ALLEGATO I – Formazione Cyber

Di seguito le proposte formative di Leonardo S.p.a. che DAC Scarl potrà offrire ai soggetti indicati nell'Accordo di collaborazione di cui il presente Allegato è parte integrante.

La proposta si compone di due macroaree:

1. Area A, inerente ai corsi di awareness:
    - Proposta A.1: Security Awareness
    - Proposta A.2: Awareness per dirigenti e quadri
    - Proposta A.3: Cyber Exercise "Crisis Simulation"
2. Area B, inerente ai corsi specialistici:
    - Proposta B.1: Corso di introduzione alla Cybersecurity
    - Proposta B.2: Corso di sicurezza amministratori IT
    - Proposta B.2: Corso di Cybersecurity Essentials
    - Proposta B.3: Corso di sviluppo del codice sicuro
    - Proposta B.4: Corso di Crisis Management

Area A: Awareness

Proposta A.1

Security Awareness

Piattaforma di formazione asincrona completa sulla Security Awareness mirata a sensibilizzare i comportamenti dell'utente all'interno dell'azienda.

Il percorso formativo mira ad ottenere:

- la massima efficacia nel trasformare il comportamento dell'utente, mantenendo alta la produttività;
- il coinvolgimento spontaneo dei dipendenti per lingua, cultura e funzione;

Il percorso si rivolge a tutta la platea aziendale

La piattaforma si suddivide in tre percorsi formativi:

1. Awareness: e-learning based program, dove l'utente collegandosi alla piattaforma, parteciperà a sessioni asincrone su tematiche specifiche. I contenuti, rilasciati mensilmente, impegnano il discente per circa 2h complessive (da distribuirsi in maniera autonoma nell'arco del mese).
2. Channel: web-series based program, dove l'utente accedendo alla piattaforma, fruisce di video-pillola formativi della durata circa di 5 min ciascuno che sfruttando la forza della narrazione e della produzione video, incrementano la sensibilizzazione ai rischi cibernetici e al corretto comportamento all'interno dell'azienda.
3. Phishing: adaptive anti-phishing training, dove l'utente, in base alle reazioni comportamentali richieste nelle mail di phishing, determina il proprio programma di addestramento esperienziale automatizzato e adattivo. Grazie a un motore di Machine Learning completamente automatizzato, la formazione raggiunge la sua massima efficienza.

I tre percorsi (pillar) possono essere attivati anche separatamente. L'utente ha a disposizione una dashboard personalizzata e il coordinamento di progetto dispone di un reporting avanzato per il monitoraggio dell'andamento del programma formativo singolo e collettivo.

Proposta A.2

Awareness per dirigenti e quadri

L'obiettivo di questo corso è quello di incrementare il livello di consapevolezza delle figure apicali in materia di Cyber Security.

Il corso si rivolge ai manager e ai dirigenti delle varie aziende e ha una durata totale di 3h, in aula fisica o virtuale con docente.

I contenuti del corso sono i seguenti:

- La sicurezza informatica come problema personale
  - Non siamo "adatti" alle tecnologie dell'informazione
  - Un mondo molto piccolo: i gradi di separazione
  - Siamo merce: l'informazione è denaro, il denaro è informazione
  - I social
- Il lato oscuro della Rete
  - Navigare in superficie: i motori di ricerca e i social network
  - Il deep web: profondo ma non troppo
  - Il dark web: i bassifondi della Rete
- La navigazione sicura sul WEB
  - Drive by download
  - Typosquatting
  - Clickjacking
  - Plug in
  - Watering hole
- Gestire le e-mail in sicurezza
  - Il mittente
  - L'oggetto
  - Il testo
  - Allegati e link
- Cosa è e come proteggersi dal social engineering
- Non sono chi pensi
- Fidarsi e bene, ma...
- Malware e Virus. Se lo consoci lo eviti
- Ransomware
- Backdoor e trojan
- IoT
- Piccole cose
- Grandi cose

Proposta A.3

Cyber Exercise "Crisis Simulation"

Il progetto prevede un'esercitazione "table top" in team (composti generalmente da 3 o 6 persone) in cui viene simulato un incidente cyber interno ad un'organizzazione che si trasforma ben presto in un evento di rilevanza nazionale.

L'obiettivo è quello di migliorare le proprie capacità di gestioni di crisi cyber e sensibilizzare le prime linee dell'azienda sui rischi inerente ad un incidente di natura cibernetica.

Il progetto è rivolto a figure manageriali che hanno potere decisionale all'interno di un'azienda, un ente pubblico o un'infrastruttura critica

Struttura della simulazione
I vari team avranno il ruolo del comitato di gestione della crisi e dovranno rispondere a una serie di domande connesse ad ogni scenario e fornire di conseguenza indicazioni sulle modalità di gestione degli eventi

Contenuti
Il progetto prevede la realizzazione di una sessione di simulazione di un evento di crisi cibernetica in modalità Passive Role Play. La simulazione avverrà in data e luogo da definire secondo le necessità del cliente. Durante la simulazione professionisti del settore simuleranno la gestione di un incidente di natura cibernetica, da parte di un Comitato di Crisi di una società di fantasia riferibile a una infrastruttura critica nazionale.
Durante la simulazione verranno forniti spunti narrativi e interpretativi utili a guidare l'audience durante la simulazione che prevede diversi livelli, da quelli interattivi con domane a quelli pratici di stesure di comunicazioni interne ed esterne.
Al termine della simulazione è prevista una sessione di Q&A aperta al pubblico in sala.

Area B: corsi specialistici

Proposta B.1

Corso di introduzione alla Cybersecurity

Questo è il corso ideale per formarsi, nel minor tempo possibile, una base sul tema della cybersecurity. Vengono chiariti i termini, gli scenari attuali e quelli del prossimo futuro, e si entra nel merito dei principali aspetti tecnici, con la possibilità di cimentarsi con alcune semplici tecniche di attacco. Consigliato a chiunque voglia frequentare con profitto qualsiasi altro corso fondativo di Leonardo Training Center.

Il corso si rivolge a chiunque abbia intenzione di intraprendere un percorso formativo nelle professioni della cybersecurity e della sicurezza delle informazioni. Per frequentare con profitto non sono richieste competenze specifiche, ma solo esperienza da utente di computer e smartphone e competenze logiche e matematiche a livello di liceo o istituto tecnico.

Il corso ha una durata di 2 giorni ed è suddiviso in due parti, la prima parte teorica e la seconda pratica.
I contenuti sono i seguenti:

Parte teorica:

- Definizioni: cybersecurity, information security, privacy, Infosec/Comsec ecc.
- L'importanza delle informazioni in quanto asset intangibile, Riservatezza/Integrità/Disponibilità, rischio, cenni alla ISO 27001
- Che cosa è e come sta evolvendo il cyberspazio: non solo social, e-mail e World Wide Web, ma sempre più warfare, IoT, infrastrutture critiche e intelligenza artificiale
- Chi è il nemico, dal mito dell'hacker alla realtà: criminalità organizzata, minacce statuali, sproporzione tra attacco e difesa
- Come ci difendiamo: dalla tradizionale difesa perimetrale ai nuovi modelli di architettura tecnologica, vulnerabilità, information sharing
- Il fattore umano come anello debole: social engineering, gestione delle password
- Riepilogo dei principi generali su cui si basa la sicurezza informatica e dell'informazione

Dimostrazioni pratiche ed esercitazioni su ambiente di laboratorio (basato su Debian Linux):

- Sicurezza del sistema: utenti, gruppi, filesystem, processi, permessi di accesso, password, path e variabili di ambiente, SUID bit
- Crittografia: introduzione teorica su cifratura a chiave simmetrica e asimmetrica, hash, firma digitale, Certification Authority e PKI, applicazioni, man-in-the-middle; password cracking con John the Ripper
- Sviluppo sicuro del software: compilazione di un programma in C, buffer overflow; programmazione web con PHP, architettura 3-tier, codice server-side e client-side, cookies, MariaDB, dimostrazione di attacco SQL Injection
- Ricognizione: network discovery e port scanning con nmap, scoperta delle vulnerabilità di un servizio usando telnet e MITRE, ricognizione da fonti aperte con whois e dig
- Network security: introduzione teorica ai protocolli di rete, sniffing del traffico e delle password con tcpdump

Proposta B.2

Corso di sicurezza amministratori IT

L'obiettivo del corso è quello di acquisire le competenze di gestione della sicurezza endpoint, incrementare le conoscenze del lifecycle management per sistemi operativi e gestire la sicurezza perimetrale, sistemi di monitoring e sistemi SIEM.

La durata del corso è di 5 giorni in aula virtuale e/o fisica con docente.

Il corso è rivolto a chi ha esperienza di amministrazione di sistemi Microsoft e Linux e chi comprende a pieno i concetti di base di rete sicurezza informatica.

I contenuti del corso sono i seguenti:

- Security Management EndPoint
  - Gestione Device
  - Enrollment di un dispositivo
  - Device Configuration Policy
  - Device Compliance Policy
  - Distribuzione di applicazioni
  - App Configuration Policy
- Vulnerability assessment
  - Definizione di vulnerabilità, attacchi, attori di minaccia, conseguenze, valore e rischio Aspetti legali e cenni normativi
  - Vulnerability assessment vs Penetration test o Metodologie di vulnerability assessment e risk scoring
  - Fasi del vulnerability assessment
- Lifecycle management per sistemi operativi e applicazioni G
- Gestione firewall e sicurezza perimetrale
  - Traffic Policy
  - VLAN
  - VPN
  - IDS
  - Analisi del traffico e Log Company General Use o Impostazione di Alert
- In ottica SIEM, impostazione di Alert al verificarsi di eventi specifici
  - Sistemi di monitoring e log management
  - Installazione di server, interfaccia web ed agent
  - Data collection (host, agent, log, snmp, ...)
  - Data visualization (grafici semplici, personalizzati, screens, slide show, network map)
  - Problem detection (trigger)
  - Gestione di eventi, notifiche ed escalation
  - Business level monitoring – IT Services, SLA, reports
  - Backup
- Sistemi SIEM e data correlation
  - Indagine su un reato innescato da eventi
  - Utilizzo dell'indice della gerarchia di rete e della gestione dei dati aggregati
  - Analizzare un attacco su larga scala nel mondo reale
  - Descrivere lo scopo della gerarchia di rete

Proposta B.3

Corso di Cybersecurity Essentials

Il corso copre i concetti e le tecniche essenziali per valutare la sicurezza informatica dei sistemi e per migliorarne la gestione dal punto di vista della sicurezza. Saranno fornite le conoscenze essenziali in tutti i principali ambiti della cybersecurity: dai protocolli di rete ai sistemi di sicurezza, dalle metodologie più comuni per la valutazione della sicurezza dei sistemi ai meccanismi di sicurezza presenti nei più diffusi sistemi operativi. Per molti degli argomenti trattati sono previste dimostrazioni e laboratori hands-on per mettere in pratica quanto discusso.

Il corso è destinato IT manager, personale IT, auditors e altri professionisti che desiderano acquisire le competenze essenziali nel campo della cybersecurity.

Ha una durata complessiva di 5 giorni in aula virtuale e/o fisica con docente.

I contenuti del corso sono i seguenti:

Architecture Security

- Networking e protocolli
- tcpdump, wireshark, tshark
- Virtualization and cloud
- Wireless networks
- Network security devices

Defense in depth

- Identity and Access Management
- Authentication and Password Security
- Security Frameworks
- Data Loss Prevention

Vulnerability Assessment & Penetration Testing

- Attacks and Malicious Software
- Web Application Security
- Digital Forensics and Incident Response

Cryptography

- Cryptographic Algorithms and Deployment

Windows Fundamentals

- Windows Access Controls
- Security Policies
- Logging and Auditing

Linux Fundamentals

- Linux Security
- Containers

Proposta B.4

Corso di sviluppo del codice sicuro

Il corso offre un'ampia panoramica sulle tecniche di secure coding, esponendo le principali problematiche legate alla messa in sicurezza delle applicazioni e fornendo esempi pratici delle diverse vulnerabilità e contromisure che si possono adottare.

Il corso è destinato a sviluppatori, analisti, programmatori, progettisti di software e IT manager.

Ha una durata complessiva di 5 giorni in aula virtuale e/o fisica con docente.

I contenuti del corso sono i seguenti:

- Introduzione alla scrittura di codice sicuro
  - Introduzione
  - Statistiche sugli scenari di attacco nel mondo IT
- Metodologie per lo sviluppo di codice sicuro
  - Ciclo di vita dello sviluppo di software
  - Analisi dei rischi
  - Threat Modeling
  - La Community OWASP
  - Linee guida per il Secure Coding
  - SAST (Static Application Security Testing) tools
- VAPT (Vulnerability Assessment e Penetration Test) di applicazioni
  - Introduzione al protocollo HTTP
  - OWASP Penetration Testing Guide
  - Tools di ausilio per attività di VAPT
- La Validazione dell'Input
  - Linee guida di Secure Coding per la validazione dell'Input
  - Vulnerabilità da Injection
  - SQL-Injection, Cross-Site Scripting, LFI/RFI, etc
  - Laboratori pratici con applicazioni sviluppate in .NET
- L'Autenticazione delle applicazioni
  - Meccanismi di autenticazione
  - Linee guida per autenticazione e gestione password
  - Attacchi all'autenticazione: attacchi brute force e Man-in-the-middle
- Sicurezza nella gestione delle sessioni
  - Introduzione alla gestione delle sessioni nelle applicazioni web
  - Linee guida per la gestione sicura delle sessioni
  - Attacchi di tipo XSRF (Cross-site Request Forgery)
- Linee guida di Secure Coding per la crittografia
  - Introduzione alla crittografia e linee guida per l'uso della crittografia
  - Algoritmi di Hashing
  - Crittografia Simmetrica e Asimmetrica
  - Crittografia Custom

Proposta B.5

Crisis Management

Questo corso fornirà le basi indispensabili per una corretta gestione della crisi secondo le migliori pratiche. Tutte le organizzazioni devono essere pronte a gestire correttamente l'operatività in condizioni eccezionali, sia in caso di incidenti di cybersecurity, come i tentativi di attacco cibernetico, defacement del sito web, attacchi di denial service e fuga di informazioni, sia in caso di disastri naturali o provocati dall'uomo. Questo corso fonirà tutte le competenze specifiche necessarie.

Il corso è destinato a Information Security Manager, CISO e tutto il personale che ha responsabilità nella gestione della continuità operativa.

Ha una durata complessiva di 3 giorni in aula virtuale e/o fisica con docente.

I contenuti del corso sono i seguenti:

- Introduzione al Contingency Planning e terminologia
- Processo di reazione agli incidenti: come si risponde a eventi anomali
- Disaster Recovery: come ripristinare le attività dopo le interruzioni
- Business Continuity: cosa serve per assicurare la continuità operativa e come le aziende assicurano tale continuità anche in caso di eventi disastrosi
- Esercitazione