SCHEDA CORSO

CND – CERTIFIED NETWORK DEFENDER v2

Descrizione

Corso tecnico-pratico ufficiale EC-Council di certificazione **Certified Network Defender** (**CND v.2**), fornisce le competenze per progettare politiche di sicurezza della rete e piani di risposta agli attacchi, grazie all'analisi e alla scansione delle vulnerabilità svolte mediante l'applicazione di controlli di sicurezza delle reti, dei protocolli, dei dispositivi perimetrali, di IDS sicuri e la configurazione di VPN e firewall.

Nella campagna "***EC-Council Network Security and Defence Global Training and Certification Initiative***", ITHUM è riconosciuta da EC COUNCIL come **CND Ambassador** per il territorio italiano!

Obiettivi

- Fornire ai professionisti IT le competenze necessarie a svolgere un ruolo attivo nella protezione delle risorse aziendali digitali e nell'individuare e reagire alle minacce informatiche, sfruttando la Threat Intelligence per prevederle prima che si verifichino con approccio "Blue Team Security Professional":
  - Protect
    - Defense-In-Depth Security
    - Properly Designed, Implemented and Enforced Security Policies
    - Security Architectures
    - Appropriate Configuration
    - Right Selection of Security Controls
  - Detect
    - Traffic Monitoring
    - Log Management
    - Log Monitoring
    - Anomalies Detection
  - Respond
    - Incident Response
    - Forensics Investigation
    - Business Continuity (BC)
    - Disaster Recovery (DR)
  - Predict
    - Risk and Vulnerability Assessment
    - Attack Surface Analysis
    - Threat Intelligence

Vantaggi

- Basato su framework di Common Job Role riconosciuti da organizzazioni di tutto il mondo
- Mappato al framework NICE 2.0
- Si concentra sulle ultime tecnologie tra cui cloud, IoT, virtualizzazione e minacce per i lavoratori remoti, analisi della superficie di attacco, intelligence sulle minacce, reti definite da software (SDN) e virtualizzazione delle funzioni di rete (NFV), nonché docker, Kubernetes e sicurezza dei container
- Copre gli strumenti, le tecniche e le metodologie più recenti utilizzate dai migliori esperti di sicurezza informatica in tutto il mondo
- Programma di certificazione accreditato ANSI / ISO/IEC 17024
- Ha vari accreditamenti e riconoscimenti, come: ANSI, GCHQ, NICF, DoD, etc.

Programma di dettaglio

- Network Attacks and Defense Strategies
- Administrative Network Security
- Technical Network Security
- Network Perimeter Security
- Endpoint Security-Windows Systems
- Endpoint Security-Linux Systems
- Endpoint Security- Mobile Devices
- Endpoint Security-IoT Devices
- Administrative Application Security
- Data Security
- Enterprise Virtual Network Security
- Enterprise Cloud Network Security

CND – CERTIFIED NETWORK DEFENDER v2	
	• Enterprise Wireless Network Security • Network Traffic Monitoring and Analysis • Network Logs Monitoring and Analysis • Incident Response and Forensic Investigation • Business Continuity and Disaster Recovery • Risk Anticipation with Risk Management • Threat Assessment with Attack Surface Analysis • Threat Prediction with Cyber Threat Intelligence
Destinatari	Network Administrators, IT Administrators, Network Engineers, Data Analysts, Network Technicians, etc.
Pre-requisiti	Conoscenza: • base in Cyber Security, Forensic Investigation e Incident Management • Inglese tecnico scritto (il corso è tenuto in italiano, materiali didattici ed esami sono in lingua inglese)
Durata e frequenza	Corso della durata di 5+1 giornate (ciascuna tra le 9:00 e le 18:00, comprese pause). La sesta giornata è offerta come ripasso complessivo e preparazione all'esame di certificazione. L'esame di certificazione si tiene in una giornata a parte. *Assenze superiori alle 4 ore consecutive pregiudicano le competenze acquisite e possono compromettere il risultato dell'esame finale.* *Si raccomanda di prevedere del tempo individuale aggiuntivo per consolidare l'apprendimento (attività individuali post-aula, riguardare o completare le esercitazioni e riesaminare la documentazione).*
Modalità di partecipazione	• In presenza in aula con docente • (eccezionalmente) In Virtual Classroom: in web-conference connessi in tempo reale dal proprio dispositivo con il docente e gli altri allievi • In ASA (Autoformazione Specialistica Assistita): autoformazione con incontri individuali con il docente • In aula remota: con gruppi di allievi distribuiti, live, su più aule fisiche, connesse in web-conference tra loro e con il docente • In e-learning: autoformazione con accesso individuale autenticato ai materiali interattivi *È anche possibile alternare le precedenti modalità*
Profilo Docenti	Docenti, consulenti e formatori ICT esperti e specializzati sui Sistemi Informatici, certificati CND e abilitati come Certified EC-Council Instructor (CEI). *Competenze e certificazioni dei docenti possono essere verificate prima dell'inizio del corso, a garanzia del valore aggiunto e del livello qualitativo dei contenuti.*
Metodologia	Per raggiungere alti livelli di apprendimento, vengono integrate diverse metodologie didattiche, in aggiunta alla programmazione, alla qualità dei materiali didattici, e alla professionalità dei docenti: • Learning by doing: imparare facendo. È la metodologia principalmente utilizzata per i corsi abilitanti, integrata dall'uso di supporti didattici di varia natura e dal coinvolgimento immediato dei discenti • Learning Experience: acquisire competenze pratiche attraverso le attività tecnico pratico e l'esperienza sul campo dei formatoti • Participatory Learning: massimizzare l'apprendimento attraverso la partecipazione attiva, l'interazione con i colleghi, i lavori di gruppo, le attività collaborative Le metodologie includono: • Lezioni frontali interattive con i docenti • Alternanza di sessioni teoriche e pratiche • Materiali didattici (ufficiali EC-Council) di elevata qualità; in inglese, accessibile h24 per 2 anni • Laboratori remoti (ufficiali EC-Council) disponibili h24 per 6 mesi

CND – CERTIFIED NETWORK DEFENDER v2	
	• Piattaforme e-learning accessibili anche fuori orario di lezione • Studio di situazioni e casi reali • Momenti di knowledge sharing • Monitoraggio dell'apprendimento • Coaching, Mentoring, Tutoraggio individuale e d'aula • Profilazione attitudinale e orientamento professionale • Forum e/o chat di discussione tra allievi anche fuori orario di lezione • Questionario di gradimento
Materiali didattici	Distribuiti in formato elettronico, tramite piattaforme e-learning ufficiali EC-Council, con accesso individuale autenticato: • Slide proiettate durante il corso • Dispense • Materiale integrativo • Laboratori ed esercitazioni • Voucher per esame di certificazione CND (attivo 1 anno) *Si raccomanda di organizzarsi per portarsi in aula i materiali didattici o su proprio supporto elettronico (notebook, Tablet, Smartphone).*
Esame di certificazione	Al termine del corso viene rilasciato un voucher d'esame della validità di 1 anno dall'attivazione per sostenere l'esame di certificazione **312-38 – CND – Certified Network Defender**, riconosciuto e accreditato in conformità ANSI 17024. L'esame è composto da 100 domande a risposta multipla ed è della durata di 4 ore. L'esame può essere sostenuto presso la sede ITHUM (Test Center ufficiale) secondo il calendario concordato in fase di iscrizione al corso. È anche possibile sostenere l'esame presso un Test Center Pearson VUE, in presenza oppure via web (con un proctor che segue a distanza), pagando una quota integrativa.
Attestato e Certificazione	• A termine del corso viene rilasciato un attestato di frequenza EC-COUNCIL-ITHUM • Al superamento dell'esame di certificazione, viene generato Attestato di certificazione **312-38 – CND – Certified Network Defender**, riconosciuto e accreditato in conformità ANSI 17024
Allestimento d'aula (Corsi in presenza)	Aule adeguate e confortevoli per svolgere attività didattiche, dotate di: • Accesso a Internet • Sistema di videoproiezione • Lavagna a fogli mobili e/o white-board, con pennarelli colorati • Tavoli e sedie mobili (non sedie con ribaltine o bloccate in configurazioni fisse) • Climatizzazione e areazione adeguata • Raggiungibilità con trasporti pubblici
A cura degli allievi	Notebook personale con accesso amministratore
Numero partecipanti	Fino a 15 allievi per edizione (*per ottimizzare l'efficacia dell'interazione e dell'apprendimento*)
Altri corsi EC-Council	In qualità di partner EC-Council, ITHUM eroga anche i corsi di certificazione, tra cui: • CEH - Certified Ethical Hacker • CHFI - Certified Hacking Forensic Investigator • CSA - Certified SOC Analyst • ECIH - EC-Council Certified Incident Handler • CTIA - Certified Threat Intelligence Analyst • CPENT - Certified Penetration Testing Professional
Informazioni e prenotazioni	• Mail: formazione@ithum.it • Telefono: (+39) 06 2158915

CND – CERTIFIED NETWORK DEFENDER v2	
	• Sito: https://www.ithum.it/formazione/cybersec/ec-council-corsi-e-certificazioni.html