EC-Council

THE 2023 C|EH HALL OF FAME ANNUAL REPORT

LEADING THE ETHICAL HACKING COMMUNITY IN 2023

MEET THE TOP 100

C|EH Certified Ethical Hacker

TABLE OF CONTENTS

ACKNOWLEDGEMENT AND **FOREWORD**

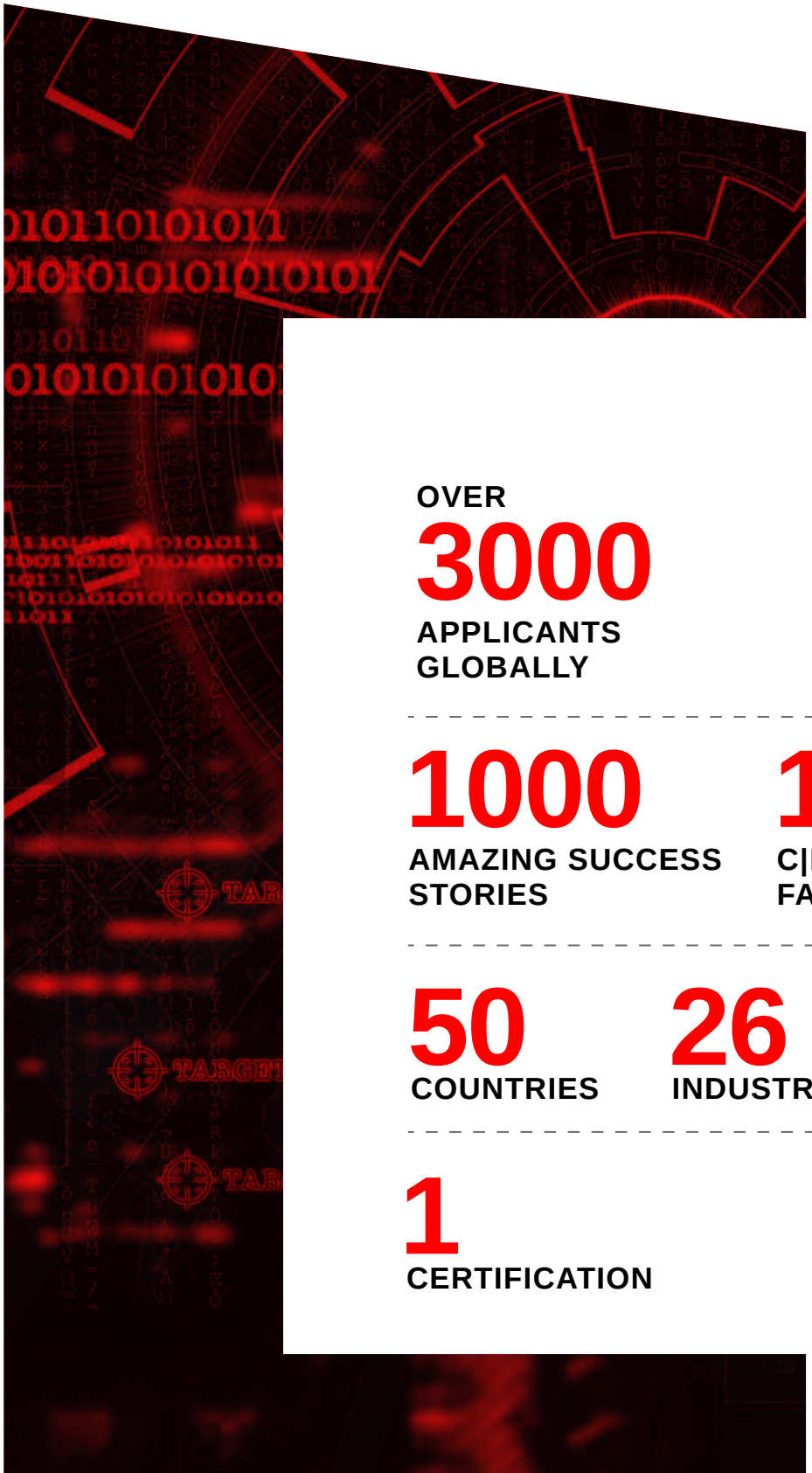
The Certified Ethical Hacker community is known for the willingness of its members to share the key experiences that mark every stage of their professional development. Both the newcomer's contagious enthusiasm and the veteran's wisdom benefit countless individuals, some who are already in the cybersecurity field and others who are considering entering it. This report is a direct outcome of that sharing attitude. It is based on a multitude of data points gathered from a detailed survey of more than 3,300 C|EH Hall of Fame applicants. Their candid responses shed light on many practical aspects of career advancement through EC-Council's C|EH certification program. They also illustrate the real-world applications of specific ethical hacker skills. The personal narratives of these hackers at widely varying points along their professional journeys provide windows into an exciting and meaningful field. The world needs more capable and dedicated cybersecurity defenders like these standout individuals, and we are grateful for their participation.

The 2023 C|EH Hall of Fame Annual Report is a comprehensive and in-depth examination of the Certified Ethical Hacker (C|EH) community. This report is based on a detailed survey of more than 3,300 C|EH Hall of Fame applicants, providing Valuable insight into the practical aspects of career advancement through the C|EH certification program and the real-world applications of ethical hacking skills.

The report also includes personal narratives of these hackers at different stages in their careers, offering a glimpse into the dynamic and rewarding field of cybersecurity and career highlights of the Hall of Famers, as well as statistics and insights from surveys of C|EH participants. Overall, this report serves as a valuable resource for anyone interested in the ethical hacking community and the role of the C|EH in advancing the field of cybersecurity.

This report provides an overview of the state of the cybersecurity industry in 2023, highlighting key challenges and achievements. It also examines the impact of the C|EH program on the careers and professional development of those in the community, including the 1,000 finalists and 100 awardees of the C|EH Hall of Fame honor.

C|EH HALL OF FAME



OVER
3000
APPLICANTS GLOBALLY

1000
AMAZING SUCCESS STORIES

100
C|EH HALL OF FAME AWARDEES

50
COUNTRIES

26
INDUSTRIES

1
CERTIFICATION

DISCLAIMER

This report is available to you on an "as is where is" basis at the sole discretion of EC-Council, subject to the terms and conditions of use below (the "Terms and Conditions"). This includes the data and information in the report. This report has been produced based on the information collected as part of the Certified Ethical Hacker (C|EH) Hall of Fame program and is considered to be true, reliable, and accurate. The editors reserved the right to make correct and/or edits statements but these would only be done with the sole intent to correct grammatical errors and/or to paraphrase some responses to maintain brevity for the benefit of the readers, while ensuring that the original statement and intent was, to the best of our knowledge, unaltered. While EC-Council has made every attempt to ensure that the information contained in this report is from reliable resources, EC-Council does not warrant the accuracy of or make any other warranties or representations regarding this report or the information contained therein. In addition, report updates may not be made available to you. The use of this report is at your sole and absolute risk. The 2023 C|EH Hall of Fame Award selections were based on applications that were received in Q3-Q4 of 2022.

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. Without the prior written consent of EC-Council or unless indicated in the terms and conditions, neither the report nor any part thereof should be reproduced, distributed, copied, downloaded, displayed, republished, posted, or transmitted in any form, by any means. Data and information in this report may be reproduced based on certain conditions as follows:

- Disclaimers in this report shall be kept in their original form and applied to the data and information in the 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.

KEY TAKEAWAYS

WHAT THE RESPONDENTS SAID:

Over 50%
Of Professionals Received Promotions after C|EH

97%
Of Professionals Stated That Skills Acquired in C|EH Helped Safeguard Their Organizations

97%
Of Professionals Found C|EH Labs to Accurately Mimic Real-World Cyber Threats

95%
Chose C|EH for Career Growth.

93%
Of Professionals Stated That C|EH Skills Improved Their Organizational Security

92%
Of Hiring Managers Prefer Candidates with C|EH For Jobs That Require Ethical Hacking Skills.

92%
Of Professionals Reported that C|EH Boosted Their Self Confidence

88%
Considered C|EH to be the Most Comprehensive Ethical Hacking Program In the Industry

85%
Of Professionals Credited C|EH to Helping Them Give Back to the Cybersecurity Community

80%
Started their cybersecurity careers with the C|EH.

KEY TAKEAWAYS

HOW BECOMING A CERTIFIED ETHICAL HACKER POSITIVELY IMPACTS YOUR CYBER CAREER

The C|EH equips professionals with skills to combat ransomware.

C|EH certification opens doors to cyber careers.

The C|EH builds a versatile skillset that is applicable across

The C|EH enhances employment opportunities in the field of cybersecurity.

The C|EH fosters a sense of social responsibility and enables professionals to give back to the community.

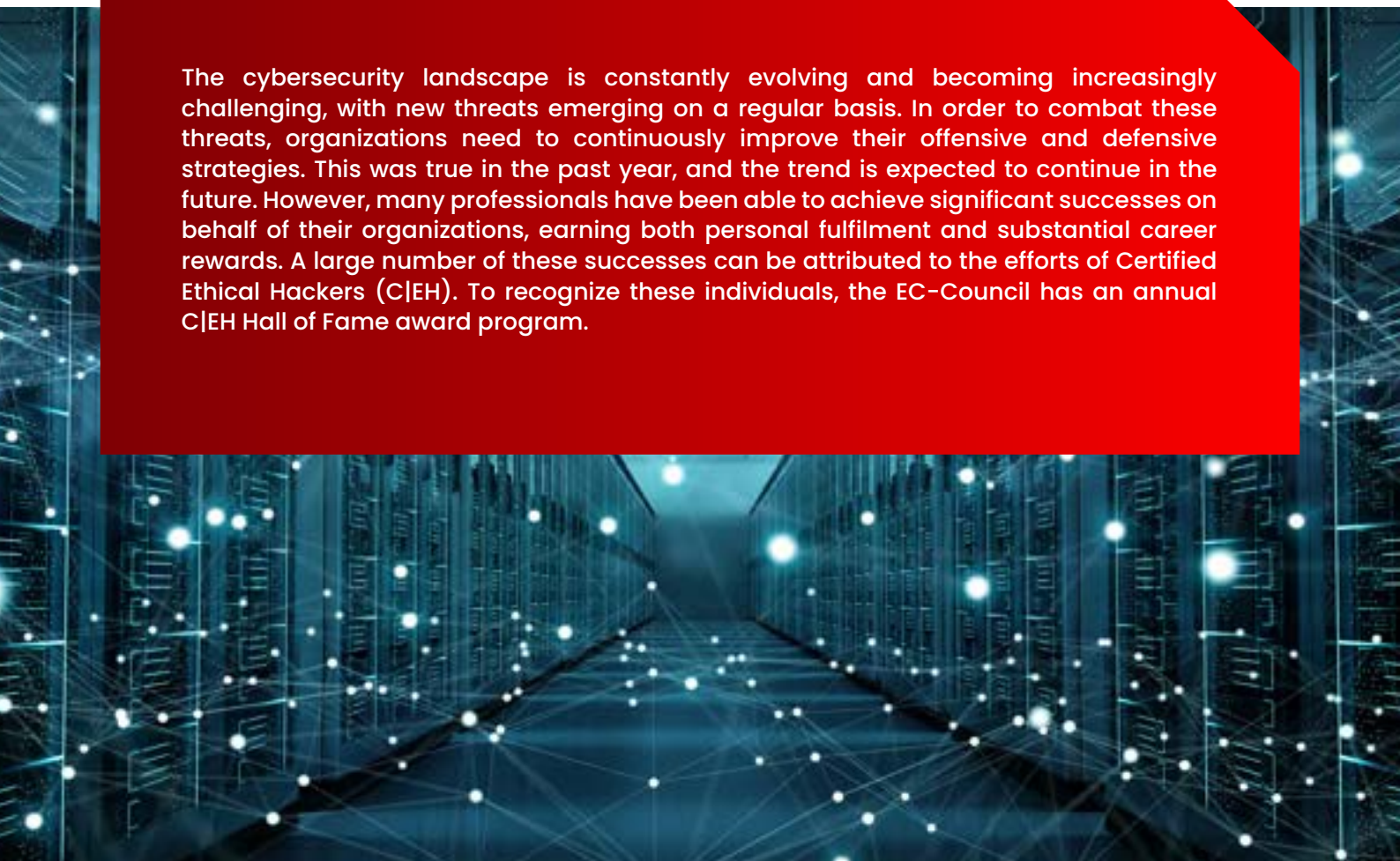
INTRODUCTION

In the cybersecurity world, it is safe to assume that things will get worse before they get better and that it is necessary to continuously ramp up offensive and defensive strategies to combat predictably growing threats. That general assessment remains true in 2023, but the good news is that many professionals are able to score significant wins on behalf of their organizations, reaping both personal fulfillment and substantial career rewards. Certified Ethical Hackers are responsible for many of those bold moves, and EC-Council recognizes thousands of them in its annual C|EH Hall of Fame award program.

We began this process by inviting people who scored 90% or higher on the C|EH certification exam to apply to the C|EH Hall of Fame. More than 3,300 answered the call, and EC-Council promoted 1,000 of them, representing 50 countries from almost every region in the world (see figure 1) to the final round. Then we evaluated each individual's unique set of career accomplishments and community contributions and selected 100 stellar Certified Ethical Hackers for induction into the C|EH Hall of Fame.

This report highlights both the overall characteristics that distinguish ethical hackers as a group and the personal journeys of the Hall of Famers who made an indelible mark within the cybersecurity community. Their stories point to the C|EH program's openness, diversity, adaptability and, most of all, effectiveness in delivering positive outcomes for the organizations that rely on ethical hackers' expertise. Their success provides ample fuel for the ambitions of those who are thinking of joining the C|EH ranks.

The cybersecurity landscape is constantly evolving and becoming increasingly challenging, with new threats emerging on a regular basis. In order to combat these threats, organizations need to continuously improve their offensive and defensive strategies. This was true in the past year, and the trend is expected to continue in the future. However, many professionals have been able to achieve significant successes on behalf of their organizations, earning both personal fulfilment and substantial career rewards. A large number of these successes can be attributed to the efforts of Certified Ethical Hackers (C|EH). To recognize these individuals, the EC-Council has an annual C|EH Hall of Fame award program.



2023 C|EH HALL OF FAME - PARTICIPATION BY REGION

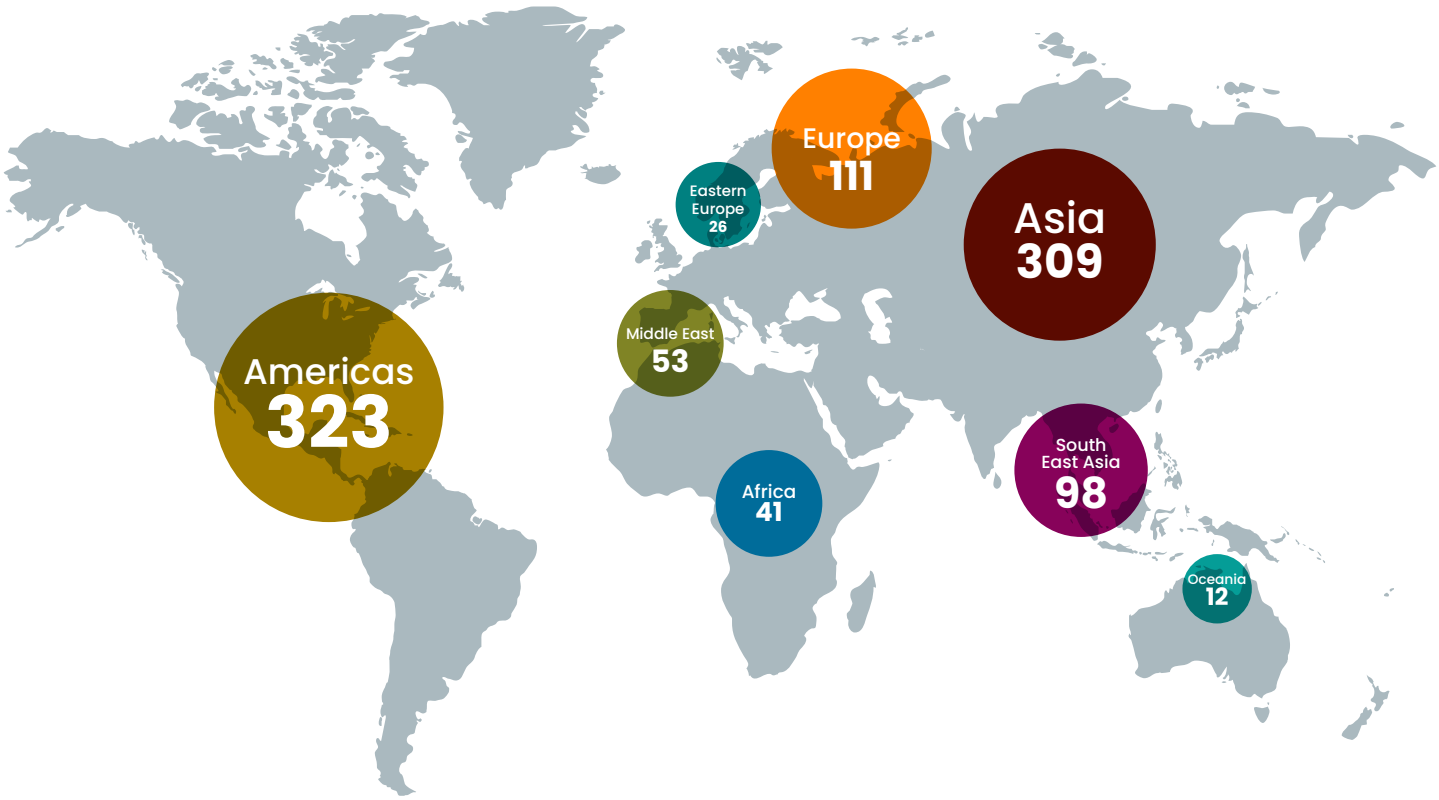
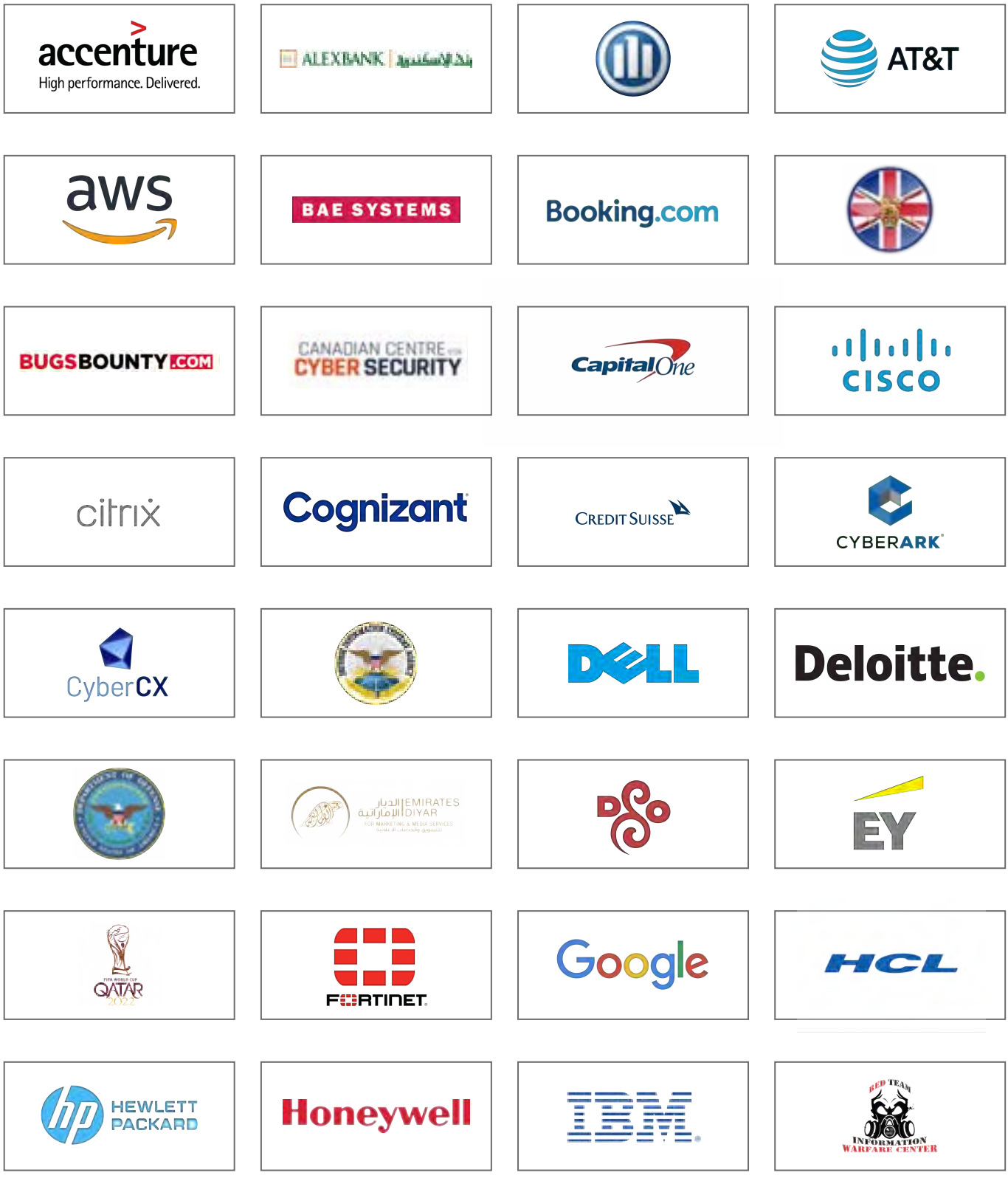


Figure 1: 2023 C|EH Hall of Fame Participation by Region (Awardees and Finalists)


C|EH
Certified Ethical Hacker
HALL OF FAME
2023
Read about the inspirational achievements of this year's Certified Ethical Hacker Hall of Fame Awardees.
Click Here

The 2023 C|EH Hall of Fame Awardees are employed at the following organizations:




intel

USM


leidos

lemongrass

LIVEPERSON

LOCKHEED MARTIN

LTI


Microsoft

Morgan Stanley

nas
NATIONAL AVIATION SERVICES

NATIONAL
GEOGRAPHIC
SOCIETY

NATO
OTAN


NOKIA

NORTHROP
GRUMMAN

NTT DATA
Global IT Innovator

ökko

orange

ORACLE

QATAR
AIRWAYS


Schneider
Electric

SIEMENS

SONY

tcs
TATA
CONSULTANCY
SERVICES

Telefónica

TEXAS CAPITAL BANK

T-
Mobile

US Army Corps
of Engineers.

UniCredit

UNITED AIRLINES



VA
U.S. Department
of Veterans Affairs

C|EH HALL OF FAME 2023 AWARDEES

(in alphabetical order by region)

Americas (North and South)

Adam Hardinger,
Department of Defense, USA

Adriano Guarato,
Via, Brazil

Andrew Marsh,
AWS, USA

Farzan Karimi,
Google, USA

Brett Riddle,
US Army, USA

Brian Cochran,
U.S. Army, USA

Bruno Odon,
ISH Tecnologia, Brasil

Chris Bush,
Defense Information Systems Agency (DISA), USA

Cinderella Almond,
Department of the Air Force, USA

Dan White,
U.S. Department of Veterans Affairs, USA

David Bifulco,
Nokia, USA

David Formato,
DoD, USA

Dwayne Hodges,
AT&T, USA

Eduardo Tovar Angulo,
Tata Consultancy Services, Mexico

Edward LaBarge,
US Army, USA

Felipe Munoz,
Oracle America, USA

Frankie Grullon,
US Air Force, USA

George Garcia,
Department of Defense, USA

Henderson Jones,
National Geographic Society, USA

Jason Harlow,
US Army, USA

Jason Lee,
Deloitte, USA

Jeremy Martin,
Information Warfare Center, USA

Jeromy Caldwell,
DOD, USA

Jessica Partin-Sawyers,
Microsoft, USA

John Packiaraj,
Visa, USA

Josue Negron,
U.S. Navy, USA

Kabiru Atta
Texas Capital Bank, USA

Kevin Daily,
Warner Bros Discovery, USA

Kojo Donkor,
Cisco Systems, USA

Lawan Cancer II,
Morgan Stanley, USA

Marcelo Da Silva,
Microsoft, USA

Masoud Shahsavari,
Fortinet, Canada

Mauricio Fernandes,
Cisco, USA

Michael Brainard,
SP Richards, USA

Michael Hildebrand,
Microsoft, USA

Nealum Veal,
U.S. Army, USA

Noel Nicolas,
US Air Force, USA

Omar Galban,
U.S. Navy, USA

Omar Zaman,
United Airlines, USA

Patrick Gladney,
U.S. Army Corps of Engineers, USA

Pierre Boisrond,
Hewlett Packard Enterprise, USA

Rajkumar Balachandar,
Cognizant, Canada

Ramin Nafisi,
Microsoft, USA

Reginald Harris,
U.S. Military, USA

Robert Weber,
Booz Allen Hamilton, USA

Roy Davis,
Zoom, USA

Sally Shamon,
DOD/DIA, USA

Samuel Kwaw,
Leidos, USA

Scott Russo,
Capital One, USA

Sofia Nicholson,
Microsoft, USA

Stephanie Loyd,
Department of Defense, USA

Stephen Reid,
U.S. Army, USA

Steve Vaillancourt,
Canadian Centre for Cyber Security, Canada

Thomas Aldrich,
Lockheed Martin, USA

Timothy Amerson,
U.S. Department of Veterans Affairs, USA

Tyree Scott,
Department of the Navy, USA

Victor Toeh,
Northrop Grumman, USA

Mark Sweet,
Department of Defense, USA

Marouane Balmakhtar,
T-Mobile, USA

Marvin Soto,
Grupo Babel and LCI Education, USA

Europe

Adam Bieniasz,
British Army, United Kingdom

Ali Karakoc,
IBM, Netherlands

Bjoern Voitel,
DSO Datenschutz Osnabrueck, Germany

Daniel Robbertse,
Skillsoft, UK

Daniele Belluccio,
Italy

Gerard Aroquianadin,
Orange, France

Guerrino Mazzarolo,
NATO, Belgium

Ilyass Soussi,
EY Consulting, France

Javier Cavero,
TÜV Rheinland, Spain

Joao Rafael,
Credit Suisse, Poland

Luca Porrini,
Unicredit, Italia

Massimo Biagi, Liveperson,
Germany

Mirko Messia, Italian MoD,
Italian Air Force, Italy

Mostafa Mohsen,
Booking.com, Netherlands

Nicola Bressan,
Yarix SRL, Italy

Ravi Gupta,
Sony Europe BV, United Kingdom

Steven Wright,
Citrix, United Kingdom

Tudor Ionut Urdes,
CyberArk, Netherlands

Valerio Severini,
EY, Italy

Middle East

Elie Khoury,
Qatar Airways, Qatar

Mohamed Abdalla,
National Aviation Services, Kuwait

Mohammad Dwairi,
FIFA World Cup Qatar 2022, Qatar

Phillip Charles,
Diyar Middle East, Qatar

Mohamed Mostafa,
Alexbank, Egypt

Africa, Asia, and Australia

Aarti Jha,
Lemongrass Consulting, India

Aden Chuen Zhen Yap,
BAE Systems Digital Intelligence, Malaysia

Amber Spence,
CyberCX, Australia

Anthony Dayrit,
Allianz Singapore, Singapore

Arinze Okeke,
Dell Technologies, Nigeria

Beekah Jonah,
Nigerian Air Force, Nigeria

Harish Shankar,
GS Schneider Electric, India

Heena Rawal,
Accenture, India

Himanshu Sharma,
Bugsbounty.com, India

Kunal Malhotra,
HCL, India

Nick Schoeffler,
Google, Australia

Shiv Kataria,
Siemens, India

Srivatsa Shashikumar,
LTI, India

Sumanta Haldar,
PricewaterhouseCoopers, India

Swapnil Sonawane
Reserve Bank Information Technology, India

Vishal Sheelwant,
Maharashtra cyber digital crime unit, India

CYBERSECURITY CHALLENGES AND GAINS IN 2022

Although all the data for 2022 are not yet compiled, a picture can be inferred from the incident reports and research findings that emerged throughout the year. To cite just a few examples:

- Cyberattacks against Ukraine's government took place prior to Russia's invasion early in 2022. Hackers also targeted the communications and defense systems of Ukraine's sympathizers, including the U.S. and NATO (NSA, 2022).
- Ransomware grew by 41% in the year prior to March 2022, according to an IBM study (IBM, 2022).
- Multiple ransomware attacks threw Costa Rica into disarray in the spring, impacting businesses and healthcare systems. The U.S. government and Microsoft stepped in to combat the cyberterrorism (Sayegh, 2022).
  Cybersecurity authorities in the U.S., Australia, Canada, and UK issued a joint advisory in September, highlighting ongoing advanced persistent threat (APT) activity related to ransomware operations originating in Iran. The threat actors were exploiting known Fortinet, Microsoft Exchange, and VMware Horizon Log4j vulnerabilities (CISA, 2022).

These accounts may seem to suggest that the situation is dire and getting worse, but that level of pessimism is not warranted. In fact, ethical hackers and other cybersecurity professionals took bold, fast action to repudiate many of the threats their organizations encountered in 2022 and to reinforce their defenses against future attempts.

Organizations broadened their recruitment efforts, resulting in more diversity and flexibility in their staffs. Many found the means to offer higher wages and to improve workplace culture and working conditions. For many organizations, adequate training and onboarding of staff were no longer viewed as luxuries (Coker, 2022).

While organizations worked to bolster their cybersecurity ranks, many individual professionals made personal contributions beyond the call of duty, mentoring newcomers to the field and volunteering for projects to better secure their communities.

For C|EH Hall of Fame finalists and awardees, the evolution of challenges in the past year is part of a continuum that extends across the entire span of their careers. Many have long been active combatants in the cybersecurity trenches, while others are relative newcomers offering fresh infusions of energy. Their combined experiences are reflected in this report

In 2022, organizations recognized the importance of having a diverse and flexible staff to deal with the ever-evolving cybersecurity landscape. They broadened their recruitment efforts, resulting in more diversity and flexibility in their staffs. Many organizations also found ways to offer higher wages and to improve workplace culture and working conditions, recognizing the importance of investing in the training and onboarding of their staff.

Individual professionals also played a crucial role in ensuring the security of their organizations and communities. They went above and beyond their job duties, mentoring newcomers and volunteering for projects to better secure their communities.

For the C|EH Hall of Fame finalists and awardees, the challenges of the past year are a continuation of the ongoing fight in the field of cybersecurity. Many have long been active in this fight, while others are newer to the field and bring fresh perspectives and energy. The experiences and insights of all these individuals are reflected in this report.

WHERE ETHICAL HACKERS TRAINED THEIR FOCUS IN 2022

To gain insight into the endeavors and accomplishments of top-performing Certified Ethical Hackers in 2022, EC-Council conducted an in-depth survey of 3,318 applicants for the C|EH Hall of Fame awards. All of these professionals had already proven their mettle by scoring 90% or better on the C|EH certification exam.

The survey respondents represented scores of industries, with their numbers concentrated heavily in the information technology, consulting, financial services and government fields (figure 2).

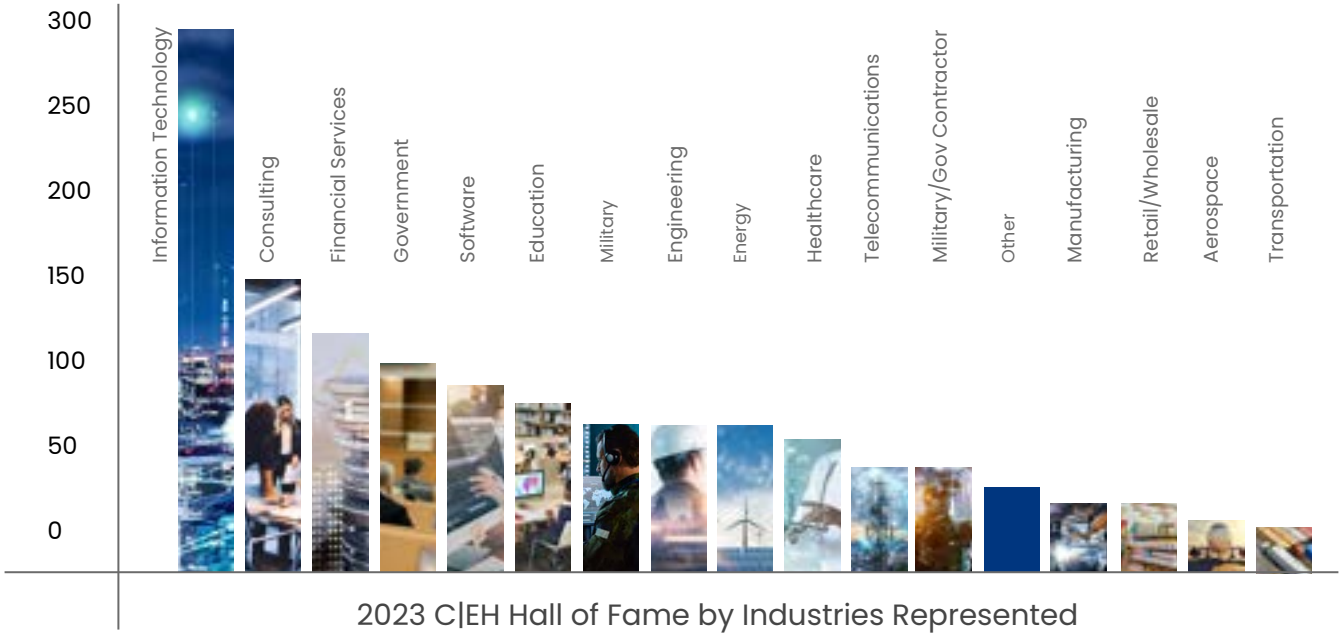


Figure 2: 2023 C|EH Hall of Fame Representation by Industry (Awardees and Finalists)

In addition to providing their personal data for the purpose of statistical analysis, participants offered a wealth of commentary on their cybersecurity-related experiences and career journeys. A sampling of their remarks is included in this report.

SECURING ORGANIZATIONAL ASSETS

The top priority for many security professionals is to improve security at their organizations, whether that means implementing new strategies and systems or optimizing those that are already in place. The skills developed in the C|EH program proved helpful in carrying out that responsibility for more than 92% of survey respondents (see figure 3), indicating that those skills have wide applications for defending organizational assets across multiple industries.

Securing organizational assets is a top priority for many security professionals, and the skills developed in the C|EH program are instrumental in achieving that goal. More than 92% of those polled found the skills they learned in the C|EH program helpful improve security at their organizations, either through implementing new strategies and systems or optimizing existing ones. The C|EH program's comprehensive curriculum covers a wide range of topics-such as penetration testing, vulnerability assessment, and incident response-that are essential for the identification and mitigation of security threats and the protection of organizational assets across a broad range of industries.

93% OF PROFESSIONALS STATED THAT C|EH SKILLS IMPROVED THEIR ORGANIZATIONAL SECURITY.

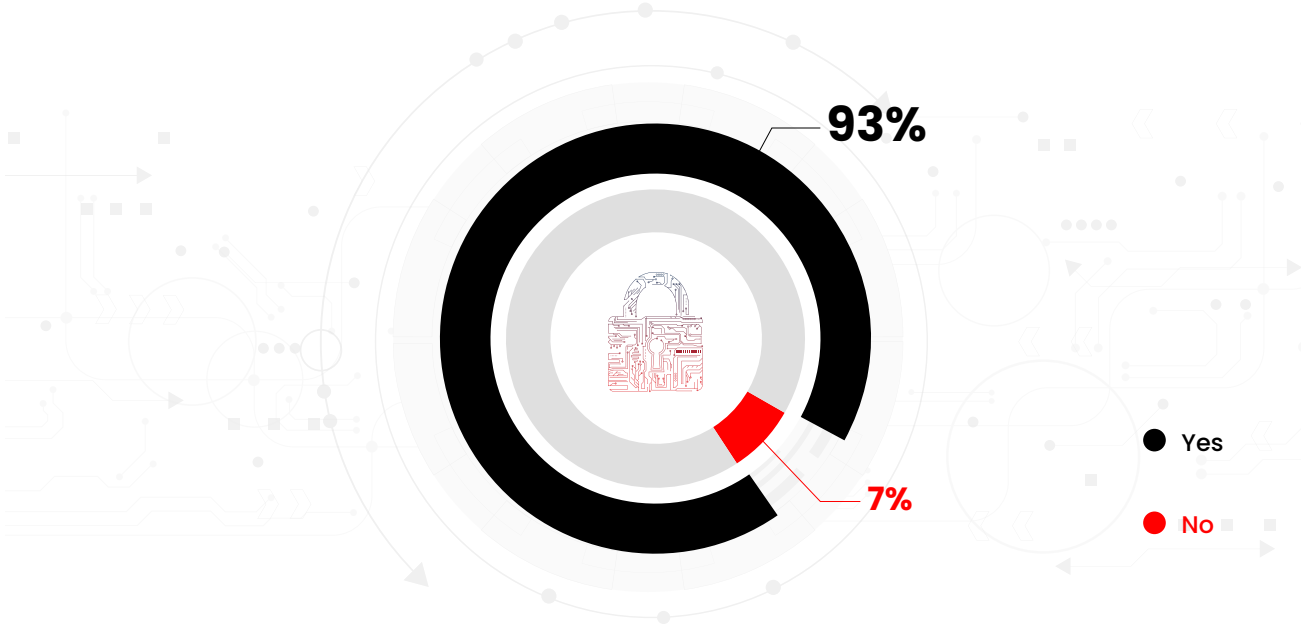


Figure 3: Value of C|EH Skills for Organizational Security

Hall of Fame awardee Sofia Nicholson, a security engineer at Microsoft in the U.S., was able to quantify one of her contributions toward improving organizational security. "**I created** detection filters that reduced false positive security alerts," she said. "This enabled the Security Operations Center to minimize attention on known activity and focus on real threats, saving the team a total of 1,784 hours of unnecessary work per month."

Thomas Aldrich, newly inducted to the Hall of Fame, neutralized an insider threat in his work on a classified project as a security officer at Lockheed Martin in the U.S. "**I monitored** and captured logs and images and successfully identified the perpetrator, which led to a successful court martial and jail time," he said.

"**I resolved** a ransomware incident in just a few hours without making any ransomware payment," reported new Hall of Fame finalist Tso Ejoe, an IT security educator at the Vocational Training Council in India.

C|EH skills helped Hall of Fame finalist Bajirao Vijaya Amol, an IT security manager for an IT managed services provider in India, strengthen his organization's security. "**I reviewed** my organization's security posture and operations from the perspective of an attacker, reconsidered the techniques for offense and defense, and contextualized pre-existing incident handling processes and procedures. Also, [these skills] helped me train my [SOC] team on the techniques explained in the C|EH training," he recalled.

"**I established** a formal penetration testing program in my organization. With this, I identified a lot of vulnerabilities and remediated all of them," said Hall of Fame finalist Akinosi Abiola, IT director at a telecommunications firm in the UAE.

C|EH alums can point to a wealth of specific contributions to their organizations, such as these examples:

- "**My team performed** over 800+ cybersecurity missions while achieving a 99.8% operational readiness rating." – Hall of Fame awardee Stephen Reid, security engineer in the U.S. Army

- "**I redefined** the security assessments service catalog and grew its business revenues to 1.2M euros from 600k." – Hall of Fame awardee Nicola Bressan, chief information officer for Yarix SRL in Italy

- "**I automated** the resolution of over 1,000 CAT II STIG vulnerabilities." – Hall of Fame awardee Brian Cochran, IT manager in the U.S. Army

- "**I conducted** a DoD Cyber Tabletop with attendance from the Office of the Undersecretary of Defense." – Hall of Fame finalist Daniel Reyes, a security engineer at Raytheon Technologies in the U.S.

- "**I led** the establishment of the Public Sector Directorate resulting in a Total Contract Value of over $21M in revenue in one year." – Hall of Fame finalist Darryl Mosley, director of the Public Sector Group at Silotech Group in the U.S.

Comprehensive Curriculum

One of the main reasons ethical hacker skills have broad applications for such a wide variety of organizations across the globe is that the C|EH curriculum is exceptionally comprehensive. In fact, more than 88% of survey respondents considered it the most comprehensive in the industry (see figure 4).

The C|EH program is widely recognized for its comprehensive curriculum, which is one of the reasons ethical hacker skills have broad applications across a wide range of organizations globally. More than 88% of survey respondents considered it the most comprehensive in the industry. The curriculum covers a wide range of topics, including penetration testing, vulnerability assessment, and incident response. It also provides hands-on experience through C|EH Labs, which allows participants to apply the knowledge and skills they have acquired in a simulated environment. The comprehensive nature of the C|EH curriculum ensures that professionals have a well-rounded understanding of the cybersecurity landscape and are equipped with the necessary skills to identify and mitigate security threats.

88% CONSIDERED C|EH TO BE THE MOST COMPREHENSIVE ETHICAL HACKING PROGRAM IN THE INDUSTRY.

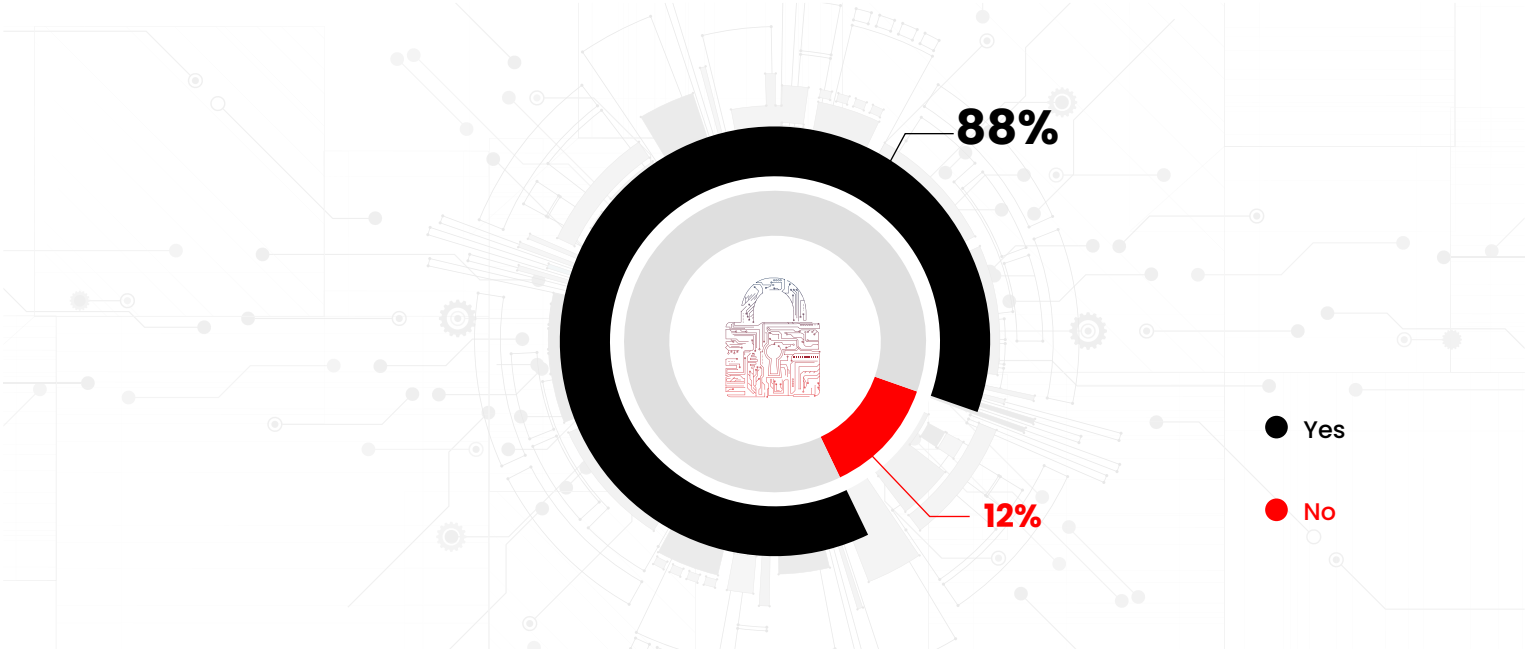


Figure 4: Comprehensiveness of C|EH Program

"C|EH is a foundational course for offensive and defensive security professionals," noted newly inducted Hall of Famer Ramin Nafisi, a security researcher at Microsoft in the U.S. "It covers a broad range of comprehensive, fundamental, and relevant security assessment topics possessed by computer and network security practitioners."

"I have not come across another certification body that offers such a broad variety of specializations," commented Hall of Fame awardee Steve Vaillancourt, a professor, educator, and trainer at the Canadian Centre for Cyber Security. "The amount of training one can leverage from EC-Council is tremendous."

One of the key ingredients in the C|EH training curriculum is C|EH Labs, which gives participants a way to safely gain hands-on experience that closely parallels the high-stakes experiences of cybersecurity professionals engaged in active combat (see figure 5).

C|EH Labs provides participants with a safe and controlled environment to gain hands-on experience. These labs are crucial in training and preparing cybersecurity professionals for the field, as they allow them to practice and apply the knowledge and skills they have learned in a safe environment that simulates high-pressure events. C|EH Labs help participants to develop their problem-solving and critical thinking skills, as well as their ability to apply their knowledge in real-world scenarios. C|EH Labs enable participants to develop a deeper understanding of the cybersecurity landscape and the many types of threats they may encounter in their careers. Overall, the hands-on experience gained through C|EH Labs is an essential component of training for cybersecurity professionals and helps to ensure they are well-prepared to meet the challenges of the field.

97% OF PROFESSIONALS FOUND C|EH LABS TO ACCURATELY MIMIC REAL-WORLD CYBER THREATS

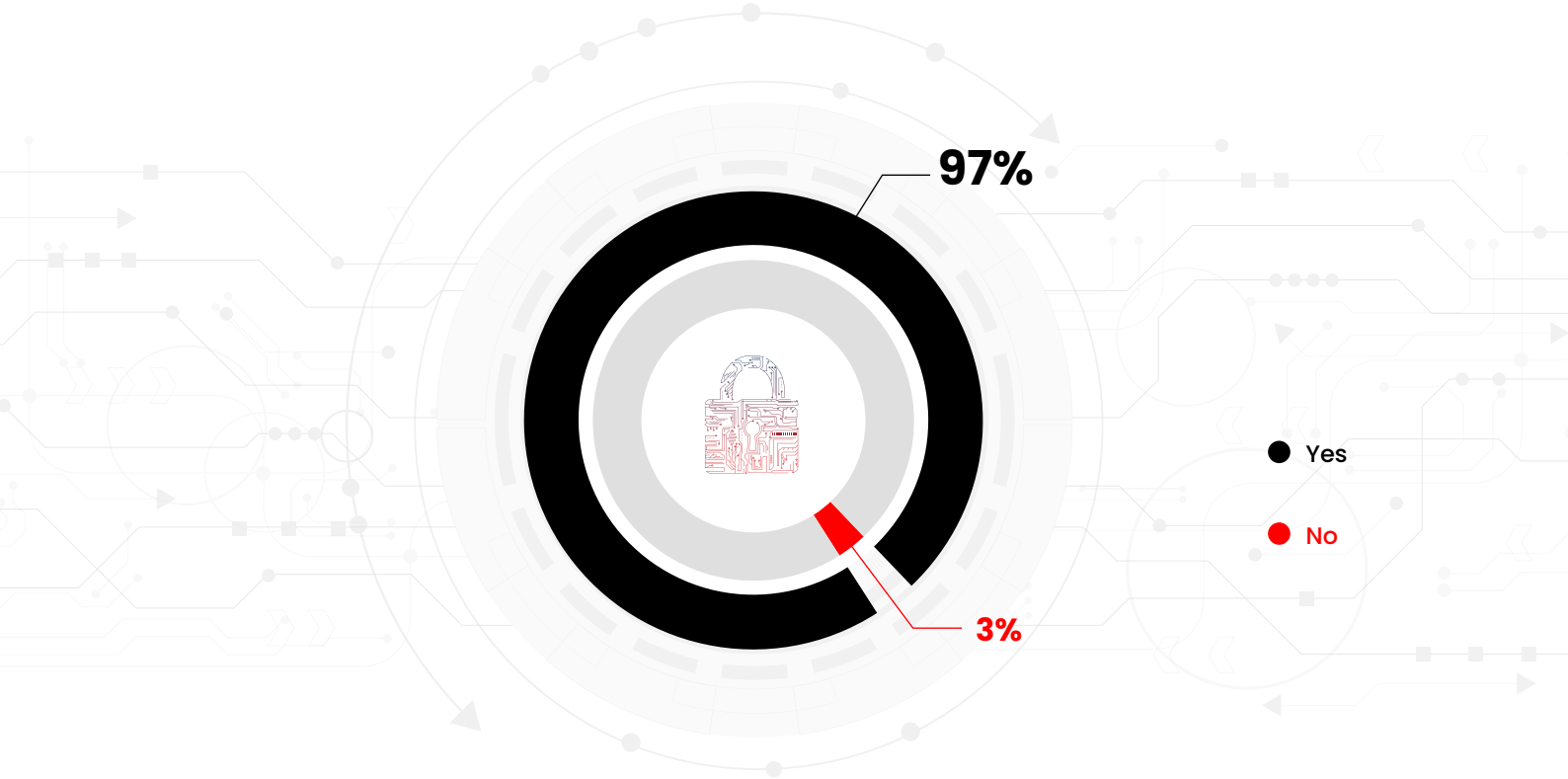


Figure 5: Simulation Accuracy of C|EH Labs

Which Sectors Need Ethical Hackers?

Certified Ethical Hackers can be found in all industry sectors, and their numbers are increasing across the board. Their specific contributions vary according to the sector's needs, but what is particularly noteworthy is that a staggering 97% of the professionals polled found the skills they acquired through their C|EH programs were relevant to their organization (see figure 6).

97% OF PROFESSIONALS STATED THAT SKILLS ACQUIRED IN C|EH HELPED SAFEGUARD THEIR ORGANIZATIONS

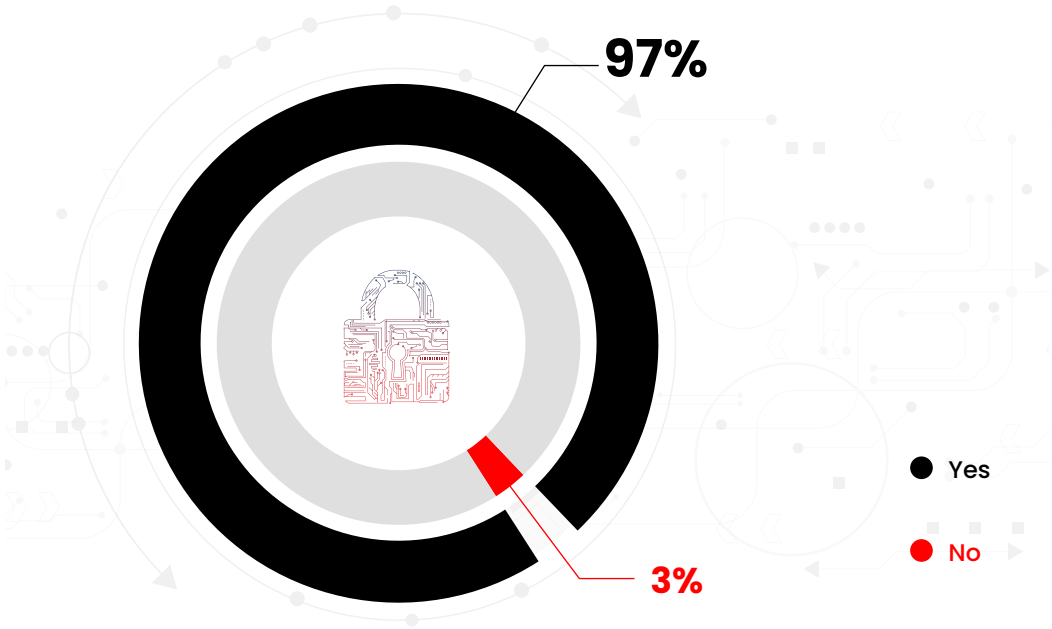


Figure 6: Relevance of C|EH Skills

Just as there are many different sectors that Certified Ethical Hackers work in, there are also many different jobs that they are hired to do. Currently, C|EH skills are in high demand and are a good fit for dozens of roles in cybersecurity including the following:

- Mid-level Information Assurance Security Auditor
- Cybersecurity Auditor
- System Security Administrator
- IT Security Administrator
- Cyber Defense Analyst
- Vulnerability Assessment Analyst
- Warning Analyst
- Information Security Analyst 1
- Security Analyst L1
- Infosec Security Administrator
- Cybersecurity Analyst level 1
- Cybersecurity Analyst level 2
- Cybersecurity Analyst level 3
- Network Security Engineer
- SOC Security Analyst
- Security Analyst
- Network Engineer
- Senior Security Consultant
- Manual Ethical Hacker
- Information Security Manager
- Junior Penetration Tester
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant
- Security Compliance Analyst
- Technology Risk and Cybersecurity Auditor

This list of job titles and responsibilities is not exhaustive and does not cover all the specialized niche roles within the field of cybersecurity. Additionally, as the cybersecurity field is constantly evolving, new roles are constantly emerging. However, there are certain capabilities that are consistently required in the field, and the C|EH program covers all of them. As one can see in figure 7, the highest percentages of survey participants reported regularly engaging in vulnerability assessment (76%), application security (62%), and penetration testing (58%) as a regular part of their work. The fewest (17%) reported working regularly on mobility security. The C|EH program provides the knowledge and skills needed for essential cybersecurity roles and prepares professionals for the coı

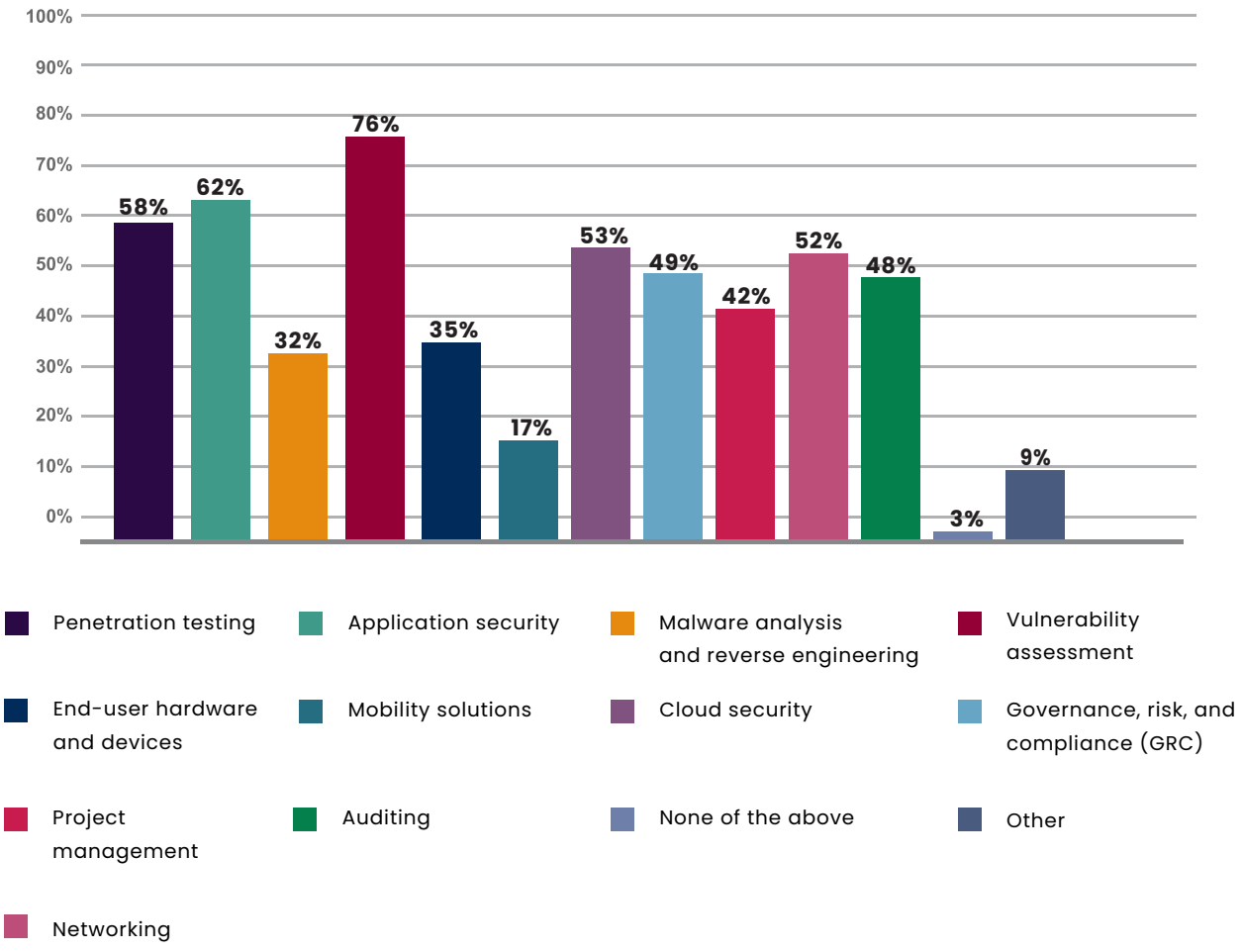


Figure 7: Application of C|EH Skills on the Job

Major Accomplishments of Certified Ethical Hackers

One of the things that drives ethical hackers to keep striving day after day is the ability to see the differences they are making—to their organizations, their communities, and the wider cybersecurity world—through very specific, concrete accomplishments. Here are just a few high points from the 2023 C|EH Hall of Famers:

I developed and implemented organizational security strategies and frameworks that reduced insider security-related breaches by 20% compared to the last three-year reports." – Hall of Fame awardee Guerrino Mazzarolo, an IT security manager for NATO in Belgium.

I developed a solution for the satellite networks to mitigate DoS and spoofing-based attacks." – Hall of Fame awardee Ali Karakoc, a security architect for IBM in the Netherlands.

I assisted our homeowners association to better secure our infrastructure. This has helped to increase the overall security for our area and residents." – Hall of Fame awardee Adam Hardinger, an IT specialist for the Department of Defense in the United States.

I spoke at DEFCON and was overwhelmed when the conference room was standing room only for my talk, with well over 1,000 people. It was aprivilege to give back to the security community by researching for several months and presenting my findings, which ultimately received the attention of ATM manufacturers and effected positive change." – Hall of Fame awardee Roy Davis, a security engineer for Zoom in the United Kingdom.

I volunteered for seven years, mentoringand coaching Cyber Patriot high school and college teams, resulting in numerous awards, grants and accolades for the schools and the students, including the following: national and state level first- and second-place awards; a mayoral letter of proclamations; HEB $100,000 grants; school board recognitions; an (ISC)² $3,000 scholarship; a Naval Academy four-year scholarship, and other college scholarships." – Hall of Fame awardee Timothy Anderson, an IT security manager for the U.S. Department of Veterans Affairs.

I won the Cyberlympics tournament in South America in 2014, one year after I got my C|EH." – Hall of Fame awardee Marcelo DaSilva, a security engineer for Microsoft in the United States.

Career Building With C|EH

All of the achievements of these ethical hackers can be traced back to one important decision: to enter the field of cybersecurity as a professional. Nearly 80% of survey respondents stated that the C|EH program was instrumental in launching their cybersecurity careers. The C|EH certification program is widely recognized as a valuable asset for professionals in the field, providing them with the knowledge and skills necessary to identify and mitigate security threats. Many professionals with C|EH certification have reported that it advanced their careers, increased their credibility and value as cybersecurity professionals, and opened doors to greater opportunities in the field. The C|EH certification is an essential step in building a successful career in cybersecurity (see figure 8).

80% OF THE HALL OF FAME FINALISTS STARTED THEIR CYBERSECURITY CAREERS WITH C|EH CERTIFICATION.

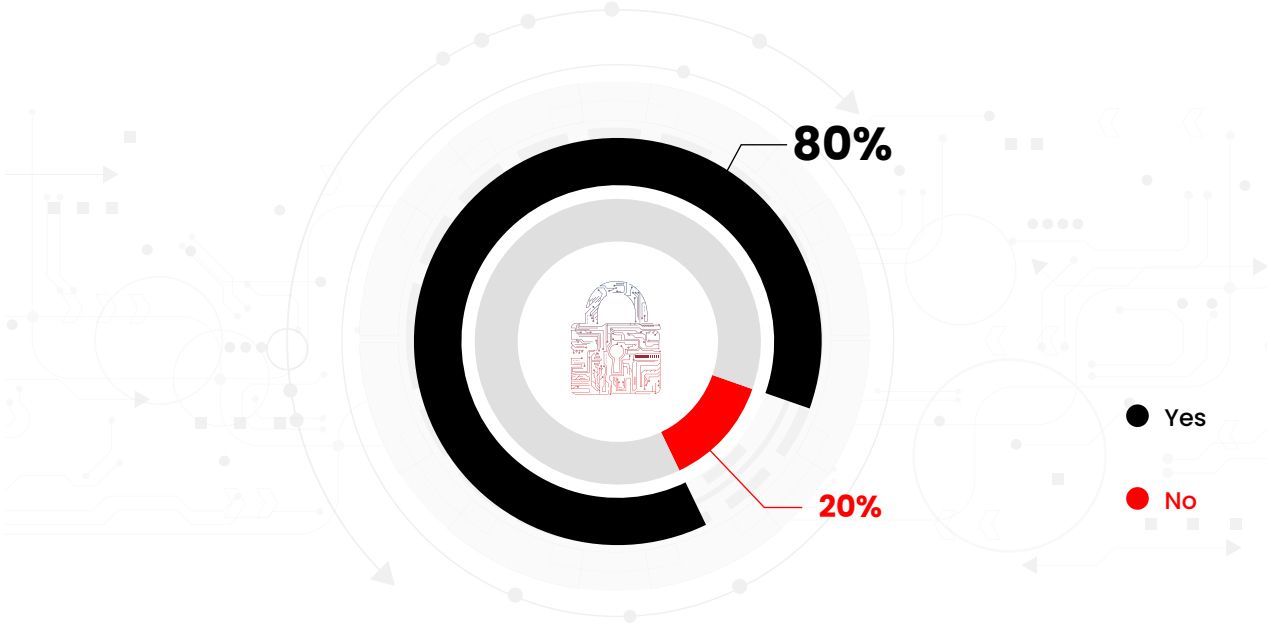


Figure 8: C|EH as Cybersecurity Career Starter

The C|EH program is a popular choice for those looking to start a career, change career direction, or advance in their chosen field in the cybersecurity industry. The decision to pursue the C|EH certification can be driven by a variety of factors. For some, the decision was handed to them by employers who recognized the value of ethical hacker skills within their organizations. However, an overwhelming number of survey respondents (95%) chose the C|EH program to advance their careers based on their own personal interests. They recognized the importance of ethical hacking skills in the field and the potential career opportunities that the certification could provide. The C|EH program is seen as a valuable asset for professionals in the field, providing them with the knowledge and skills necessary to identify and mitigate security threats and advance their careers in the cybersecurity industry **(see figure 9)**.

95% CHOSE C|EH FOR CAREER GROWTH.

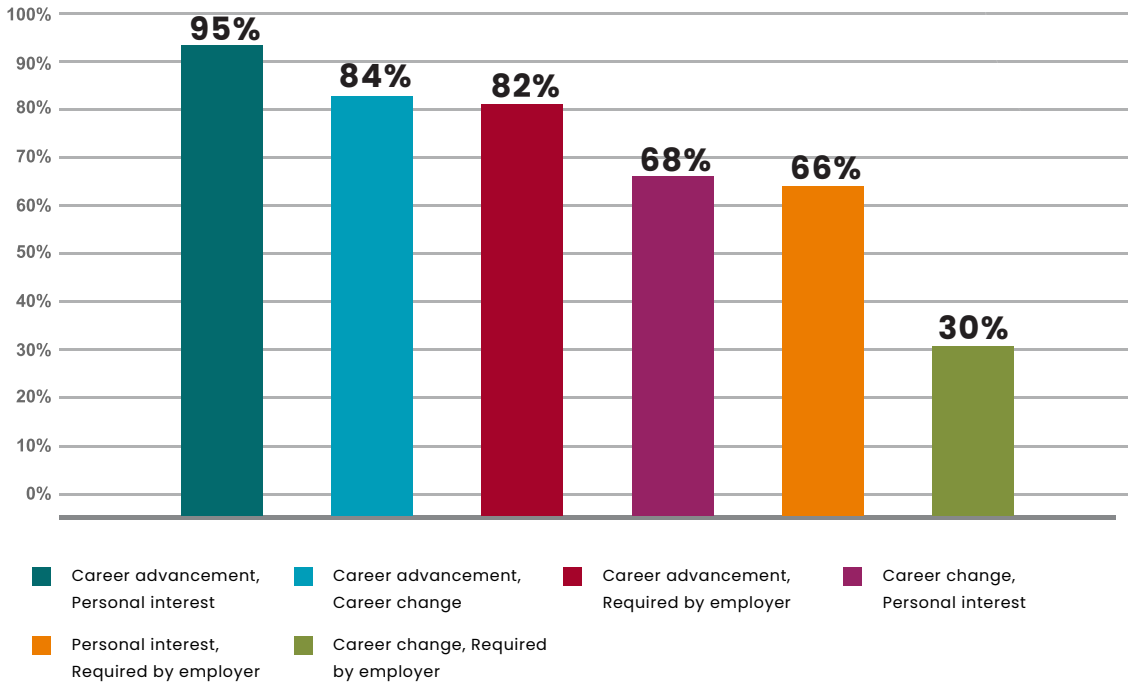


Figure 9: Reasons for Choosing the C|EH Program

One crucial requirement for anyone starting fresh in an industry or transitioning into a new career or role is confidence. C|EH Hall of Famers found that their experiences with the program helped them not only talk the talk, but walk the walk with faith in their newly-acquired capabilities. 92% of survey respondents felt that infusion of confidence, thanks to earning their C|EH credentials **(see figure 10).**

92% OF PROFESSIONALS REPORTED THAT C|EH BOOSTED THEIR SELF CONFIDENCE

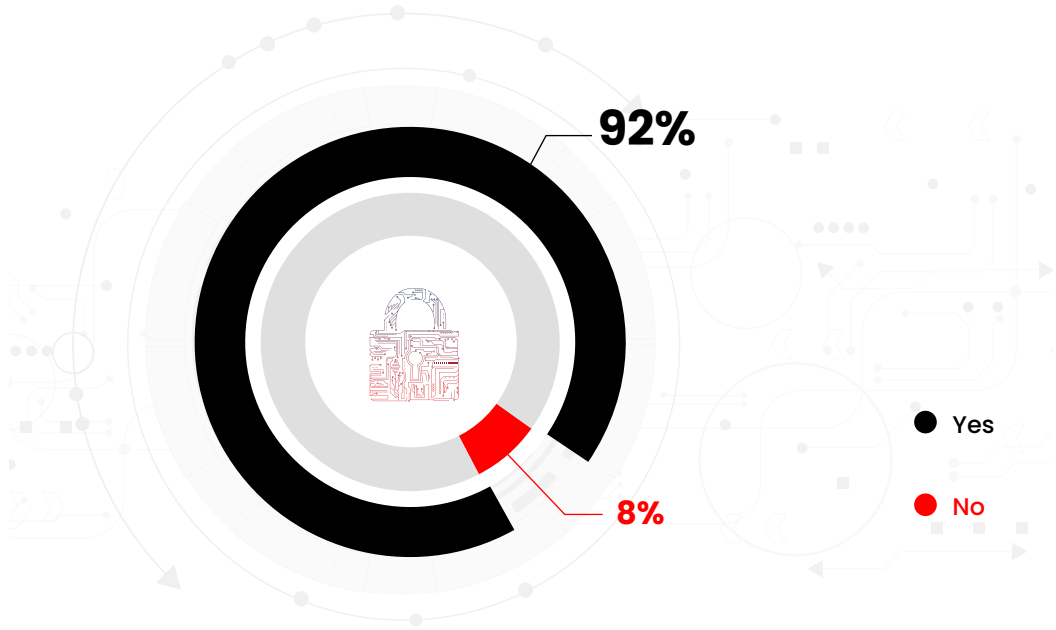


Figure 10: C|EH Impact on Confidence

The knowledge and skills gained through the C|EH program helped Hall of Fame awardee Noel Nicolas, a threat hunter for the U.S. Air Force, to speak the same language as other professionals. "It helps conversations and meetings go much faster. I can speak with confidence at these meetings to talk at a high level and a very technical level," he said.

"I can handle tasks with greater confidence, and also my colleagues are confident with my decisions," said Hall of Fame finalist Anthony Dayrit, chief information security officer at Allianz Singapore. "They also expressed keen interest to take up C|EH."

The Importance of Continuously Upgrading Skills

Few fields are as volatile as cybersecurity when it comes to major shifts due to crafty new exploits. It is critical to choose the right program when entering the cybersecurity field or changing roles. However, those major career milestones are not the only times to work on professional development. It is important to hone one's skills continuously, because threat actors are working nonstop to devise new schemes.

Successful cybersecurity professionals, including C|EH Hall of Fame awardees and finalists, are well aware of the need to maintain their positions on the leading edge of the industry through constantly deepening their expertise. A majority of survey respondents (56%) reported working on building skills on a daily basis **(see figure 11)**. Nearly 30% sharpened their skills weekly, and about 12% made time for skill development on a monthly basis. Only about 2% of those polled polished their skills once a year or less.

85% OF PROFESSIONALS SHARPEN THEIR SKILLS AT LEAST ONCE PER WEEK.

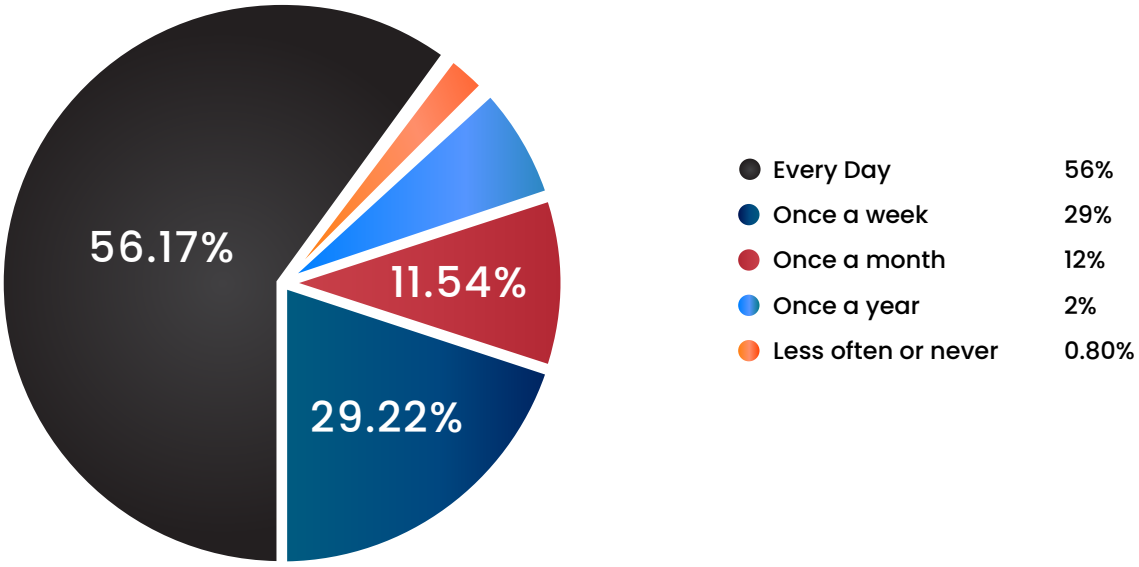


Figure 11: Time Devoted to Building Cybersecurity Skills

That relentless attention to refining their skills has paid off handsomely for C|EH Hall of Fame finalists and awardees. Many of them have risen to positions that include responsibility for making hiring decisions for their organizations. An overwhelming majority of the hiring managers among survey respondents acknowledged that they would give preference to job applicants with the C|EH certification when filling positions that require ethical hacking skills (see figure 12).

92% OF HIRING MANAGERS PREFER CANDIDATES WITH C|EH FOR JOBS THAT REQUIRE ETHICAL HACKING SKILLS.

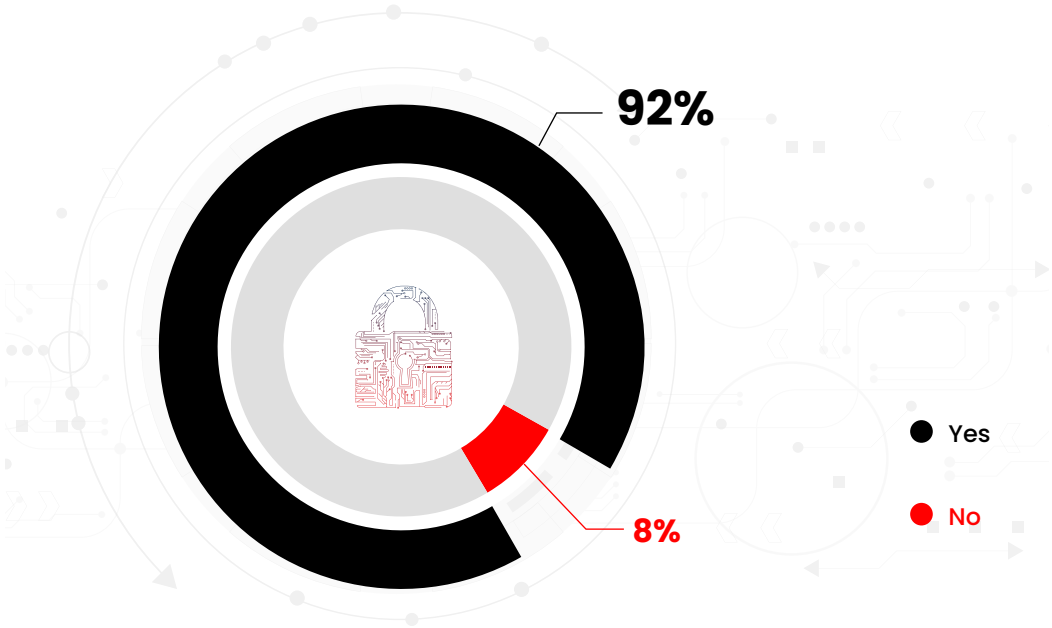


Figure 12: Preference for Job Applicants With C|EH

Impact of C|EH on Hall of Fame Awardees and Finalists

For the 1,000 professionals who were named as finalists and the 100 who were inducted into the 2023 C|EH Hall of Fame, obtaining a Certified Ethical Hacker (C|EH) certification had a significant impact on their careers. It led to advancements in their positions, increased responsibilities, and opportunities for growth, as well as recognition as leaders in the industry

Here are a just a few of their stories:

I started six year ago as a junior IPS/IDS admin and then got promoted to escalations engineer within the same department," recalled Hall of Fame awardee David Gomez, a security specialist for IBM in Costa Rica. "After four years on that team, I decided to continue my professional path with the threat monitoring team—first as a TM analyst. I was then promoted to TM escalation engineer."

I have spent my career across different domains. I started out in the helpdesk, working my way through system administration," said Hall of Fame awardee Jason Lee, a security consultant for Deloitte in the U.S. "I pivoted into networking and ultimately went into network security. I have spent the last 10 years as a network security professional, with a focus on network pentesting and remediating findings to develop secure infrastructure."

I am the chief of training and military advisor to the 16th numbered Air Force, A6IC division, under Air Combat Command for the United States Air Force," said Hall of Fame awardee Frankie Grullon, a cybersecurity professor, educator, and trainer for the U.S. Air Force. "I am responsible for the curriculum development, instruction, and management of the AF intelligence community's training division program. I also provide senior leaders with strategic and tactical employment of Air Force resources for specialized cyber and intelligence mission sets. I am fully qualified in the domain of cyberspace and information operations. I have over 21 years of experience, starting as a humble help desk administrator and eventually working my way to becoming a director of information technology and chief cyber information security officer. My experience has ranged from the medical and education fields to government sectors in both contractor and public servant roles. I also run my own nonprofit cybersecurity firm that teaches cyber dangers to underprivileged and disadvantaged communities."

I'm managing alliance partners focusing on expanding security offerings available on the Google Cloud Platform—working closely with companies including Palo Alto Networks, Exabeam, and Elastic to deliver end-to-end security offerings for Google's customers," said Hall of Fame awardee Nick Schoeffler, technology partnerships lead, security, for Google in Australia. "I worked for almost 20 years at Microsoft in their consulting and sales businesses—providing solutions, consulting, and architecture to all industries with a focus on modern workplace technologies and securing their environments. My last three years have been with Google, managing one of their key businesses and being a regional spokesperson for security in the workplace."

I remember when I read my first book named Hacking University. It was my first trigger, and then I fell in love with cybersecurity," said Hall of Fame finalist Ciro Jesus, IT security director at Oiti, a financial services firm in Brazil. "So, I decided to direct my hacking studies in 2013. In 2018 I started planning the Cyber Security Labs development strategy at Logicalis and it motivated me a lot. I received a challenge in Bogota, Colombia—I spent three months developing a SOC and cyber processes for a financial customer. I used the NIST Incident Handling Guide a lot to structure the incident response processes. I recently joined Oiti, and we are evolving the cybersecurity program, building more security controls. I am very happy to be here and to increase cybersecurity maturity in a company that places security as a strategic pillar. I'm really excited about everything around here and I hope that C|EH will also help me on this path."

MANY C|EH HOLDERS CREDITED CERTIFICATION AS A MAJOR FACTOR IN GETTING PROMOTED AND ACHIEVING CAREER SUCCESS.

Promotion within 6 months…"

Ahmar Rizwan, Tata Consultancy Services

I received a promotion to the top tier in the government…"

Ahmar Rizwan, Tata Consultancy Services

Promoted as head of red team after one year as specialist…"

Nicola Bressan, Yarix SRL

Promotion to the position of a Senior Consultant after one year of joining KPMG…"

Boluwarin Aremu, KPMG, Nigeria

Achieving the rank/promotion of E-8 in the USAF as a cyber professional…"

Krystal Hughes, USAF

I was promoted to the next level after showing the security control implementation to protect the organization's ICT environment with learning from C|EH."

Boluwarin Aremu, KPMG, Nigeria

After taking the C|EH program, I am getting promoted because of thinking out of the box and addressing the issues very well and mitigating the risk at an acceptable level."

Vaibhav Pandya, Etek International

I started in my current company as cybersecurity analyst for three years. Then I was promoted to cybersecurity manager last year and this year I have been promoted to CISO."

Jesus Abascal, ClarkeModet

Being promoted to L2 level in SOC operations..."

Sidhartha Priya, EY

C|EH helped me to advance my career by looking into a more senior role and getting an early promotion in my professional life..."

Muhammad Taha, CanadianCyber

Got promoted to SOC supervisor..."

Hussam Bokhari, Saudi National Bank

Being promoted to a team lead role after working for a year in a Big 4 firm..."

Neil Kendall, Nuclear Decommissioning Authority

Consistent growth and promotions and building world class teams in cybersecurity..."

Sakthiswaran Rangaraju, WMware

Got promoted as assistant manager..."

Rayudu Babu, Standard Chartered Bank GBS

The Influence of C|EH on the Cybersecurity Community

From their accounts, it is clear that possessing cybersecurity skills-and, in particular, ethical hacking opens countless doors to career success and personal fulfillment. As great as raises, promotions, and increased professional recognition are, they are not the only objectives for C|EH top performers.

A great many Hall of Fame finalists and awardees make meaningfulcontributions to strengthening the cybersecurity field overall through mentoring, training, educating the public, and many other activities. Of those surveyed, 85% expressed their satisfaction in being able to share their expertise in volunteer capacities and credited the C|EH program with making it possible (see figure 13).

85% OF PROFESSIONALS CREDITED C|EH TO HELPING THEM GIVE BACK TO THE CYBERSECURITY COMMUNITY

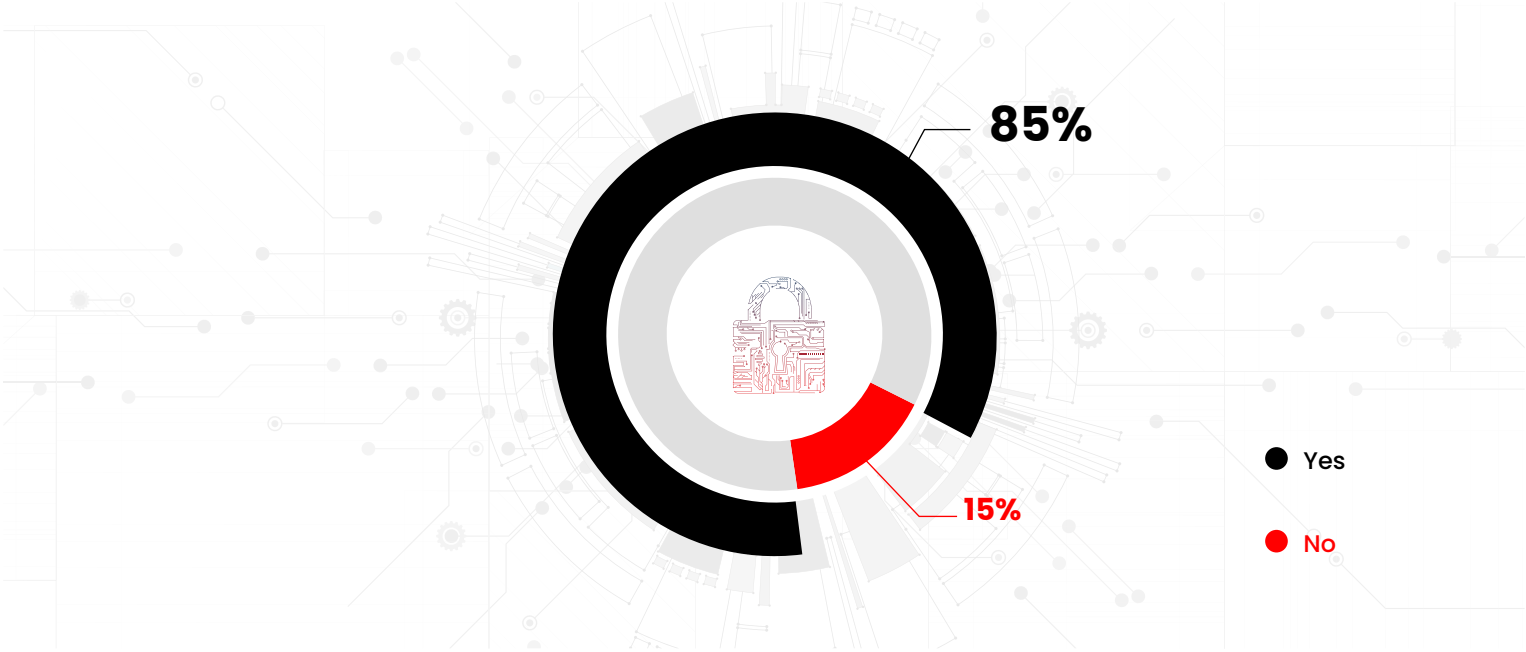


Figure 13: C|EH as Facilitator of Community Contributions

By providing glimpses into their world, C|EH Hall of Fame awardees and finalists have contributed much more than information about their career trajectories. They have communicated the driving force that propels them toward achieving their organizations' objectives and reaching their own personal goals: a passionate interest in making the world safer and more secure.

BLAST FROM THE PAST

100

Certified Ethical Hacker Hall of fame Awardees 2021-2022

View Now

C|EH Certified Ethical Hacker

C|EH Hall of Fame Report 2021-2022: Leaders of the Ethical Hacking Community 2021-2022

Read Report

ABOUT EC-COUNCIL

The International Council of E-Commerce Consultants, also known as EC-Council, is the world's largest cybersecurity technical certification body. It operates in 145 countries globally and is the owner and developer of the world-famous Certified Ethical Hacker (C|EH), Computer Hacking Forensics Investigator (C|HFI), and License Penetration Testing (Practical) programs, among others. EC-Council has trained and certified more than 200,000 information security professionals who have influenced the cybersecurity mindset of countless organizations worldwide.

EC-Council was founded by Jay Bavisi in 2001, in the aftermath of the 9/11 attacks in the United States. Its mission is "to validate information security professionals who are equipped with the necessary skills and knowledge required in a specialized information security domain that will help them avert a cyberconflict, should the need ever arise" (EC-Council, About Us, n.d.). The organization is committed to upholding the highest level of impartiality and objectivity in its practices, decision making, and authority in all matters related to certification.

EC-Council's certification programs are approved under the United States government's Montgomery GI Bill®. Furthermore, the US Government National Security Agency (NSA) and the Committee on National Security Systems (CNSS) have certified EC-Council's Certified Ethical Hacking (C|EH), Certified Network Defender (C|ND), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), and Licensed Penetration Tester (LPT) programs for meeting the training requirements for information security professionals set forth in standards 4011, 4012, 4013A, 4014, 4015 and 4016). EC-Council is also accredited by the American National Standards Institute (ANSI).

REFERENCES

Coker, J. (2022, October 20). "Cybersecurity Workforce Gap Grows by 26% in 2023 ." InfoSecurity Magazine. https://www.infosecurity-magazine.com/news/cybersecurity-workforce-gap-grows/

Cybersecurity & Infrastructure Security Agency (CISA). (2022, September 14). "Iranian Islamic Revolutionary Guard Corps-Affiliated Cyber Actors Exploiting Vulnerabilities for Data Extortion and Disk Encryption for Ransom Operations." https://www.cisa.gov/uscert/ncas/alerts/aa22-257a

EC-Council. (n.d.). "About Us." https://www.eccouncil.org/about/

Fortinet. (2022). 2022 Cybersecurity Skills Gap. https://www.fortinet.com/content/dam/fortinet/assets/reports/report-2022-skills-gap-survey.pdf

Iacono, L., Wojcieszek, K., Glass, G. (2022 , November 8). "Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022 ." Kroll. https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse

IBM. (2022). "Cost of a Data Breach Report 2022." IBM Security. https://www.ibm.com/resources/cost-data-breach-report-2022

National Security Agency (NSA). (2022, December 15). NSA Cybersecurity 2022. chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/0139_CSD_YIR22_FINAL_LOWSIDE_ACCESSIBLE_FINAL_V2.PDF

Powell, O. (2022, December 2). "The top 10 hacks and cyber security threats of 2022." Cyber Security Hub. https://www.cshub.com/attacks/articles/the-top-10-hacks-and-cyber-security-threats-of-2022

Sayegh, E. (2022 , December 13). "2022 In Review: An Eventful Cybersecurity Year." Forbes. https://www.forbes.com/sites/emilsayegh/2023/12/13/2022-in-review-an-eventful-cybersecurity-year/?sh=45559690352f

EC-Council
Learning Track

Executive

EXECUTIVE LEADERSHIP

C|CISO Certified Chief Information Security Officer

Specializations

VULNERABILITY ASSESSMENT & PEN TESTING	NETWORK DEFENSE	INCIDENT HANDLING & RESPONSE	APPLICATION SECURITY	BLOCKCHAIN
	INDUSTRIAL CONTROL SYSTEMS & SUPERVISORY CONTROL AND DATA ACQUISITION ISC / SCADA			
	IOT C|IP Certified IoT Professional			
C|PENT Certified Penetration Testing Professional	THREAT INTELLIGENCE C|TIA Certified Threat Intelligence Analyst	DISASTER RECOVERY EC-Council Disaster Recovery Professional	DEVSECOPS E|CDE EC-Council Certified DevSecOps Engineer	B|DC Blockchain Developer Certification
WEP APP HACKING W|AHS Web Application Hacking & Security	CLOUD SECURITY C|CSE Certified Cloud Security Engineer	INCIDENT RESPONSE E|CIH EC-Council Certified Incident Handler	C|ASE .NET Certified Application Security Engineer	B|FC Blockchain Fintech Certification
C|EH Certified Ethical Hacker MASTER	SOC ANALYST C|SA Certified SOC Analyst	DIGITAL FORENSICS C|HFI Computer Hacking Forensic INVESTIGATOR	C|ASE JAVA Certified Application Security Engineer	B|BLC Blockchain Business Leader Certification

Core

ETHICAL HACKING
C|EH Certified Ethical Hacker

NETWORK DEFENSE
C|ND Certified Network Defender

Cyber Technician

CYBER TECHNICIAN
C|CT Certified Cybersecurity Technician

Cyber Essentials

ESSENTIALS SERIES
N|DE Network Defense Essentials
E|HE Ethical Hacking Essentials
D|FE Digital Forensics Essentials

SECURITY SPECIALIST
E|CSS EC-Council Certified Security Specialist

Knowledge Workers

CYBERSECURITY AWARENESS
C|SCU Certified Secure Computer User

PHISHING AWARENESS
aware

Individual Courses

ENCRYPTION
E|CES EC-Council Certified Encryption Specialist

codered FROM EC-COUNCIL

World's Largest Online Cybersecurity Course Library

www.eccouncil.org

EC-Council

www.eccouncil.org

EC-Council's mission is to help organizations, educators, governments, and individuals address global workforce problems by developing and curating world-class cybersecurity education programs and certifications while providing cybersecurity services to some of the largest businesses around the world. EC-Council is trusted by seven of the Fortune 10, 47 of the Fortune 100, the Department of Defense, global intelligence communities, NATO, and more than 2,000 of the best universities, colleges, and training companies. EC-Council programs have made their way to more than 140 countries and have set the bar in cybersecurity education. To learn more, visit https://www.eccouncil.org/.