SPECIALE

SECURITY TECHNOLOGIES MANAGEMENT COMPLIANCE SUMMIT

ROMA 2012

Indice

1. PRESENTAZIONE

Sono aperte le iscrizioni al Security Summit di Roma, che si terrà nei giorni 6 e 7 giugno presso l'SGM Conference Center
www.sgmconferencecenter.it

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/user/register

2. PROGRAMMA DEL 6 GIUGNO

09.00 Registrazione - Welcome Coffee

09:45-12:30 - AUDITORIUM - CONVEGNO DI APERTURA - TAVOLA ROTONDA

"La sicurezza ICT e le proposte per l'Agenda Digitale e l'innovazione in Italia"

Il convegno di apertura del summit sarà costituito da una Tavola Rotonda sul tema della sicurezza ICT in Italia. Si inizierà con la presentazione dal Rapporto Clusit 2012, aggiornato per l'occasione con l'analisi su cybercrime ed eventi dannosi verificatesi negli ultimi mesi, passando quindi alle iniziative dell'Agenda Digitale proposte in Cabina di Regia all'attenzione del Ministro Passera e del Governo Monti e più in generale a quali sono le priorità per 2012 e 2013.

La Tavola Rotonda sarà moderata da Gigi Tagliapietra, Presidente Clusit.

Partecipano:

- **Antonio Apruzzese, Direttore Polizia Postale e delle Comunicazioni**
- **Paolo Campobasso, Senior Vice President and Group Chief Security Officer Finmeccanica**
- **Domenico Casalino, Amm. Del. Consip SpA (Ministero dell'Economia e delle Finanze - MEF)**
- **Gastone Nencini, Senior Technical Manager Trend Micro**
- **Giovanni Todaro, IBM Security Systems Leader**
- **Alessandro Vallega, Oracle Security Business Development Manager e Responsabile dell'Oracle Community for Security.**

12.30-14.00 LUNCH-BUFFET e visita all'area espositiva

14:00-15:30 - AUDITORIUM - PERCORSO PROFESSIONALE LEGALE

"Privacy nel Cloud dal punto di vista di un Titolare italiano"

La sicurezza e la privacy rappresentano la principale preoccupazione delle aziende che intendono adottare soluzioni di public cloud, e questo fa da contraltare ai grandi benefici, economici, di qualità e flessibilità, che sono previsti. Come deve comportarsi un'azienda italiana titolare dei trattamenti per adottare il Cloud? Quali misure di sicurezza servono, cosa negoziare con i fornitori, come adeguare l'organizzazione? La legge italiana ne ostacola l'adozione?

Il Cloud è una necessità dell'Europa. Oltre che usarlo è necessario promuoverne attivamente la realizzazione e rimuovere gli ostacoli tecnologici e normativi. La pubblica amministrazione può giocare il duplice ruolo di cloud consumer e di cloud provider. Quali settori ne potrebbero beneficiare per primi? Quali modelli di servizio e di deployment sono i più indicati? Cosa serve a livello di governance?

Modera: Alessandro Vallega

Intervengono: Rosario Piazzese, Gerolamo Pellicanò, Giuseppe Russo, Guglielmo Troiano

È stato invitato un rappresentante dell'Autorità Garante per la protezione dei dati personali.

14:00-15:30 SALA LUCIA - PERCORSO PROFESSIONALE TECNICO

" L'oro dei nostri giorni. I dati aziendali, i furti, la loro protezione in un ambiente oltre i confini"

Perché i rapinatori di treni miravano ai treni carichi d'oro? L'oro era un valore e il treno era il posto più facile per rubarlo.

Che si tratti di dati finanziari, dati personali o dati intellettuali, tutto ha un valore elevato per i criminali che li rubano e in un ambiente caratterizzato dalla mancanza di confini aziendali, dati in-the-cloud e utilizzo di device personali per lavoro, il problema della protezione dei dati diventa ancora più complesso.

In questo seminario cercheremo di evidenziare opportunità e pericoli, così da conoscere le domande giuste da farsi nel momento in cui ci si scontrerà, volenti o nolenti, con queste problematiche.

Docenti: Alessio Pennasilico e Gastone Nencini

14:00-14:45 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Sicurezza dei pagamenti via internet"

La sicurezza dei pagamenti via internet, che avvengano tramite carte di credito, mandati di pagamento, carte virtuali, trasferimento di credito o borsellini elettronici, è un prerequisito importante per il commercio elettronico e il contrasto alla criminalità organizzata. Recentemente il Forum Europeo sulla Sicurezza dei Pagamenti Retail, SecuRe Pay, costituito da numerose autorità bancarie e regolatorie europee, tra le quali la Banca d'Italia, ha raccomandato una serie di misure organizzative e tecnologiche che dovranno essere adottate dai Payment Service Processor e spinte presso gli eMerchants. In questo atelier si analizza questo contributo e se ne discute con i partecipanti raccordando le raccomandazioni e le best practice con le tecnologie.

Docenti: Fabio Guasconi e Domenico Catalano

14:45-15:30 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Security Intelligence: un approcccio predittivo per la protezione di infrastruttura, dati e applicazioni"

Nell'epoca dei Big Data, nell'impresa ci sono più informazioni utili che mai, subito accessibili praticamente a chiunque. Mano a mano che le aziende si rendono conto di quanto preziosi siano effettivamente questi dati, si accorgono ben presto di aver bisogno di metodi migliori per proteggere questo patrimonio. Naturalmente la sfida sta nel fatto che i dati che richiedono protezione, ora come ora, sono ovunque. Ecco perché le organizzazioni IT hanno bisogno di un approccio olistico alla sicurezza dati che includa valutazioni della vulnerabilità e monitoraggio dell'attività dei database, cifratura e automatic data discovery. Questa combinazione di strumenti di sicurezza e analitica intelligente rende possibile non solo proteggere i dati critici, ma anche correlare eventi per identificare possibili pattern di abuso sui dati aziendali da parte di insider.

Docenti: Giovanni Abbadessa e Marco Ercolani

15.30-16.00 Visita all'area espositiva

16:00-17:30 - AUDITORIUM - PERCORSO PROFESSIONALE LEGALE

"Mobile Privacy: rischi, requisiti formali, misure minime ed idonee da considerare..."

La sessione presenta i risultati di un gruppo di lavoro multidisciplinare realizzato negli ultimi mesi da aziende con diverse competenze specifiche (legali, tecniche, metodologiche ed organizzative), riunite sotto il comune ombrello della Oracle Community for Security. In particolare il gruppo di lavoro si è focalizzato sull'analisi dei rischi, dei requisiti formali, delle misure minime, obbligatorie ed idonee relativi ai trattamenti di dati personali effettuati in ambito aziendale mediante dispositivi mobili evoluti (smartphone e tablet). Il risultato dell'analisi è un contributo strutturato che sulla base della normativa attuale e dei rischi indicati dalla bibliografia esistente, individua quali sono i requisiti che un'azienda che adotti tali dispositivi dovrebbe tenere in considerazione, fornendo altresì qualche spunto di riflessione originale.

Modera: Alessandro Vallega

Intervengono: Riccardo Abeti, Luca Boselli, Jonathan Brera, Paolo Capozucca, Sergio Fumagalli, Barbara Indovina

È stato invitato un rappresentante dell'Autorità Garante per la protezione dei dati personali.

16:00-17:30 SALA LUCIA - PERCORSO PROFESSIONALE TECNICO

"Cyber Warfare 2.0"

In questo intervento i due relatori analizzeranno tematiche quali social intelligence, organized (cyber)crime, cyberweapons, SEA (state-Endorsed Attacks) come Cina, India e Pakistan, ma anche NATO, US DoD e molto altro...

Ospite speciale l'Avvocato Stefano Mele, esperto sul tema e-weapons e "cyber*".

Docenti: RaouL Chiesa, Andrea Zapparoli Manzoni, Stefano Mele.

16:00-16:45 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Il DNS: un'infrastruttura critica di supporto"

Si definisce infrastruttura critica un sistema che ha un forte impatto sulla vita dei cittadini e che, se danneggiato, può mettere a rischio la loro sicurezza. Esempi di infrastrutture critiche comunemente accettate come tali sono reti elettriche, impianti chimici, gasdotti, ma anche ospedali, sistemi di controllo aereo e così via.

Tali infrastrutture sono oggi esposte a numerose minacce dovute all'utilizzo di reti informatiche al fine di espanderne le capacità ed i servizi. Alla luce di tali considerazioni, questo atelier punterà ad evidenziare la rilevanza del Domain Name System nell'operatività delle infrastrutture critiche classiche (e di conseguenza la necessità di annoverare il DNS stesso tra le infrastrutture critiche).

Dopo aver illustrato gli elementi funzionali ed operativi del DNS, ed aver presentato le sue vulnerabilità, verrà mostrato come un attacco al Domain Name System od un suo fault accidentale, possa seriamente impattare sull'operatività di una infrastruttura complessa e critica come quella elettrica. Verrà in particolare mostrato come un fallimento del DNS possa danneggiare l'operatività dell'infrastruttura elettrica sia ad alto livello (mercato energetico, coordinamento tra gli operatori, crisis management ecc.) sia a basso livello (es. operatività di una centrale elettrica).

Successivamente verrà fornita una panoramica delle specifiche DNSSEC, che definiscono delle estensioni di sicurezza per il protocollo DNS e la cui adozione è attualmente in corso. Infine, saranno descritti alcuni meccanismi adottati ad esempio per i root nameserver come protezione dai denial-of-service distribuiti.

Docenti: Igor Nai Fovino, Claudio Telmon

16:45-17:30 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Nuovi protocolli per nuovi servizi"

In un futuro molto prossimo, nuovi protocolli per la trasmissione dati e tecnologie di produzione CMOS a livelli di pochi nanometri consentiranno di concepire un'ampia gamma di nuovi servizi in grado di interagire, in modo anche molto complesso e con assoluta trasparenza per gli utenti, con i client e l'ambiente che li circonda. Preludio di questo nuovo paradigma di elaborazione distribuita sono, in particolare, le reti di sensori e gli smartphones. Queste piattaforme operative implementano già oggi una serie di funzionalità operative ed abilitano a modalità d'uso difficilmente immaginabili pochi anni fa, in ambiti che vanno dal monitoraggio ambientale, al controllo di filiera, fino alla virtualizzazione in mobilità di servizi di sportello ed alla pletora di applicazioni di natura partecipativa cui ci stanno abituando le reti sociali.

Tuttavia, molti di questi servizi sono e saranno soggetti a nuove e complesse minacce volte a sovvertirne il funzionamento o a violare in qualche modo le risorse da essi gestite. In molti casi, i vincoli in termini di risorse computazionali o imposti dai requisiti funzionali non consentono di ricorrere alle implementazioni crittografiche tradizionali, o richiedono addirittura nuove tecniche e protocolli.

Questo intervento illustra alcune delle attività di ricerca e sviluppo su questi temi svolte dall'Istituto di Calcolo e Reti ad Alte Prestazioni (ICAR) del CNR, anche in collaborazione con vari gruppi universitari. L'intervento vorrebbe anche promuovere sinergie e collaborazioni tra il mondo delle imprese e quello della ricerca, sensibilizzando le aziende - sia in qualità di partner di sviluppo, sia come potenziali fruitori - su questi temi. Le opportunità di sviluppo e di profitto, soprattutto nel mercato delle Tecnologie dell'Informazione, sono invero proporzionali ad immaginare nuovi scenari funzionali e applicativi, ed a concepirne e realizzarne i metodi e le tecnologie abilitanti.

Docente: Giovanni Schmid

Seguono:

18.00-20.00 HACKING FILM FESTIVAL

20.00-21.00 APERITIVO

3. PROGRAMMA DEL 7 GIUGNO

09:00 Registrazione

09:30-11:00 - AUDITORIUM - PERCORSO PROFESSIONALE TECNICO

"Cloud, Hacker, Media: cosa succede davvero?"

Leggiamo quotidianamente sui ogni media notizie che riguardano la tecnologia, gli attacchi, i rischi. Non sempre le notizie riportano una analisi dell'accaduto. Cercheremo di correlare un po' di fatti di cronaca per capire il contesto, le implicazioni e soprattutto cosa gli hacker hanno a che fare con quel che accade. Ci focalizzeremo anche sul caso MegaUpload per avere un esempio concreto ed esplicativo.

Docente: Alessio Pennasilico

09:30-11:00 SALA LUCIA - PERCORSO PROFESSIONALE LEGALE

"La legge, la tecnologia e la sicurezza dei dati e dei sistemi: dalla normativa sulla privacy ai modelli organizzativi e di controllo"

La sicurezza e la riservatezza nel trattamento dei dati trovano sempre più spazio nelle normative comunitarie e nazionali. Allo stato, le normative più interessanti sono certamente il D.Lgs. 196/03 sul trattamento dei dati personali e il D.Lgs. 231/01 sulla responsabilità amministrativa delle persone giuridiche, delle società e delle associazioni. Con la recente abrogazione dell'obbligo di tenere un aggiornato Documento Programmatico sulla Sicurezza, tuttavia, i modelli organizzativi ex D.Lgs. 231/01 rappresentano l'ultima misura di sicurezza documentale obbligatoria rimasta, sebbene limitatamente ai reati presupposto della legge. Nel corso dell'intervento si illustreranno gli obblighi di sicurezza ancora esistenti per legge e il loro impatto sulle aziende.

Docente: Pierluigi Perri

09:30-10:15 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Il ruolo di una rete satellitare nella garanzia di sicurezza"

L'attività di violazione o di protezione dei dati è principalmente svolta a livello di applicazione sia in termini di identificazione di vulnerabilità che di attuazione di contromisure. Pertanto, l'attenzione è rivolta a quella fase del processo che genera le informazioni o che ha come scopo la fruizione delle stesse.

Raramente si pone attenzione alla infrastruttura di telecomunicazioni, dal punto di vista logico al di sotto dell'applicazione, che rappresenta il mezzo attraverso cui le informazioni fluiscono dalla sorgente al destinatario, che presenta specifiche vulnerabilità e necessità dell'attuazione di adeguate contromisure. In particolare, le architetture di rete adottate sono spesso dettate da necessità di ottimizzare le

prestazioni che talvolta può rappresentare un obbiettivo antitetico rispetto alla sicurezza. Tale è il caso di reti eterogenee per le quali occorre armonizzare tecniche trasmissive e le architetture protocollari e caso ancora più particolare è rappresentato dalle reti satellitari o da reti in cui il segmento satellitare è una componente importante.

In questo caso, alcune caratteristiche garantiscono dei livelli intrinseci di sicurezza mentre altre rappresentano degli elementi peculiari di vulnerabilità che vanno pertanto trattati e contrastati in maniera altrettanto peculiare.
Il gruppo di Telecomunicazioni Multimediali Satellitari dell'università di Roma Tor Vergata, che espone una pluriennale esperienza nel settore con particolare riguardo alla sicurezza, si propone di affrontare il tema, si ribadisce, poco trattato della rilevanza della infrastruttura e delle architetture protocollari nell'approccio alla protezione dei dati. Il gruppo ha inoltre sviluppato un emulatore di rete satellitare in grado di riprodurre fedelissimamente il funzionamento di una rete vera (protocolli, pacchetti, instradamento, generazione di traffico, multiterminali, interfacce) che può essere mostrato e utilizzato per attività di dimostrazione in loco ed in tempo reale di casi di studio reali di attacchi e di attuazione di contromisure.

L'intervento è rivolto a:
chi si interessa della progettazione, realizzazione e gestione di una rete di telecomunicazioni, che possibilmente includa un segmento satellitare, che abbia l'obbiettivo di garantire protezione dei dati; chi si occupa di sicurezza a livello applicativo e vuole validare approcci e concetti su un sistema di telecomunicazioni senza dovere ricorrere ad una rete operativa che oltre ai maggiori costi offre minore flessibilità; chi vuole acquisire conoscenza sul ruolo dell'infrastruttura nella fornitura di sicurezza.

Modalità di svolgimento:
Presentazione del problema della sicurezza in una rete satellitare nella considerazione delle peculiari caratteristiche architetturali e protocollari.

Presentazione di casi di studio con dimostrazione in tempo reale effettuata utilizzando l'emulatore di rete.

Docenti: Michele Luglio, Cesare Roseti, Francesco Zampognaro

10:15-11:00 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Crittografia e Enterprise Key Management una sfida possibile da affrontare"

Le moderne esigenze di protezione dei dati richiedono un sempre maggiore utilizzo della crittografia. L'introduzione in ambito aziendale di tecniche crittografiche per la protezione delle informazioni è fonte di una nuova problematica: la buona gestione delle chiavi di crittografia coinvolte. In questo intervento vedremo come la crittografia e gli strumenti di Enterprise Key Management sono implementati negli approcci di Oracle e SafeNet.

Docenti: Simone Mola e Giuseppe Russo

11.00-11.30 coffee Break e visita all'area espositiva

11:30-13:00 AUDITORIUM - PERCORSO PROFESSIONALE TECNICO

"Cybercrime: evoluzione del malware e degli attacchi"

Docenti: Raoul Chiesa e Cesare Radaelli

11:30-13:00 SALA LUCIA - PERCORSO PROFESSIONALE TECNICO

"La sicurezza in ambiente Mobile"

Docenti: Andrea Zapparoli Manzoni e Antonio Gallotti

11:30-12:15 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Proteggere i dati dove stanno: nel database"

Il furto di dati e la perdita di riservatezza avviene nella grande maggioranza dei casi dal database. Il database ben protetto all'interno del data center è uno dei bersagli più ambiti dai criminali o dagli utenti disonesti per via del valore informativo che esso rappresenta. Vi si trovano dati importanti come segreti industriali (prezzi di acquisto nel caso della GDO, piani di prospezione geologica per l'industria petrolifera...), liste di carte di credito per merchant, acquirer ed issuer o dati protetti per legge (personali sanitari, giudiziari e altri dati sensibili) ecc.

Quali sono le principali motivazioni di un progetto di sicurezza in questo ambito? Come si affronta la tematica per massimizzare i propri investimenti? Che tecnologie si possono utilizzare per proteggersi da hacker e amministratori di sistema disonesti?

Docenti: Guido Milana e Angelo Bosis

12:15-13:00 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Dalla virtualizzazione al Cloud Computing: identificare le corrette strategie di sicurezza per la protezione dei dati critici"

La razionalizzazione dei costi trasversali dell'IT è, per le imprese, un obiettivo sempre più importante in tempi difficili come quelli che stiamo vivendo. In questo contesto, virtualizzazione e cloud, sono visti come sistemi che possono portare grandi benefici, come la riduzione del consumo di energia, la migliore gestione di hardware, software, risorse umane, e altri costi, liberando tempo per produrre business.

Il futuro prossimo vedrà un'IT sempre più dinamica, interattiva, e questo riguarderà gli accessi, i dati e tutte le risorse computazionali. Grazie anche al fenomeno della "consumerizzazione", gli utenti mobili avranno

accesso a gigabyte di informazioni.Questi profondi cambiamenti porteranno sicuramente a riconsiderare tutti gli aspetti della sicurezza.

Per Trend Micro il cloud computing è sinonimo di cloud security, e se le aziende vogliono fare affidamento sul cloud Internet per archiviare i dati e condurre il business, debbono disporre di una garanzia di una sicurezza superiore, progettata per la protezione in-the-cloud.

Docente: Maurizio Martinozzi

13.00-14.30 LUNCH-BUFFET e visita all'area espositiva

14:30-16:00 AUDITORIUM - PERCORSO PROFESSIONALE TECNICO

"Protezione dei dati in azienda: la difficoltà di coniugare obiettivi e complessità "nonostante" l'ampia disponibilità di strumenti per la sicurezza"

Avere chiarezza degli obiettivi, visione e conoscenza del contesto è determinante nel raggiungimento di uno standard di sicurezza adeguato per le informazioni aziendali, sebbene la realtà quotidiana e la complessità di processi/organizzazione rendano questo compito estremamente difficile. La stessa disponibilità di soluzioni di sicurezza, in questo scenario, non sempre offre i risultati attesi, come le cronache di quest'anno hanno dimostrato.

Durante l'intervento saranno esaminate (a partire da esperienze reali) metodologie e tecnologie adottate dalle imprese nell'ambito dei processi fondamentali della sicurezza, per individuarne i principali limiti e le opportunità mancate, cercando di offrire spunti di riflessione circa le possibili aree di miglioramento relativamente alla protezione dei dati.

L'intervento si chiuderà con un Case Study che descriverà i principali vettori di ingresso ed i rischi concreti rilevati durante un caso reale di Penetration Test, evidenziando metodi e soluzioni di mitigazione delle minacce basati su un approccio trasversale.

Docenti: Luca Bechelli e Riccardo Morsicani

14:30-16:00 SALA LUCIA - TAVOLA ROTONDA

"La sicurezza ICT nella PA: novità, previsioni e limiti in tempo di crisi"

Modera: Giovanni Manca

Intervengono:

- Giuseppe Cattaneo, Università di Salerno, su "La sicurezza ICT nella PA: stato dell'arte e metodologie di valutazione"
- Stefano Arbia, DigitPA, "Le emanande Regole Tecniche: principali novità e previsione sull'emanazione dei provvedimenti notificati alla Commissione Europea"

- Armando Leotta, Banca d'Italia, "La sicurezza ICT nella PA: possibili approcci e vincoli operativi e d'esercibilità".

14:30-15:15 SALA SCOLASTICA - ATELIER TECNOLOGICO

"Social Network: dalla Percezione del rischio dell'utente alla Valutazione del rischio del cybercriminale"

E' innegabile il contributo sociale ed economico che può scaturire dall'uso dei social network. Ma altrettanto evidenti sono le opportunità criminogene che essi possono fornire. Il rischio, nella sua percezione e valutazione, costituisce il comune denominatore tra l'utente e il cybercriminale. Ma con approcci ovviamente diversi. Quali i meccanismi psicologici e criminologici? L'intervento intende analizzare questi aspetti.

Docenti: Isabella Corradini e Andrea Zapparoli Manzoni

15:15-16:00 SALA SCOLASTICA - ATELIER TECNOLOGICO

"L'anello debole nella catena della fiducia in Rete"

I recenti casi di attacchi alle Certification Authorities hanno messo in luce la fragilità della catena di fiducia in Rete. Le infrastrutture critiche non sono solo quelle da cui dipende il funzionamento della Rete: il vero punto debole sono i servizi da cui dipende la Rete stessa.

Docente: Corrado Giustozzi

16.00-16.30 Visita all'area espositiva

16:30-18:00 – AUDITORIUM - SEMINARIO ITSecPro (Italian Security Professionals Group)

"Security Intelligence e Cloud: la sfida a Botnet, APT e 0day"

Il crescente numero e la sempre maggiore complessità degli attacchi mirati sta rivoluzionando il panorama della sicurezza informatica. Le tecnologie tradizionali basate su pattern di riconoscimento statici non sono più sufficienti a contrastare efficacemente le minacce, e stanno lasciando il passo ad un nuovo modello che vede nella condivisione delle informazioni nel cloud la chiave di successo per mitigare fenomeni quali Botnet, APT e 0day. Questo approccio è chiamato Security Intelligence ed è l'argomento della tavola rotonda. Il fatto di poter rilevare e contrastare minacce informatiche sino a ieri invisibili apre la strada a nuove problematiche del tutto inedite, di conseguenza l'argomento verrà affrontato in un'ampia prospettiva che include aspetti tecnologici, organizzativi e legali.

Modera: Paolo Passeri
Intervengono: Andy Dancer, Raoul "Nobody" Chiesa e Stefano Mele

16:30-18:00 SALA SCOLASTICA - SEMINARIO AIIC (Associazione Italiana esperti in Infrastrutture Critiche)

"AIIC, Associazione Italiana Esperti Infrastrutturee Critiche, ed i suoi Gruppi di Lavoro"

Sulla scia del successo nell'anno 2011 del Gruppo di Lavoro sul PSO (Piano Sicurezza Operatore) il cui Rapporto Finale è disponibile sul sito AIIC, il Consiglio Direttivo AIIC ha deciso di sostenere per l'anno 2012 i seguenti quattro GdL:

1) **"Aspetti legali per la redazione del PSO", coordinatore Alessandro Lazari**
2) **"Definizione di un Data Model per il PSO", coordinatore Bruno Carbone**
3) **"Sicurezza dei Sistemi Idrici", coordinatori Enzo Maria Tieghi e Roberto Setola**
4) **"Sicurezza dei Sistemi SCADA", coordinatore Stefano Panzieri**

I Coordinatori presentano le attivitá svolte e quelle in corso e rinnovano la richiesta a tutti i professionisti della security per condividere esperienze e di unirsi ai vari GdL.

Segue tavola rotonda con i Coordinatori, che sono disponibili a qualsiasi chiarimento con tutti gli intervenuti

16:30-18:00 SALA LUCIA - SEMINARIO IISFA (International Information Systems Forensics Association)

"Challenge-Response IISFA: gli esperti rispondono"

Una sessione di domande e risposte con gli esperti di IISFA, animata da Gerardo Costabile e Massimiliano Graziani.

4. HACKING FILM FESTIVAL

E' l'evento culturale "satellite" del Security Summit dedicato ai lungometraggi e documentari indipendenti sul tema dell'hacking e della (in)sicurezza, che per questa terza edizione romana si terrà il 6 giugno dalle 18:00 alle 20:00 e sarà seguito da un aperitivo.

La proiezione sarà presentata e commentata da: Cristiano Cafferata, Raoul Chiesa, Corrado Giustozzi, Alessio Pennasilico e Pierluigi Perri.

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.

Sarà proiettato "Cybercriminals", di Misha Glenny. Autore del libro-cult "McMafia", Misha Glenny ha recentemente pubblicato (2011) il best-seller "Dark Market: Cyberthieves, Cybercops and You".

In questi 18, impressionanti minuti al "TED", Misha analizza i profili di sei cybercriminali e ne racconta la storia, non tralasciando aspetti psicologici e personali.
Un "must-see", un importante insight, per poi commentare insieme al pubblico le diverse opinioni.

La partecipazione è gratuita, ma è necessario iscriversi via email a info@clusit.it. Al termine, gli spettatori sono invitati a partecipare ad un aperitivo.

5. ATTESTATI E CREDITI CPE

Le sessioni che prevedono il rilascio di Attestati di Presenza e l'attribuzione di Crediti CPE sono:

- i Percorsi Professionali (tecnico o legale);
- gli Atelier Tecnologici;
- la tavola rotonda sulla sicurezza ICT nella PA del 7 giugno.

Tutte queste sessioni sono tenute da esperti del mondo accademico e da professionisti del settore e 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 al termine di ciascuna sessione solo a chi ha assistito all'intera sessione e risulta regolarmente registrato. Gli attestati potranno anche essere emessi al termine del Security Summit e inviati per email.
A chi avrà assistito, secondo le regole di cui sopra, a tre sessioni di uno stesso percorso Professionale sarà rilasciato un Diploma.

6. GLI SPONSOR DEL SECURITY SUMMIT ROMA 2012

Sponsor Partner

IBM

TREND MICRO

Oracle Community For Security

ORACLE

ALFA GROUP

KPMG cutting through complexity

SafeNet. THE DATA PROTECTION COMPANY

The Innovation Group

Sponsor Platinum

McAfee An Intel Company

OMNITECH

paloalto NETWORKS the network security company

SONICWALL

Sponsor Silver

Albaest

iDIALOGHI

mediaservice.net

Westcon Security

f5

HP ENTERPRISE SECURITY

Sponsor dell'Hacking Film Festival

Oracle Community For Security

SONICWALL

All'interno dell'SGM Conference Center è previsto uno spazio espositivo a disposizione delle aziende sponsor, in cui incontrare i partecipanti al Security Summit, illustrare i loro prodotti, svolgere dimostrazioni e presentazioni.
Per chi lo desidera, è possibile fissare in anticipo degli incontri, della durata di circa 20 minuti. Per maggiori informazioni e per prenotarsi: https://www.securitysummit.it/page/spazio_espositivo.

CLUSIT - ASSOCIAZIONE ITALIANA PER LA SICUREZZA INFORMATICA*

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

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