EC-Council

Leaders of the Ethical Hacking Community 2021

A C|EH Hall of Fame Annual Report

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

C|EH Certified Ethical Hacker

www.eccouncil.org

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. 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.

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.

www.eccouncil.org/ceh-hall-of-fame/

Contents

2021 C|EH Hall of Fame Annual Report

1

Acknowledgment and Foreword

This report would not be possible without the generosity of the 2021 C|EH Hall of Fame nominees and finalists in sharing their experiences and perspectives on their personal cybersecurity journeys. We are grateful for their contributions, which have proven invaluable for this analysis.

Cyber adversaries have been stepping up their efforts to compromise the integrity, availability, and confidentiality of data belonging to organizations, governments, and individuals all over the world. To meet the growing threat, a workforce with the right knowledge and skills is essential. However, just when more and better-trained professionals are needed, the cybersecurity skills gap has widened.

This report highlights the importance of training and certification—specifically, the Certified Ethical Hacker (C|EH) program offered by EC-Council—in growing a cybersecurity talent pool to fill the hundreds of thousands of vital positions that remain open today. It also highlights the role of skills training for increasing job satisfaction of those working in the field. The right training not only increases the supply of new entrants but also encourages the retention of indispensable middle- and upper-tier professionals by opening doors to exciting and lucrative career specializations.

> To close the skills gap, cybersecurity training is essential.

Key Takeaways

REPORT HIGHLIGHTS

- Cyberthreats are increasing in volume and sophistication, exacerbating skill shortage globally
- Demand for cybersecurity talent far exceeds supply
- To close the skills gap, cybersecurity certification is essential
- Cybersecurity certifications are essential in closing the industry's skills gap
- C|EH builds skills that help thwart ransomware
- C|EH certification opens doors to government careers
- C|EH builds communities
- The hands-on C|EH training improves job readiness
- C|EH-certified professionals have extensive industry experience
- C|EH certification boosts hiring and salary potential

Hall of Fame 2021

3500+ Applicants

900 Finalists

100 Awardees

59 Countries

Top 10

The C|EH ranks in the top 10 most widely recognized, important, and required certifications for both beginning and established cybersecurity professionals.

79% ▲

of C|EHs reported a salary increase of more than 20% compared with their peers.

84%

of IT employers who responded to a survey released in February 2020 considered cybersecurity certifications like the C|EH to be the gold standard when hiring.

50%

of C|EH Hall of Fame nominees and finalists work in the IT industry.

#4

The C|EH was ranked fourth in an opinion poll ISCN conducted of its 90,000 LinkedIn members on the 50 leading cybersecurity industry certifications and courses.

21% ▲

of C|EHs reported a salary advantage of at least 40% over their peers.

3

Introduction

Each year, EC-Council recognizes the top performers of the C|EH program—those who score 90% and above on the C|EH certification exam. The top performers receive an invitation to apply to the C|EH Hall of Fame.

In 2021, out of thousands of applications, 1,000 cybersecurity professionals were shortlisted for the first round. From that pool of finalists, only 100 professionals were inducted into the EC-Council Hall of Fame based on their capabilities, achievements, career growth, and contributions to the community.

The 2021 C|EH Hall of Fame nominees and finalists represent 59 countries spread across the globe (Figure 1).

These participants are much more than a group of talented ethical hackers. They represent a new hope in the battle to reverse current global threat trends by narrowing the cybersecurity skills gap. C|EH Hall of Fame nominees and finalists not only make positive individual contributions toward mitigating cyberthreats but also inspire others through their teaching, mentorship, and example. They play a pivotal leadership role in increasing the number of well-prepared applicants for cybersecurity job vacancies around the world.

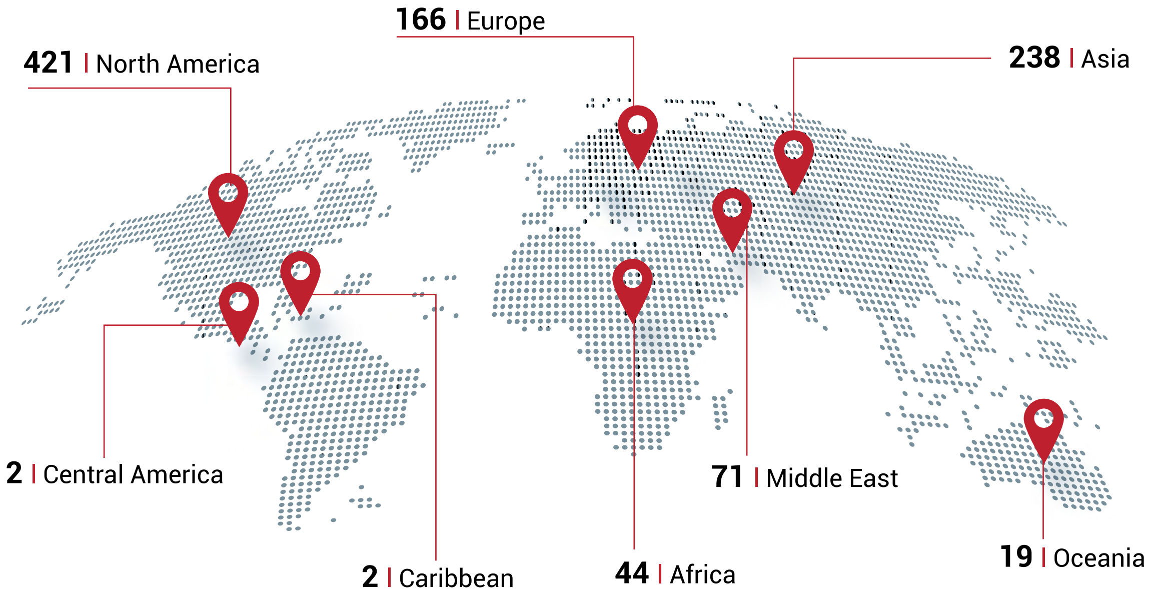


Figure 1: C|EH Hall of Fame 2021 Participation by Region (Nominees and Finalists)

Source: EC-Council

C|EH™
Certified Ethical Hacker

Hall of Fame

2021

Celebrating Ethical Hackers

Honoring the Best and Brightest in Our Global Community

The C|EH Hall of Fame 2021 nominees are employed at:

Microsoft	FedEx Express	Infosys	Standard Chartered	IBM
DELL	pwc	Trustwave	FOXCONN	proximus
amazon	Deloitte.	ORACLE	hp	REPSOL
T · ·	STEDIN.NET	citi	NetApp	SECURITY
FirstBank	JPMorganChase	YOKOGAWA	IoT.nxt bridging the edge	Lenovo
cisco	appknox	entsika	CDW PEOPLE WHO GET IT	DEPARTMENT OF DEFENSE 50 COMMEMORATION
LOCKHEED MARTIN	NTT DaTa	CiTRiX	Kellogg's	EY Building a better working world
ManTech International Corporation	opentext™	Tech Mahindra	TATA TATA CONSULTANCY SERVICES	HCL HCL TECHNOLOGIES
DEFENSE HEALTH AGENCY DEPARTMENT OF DEFENSE	U.S. DEPARTMENT OF COMMERCE BUREAU OF THE CENSUS	STATE TREASURER THE SEAL OF THE ... OF WEST VIRGINIA	Raytheon Technologies	REPUBLIC OF TURKEY MINISTRY OF HEALTH GENERAL DIRECTORATE OF PUBLIC HEALTH
Npo	THE UNIVERSITY OF SCRANTON A JESUIT UNIVERSITY	日本総研 The Japan Research Institute, Limited	SBER	DAIMLER
IPKeys	KSM Castings	HADEF & PARTNERS		Schlumberger
	K.T. UNIVERSITY	جامعة آل البيت Al albayt University	lightech	NOTE MACHINE
MK College	ALVAREZ & MARSAL		HONDA The Power of Dreams	عمانتل Omantel

Disclaimer:
Any product names, logos, brands and/or other trademarks or images featured or referred to are the property of their respective owners and are not intended to imply endorsement or sponsorship by any of these companies of any EC-Council products or services. They are intended to represent the companies that C|EH Hall of Fame nominees work at. All company logo's, names, product and service names used in this report are for identification purposes only.

C|EH Hall of Fame 2021 Awardees

(in alphabetical order by region)

America (North and South)

Adrian Guillen Brizuela
Kelloggs, USA

Alexander Kem
Amazon, USA

Anna Boom
Cisco, USA

Babashola Madariola
Madarson IT, USA

Brad Bitterman
Lenovo, USA

Christopher Moore
Cook County Sheriff's Dept.
USA

Christos Simotas
CAE, Canada

Cory Miller
Citrix, USA

Daniel Bechtel
Deloitte & Touche, USA

Denis Cyrillo
Honda, Brazil

Diego Pereyra
Lightech S.A., Argentina

Edgar Diaz Huerta
Ceico ITT S.A. de C.V.,
Mexico

Eduardo Naranjo Pessota
Tecnologia Bancária
S.A. Brazil

Fasihuddin Qureshi
U.S. Department of
Commerce, USA

Fuad Mustapha
CDW, Canada

Gilberth Contreras
IBM, Costa Rica

Giulio Astori
Microsoft, USA

Greg Cottingham
Microsoft, USA

Haslyn Martin
Citi, USA

John Branch
NTT Data, USA

Joshua Erwin
Deloitte, USA

C|EH Hall of Fame 2021 Awardees — America (North & South)

Juan Torres
Herbalife, Mexico

Juan Sanchez
22nd Century Technologies Inc. USA

Justen Long
ManTech International Corporation, USA

Khagani Jamal Aydin
Microsoft, USA

Kiedra Gerl
D.R. Horton, USA

Leo Colmenares
Lockheed Martin, USA

Michael Bhim
ANSI, USA

Michael Peters
RIMS, USA

Michael Turner
Lockheed Martin, USA

Michael Williams
Raytheon Technologies, USA

Mehmet Bastug
University of Scranton, USA

Nathan Van Vliet
NetApp, USA

Nkoli Emelife
Deloitte, USA

Olanrewaju Ogunsanmi
IPKeys Technologies, USA

Olatunji Taiwo
JPMorgan Chase, USA

Paul Rogers
Oracle, USA

Ralphaella Beal
Deloitte, USA

Rex Crouser
West Virginia State Treasury, USA

Richard Medlin
Information Warfare Center, USA

Richard Yinchun Zhou
OpenText, USA

Riley Bender
Booz Allen Hamilton, USA

Robert Kayl
Defense Health Agency, USA

S. Raschid Muller, Ph.D.
Department of Defense, USA

Sardor Kasymov
NCR Corp., USA

Sheena Grewal
BAE Systems, USA

Sidhant Gupta
EY, USA

Smail Dahmoun
KSM Castings, USA

Tim Cavanaugh
Maiden Global Servicing Company, LLC, USA

Tyler Krist
Deloitte, USA

Yakov Shmelev
PwC, USA

Yuri Novikov
LoyaltyOne,
Canada

C|EH Hall of Fame 2021 Awardees

Europe

Adam Pogorzelski
T-Mobile, Poland

Charalampos Athanasoulas
Hellenic Navy, Greece

Franco Bellotti
Npo Sistemi, Italy

Ignacio Urioste Sanchez
Repsol, Spain

James Booth
Milton Keynes College,
United Kingdom

Juan Rafael Villén Pulido
Mercedes-Benz AG, Spain

Kumara Rangaiah
FedEx,
Netherlands

Leon Stok
Yokogawa Europe,
Netherlands

Mahdi Rahimi Ghazi Kalayeh
Codemetrix GmbH,
Germany

Marco Seidler
Daimler, Germany

Natacha Bakir
HP, Switzerland

Nick Mitropoulos
Alvarez and Marsal,
Greece

Nikos Vrakas
IBM, Greece

Paul Mahoney
Notemachine UK Ltd.
United Kingdom

Peter Berends
Stedin, Netherlands

Peter Duku
Parliament,
United Kingdom

Ruben Amzallag
Accenture,
France

Stijn Huyghe
Proximus, Belgium

Timo Sablowski
Fashion Digital GmbH
& Co. KG, Germany

Tomáš Sova
Foxconn EMEA, Czech
Republic

Tobie Alberts
IoT.nxt, Netherlands

Middle East

Abdul Rahman
Omantel,
Oman

Ariston D’Souza
Hadef & Partners LLC,
United Arab Emirates

Gader Al-Khawaldeh
Al al-Bayt University, Jordan

Karl Biron
Trustwave,
United Arab Emirates

Maxim Balin
Dell, Israel

C|EH Hall of Fame 2021 Awardees

Africa, Asia, and Australia

Abiodun Soyombo
Gateway Mortgage Bank, Nigeria

Anupum Jaiswal
HCL Technologies, India

Arvind Kumar
TCS, India

Ashish Mohanty
Annapurna Finance Pvt. Ltd., India

Carol Lee
Hang Lung Properties Limited, Hong Kong

Cynthia Rethnasamy
Microsoft Surface, Malaysia

Denis Ratchenko
Schlumberger, Russia

Erdal Ozkaya
Standard Chartered Bank, Australia

Harsimran Singh
Tech Mahindra, India

Javed Shaik
Cisco, India

Jithin Joseph
MicroCenter Group, India

Karthik Sunkenepalli
Tech Mahindra, India

Mustafa Cicek
Turkish Ministry of Health, Turkey

Nipun Siddhrau
State Bank of India, India

Raymond Lee
Japan Research Institute Ltd, Singapore

Sai Vanka
Deloitte, India

Saket Taneja
Appknox, India

Saurabh Sinha
UnitedHealth Group, India

Shubham Verma
Infosys, India

Siddhardha Goparaju
KL University, India, India

Takudzwa Tsotsonga
Entsika Consulting Services, South Africa

Zechariah Akinpelu
Unity Bank, Nigeria

The Skills Shortage in Cybersecurity

How serious is the current skill shortage in the cybersecurity industry, and what are the potential negative consequences if it's not addressed?
"It's scary. I don't think the companies realize the problems around the corner. There's just not enough skilled labor out there," said Jeff Macre, cybersecurity project manager at 1898 & Co. (Bowcut, Labor Shortage, 2021). "Currently, there's 597,000 job openings just here in the United States. That's actual openings—that's not a projected number."

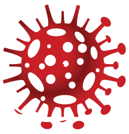
Cyberthreats Are Increasing in Volume and Sophistication, Exacerbating the Global Skill Shortage

At the same time, the number of cyberattacks has been climbing sharply upward. Based on a survey of IT and business decision makers conducted in fall 2021, McAfee Enterprise and FireEye concluded that 81% of global organizations experienced increased cyberthreats during the COVID-19 pandemic (McAfee and FireEye, 2021).

Multinational networking giant Cisco analyzed internet traffic spanning 190 countries for its 2021 threat trends report and found that cryptomining, phishing, ransomware and trojans were the dominant threats in 2020. The firm noted "a continuation of the trend we have been seeing toward more complex, multi-staged attacks that involve multiple threat types" (Cisco, 2021).

That complexity was evident in the massive SolarWinds supply chain attacks that occurred in 2019-2020, which had major repercussions for roughly 18,000 government agencies and businesses around the world, including the United States Departments of Justice, State, Treasury, Energy, and Commerce. From a software engineering perspective, SolarWinds "is the largest and most sophisticated attack the world has ever seen," Microsoft President **Brad Smith** said in an interview on *60 Minutes* (Whitaker, 2021).

Developing more sophisticated cybersecurity defense strategies and building more robust security architectures requires professionals with the right skill sets to apply to the effort—and the best way for individuals to quickly acquire those skills is to engage in the right kind of training.



81%
of global organizations experienced increased cyberthreats during the COVID-19 pandemic.

18,000
government agencies and businesses around the world faced major repercussions from the massive SolarWinds supply chain attacks that occurred in 2019-2020.

Cryptomining, phishing, ransomware, and trojans were the dominant threats in 2020

2021 C|EH Hall of Fame winner **Giulio Astori**, a principal program manager at Microsoft, was able to help his organization investigate the SolarWinds attacks, thanks to his C|EH background. Astori ranks the development of hunting queries to investigate SolarWinds hack traces among his major accomplishments.

C|EH Training Builds Skills by Addressing a Wide Variety of Cyberthreat Scenarios

Supply chain attacks represent just one area of growing concern. The European Union Agency for Cybersecurity published a report in October 2021 identifying nine major threats: ransomware, malware, cryptojacking, email-related threats, threats against data, threats against availability and integrity, disinformation and misinformation, non-malicious threats, and supply chain attacks (ENISA, 2021).

There are many accounts of the usefulness of C|EH training in responding to this wide variety of threat scenarios.

I led

"I led a team of phenomenal cybersecurity and fraud experts to identify a significant threat actor, mitigate the actor's operations, protect the ecosystem from attacks, and contribute to the takedown of the threat actor's operations in 2020," recounted Hall of Fame finalist **David Capezza**, senior director of Visa Payment Systems Intelligence.

I analyzed

Hall of Fame nominee Richard **Yinchun Zhou**, a senior security consultant at an information management solutions firm, drew from his C|EH experience to address pandemic-related security issues. "I analyzed a few malware samples related to Covid-19 and then hosted a webinar to show the audience members how to improve their cyber resilience against advanced cyberthreats," he said.

The number of U.S. data breaches was record-breaking in 2021—the most of any year since 2003, according to the 2022 ITRC Annual Data Breach Report. "The vast majority of data compromises that occur today represent highly sophisticated, highly complex cyberattacks that require aggressive defenses to prevent," noted ITRC CEO **Eva Velasquez** (ITRC, 2022).

I removed

Having Certified Ethical Hackers on board is an advantage when it comes to mounting aggressive defenses. For example, Hall of Fame nominee **Michael Bhim**, a senior enterprise infrastructure engineer for a standards nonprofit, takes pride in having removed a vulnerable application before any compromise was discovered, an action that may have prevented a big security breach at his organization and at a number of government agencies that used the software.

The C|EH Builds Skills That Help Thwart Ransomware Attacks

"Our firm was hit with a ransomware attack in 2017. Because of my C|EH training, I was able to quickly identify the root cause of the attack and then mitigate, remediate, and harden the network."

Joseph Narvaez
CTO at an asset management firm
C|EH Hall of Fame finalist

C|EH Builds Skills That Help Thwart Ransomware Attacks

One of the most problematic threats in recent years is ransomware. A series of devastating ransomware attacks in 2021 succeeded in draining millions of dollars from the companies targeted. Insurance giant CNA Financial Corp. reportedly paid bitcoin equivalent to US$40 million to prevent the exposure of critical data. Colonial Pipeline paid $4.4 million in bitcoin, and JBS Foods USA parted with $11 million, also in bitcoin (Simpson, 2021).

"Ransomware and cyberattacks are victimizing businesses large and small across America and are a direct threat to our economy," Treasury Secretary **Janet Yellen** said, as she promised a heightened government response. Ransomware payments amounted to an estimated $400 million in 2020, according to the U.S. Treasury Department—quadruple the level reported for 2019—and ransomware represents just the tip of the cyberattack iceberg when it comes to economic damages (U.S. Department of the Treasury, 2021).

$400 MILLION

Ransomware payments amounted to an estimated $400 million in 2020, according to the U.S. Treasury Department

The ability of Certified Ethical Hackers to get inside the heads of the attackers gives them an edge.

I identified

"Our firm was hit with a ransomware attack in 2017. Because of my C|EH training, I was able to quickly identify the root cause of the attack and then mitigate, remediate, and harden the network," said C|EH Hall of Fame finalist **Joseph Narvaez**, CTO at an asset management firm.

I recovered

Hall of Fame finalist **Bradley Newberry**, an IT administrator for a municipality, said C|EH equipped him to direct the recovery from a ransomware incident in just a few hours without making any ransomware payment. He was also able to provide the FBI with forensic data in the form of correlated logs.

Demand For Cybersecurity Talent Far Exceeds Supply

Although cybersecurity is a complicated, shifting terrain, one pattern is clear: The global threat level has skyrocketed in recent years. In general, the attackers seem to be making much more headway than the defenders. In some cases, that may be a consequence of organizations lagging in terms of recognition of the threat level. Or it may be that organizations are aware of the risk but cannot squeeze funding out of bare-bones budgets to ramp up their security efforts.

However, even organizations that have made cybersecurity a high priority and are willing to make the necessary financial outlays are faced with a challenge: The demand for skilled security professionals far exceeds the supply.

The global shortfall of skilled professionals affected more than half the organizations represented in a survey of cybersecurity professionals conducted by ISSA in 2021. Ninety-five percent of respondents saw no recent improvement, and 44% said the situation had gotten worse. The biggest problems associated with the skills gap include new positions remaining unfilled for weeks or months, heavier workloads for existing cybersecurity staff, and inability to learn how to use the latest security technologies (Oltsik and Lundell, 2021).

There are cybersecurity positions open on every rung of the career ladder—from entry-level to the C-suite. Roles in strong demand include cloud security specialist, cybersecurity analyst, security investigator, security system administrator, application security specialist, Linux server administrator, digital forensics specialist, risk analysis specialist, penetration tester, network security administrator, mobile security specialist, database security specialist, incident response manager, security auditor, and more.

According to the U.S. Bureau of Labor Statistics, information security analyst will be the 10th fastest-growing occupation this decade, with a projected growth rate of 31 % versus 4%, on verage, for all occupations (U.S. Bureau of Labor Statistics, n.d.).

To Close the Skills Gap, Cybersecurity Certifications Are Essential

Cybersecurity training and certification is the most critical ingredient for addressing the skills gap—both to prepare a new crop of job candidates for entering the profession and to enable those already working in the field to learn new tools and techniques, increasing their value to their organizations and advancing their personal career goals.

One often-overlooked benefit of cybersecurity training and certification is the positive impact hiring entry-level staff can have on senior staff retention. Adding well-trained personnel to handle basic cybersecurity functions means existing staff can focus on the complexities that require advanced skills, increasing their satisfaction.

The Role of C|EH

Organizations that have certified cybersecurity professionals orchestrating their defenses stand a better chance of withstanding the increasing onslaught of cyberattacks. Certifications from globally reputable organizations are one of the best indicators of readiness to join the battle.

One of the most recognized certifications on the planet is the Certified Ethical Hacker (C|EH), awarded to those who are able to pass a comprehensive cybersecurity exam offered by EC-Council. The C|EH is recognized globally in both the private and public sectors. It is popular with novices entering the field and with experts seeking to round out their professional portfolios.

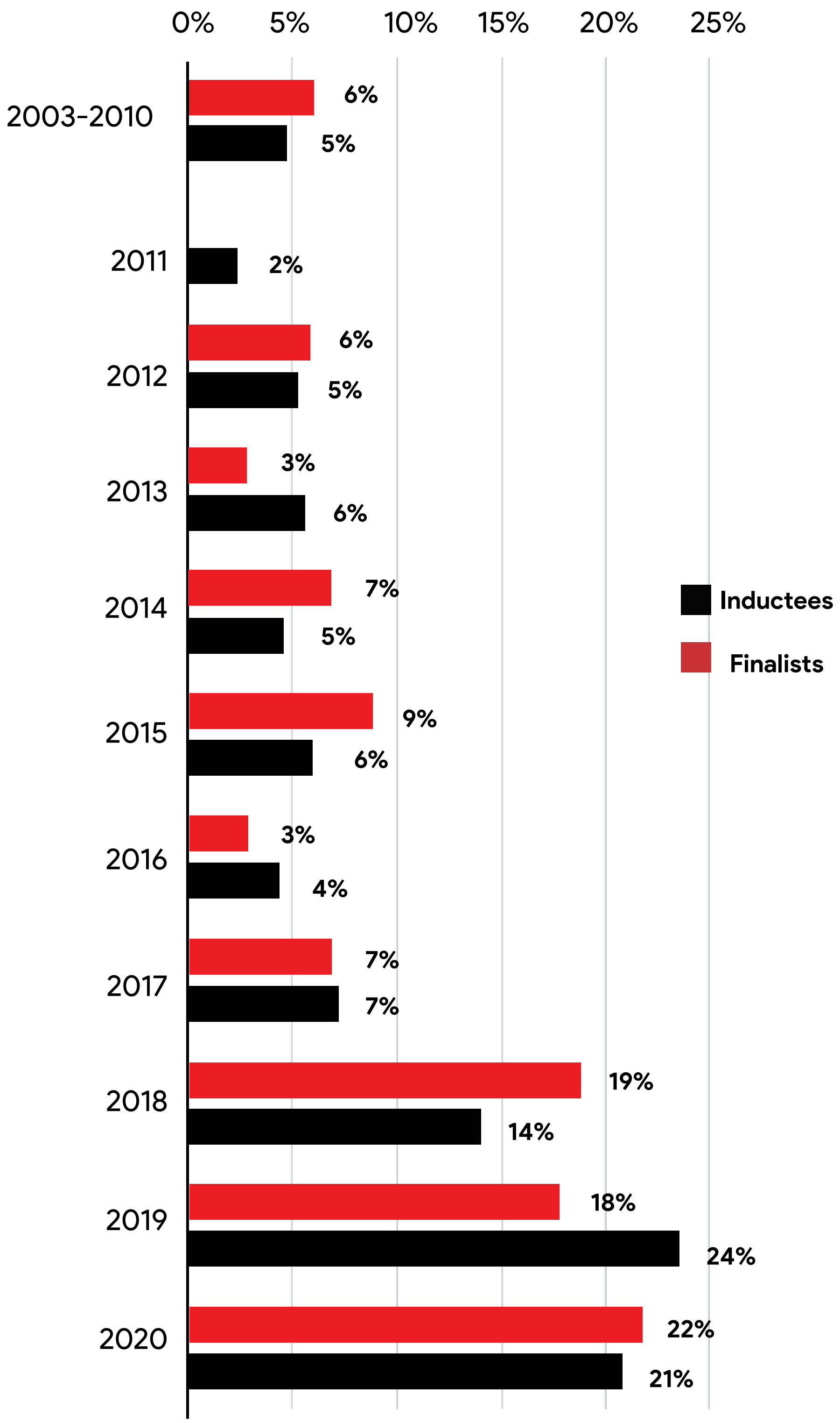
The C|EH Program Draws from 20 Years of Experience

Fundamental to the C|EH approach is its aim to teach students to think like a hacker. The program opens a window into the minds of cyberattackers, training participants to understand their motives and to use the strategies and methods they employ. C|EH participants become proficient with a variety of offensive and defensive hacking tools and methodologies to protect networks and thwart intruders.

> The purpose of the CEH credential is to establish and govern minimum standards for credentialing professional information security specialists in ethical hacking measures; inform the public that credentialed individuals meet or exceed the minimum standards; and reinforce ethical hacking as a unique and self-regulating profession” (EC-Council, Certified Ethical Hacker, n.d.)

Introduced in 2003, the C|EH program has logged nearly 20 years of experience in cybersecurity skills building, equipping participants to lawfully penetrate information technology systems as a means of detecting vulnerabilities and defending against threat actors.

Among the 2021 C|EH Hall of Fame nominees and finalists are cybersecurity professionals who have been associated with the program since its early days. The continuing engagement of professionals with up to 17 years of history with C|EH (Figure 2) is an indication of the value they place on it.

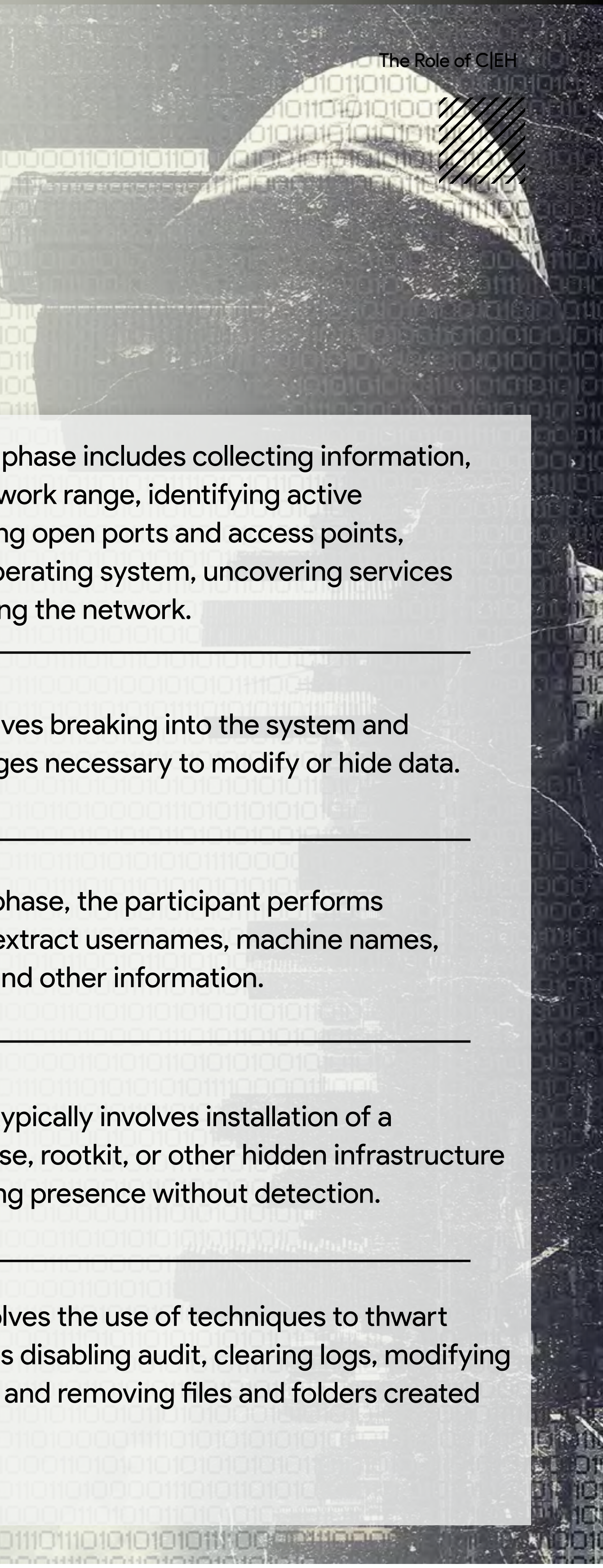


Source: EC-Council

Figure 2: Duration of Top Performers' Affiliation with C|EH Program

C|EH Utilizes a Unique Training Framework

The C|EH program trains participants to develop an offensive mindset through a five-phased structured approach: reconnaissance, gaining access, enumeration, maintaining access, and covering tracks.



1 Reconnaissance

The reconnaissance phase includes collecting information, determining the network range, identifying active machines, discovering open ports and access points, fingerprinting the operating system, uncovering services on ports, and mapping the network.

2 Gaining Access

Gaining access involves breaking into the system and acquiring the privileges necessary to modify or hide data.

3 Enumeration

In the enumeration phase, the participant performs directed queries to extract usernames, machine names, network resources and other information.

4 Maintaining Access

Maintaining access typically involves installation of a backdoor, Trojan horse, rootkit, or other hidden infrastructure to ensure a continuing presence without detection.

5 Covering Tracks

Covering tracks involves the use of techniques to thwart investigators, such as disabling audit, clearing logs, modifying logs or registry files, and removing files and folders created during the intrusion.

C|EH training focuses on the major attack vectors identified by the Open Web Application Security Project (OWASP). The top 10 vulnerabilities in 2021 were injection, broken authentication, sensitive data exposure, XML external entities, broken access control, security misconfigurations, cross-site scripting, insecure deserialization, using components with known vulnerabilities, and insufficient logging and monitoring (OWASP, 2021).

The C|EH program also covers Internet of Things (IoT) hacking, vulnerability analysis, advanced persistent threats (APTs), fileless malware, Web API threats, Webhooks, Web shells, operational technology (OT) attacks, cloud attacks, artificial intelligence (AI) attacks, and machine learning (ML) attacks.

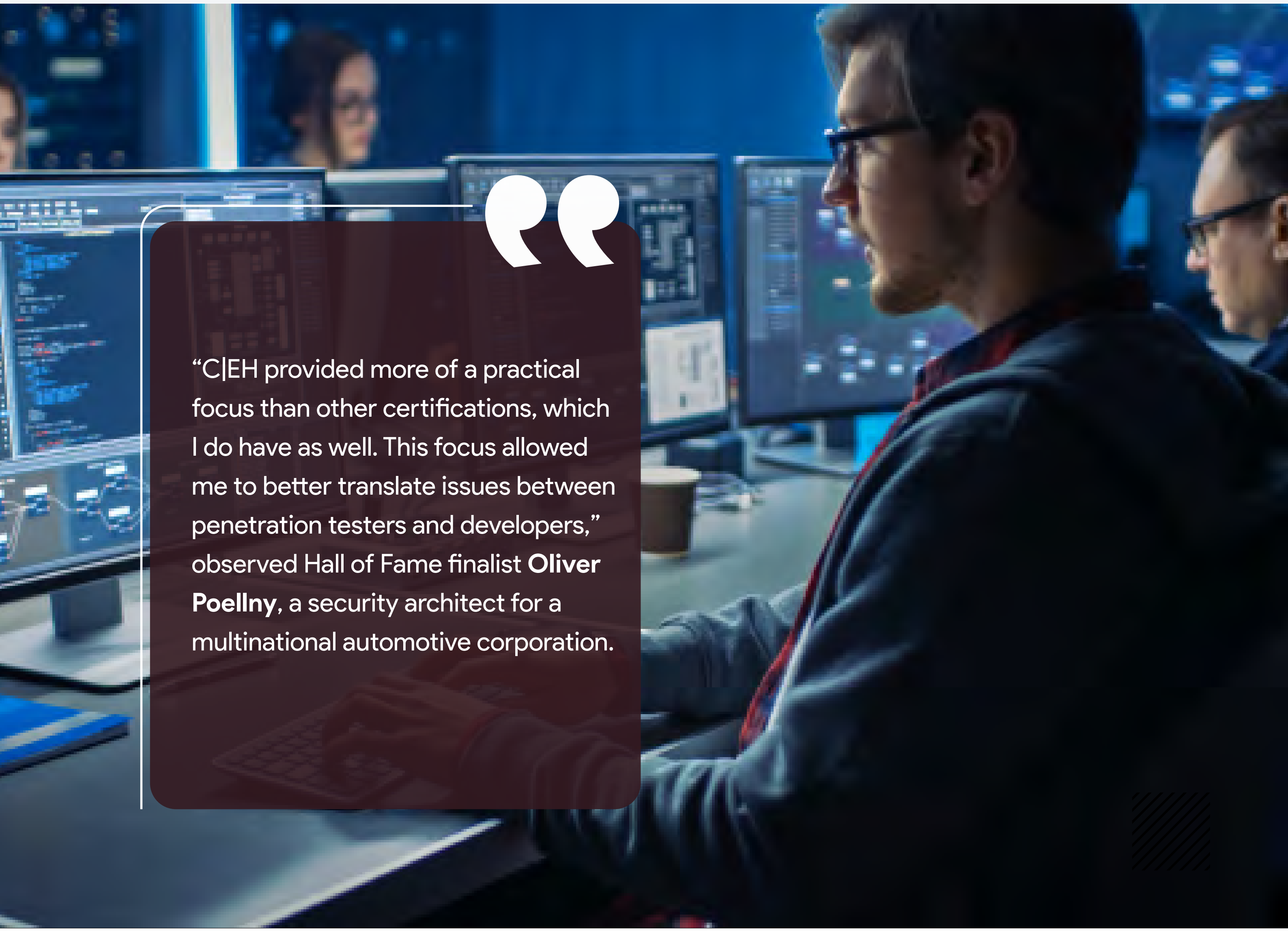
In addition, C|EH participants gain knowledge of malware analysis tactics, container technologies (including Docker and Kubernetes), cloud computing threats, advanced social engineering practices, and more.

The C|EH Program Offers Practical, Hands-On Experience

EC-Council iLabs offers hands-on learning experiences with the use of real tools in real-world scenarios. Cloud-hosted and fully automated, iLabs allows customization to accommodate every level, from beginner to expert. iLabs gives participants full access to virtual machines with preconfigured targets, networks, and attack tools for creating exploits.

Those who have achieved C|EH certification can go a further step by challenging the C|EH Practical, an intense six-hour exam that requires participants to discover and address operating system, database, and network vulnerabilities in 20 scenarios relevant to the ethical hacking domain.

Everyone who earns the C|EH credential leaves the program with an arsenal of tools, a set of impressive hands-on skills, and a wealth of knowledge to bring to the cybersecurity fight. Perhaps the Certified Ethical Hacker's greatest edge, however, is the ability to flip an internal switch and view the world—a world filled with potential targets—the same way a cyberattacker does.



"C|EH provided more of a practical focus than other certifications, which I do have as well. This focus allowed me to better translate issues between penetration testers and developers," observed Hall of Fame finalist **Oliver Poellny**, a security architect for a multinational automotive corporation.

Grow Your Career With C|EH

C|EH Training Extends Beyond Ethical Hacking

The ability to think creatively, a skill that is well-honed in C|EH training, opens the door to jobs that extend far beyond the ethical hacking domain (Figure 3). Titles include computer forensics analyst, cybersecurity auditor, information security analyst, IT security administrator, network security engineer, and penetration tester, among many others.

Common Job Roles for C|EH

- 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
- Jr Penetration Tester
- Senior SOC Analyst
- Solution Architect
- Cybersecurity Consultant
- Security Compliance Analyst
- Technology Risk and Cybersecurity Audit

Following are some of the most in-demand and well-paying job titles for a C|EH, along with their average salaries, according to Infosec Institute (Brecht, 2022):

Info Security Manager	**$117,528**
Cybersecurity Engineer	**$109,706**
Penetration Tester	**$94,405**
Security Analyst	**$72,118**
Security Consultant (computing/networking/information technology)	**$101,939**

The C|EH Program Is Highly Recognized

In the U.S., the C|EH is recognized by the Department of Defense, the U.S. Marine Corps, U.S. Army, U.S. Navy, USAF, and the FBI, among other government and military institutions. Notably, C|EH is a recognized certification for the DoD's computer network defense service providers (CND-SPs), a specialized personnel classification within DoD's information assurance workforce.

The UK intelligence agency GCHQ (Government Communications Headquarters) recognizes the C|EH program with its GCHQ Certified Training accreditation.

C|EH is accredited by the American National Standards Institute (ANSI), which provides a framework for fair standards development and represents the interests of a standards community of more than 270,000 organizations and 30 million professionals worldwide. The C|EH program is also 100% compliant with the NICE 2.0, CREST, and IISP skills frameworks.

In published compilations of the cybersecurity programs considered most beneficial for career advancement, C|EH typically appears among the top certifications. For example, when the Information Security Careers Network (ISCN) sought the opinions of its 90,000 LinkedIn members on 50 leading cybersecurity industry certifications and courses, C|EH ranked No. 4 (SecurityExpert, 2021).

C|EH ranks in the top 10 of "the most widely recognized, important, and required certifications for both beginning and established cybersecurity professionals," according to *Datamation* (Kime, 2022).

Weighing in on career-boosting cybersecurity certifications, TechTarget also places C|EH among the "10 cybersecurity certifications most valuable for aspiring and seasoned cybersecurity professionals" (Zurier, 2022).

"For security professionals desiring to indicate to their current or future employer that they possess the knowledge and skills required to think like an adversary, the CEH is likely the best choice for professional certification," wrote **Stephen Bowcut**, founder and managing editor of Brilliance Security Magazine and a senior editor for Cybersecurity Guide.

"For many, it is only one stepping stone towards their 'top of the industry' goal, but a crucial step, not to be missed" (Bowcut, Certified Ethical Hacker, 2021).

"C|EH certification made my CV outstanding compared to my peers, It has landed me an exciting role at EY."

Sidhant Gupta,
Senior Security Consultant,
Hall of Fame nominee
(EC-Council, How C|EH Helped Me, 2021).

"What C|EH gives you is a 360-degree view. So, what it leaves you with is a desire to learn more and more about an infinitely large subject where the individual matters little and the team matters a lot."

Lorenzo Neri,
Security Specialist,
Hall of Fame finalist.

The Impact of C|EH on Hall of Fame Nominees

Earning a C|EH credential is an impressive accomplishment for any cybersecurity professional, but there is a special place of honor for those who excel—the C|EH Hall of Fame.

In 2021, cybersecurity professionals who scored 90% and above on the C|EH exam were invited to submit an application to be considered for the Hall of Fame. Applicants were analyzed based on outstanding achievements in career growth and successes within their organizations, as well as their contributions to their communities and society at large. Of those applicants, 1,000 were shortlisted as finalists. Of those finalists, 100 were nominated to the C|EH Hall of Fame.

An analysis of the data obtained from the 100 nominees and 900 finalists produced valuable insight into the composition of this talented group of cybersecurity experts and the C|EH program itself.

C|EH Hall of Fame Nominees Originate from Various Industries

Cyberthreats do not spare any type of organization. Risk is ubiquitous for businesses small and large, for nonprofit organizations, and for public agencies at every level of government. The C|EH program is useful across the board, as evidenced by the distribution of C|EH Hall of Fame nominees and finalists by industry (Figure 4).

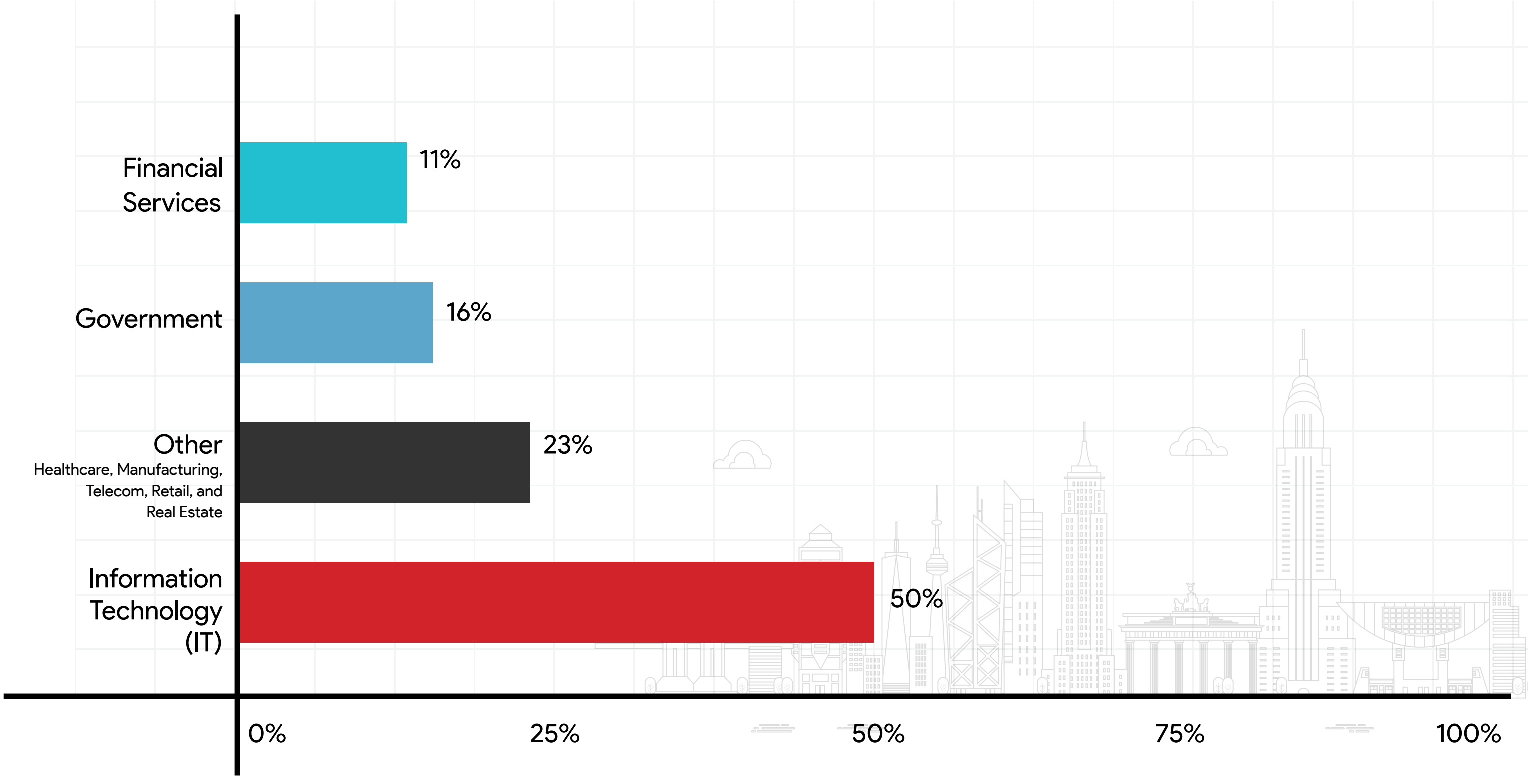


Figure 4: C|EH Hall of Fame Nominees and Finalists by Industry

I led

"I led a team of phenomenal cybersecurity and fraud experts to identify a significant threat actor, mitigate the actor's operations, protect the ecosystem from attacks, and contribute to the takedown of the threat actor's operations in 2020."

David Capezza,
Senior Director,
Visa Payment Systems Intelligence,
Hall of Fame finalist

I analyzed

"I analyzed a few malware samples related to Covid-19 and then hosted a webinar to show the audience members how to improve their cyber resilience against advanced cyberthreats."

Yinchun Zhou,
Senior Security Consultant at an information management solutions firm,
Hall of Fame nominee

I removed

"Our firm was hit with a ransomware attack in 2017. Because of my C|EH training, I was able to quickly identify the root cause of the attack and then mitigate, remediate, and harden the network."

Joseph Narvaez,
CTO at an asset management firm,
C|EH Hall of Fame finalist

I secured

"I have expanded my knowledge of computer hacking and forensics broadly, as a result, I was able to more securely protect my organization infrastructure."

Michael Peters,
CIO at a global risk management organization.
2021 Hall of Fame nominee

I developed

"Using the technical know-how I gained through CEH, I was able to understand risk factors and develop attack vectors/exploits. Using those exploits, I discovered important vulnerabilities in the healthcare domain which helped in minimizing risk."

Gaurav Kulkarni,
Senior security engineer at
a multinational software company,
2021 Hall of Fame finalist.

I recovered

"C|EH equipped me to direct the recovery from a ransomware incident in just a few hours without making any ransomware payment. He was also able to provide the FBI with forensic data in the form of correlated logs."

Bradley Newberry,
IT administrator for a municipality,
Hall of Fame finalist.

I progressed

"Becoming a C|EH Master has given me the belief that I can progress further in the cybersecurity industry and inspired me to go further with my professional qualifications, hopefully enabling me to attain CREST accreditation."

Paul Mahoney,
Network security and resilience manager
for a large ATM deployer,
2021 Hall of Fame finalist.

C|EH Opens Doors to Government Careers

In addition to providing a solid foundation for roles in a broad range of industries in the private sector, C|EH is in high demand for government and military cybersecurity jobs as well.

> "C|EH certification is one of the requirements for my position, so without it I would not even be able to have my current job with a DoD Contractor."
>
> **Juan Sanchez,**
> A cyber defense analyst,
> Hall of Fame nominee

> "This course and certification made me realize how much technology constantly evolves, how vulnerable our networks can be, and what it takes to protect information."
>
> **Valerie Rodriguez,**
> An IT specialist, U.S. Army,
> Hall of Fame finalist

C|EH was instrumental in achieving the organizational goal of a secure IT ecosystem at the multinational public sector bank where Hall of Fame nominee **Nipun Siddhrau** works as assistant general manager. The C|EH skillset helped the bank become a "pioneer in cyberspace," he said.

In general, industry certifications that align with cyber-related U.S. military job roles give candidates a boost in the hiring process. Eighty-four percent of the 256 IT employers who responded to a survey released in February 2020 considered such certifications to be the gold standard when hiring. Nearly a quarter of the IT employers highlighted the C|EH as an industry certification prospective employees should have (EC-Council, 84% of Employers, 2020).

> "C|EH has inspired me to become a leader in my field by providing a baseline of core competencies and security practices."
>
> **Dakota Samuels,**
> A cyber operations officer in the U.S. Army,
> Hall of Fame finalist

Nearly a quarter of the IT employers highlighted the C|EH as an industry certification prospective employees should have (EC-Council, *84% of Employers*, 2020).

C|EH Builds Communities

One of the benefits of the C|EH program is the confidence that inspires many participants to become teachers and mentors, thus encouraging and enabling more professionals to embark on a cybersecurity career, building communities.

“Besides being the director of the Army’s major cybercrime unit, criminal investigation command, I also teach college courses in the field of cybersecurity. Being able to give students real world information and to help them succeed in the cybersecurity field is one of my major accomplishments. My skills have allowed me to publish articles through the Army’s public affairs office on cybercrime trends and other areas to protect the total Army—active duty, civilians, and contractors.”

Edward LaBarge,
C|EH Hall of Fame finalist

C|EH has allowed me to help shape secure standard operating procedures to protect information for a large military academy that transitioned to a fully online environment. I have used the skills learned in C|EH to mentor 10 veterans.”

Joel Sweeney,
A cyber threat intelligence analyst at a multinational technology corporation.
Hall of Fame finalist

His C|EH experience made it possible “to teach the skills I have learned to fellow soldiers, so they will be more effective in their cybersecurity roles,” said Hall of Fame finalist **Dustin Baumann**, a cloud network engineer for the U.S. Army. “It has sparked a passion in me to want to learn more and pursue a career in cybersecurity.”

C|EH Hands-On Training Improves Job Readiness

Both iLabs training and success in challenging the C|EH Practical make cybersecurity professionals more job-ready, since their skills are validated in non-simulated, real-life attack scenarios.

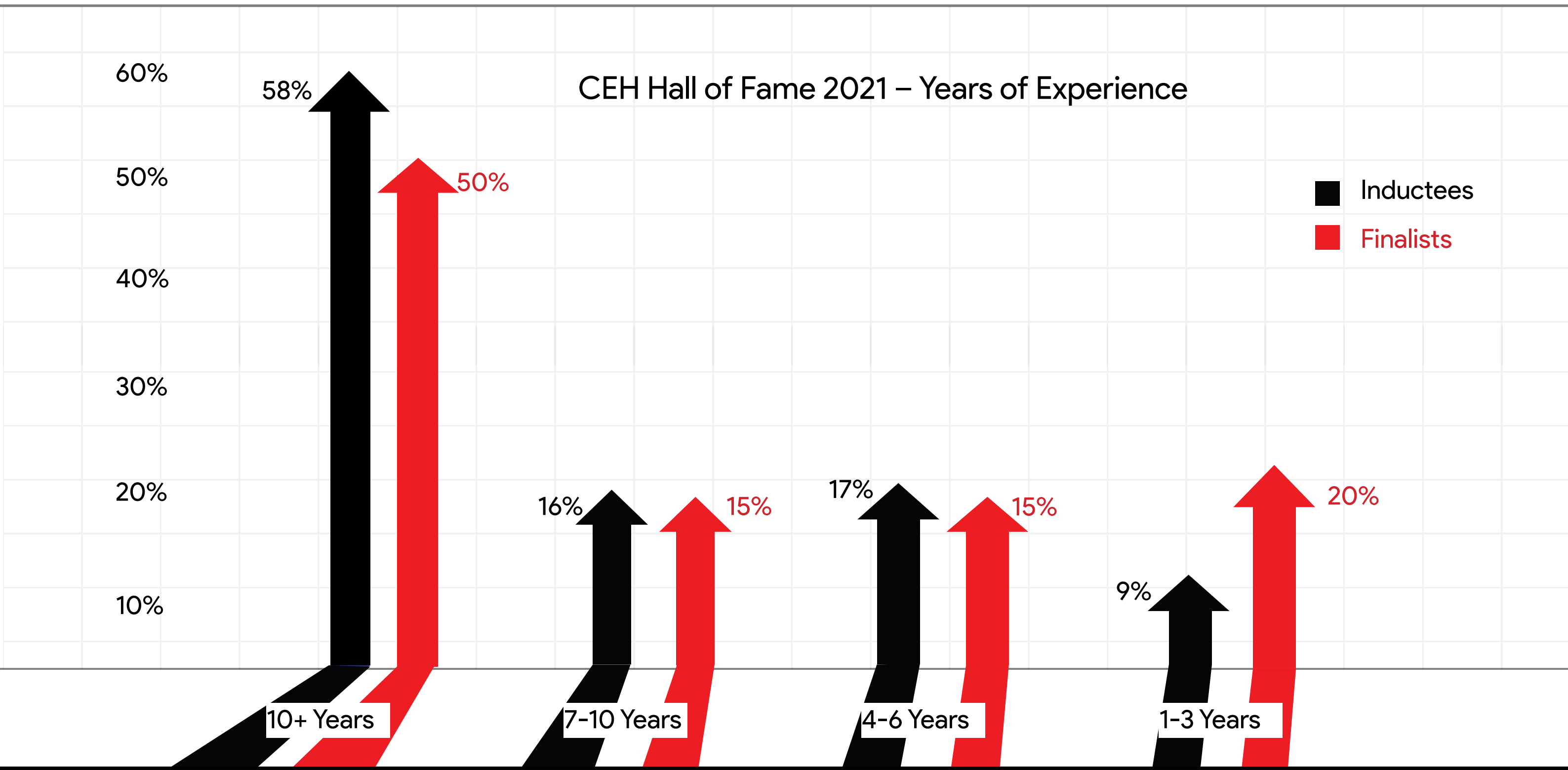
> “I really like hands-on training, the labs are very intuitive. The program walks you through every step and breaks it down so you can understand it.”
>
> **Richard Medlin,**
> Pentester and Cybersecurity analyst, an active-duty Marine and newly inducted member of the C|EH Hall of Fame. (EC-Council, *An Active Duty Marine’s Journey*, 2021)

> “C|EH provided us with a web server in the lab, and we were able to run a DDoS attack on that web server. We tried to access the webserver, but it wasn’t accessible due to the tools and techniques we used to attack it. The C|EH Practical helped me understand some industry-standard tools such as Nmap and Metasploit, and password-cracking tools like John the Ripper.”
>
> **Fuad Mustapha,**
> Information security analyst, Hall of Fame nominee

> “The CEH Practical helped me obtain very valuable knowledge about techniques used by attackers, I use this knowledge every day in my job.”
>
> **Gilberth Contreras Lobo,**
> Cyber Threat Responder, C|EH Hall of Fame nominee.

C|EH Professionals Have High Levels of Career Experience

The C|EH program is attractive to professionals who have been in the cybersecurity industry for significant periods of time and who have substantial experience in the field. The majority of 2021 C|EH Hall of Fame nominees (58 percent) and half the finalists were cybersecurity professionals with 10-plus years on the job (Figure 5).



2021 CEH Hall of Fame winner **Erdal Ozkaya**, who holds a doctorate in information technology, cybersecurity, traces his career success to his introduction to C|EH in 2006 (EC-Council, *Succeeding in Cybersecurity*, 2021). Currently the chief cybersecurity strategist at a cybersecurity solutions provider, he previously worked as regional CISO at a multinational banking and financial services company.

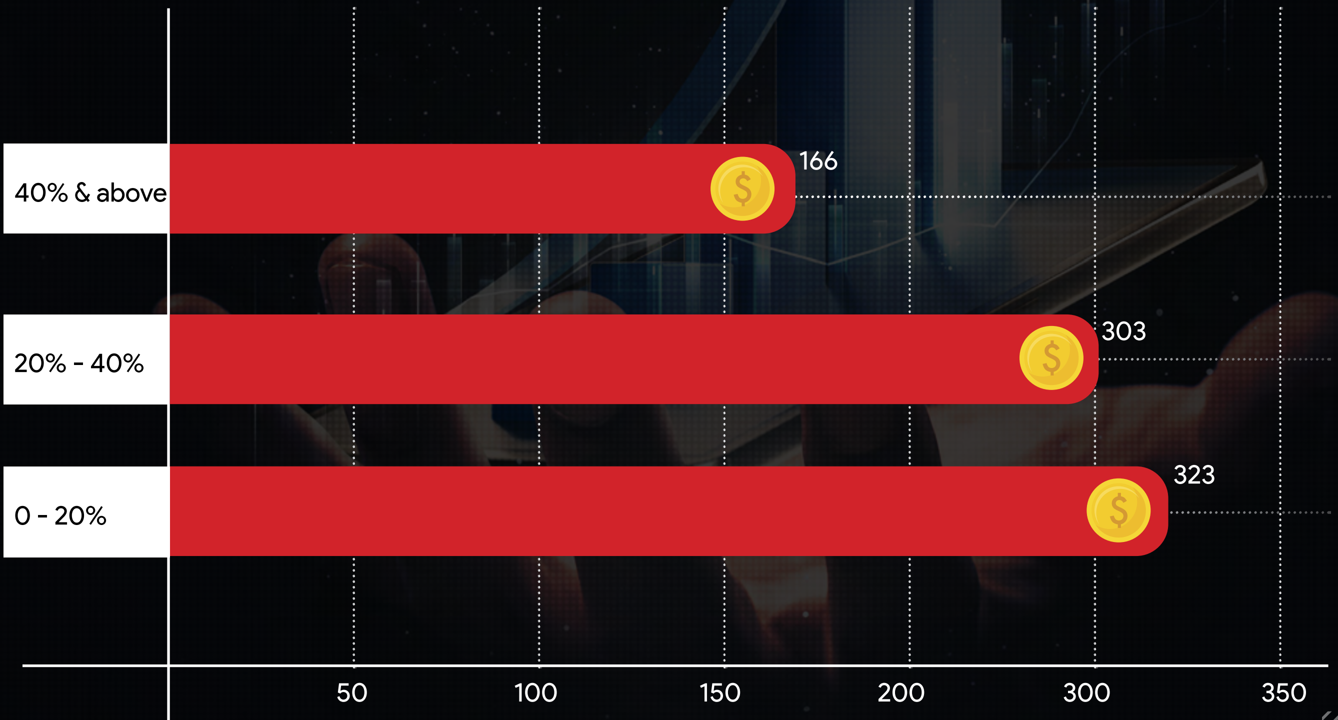
"C|EH was my first security certificate. It made me aware of the future and opened my eyes, which led me to go all the way to my doctorate," he remarked. Ozkaya himself prefers to hire candidates with the C|EH certification. "I want the people I am going to hire to have this set of skills, because I benefited from having them. If people use their C|EH training as I've used it in the past, I'm pretty sure they will benefit from it as well."

It's noteworthy that a full 20 percent of C|EH Hall of Fame finalists had just one to three years of cybersecurity work experience, suggesting that the C|EH training may have contributed more to their high performance than their job experience did. That seems to support Ozkaya's observation about the value of the skillsets developed through the program.

C|EH Boosts Hiring and Salary Potential

Both C|EH Hall of Fame nominees and finalists attributed concrete salary advantages to their acquisition of the C|EH credential.

Roughly 79% reported a salary increase of more than 20% compared to their peers after attaining the C|EH. About 21% reported a 40% salary advantage over their peers (Figure 5).



Source: EC-Council

Figure 5: Top Performers' Salary Advantage Credited to C|EH

C|EH certification led to a better job with a better salary.

– Leonardo La Rosa

"I was compensated with a salary increase at my present job due to the C|EH certification and got more recognition in the job market," said Hall of Fame nominee **Mustapha**.

"I was able to learn a lot of techniques which helped me become a better consultant. Since I became a C|EH, I have received more job offers than I used to. Also, becoming a C|EH improved my salary."

Gabriel Diaz Guimaraens, Security Consultant for a cybersecurity services provider, Hall of Fame finalist.

For C|EH Hall of Fame finalist **Leonardo La Rosa**, cybersecurity and infrastructure manager at a cybersecurity training academy, C|EH certification led to a better job with a better salary. "I started producing cybersecurity content to engage other students, and I became an EC-Council Certified Instructor," he said.

Closing the Skills Gap

C|EH helps to close the cybersecurity skills gap directly, by expanding the pool of qualified candidates for jobs that urgently need to be filled in government and the private sector. Another direct effect is increasing the value of existing employees—as evidenced by the higher salaries many enjoy as a result of earning the certification.

The added protection an organization realizes as a result of the training its employees gain through C|EH is another major plus.

> "With my C|EH badge and knowledge, I was able to build credibility with my peers and management. I was able to get my management to invest in significant security technology and establish security functions/teams, which were crucial to secure the organization."
>
> **Arjun BM,**
> Chief Security Architect,
> C|EH Hall of Fame finalist

What is it worth to have a cybersecurity specialist on board who can think like a hacker and knows how to detect and block even the most complex intrusion attempts, versus an overburdened, undertrained, underpaid employee—or worse yet, no one at all—to fill that role?

There is no single weapon that can bring the increasingly sophisticated armies of cyberattackers to their knees. However, those who have earned the title of Certified Ethical Hacker are on the vanguard of the world's cybersecurity defenses. And those who have earned a place in the C|EH Hall of Fame are the generals whose strategic skills can help win the war, one battle at a time.

Life-Changing Opportunities

For many C|EH Hall of Fame nominees and finalists, becoming a Certified Ethical Hacker has led to active courtship by recruiters and potential employers.

“My job interview with a financial institution, which was scheduled for 30 minutes, ended up being two and a half hours. Definitely, without the knowledge that C|EH gave me, it would not have been the same.”

Karla Herrera,
Senior Security Advisor,
C|EH Hall of Fame finalist

For others it has paved the way to exciting new specialties within the cybersecurity field.

“C|EH helped my career immensely as it helped me transition from software developer to security consultant.”

Gunjan Sharma Sehgal,
Lead information security architect, C|EH Hall of Fame finalist

“C|EH satisfied the DoD 8570 requirements, directly leading to my employment with the US Air Force.”

Jeremy Young,
Technical Manager,
C|EH Hall of Fame finalist

Cybersecurity has always been my career path, and C|EH training and materials gave me a solid foundation to drive where I want to go on my career.”

Rapule Kgalaki,
Deputy director of technical audits, C|EH Hall of Fame finalist

C|EH stands apart from other cybersecurity programs for its ability to deliver practical knowledge based on a clear concept—to think like a hacker—using a robust framework that is highly adaptable to the constantly shifting threat landscape. Perhaps Hall of Fame nominee Michael Turner, CISO at a global security and aerospace company, put it best:

“While other certifications talk the talk, C|EH walks the walk and is recognized by the Department of Defense.”

About EC-Council

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 U.S. 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) program 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

Bowcut, S. (2021, October 19). “Certified Ethical Hacker: CEH Certification guide.” *Cybersecurity Guide*. https://cybersecurityguide.org/programs/cybersecurity-certifications/ceh/

Bowcut, S. (2021, November 29). “Labor Shortage for IT and OT Cybersecurity [Podcast].” Brilliance Security Magazine Podcast. https://anchor.fm/steven-bowcut/episodes/Labor-Shortage-for-IT-and-OT-Cybersecurity-e1anduv

Brecht, D. (2022, January 12). “Certified Ethical Hacker (CEH) Job Outlook [updated 2022].” Infosec. https://resources.infosecinstitute.com/certification/certified-ethical-hacker-job-outlook/

Cisco. (2021). “2021 Cyber security threat trends: phishing, crypto top the list.” https://learn-umbrella.cisco.com/ebooks/2021-cyber-security-threat-trends-phishing-crypto-top-the-list

EC-Council. (n.d.). “Certified Ethical Hacker.” https://cert.eccouncil.org/certified-ethical-hacker.html

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

EC-Council. (2020, February 19). “84% of Employers find Cybersecurity Certifications that align with Military Job Roles as the Gold Standard for Hiring.” *https://www.eccouncil.org/84-of-employers-find-cybersecurity-certifications-that-align-with-military-job-roles-as-the-gold-standard-for-hiring/*

EC-Council. (2021, October 20). *Succeeding in Cybersecurity, Your Career Guide* [Video]. YouTube. https://www.youtube.com/watch?v=F3zyirh2S1I&list=PL7fZapE6MM9XBptzYarhRv9apQZXMCZTh&index=9

EC-Council. (2021, September 23). *An Active Duty Marine’s Journey into Penetration Testing with C|EH Practical* [Video]. YouTube. https://www.youtube.com/watch?v=YL05xgGjwLQ&list=PL7fZapE6MM9XBptzYarhRv9apQZXMCZTh&index=5

EC-Council. (2021, September 23). *How Certified Ethical Hacker Helped Me Land a Job with Big4.* [Video]. YouTube. https://www.youtube.com/watch?v=PLvVyh96n8M

ENISA. (2021, October 27). *ENISA Threat Landscape 2021.* European Union Agency for Cybersecurity. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021

ImmuniWeb. (n.d.). “OWASP Top 10 Security Risks and Vulnerabilities.” https://www.immuniweb.com/resources/owasp-top-ten/

ITRC. (2022, January 24). *Data Breach Annual Report. Identity Theft Resource Center.* https://notified.idtheftcenter.org/s/

Kime, C. (2022, January 31). “10 Top Cybersecurity Certifications.” *Datamation*. https://www.datamation.com/careers/cybersecurity-certifications/

McAfee Enterprise and FireEye. (2021). “Cybercrime in a Pandemic World: The Impact of COVID-19.” https://www.mcafee.com/enterprise/en-us/assets/infographics/1121-mfe-fe-holiday-infographic-v3.pdf?download=1

Oltsik, J., Lundell, B. (2021, July). *The Life and Times of Cybersecurity Professionals 2021.* https://2ll3s9303aos3ya6kr1rrsd7-wpengine.netdna-ssl.com/wp-content/uploads/2021/07/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Jul-2021.pdf

OWASP. (2021). “OWASP Top 10 – 2021.” https://owasp.org/Top10/

SecurityExpert. (2021, January 5). “The Top Cybersecurity Certifications in 2021.” *Security Boulevard.* https://securityboulevard.com/2021/01/the-top-cybersecurity-certifications-in-2021/

Simpson, A. (2021, December 6). “*Lessons from Ransomware Payments by CNA, JBS and Colonial Pipeline,*” Insurance Journal. https://www.insurancejournal.com/magazines/mag-features/2021/12/06/644276.htm

U.S. Bureau of Labor Statistics. (Last modified 2021, September 8). “Occupational Outlook Handbook,” https://www.bls.gov/ooh/fastest-growing.htm

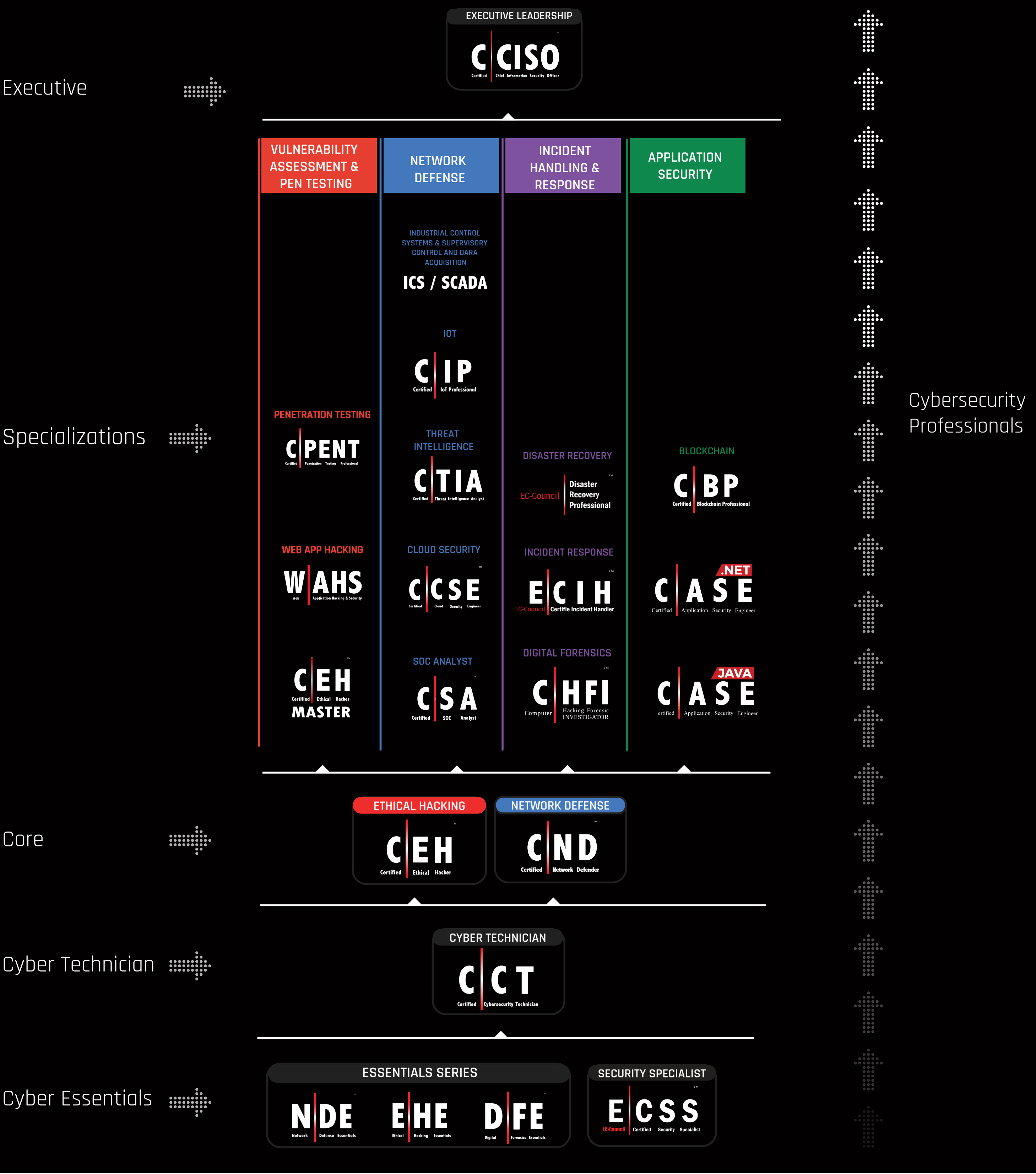
U.S. Department of the Treasury. (2021, September 21). *Treasury Takes Robust Actions to Counter Ransomware* [Press release]. https://home.treasury.gov/news/press-releases/jy0364

Whitaker, B. (2021, February 14). “SolarWinds: How Russian spies hacked the Justice, State, Treasury, Energy and Commerce Departments,” *CBS News.* https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-02-14/

Zurier, S. (last published 2022, February). “10 cybersecurity certifications to boost your career in 2022.” *TechTarget.* https://www.techtarget.com/searchsecurity/tip/10-cybersecurity-certifications-to-boost-your-career-in-2021

EC-Council

Learning Track



Executive

EXECUTIVE LEADERSHIP
CCISO
Certified Chief Information Security Officer

Specializations

VULNERABILITY ASSESSMENT & PEN TESTING

PENETRATION TESTING
CPENT
Certified Penetration Testing Professional

WEB APP HACKING
WAHS
Web Application Hacking & Security

CEH MASTER
Certified Ethical Hacker

NETWORK DEFENSE

INDUSTRIAL CONTROL SYSTEMS & SUPERVISORY CONTROL AND DARA ACQUISITION
ICS / SCADA

IOT
CIP
Certified IoT Professional

THREAT INTELLIGENCE
CTIA
Certified Threat Intelligence Analyst

CLOUD SECURITY
CCSE
Certified Cloud Security Engineer

SOC ANALYST
CSA
Certified SOC Analyst

INCIDENT HANDLING & RESPONSE

DISASTER RECOVERY
EC-Council Disaster Recovery Professional

INCIDENT RESPONSE
ECIH
EC-Council Certifie Incident Handler

DIGITAL FORENSICS
CHFI
Computer Hacking Forensic INVESTIGATOR

APPLICATION SECURITY

BLOCKCHAIN
CBP
Certified Blockchain Professional

CASE .NET
Certified Application Security Engineer

CASE JAVA
ertified Application Security Engineer

Cybersecurity Professionals

Core

ETHICAL HACKING
CEH
Certified Ethical Hacker

NETWORK DEFENSE
CND
Certified Network Defender

Cyber Technician

CYBER TECHNICIAN
CCT
Certified Cybersecurity Technician

Cyber Essentials

ESSENTIALS SERIES
NDE
Network Defense Essentials
EHE
Ethical Hacking Essentials
DFE
Digital Forensics Essentials

SECURITY SPECIALIST
ECSS
EC-Council Certified Security Specialist

Knowledge Workers

Cybersecurity Awareness
CSCU
Certified Secure Computer User

Phishing Awareness
aware

Knowledge Workers

Individual Courses

ENCRYPTION
ECES
EC-Council Certified Encryption Specialist

codered FROM EC-COUNCIL

Browse a catalog of over **10,000 courses**

EC-Council

www.eccouncil.org

Disclaimer: Any product names, logos, brands and/or other trademarks or images featured or referred to are the property of their respective owners and are not intended to imply endorsement or sponsorship by any of these companies of any EC-Council products or services. They are intended to represent the companies that C|EH Hall of Fame nominees work at. All company logo's, names, product and service names used in this report are for identification purposes only.