

The cybersecurity landscape and the need for training



You are Invited

À la formation:

Certified Ethical Hacker v10

Du 12 au 16 novembre 2018

Montréal · en ligne

Période promo: -20%
CODE: CEHV10NOV2018

Le départ est garanti · joignez-vous à nous!

Montreal, Oct 19, 2018 (IssueWire.com) - We all remember the early 2000s, that time when systems and networks administrators were primarily concerned to "make the computer systems work". At the time, the primary focus was to ensure stability of the very unstable environments we have to deal with - not much was dedicated to ensure information security was in place. Objectives were not the same - hackers hacked because of their curiosity, the desire to explore something else and to become the first at doing it. Today, hacking is a crime that is driven by cybercriminals all over the world, affecting millions of our production networks and creating billions of dollars of damage to companies' reputation, data (the most expensive component of a cyber-attack is information loss, which represents 43 percent of costs, source: Accenture), and to its people.

But, what else has changed? Today, we take a lot for granted - everyone needs to have information synchronized everywhere, and the amount of data that we exchange and store every day is not to be compared with that time. So, that changes the landscape of how we ensure information is now safe - hackers, accessibility, and volume. What is to be done now to ensure information security is in place?

Over the years, companies had to adapt to the changes and begin implementing countermeasures that had to be sufficiently reliable to stop most common threats (damage related to cybercrime is projected to hit \$6 trillion annually by 2021 according to Cybersecurity Ventures). Then, it goes further - sophisticated attacks cannot be easily detected, thus a comprehensive cyber defense plan has to be setup and revised regularly to keep up with these kinds of threats.

But, technology to prevent the majority (if not all) of cyberattacks is present and quite mature. In fact, it has been like this for many years. Cybersecurity companies have seen an opportunity at the very beginning. The question is: do we have skilled individuals that know which solution can be used best at a specific moment to reduce the risks and ensure a safe operation of our systems? If not, how can we leverage cybersecurity knowledge? Is there a "universal formula" that solves the problem related to information leakage, system destruction or data tampering?

In collaboration with EC-Council, Eccentrix is offering a wide range of cybersecurity trainings which objectives are numerous - information security awareness, penetration testing, system hacking, forensics, and multiple other disciplines. Knowledge of how the cybersecurity landscape is today, and how it affects organizations and individuals is key in understanding the countermeasures - the defense mechanisms that need to be put in place to prevent cybersecurity attacks.

"Exponential rise in Cybercrime in recent times has become one of the most critical challenges plaguing North America along with a lack of capable cybersecurity personnel in the market adds to the predicament. A new report out from Cybersecurity Ventures estimates there will be [3.5 million unfilled cybersecurity jobs by 2021](#), up from 1 million openings in 2016. It's the perfect time for Canadians to opt for Cybersecurity as a career and be part of one of the years highest paying and most in demand profession. EC-Council together with Eccentrix aims to equip Canadians with relevant Cyber skills that are considered a benchmark for Cyber Capabilities by both the [Government and the Corporate entities](#) in North America," said Danish Arshad, Executive Director EC-Council.

Our flagship training, the [Certified Ethical Hacker v10](#) is the most comprehensive offense-driven course teaching professionals how these cyberattacks are executed so that they know exactly what they can do to prevent them. This rigorous training is composed of more than 20 topics on cybersecurity software, and extensive labs that cover the most realistic attack methods. The course also prepares participants for the CEHv10 certification and is provided with many benefits, such as extended lab access, a

complementary [STORM device](#) as well as an exam voucher – all included in the training cost.

For more information, visit our [website](#) to learn more about the course and the additional course offering we have in partnership with EC-Council. Don't miss the opportunity to protect your networks from cyberattacks!

About EC-Council

The International Council of E-Commerce Consultants (EC-Council) is a member-based organization that certifies individuals in various e-business and security skills. EC-Council is the owner and developer of the world-famous E-Council Certified Ethical Hacker (CEH), Computer Hacking Forensics Investigator (CHFI), Certified Security Analyst (ECSA), License Penetration Tester (LPT) programs, and various others offered in 150 countries around the globe. EC-Council has certified over 200,000 information security professionals globally.

EC-Council certification programs are recognized worldwide and have received endorsements from various government agencies including the US Federal Government via the Montgomery GI Bill, the US Government National Security Agency (NSA), the Committee on National Security Systems (CNSS) certifying EC-Council's Certified Ethical Hacking (CEH), Network Security Administrator (ENSA), Computer Hacking Forensics Investigator (CHFI), Disaster Recovery Professional (EDRP), Certified Security Analyst (ECSA), Licensed Penetration Tester (LPT) program for meeting the 4011, 4012, 4013A, 4014, 4015 and 4016 training standards for information security professionals and most recently EC-Council has received accreditation from the American National Standards Institute (ANSI).

Media Contact

Eccentrix

info@eccentrix.ca

1-888-718-9732

2000 McGill College Avenue, 6f

Source : Eccentrix

See on IssueWire : <https://www.issuewire.com/the-cybersecurity-landscape-and-the-need-for-training-1614760597150397>