EC-Council
Building A Culture Of Security

THEIR WINNING MOVES

MEET THE *TOP 100 LEADERS* OF *ETHICAL HACKING* COMMUNITY 2025

C|EH
Certified Ethical Hacker

Certified Ethical Hacker Hall of Fame 2025 Industry Report

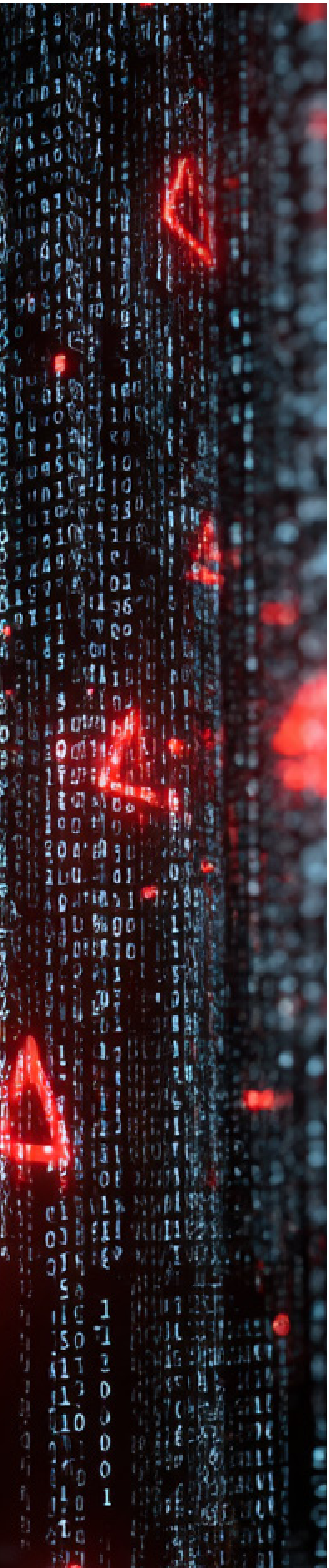


TABLE OF CONTENTS:

Executive Summary:

The Certified Ethical Hacker (C|EH) Hall of Fame 2025 Annual Report offers an in-depth examination of the professional growth journeys, skill applications, and career outcomes of top-performing ethical hackers from EC-Council's global community. Based on responses from 460 respondents, including 100 Hall of Fame inductees, this report presents a data-driven and narrative-rich account of how the C|EH credential empowers cybersecurity professionals to meet the evolving demands of the threat landscape.

This year's report examines the practical impact of the C|EH training on individuals at different stages of career development, from early practitioners to seasoned experts. Drawing from firsthand accounts and questionnaire responses, the report highlights how ethical hackers apply their C|EH knowledge to real-world scenarios, drive innovation in their organizations, and contribute meaningfully to global cyber resilience.

Key Highlights Include:

- First-person accounts of Certified Ethical Hackers Hall of Fame respondents on their career progression
- Statistical analysis of C|EH's influence on promotions, salary growth, and role expansion
- A broader industry outlook on cybersecurity workforce trends and emerging opportunities

With an increasing need for skilled cybersecurity professionals, this report provides essential insights for organizations, hiring managers, and individuals seeking to understand the value of EC-Council's C|EH program. The collective achievements of this year's finalists underscore the role of C|EH not just as a certification, but as a catalyst for career transformation and industry impact. To ground these insights in data, the following section details the rigorous methodology and respondent base behind the report.

DATA SOURCE & METHODOLOGY

The findings presented in the 2025 C|EH Hall of Fame Annual Industry Report are grounded in a robust, data-driven methodology, based on information collated during 2024. This approach is designed to capture the diverse experiences and career trajectories of high-performing ethical hacking professionals worldwide. This report draws upon a comprehensive online survey administered globally to a pool of individuals who achieved a score of 80% or higher on the C|EH certification exam—demonstrating their technical proficiency and a deep understanding of ethical hacking principles and methodologies

To ensure the depth and relevance of the insights, the survey engaged **460 respondents from 93 countries.** From this distinguished global cohort, **100 elite Certified Ethical Hackers were inducted into the Hall of Fame.** Selection was based on a rigorous evaluation process that assessed key criteria, including leadership in ethical hacking, contributions to the cybersecurity community, innovation in threat mitigation, and measurable career progression since certification.

The report synthesizes both quantitative and qualitative data, incorporating statistical trends alongside narratives to offer a multidimensional understanding of how the C|EH **certification shapes cybersecurity careers across regions, industries, and experience levels.** The analysis spans sectors including government, defense, finance, healthcare, and technology, providing a cross-sectional view of certification impact at both individual and organizational levels. To assess the impact of C|EH on salary growth, particularly for respondents who changed job markets internationally, all monetary values were standardized using **Xe.com currency conversion rates** to ensure consistency and comparability.

Where applicable, select numerical values have been rounded up to the nearest whole number in accordance with standard reporting conventions, particularly in cases where decimal values approached the next integer. This approach was adopted to ensure uniformity and clarity in data presentation without compromising interpretive accuracy.

Each insight presented in this report is based on a specific sample size. N denotes the number of respondents for each data point or chart. This figure reflects the total number of individuals who completed the specific question. Please consider the sample size when interpreting the results. While the findings offer valuable directional insights, they may not be representative of the broader population.

By leveraging a highly skilled respondent base, this report delivers credible, evidence-based insights that reflect the global relevance and transformative power of the C|EH certification in advancing ethical hacking capabilities and workforce readiness in today's complex threat landscape.

EC-Council celebrates these professionals' exceptional contributions through the prestigious C|EH Hall of Fame recognition.

Certified Ethical Hacker Hall of Fame 2025 Industry Report

KEY TAKEAWAYS:

100%
say C|EH increased respect and recognition in the workplace.

100%
would recommend C|EH to peers.

99%
say investing in C|EH benefited their career and professional growth.

99%
found virtual labs in C|EH helpful to varying extents for developing real-world ethical hacking skills.

98%
credit C|EH as crucial to their cybersecurity career shift.

97%
say C|EH effectively covered emerging threats and trends

91%
feel C|EH gives them a competitive edge over other certifications.

86%
reported increased job opportunities after C|EH.

86%
credited C|EH with advancing their skills in penetration testing.

83%
cite industry recognition as a key reason for choosing C|EH.

ORGANIZATIONS THAT EMPLOY 2025 C|EH HALL OF FAME AWARDEES

Google	DEPARTMENT OF DEFENSE UNITED STATES OF AMERICA	BANK OF AMERICA	Microsoft
accenture	EY Parthenon	AKIMA	ALPHATECHNOLOGIES
axcend	ELEVATORS POWER AMERSON Amerson ARD India Pvt.Ltd.	AOS Solutions	DELL
ART INSTITVTE CHICAGO	BROWARD COUNTY FLORIDA	Cargill™	citibank
cisco	CLOUDGRID NETWORKS	cognizant	consor
CoServ	crixto	CROWDSTRIKE	CYBERARK
CyberTech	NATIONAL PARK SERVICE	DLTCode	EVERGREEN TECHNOLOGY SOLUTIONS, LLC
EAST CAROLINA UNIVERSITY GREENVILLE, N.C.	Fidelis Security	FirstBank Since 1894	Flipkart
FORTINET	FRANKLIN COUNTY 1784 PENNSYLVANIA	Grant Thornton	GLS.
TUNIVERSITY	Phoenix TS	itm8®	GOVTECH SINGAPORE
RingCentral®	HITACHI Inspire the Next Hitachi Sunway Information Systems	AcuityBrands	HOSPITAL SÍRIO·LIBANÊS

ORGANIZATIONS THAT EMPLOY 2025 C|EH HALL OF FAME AWARDEES

WORLD BANK GROUP	United Nations	भारत सरकार GOVERNMENT OF INDIA सत्यमेव जयते	रक्षा मंत्रालय MINISTRY OF DEFENCE सत्यमेव जयते
KPMG	wipro	HBC	P&G
KARNATAKA STATE POLICE	MERKEZİ KAYIT İSTANBUL	Interactive Security Training	pwc
AADHAAR	ISACA.	Koniag Government Services	IGI The Cybersecurity People™
LANNAN TECHNOLOGIES	Q8	L9 CORPORATION	LOGICALIS Architects of Change
LATAM AIRLINES	MoneyGram.	MADARSONIT	Paytm
new era. TECHNOLOGY	paloalto® NETWORKS	POTOMAC ECONOMICS	Peraton
RTX		SAIC	SEMPRA INFRASTRUCTURE
Viasat	SOCHISI FUNDACIÓN SOCIEDAD CHILENA DE SEGURIDAD DE LA INFORMACIÓN	الشركة العربية للاستثمار ش.م.ع. THE ARAB INVESTMENT COMPANY S.A.A.	TRIAD SQUARE INFOSEC PVT.LTD
ZIMMER BIOMET	Penn UNIVERSITY of PENNSYLVANIA	UoPeople UNIVERSITY OF THE PEOPLE	

C|EH HALL OF FAME AWARDEES

(In Alphabetical Order by Region)

Americas (North & South)

Alfred Basta,
University, USA

Altan Tugay Bulut,
The World Bank, USA

Andres Javier Duarte,
Consor Engineers, USA

Anibal Meza Cajahuamán,
Allpha Technology, Peru

Armando Hernandez,
Peraton, USA

Babashola Madariola,
Madarson IT, USA

Benoit Desjardins,
University of Pennsylvania, USA

Bernard Garcia,
U.S. Department of Defense, USA

Brandon Bell,
IT Infrastructure & Security Freelance Consultant, USA

Brian Auten,
U.S. Department of the Interior - National Park Service, USA

Carl Arce,
Koniag Government Services, USA

Carlo Tannoury,
Phoenix TS, USA

Carlos Zambrano,
Carlos Zambrano Security Advisory, Colombia

Cecilia Milanezi Neves,
Sempra Infrastructure, Mexico

Chris Johnson,
Art Institute of Chicago, USA

Corey Green,
Evergreen Technology Systems, USA

Dane Burford,
SAIC, USA

Daniel Reyes,
RTX Corporation, USA

Danvers Budhwa,
Hudson's Bay Company, USA

David Carraway,
East Carolina University, USA

Deniz Mazlum,
RingCentral, USA

Bayo Omoyiola,
University of the People, USA

Duane Parker,
Franklin County Government, USA

Eric Peterson,
New Era Technology, USA

Essa Alshammari,
Palo Alto Networks, USA

Farid Abdelkader,
ISACA, USA

Francisco Llaguno,
Septron, Mexico

Frank Asamoah,
CoServ, USA

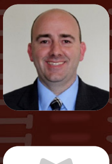
Frankie Grullon,
Level 9 Corporation, USA

Garrett Smiley,
Platinum Ox Consulting, USA

George Nkwonta,
Microsoft, USA

Gowthamaraj Rajendran,
Cisco, USA

Hector Hernandez,
Logicalis, USA


Howard Wolfe,
FirstBank, USA

Isaac Appiah,
Axcend Inc., USA

Jason Rorie,
Triad InfoSec, USA

C|EH HALL OF FAME AWARDEES

(In Alphabetical Order by Region)

Americas (North & South)

Jayson Ferron,
Interactive Security Training, USA

Jody Blanchard,
Zimmer Biomet, USA

Joe Kattner,
Fidelis Security, USA

Jorge Fernandez,
Cloud Grid Networks, USA

Joseph Morelli,
Remote Managed Services, USA

Joshua Phillips,
GLS, USA

Julio Briones,
SOCHISI, Chile

Junaid Khan,
Potomac Economics, USA

Justin Amerson,
Southern Tier Security, USA

Karen Macdougall,
Broward County Aviation Department, USA

Keith Frederick,
Viasat, USA

Leandro Ribeiro,
Hospital Sírio-Libanês, Brazil

Mahynour Sayed Ahmed,
Grant Thornton, Canada

Mario Villalobos,
Government, USA

Masoud Shahsavari,
Fortinet, Canada

Ousmane Barry,
Akima, USA

Scott Davis,
Acuity Brands, USA

Scott Zeltinger,
Cargill, USA

Shidarion Clark,
Lannan Technologies / 1 Sync Technologies, USA

Shruti Kalsi,
EY-Parthenon, USA

Smail Dahmoun,
IGI Cybersecurity, USA

Teobaldo Ernesto Rodríguez Espinoza,
CRIXTO, Venezuela

Wagner Morais,
LATAM Airlines, Brazil

Zakaria Bayahmed,
Ernst & Young, Canada

Europe

Alex Haynes,
IBS Software, Europe

Antonio Fernández,
DLTCode, Europe

Boris Krajnc,
I.T. Tim D.O.O., Europe

Celine Beaumel,
AOS Solution Informatique, Europe

Daniel Fai,
Procter & Gamble, Europe

Gabriel Avramescu,
ITUniversity.ro, Europe

Jeffrey Agomate,
Accenture, Europe

Johnni Rude,
itm8, Europe

Mandar Jadhav,
Amazon, Europe

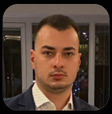
Murat Celebi,
Merkezi Kayıt Kuruluşu A.Ş., Europe

Ruben Amzallag,
Fortinet, Europe

Soner Çelik,
MoneyGram International Inc, Europe

C|EH HALL OF FAME AWARDEES

(In Alphabetical Order by Region)

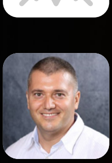

Tudor Ionut Urdeș,
CyberArk, Europe

Utku Yildirim,
Hoffmann Cybersecurity, Europe

Middle East

Abdelmajed Saeed,
CyberTech, Saudi Arabia

Hesham Dergham,
Kuwait Petroleum International, Kuwait


Maxim Balin,
Dell, Israel

Sayed Ossman,
The Arab Investment Company, Saudi Arabia

Africa, Asia, Australia

Abhishek Pandey,
Ernst & Young LLP, India

Amarjit Singh,
United Nations, India

Andy Ho,
GovTech, Singapore

Ashish Gupta,
Wipro, India

Ben Antony,
PwC, India

Bryan Chee,
Citibank, Singapore

Denis Nikolayev,
CrowdStrike, Australia

Jaikishan Sah,
Cisco, India

Juli Agarwal,
Flipkart, India

Kaustubh Choudhary,
Ministry of Defence, Government of India, India

Navateja Nami,
Bank of America, India

Praveen Kumar,
Cognizant, India

Rashtra Shourya,
Paytm, India

Roshan Reju,
Google, India

Ruhiish Vijaian,
Hitachi Sunway Information Systems, Malaysia

Sandeep Khanna,
Unique Identification Authority of India (UIDAI), India

Shafique Umar,
Wipro, India

Shivanand Adahalli,
Karnataka State Police, India

Supriyo Guha,
Government of India, India

Tejas Pingulkar,
KPMG, India

Vivek Kumar Gupta,
Reserve Bank Information Technology, India

Zechariah Akinpelu,
First Bank of Nigeria, Nigeria

{IMPACT QUADRANT}

The following insights developed through the combined experiences and career contributions of the C|EH Hall of Fame respondents and awardees highlight the tangible outcomes of the C|EH certification. The insights are mapped across the **Impact Quadrant:** Career Advancement, Industry Recognition, Hands-On Proficiency, and Skills Gained

1 Career Advancement

C|EH certification is driving upward mobility in cybersecurity careers, shaping salary outcomes, and opening doors to new job roles in a highly competitive landscape.

Key focus areas include:

- Career Mobility
- Salary Impact
- Job Market Advantage

2 Industry Recognition

Professionals are gaining credibility, peer recognition, and increased visibility in the workplace through C|EH.

Key focus areas include:

- Global Reputation
- Peer & Employer Respect

3 Hands-On Proficiency

Uncover the most in-demand skills developed through C|EH, backed by hands-on labs and real-world tools.

Key focus areas include:

- Virtual Labs & CTFs
- C|EH Compete

4 Skills Gained

C|EH is helping professionals build deep, hands-on expertise in areas like penetration testing, network security, and web application security.

Key focus areas include:

- Skill Advancement in Specialized Areas
- Modern Threat Coverage

CAREER ADVANCEMENT

Snapshot of Findings

99%

Say investing in C|EH benefited their career and professional growth.

98%

Credit C|EH as crucial to their cybersecurity career shift.

91%

Feel C|EH gives them a competitive edge over other certifications.

86%

Reported increased job opportunities after C|EH.

CAREER ADVANCEMENT

Career Mobility

98% Credit C|EH as crucial to their cybersecurity career shift. N=306

99% Say investing in C|EH benefited their career & professional growth. N=308

Salary Impact

93% Reported salary growth after obtaining C|EH. N=231

C|EH Is a Proven Catalyst for Career Transformation in Cybersecurity

Respondents consistently emphasize the credential's value as C|EH equips professionals with the technical skills and practical capabilities required to navigate complex threat environments, while also enhancing their credibility and visibility within the workplace. As cybersecurity roles become increasingly specialized and competitive, the certification serves not only as a gateway into the industry but also as a lever for upward mobility, positioning individuals for advanced roles in offensive and defensive security. This trend reaffirms C|EH's continued relevance as a career-shaping credential that supports both entry-level integration and long-term advancement in the cybersecurity profession.

Attaining the C|EH Commands Higher Compensation

Attaining the Certified Ethical Hacker (C|EH) certification underscores its relative impact on future earning potential. Data from the respondents demonstrates the financial value of the certification, reflecting the high demand for skilled ethical hackers in the cybersecurity industry. By validating advanced skills and ethical hacking expertise, the C|EH credential helps professionals negotiate better compensation and secure rewarding roles. C|EH's reputation as a globally recognized certification further solidifies its role in driving both career advancement and salary growth.

Important note: The notation N = [number] denotes the number of respondents for each data point or chart.

Job Market Advantage

91% Feel C|EH gives them a competitive edge over others.

N=313

86% Reported increased job opportunities after C|EH.

N=313

81% Saw expanded professional opportunities after C|EH.

N=321

C|EH Enhances an Individual's Competitiveness in the Cybersecurity Job Market

C|EH's widespread industry recognition has positioned it as an indispensable credential for cybersecurity professionals. It plays a critical role in enabling career progression, expanding opportunities, and validating expertise in ethical hacking and proactive threat management. As organizations seek highly capable security talent, the certification remains a key benchmark for advancing within a competitive and rapidly evolving landscape.

Earned a promotion after obtaining C|EH

"Right after passing the C|EH I was promoted to a Security Engineer role, where I received the opportunity to use the skills I have learned throughout the C|EH program.
I now manage and oversee a cybersecurity program for my organization, working with other stakeholders to manage and reduce organizational cyber risk."

Junaid Khan,
IT Security Director,
Potomac Economics

Important note: The notation N = [number] denotes the number of respondents for each data point or chart.

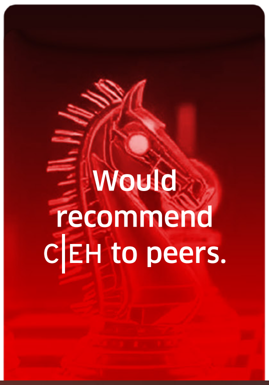
INDUSTRY RECOGNITION

Snapshot of Findings

100%

Say C|EH increased respect and recognition at workplace.

100%



Would recommend C|EH to peers.

83%

Cite industry recognition as a key reason for choosing C|EH.

INDUSTRY RECOGNITION

Peer & Employer Respect

100% Say C|EH increased respect and recognition in the workplace.

N=313

100% Would recommend C|EH to peers.

N=306

Global Reputation

83% Cite industry recognition as a key reason for choosing C|EH.

N=313

C|EH Demonstrates Practical and Job Readiness, Earning Peer Respect

Attaining the Certified Ethical Hacker (C|EH) credential elevates a professional's standing among both peers and employers. By validating real-world, hands-on expertise through rigorous practical training and dual-exam assessment, C|EH demonstrates an individual's readiness to contribute to complex security environments. This proven capability garners respect in the workplace and positions professionals as trusted contributors in cybersecurity strategy and execution. The strong peer endorsement further reflects C|EH's credibility, signifying not just personal achievement, but professional validation within the global cybersecurity community.

C|EH Is Recognized and Respected Across Borders

C|EH's strong global reputation stems from over two decades of leadership, innovation, and trust in cybersecurity education by organizations and professionals. Trusted by Fortune 500 companies, governments, and defense organizations, the C|EH certification has become a benchmark for validating hands-on ethical hacking expertise. What sets C|EH apart is its continual evolution, integrating AI-driven cybersecurity tools, aligning with globally adopted frameworks like MITRE ATT&CK, NICE and NIST Framework, and staying mapped to 49 real-world job roles. Its dual-assessment model (Knowledge + Practical), ANAB accreditation (ANSI National Accreditation Board) under ISO/IEC 17024 standards, and approval by the U.S. Department of Defense (DoD) under Directive 8140 further reinforce its industry credibility. The widespread recognition of C|EH not only makes it a preferred choice among professionals but also positions it as a globally endorsed standard for cybersecurity readiness.

C|EH opened doors for leadership in cybersecurity

"One highlight for me was the chance to speak on a panel at a security conference. With over 100 people attending my panel, I was asked a large variety of questions spanning the entire cybersecurity realm. I always say that the C|EH is a validation of actual skills and having the confidence to give your thoughts and opinions on cybersecurity is incredibly rewarding."

**Joe Kattner,
Director of Systems Engineering,
Fidelis Security**

Important note: The notation N = [number] denotes the number of respondents for each data point or chart.

HANDS-ON PROFICIENCY

Snapshot of Findings

99%

Found virtual labs in C|EH helpful to varying extents for developing real-world ethical hacking skills.

98%

Agree that C|EH Compete has made C|EH a continuous learning path, key to red teaming skill development.

HANDS-ON PROFICIENCY

Virtual Labs

99%

Found virtual labs in C|EH helpful to varying extents for developing real-world ethical hacking skills.

N=317

1 in 2

Found hands-on labs to be one of the most beneficial components of the C|EH training.

N=254

C|EH Global Competition

98%

Agree that C|EH Compete has made C|EH a continuous learning path, key to red teaming skill development.

N=313

C|EH Focuses on Practical Training for Today's Cybersecurity Challenges

The C|EH program places real-world readiness at its core through an extensive set of hands-on labs. These labs are designed to simulate real attack environments and walk learners through each phase of an ethical hacking operation, from reconnaissance to exploitation and defense. They empower professionals to sharpen their skills through repetition, experimentation, and scenario-based learning. This immersive, experiential format makes C|EH not just a certification but a skill-building engine that prepares candidates for high-pressure roles in offensive and defensive security.

C|EH Fosters Continuous Mastery

The integration of C|EH Compete into the C|EH program transforms it from a one-time credential into an ongoing learning journey. With 12 real-world Capture the Flag (CTF) challenges, C|EH Compete offers professionals a dynamic platform to sharpen red teaming techniques and offensive security skills. By engaging in repeatable, high-pressure simulations, learners build tactical expertise far beyond traditional coursework. C|EH Compete reinforces C|EH's relevance in modern cybersecurity—where readiness, adaptability, and hands-on ability are essential. As a result, professionals remain competitive, current, and confident in the face of evolving threats.

Used hands-on techniques to assess infrastructure risks and prevent a potential data breach

"Through thorough analysis and exploitation simulation, I provided actionable recommendations to mitigate an identified infrastructure risk effectively. This proactive approach prevented a potential data breach."

Masoud Shahsavari,
Security Engineer,
Fortinet

Important note: The notation N = [number] denotes the number of respondents for each data point or chart.

SKILLS GAINED

Snapshot of Findings

97%

Say C|EH effectively covered emerging threats and trends.

86%

Reported enhanced proficiency in penetration testing.

SKILLS GAINED

Skill Advancement in Specialized Areas

86% Reported enhanced proficiency in penetration testing.
N=321

82% Gained stronger capabilities in network security.
N=321

71% Advanced their skills in web app security.
N=321

Modern Threat Coverage

97% Say C|EH effectively covered emerging threats and trends.
N=315

96% State the inclusion of advanced topics (MITRE ATT&CK, Fog, Edge computing, etc.) enhanced their real-world preparedness.
N=312

C|EH Is Engineered to Deliver Real-World Cybersecurity Readiness

According to learners, the most significant skill improvements from C|EH were in penetration testing, network security, and web application security. Covering the full cyber kill chain, from network enumeration to defensive evasion, the curriculum equips professionals with a comprehensive understanding of attacker methodologies and corresponding defensive strategies. Its in-depth focus on network vulnerabilities, intrusion tactics, and infrastructure defenses builds hands-on expertise in packet sniffing, IDS evasion, firewall analysis, and honeypot bypassing. Additionally, C|EH provides practical training on OWASP Top 10 risks, including AI system exploitation, session hijacking, and SQL injection, enabling learners to identify and remediate real-world web application vulnerabilities. Together, these capabilities position certified professionals to detect, mitigate, and respond effectively to evolving cybersecurity threats.

C|EH Keeps Pace with the Evolving Threat Landscape

The C|EH curriculum is purpose-built to equip professionals with cutting-edge knowledge of today's most dynamic attack surfaces, from AI-driven exploits to vulnerabilities in fog, edge, and hybrid cloud environments. With frameworks like MITRE ATT&CK and coverage of modern architectures including IoT and cloud, C|EH prepares learners to confidently navigate complex and modern real-world threat scenarios. More than theory, C|EH offers a forward-leaning, application-first learning experience. Its integration of advanced tools and evolving tactics ensures professionals aren't just aware of modern threats, they're equipped to detect, defend, and adapt. This makes C|EH a vital asset for building real-world cyber resilience.

C|EH helped in building a comprehensive penetration testing infrastructure

"The skills I learned through the C|EH were instrumental in ensuring no stone was left unturned as we developed our penetration testing infrastructure."

Scott Davis,
Director of Software Engineering,
Acuity Brands

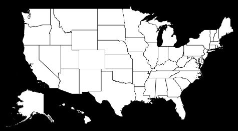
Important note: The notation N = [number] denotes the number of respondents for each data point or chart.

HALL OF FAME REPORT: COMMUNITY PROFILE

Geographic Distribution of Respondents

The largest share of C|EH Hall of Fame respondents come from Asia, reflecting the region's growing investment in cybersecurity talent and certification.

Asia 37%



Representing North and South America, this region showcases a strong adoption of C|EH across both corporate and government cybersecurity roles.

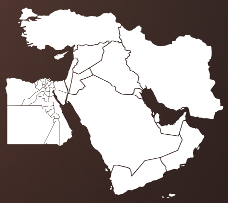
Americas 24%

With established cyber infrastructure and mature security markets, Europe continues to be a key hub for C|EH-certified professionals.

Europe 22%

The rising presence of C|EH holders indicates the growing awareness of ethical hacking and demand for certified professionals across the continent.

Africa 9%



Cybersecurity is a regional priority, with C|EH gaining traction among professionals in both public and private sectors.

Middle East 7%

A small but notable segment from Australia is showing a growing demand for skilled Certified Ethical Hackers.

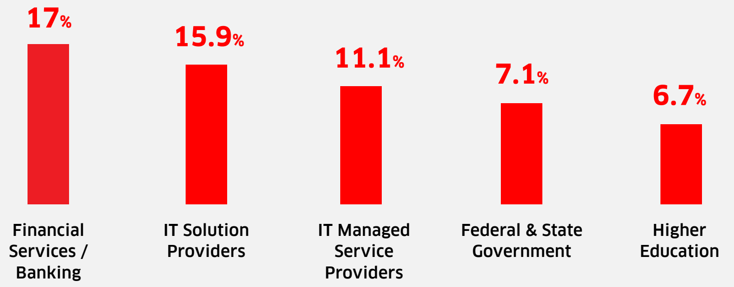
Australia 1%

Experience Level

6-10 years	25%
11-15 years	22%
21+ years	20%
16-20 years	19%
0-5 years	14%

Industry/Sector Representation

Top Industries Include:



Other Sectors Represented:

- Energy, Telecommunications, Healthcare, Manufacturing
- Aerospace, Automotive, Retail, and Non-Profit

Job Titles and Roles of Respondents

Mid-Level Technical – (Includes Security Engineers, Analysts, Architects, Consultants, Researchers)	43%
Executive Leadership – (CEOs, CISOs, CTOs, CIOs, VPs, Presidents, Directors)	22%
Senior Management – (Security/IT Managers, Leads, Heads, Senior Roles)	19%
Technical Support & Education – (Trainers, Support Engineers, Lecturers, Admins)	8%

Job Title Distribution

Predominantly technical and mid-to-senior roles:

• **IT Security Manager**	9.4%
• **CISO**	7.7%
• **Security Engineer**	7.5%
• **Security Consultant/Advisor**	7.1%
• **Security Analyst**	6.3%

Additional Roles Include:

- Penetration Testers, Architects, IT Directors
- CEOs, CTOs, CISOs, and Security Officers
- Cybersecurity Educators and Trainers

Respondents with Niche Titles:

- Threat Hunters, Product Security Leads, and Bug Bounty Specialists

SUCCESS STORIES OF CERTIFIED ETHICAL HACKERS

Used ethical hacking techniques to proactively identify and resolve a critical security vulnerability

"By employing advanced penetration testing techniques and ethical hacking principles, I identified a previously undetected exploit that could have allowed unauthorized access to sensitive data. By designing and implementing a bespoke security patch in collaboration with the IT team, we fortified the network's defenses, preventing potential data breaches."

Barry Ousmane, Security Manager, Akima (USA)

Applied concepts from C|EH to develop secure cyber tools with cryptographic solutions

"I built several cyber tools that deal with cryptographic solutions. This achievement was significant because it saved the organization significant costs due to the alternative being the purchase of expensive crypto solutions. I learned from the C|EH that identifying an attack surface was important, so I built my design with this concept in mind."

Daniel Reyes, Security Engineer, RTX Corporation

C|EH skills helped in advancing threat detection and research

"Working at Cisco as a Security Researcher, I was responsible for creating advanced threat detection rules for customers. Using the skills I gained through the C|EH program, my work has been published and cited over 100 times."

Gowthamaraj Rajendran, Threat Detection Engineer, Cisco

C|EH enhanced my role and security control implementation

"I used the skills from C|EH to refine my skills on the SOC floor, excelling at the position and getting promoted to the Cyber Infrastructure team. I used the knowledge and skills I learned to conduct multiple investigations on intrusion attempts and resolve these events in a timely fashion."

Dane Burford, Security Engineer & Non-Profit Contractor, SAIC

SUCCESS STORIES OF CERTIFIED ETHICAL HACKERS

Reduced security incidents through enhanced employee awareness with C|EH knowledge

"I spearheaded the implementation of a robust cybersecurity awareness training program, reducing the frequency of security incidents by 30% through enhanced employee vigilance and adherence to best practices."

Babashola Madariola, CEO, Madarson IT

Advanced techniques from C|EH helped uncover critical vulnerabilities in network infrastructure

"During a penetration testing project for a high-profile client, I utilized advanced techniques learned from the C|EH program where I uncovered critical vulnerabilities in their network infrastructure, including misconfigurations and outdated software. By simulating real-world cyberattacks, I demonstrated potential exploitation scenarios and provided actionable recommendations for remediation. My thorough analysis and strategic approach not only impressed the client but also resulted in immediate security enhancements, safeguarding their assets and bolstering their confidence in our cybersecurity expertise."

Essa Alshammari, Systems Engineer, Palo Alto Networks

Empowering informed decision-making at the executive level with C|EH expertise

"I served as a trusted advisor to C-suite executives, board members, and senior management, providing strategic guidance and insights on cybersecurity risks, trends, leading to the enablement of informed decision-making and investment prioritization across the organization."

Zakaria Bayahmed, Senior Advisor, Ernst & Young

Clear concepts of C|EH helped me reverse engineer and leverage scanning of networks and devices

"It would not be possible to perform reverse engineering, think like a hacker, and implant vulnerabilities if I had not had clear concepts from C|EH. I then leveraged the scanning I learned during C|EH for my second job at Xerox Technologies as an Information Security Analyst, where I used to scan networks and devices for Xerox global network."

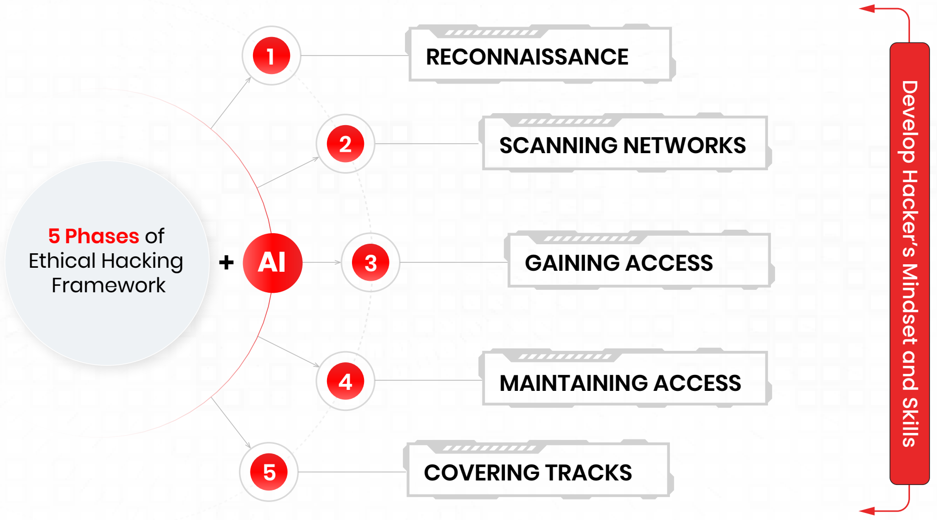
Shruti Kalsi, IT Security Director, EY-Parthenon

AN EVOLVED C|EH FOR AN EVOLVING THREAT LANDSCAPE

Certified Ethical Hacker Powered by AI

1. Lean | 2. Certify | 3. Engage | 4. Compete

Practical Learning for Job Ready Skills Mapped to 45+ Job Roles



5 Phases of Ethical Hacking Framework + AI

1 RECONNAISSANCE

2 SCANNING NETWORKS

3 GAINING ACCESS

4 MAINTAINING ACCESS

5 COVERING TRACKS

Develop Hacker's Mindset and Skills

Knowledge-Based & Practical Exam
Validates Your Ethical Hacking Skills Prowess to Employers

The annual exercise of surveying the top ethical hackers and drawing upon their professional experience has proved valuable in understanding the evolving challenges and impact of C|EH. In keeping with EC-Council's goal of building a secure cyber future, these surveys have been instrumental in helping us stay ahead of the ever-evolving cyber threats.

One such urgent trend is the rise of AI-driven cyberattacks, which are rapidly increasing in complexity and frequency—signaling a rapid shift in threat methodologies. Compared to organizations, threat actors are increasingly leveraging AI. For instance, AI generated phishing mails have higher open rates (IBM, 2023). Moreover, over **74% of organizations surveyed observed a surge in AI-powered cyberattacks** and **66% admitted to being ill-prepared for AI-driven cyber threats** (EC-Council, 2025). As adversaries leverage automation and intelligent attack vectors, the need for ethical hackers trained in modern, AI-integrated defense strategies has become more urgent than ever.

In direct response to the growing sophistication of threat actors and the urgent need for faster, smarter defenses—as highlighted in the EC-Council C|EH Threat Report 2025—EC-Council became the first to launch a free Cyber AI Toolkit for its global community. Building on this proactive stance, the latest version of the Certified Ethical Hacker (C|EH$^{\text{AI}}$) certification has been significantly upgraded to include expanded, AI-enabled features. Designed to combat the rise of AI-powered cyberattacks, C|EH$^{\text{AI}}$ equips cybersecurity professionals with multi-platform capabilities to detect and remediate advanced vulnerabilities. The future-ready certification leverages AI for faster threat detection, improved decision-making, and streamlined reporting. Following is a glimpse into the latest, version 13 of C|EH.

CERTIFIED ETHICAL HACKER (C|EH AI) POWERED WITH AI CAPABILITIES

Key Features:

1. Globally Recognized

C|EH AI has been the world's No. 1 ethical hacking certification for 20 years. It is the only ethical hacking certification to teach AI-driven cybersecurity skills.

2. Learning Framework

C|EH AI is the only cybersecurity training program with a unique learning framework: (i) Learn, (ii) Certify, (iii) Engage, and (iv) Compete.

A) C|EH AI Learn:

- 20 modules covering core skills of cybersecurity.
- Hands-on 221 labs and 4,000 hacking tools for practical learning.
- Labs to practice AI skills.
- 551 attack techniques to prepare for real-world scenarios.

B) C|EH AI Certify:

Dual Exams:

- 4-hour, 125-question knowledge-based exam.
- 6-hour practical exam featuring 20 practical scenarios to validate skills.
- Both exams are ANAB 17024 approved and U.S. DoD accredited.

C) C|EH AI Engage:

- Real-world hacking simulations on real networks for immersive training.

D) C|EH AI Compete:

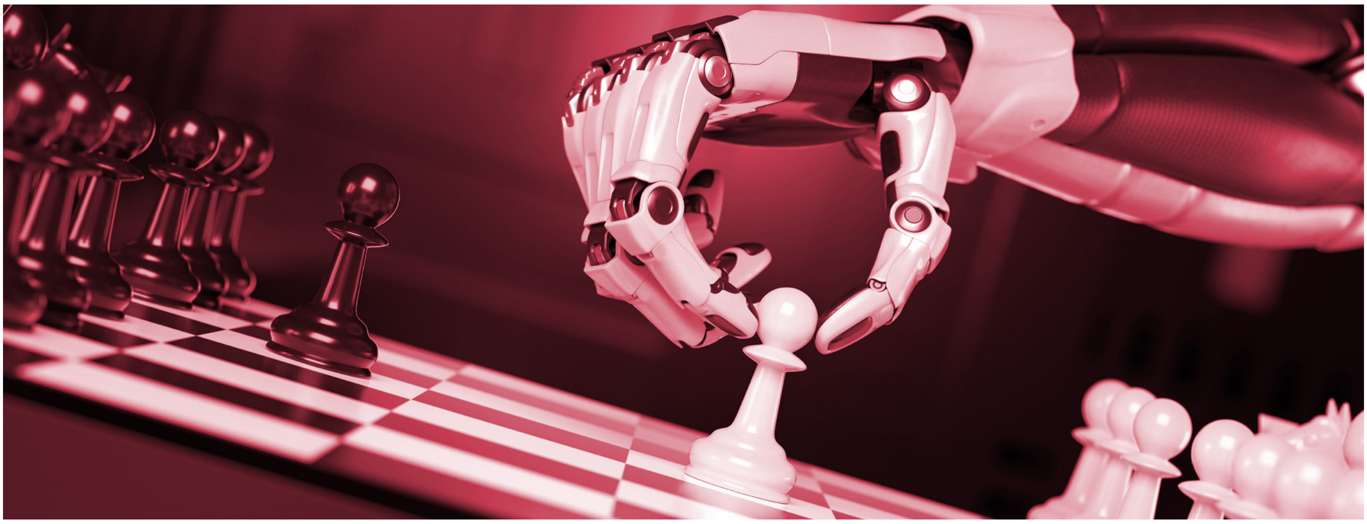
- One-year access to 12 Capture the Flag (CTF) challenges for skill refinement, providing a continuous learning platform.

3. AI-Driven Skills

Professionals can master AI-based cybersecurity skills and learn to hack AI attack systems.

4. Job-Ready Certification

C|EH is mapped to 49 cybersecurity job roles, boosting employability rates.



JOB ROLES MAPPED TO C|EH AI

Certified Ethical Hackers continue to operate across all industries and sectors. Recent reports indicate demand for these and similar roles is expected to rise nearly 30% through 2030 (Cambridge College of Healthcare and Technology). A staggering 97% of polled cybersecurity professionals found that the skills developed via the C|EH address emerging cybersecurity threats and trends, assisting them with effectively securing their organization. Certified Ethical Hackers bring versatile skills that are highly desired and are well-suited for numerous cybersecurity roles, including:

- Mid-Level Information Security Auditor
- Cybersecurity Auditor
- Security Administrator
- IT Security Administrator
- Information Security Analyst 1
- Information Security Administrator
- Cybersecurity Analyst (Levels 1, 2, & 3)
- Network Security Engineer
- SOC Security Analyst
- Network Engineer
- Senior Security Consultant
- Information Security Manager
- Senior SOC Analyst
- Solutions Architect
- Cybersecurity Consultant
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- All-Source Analyst
- Cyber Defense Incident Responder
- Research & Development Specialist
- Senior Cloud Security Analyst
- Third-Party Risk Management
- Threat Hunting Analyst
- Penetration Tester
- Cyber Delivery Manager
- Application Security Risk
- Threat Modeling Specialist
- Web Application Penetration Tester
- SAP Vulnerability Management – Solution Delivery Advisor
- Ethical Hacker
- SIEM Threat Responder
- Product Security Engineer/Manager
- Endpoint Security Engineer
- Cybersecurity Instructor
- Red Team Specialist
- Data Protection & Privacy Officer
- SOAR Engineer
- AI Security Engineer
- Senior IAM Engineer
- PCI Security Advisor
- Exploitation Analyst (EA)
- Zero Trust Solutions Engineer/Analyst
- Cryptographic Engineer
- AI/ML Security Engineer
- Machine Learning Security Specialist
- AI Penetration Tester
- AI/ML Security Consultant
- Crypto Security Consultant

CONCLUSION

The Certified Ethical Hacker Hall of Fame 2025 Industry Report reflects a global movement where ethical hacking has become a driving force in shaping resilient digital ecosystems. These professionals stand at the intersection of technical depth, leadership, and continuous learning, strengthening organizational defenses while enabling businesses, governments, and institutions to navigate increasingly sophisticated threats.

As Jay Bavisi, Group President of EC-Council, remarks, these inductees have elevated ethical hacking into a strategic discipline, where their expertise extends far beyond protection, becoming a catalyst for growth, trust, and long-term security. Their work defines a new standard for what it means to lead in cybersecurity today.

With AI-driven threats accelerating the complexity of the landscape, the demand for professionals equipped with hands-on mastery and adaptive thinking has never been more critical. The CEH program continues to evolve to meet this need, now powered with AI capabilities, immersive labs, real-world simulations, and mapped pathways to emerging job roles.

The Certified Ethical Hacker Hall of Fame 2025 Industry Report is not simply a recognition of past achievement. It signals the growing influence of ethical hackers in charting the future of cybersecurity and preparing organizations worldwide to move forward with confidence.

ABOUT EC-COUNCIL

EC-Council is the creator of the Certified Ethical Hacker (C|EH) program and a leader in cybersecurity education. Founded in 2001, EC-Council's mission is to provide high-quality training and certifications for cybersecurity professionals to keep organizations safe from cyber threats. EC-Council offers over 200 certifications and degrees in various cybersecurity domains, including forensics, security analysis, threat intelligence, and information security.

An ISO/IEC 17024 accredited organization, EC-Council has certified over 350,000 professionals worldwide, with clients ranging from government agencies to Fortune 100 companies. EC-Council is the gold standard in cybersecurity certification, trusted by the U.S. Department of Defense, the Army, Navy, Air Force, and leading global corporations.

TERMS AND CONDITIONS OF USE

EC-Council's intent in posting this report is to make the report available for informational purposes and personal use of the public. You are welcome to post, repost, and distribute the report provided it remains unmodified and in its original form, and you must reference and link to the following reference. Link: Reference: 2025 C|EH Hall of Fame Annual Industry Report

- No modifications shall be made to the data and information;
- This report shall be identified as the original source of the data and information;
- EC-Council's website shall be identified as the reference source for the report's data and information; and
- the reproduction shall not be marketed or labeled as an official version of the materials in the report, nor as being endorsed by or affiliated with EC-Council.

EC-Council disclaims any representation or warranty, express or implied, as to the accuracy or completeness of the material and information contained herein, and EC-Council shall under no circumstances be liable for any damages, claims, causes of action, losses, legal fees, expenses, or any other cost whatsoever arising out of the use of this report or any part thereof, regardless of any negligence or fault, for any statements contained in, or for any omissions from, this report. By accessing and using this report, you agree to indemnify and hold EC-Council harmless from all claims, actions, suits, procedures, costs, expenses, damages, and liabilities, including attorneys' fees, brought as a result of misuse of the report or in violation of the authorizations as provided herein.

EC-Council

Building A Culture Of Security

EMPOWERING ETHICAL HACKERS WORLDWIDE

Celebrating the C|EH Hall of Fame—EC-Council's commitment to advancing cybersecurity leadership, innovation, and global impact.

www.eccouncil.org