

Corso CSA Supply Chain e CRA

16 e 17 Aprile 2026 - Milano

Saper affrontare i nuovi rischi con spunti tecnici e di governo

Abbiamo scelto di focalizzare il corso su 2 argomenti che interessano a molti degli associati. Nella prima giornata vedremo più aspetti tecnici e strumenti mentre la seconda sarà più in ambito governance.

Per la SC:

- Gestione del Rischio (Art. 21)
 - Le aziende non devono solo proteggere il proprio perimetro, ma sono responsabili della sicurezza dell'intero ecosistema di fornitori.
 - Analisi dei Fornitori: È obbligatorio identificare e mappare tutti i fornitori critici e sub-fornitori che hanno accesso a dati o sistemi sensibili.
 - Valutazione della Qualità: Devi valutare la qualità complessiva delle pratiche di cybersicurezza dei fornitori e dei loro prodotti, inclusi i processi di sviluppo sicuro del software.
- Contrattualistica e Compliance
 - Il rapporto con i partner deve essere formalizzato attraverso requisiti di sicurezza stringenti:
 - Clausole Contrattuali: Inserimento di obblighi specifici per la notifica di incidenti, diritti di audit e standard di sicurezza minimi.
 - Audit Regolari: Non basta una valutazione iniziale; sono necessari controlli e verifiche periodiche per confermare che i fornitori mantengano gli standard concordati

Per il CRA

- Audit e valutazione dei rischi: Condurre un'analisi dei rischi di cibersicurezza e un gap analysis sui prodotti attuali.
- Sicurezza fin dalla progettazione: Adottare processi di secure software development per garantire che i prodotti siano privi di vulnerabilità note al momento dell'immissione sul mercato.
- Gestione delle vulnerabilità: Implementare processi per rilevare, analizzare e correggere le vulnerabilità, con obbligo di segnalare exploit attivi all'ENISA entro 24 ore.
- Documentazione tecnica (SBOM): Creare e mantenere un inventario dettagliato delle componenti software (Software Bill of Materials) e la documentazione necessaria per la marcatura CE.
- Aggiornamenti di sicurezza: Fornire patch di sicurezza tempestive e automatiche per il periodo di supporto definito.
- Formazione: Istruire i team tecnici e legali sul nuovo regolamento.

Al termine della prima giornata ci sarà la **prima cena CSA 2026** vicino alla sede del corso. Il costo della cena è incluso nella quota di partecipazione e potranno partecipare anche i soci CSA che non hanno frequentato il corso.

1^ Giornata: 16 Aprile **FOCUS: Supply Chain senza budget** *Docente Marco Dal Broi*

1. Introduzione al contesto e agli obiettivi del corso

Il corso ha l'obiettivo di fornire metodologie tecniche e operative per:

- Identificare e analizzare i rischi della supply chain
- Valutare la postura di sicurezza dei fornitori
- Utilizzare tecniche di ingegnerizzazione OSINT (Open Source Intelligence)
- Integrare informazioni provenienti da fonti terze
- Supportare il raggiungimento dei livelli di compliance richiesti alle strutture territoriali

2. Fondamenti di Supply Chain Risk Management (NIST C-SCRM e NIST SP 800-161 Rev. 1)

2.1 Definizione di rischio nella supply chain

- Rischio operativo
- Rischio cyber
- Rischio reputazionale
- Rischio normativo
- Rischio geopolitico

2.2 Minacce tipiche alla supply chain

- Compromissione di fornitori software
- Vulnerabilità nei servizi cloud
- Dipendenze tecnologiche non mappate
- Fornitori critici non monitorati
- Attacchi di tipo "trusted relationship" (T1199 Mitre ATT&CK)

3. OSINT applicato alla valutazione dei fornitori

3.1 Principi di OSINT

- Raccolta strutturata di informazioni pubbliche
- Correlazione e validazione delle fonti
- Riduzione dei falsi positivi

3.2 Fonti OSINT utilizzabili

- Registri camerali e societari
- Database di vulnerabilità (es. National Vulnerability Database e EUVD)
- Motori di ricerca di esposizione servizi
- Certificazioni pubbliche

- Data breach pubblici
- Marketplace underground (analisi indiretta tramite fonti secondarie)

3.3 Ingegnerizzazione OSINT

Metodologia strutturata:

1. Identificazione del perimetro del fornitore
2. Enumerazione delle tecnologie utilizzate
3. Mappatura superficie d'attacco
4. Identificazione vulnerabilità note
5. Analisi esposizione pubblica
6. Valutazione maturità cyber

4. Identificazione delle tecnologie utilizzate dal fornitore

- DNS e subdomain enumeration
- Certificate transparency
- Identificazione CMS e framework

4.1 Analisi stack tecnologico

- Web server
- Middleware
- Database

4.3 Valenza posturale degli elementi tecnici

Esempi:

Elemento Tecnico | Valenza Posturale
Software non aggiornato | Bassa maturità patch management
Certificati TLS scaduti | Debole governance IT

DNS mal configurato | Rischio spoofing / takeover
Esposizione RDP pubblica | Elevata superficie d'attacco

5. Valutazione della Postura di Sicurezza

5.1 Indicatori di maturità

- Presenza di certificazioni (ISO 27001)
- Pubblicazione di policy di sicurezza
- Bug bounty attivo
- Disclosure policy pubblica
- Tempo medio di remediation

5.2 Scoring della postura

Costruzione di un modello di scoring basato su:

- Esposizione tecnica
- Vulnerabilità note
- Compliance normativa
- Criticità del servizio fornito
- Dipendenza strategica

6. Integrazione con fonti terze

6.1 Tipologie di fonti esterne

- Società di rating cyber
- Database di breach
- Threat intelligence provider
- Autorità di settore

2^ Giornata: 17 Aprile **FOCUS: Rischi Supply Chain e CRA** *Docente Cesare Gallotti*

1. **Approfondimento Supply Chain (mattino):**

- Rischi possono essere: Interruzione di servizi di fornitori (per esempio a causa di fallimento, chiusura, incidenti), dipendenza da un unico fornitore, compromissione dei sistemi IT dei fornitori, rivelazione di informazioni da parte dei fornitori, malfunzionamenti o compromissione software sviluppati dai fornitori.
- Selezione con analisi preventiva per le forniture IT (valutando tipologia di dati personali, criticità dei dati trattati, integrazione con sistemi dell'organizzazione, tipo di fornitura, complessità, eventuale necessità di un passaggio di consegne, dipendenze sicurezza, fornitore italiano o estero (con diversità culturali). fornitore con competenze nel settore dell'organizzazione.
- Censimento.
- Condizioni contrattuali.

- Monitoraggio.
- Audit.

2. **Approfondimento CRA (pomeriggio):**

- Regolamento UE 2024/2847, detto cyber resilience act (CRA):
<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32024R2847>.
- Regolamento di esecuzione (UE) 2025/2392 che definisce le categorie tecniche di prodotti con elementi digitali "importanti e critici" ai sensi del Cyber Resilience Act:
<https://eur-lex.europa.eu/legal-content/IT/TXT/?uri=CELEX:32025R2392>.
- A chi si applica;
- Tempi di applicabilità;
- Altri punti che ho già elencato su questo post:
<https://blog.cesaregallotti.it/2024/11/pubblicato-il-cyber-resilience-act-cra.html>.

CORSO in presenza di 2 lezioni

- **16 Aprile 2026 Ore 10:00 – 18:00 – CENA CSA INCLUSA**
- **17 Aprile 2026 Ore 10:00 – 18:00**

SEDE Selexi S.r.l. Via Gerolamo Vida, 11 - 20127 Milano (Italy) - LAB 03

COSTO Corso a persona:

- **Socio CSA 1.400 Euro**
 - **non Socio CSA 1.600 Euro**
 - **non Socio + Iscrizione CSA 2026 1.900 Euro**
- Importi + IVA Pagamento all'ordine**

Il corso verrà svolto al superamento delle 5 conferme formali. In caso di mancato svolgimento l'ordine formale viene considerato annullato.

Per informazioni scrivere a: moderatore@cybersecurityangels.it

CYBER SECURITY ANGELS

✉ moderatore@cybersecurityangels.it

<https://cybersecurityangels.it>

<https://www.linkedin.com/groups/13573019/>

