

EC-Council | Academia



Agenda

- Introduction to EC-Council
- Cyber Security Threat Landscape
- Certified Ethical Hacker Lab Demonstrations
- Threats to Industry & Threats to You
- EC-Council Academia Programmes
- Who is looking for Cyber Security Professionals and why
- Q & A

EC-COUNCIL AT A GLANCE

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.



Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted ECC to develop and advance their security infrastructure.

ICECC

International Council of E-Commerce Consultants
EC-Council Group

ECCU

EC-Council University
Division of Academic Education

ECC

EC-Council Training & Certification
Division of Professional Workforce Development

EGS

EC-Council Global Services
Division of Corporate Consulting & Advisory Services

EGE

EC-Council Global Events
Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF

EC-Council Foundation
Non-Profit Organization for Cyber Security Awareness Increase.

**WE ARE
INFORMATION
SECURITY**

15+ YEARS EXPERIENCE

40+ TRAINING & CERTIFICATION PROGRAMS

145+ COUNTRIES

350+ SUBJECT MATTER EXPERTS

700+ TRAINING PARTNERS WORLDWIDE

3000 TOOLS & TECHNOLOGIES

200,000 CERTIFIED MEMBERS

DOMINANCE IN THE MARKET

WE ARE PROUD TO HAVE PLAYED A ROLE IN THE CYBER SECURITY OF

BLUE CHIP CUSTOMER BASE



- Accenture
- Allianz
- Axiata
- American Express
- Barclays Capital
- British Airways
- British Telecom
- Cambridge Experts
- Capgemini
- CCL-Forensics Ltd.
- Celcom
- Criminal Justice IT
- Deloitte
- E&Y
- Harvard Engineering
- Honda Malaysia
- J P Morgan Wells
- Jefferson KPMG
- Logica
- Metropolitan Police Service
- Ministry of Defence UK
- Motorola
- PWC
- Royal Bank of Scotland Group
- Royal Navy
- Shell
- Vodafone
- Fujitsu
- General Dynamics UK
- Ceridian
- De Montfort University
- HP
- IBM
- Lancaster University
- Oracle Corporation
- Police Service of Northern Ireland
- Royal Bank of Scotland
- The British Library
- UK Ministry of Defense
- University of Bedfordshire
- University of East London
- University of Sunderland

GLOBAL RECOGNITIONS (CONT'D)

EC-COUNCIL TRAINS PENTAGON D.C DOD, US NAVY, US AIRFORCE AND US ARMY

United States Air Force Information Operations Center partners with EC-Council to support Mission Qualification Training

The United States Air Force's Information Operations Center is now training the Certified Ethical Hacker (CEH) to its IT Security Specialists. This new affiliation with EC-Council is expected to produce many Certified Ethical Hackers in the years to come, further fortifying Air Force Operations and Security.

Albuquerque June 11, 2009 - The United States Air Force Information Operations Center (AFIOC) and EC-Council announced today under special provision that the Certified Ethical Hacker (CEH) will become a supporting element to Mission Qualification Training conducted by AFIOC to train highly specialized Information Security Professionals inside the U.S. Air Force.



CNN Tech • Gadgets | Cyber Security | Innovation Nation | Vital Signs

Part of complete coverage on: **Navigating Your Online World**

Pentagon trains workers to hack Defense computers

By Larry Shaughnessy, CNN Pentagon Producer
March 15, 2010 -- Updated 14:14 GMT (22:14 HKT)

Washington (CNN) -- The Pentagon is training people to hack into its own computer networks.

"To beat a hacker, you need to think like one," said Jay Bavisi, co-founder and president of the International Council of Electronic Commerce Consultants, or EC-Council. His company was chosen by the Pentagon to oversee training of Department of Defense employees who work in computer security-related jobs and certify them when the training is complete.

The Department of Defense does not consider this hacking.

"DoD personnel are not learning to hack. They are learning to defend the network against hackers," said spokesman Lt. Col. Eric Butterbaugh.

The idea behind the Pentagon's training is that thinking like a hacker can beat a hacker.

STORY HIGHLIGHTS

- "Certified Ethical Hacker certification" trains employees to defend computer networks.
- Almost 45,000 attacks on Defense computers reported in the first half of 2009.
- Aim of hacker training is to help

KEY ENDORSEMENTS – DOD 8570 MANDATE

The credential and job role of a Certified Ethical Hacker was first mooted and developed by EC-Council globally.

Thousands of jobs are created globally due to this initiative. EC-Council has

continues to expand it's contribution in this space with the introduction of 33 certifications.

EC-Council programs have a been accredited by the **DHS/NSA CNSS** standards and are one of the very few originations to have attained the **ISO/IEC 17024** standards.

As a result, the US Department of Defense listed EC-Council's CEH certification into its **DoD 8570 mandate** which provides approved training opportunities to its thousands of IT security staff and contractors.

EC-Council programs map to the **NICE Framework** too.



Table AP3.T2. DoD Approved Baseline Certifications

IAT Level I		IAT Level II		IAT Level III					
A+-CE Network+ CE SSCP		GSEC Security+ CE SSCP		CISA GCIH GSE CISSP (or Associate)					
IAM Level I		IAM Level II		IAM Level III					
CAP GISF GSLC Security+ CE		CAP GSLC CISM CISSP (or Associate)		GSLC CISM CISSP (or Associate)					
IASAE I		IASAE II		IASAE III					
CISSP (or Associate)		CISSP (or Associate)		CISSP - ISSEP CISSP - ISSAP					
CNDSP Infrastructure Support									
CNDSP Analyst		CNDSP Incident Responder		CNDSP Auditor		CNDSP Manager			
GCIA CEH GCIH		SSCP CEH		GCIH CSIH CEH		CISA GSNA CEH		CISSP-ISSMP CISM	



WORLD ECONOMIC FORUM

Cyber Attacks have been ranked as one of the top global threats in The World Economic Forum's (WEF) annual study also —The Global Risks Report 2018. With Data Fraud/Theft being on the list for most likely threats

The risk of cyber-attacks is ranked highly by the WEF because the organization is concerned that this year, cyber-attacks not only have a strong likelihood of happening, they also have the potential to make a considerable impact.

“Cybersecurity risks are also growing, both in their prevalence and in their disruptive potential. Attacks against businesses have almost doubled in five years, and incidents that would once have been considered extraordinary are becoming more and more commonplace”

Top 10 risks in terms of Likelihood

- 1 Extreme weather events
- 2 Natural disasters
- 3 Cyberattacks
- 4 Data fraud or theft
- 5 Failure of climate-change mitigation and adaptation
- 6 Large-scale involuntary migration
- 7 Man-made environmental disasters
- 8 Terrorist attacks
- 9 Illicit trade
- 10 Asset bubbles in a major economy

Top 10 risks in terms of Impact

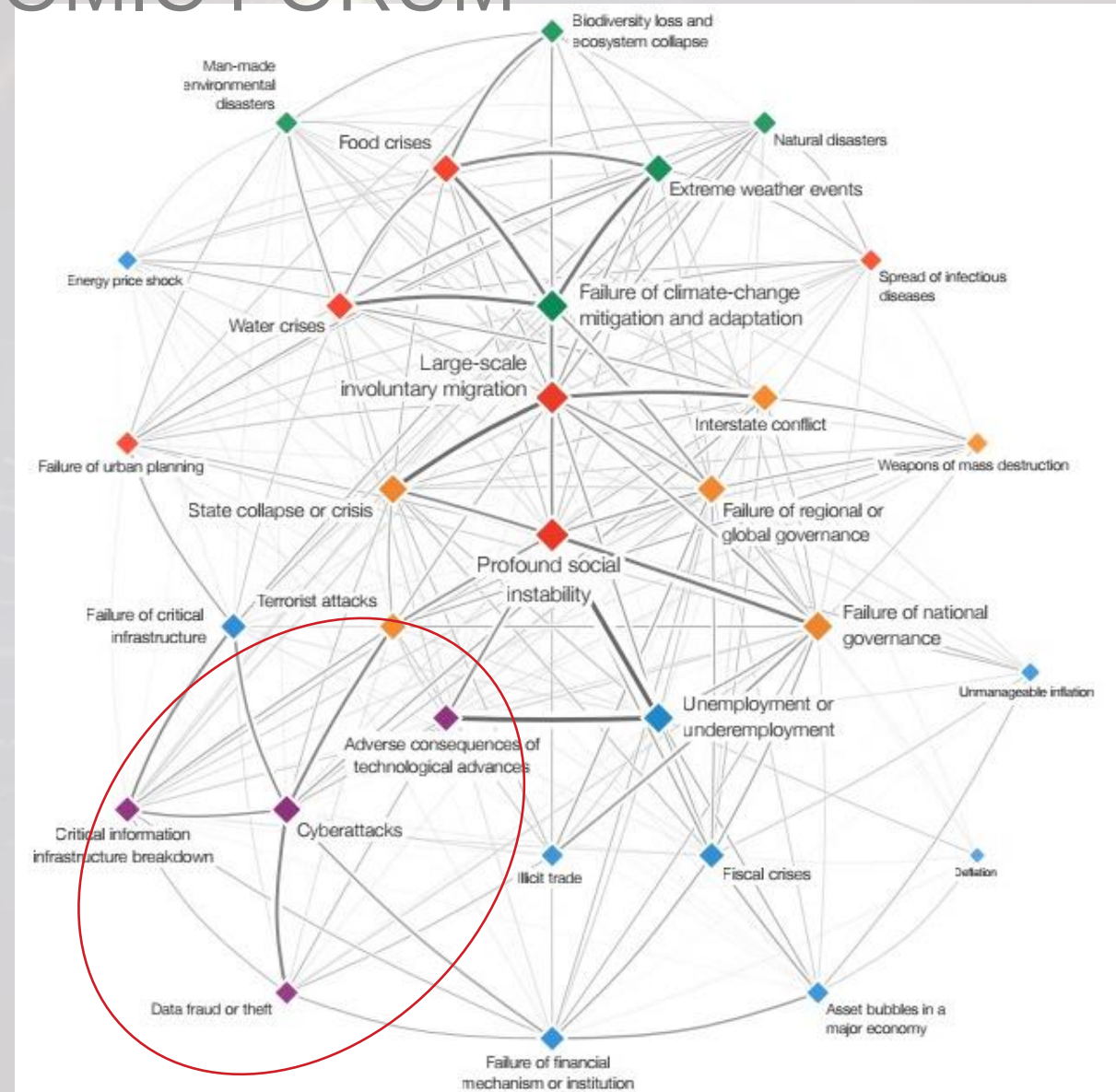
- 1 Weapons of mass destruction
- 2 Extreme weather events
- 3 Natural disasters
- 4 Failure of climate-change mitigation and adaptation
- 5 Water crises
- 6 Cyberattacks
- 7 Food crises
- 8 Biodiversity loss and ecosystem collapse
- 9 Large-scale involuntary migration
- 10 Spread of infectious diseases

Source: World Economic Forum Global Risks Perception Survey 2017–2018.

WORLD ECONOMIC FORUM

A 2017 study of 254 companies across seven countries put the annual cost of responding to cyberattacks at £11.7 million per company, a year-on-year increase of 27.4%

“The cost of cybercrime to businesses over the next five years is expected to be US\$8 trillion”



GLOBALLY CYBER CRIME IS ON A RISE

Dyn Cyberattack (2016)

The 2016 Dyn cyberattack took place on October 21, 2016, and involved multiple denial-of-service attacks (DoS attacks) targeting systems operated by Domain Name System (DNS) provider Dyn which made major Internet platforms and services unavailable to large swathes of users in Europe and North America. The groups Anonymous and New World Hackers claimed responsibility for the attack, but scant evidence was provided.

DCCC Cyber Attacks (2016)

On Friday July 29, 2016 the Democratic Congressional Campaign Committee reported that its computer systems had been infiltrated. It is strongly believed by US intelligence sources that the infiltrator groups are Russian foreign intelligence groups that breached the Democratic National Committee's computer systems. These groups are known as Fancy Bear and Cozy Bear.

Democratic National Committee Cyber Attacks (2016)

The Democratic National Committee cyber attacks took place in 2015 and 2016, in which computer hackers infiltrated the Democratic National Committee (DNC) computer network, leading to a data breach.

Sony Pictures Hack (2014)

On November 24, 2014, a hacker group which identified itself by the name "Guardians of Peace" (GOP) leaked a release of confidential data from the film studio Sony Pictures. The data included personal information about Sony Pictures employees and other information.

Russian Hacker Password Theft (2014)

The 2014 Russian hacker password theft is an alleged hacking incident resulting in the possible theft of over 1.2 billion internet credentials, including usernames and passwords, with hundreds of millions of corresponding e-mail addresses.

Ashley Madison Data Breach (2015)

In July 2015, a group calling itself "The Impact Team" stole the user data of Ashley Madison, a commercial website billed as enabling extramarital affairs. The group copied personal information about the site's user base.

Bangladesh Bank Heist (2016)

In February 2016, instructions to steal US\$951 million from Bangladesh Bank, the central bank of Bangladesh, were issued via the SWIFT network. Five transactions issued by hackers, worth \$101 million and withdrawn from a Bangladesh Bank account at the Federal Reserve Bank of New York, succeeded, with \$20 million traced to Sri Lanka (since recovered) and \$81 million to the Philippines (about \$18 million recovered).

SWIFT banking hack (2015–16)

SWIFT banking hack (2015–16)
In 2015 and 2016, a series of cyberattacks using the SWIFT banking network were reported, resulting in the successful theft of millions of dollars. The attacks were perpetrated by a hacker group nicknamed "Lazarus" by researchers.

Office Of Personnel Management Data Breach (2015)

In June 2015, the United States Office of Personnel Management (OPM) announced that it had been the target of a data breach targeting the records of as many as four million people. Later, FBI Director James Comey put the number at 18 million.

VTech Data Breach (2015)

In November 2015, Lorenzo Bicchieri, writing for Vice magazine's Motherboard, reported that VTech's servers had been compromised and the corporation was victim to a data breach which exposed personal data belonging to millions of individuals.

Hacking Team (2015)

On July 5, 2015, the Twitter account of the company was compromised by an unknown individual who published an announcement of a data breach against HackingTeam's computer systems

Commission on Elections Data Breach (2016)

On March 27, 2016, hackers under the banner, Anonymous Philippines hacked into the website of the Philippine Commission on Elections (COMELEC) and defaced it.

Source(s): Compiled from Wikipedia, https://en.wikipedia.org/wiki/Category:Hacking_in_the_2010s

GOVERNMENT CYBER FOCUS

Singapore launches new cyber security regime

By Liz Heron on 11/02/2018

Share 23 Tweet G+ Pin it in Share Email

Singapore is to have a new cybersecurity tsar with wide-ranging powers to seize confidential information and impose penalties under legislation passed by its parliament on Monday last week.

The Cybersecurity Bill requires owners of computer systems involved in the provision of essential public services in 11 designated areas to meet a set of statutory obligations overseen by a commissioner of cybersecurity.

The new post will be filled by David Koh, who is chief executive of the Cyber Security Agency of Singapore (CSA) and also serves as deputy secretary (special projects) and cyber chief in the Ministry of Defence.

Companies and organisations that own such "critical information infrastructure" (CII) will have



Aerial view of Singapore's Civic District including the Singapore Parliament.

FINANCIAL TIMES

UK COMPANIES MARKETS OPINION WORK & CAREERS LIFE & ARTS

Ministry of Defence UK

Missed 2% defence spending target, report claims



A UK ministerial pre-emptive strike



MoD slammed over potential £21bn procurement black hole

Ministry of Defence UK

+ Add to myFT

Ministry of Defence steps up cyber security operations

Government earmarks £40m for new centre to be based at Corsham

U.S. EDITION Mon, Feb 19, 2018

Newsweek

U.S. | World | Business | Tech & Science | Culture | Sports | Health | Opinion | Green Rankings

OANDA
FX & CFD Trading

1.2 on EUR/USD
No Commissions

No third party software fees
No dealing desk intervention

Start My Free Demo

NATO TO SPEND BILLIONS ON MASSIVE CYBERSECURITY, DEFENSE COMMUNICATIONS BOOST

BY TOM O'CONNOR ON 3/27/17 AT 10:55 AM



GOVERNMENT CYBER FOCUS

“Promote the training of professionals, give impetus to industrial development and strengthen the R&D&I system in cyber security matters” – National Cyber Security Strategy, Spain

“Besides raising the awareness of the youngest subjects, training in digital technology professions should provide future professionals in the field with extensive information systems security skills, which remains currently absent from many higher education programmes.” – National Digital Security Strategy, France

“Knowledge is an extremely important asset in the Netherlands. Dutch society, and digital security in particular, depends on the development and use of knowledge” – National Cyber Agenda, Netherlands

“In businesses, many staff members are not cyber security aware and do not understand their responsibilities in this regard, partially due to a lack of formal training. The public is also insufficiently cyber” – National Cyber Security Strategy, UK

GOVERNMENT CYBER FOCUS

Experts: US Is Not Prepared to Handle Cyber Attacks

In Congressional testimony, authorities on cyber defense say neither government agencies nor private companies are ready for what may come

By Tim Wilson
Site Editor, *Dark Reading*

If the bad guys launched a coordinated cyber attack on the United States tomorrow, neither government nor industry would be able to stop it, experts warned legislators yesterday.

At a hearing held by the House Permanent Select Committee on Intelligence, cyber defense experts testified that government agencies are insufficiently coordinated to handle an attack, and that efforts to build a defense have not adequately addressed issues in the private sector.

"The Department of Homeland Security lacks the personnel, capability, authority, and culture required to do the job entrusted to them by the President and Congress," said Amit Yoran, CEO of NetWitness Corp. and former director of the National Cyber Security Division at DHS. "DHS's cyber efforts are disorganized and disjointed, and practical operations continued to be buried deeper within the organization."

GOVERNMENT CYBER FOCUS

Hello Anon - Login

DeepPaste

Your Deep-Shit Hoster for special shit

Results for 1947cc01e56ed46b8e38e345f2c10a4f:

William Welna FBI snitch has SSNs

Anon, May 10, 2018 - 2:55 pm UTC

```
05:13:33 [SanguineRose ] some weird shit going on On Sabu being in doxbin, SSNs, Jennifer Emick's FBI handler, and awinee
05:36:00 [-nachash ] All they got, though
05:36:05 [-nachash ] was you vs awinee that time
05:36:07 [-SanguineRose ] lol
05:36:10 [-SanguineRose ] not much in there
05:36:13 [-nachash ] and ev0's misadventures at white castle
05:36:16 [-SanguineRose ] and they seen pc nude
05:36:20 [-nachash ] plus little random bullshit
05:36:20 [-SanguineRose ] :3
05:36:29 [-nachash ] that doesn't add up to anything
05:36:32 [-SanguineRose ] well I never admitted to doing the dox
05:36:33 [-nachash ] Yeah, and that lol
05:36:39 [-SanguineRose ] he just tweeted it for me and shadow
05:36:48 [-nachash ] lol
05:36:51 [-nachash ] Well, gl finding you anyway
05:36:53 [-SanguineRose ] not sure if it will become an issue but I doubt it
05:36:58 [-nachash ] I'm opretty sure those dox you have up are fake
05:37:02 [-SanguineRose ] lol
05:37:02 [-nachash ] pretty
05:37:08 [-nachash ] I'm personally not worried
05:37:09 [-SanguineRose ] nah, its my real name
05:37:11 [-SanguineRose ] lol
05:37:19 [-nachash ] I've known feds have had me in their crosshairs
05:37:28 [-nachash ] because of ev0's blatant attempts at entrapment
05:37:42 [-SanguineRose ] he tried entrapping me too
05:37:47 [-SanguineRose ] but I already knew he was a fed
05:37:48 [-SanguineRose ] for ages
05:37:50 [-SanguineRose ] lol
05:37:57 [-SanguineRose ] I loled balls when ev0 and krashed got together
05:39:38 [-nachash ] lol, same
```

DeepPaste

Your Deep-Shit Hoster for special shit

Results for 6f434c51201ecf5dc794535f3d15c15b:

FBI Database Emails w Passwords

PunkNugget666, February 8, 2018 - 9:39 pm UTC

```
tthew.giacobbi@ic.fbi.gov - a374090d426651ef8a8338775378406eaf8bb294
erickbolt@ic.fbi.gov - 49eald8fc96f105e62f79f84c86f3189e385b960
cywatch@ic.fbi.gov - 3f0291d3a60edb29cd6f168369fd8ae9581f65cd
sacramento@ic.fbi.gov - 971636691d06c3e641150ddd661db9a8517d0827
kevin.oconnor@ic.fbi.gov - f0964c1bfffaf353920e89b2da2799ce509b7cc42
andrea.krauth@ic.fbi.gov - 129dad5ea12de65aaf750b92d7dfc494edadb62
justina.acayan@ic.fbi.gov - abc5d98fa429263c380491d19174f2e767c0e8fd
myloshia.robinson@ic.fbi.gov - 63236eadddbb3b803714c629323b2f2bf5fc25df
james.laflin@ic.fbi.gov - f4c6f59d534b67d338c18e4992f68e7b62594d0c
washington.field@ic.fbi.gov - 7d47638011e6a12e343123e9f9740d70cbd459a8
j.colleen.brown@ic.fbi.gov - 00a084333f997849e38c353d08c670b2bc8404fa
lorraine.kratzer@ic.fbi.gov - 868bc98486968c23c0e34b1fdce6b0ae2b523f9b
markgiuliano@ic.fbi.gov - c89751625dabc5699262727a62e8697600c1bee0
andrew.mccabe@ic.fbi.gov - c4c261406f09f057f19ea816317e75b5d25cb9df
jason.pack@ic.fbi.gov - 841aabc3f1e09acf671e25ae84bf0a51a52b5f3d
daniel.garrabrants@ic.fbi.gov - celsa3900f44ac96e4dc9707f69d8c1cldb0759937
julie.rosplach@ic.fbi.gov - 854e9bba1fe309419663c51f0cd29b1406cd9096
celia.longoria@ic.fbi.gov - 1d0db1fef602ba79b4375520bdebe18055b85b05
joshua.campbell@ic.fbi.gov - 10e39531cda0e8478203f250ec41a461130e6bd
shawn.scott@ic.fbi.gov - a981436d2b9ca8d8c4130fc9bd93a0131ee44a08
john.dziedzic@ic.fbi.gov - 46311ba2bbee14b95749dd71ae0ae02f8bd7d4e70
kathleen.hotakainen@ic.fbi.gov - 777ef8c5bd9d947228b7732e23d0c5d2dda9cca2
richard.lara@ic.fbi.gov - 214039fd957891597dc731452cbe047a12c228da
theresa.powell@ic.fbi.gov - 934bd6f879749ba66e7c46eb355f477f2504e799
mueller.cv@ic.fbi.gov - 9746633027a1e45a21fba5e02a476edd35ea2fa0
marc.cappellini@ic.fbi.gov - 7d3d3978c540e72a57fc7ad644da4cadd4f01f17
ron.avila@ic.fbi.gov - ef1da87cc7abdb956a2ec3614f532b5da263953a
leoka.statistics@ic.fbi.gov - 488c7eb05d7b7e6abe7f0c11c7dc20df310aab7
jeanette.harper@ic.fbi.gov - c49b7ad104f0e68cfea7ba3da3205feeb930dcda
selwyn.jamison@ic.fbi.gov - 2dad125c0c244a8cad69951515ecdeb75b0b1daa
craig.betbeze@ic.fbi.gov - 762a4d4bc0c6cdd0a2bcf6b7c7e125f35cb3bb88
```

STATE SPONSORED HACKING



SOME RECENT CASES: PRIVATE SECTOR



THE SCALE OF CONSUMER CYBERCRIME

378 MILLION VICTIMS PER YEAR

NEARLY 2.8 TIMES AS MANY BABIES BORN EACH YEAR

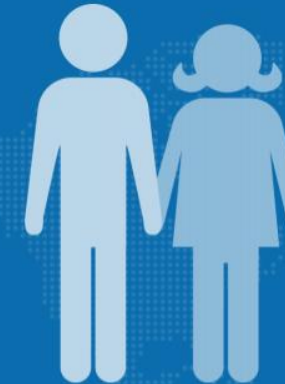


1 MILLION +
VICTIMS PER DAY

ENOUGH TO FILL WEMBLEY STADIUM (ENGLAND) MORE THAN 10 TIMES



12 VICTIMS PER SECOND



50% OF ONLINE ADULTS

HAVE BEEN VICTIMS OF CYBERCRIME AND / OR NEGATIVE ONLINE SITUATIONS IN THE PAST YEAR
(e.g., RECEIVED NUDE IMAGES FROM STRANGERS OR WERE BULLIED OR STALKED ONLINE)

41% OF ONLINE ADULTS

HAVE FALLEN VICTIM TO ATTACKS SUCH AS MALWARE, VIRUSES, HACKING, SCAMS, FRAUD AND THEFT



Global Cybersecurity Challenges

- Threat actors becoming more sophisticated
- Digital data is more pervasive
- Corporation are becoming more “open”
- Complications of cross platform solutions and interconnectivity
- Lack of available skilled cyber manpower
- High costs related to cyber manpower
- Difficulty in assessing background and experience
- Lack of quality flexible training options in cyber

The background is a dark blue, futuristic digital interface. On the left side, there is a large, glowing orange and yellow circular light effect, resembling a lens or a portal. Overlaid on this are various semi-transparent, light blue geometric shapes and lines, some containing text. The text includes 'LINKED DATA', 'SENSORS', 'VIRTUAL PROPERTY', 'CLOUD COMPUTING', 'MATERIALS', 'USER INTERFACE', and 'MEDIA'. There are also numbered circles (1, 2, 3, 4, 5, 6) connected by lines, suggesting a sequence or a process. The overall aesthetic is high-tech and digital.

Phishing Demo

The background is a dark blue gradient with futuristic, semi-transparent digital overlays. On the left, there's a large circular graphic with concentric rings and a bright orange-yellow light source. Various text labels are scattered throughout: 'LINKED DATA', 'SENSORS', 'VIRTUAL PROPERTY', 'CLOUD COMPUTING' in the top left; 'MATERIALS' and 'USER INTERFACE' in the center; 'MEDIA' in the bottom right; and 'ROBOTICS' and 'CLOUD' in the bottom left. A small bar chart is visible in the top right corner of the overlay area.

Threats To Industry

Threats to Industry

‘Those critical elements of infrastructure... which could result in:

- a) Major detrimental impact... essential services
- b) Significant impact on national security, national defence, or the functioning of the state.’

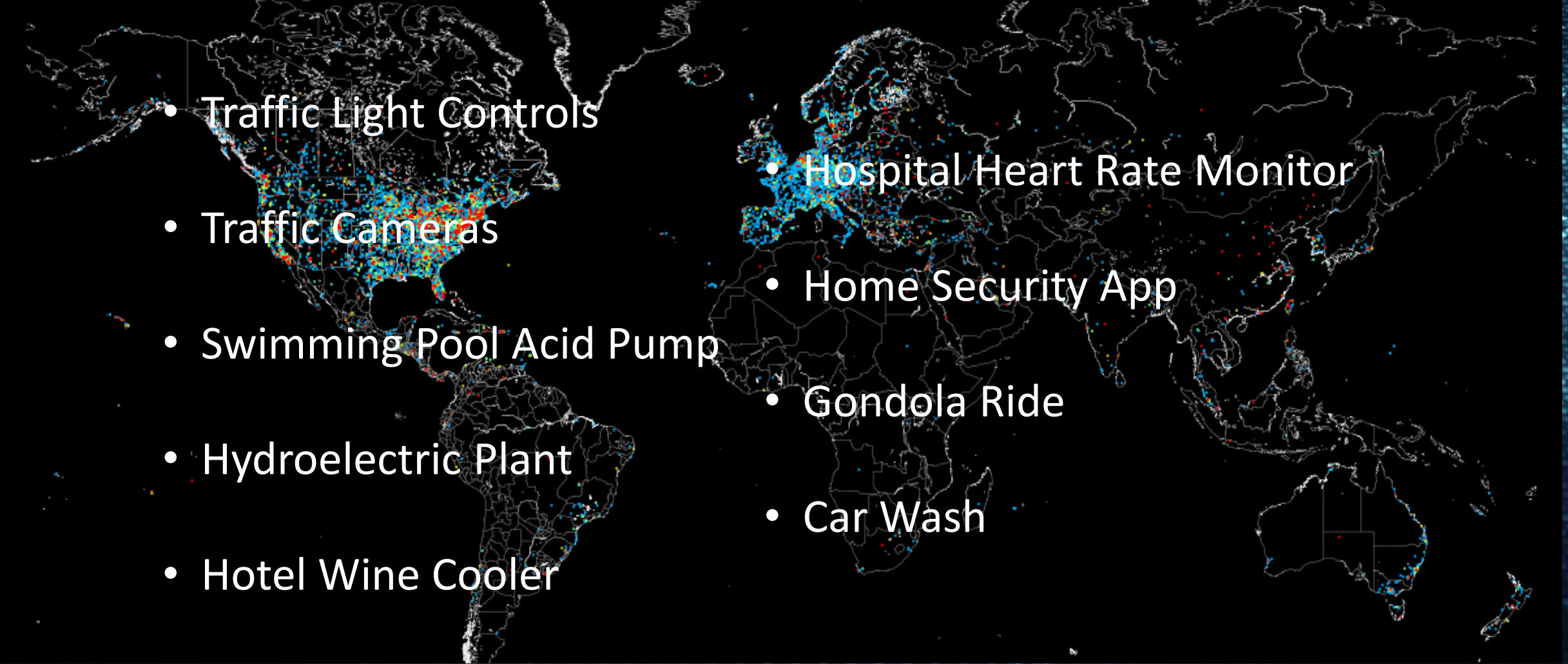
Critical National Infrastructure:

- Energy
- Government
- Health
- Transport



Client Projects

Map of Industrial Control Networks on the Internet

- 
- A world map with a dark background, showing the outlines of continents. Numerous small, multi-colored dots (red, blue, green, yellow) are scattered across the map, representing the locations of industrial control networks connected to the Internet. The dots are most densely clustered in North America and Europe.
- Traffic Light Controls
 - Traffic Cameras
 - Swimming Pool Acid Pump
 - Hydroelectric Plant
 - Hotel Wine Cooler
 - Hospital Heart Rate Monitor
 - Home Security App
 - Gondola Ride
 - Car Wash

The background is a dark blue gradient with a futuristic, high-tech aesthetic. On the left side, there is a complex digital interface. It features a large, glowing orange and yellow circular light source, possibly representing a sun or a powerful energy source. Overlaid on this are various semi-transparent, light blue and white geometric shapes, including circles, rectangles, and lines, which form a network or data structure. Text labels in a clean, sans-serif font are scattered throughout the interface, including "LINKED DATA", "SENSORS", "VIRTUAL PROPERTY", "CLOUD COMPUTING", "MATERIALS", "USER INTERFACE", and "MEDIA". Some of these labels are enclosed in small, light blue rectangular boxes. The overall effect is one of advanced technology and digital connectivity.

For You

How Secure are your Devices?



The screenshot shows the Shodan website homepage. The browser address bar displays 'https://www.shodan.io'. The navigation bar includes links for 'Shodan', 'Developers', 'Book', and 'View All...'. The main header features the Shodan logo, a search bar, and buttons for 'Explore', 'Developer Pricing', 'Enterprise Access', 'Contact Us', 'New to Shodan?', and 'Login or Register'. The main content area has a large heading 'The search engine for the Web' with 'the Web' highlighted in red. Below this, it states 'Shodan is the world's first search engine for Internet-connected devices.' and provides buttons for 'Create a Free Account' and 'Getting Started'. The background of the main content area features a wireframe globe with red virus-like icons and IP addresses such as '67.20.69.105', '50.87.75.184', and '104.18.61.231'.



Explore the Internet of Things

Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.



See the Big Picture

Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!



Monitor Network Security

Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.



Get a Competitive Advantage

Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

How Secure are your Devices?



The background is a dark blue, futuristic digital interface. On the left side, there are several circular and rectangular panels with glowing orange and yellow light effects. These panels contain various labels and icons: 'LINKED DATA', 'SENSORS', 'VIRTUAL PROPERTY', 'CLOUD COMPUTING', 'MATERIALS', 'USER INTERFACE', and 'MEDIA'. There are also numbered circles (1, 2, 3, 4, 5, 6) and a bar chart icon. The overall aesthetic is high-tech and digital.

End User Best Practices

End User Best Practices

**Always lock your
Devices**

**Use a Secure
Network
Connection**

**Beware of phishing
websites**

**Keep your software
updated**

**Don't bypass
protocols e.g.
firewalls, antivirus
etc**

**Back-up your
devices and data**

**Password
Management**

Use Encryption

Be Cautious

**Multi Factor
Authentication**

Why Are We Here?

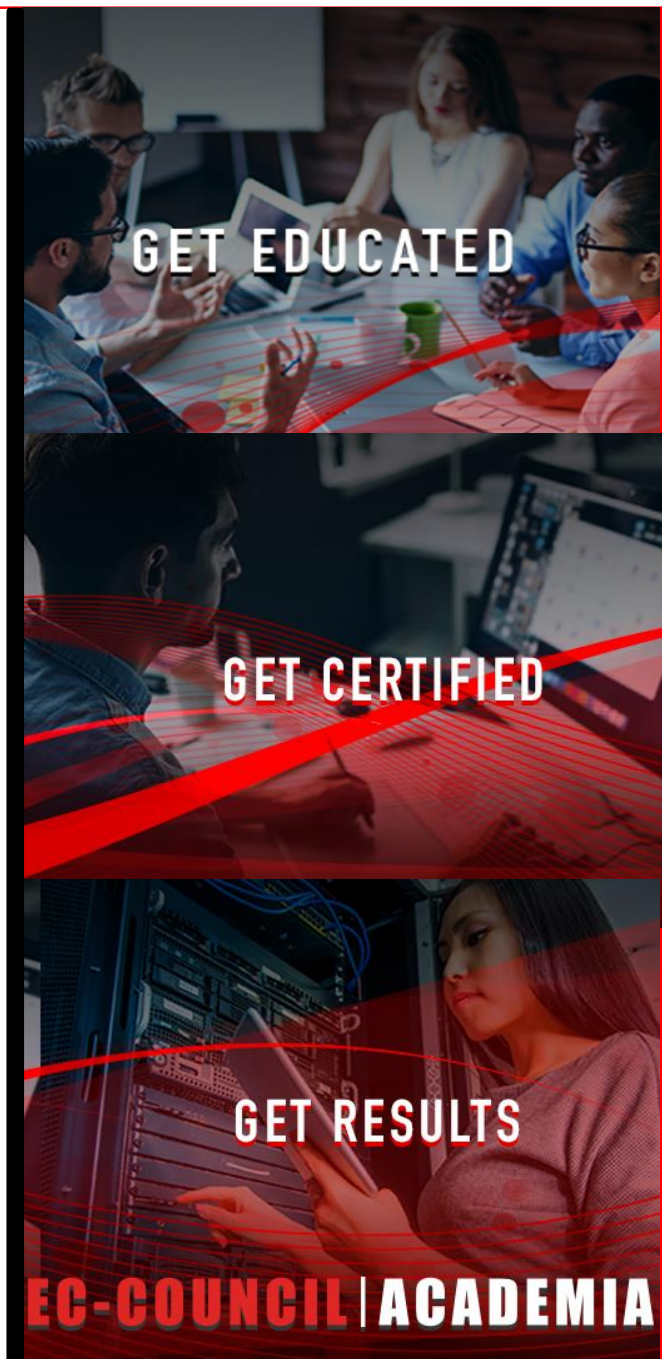
EC-Council is on a mission to raise Cybersecurity education standards across the United Kingdom and Europe...

Workforce training methods have proven success, but within education, there is a long way to go...

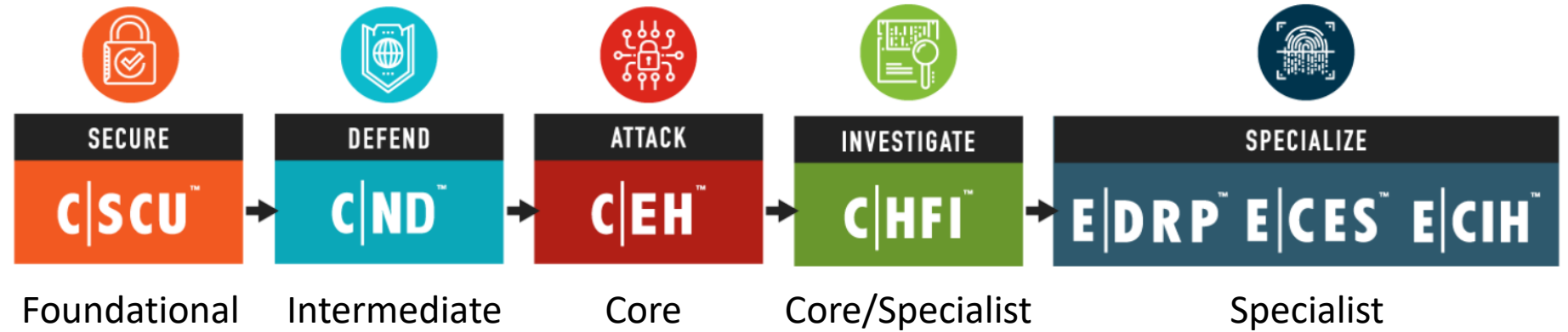
We will achieve this mission one partner at a time...

Formative Outline:

- 1) **EC-Council Certification Outcomes and Overview**
- 2) **EC-Council | Academia Partnership**
- 3) **How We Support Our Academic Partnerships**
- 5) **Graduation to Careers**
- 6) **Uniting Academia, Industry, and Government**



EC-Council Certification Outcomes and Overview



- All Computer Users

- Network Administrators
- Network security Administrators
- Network Security Engineer
- Network Defense Technicians
- CND Analyst
- Security Analyst
- Security Operator
- And more...

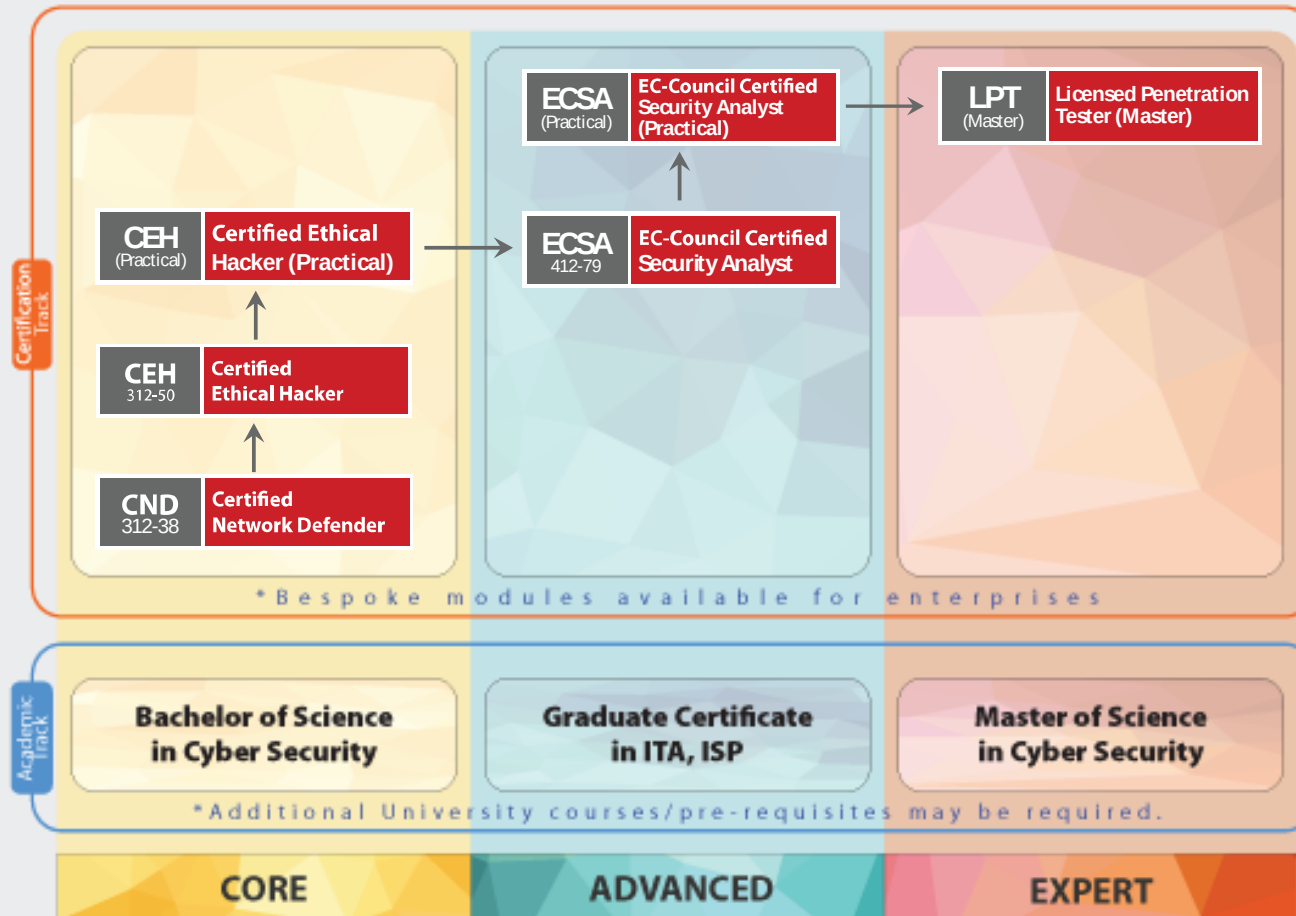
- Security Officers
- Auditors
- Security Professionals
- Site Administrators
- And more...

- Police and other law enforcement personnel
- Defense and Military personnel
- e-Business Security professionals
- Systems administrators
- Legal professionals
- Banking, Insurance and other professionals
- Government agencies
- IT managers
- And more...

- IT Professionals in the BC/DR or System Administration domain
- Business Continuity and Disaster Recovery Consultants
- IT Risk Managers and Consultants
- CISOs and IT Directors
- Incident handlers,
- Risk assessment admins
- Penetration testers,
- And more...

EC-Council

Vulnerability Assessment & Penetration Testing (VAPT)



This track maps to NICE's Specialty Areas:

1. Protect and Defend (PR)

- a. Cybersecurity Defense Analysis (DA)
- b. Cybersecurity Defense Infrastructure

- Support (INF)
- c. Incident Response (IR)
- d. Vulnerability Assessment and Management (VA)

2. Securely Provision (SP)

- a. Test and Evaluation

3. Analyze (AN)

- a. Threat Analysis (TA)
- b. Exploitation Analysis (XA)

Job Roles

- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Security Analyst
- Information Security Officers
- Information Security Auditors
- Risk/Vulnerability Analyst

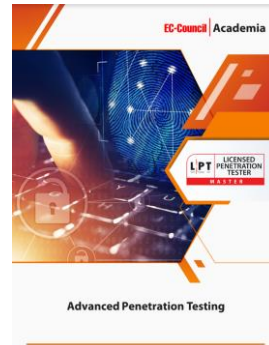
Our Certified VAPT Professionals are Employed at:



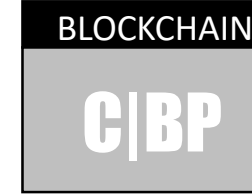
EC-Council Certification Outcomes and Overview



Advanced / Expert



Executive



Blockchain



- Ethical Hackers
- Penetration Testers
- Network server administrators
- Firewall Administrators
- Security Testers
- System Administrators and Risk Assessment professionals
- And more...

- CISO's
- Information Security Managers
- CIO's
- CTO's
- Anyone in Executive Leadership

- Business Professionals & Technology Enthusiasts

EC-Council

EC-Council
Certification
Outcomes and
Overview

Practical Assessments

EC-Council



CORE

(6 Hour Practical)

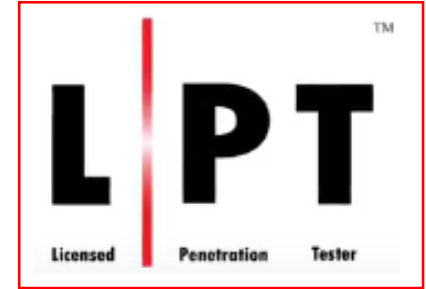
6 Hours Total



ADVANCED

(6 Hour Practical)
+
(6 Hour Practical)

12 Hours Total



MASTER EXPERT

(6 Hour Practical)
+
(6 Hour Practical)
+
(6 Hour Practical)

18 Hours Total

EC-Council Certification Outcomes and Current Trends

Content Refresh Cycles: Why institutions rely on us...

EC-Council | Academia



2 Year Full
Program Refresh



Brand new tools,
technology &
tactics

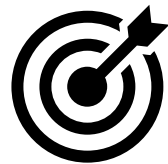


New eBooks,
labs, videos



Assessment &
Exam Updates

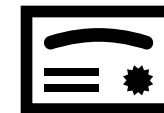
Maintaining Accreditations: Why educators take pride in partnering with us...



Maintaining
NCWF
Mapping
Standards



Maintaining
Industry
Recognition



Maintaining
ANSI
Accreditation



Maintaining
8570, VA,
COOL,
Standards

EC-Council

EC-Council Certification Outcomes and Current Trends

EC-Council

Relevant Content:

This is the worlds most advanced certified ethical hacking course with 20 of the most current security domains any individual will ever want to know when they are planning to beef up the information security posture of their organization. In 20 comprehensive modules, the course covers 340 attack technologies, commonly used by hackers.



The ECSA penetration testing course provides you with a real world hands-on penetration testing experience and is a globally accepted hacking and penetration testing class available that covers the testing of modern infrastructures, operating systems and application environments while teaching the students how to document and write a penetration testing report.

How do you create an Advanced Penetration Tester? How do you ensure that students are trained on the secrets of the trade while being pushed to their limit? The Advanced Penetration Testing course from EC-Council is built on the backbone of the Advanced Penetration Testing Cyber Range (ECCAPT) and this was designed by experts who each have more than 25 years of professional security testing across the globe. The program comes with multiple ranges designed to hone a specific set of real life pen testing skills. The ECCAPT contains more than 180 machines with more than 250 GB RAM and more than 4000 GB of storage segregated in complex network ranges with multiple militarized and demilitarized zones. It facilitates learning and demonstration of current attack vectors, penetration testing methodology, and tools. A typical range consists of 5 to 8 subnets where each subnet represents a different business unit and comprises semi-hardened and hardened machines with more than 15 Windows and Linux OS flavors.



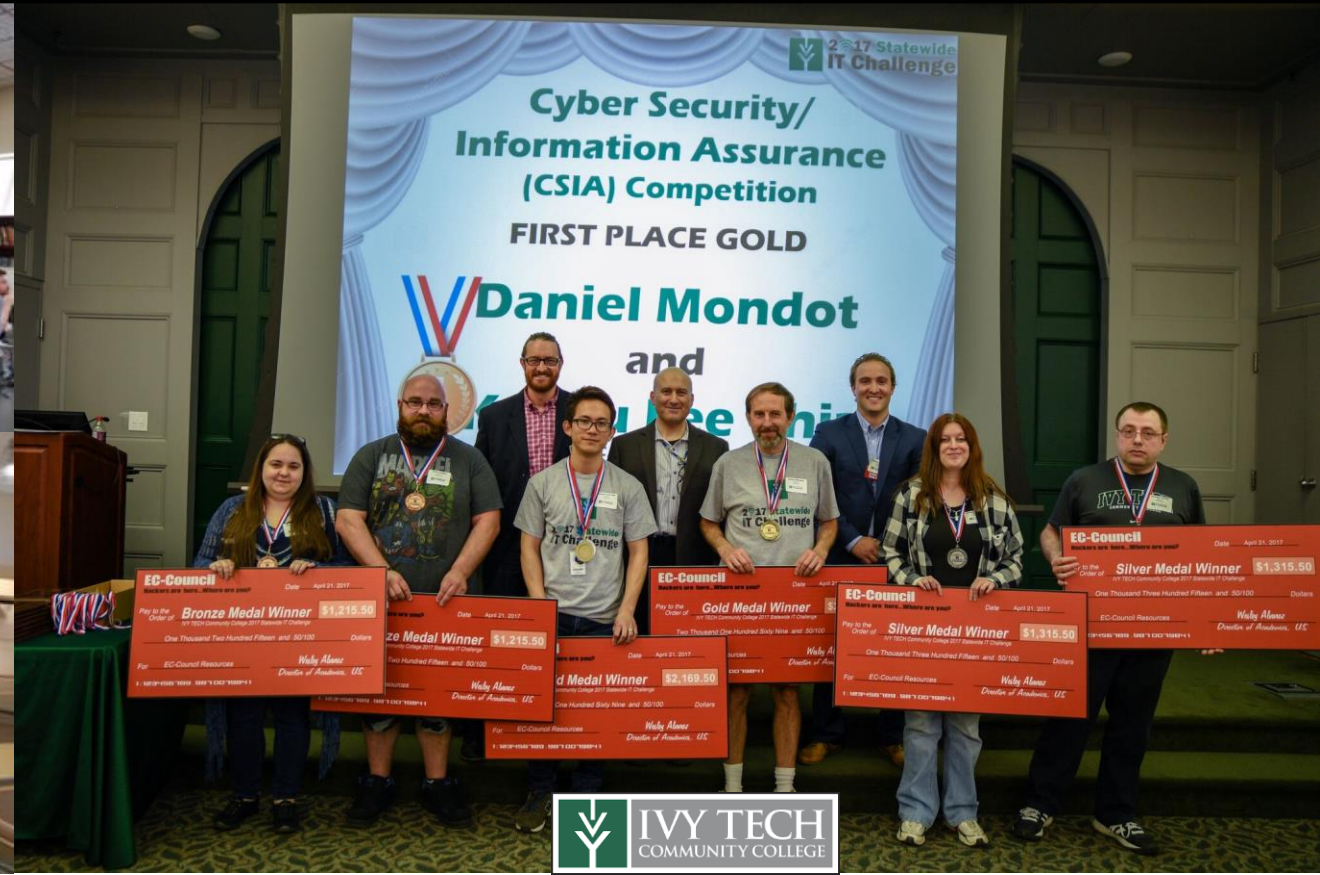
EC-Council | Academia Partnership

EC-Council academic resources have educated thousands of students across the most prestigious university degree programs since 2007...

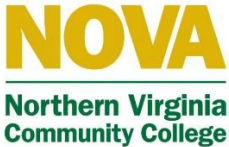


EC-Council

We Support Top Academia Events!



EC-Council | Academia 2018 Partner Awards (Invite Only)



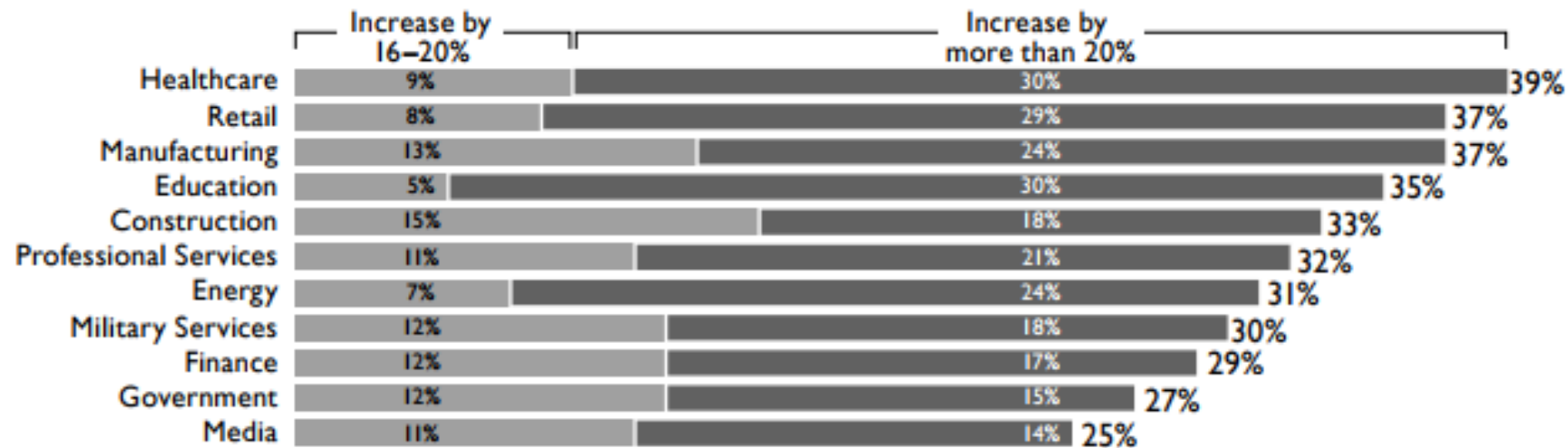


WHO?

EMPLOYMENT OPPORTUNITIES

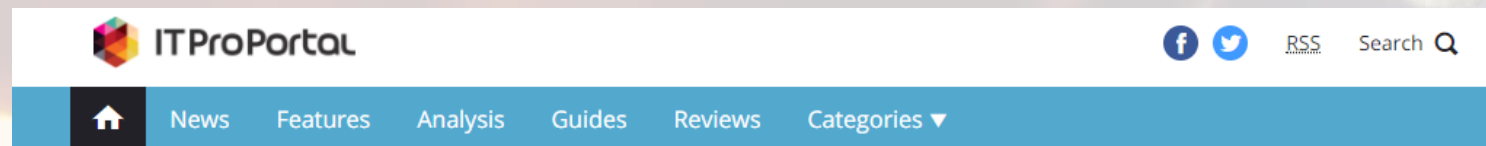
2017 Global Information Security Workforce Study

Exhibit 6: Hiring Managers Expecting to Increase Workforce by 15% or More By Industry (Among Managers Expecting to Increase Workforce)



Source: 2017 Global Information Security Workforce Study, (n = 2,906)

EMPLOYMENT OPPORTUNITIES



Demand for cybersecurity experts to soar in 2018

By Sead Fadilpašić December 18, 2017 [News](#)

Skills gap and high profile breaches are main causes behind increase in demand.



GET WEEKLY NEWS AND ANALYSIS

Sign up below to get the latest from IT Pro Portal, plus exclusive special offers, direct to your inbox!



Indeed Spotlight: The Global Cybersecurity Skills Gap

Posted on January 17, 2017



ANALYSIS

Cybersecurity skills shortage creating recruitment chaos

Because of the global cybersecurity skills shortage, nearly half of all cybersecurity professionals are solicited to consider other jobs at least once per week.

EMPLOYMENT OPPORTUNITIES

News › Business › Business News

A widening cyber-security skills gap is threatening UK companies

The UK corporate sector has been marred by several high-profile cases of cyber security breaches

Find a job Sign in Search ▾

on | **Sport** | **Culture** | **Lifestyle** | More ▾

UK edition ▾
The Guardian

Calling all millennials: your cybersecurity industry needs you

Global demand for cybersecurity professionals is increasing rapidly, as are the rewards accrued by those in the industry – and employers are looking to millennials to fill the gaps

Advertisement



Boost your **business**
& career today by

AVERAGE SALARY OF CYBER SECURITY PROFESSIONALS

What is the average salary for Cyber Security jobs?

The average salary for Cyber Security jobs is £72,500.

In January 2018, the average salary for Cyber Security jobs rose by £1,386 (16%).

Read on to find out how much Cyber Security jobs pay across various UK locations and industries.



How do Cyber Security jobs salaries vary across industries?

The industry with the highest salary for Cyber Security jobs is Permanent. The average Permanent salary for Cyber Security jobs is £72,500. In the last month, the salary has risen by 16 per cent.

Industry/sector	Average	Range	Monthly change*	Jobs*
Permanent	£72,500	£52,500-£82,500	▲ 16%	view jobs (113)

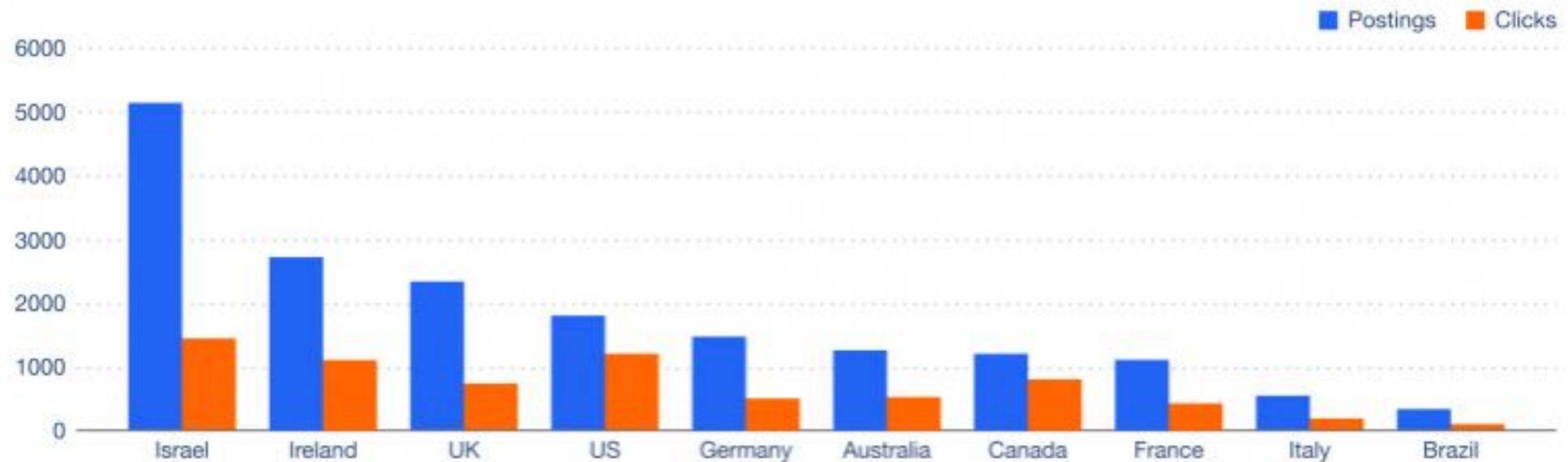
*compared to the previous month. A minus figure means the salary has gone down. Job counts are based on last month's totals.

Source: <https://www.cwjobs.co.uk/salary-checker/average-cyber-security-salary>

HOW DOES THE UK COMPARE?

Cyber Security Skills Deficit Persists Across Countries

Cyber security postings and clicks per million postings and clicks (2016Q3)



Source: Indeed

indeed

HOW DOES THE UK COMPARE?

Not Enough Job Seekers Interested in Cyber Security Postings

Share of clicks / share of postings for cyber security (2016Q3)



Israel 28.4%



UK 31.6%



Brazil 33.0%



Germany 35.0%



Italy 35.9%



France 38.6%



Ireland 38.8%



Australia 42.3%



US 66.7%



Canada 68.1%

Source: Indeed

indeed

EMPLOYMENT OPPORTUNITIES

Company Job Advertisements (CEH)

Security Analyst

Bank of England - ★★★★★ 54 reviews - London

CISSP, OSCP, Security+, CEH) being a distinct advantage. The IT Security function is part of the Technology Division within the Bank of England, and is...

3 days ago - [save job](#) - [more...](#)

Security Analyst

Legal & General Group Plc. - ★★★★★ 5 reviews - Hove

£40,000 a year

Appropriate security qualification for the role would include Security+, SSCP, GIAC Cyber Defence certifications, CEH or CISSP...

30+ days ago - [save job](#) - [more...](#)

Information Security Analyst - Bournemouth

JP Morgan Chase - ★★★★★ 14,982 reviews - Bournemouth BH7

Professional Qualification such as CEH, CISSP, CISA, CISM an advantage but not essential. As one of the main technology HUBS For EMEA the scope of work in...

JPMorgan Chase - 26 days ago - [save job](#) - [more...](#)

Security Analyst

Thames Valley Police - ★★★★★ 60 reviews - Southampton

£40,000 a year

Security+, CEH, MCSE, CCNA etc.). Thames Valley Police is the territorial police force responsible for policing the Thames Valley area covered by the counties...

CWJobs.co.uk - 25 days ago - [save job](#) - [more...](#)

Security Operations Centre Analyst

Maersk Line - ★★★★★ 531 reviews - Maidenhead

Qualifications within IT Security such as CISSP, CEH desirable though not essential. Maersk Line is a highly international and inspiring environment with an...

Sponsored by Jobsite UK - [save job](#)

Regional Chief Information Security - UK & EMEA

Estee Lauder - ★★★★★ 722 reviews - United Kingdom

Applicants will be qualified to Bachelor's Degree level as a minimum and have and have CISM, CISSP, CEH, CIPP, CISA certifications or equivalent....

11 days ago - [save job](#) - [more...](#)

GLOBALLY RECOGNISED INFOSEC CERTIFICATION

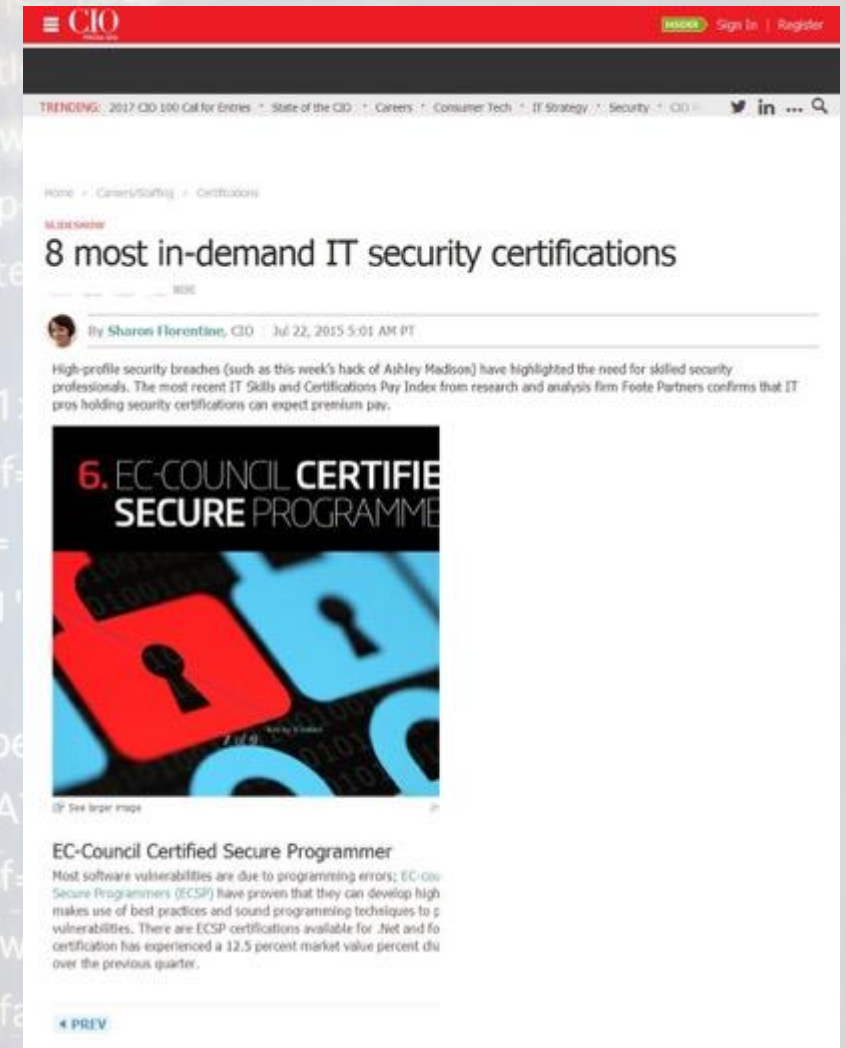
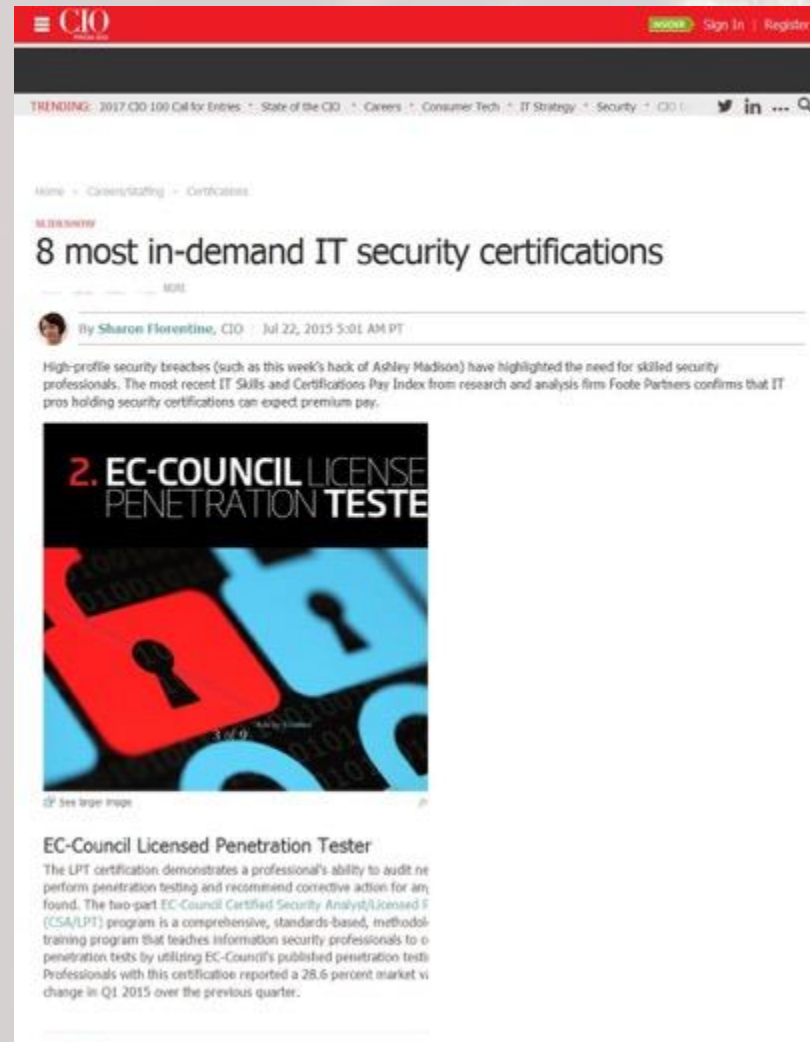
EC-Council's Certified Ethical Hacker (CEH) is placed at number one in "Best Information Security Certifications 2018" by Business News Daily.

The screenshot shows the top of a Business News Daily website. The header includes the site logo, navigation links for 'START Your Business', 'GROW Your Business', 'BUILD Your Career' (which is highlighted), 'LEAD Your Team', and 'FIND A Solution'. There are also social media icons for search, Facebook, Twitter, LinkedIn, and Pinterest. Below the header is a teal bar with links: 'GET THE JOB', 'GET AHEAD', 'OFFICE LIFE', 'WORK-LIFE BALANCE', and 'HOME OFFICE'. A large banner for Microsoft Azure is visible, with the text 'Migrate your on-premises workloads to the cloud with confidence' and a 'Try Azure for free' button. Below the banner, a disclaimer states: 'Product and service reviews are conducted independently by our editorial team, but we sometimes make money when you click on links. Learn more.' The article title 'Best Information Security Certifications 2018' is prominently displayed, followed by the byline 'By Ed Tittel and Kim Lindros, Business News Daily Contributing Writers | April 23, 2018 12:39 pm EST'. Social sharing icons for Facebook, Twitter, LinkedIn, Reddit, and StumbleUpon are shown with a 'MORE' dropdown. The article content begins with a Microsoft Azure banner and the text: 'The year 2017 marked another milestone for information security: more breaches, bigger losses, more coverage and more jobs and opportunities for IT and programming'. A photo of a man working on a laptop is visible on the right side of the article.

Source: <http://www.tomsitpro.com/articles/information-security-certifications,2-205-3.html>

GLOBALLY RECOGNISED INFOSEC CERTIFICATION

EC-Council's License Penetration Tester (LPT) and Certified Secured Programmer Hacker (CSP) covered in “8 most in demand IT Security Certifications” by CIO magazine.



Source: <http://www.cio.com/article/2951115/certifications/8-most-in-demand-it-security-certifications.html>

GLOBALLY RECOGNISED INFOSEC CERTIFICATION (CONT'D)

EC-Council's Certified Incident Handler (CIH) and Computer Hacking Forensic Investigator are featured in the ranking of "25 tech certifications earning the highest cash premiums right now" by David Foote

The screenshot shows a ComputerWorld article from the IDG Contributor Network. The article is titled "25 tech certifications earning the highest cash premiums right now" and is written by David Foote. It discusses the value of various IT certifications in the current market. The top two certifications listed are EC-Council's Certified Incident Handler (CIH) and Certified Hacking Forensic Investigator (CHFI), which are tied for the highest cash premiums. Other certifications listed include GIAC's Certified Forensics Analyst, Certified Forensics Examiner, Exploit Researcher and Advanced Penetration Tester, Web Application Penetration Tester, Open Group Master Certified IT Specialist, PMI's Professional in Business Analysis and Program Management Professional, Cisco's Certified Architect, EMC's Cloud Architect Expert (IT-as-a-Service), GIAC's Enterprise Defender, Secure Software Programmer -- Java, InfoSys Security Architecture Professional (ISSAP/CISSP), PMI's Agile Certified Practitioner, and PMI's Portfolio Management Professional.

4. (Tie) EC-Council Certified Incident Handler
EC-Council Computer Hacking Forensic Investigator
GIAC Certified Forensics Analyst
GIAC Certified Forensics Examiner
GIAC Exploit Researcher and Advanced Penetration Tester
GIAC Web Application Penetration Tester
Open Group Master Certified IT Specialist
PMI Professional in Business Analysis
PMI Program Management Professional

5. (Tie) Cisco Certified Architect
EMC Cloud Architect Expert (IT-as-a-Service)
GIAC Enterprise Defender
GIAC Secure Software Programmer -- Java
InfoSys Security Architecture Professional (ISSAP/CISSP)
PMI Agile Certified Practitioner
PMI Portfolio Management Professional

Source: <http://www.computerworld.com/article/3144525/it-management/25-tech-certifications-earning-the-highest-cash-premiums-right-now.html>

GLOBALLY RECOGNISED INFOSEC CERTIFICATION

EC-Council Certified Chief Information Security Officer Certification (C|CISO) and Certified Ethical Hacker (CEH) made into the list of Top 75 Salary Earners List

The Salary Survey 75

This year's Salary Survey included more than 800 certifications. (Seriously, people, stop creating new IT certifications.) This list of 75, ranked by average base salary in 2015, was drawn from the most statistically relevant certs in the survey — those held by the largest numbers of survey respondents. Yes, even years after the last time that you rented a powder blue tuxedo or bought a new dress for the high school prom, life is still a popularity contest. (Some things never change.) The Salary Survey is global, but roughly 42 percent of all respondents this year are from the United States, nearly four times as many as came from any other country. Accordingly, our results are shown with average U.S. salaries listed separately, followed by an average of all non-U.S. salaries, followed by a global average that combines those two groups.

CERTIFICATION	SALARY (U.S. ONLY)	SALARY (ALL NON-U.S.)	SALARY (U.S. AND WORLD)
1) PMI Program Management Professional	\$147,120	\$84,780	\$116,750
2) Open Group TOGAF 9	\$144,250	\$76,120	\$91,110
3) (ISC) ² Certified Secure Software Lifecycle Professional (CSSLP)	\$143,210	\$104,500	\$131,580
4) EC-Council Certified Chief Information Security Officer (CCISO)	\$143,050	\$116,790	\$137,800
5) (ISC) ² Certified Information Systems Security Professional (CISSP) Architecture	\$141,230	\$103,060	\$125,320
37) Cisco Certified Design Professional (CCDP)	\$118,670	\$78,330	\$99,420
38) EC-Council Certified Ethical Hacker (CEH)	\$118,370	\$79,930	\$99,880
39) Microsoft Certified Solutions Expert (MCSE) Server Infrastructure	\$117,430	\$67,430	\$88,610
40) Cisco Certified Network Professional (CCNP) Routing and Switching	\$116,210	\$67,270	\$89,670

Source: <http://certmag.com/salary-survey-2016-annual-salary-survey/>

GLOBALLY RECOGNISED INFOSEC CERTIFICATION

EC-Council Certified Ethical Hacker (CEH) and Computer Hacking Forensics Investigator (CHFI) is rated within the Top 50 most desired certifications of 2016.

Source: <http://certmag.com/salary-survey-2015-interest-certification-still-strong>



GLOBAL RECOGNITIONS (CONT'D)

EC-COUNCIL IS RECOGNISED AS A WORLD LEADER BY THE UK GOVERNMENT

EC-Council Courseware

1. In high demand on UK Government contracts
2. Four EC-Council certifications required by the Nuclear Decommissioning Authority
3. More than any other Cyber Security Vendor

The screenshot shows the GOV.UK Contracts Finder interface. At the top, the GOV.UK logo and 'Contracts Finder' title are visible. Below the header, a 'BETA' banner states 'This is a new service - your feedback will help us improve it.' with 'Register' and 'Sign in' links. The breadcrumb trail reads 'Home > Search results > Cyber Security Training'. The main heading is 'Cyber Security Training' with the subtext 'NUCLEAR DECOMMISSIONING AUTHORITY'. A notice states: 'Closed opportunity - This means that the contract is currently closed. The buying department may be considering suppliers that have already applied, or no suitable offers were made.' To the right of this notice are two green buttons: 'Watch this notice' and 'Print this notice'. Below the notice, the 'Contract summary' section includes 'Industry' (Construction and Real Estate, Printing and Publishing, Education), 'Location of contract' (Any region), and 'Description'. The description lists various training courses: 'Provision of the following training courses to NDA: EC Council Certified CISO, GIAC Certified Incident Handler (GCIH), EC Council Certified Incident Handler (ECIH), EC Council Certified Network Defender, ISACA Certified in Risk and Information Systems Control (CRISC), GIAC Global Industrial Control System Professional (GISCP), GDPR Master Class, ISO 27001 Lead Implementer, ISO 27001 Lead Auditor, ISACA Certified Information Systems Auditor (CISA), GIAC Information Security Fundamentals (GISF), EC Council Computer Hacking Forensic Investigator (CHFI)'. The last four items are highlighted with red boxes. At the bottom of the description, it says 'To include certification and examination costs.'

GLOBAL RECOGNITIONS (CONT'D)



Certified Ethical Hacker Certification

COURSEWARE LEVEL

- PROVIDED BY **EC-COUNCIL** -

KNOWLEDGE AREA(S)

**Malware and Attack Technologies | Operating Systems & Virtualisation
Security | Secure Software Design and Development | Security Operations and
Incident Management**

The courseware only for this certification has been certified for use as part of a fully certified GCHQ-certified Training package.

 Focus skills: C2, D2, E1, E3 | Supporting skills: D1, E2, F2, F3, G1

 **CLASSROOM COURSE**  **UNITED KINGDOM**

THANK YOU

EC-Council



Philip Blake

EC-Council

European Country Manager

Philip.blake@eccouncil.org