ASSINTEL
ASSOCIAZIONE NAZIONALE
IMPRESE ICT

DIDATTICA CORSO CYBER SECURITY

durata: 30gg.

Fondamenti di sicurezza 2gg.

- Basi di sicurezza
- Ciclo di deming
- Gestione delle vulnerabilità
- Tiade CIA
- Procedure, people & technology
- Difesa in profondità (layer per proteggere i dati)
- Il tramonto degli Antivirus: ormai non ci proteggono più
- Analisi dei rischi
- Cenni Normativi
- Sicurezza fisica, logica e procedurale
- Crittografia

Architetture 2gg.

- Architetture multi layer
- Tipologie di autenticazione di rete, 802.1x, …
- Firewall: Application & Statefull Firewall
- IDP e IPS, differenze
- Wifi tipologie
- Infrastrutture Cloud, IaaS, PaaS, SaaS
- IoT, network industriale
- Vulnerabilità multi layer
- Hardening di Server e Client
- Patch Management

Sicurezza offensiva & Esercitazioni di laboratorio 12gg.

- Fasi e metodologia di hacking
- Phase 1 - Reconnaissance

- Phase 2 - Scanning
- Phase 3 – Gaining Access
- Phase 4 – Maintaining Access
- Phase 5 – Covering Tracks
- Types of Attacks on a System
- Operating System Attacks
- Attacchi Application-Level
- Scansioni ed enumerazioni con tools (con pratica)
- Introduzione ai tools di VA
- Scansioni di sistemi di test (con pratica)
- Panoramica sulle principali tecniche di cyber attacco.
- Cos'è il Social Engineering e come difendersi
- Attacchi Mobile
- Attacchi Cloud
- Contromisure
- Antivirus Evasion

Incident Handling & Response (IH&R) & Esercitazioni di laboratorio 7gg.

- Introduction to Incident Handling and Response
- Incident Handling and Response Process
- Forensic Readiness and First Response
- Handling and Responding to Malware Incidents
- Handling and Responding to Email Security Incidents
- Handling and Responding to Network Security Incidents
- Handling and Responding to Web Application Security Incidents
- Handling and Responding to Cloud Security Incidents
- Handling and Responding to Insider Threats
- Analisi dei log
- Il Ransomware, come attacca e come proteggersi
- Cosa fare se siamo stati colpiti da un ransomware: le opzioni possibili
- Implicazioni giuridiche per le vittime dei ransomware

Secure Coding & Mobile Security 3gg.

- Robustezza, Performance e Sicurezza del Software
- Cause delle vulnerabilità
- Costi dei Bugs di sicurezza
- Tipologie di vulnerabilità
- Ciclo di scrittura codice sicuro
- Sicurezza Architetturale e By-Design
- Tipologie di sicurezza
  - Sicurezza per le applicazioni Web
  - Sicurezza per le applicazioni Desktop
  - Sicurezza per le applicazioni Mobile
- Validazione Input utente
- Autenticazione
- Autorizzazione
- Web Security
- Web Service Security
- Framework Security
- Mobile Security

Privacy & Normativa europea e Compliance Internazionali 2gg.

- GDPR – General Data Protection Regulation
- Le ragioni della normativa
- L'ambito di applicazione
- Principi generali
- Diritti dell'interessato ed informativa; titolare del trattamento; responsabile del trattamento
- Data Protection Officer
- Registro delle attività di trattamento e la valutazione di impatto sulla protezione dei dati
- Obblighi di consultazione con l'autorità di controllo
- Codici di condotta e certificazione
- Trasferimento dei dati e problematiche di diritto extracomunitario
- Cybersecurity e Privacy, la protezione dei dati personali
- La cyber-security nel panorama italiano: norme, politiche e istituzioni
- Che cos'è la ISO/IEC 27001 e come si collega e si integra con il GDPR (General Data Protection Regulation)

Cloud & Security 2gg.

- Economia del Cloud Computing
- Cloud Adoption – Practices, Priorities & Responsibility
- Come i servizi Cloud aiutano a mitigare i rischi legati agli attacchi informatici
- Responsabilità SaaS, PaaS, IaaS
- IoT Cloud Security
- Crittografia e sicurezza