Ti sei perso nel cyberspazio?

SEC4U

ti aiuta a trovare la strada

IT'S TIME TO RETHINK THE SECURITY CONCEPT!

è il nostro motto e corrisponde alla nostra visione di security, che deve avere come elemento fondamentale LA PERSONA.

SEC4U è un'azienda italiana attiva nel campo della Cyber Security, dell'Ethical Hacking e dello sviluppo applicativo.

Grazie alle conoscenze del proprio team ed alle soluzioni fornite attraverso i diversi business partner, SEC4U diventa il collaboratore ideale per mettere al sicuro la tua organizzazione e gli asset della stessa. Di seguito ti mostriamo com'è organizzata la nostra azienda.

#CyberSecurity

WHAT WE DO

Gli obiettivi principali della Cyber Security sono mettere in atto misure di prevenzione (con lo scopo di ridurre la possibilità che una determinata minaccia accada) e misure di protezione (che agiscono riducendo la gravità del danno realizzato da una minaccia). Per raggiungere questi obiettivi ci poniamo sotto due diversi punti di osservazione:

"L'attacco migliore è quello che non fa capire dove difendersi. La difesa migliore è quella che non fa capire dove attaccare."

Sun Tzu
L'arte della guerra

RED TEAM

osserviamo il target dal punto di vista dell'attaccante che ha lo scopo di violare i sistemi dell'organizzazione al fine di ottenerne un vantaggio

- Offensive Security
- Vulnerability Assessment
- Penetration Test
- Black Box Testing
- Social Engineering
- Web App Testing
- SCADA/PLC Testing
- Drone Patrol
- Physical Security Testing

BLUE TEAM

osserviamo il target dal punto di vista del difensore, affiancando nelle attività quello che di norma è il reparto IT dell'organizzazione

- Defensive Security
- Infrastructure Protection
- Data Breach PoC
- Early Warning
- ETEL game
- Security Training
- Gap Analysis
- Ransomware Protection
- Incident Response

#CyberSecurity

RED TEAM

"Nell'operazione militare vittoriosa prima ci si assicura la vittoria e poi si dà battaglia. Nell'operazione militare destinata alla sconfitta prima si dà battaglia e poi si cerca la vittoria."

Sun Tzu
L'arte della guerra

Come viene vista la tua organizzazione dagli occhi di un attaccante?

Attraverso le nostre attività di sicurezza offensiva, analizziamo tutti gli aspetti di un'organizzazione:

- Network Infrastructure
- Application Security
- Physical Security Control
- Business Process
- Human Behavior

Quali tipologie di attacco utilizziamo?

Information Gathering: in questa prima fase un cybercriminale sfrutta le briciole che un'organizzazione lascia nel tempo, piccoli brandelli di informazione che se uniti possono creare un dettaglio così importante da poter essere sfruttato da chi vuole violare la sicurezza di un'infrastruttura.

Infrastructure Attack: verifichiamo la superficie di attacco infrastrutturale delle organizzazioni. In questa fase cerchiamo di bypassare gli eventuali controlli posti in essere per arrivare al cuore dell'infrastruttura e dimostrare la violabilità della stessa.

Social Engineering: sfruttiamo alcuni elementi del comportamento umano per violare i sentimenti delle persone e indurle in errore, convincendole a rilasciare informazioni o facendogli compiere azioni che vanno a minare le fondamenta della sicurezza dell'organizzazione.

Physical Access: il presidio degli spazi fisici è fondamentale per la sicurezza di qualsiasi organizzazione. Attraverso diverse attività (Impersonation, Shoulder Surfing, Lockpicking, Drone Patrol) verifichiamo la corretta predisposizione di misure atte a difendere e a limitare l'accesso.

C|EH™
Certified Ethical Hacker

Qual è il nostro obiettivo?

Vogliamo aiutarti a migliorare la postura difensiva della tua organizzazione, dopo averne messo in evidenza i rischi ed i conseguenti possibili impatti sul business.

#CyberSecurity

BLUE TEAM

Security Training
Proponiamo corsi di formazione taylor-made su cybersecurity, programmazione sicura, hardening dei sistemi. Organizziamo campagne di awareness con contenuti esclusivi che assicurano un elevato ritorno formativo.

Gap Analysis
Individuiamo il livello attuale di rischio presente, basandoci sulle linee guida CIS Controls sviluppate dal SANS Institute.

Data Breach PoC
I nostri analisti sono costantemente alla ricerca di eventuali data breach rilasciati in rete e sono in grado di fornire una Proof of Concept (PoC) del grado di esposizione della propria organizzazione.

"Il meglio del meglio non è vincere cento battaglie su cento bensì sottomettere il nemico senza combattere."

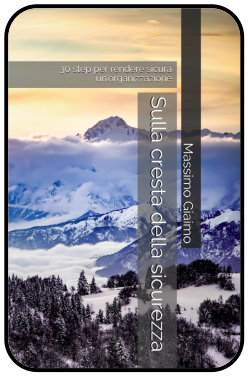
Sun Tzu
L'arte della guerra

ETEL - Exploiting The Eight Layer ®
Abbiamo sviluppato un gioco di ruolo innovativo, che consente di aumentare la consapevolezza riguardo agli elementi di ingegneria sociale utilizzati negli attacchi informatici.

Ransomware Protection
Preveniamo la diffusione del malware attraverso un'attenta progettazione dell'architettura di rete. Possiamo proporre le migliori soluzioni presenti sul mercato per la protezione da virus e malware.

Security Coaching
Attraverso incontri face-to-face periodici affianchiamo l'IT manager o chi all'interno dell'organizzazione si occupa di security, aiutandolo ad individuare nel tempo le migliori strategie e modalità di gestione della sicurezza.

Early Warning
A fronte delle tecnologie utilizzate forniamo evidenza, nel continuo, della scoperta di nuove vulnerabilità e di exploit volti a sfruttarle.



CONTACT US:

team@sec4u.co
+39 0464 350495
Progetto Manifattura
Piazza Manifattura, 1 38068 Rovereto (TN)

VISIT US:

www.sec4u.co
facebook.com/sec4uco
twitter.com/sec4u_team
linkedin.com/company/sec4ucompany