EC-Council Certified Incident Handler v2 (ECIH)

EC-Council Certified Incident Handler v2 (ECIH)

За Курса

This latest iteration of EC-Council's Certified Incident Handler (E|CIH) program has been designed and developed in collaboration with cybersecurity and incident handling and response practitioners across the globe.

It is a comprehensive specialist-level program that imparts knowledge and skills that organizations need to effectively handle post breach consequences by reducing the impact of the incident, from both a financial and a reputational perspective.

Following a rigorous development which included a careful Job Task Analysis (JTA) related to incident handling and incident first responder jobs, EC-Council developed a highly interactive, comprehensive, standards-based, intensive 3-day training program and certification that provides a structured

approach to learning real-world incident handling and response requirements.

Цели – Какво ще научите (Course Goals):

- Understand the key issues plaguing the information security world
- Learn to combat different types of cybersecurity threats, attack vectors, threat actors and their motives
- Learn the fundamentals of incident management including the signs and costs of an incident
- Understand the fundamentals of vulnerability management, threat assessment, risk management, and incident response automation and orchestration
- Master all incident handling and response best practices, standards, cybersecurity frameworks, laws, acts, and regulations
- Decode the various steps involved in planning an incident handling and response program
- Gain an understanding of the fundamentals of computer forensics and forensic readiness
- Comprehend the importance of the first response procedure including evidence collection, packaging, transportation, storing, data acquisition, volatile and static evidence collection, and evidence analysis
- Understand anti-forensics techniques used by attackers to find cybersecurity incident cover-ups
- Apply the right techniques to different types of cybersecurity incidents in a systematic manner including malware incidents, email security incidents, network security incidents, web application security incidents, cloud security incidents, and insider threat-related incidents

---

Формат на курса (Course Format):

[table id=1 /]

Език на курса (Course Language Option)

[table id=2 /]

Може да изберете Език на който да се проведе обучението – български или английски. Всичките ни инструктори владеят свободно английски език.

Учебни Материали (Student Guides):

Учебните материали са достъпни в електронен формат. Могат да се ползват online/offline на всяко устройство. Доживотен достъп.

Лабораторна среда (Lab Environment):

Всеки курсист разполага със собствена лаб среда, където се провеждат упражненията, част от курса. Не е необходимо да инсталирате софтуер на компютър или специални изисквания за хардуер.

Участниците в присъствен формат в Учебния ни център разполагат с индивидуален компютър по време на обучението.

След завършване получавате (At Course Completion):

[table id=3 /]

Доживотен достъп до видео архив с запис на всяка отделна лекция.

Официален международно признат сертификат за завършен курс на обучение.

Продължителност (Course Duration):

- 3 работни дни (понеделник – петък 09:00 – 17:00)

или

- **32 уч.ч. обучение (теория и практика) в извънработно време с продължителност 1 седмици**
- събота и неделя 10:00 – 14:00, 14:00 – 18:00, 18:00 – 22:00
- понеделник и сряда 19:00 – 23:00
- вторник и четвъртък 19:00 – 23:00

Плащане

Заявка за издаване на фактура се приема към момента на записването на съответния курс.

Фактура се издава в рамките на 7 дни от потвърждаване на плащането.

Предстоящи Курсове

[tribe_events_list category="ceh"]

За повече информация използвайте формата за контакт.

Ще се свържем с Вас за потвърждаване на датите.