DFA OPEN DAY 2014
5 GIUGNO 2014

OSINT e Investigazioni digitali
Security e Incident Response aziendale

EVENTO ACCREDITAMENTO DALL'ORDINE DEGLI AVVOCATI DI MILANO: 6 CREDITI

SPONSOR UFFICIALE
GFI MAX™
Easy, Affordable Hosted IT Solutions

08.45-09.00	*Registrazione dei partecipanti*
09.00-09.45	***Avv. Valerio Vertua,*** *Presidente Digital Forensics Alumni DFA* ***Dott. Loris Angeloni,*** *GFI Max* *Saluti ed introduzione*
09.45-10.30	***Dott. Giuseppe Colazzo, Dott. Ferdinando Ditaranto*** *OSINT: tecniche investigative basate sulle fonti aperte su Internet*
10.30-11.15	***Avv. Giuseppe Vaciago, Dott.ssa Francesca Bosco*** *Security of the Digital Natives*
11.15-11.30	**Pausa caffè**
11.30-12.15	***Matteo G.P. Flora*** *Analizzare la Rete: dalla Reputazione al Digital Profiling per una scienza tra Marketing ed Intelligence*
12.15-13.00	***Avv. Donato La Muscatella, Dott. Mattia Epifani*** *Electronic Evidence Guide – Traduzione Italiana*
13.00-14.00	**Pausa pranzo**
14.00-14.45	***Dott. Nicla Diomede*** *Gestione efficiente degli incidenti di sicurezza in una rete complessa ed eterogenea: un caso reale*
14.45-15.30	***Ing. Marco Carlo Spada*** *Incident Response aziendale: il DDOS su NTP del 10/2/2014*
15.30-15.45	**Pausa caffè**
15.45-16.30	***Avv. Giuseppe Serafini, Ing. Gloria Marcoccio, Dott.ssa Claudia Ciampi*** *Interazioni Cloud, Forensics, Sicurezza e responsabilità amministrativa degli enti*
16.30-17.15	***Dott. Paolo Dal Checco*** *DEFT come strumento di Incident Response*
17.15	*Q&A e chiusura lavori*

SEDE EVENTO:	**ACCESSO:**
Aula 400 – III piano Facoltà di Giurisprudenza Università degli Studi di Milano Via Festa del Perdono, 3	Accesso libero e gratuito. Registrazione su www.perfezionisti.it o http://www.eventbrite.it/e/biglietti-dfa-open-day-2014-11614831273
info@perfezionisti.it	**www.perfezionisti.it**

Con il patrocinio di: Clusit, CSA cloud security alliance, Adeft Associazione, Tech and Law Center

SINTESI DEGLI INTERVENTI

OSINT: tecniche investigative basate sulle fonti aperte su Internet
(Dott. Giuseppe Colazzo, Dott. Ferdinando Ditaranto)
Le fonti aperte costituiscono un enorme serbatoio di informazioni che possono essere sfruttate per l'espletamento delle attività di indagine. Analisi delle più comuni tecniche.

Security of the Digital Natives
(Avv. Giuseppe Vaciago, Dott.ssa Francesca Bosco)
Il progetto Security of the Digital Natives intende studiare il livello di consapevolezza e percezione della sicurezza informatica da parte degli studenti universitari con particolare attenzione al mondo dei dispositivi mobili. La ricerca ha interessato 1012 studenti di oltre 15 diverse università. In considerazione dei risultati, è stata proposta un'implementazione di misure, tecniche e legali, per ridurre, in futuro, i problemi connessi all'errata o non accorta adozione di misure di sicurezza sui propri dispositivi mobili. Video https://www.youtube.com/watch?v=9Dh2quUAjQY&feature=youtu.be.

Analizzare la Rete: dalla Reputazione al Digital Profiling per una scienza tra Marketing ed Intelligence
(Matteo G.P. Flora)
Un excursus pratico tra le varie discipline e tecnologie per capire come sia oggi possibile capire, analizzare ed interpretare le "voci" sulla rete con fini nobili o meno nobili e con incredibili potenzialità da capire, da valutare e, forse, da normare.

Electronic Evidence Guide – Traduzione Italiana
(Avv. Donato La Muscatella, Dott. Mattia Epifani)
La *Guida alla prova digitale* è una "field guide" per forze dell'ordine e autorità giudiziaria. La versione italiana nasce dallo sforzo congiunto delle associazioni Digital Forensics Alumni, Tech and Law Center e DEFT Association.
Link italiano: https://docs.google.com/forms/d/1gwHSgAjlyKWT10FEh8JNIAt_OQBRaCV4Jgt_-SLUWhU/viewform
Link inglese:
http://www.coe.int/t/dghl/cooperation/economiccrime/cybercrime/Documents/Electronic%20Evidence%20Guide/default_en.asp

Gestione efficiente degli incidenti di sicurezza in una rete complessa ed eterogenea: un caso reale
(Dott. Nicla Diomede)
Uno degli aspetti fondamentali nella risposta ad un incidente di sicurezza è la tempestività nell'individuazione dello stesso e nel mettere in atto la relativa azione di contenimento. L'intervento mira ad evidenziare alcune azioni che possono essere intraprese per rendere più efficiente l'Incident Response in uno scenario complesso.

Incident Response aziendale: il DDOS su NTP del 10/2/2014
(Ing. Marco Carlo Spada)
Come l'ho individuato e come ho risposto presso un mio cliente, considerazioni sull'infrastruttura.

Interazioni Cloud, Forensics, Sicurezza e responsabilità amministrativa degli enti
(Avv. Giuseppe Serafini, Dott.ssa Gloria Marcoccio, Dott.ssa Claudia Ciampi)
Presentazione studio con CSA, dedicato alla verifica di alcune delle condizioni di applicabilità del D.lgs. 231/2001 in materia di responsabilità amministrativa delle persone giuridiche, ad alcune fattispecie dei contratti di cloud computing, quali emergenti dalle relazioni di diritto sostanziale, con riferimento alla sicurezza dei dati personali ed ai reati informatici, che si instaurano, per effetto dell'applicazione, alle corrispondenti vicende negoziali, delle disposizioni del Codice in materia di protezione dei dati personali, nonché di alcune previsioni dello standard ISO/IEC 27037.

DEFT come strumento di Incident Response
(Dott. Paolo Dal Checco)
La "dart side" di DEFT (il typo è voluto) consiste in una suite di strumenti aggregati in un framework - espandibile tramite linguaggio XML - che ne permette la ricerca veloce, l'avvio centralizzato e la verifica d'integrità. Il lato Linux e quello Windows di DEFT forniscono gli strumenti per poter gestire in maniera ottimale incidenti informatici, raccogliendo il maggior numero di dati e seguendo le best practice dell'Incident Response. Durante il talk verrà mostrata una panoramica delle potenzialità della suite DEFT con l'estensione di DART, accompagnata da alcuni esempi di utilizzo e case study.