D.THINKS
DIGITAL THINKS A DGS COMPANY

Security Education

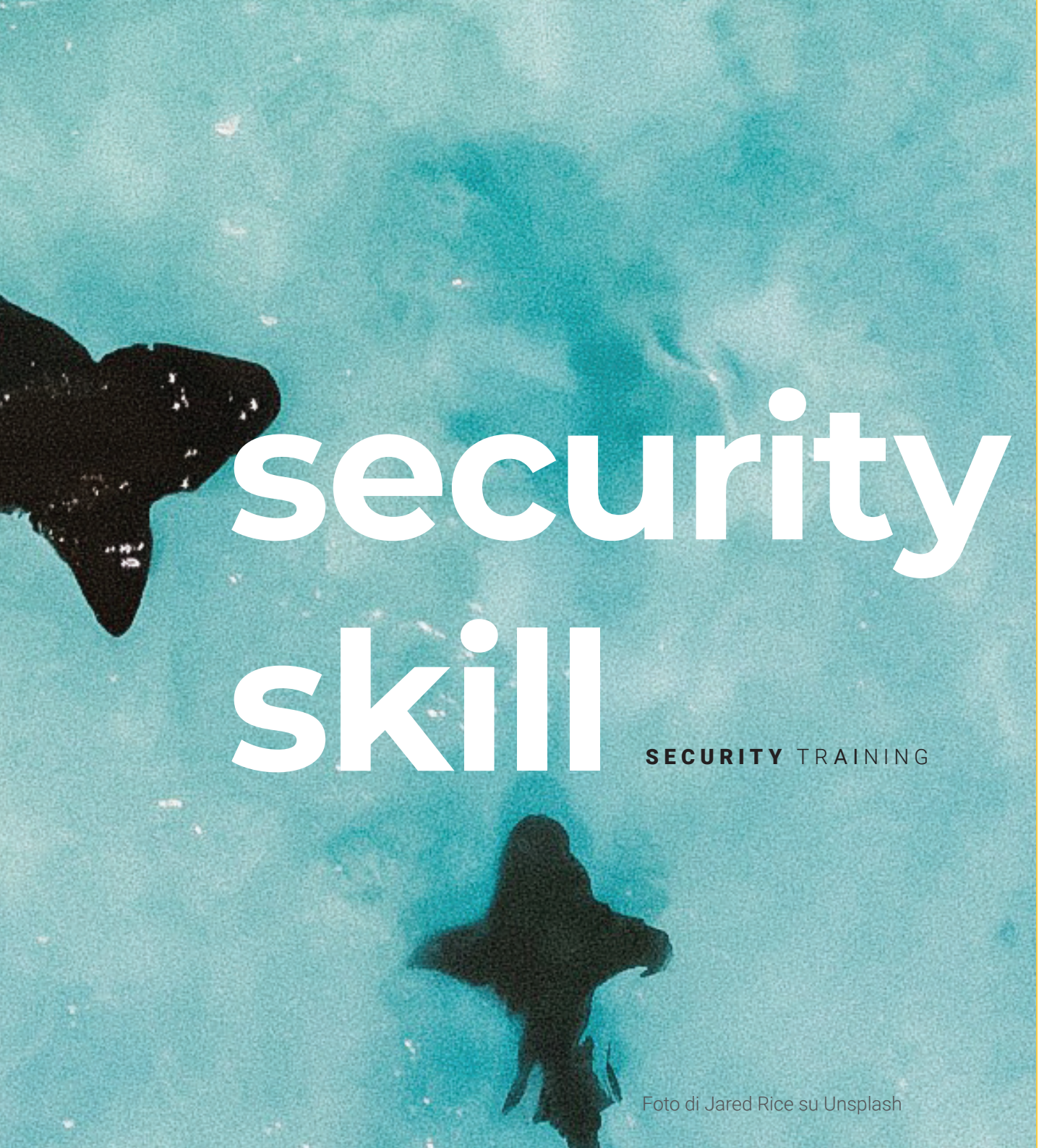


Foto di Jared Rice su Unsplash

CYBERSECURITY, TECNOLOGIA EMERGENTE E RISCHIO SISTEMICO

A meno che non si intervenga ora, entro il 2025 la **tecnologia di prossima generazione**, su cui il mondo farà sempre più affidamento, **ha il potenziale per sopraffare le difese della comunità della sicurezza globale**. La sicurezza informatica avanzata è l'unico mezzo con cui questa sfida può essere affrontata, ma l'approccio alla sicurezza informatica deve essere rivisto prima che il settore si trovi in uno stato idoneo ad affrontare la minaccia.

WEF - Future Series: Cybersecurity, tecnologia emergente e rischio sistemico.

Digital Thinks è Accredited Training Partner EC-Council.
EC-Council è un leader globale nei programmi di certificazione InfoSec Cyber Security, Certified Ethical Hacker e Computer Hacking Forensic Investigator.

Cybersecurity

LA FORMAZIONE COME STRUMENTO PER AFFRONTARE IL CYBER RISK

Uno strumento sottovalutato a disposizione di tutte le aziende è sicuramente la **formazione**, che non si limita ad accrescere le competenze delle singole risorse ma che è **necessaria per creare un know how fondamentale a tutti livelli aziendali**.

È infatti indispensabile sia un maggior livello di consapevolezza dei rischi da parte di tutti gli utenti, sia la capacità di affrontare i rischi a livello tecnico e a livello manageriale.

Sono tre le aree che ogni azienda deve presidiare con risorse adeguatamente formate:

1 SECURITY AWARENESS

- aiuta a raggiungere una **maggiore consapevolezza** dei rischi informatici e ha lo scopo di **sviliuppare le competenze essenziali**, le tecniche e i metodi per prevenire il più possibile gli incidenti di sicurezza e reagire al meglio a fronte di eventuali problemi.

2 SECURITY IT

- l'avvento continuo di **nuove tecnologie** richiede un costante **aggiornamento** delle **competenze** tecniche. Il proliferare di nuove minacce ha creato una domanda sempre più alta di professionisti della sicurezza informatica, aprendo le porte a una vasta gamma di **ruoli specializzati**.

3 SECURITY COMPLIANCE

- il rischio informatico non è più solo una questione tecnica, negli ultimi anni sono state messe a punto numerose **leggi**, **regolamenti** e **standard di cybersecurity da rispettare** (NIS2, ISO 27000, NIST, GDPR ecc.) e che è necessario comprendere e padroneggiare.

Hacking & Security

CODICE	TITOLO	GG	PREZZO
DT0100	Certified Ethical Hacker (CEH)	5	3.390,00
DT0101	Certified Application Security Engineer .NET (CASE)	3	2.100,00
DT0102	Certified Hacking Forensic Investigator (CHFI)	5	3.500,00
DT0103	Certified Incident Handler (CIH)	3	2.100,00
DT0104	Certified Network Defender (CND)	5	3.500,00
DT0105	Certified Secure Computer User (CSCU)	2	1.400,00
DT0107	Certified SOC Analyst (CSA)	3	2.100,00
DT0108	Certified Threat Intelligence Analyst (CTIA)	3	2.100,00
DT0109	Disaster Recovery Professional (EDRP)	5	3.500,00
DT0184	Certified Chief Information Security Officer (CCISO)	5	3.500,00
DT0228	Certified Cybersecurity Technician (CCT)	5	3.500,00
DT0244	ICS-SCADA Cybersecurity	3	2.100,00

CODICE	TITOLO	ORE	PREZZO
DT0207	Network Defense Essentials (NDE)	14	Materiale del corso e video free. Lab e Voucher esame a pagamento.
DT0208	Ethical Hacking Essentials (EHE)	15	
DT0209	Digital Forensics Essentials (DFE)	11	

ESAME INCLUSO: la quota di iscrizione include il voucher per sostenere l'esame di certificazione

CEH | **CERTIFIED ETHICAL HACKER**

Professionisti della sicurezza

Il Certified Ethical Hacker (CEH) fornisce una comprensione approfondita delle fasi di hacking etico, dei vari vettori di attacco e delle contromisure preventive.
Giunto alla dodicesima versione, CEH continua ad evolversi con i più recenti sistemi operativi, strumenti, tattiche, exploit e tecnologie

DT0100 | 5 GIORNI | 3.390,00 €

CHFI | **CERTIFIED HACKING FORENSIC INVESTIGATOR**

Professionisti nella computer forensics

Il corso Certified Hacking Forensic Investigator (CHFI) aggiornato, alla versione 11, fornisce ai suoi partecipanti una solida padronanza della digital forensics, presentando un approccio dettagliato e metodologico alla digital forensics e all'analisi delle prove che ruota anche intorno al Dark Web, IoT e Cloud Forensics.

DT0102 | 5 GIORNi | 3.500,00 €

CND | **CERTIFIED NETWORK DEFENDER**

Amministratori della rete

Allo scopo di ottenere le competenze operative nella sicurezza di difesa delle reti, la formazione prepara gli amministratori rete alle ultime tecnologie e pratiche di sicurezza. Il programma Certified Network Defender è stato aggiornato alla versione 3 per dare agli studenti tutte le risorse e conoscenze necessarie per aiutare il Blue Team a difendere gli assets.

DT0104 | 5 GIORNI | 3.500,00 €

CTIA | **CERTIFIED THREAT INTELLIGENCE ANALYST**

Professionista della sicurezza informatica

Il corso Certified Threat Intelligence Analyst (CTIA) aggiornato alla versione 2 si pone l'obiettivo di aiutare gli organismi ad identificare e ridurre i rischi presso un'azienda scoprendo le minacce interne ed esterne finora sconosciute.
Questo corso di 3 giorni, basato sul Job Task Analysis (JTA), insegna in dettaglio una metodologia che ha lo scopo di stabilire una threat intelligence efficace.

DT0108 | 3 GIORNI | 2.100,00 €

CSA | **CERTIFIED SOC ANALYST**

Analisti SOC e aspiranti SOC. Amministratori Rete e Sicurezza

Il programma Certified SOC Analyst (CSA) è il primo passo per entrare a far parte di un Security Operations Center (SOC). Il corso intensivo copre i fondamenti delle operazioni SOC, la gestione e correlazione dei logs, l'implementazione SIEM, il rilevamento avanzato degli incidenti e della risposta agli incidenti. Inoltre, il candidato imparerà a gestire vari processi SOC e collaborerà con i CSIRT.

DT0107 | 3 GIORNI | 2.100,00 €

C|CISO | **CERTIFIED CHIEF INFORMATION SECURITY OFFICE**

Professionisti della sicurezza che vogliono migliorare le competenze manageriali

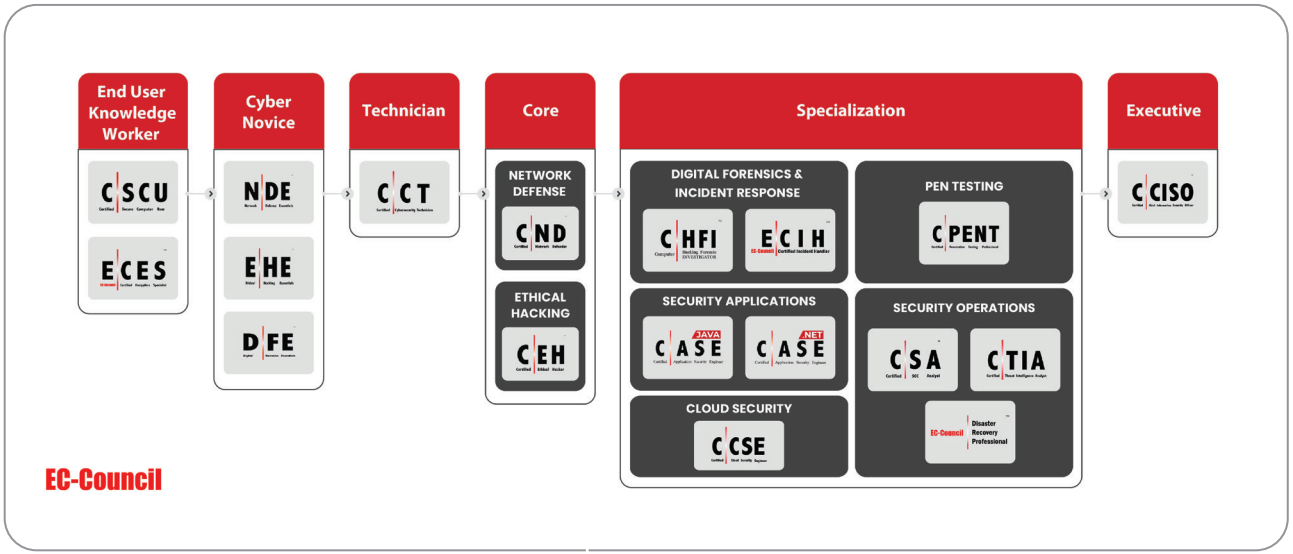
Il programma C|CISO mira a colmare il divario tra le conoscenze di gestione esecutiva di cui hanno bisogno i CISO e le conoscenze tecniche di cui dispongono molti CISO attuali e aspiranti ed è la chiave per una transizione di successo ai livelli più alti della gestione della sicurezza delle informazioni

DT0184 | 5 GIORNI | 3.790,00 €

Mappa delle certificazioni Security

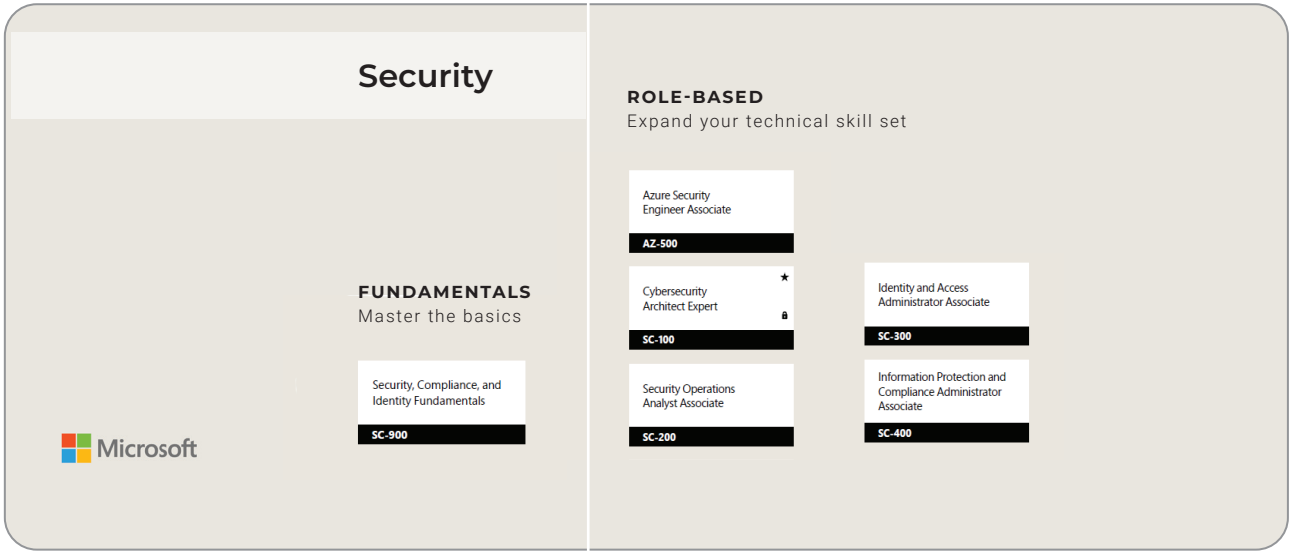
EC-COUNCIL

EC-Council, è il più grande organismo al mondo di certificazione tecnica per la sicurezza informatica, nel corso degli anni ha formato e certificato oltre 200.000 professionisti. Le specializzazioni in ambito cyber security sono oggi tra le più richieste dal mercato del lavoro e le certificazioni EC-Council sono un attestato di competenza riconosciuto. Le certificazioni EC-Council si possono raggruppare su 6 livelli di competenza da End User a Executive con diversi ambiti di specializzazione.



MICROSOFT

Microsoft ha da tempo messo a disposizione delle imprese risorse e soluzioni dedicate alla sicurezza informatica. Per affrontare con successo la sfida della cybersecurity, è cruciale comprendere l'importanza di un approccio completo che includa si strumenenti e soluzioni ma anche risorse in grado di utiizzarli al meglio. La formazione e le certificazioni cybersecutity vanno in questa direzione.



Hacking & Security

#microsoft

CODICE	TITOLO	GG	PREZZO
SC-100T00	Microsoft Cybersecurity Architect	4	1.400,00
SC-200T00	Microsoft Security Operations Analyst	4	1.400,00
SC-300T00	Microsoft Identity and Access Administrator	4	1.400,00
SC-400T00	Administering Information Protection and Compliance in Microsoft 365	3	1.100,00
SC-900T00	Microsoft Security, Compliance, and Identity Fundamentals	1	360,00
AZ-500T00	Microsoft Azure Security Technologies	4	1.400,00

CODICE	TITOLO	GG	PREZZO
DT0047	Cybersecurity nella Pubblica amministrazione e negli enti pubblici	1	400,00
DT0048	Data Breach	1	400,00
DT0049	Direttiva NIS, Cybersecurity Act e Perimetro di sicurezza Nazionale Cibernetico	1	400,00
DT0050	DPO Specialist	4	1.600,00
DT0051	GDPR, normativa Cinese e Americana (CCPA) in materia di Privacy e Cybersecurity	1	400,00
DT0052	General Data Protection Regulation	1	400,00
DT0053	Modelli 231 e sicurezza informatica	1	400,00
DT0210	GDPR e AI: cybersecurity	1	400,00
DT0110	Active Directory: attacco e difesa	3	2.800,00
DT0111	Red Teaming challenge: scenari di attacco dall'esterno	3	2.800,00
DT0112	Cyber Security for executive	2	1.500,00
DT0113	Penetration Testing	5	2.490,00
DT0114	Security by design	3	2.100,00
DT0116	Sicurezza dei dispositivi mobili	1	500,00
DT0117	Sicurezza informatica per utenti	1	400,00
DT0182	Lead Auditor ISO 27001	4	1.950,00
DT0183	Guida alla implementazione della ISO IEC 27001:2013	4	1.950,00
DT0188	Cyber Resilience and deception	1	500,00
DT0189	Quantum Cryptography	1	500,00
DT0191	Malware Analysis	5	2.490,00

Security Awareness

Tra le tecniche di attacco il **phishing** che, nel 2023, rispetto al totale cresce solo di un solo punto percentuale, evidenzia una **crescita dell'87%** in valore assoluto, dimostrando l'efficacia duratura di questa tecnica.

Rapporto Clusit 2024

PHISHING: NEMICO NUMERO UNO

Un attacco di phishing quando colpisce ha una efficacia di ordini di grandezza superiore rispetto agli attacchi massivi e di bassa qualità.
Le campagne di phishing simulato sono lo strumento ideale per andare a misurare in modo rigoroso la permeabilità di una organizzazione al phishing. Rappresentano uno strumento di misura ancora più efficace dell'analisi delle campagne di phishing reali e non solo perché una parte di queste attività illecite resta inosservata falsandone la percezione, ma anche perché nelle campagne simulate si elimina gran parte della variabilità e dell'aleatorietà.

Digital Thinks è in grado di offrire un insieme di servizi per misurare il livello di rischio presente in azienda, fornire misure correttive e verificarne l'efficacia.

1 VULNERABILTA'

CAMPAGNA DI PHISHING SIMULATA

Il modo più semplice per scoprire il livello di vulnerabilità è simulare una campagna di Phishing.

- Creazione di una campagna di Phishing
- Condivisione della campagna con i servizi IT dell'azienda
- Analisi dell'esito
- Redazione di una reportistica dettagliata

2 REMEDIATION

SOLUZIONI

Sulla base del report finale si decidono le azioni da intraprendere per eliminare o ridurre drasticamente le vulnerabilità riscontrate.

- Sensibilizzazione, rendere gli utenti consapevoli delle minacce per migliorare il loro livello di attenzione
- Formazione, con lo scopo di sviluppare le competenze essenziali in tema security

3 VERIFICA

MISURAZIONE EFFICACIA

- A distanza di tempo la ripetizione del primo step con una nuova campagna di phishing e analisi dei risultati consente di verificare il reale livello di comprensione del rischio dei dipendenti e il conseguente livello di rischio a cui è esposta l'azienda.

P.zza Indro Montanelli, 20
20099 Sesto San Giovanni (MI)

(02) 87 21 132
info@dthinks.it
www.dthinks.it

LinkedIn
Facebook
Instagram
X

D.Thinks

D.THINKS
DIGITAL THINKS A DGS COMPANY

WWW.DTHINKS.IT