Cyber Security Journey

Attività di formazione e affiancamento

Fòrema – UNIS&F – Punto Confindustria

Alberto Mercurio

La nostra chiave di lettura

Affiancare l'azienda facendo **sviluppare le competenze per procedere poi in autonomia.** Di fatto il personale aziendale sarà coinvolto con modalità di **training e simulazione**, per fare esperienza di come condurre determinate analisi, sulla base di framework riconosciuti a livello internazionale.

CLUB BIT

Seguendo le buone pratiche di

Clusit
Associazione Italiana per la Sicurezza Informatica

Art. 24

Schema di decreto legislativo recante recepimento della direttiva (UE) 2022/2555 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva UE 2016/1148

2. Le misure di cui al comma 1 sono basate su un approccio multi-rischio, volto a proteggere i sistemi informativi e di rete nonché il loro ambiente fisico da incidenti, e comprendono almeno i seguenti elementi:
   - *a)* politiche di analisi dei rischi e di sicurezza dei sistemi informativi e di rete;
   - *b)* gestione degli incidenti, ivi incluse le procedure e gli strumenti per eseguire le notifiche di cui agli articoli 25 e 26;
   - *c)* continuità operativa, ivi inclusa la gestione di backup, il ripristino in caso di disastro, ove applicabile, e gestione delle crisi;
   - *d)* sicurezza della catena di approvvigionamento, ivi compresi gli aspetti relativi alla sicurezza riguardanti i rapporti tra ciascun soggetto e i suoi diretti fornitori o fornitori di servizi;
   - *e)* sicurezza dell'acquisizione, dello sviluppo e della manutenzione dei sistemi informativi e di rete, ivi comprese la gestione e la divulgazione delle vulnerabilità;
   - *f)* politiche e procedure per valutare l'efficacia delle misure di gestione dei rischi per la sicurezza informatica;
   - *g)* pratiche di igiene di base e di formazione in materia di sicurezza informatica;
   - *h)* politiche e procedure relative all'uso della crittografia e, ove opportuno, della cifratura;
   - *i)* sicurezza e affidabilità del personale, politiche di controllo dell'accesso e gestione dei beni e degli assetti;
   - *l)* uso di soluzioni di autenticazione a più fattori o di autenticazione continua, di comunicazioni vocali, video e testuali protette, e di sistemi di comunicazione di emergenza protetti da parte del soggetto al proprio interno, ove opportuno.

Le competenze necessarie

- Ethical hacking
- Threat hunting e intelligence
- Compliance ISO 27001 e NIST
- Audit in materia di Information Security
- Security policy writing e governance
- System integration
- Security by design
- Vulnerability management
- Gestione remediation
- Infrastructure assessment

Le 5 domande (in ambito Cyber Security)

1. Consideri il fattore umano?
2. Conosci la tua situazione attuale?
3. Testi con frequenza la tua sicurezza?
4. Vivi la cyber security come un processo continuo?
5. Sei pronto a intervenire rispetto agli incidenti in corso?

- **Domanda bonus: conosci le possibilità di finanziamento?**

ITS – Mario Volpato

https://itsdigitalacademy.com/corsi/cyber-security-specialist/

ITS DIGITAL ACADEMY
MARIO VOLPATO

fòrema LEARNING ECOSYSTEM PUNTO CONFINDUSTRIA UNISEF

Executive Master

https://unisef.it/formazione/executive-master-in-cyber-security-ca-ict-f031-24

con il patrocinio di

Clusit Associazione Italiana per la Sicurezza Informatica

CLUB BIT

Formazione awareness e tecnica

- Cyber Security Awareness + simulazione phishing
- Sicurezza OT
- Pensare e agire con gli occhi dell'hacker
- Cyber Security e continuità operativa
- Backup a prova di incidente
- Glossario degli strumenti per la cyber security
- Anatomia di un attacco sociale
- Impatto della direttiva NIS2
- Gestione della crisi aziendale al tempo della cyber security
- Ma anche: Analisi AS IS dell'infrastruttura e dei processi IT con simulazione teorica di blocco dell'operatività, GAP dalla 27001, Addestarmento per la compilazione guidata del questionario assicurativo in ottica di protezione cyber, Business Continuity, Crisis Management.

Cyber Security Assessment e road to NIS2

Delinare un perimetro di rischio generale dell'azienda
e tracciare una roadmap di miglioramento

→ *Cyber Security Risk Assessment (es: Road to NIS2)*

Cyber Security Test

Garantire la sicurezza dell'infrastruttura IT,
capire le vulnerabilità dei sistemi e porvi rimedio

- → *Vulnerability Assessment / Vulnerability Management*
- → *Red Team / Penetration Test*
- → *Infrastructure Assessment: Security By Design, Security Hardening*

Cyber Security Governance e Policies

Creare un sistema di gestione della Cyber Security

- → *Security Policies & Procedures*
- → *Benchmark e progettazione soluzioni*
- → *Advisory per CISO*

Cyber Security Management

Gestire gli incidenti e le minacce in corso

- → *Incident Response*
- → *Threat Hunting*

Grazie!

0422916481
informatica@unisef.it