: Corrado Giustozzi, Membro del Permanent Stakeholders' Group di ENISA

Partecipano:

- alcuni degli autori del Rapporto: Andrea Zapparoli Manzoni, Davide Del Vecchio, Domenico Raguseo, Paolo Bufarini
- Antonio Apruzzese, Direttore del Servizio Polizia Postale e delle Comunicazioni
- Col. Marco Fanti, Nucleo Speciale Frodi Tecnologiche, Guardia di Finanza
- Federico Santi, HP Enterprise Services, Client Principal – Southern Europe
- Alessandro Vallega, Oracle, Security Business Development Manager

11:00-11:30 coffee Break e visita all'area espositiva

11:30-13:00 – Sala Lorenzo – Percorso Professionale Tecnico

"Dati aziendali e smartphone: senza controllo, la pura potenza è causa di continui incidenti"

Un noto slogan di qualche anno fa citava che "la potenza è nulla senza controllo". Questo è particolarmente vero in un'epoca di device potentissimi, troppo spesso utilizzati come strumenti personali, strabordanti di dati aziendali. Con tutti i rischi che le moderne esigenze di collaboration richiedono. Vedremo come il corretto approccio alla

governance ed al risk management, uniti agli strumenti corretti, possono portare ad una forte diminuzione degli incident, oltre che ad un minor impatto del rischio residuo sul business. La consapevolezza, infatti, diventa il fattore determinante per minimizzare i rischi che la complessità di ogni necessaria moderna soluzione porta con se.

Docenti: Alessio Pennasilico, Alessio Banich e Diego Ghidini

11:30-13:00 – Sala Cosimo – Tavola Rotonda

"Diritto alla cura o diritto alla privacy? La sicurezza dei dati in ambito sanitario-ospedaliero"

L'efficienza e l'efficacia dei processi di cura in ambito sanitario non può prescindere dall'utilizzo dell'informatica per trattare i dati personali sanitari; di conseguenza tali sistemi devono necessariamente essere allo stato dell'arte con particolare riferimento alla riservatezza, all'identità personale e al diritto alla protezione dei dati personali. L'autorità Garante per la protezione dei dati personali ha recentemente condotto diverse attività ispettive nei confronti di soggetti sanitari, rilevato irregolarità e dichiarato illeciti alcuni trattamenti. Gli ospedali e le ASL si trovano così nella forbice tra il diritto alla privacy e quello alla cura e devono affrontare le normali difficoltà di security di ogni settore industriale ma esacerbate dagli scarsi investimenti IT degli anni scorsi, dalla frammentazione dei sistemi informativi e applicazioni e dalla rapida evoluzione tecnologica.

La sessione è aperta dall'intervento dell'Autorità Garante che illustrerà sinteticamente le priorità e i riscontri ottenuti dall'attività ispettiva e viene seguita da un serrato confronto su questi temi, con la certezza di fornire elementi utili al miglioramento della situazione attuale in una chiave e con una logica anche tecnologica di security ed organizzativa.

Modera: Alessandro Vallega, Comitato Direttivo Clusit

Partecipano:

- Claudio Filippi, Direttore Dipartimento libertà pubbliche e vice Segretario Generale, Autorità Garante per la protezione dei dati personali
- Cosimo Comella, Dirigente Dipartimento risorse tecnologiche, Autorità Garante per la protezione dei dati personali
- Claudio Caccia, Presidente, AISIS – Associazione Italiana Sistemi Informativi in Sanità
- Vittorio Gallinella, Responsabile dell'area di Tecnologie Infrastrutturali, LAit – Lazio Innovazione Tecnologica
- Francesco Grasso, CIO, Policlinico Umberto Primo
- Raffaella Tibaldi, Product Manager EMR Marketing, NoemaLife
- Luca Boselli, Associate Partner, KPMG Advisory
- Angelo Bosis, Technology Sales Consultant Director, Oracle Italia

– Paolo Capozucca, VP Security e Compliance, Alfa Group

11:30-13:00 – Sala Giuliano – Percorso Professionale Legale

"Sicurezza informatica: attuale panorama normativo e linee di tendenza"

Questa sessione si pone l'obiettivo di fare chiarezza in merito all'attuale panorama normativo analizzando le scelte del legislatore e della Autorità degli ultimi anni e prefigurando le linee di tendenza più rilevanti che si possono intravedere anche alla luce del draft di Regolamento UE oggi disponibile per l'analisi.

Docente: Gabriele Faggioli

13:00-14:00 LUNCH-BUFFET e visita all'area espositiva

14:00-15:30 – Sala Lorenzo – Percorso Professionale sulla Gestione della Sicurezza

"Defence in Depth – Le strategie di riduzione della superficie d'attacco e dei rischi informatici"

La superficie di attacco a cui si espone un'azienda o un'amministrazione è molto ampia e a "geometria variabile". Un attacco informatico può avvenire attraverso differenti vettori, anche combinati tra di loro, allo scopo di colpire tra le pieghe "scoperte" della superficie.

Nella prima parte dell'intervento sarà presentato lo scenario di sicurezza italiano e casi reali di attacco nei quali si combinano diverse tecniche di offesa (targeted malware, social engineering, presa di controllo di dispositivi mobili o di sistemi non direttamente esposti su Internet, etc). Successivamente, saranno definite le possibili strategie di riduzione del rischio e di difesa della superficie esposta agli attacchi, attraverso una serie di contromisure che nel loro insieme si rivelano efficaci. Parleremo di "bastioni", di catene e anelli deboli, di "human factor" e di profondità!

Docenti: Luca Bechelli, Ugo di Nola e Roberto Banfi.

14:00-14:45 – Sala Cosimo – Atelier Tecnologico

"CryptoLocker la punta dell'iceberg, impariamo a difenderci dagli attacchi mirati"

Prendendo spunto (insegnamento) dal Ransomware CryptoLocker, la sessione esamina la tematica degli attacchi mirati e le soluzioni tecnologiche sviluppate da Trend Micro per difendersi.

Relatore: Patrick Gada

14:00-14:45 – Sala Giuliano – Atelier Tecnologico

"Mass scanning delle rete IP italiana & Wardialing dei numeri verdi"

(Cosa emerge da un'analisi svolta sullo stato di salute della rete italiana? Possiamo permetterci di considerarci immuni da minacce o vettori di attacco considerati obsoleti?)

Un'attività' di osservazione realizzata a livello statistico, volta a dimostrare come le attuali tecnologie a portata di tutti e la banda utilizzabile a basso costo possano essere sfruttate da un' agente di minaccia al fine di individuare velocemente e su vasta scala nuovi target e riuscire ad utilizzare efficacemente ancora oggi vettori di attacco considerati obsoleti.

Relatore: Maurizio Agazzini

14:45-15:30 – Sala Cosimo – Atelier Tecnologico

"Privacy e sua gestione secondo i nuovi standard ISO/IEC"

Il prestigioso comitato ISO/IEC SC27, già papà della norma 27001, sta iniziando a pubblicare le prime norme internazionali in materia che saranno utilizzate come riferimento internazionale anche al di fuori dell'Europa per garantire la sicurezza dei trattamenti di dati personali. I temi principali sono le attività di privacy impact assessment, i controlli specifici in materia di data privacy e la gestione delle identità digitali.

Nel corso dell'intervento si darà visione di cosa è stato già fatto finora e, soprattutto, quanto vi è di prossima pubblicazione, cercando di spiegare il motivo per cui queste norme stanno suscitando tanto interesse anche da parte delle autorità garanti.

Relatori: Fabio Guasconi e Francesco Morini

14:45-15:30 – Sala Giuliano – Atelier Tecnologico

"Aspetti di sicurezza di sistemi SCADA e Smart Metering"

I sistemi SCADA e Smart Metering rappresentano una componente centrale nel governo delle infrastrutture industriali e gran parte delle infrastrutture critiche.

Un loro malfunzionamento può avere importanti ripercussioni sia sulla sicurezza e la disponibilità di servizi strategici quali l'energia i trasporti e la sanità, sia sui processi di business.

L'intervento si propone quindi di fornire una panoramica sulle caratteristiche tecnologiche principali di tali infrastrutture, rivolgendo una particolare attenzione agli aspetti di sicurezza e sui profili di rischio, fornendo degli esempi tratti da esperienze concrete.

L'intervento affronterà inoltre i temi della normativa e della regolamentazione esistente o in via di sviluppo per queste aree,

indicando infine delle linee di sviluppo efficaci per aumentare l'affidabilità e la protezione di tali sistemi.

Relatore: Danilo Benedetti

15:30-16:00 - Visita all'area espositiva

16:00-16:45 – Sala Lorenzo – Atelier Tecnologico

"Verso nuovi livelli di Cyber Security Intelligence & Efficacy, a maggiore protezione degli asset, dei dati e delle identità"

L'attenzione e gli investimenti sulla sicurezza IT si sono spostati da tempo sul tema delle Applicazioni come, di recente, sulle minacce avanzate persistenti. Tutto il resto, come i sistemi anti-intrusione e prevenzione, GAV, anti-spam o sistemi di URL filtering, sembrano andare sullo sfondo, assieme all'importanza di dotarsi di politiche di sicurezza e di avere visibilità delle operazioni e del traffico di rete (senza complicare procedure e perdere performance). É tutto questo insieme di questioni che, integrate ad arte e coadiuvate da strumenti efficaci e semplici da usare, forniscono un nuovo livello di Security Intelligence ; Efficacy agli operatori del settore, a maggiore protezione degli asset, dei dati e delle identità.

Relatore: Emilio Tonelli

16:00-16:45 – Sala Cosimo – Atelier Tecnologico

"Infrastrutture convergenti per un'azienda distribuita sicura"

Approfondimenti sull'importanza del nuovo modello convergente che garantisce consolidamento, prestazioni e sicurezza di dati e applicazioni nel data center.

Aspetti tecnici ed esempi concreti di aziende che hanno già implementato SteelFusion, una soluzione che consente alle organizzazioni di ottenere il meglio da entrambi i mondi: centralizzando i dati, eliminando il downtime delle filiali e riducendo il TCO.
Relatori: Valter Villa e Pietro Felisi

16:00-16:45 – Sala Giuliano – Atelier Tecnologico

"La Sicurezza Continua, Selettiva ed Estesa dal Cloud al Perimetro Globale dell'Impresa"

L'ambiente di lavoro di oggi ci porta inevitabilmente ad aprirci sempre più verso l'esterno, tuttavia questo non può avvenire a scapito dell'integrità dell'infrastruttura IT. Come fare per garantire la visibilità continua e totale della propria infrastruttura interna e web? Come permettere la selezione automatica della informazioni critiche di sicurezza, nel mare di dati che transitano? Come fare per proteggere gli

endpoint mobili? Solo soluzioni Cloud evolutive come Qualys possono proporre un modello di sicurezza continua, selettiva ed estesa, garantendo allo stesso tempo di fondersi naturalmente all'interno dei vari centri operativi.

Relatore: Giorgio Gheri

17:00-18:00 – Sala Lorenzo – Seminario a cura dell'(ISC)2 Italy Chapter

"Hic sunt leones ovvero il Deep & Dark Web"

Cosa si nasconde nella parte oscura della rete? Quali sono gli attori principali di un mondo sconosciuto alla maggior parte degli internauti?

A questa ed a molte altre domande su Deep e Dark Web cercheremo di dare risposta dissolvendo i dubbi su questi due termini spesso utilizzati in maniera impropria. I relatori si ripropongono di fare chiarezza iniziando con una disamina tecnica di come funzionano i sistemi per accedere alle risorse del deep e dark web, per proseguire su come si utilizzano, cosa vi si può trovare e per dare infine alcuni suggerimenti per ridurne i rischi di esposizione alle principali minacce che questo mondo sommerso ospita.
Docenti: Stefano Ramacciotti e Pierluigi Paganini

17:00-18:00 – Sala Cosimo – Seminario a cura dell'Associazione Informatici Professionisti (AIP)

17:00-18:00 – Sala Giuliano – Seminario a cura del Centro Italiano di Strategia e Intelligence (CISINT)

"Cyber Jihad"

Docente: Antonio Albanese

3. PROGRAMMA DEL 11 GIUGNO

09:00 Registrazione

09:30-11:00 – Sala Loggia dei Signori – Sessione plenaria

"Il Sistema Pubblico per la gestione dell'Identità Digitale (SPID): stato dell'arte e prospettive dal punto di vista della sicurezza"

Lo Spid nasce per garantire a tutti i cittadini e le imprese un accesso sicuro e protetto ai servizi digitali della PA e dei soggetti privati. La sfida è garantire un adeguato equilibrio tra sicurezza e usabilità , tenendo in conto la potenziale appetibilità delle milioni di future Identità Digitali in relazione ai servizi pubblici e privati che saranno accessibili, ai dati personali che potranno essere trattati e all'evoluzione tecnologica della PA nell'ambito dell'attuazione del programma dell'Agenda Digitale.

Ne parliamo con:

- Enrico Pagliarini, Giornalista Radio24, Moderatore
- Stefano Quintarelli, Deputato, Presidente del Comitato di Indirizzo dell'Agenzia per l'Italia digitale
- Marzia Minozzi, Responsabile relazioni istituzionali e regolamentazione, ASSTEL
- Anna Pia Sassano, Responsabile Architetture Digitali e Servizi per la Pubblica Amministrazione, Poste Italiane
- Cosimo Comella, Dirigente Dipartimento risorse tecnologiche, Autorità Garante per la protezione dei dati personali.

11:00-11:30 coffee Break e visita all'area espositiva

11:30-13:00 – Sala Lorenzo – Percorso Professionale Tecnico

"Nuove strategie per alzare le difese: gestire la complessità"

Con l'ascesa di minacce sempre più sofisticate è quasi impossibile per i singoli prodotti offrire un livello di protezione e di sicurezza efficace. È quindi necessario sviluppare una strategia di governance che tenga conto delle minacce da affrontare da affiancare alle corrette soluzioni di sicurezza, che tra le altre cose devono essere in grado di collaborare fra loro e di condividere informazioni, al fine di diminuire l'impatto di gestione ed aumentare l'efficacia.

Docenti: Alessio Pennasilico e Giovanni Giovannelli

11:30-13:00 – Sala Cosimo – Percorso Professionale sulla Gestione della Sicurezza

"Dall'Information Security alla CyberSecurity, e ritorno (Come migliorare la sicurezza dell'azienda attraverso un efficace governo degli incidenti)"

A fronte dell'escalation delle minacce informatiche degli ultimi tempi, i modelli di gestione della sicurezza devono cambiare? In che modo?

A partire da casi reali e da esperienze sul campo, parleremo di risposta agli incidenti, di come essa possa supportare il governo della sicurezza, di CyberSecurity e di Information Security e di come i due ambiti possano operare in modo coordinato per il miglioramento della protezione delle aziende.

Docenti: Luca Bechelli, Marco Di Leo, Fabio Vernacotola

11:30-12:15 – Sala Giuliano – Atelier Tecnologico

"Database Security questa sconosciuta"

Nel corso degli ultimi tre anni Oracle Italia ha definito ed attuato sui suoi più grandi clienti italiani una metodologia di valutazione della sicurezza del database che poi ha esportato come best practice in Europa. Svolgendo questo lavoro in Italia e all'estero ci siamo resi conto che praticamente tutti fanno gli stessi errori e di questi errori vogliamo parlare affinché vi si possa porre più facilmente rimedio; ma – attenzione – il livello dell'interlocuzione non sarà così tecnico da essere comprensibile ai soli database administrator! Infatti il metodo ha avuto ampio successo perchè ha individuato una modalità per colmare la distanza tra i tecnici e il management ed ha tra i suoi obiettivi l'aumento della consapevolezza del top management.

Relatori: Alessandro Vallega e Angelo Bosis

12:15-13:00 – Sala Giuliano – Atelier Tecnologico

"L'evoluzione della sicurezza delle informazioni: da supporto alle operazioni IT a componente dei processi di business"

Le esigenze di sicurezza di una moderna azienda sono oggi diverse, più estese e complesse rispetto a quelle di qualche anno fa. Le organizzazioni di oggi devono affrontare una realtà ostile fatta di rischi e minacce spesso interamente nuovi.

Essendo cambiato il ruolo stesso della tecnologia dell'informazione, che da mero supporto operativo è diventato fattore abilitante del business, è cambiato di conseguenza il ruolo della sicurezza: non più elemento puramente tecnologico avulso dalle attività aziendali, ma componente stesso dei processi di business.

È dunque importante che le aziende si dotino di un modello organizzativo che, integrando le esigenze di tutela e protezione dei processi di business all'interno dei processi stessi, attui un sistema virtuoso di corporate governance in grado di assicurare il raggiungimento degli obiettivi minimizzando incidenti e disfunzioni.

Relatori: Corrado Giustozzi e Pietro Monti

13:00-14:00 LUNCH-BUFFET e visita all'area espositiva

14:00-15:30 – Sala Lorenzo – Tavola Rotonda

"Casi di studio di attacchi informatici: il contributo dei CERT"

Modera: Corrado Giustozzi

Partecipano:

- Sandro Mari, CERT Nazionale
- Mario Terranova, CERT PA
- Simona Venuti, GARR-CERT
- Andrea Volponi, CERT Poste Italiane

14:00-15:30 – Sala Cosimo – Percorso Professionale Tecnico

"Come interrompere la "Kill Chain" prima che sia troppo tardi: esempi pratici"

I due principali problemi che i difensori devono affrontare oggi sono da un lato come acquisire la capacità di individuare con tempestività un attacco in corso e dall'altro come intervenire in modo efficace per ridurne al massimo l'impatto.

Risolvere questi problemi significa riuscire a combattere ad armi pari con gli attaccanti, applicando al meglio processi, competenze e tecnologie per fare prevenzione e per accelerare le attività di incident response. In questo seminario saranno illustrati alcuni tipici scenari di attacco e come affrontarli correttamente per interrompere la "kill chain" prima che i danni potenziali diventino effettivi.

Docenti: Andrea Zapparoli Manzoni e Stefania Iannelli

14:00-15:30 – Sala Giuliano – Percorso Professionale Tecnico

"Authentication, Authorization & Security Analytics: accesso ragionato alle risorse in base all'indice di rischio"

Progettare e implementare reti sicure in grado di prevenire ogni minaccia e capaci di concedere o negare accesso alle risorse in maniera dinamica ed in real time.

Docenti: Claudio Dell'Ali e Alessio lo Turco

15:30-16:00 Visita all'area espositiva

16.00-16.45 – Sala Cosimo – Atelier Tecnologico

"Approcci innovativi alla gestione delle vulnerabilità software – Il caso di successo di Gaz De France"

Come la tecnologia Skybox Vulnerability Control ha permesso ad Atos di risolvere il problema di Gaz De France nella gestione delle vulnerabilità software. Gaz De France ora può prevenire le intrusioni e non deve più limitarsi a reagire; allo stesso tempo ha diminuito i costi, ha aumentato velocità e precisione delle sue azioni correttive, e può monitorare l'efficacia dei suoi piani d'azione.

Agenda: Il problema: descrizione della situazione iniziale del cliente "Gaz De France – Suez" (Francia); Cenni sulla gara e sui vincoli esistenti; Descrizione della soluzione vincente: Skybox Vulnerability Control + Skybox Vulnerability Detector + sonde nessus a basso costo ingegnerizzate da Atos; Implementazione del progetto e consegna "chiavi in mano"; Risultati e pareri del cliente.

Relatori: Mauro Cicognini e Marco Conflitti

16.00-16.45 – Sala Giuliano – Atelier Tecnologico

"Security Analytics attraverso i Machine Data, ovvero la gestione delle minacce note e non"

La presentazione spiega agli esperti di Security come l'innovazione portata dall"Operational Intelligence" venga ulteriormente ampliata e valorizzata nei casi di Security Intelligence & Analytics grazie allo sfruttamento in Tempo Reale dei Machine Data (il segmento dei BIGDATA a più alta crescita, con la più estesa varietà e a maggior valore) creando un nuovo standard che va oltre i limiti dei SIEM tradizionali.

Relatore: Emanuele Pasqualucci

17:00-18:00 – Sala Lorenzo – Percorso Professionale Tecnico – SESSIONE IN LINGUA INGLESE

"e-Crime Intelligence in .MIL, .GOV and other environments: real-life examples and field experiences"

This presentation will provide a final explanation of the e-Crime Intelligence, aka "Cyber Intelligence", a terminology which is too often misunderstood.

The speakers will deliver to the audience their professional experiences, highlighting how such sources can definitely help out organizations when it's about avoiding data breaches, targeted attacks and serious, unexpected security issues.

Docenti: Raoul Chiesa e Andrew Komarov

17:00-18:00 – Sala Cosimo – Seminario a cura dell'Italian Chapter di IISFA (International Information Systems Forensics Association)

Modera: Gerardo Costabile, Presidente dell'Italian Chapter di IISFA

Interventi:

"Dall' acquisizione del device all'analisi dei dati e dei tabulati di traffico"

Nell'intervento verranno analizzate le metodologie attinenti la repertazione di dispositivi mobili in sede di sequestro, la successiva fase dell'esame tecnico e un approfondimento su quello che sono le aree di copertura delle BTS e relativa interpretazione del dato acquisito presso il gestore di riferimento.

Docente: Giuseppe Dezzani

"Il valore probatorio dei documenti e della posta elettronica nelle indagini informatiche: aspetti giuridici e giurisprudenziali di tali acquisizioni forensi anche alla luce delle nuove norme introdotte con la legge Antiterrorismo (art. 234 bis c.p.p)"

Nell'intervento verranno analizzati i profili giuridici e processuali dell'acquisizione dei dati informatici e della posta elettronica tenendo presente i fondamentali principi di garanzia dei diritti di tutte le parti processuali. Oggi più di prima, strumenti tecnologici avanzati consentono l'acquisizione di dati informatici (e quindi di posta elettronica e più in generale di corrispondenza) da una parte all'altra del mondo.

Forze di polizia, magistratura e avvocatura, il mondo dei consulenti tecnici e soprattutto il legislatore italiano ed europeo si trova di fronte ad una nuova sfida culturale sulla quale si baserà il futuro della riservatezza e della sicurezza dei cittadini

Docente: Stefano Aterno

17:00-18:00 – Sala Giuliano – Seminario a cura dell'Associazione Nazionale per Operatori e Responsabili della Conservazione Digitale (ANORC)

"La sicurezza nei sistemi di conservazione digitale"

Come cambiano le regole sulla conservazione dopo l'introduzione del DPCM 3 dicembre 2013

Il sistema di conservazione e i modelli organizzativi

L'importanza dell'Analisi del rischio per la determinazione delle misure di sicurezza da adottare

Gli standard per la gestione degli archivi e la conservazione dei documenti (ISO 14721– OAIS; ISO 15489, UNI 11386 – UNI SINCRO)

Gli standard di sicurezza nella gestione delle informazioni (ISO 27000)

Docenti: Andrea Lisi e Fabio Guasconi

4. HACKING FILM FESTIVAL

La VII edizione dell'Hacking Film Festival, evento culturale "satellite" del Security Summit, sarà dedicata a cortometraggi e filmati indipendenti sul tema dell'hacking e della (in)sicurezza.

Al termine della prima giornata, mercoledì 10 , dalle 18.30 alle 20.30 saranno proiettate opere che illustrano "dall'interno" l'ambiente e il fenomeno hacker, i casi giudiziari più importanti che hanno attraversato il panorama tecnologico underground e le problematiche di sicurezza e vulnerabilità dei sistemi.

Durante il Festival Alessio Pennasilico, Cristiano Cafferata, Davide Del Vecchio e Corrado Giustozzi coordineranno un breve dibattito sui contenuti e ascolteranno e commenteranno le osservazioni del pubblico.

L'Hacking Film Festival è realizzato in collaborazione con la Facoltà di Informatica Giuridica dell'Università degli Studi di Milano. Si ringrazia il prof. Giovanni Ziccardi, responsabile scientifico del Festival.

PROGRAMMAZIONE

10 giugno, orario 18.30 – 20.30

Telefilm Scorpion: prima puntata (pilot)
Ovvero cosa pensa il mondo degli hacker e della sicurezza informatica.

5. ATTESTATI E CREDITI CPE

Tutte le sessioni, tenute da esperti del mondo accademico e da professionisti del settore, danno diritto a crediti/ore CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua. L'Attestato di Partecipazione viene rilasciato solo a chi ha assistito all'intera sessione e risulta regolarmente registrato.

Gli attestati saranno inviati, per email, solo a chi ne farà richiesta a attestati@clusit.it.

La registrazione è possibile solo online sul portale e non sono accettate altre modalità di registrazione come email o fax.

Le registrazioni potranno essere accettate anche direttamente alla Reception del Security Summit, ma non potrà essere garantita la disponibilità del posto in sala, né l'eventuale materiale didattico.

6. GLI SPONSOR

Sponsor Partner

Oracle Community For Security

Sponsor Platinum

Sponsor Gold

Sponsor Silver

Sponsor Tecnico

Sponsor dell'Hacking Film Festival

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*

Dipartimento di Informatica - Università degli Studi di Milano
Via Comelico 39 - 20135 MILANO - cell. 347.2319285

* associazione senza fini di lucro, costituita il 4 luglio 2000