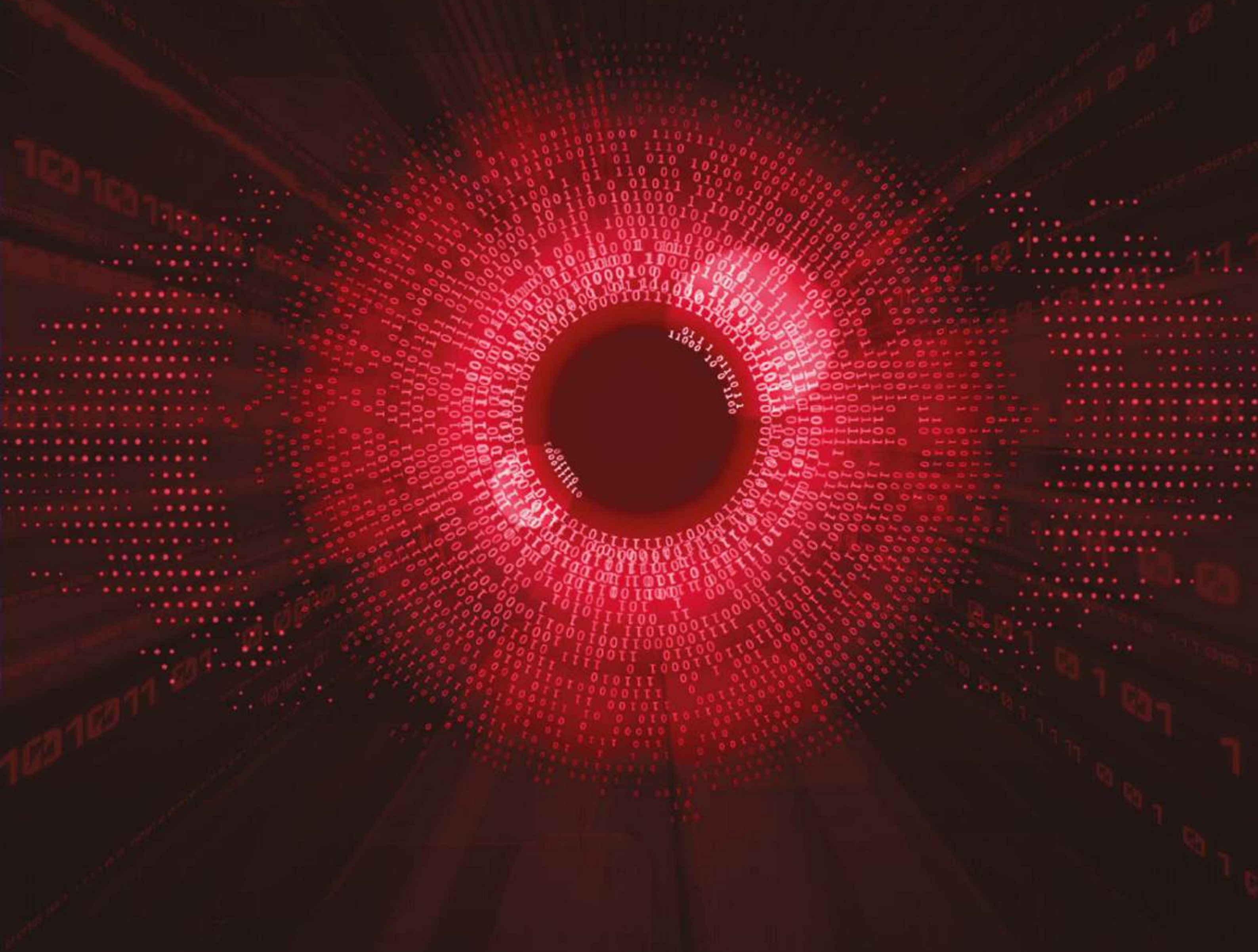
EC-Council



Ethical Hacking as a Career:

THE ULTIMATE GUIDE

(An In-Demand Job Role and Must-Have Cybersecurity Skill)

What Is Ethical Hacking?

Ethical hacking simulates an attack on an organization's networks and systems. Also known as white hat hacking, it is performed to identify vulnerabilities and security gaps before malicious actors can exploit them. Ethical hacking allows companies to see their IT infrastructure from a hacker's perspective to help strengthen the cybersecurity posture and better safeguard their data. Though ethical hackers employ similar tactics and approaches as

What Is the Role of an Ethical Hacker?

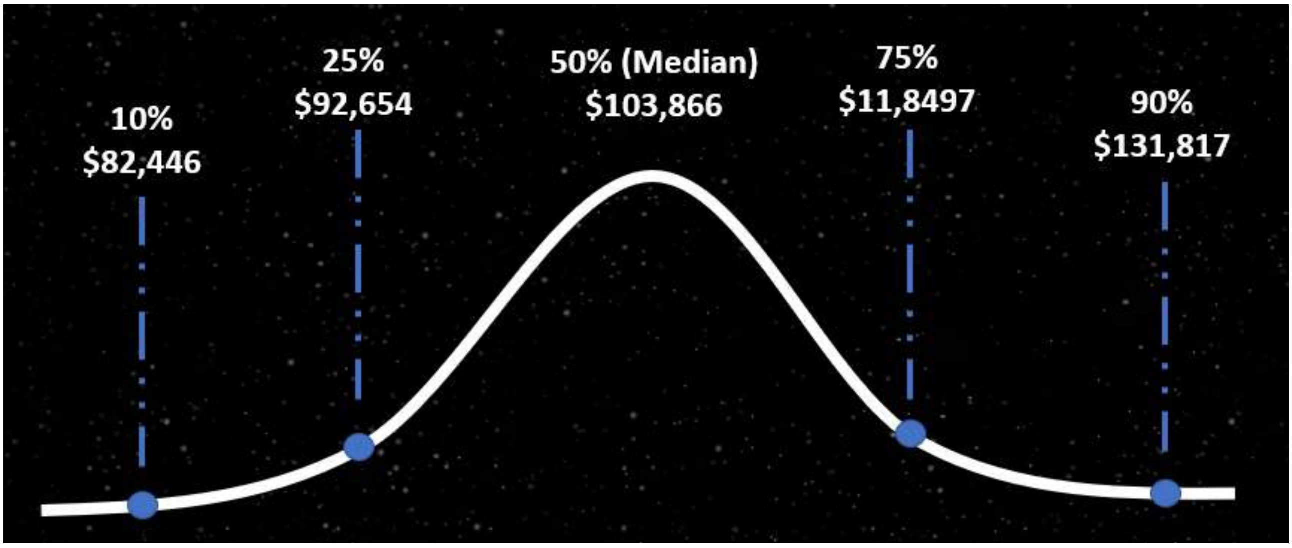
Ethical hackers infiltrate computer devices or networks to assess the effectiveness of security strategies and uncover vulnerabilities and potential threats. Some common vulnerabilities they discover are broken authentication, security misconfigurations, injection attacks, and distributed denial-of-service (DDoS) attacks. Ethical hackers demonstrate how threat actors operate and help organizations prepare for cyberattacks. The information obtained from ethical hacking evaluations enables companies to make informed decisions to manage risks.

Here's a list of some of the responsibilities of ethical hackers:

- Uncovering information about the target via public sites, social media, or by directly interacting with the target
- Scanning for vulnerabilities and weaknesses
- Remediating loopholes and documenting their findings
- Analyzing the existing security solutions and developing countermeasures

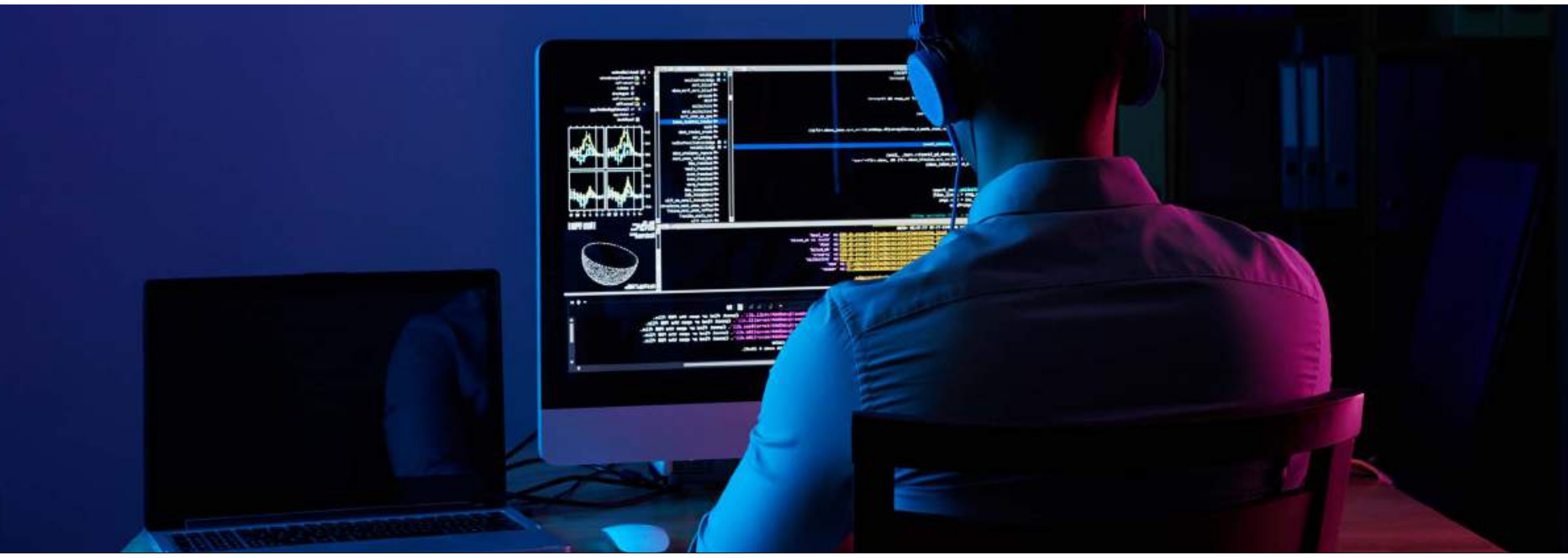
The Average Salary of an Ethical Hacker

The pay scale of an ethical hacker usually ranges between $92,914 and $118,825 in the United States, and the average salary as of July 26, 2022, stands at $104,156. [1]
* Data based on HR-reported survey using national average and geographic differential



Certified Ethical Hacker is Mapped to 20+ Job Roles

- **Mid-Level Information Security Auditor:** Assesses and audits a company's databases and systems to prevent cybertheft and attacks
- **Cybersecurity Auditor:** Audits online security systems and networks
- **Security Administrator:** Monitors network traffic, conducts security audits, and installs security solutions
- **IT Security Administrator:** Oversees and troubleshoots the security issues and solutions of an organization
- **Cyber Defense Analyst:** Monitors network traffic, suspicious activities, and security threats
- **Vulnerability Assessment Analyst:** Identifies flaws in systems and networks to mitigate cyberthreats
- **Warning Analyst:** Gathers, conducts, examines, and reports cyberthreat evaluations
- **Information Security Analyst 1:** Analyzes and inspects organizational security protocols and policies
- **Security Analyst L1:** Conducts network security monitoring and incident response plans; evaluates and records security reports
- **Infosec Security Administrator:** Oversees security protocols to protect organizational infrastructures
- **Network Security Engineer:** Safeguards a company's networks and systems from cyber threats, unauthorized intrusions, and data theft
- **SOC Security Analyst:** Monitors and assesses a company's IT infrastructure, delegates tasks to the team, and reviews cybersecurity processes
- **Security Analyst:** Identifies security-related issues and resolves incidents
- **Network Engineer:** Oversees and maintains the connectivity of networks in wired and wireless network services within an organization
- **Senior Security Consultant:** Formulates security policies and protocols to protect company data and systems
- **Information Security Manager:** Manages IT and IS teams, delegates tasks, and conducts security investigations
- **Senior SOC Analyst:** Part of the SOC team; advises security procedures and offers threat and vulnerability analysis
- **Solution Architect:** Designs roadmaps for security solutions and analyzes security protocols
- **Cybersecurity Consultant:** Assesses clients' cybersecurity infrastructures and security solutions
- **Security Compliance Analyst:** Evaluates security and compliance strategies



Common Job Roles and Average Salaries in the U.S.

Entry-Level Cybersecurity Analyst:	Information Security Analyst:	Cyber Security Engineer:	Security Engineer:
$73,028 [2]	$83,580 [3]	$140,007 [4]	$134,104 [5]
Penetration Tester:	Information Security Manager:	Security Analyst:	Information Security Engineer:
$120,438 [6]	$138,904 [7]	$85,872 [8]	$140,007 [9]
Security Architect, IT:	Information Systems Security Officer:	Chief Information Security Officer:	Network Security Engineer:
$130,193 [10]	$95,473 [11]	$232,090[12]	$93,074 [13]

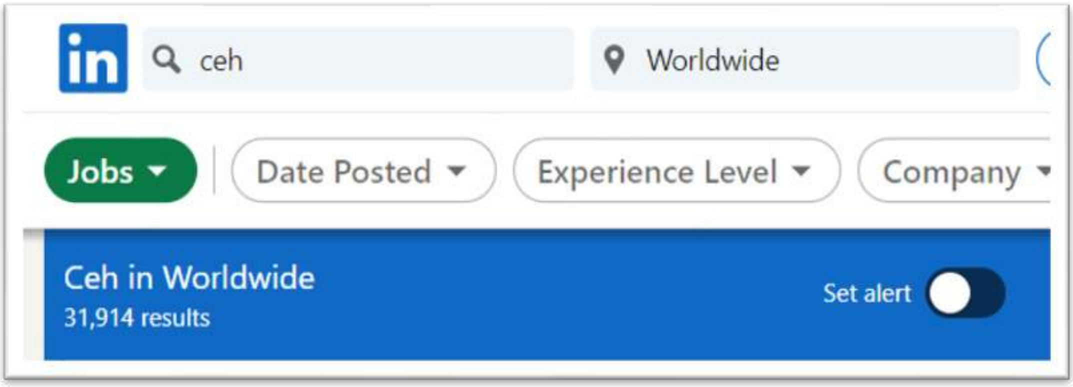
https://www.salary.com/research/salary/posting/entry-level-cyber-security-analyst-salary

Information Security Analyst: Career Outlook

The U.S. Bureau of Labor Statistics revealed that the employment of information security analysts is expected to grow 33% from 2020 to 2030, much faster than average. It was also reported that information security analysts usually need a bachelor's degree in computer science and related work experience. Recruiters prefer to hire analysts who have professional certification. [14]

Job Opportunities

As of Aug 17, 2022, there were 31,626 job openings on LinkedIn. [15]



ceh

Worldwide

Ceh in Worldwide

31,914 results

What Does It Take to Become an Ethical Hacker?

Ethical hackers play an important role in bolstering an organization's security posture. They are subject matter experts with a wide range of computer skills. Before you decide to learn ethical hacking, let's look at some of the technical skills required to become an ethical hacker:

- In-depth knowledge of computer devices and basic computer skills such as data processing
- Awareness of programming languages such as Python, JavaScript, C++, etc.
- Proficiency in computer networks and different network topologies
- Comprehensive knowledge of databases
- Expertise in cryptography
- Knowledge of reverse engineering

Tips to Choose the Right Ethical Hacking Course

Given the huge number of ethical hacking courses in the market today, choosing the right program can be challenging. Here are some tips that can help you pick out the right course:

Research:

Conduct extensive research on the ethical hacking programs you're interested in—narrow your list based on the curriculum, faculty, admission requirements, and budget. Opting for courses that provide hands-on training and industry exposure is always better.

Career Options:

Check the job roles mapped to ethical hacking programs. Make sure that the career options are suited to your interests and goals. Opt for a course that opens the door to multiple job opportunities and helps you advance your career.

Mode of Training:

An on-campus program will not work with the schedule of a working professional. Today, students can pick a flexible learning program to suit their busy schedules. By taking an ethical hacking course online, students can find a way to balance their work and education.

Check for Accreditation:

When selecting an ethical hacking course, look for accreditations and affiliations. A recognized training program will boost your employability and help you stand out.

Why You Should Join EC-Council's Certified Ethical Hacker (C|EH® v12)

The Certified Ethical Hacker (C|EH®) Certification by EC-Council—globally recognized in the industry with 20+ years of experience in cybersecurity training and certification—is the world's no.1 ethical hacking certification. C|EH® v12 is a one-of-a-kind certification that provides comprehensive training in ethical hacking with hands-on training, labs, assessment, mock engagement, and global hacking competitions to ensure that students are at the top of their game.

1. C|EH® Training and Practice (C|EH® Learn)

The C|EH training program includes 20 modules that cover various technologies, tactics, and procedures, providing prospective ethical hackers with the core knowledge they need to thrive in cybersecurity. The concepts covered in the training program are split 50/50 between knowledge-based training and hands-on application through our cyber range. Delivered through a carefully curated training plan that typically spans five days, C|EH continues to evolve to stay up-to-date with the latest operating systems, exploits, tools, and techniques.

2. Exam Based on Real Challenges + Hands-On Approach (C|EH Certify)

The C|EH® exam maintains high integrity and is provided in multiple forms. The questions assess the candidate's capability to apply their technical knowledge to real-world situations. C|EH® (Master), introduced in 2019, is one of the newest additions to the C|EH® v12 program. To achieve the C|EH® (Master) credential, you must pass the C|EH® (MCQ Exam) and the C|EH® (Practical) Assessment. After successfully passing both, you will be awarded the C|EH® (Master) credential.

The C|EH® (MCQ Exam) contains 125 questions with a duration of four hours. Each question bank is assessed via beta testing by a panel of subject matter experts, and each question is rated based on its difficulty level. Passing scores are determined based on the exam form and can range from 60% to 85%.

The C|EH® (Practical) is a six-hour, hands-on live exam that can be taken anytime, anywhere. Designed by subject matter experts in the ethical hacking domain, C|EH® (Practical) tests the candidate's skills and abilities in techniques such as vulnerability detection, SQL injection methodology, cryptography, and wireless encryption against 20 real-life scenarios. A practical exam proctored anywhere in the world will allow organizations to quickly train, test, and deploy their cyber ready workforce.

3. Intensive Lab Practices (C|EH® Engage)

EC-Council labs are hosted online with lab trainers who assist you by providing feedback, enabling you to defend networks and systems against attacks. With 50% of the time dedicated to practical learning, C|EH® provides a hands-on learning experience. The labs provide maximum exposure through the real-time environment comprising the latest hacking techniques, methodologies, tools, and tricks. They are configured with firewalls, domain controllers, and vulnerable web applications that allow you to hone your hacking skills.

4. Competition-Based Learning (C|EH® Compete)

The C|EH® Global Challenges occur every month, providing capture-the-flag style competitions that give students exposure to various new technologies and platforms, from web applications, OT, IoT, SCADA, and ICS systems to cloud and hybrid environments. Our compete structure lets ethical hackers fight their way to the top of the leaderboard each month in these 4-hour curated CTFs. Objective-based flags are designed around the ethical hacking process, keeping skills current, testing critical thinking abilities, and covering the latest vulnerabilities and exploits as they are discovered. Hosted 100% online in EC-Council's Cyber Range, candidates race the clock in scenario-based engagements against fully developed network and application environments with real operating systems, networks, tools, and vulnerabilities to practice, engage, compete, build, and hone their cyber skills against various new target organizations.

5. Mapped to NICE 2.0

The National Initiative for Cybersecurity Education (NICE) framework, led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, aims to address cybersecurity challenges through standards and best practices. C|EH® is mapped to specialty areas under the NICE 2.0 framework's protect and defend job roles. It also overlaps with other job roles, including Analyze (AN) and Securely Provision (SP).

6. Accredited by ANSI

The C|EH® v12 is accredited by the American National Standards Institute (ANSI), a private non-profit certification body that develops standards and technical regulations. It is trusted by Fortune 500 companies such as IBM, Microsoft, Ford, and more. The program is also endorsed by the United States Department of Defense (DoD).

Maintain Sanctity of the Exam

"The biggest issue for CISOs is the need to differentiate candidates with the knowledge, skills, and abilities to do the job, abilities that represent true technical and security challenges faced at the workplace. Many Fortune 500 companies developed creative ways to find and hire those that could do the job, and they've spent millions of dollars and countless amounts of time and management to achieve that. Today, we offer a solution to this problem."

– Jay Bavisi, President and CEO of EC-Council

All EC-Council exams are remotely proctored, which means you can take the exam online from the comfort of your home, proctored by a dedicated EC-Council Proctor certification team. The certification allows candidates to gain real-world experience. The wide number of tools and focus on hands-on learning help individuals become competent. Recruiters across the world recognize C|EH®.

Here's What People Are Saying About the Course

C|EH® was ranked #1 as the best certification in ethical hacking by **ZDNet**. [16]

"C|EHv11 teaches students about today's modern hacking techniques, exploits, emerging cybersecurity trends and attack vectors, and how to use commercial-grade tools to effectively break into systems. Modules also include cyberattack case studies, malware analysis, and hands-on hacking challenges. Hacking challenges are introduced at the end of each module to put theory into practice, pushing learners to apply their new knowledge of attacks to business settings."
– ZDNet

C|EH® was ranked #4 in the top 10 cybersecurity certificates listed for cybersecurity positions. [17]

C|EH® has been among the 10 most popular cybersecurity certifications for 20 years.

C|EH® HALL OF FAME 2021 REPORT FINDINGS

The Impact of C|EH® on Cyber Careers

3500+	**Applicants, 900 Finalists, 100 Awardees, 59 Countries**
70%	**of C|EHs reported a salary increase of more than 20% compared to their peers.**
21%	**of C|EHs reported a salary advantage of at least 40% over their peers.**

Insights from Certified Ethical Hackers

“I led a team of phenomenal cybersecurity and fraud experts to identify a significant threat actor, mitigate the actor’s operations, protect the ecosystem from attacks, and contribute to the takedown of the threat actor’s operations in 2020.”
– **David Capezza**, senior director at Visa Payment Systems Intelligence

“I analyzed a few malware samples related to Covid-19 and then hosted a webinar to show the audience members how to improve their cyber resilience against advanced cyberthreats.”
– **Yinchun Zhou**, Senior Security Consultant at an information management solutions firm

“I have expanded my knowledge of computer hacking and forensics broadly, as a result, I was able to more securely protect my organization infrastructure.”
– **Michael Peters**, CIO at a global risk management organization

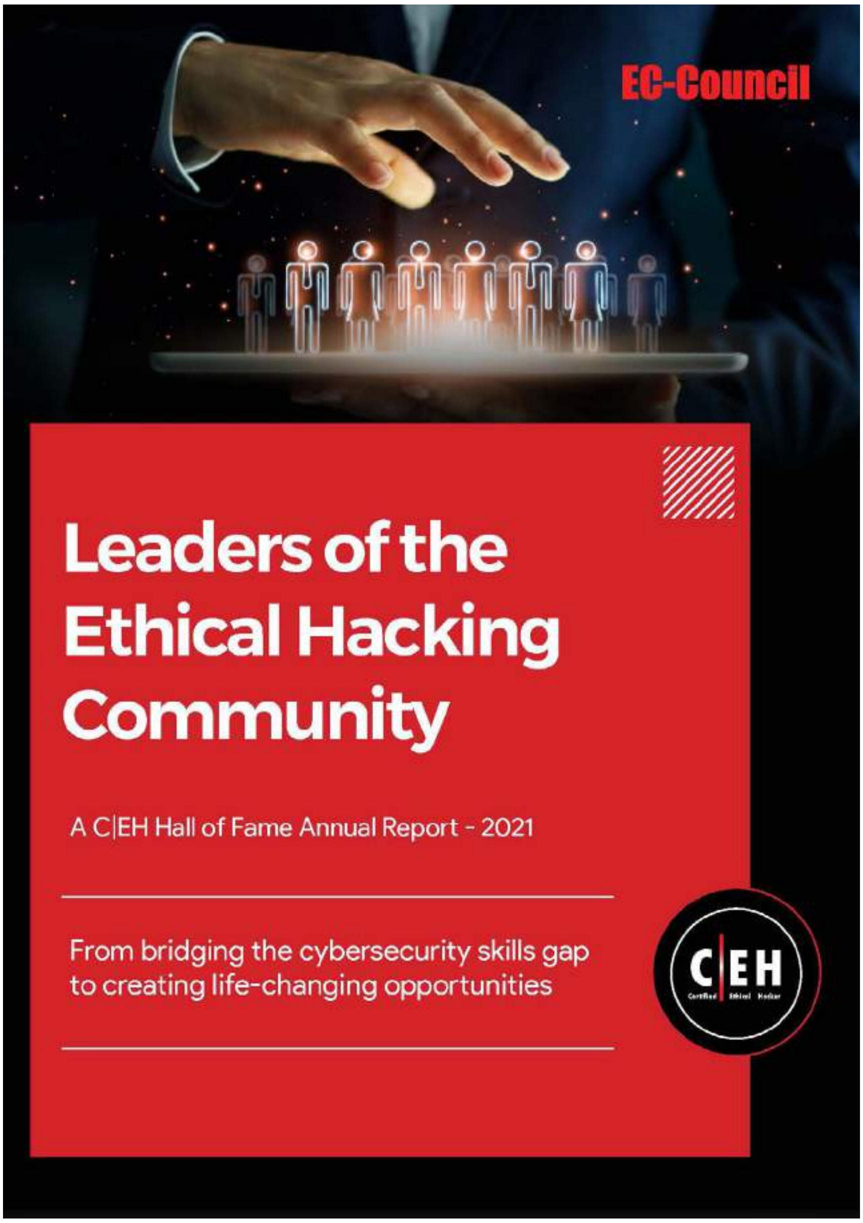
“C|EH® equipped me to direct the recovery from a ransomware incident in just a few hours without making any ransomware payment. I also provided the FBI with forensic data in the form of correlated logs.”
– **Bradley Newberry**, IT administrator for a municipality

“C|EH® certification made my CV outstanding compared to my peers. It has landed me an exciting role at EY.”
– **Sidhant Gupta**, senior security consultant, UK

“I was one of the lucky candidates to get a scholarship for Certified Ethical Hacker (Practical). The ethical hacking certification has certainly benefited me a lot and accelerated my career, as I was recognized and promoted by my organization post the C|EH Hall of Fame achievement.”
– **Fuad Mustapha**, senior cyber security analyst, CTW, Canada

Check out the full report for industry insights, success stories, and learning experiences from C|EH® alumni.

DOWNLOAD REPORT



EC-Council

Leaders of the Ethical Hacking Community

A C|EH Hall of Fame Annual Report - 2021

From bridging the cybersecurity skills gap to creating life-changing opportunities

C|EH

References

[1]https://www.salary.com/research/salary/posting/ethical-hacker-salary
[2]https://www.salary.com/research/salary/posting/entry-level-cyber-security-analyst-salary
[3]https://www.salary.com/research/salary/listing/information-security-analyst-salary
[4]https://www.salary.com/research/salary/listing/cyber-security-engineer-salary
[5]https://www.salary.com/research/salary/recruiting/security-engineer-salary
[6]https://www.indeed.com/career/penetration-tester/salaries
[7]https://www.salary.com/research/salary/benchmark/information-security-manager-salary
[8]https://www.indeed.com/career/security-analyst/salaries
[9]https://www.salary.com/research/salary/listing/information-security-engineer-salary
[10]https://www.payscale.com/research/US/Job=Security_Architect%2C_IT/Salary
[11]https://www.salary.com/research/salary/position/information-systems-security-officer-salary
[12]https://www.salary.com/research/salary/benchmark/chief-information-security-officer-salary
[13]https://www.salary.com/research/salary/listing/network-security-engineer-salary
[14]https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[15]https://www.linkedin.com/jobs/search/?currentJobId=3220349414&geoId=92000000&keywords=C|EH&location=Worldwide&refresh=true
[16]https://www.zdnet.com/education/computers-tech/best-ethical-hacking-certification/
[17]https://www.datamation.com/careers/cybersecurity-certifications

EC-Council

Ethical Hacking as a Career:
THE ULTIMATE GUIDE

www.eccouncil.org