

INDICE

1. Security Summit Academy
2. Pubblicazioni - Articoli
3. Attività di Formazione
4. Reopening the office Readiness - Questionario di self-assessment

NUOVI SOCI

Diamo il benvenuto a:

- Advanction S.A. (Corteglia - Svizzera)
- Maxwell Group (Assago - MI)

1. Security Summit Academy

Continuano gli Atelier della Security Summit Academy.

Questi i prossimi appuntamenti:

- 2 luglio 2020 ore 15:00 - 16:00: "Email threat modeling da strumento di lavoro a principale vettore d'attacco: analisi di scenari avanzati e prevenzione"
<https://securitysummit.it/eventi/academy-2020/sessioni/email-threat-modeling-da-strumento-di-lavoro-a-principale-vettore-dattacco-analisi-di-scenari-avanzati-e-prevenzione>
- 7 luglio 2020 ore 11:00 - 12:00: "Modernizzare le Security Operation: approccio ed esperienze sul campo"
<https://securitysummit.it/eventi/academy-2020/sessioni/modernizzare-le-security-operation-approccio-ed-esperienze-sul-campo>
- 16 luglio 2020 ore 15:00 - 16:00: "Perché la mia infrastruttura sicura è stata bucata proprio ora?"
<https://securitysummit.it/eventi/academy-2020/sessioni/perche-la-mia-infrastruttura-sicura-e-stata-bucata-proprio-ora>

Il calendario è in continuo aggiornamento su <https://securitysummit.it/eventi/academy-2020/agenda>.

La partecipazione è gratuita ma con iscrizione obbligatoria.

Per assistenza nelle iscrizioni: supporto@astrea.pro

È previsto il rilascio di attestati con crediti CPE.

Ogni Atelier, se seguito in diretta e nella sua interezza, dà diritto a 1 credito CPE. Le richieste vanno inviate a: attestati@clusit.it

I video sono disponibili, previa registrazione, su <https://clusit.it/ateliers/>

2. Pubblicazioni - Articoli



"Cybercrime e Darknet Market: cresce la richiesta di deepfake e botnet IoT", un report a cura di Trend Micro.

https://www.trendmicro.com/it_it/about/newsroom/press-releases/2020/20200527-cybercrime-e-darknet-market-cresce-la-richiesta-di-deepfake-e-botnet-iot.html



"Metamorfo: il potente malware che ruba i dati bancari e altri dati personali all'utente", a cura di Bitdefender

<https://www.bitdefender.it/news/metamorfo:-il-potente-malware-che-ruba-i-dati-bancari-e-altri-dati-personali-all&039;utente-3853.html>



Cybercrime e phishing, quanto conta il fattore umano?", di *Salvatore Lombardo*

<https://www.key4biz.it/cybercrime-e-phishing-quanto-counta-il-fattore-umano/308975/>



"Smart working, la nuova dimensione del lavoro", di *Antonino Caffo*.

<http://www.datamanager.it/2020/06/smart-working-la-nuova-dimensione-del-lavoro/>



"Il Rapporto Clusit 2020 e lo stato della sicurezza informatica in pandemia", di *Debora Casalini*.

<https://www.margas.it/il-rapporto-clusit-2020-o-lo-stato-della-sicurezza-informatica-in-pandemia/>



"Supply chain ICT, l'importanza della sicurezza", di *Roberto Obialero*.

<http://www.datamanager.it/2020/06/supply-chain-ict-limportanza-della-sicurezza/>



Relazione sulle attività svolte dall'Autorità Garante per la protezione dei dati personali nel 2019.

<https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/9427952>



"Il codice QR, una scorciatoia che ha fatto strada", *Alessio L.R. Pennasilico* a colloquio con La Stampa Torino sulle possibili criticità di sicurezza di questa "scorciatoia".

<https://www.facebook.com/groups/64807913680/permalink/10157645698768681/>

3. Attività di formazione

Il socio Advanction ci segnala il corso ISO/IEC 27032 Lead Cybersecurity Manager, che permette di conseguire la relativa certificazione rilasciata da PECB.

Il corso si terrà in videoconferenza nelle giornate del 24-25 settembre / 1-2 ottobre 2020.

Ai soci Clusit sono riservate condizioni di favore.

Maggiori informazioni su <https://advanction.com/it/corso-iso-iec-27032-lead-cybersecurity-manager-settembre-2020/>

Il socio ITHUM segnala l'opportunità di frequentare in Virtual Classroom (invece che in aula) i corsi per le certificazioni su Cyber Security e Intelligence.

Ai soci Clusit sono riservate condizioni di favore.

Informazioni e dettagli su <https://www.ithum.it/formazione.html>

4. Reopening the office Readiness - Questionario di self-assessment

Segnaliamo una iniziativa del team Cyber Security Information Resilience di BSI, che ha predisposto un questionario che verifichi quanto le aziende siano pronte alla riapertura in sicurezza degli uffici.

D'ora in avanti, il lavoro da casa e dall'ufficio verranno utilizzati dalle organizzazioni in modo intercambiabile, combinando le due modalità e questo impatta sulla sicurezza.

Vengono poste domande su argomenti come Physical security, Data protection and privacy, Asset management, Access control, Network security, Vulnerability management, Incident management.

Al termine del questionario si riceve uno score che indica le diverse aree e la preparazione delle aziende.

https://forms.office.com/Pages/ResponsePage.aspx?id=_G-UVNNoVUmseNynJtRFtGrG8rBeBslNq37pnwGMo1JUMUVNM1hSUUpNUUY2SIM4RUNBQUo1V0c2NS4u.