ZETA-WEB
BUSINESS SOLUTIONS

...we make IT work

Cyber SECURITY

EC-Council
Accredited
Training Center
Cert ID: EATC322378

Our Vision

To be the preferred ICT solutions provider creating value for our customers through innovative and reliable enterprise solutions across Africa.

Our Mission

Our mission is to effectively facilitate diverse methods of empowerment and profrssionally based performance deliverrables through product uniqueness that meet our customers' needs. We are positioned to provide all-inclusive ICT solutions to our diverse customer base.

ABOUT US

Zeta-Web Nigeria is your IT Partner for all your Business-enabling, Operational and Security needs.

We offer a full range of IT Solutions and Security services to meet organizational needs and requirements.

For your peace of mind, we carry-out comprehensive analysis of your business and proffer solutions to areas that are most vulnerable to security breaches and/or enhance your existing infrastructure to make them up to date.

We provide you with training solutions and services that allows you **Save Cost** by helping you build a cost-effective structure, **Reduce Complexity** by adopting an approach for simplified management and automated operations; and enable you to **Grow Efficiently** by protecting your equipment, business data and applications related to your day-to-day activities.

OUR SECURITY PHILOSOPHY

At Zeta-Web Nigeria, Data Security ***always*** comes First. Our systematic approach to establishing and maintaining the highest standards of Security (data) means you can focus on getting the job done without risk to your people, services or business.

OUR PEOPLE

Our people are quite knowledgeable in their different areas of specialization, thereby guaranteeing the very best in Customer Service and Retention.
We adopt a collaborative approach – **Working as One Team with One Goal**, means that our customers get a solution that is *just right* for them – **On Time** and **On Budget!**

OUR TRAINING

Our people are industry leaders and undergo continuous training and professional development, thereby guaranteeing the very best in customer service.

Our instructors (local and international) are quite versatile in EC Council's Cybersecurity and how it can be effectively put to use especially for the peculiarities of the African community, and as such you are getting **High Value for Less!**

With cyber-attacks becoming more oriented towards data theft, it is vital for both businesses and individuals to take extra precautionary methods when it comes to data protection and that protection is what we offer you – your staff, which will translate to huge cost savings for your business.

CYBERSECURITY

What you need to know

Mishandling data can lead to customers mistrust in your business, ultimately leading to huge loss in revenue for the company. It is hard to see cybersecurity as anything, but a **Business Risk Issue**.
The fear of reputational damage to an organization is slowly forcing businesses to participate more actively in cybersecurity strategies and ensuring adequate controls are put in place.

Although the complete elimination of cyber risk is impossible, it is important for a company to understand the importance of linking cybersecurity and business strategies as this will enable them face challenges head-on, make better decisions, and provide customers and employees with better disclosure.

Businesses must confront cybersecurity as a business risk to help increase insider safety and contain outside threats. To be able to treat cybersecurity as a business risk, top management in any company/business should have an understanding of what their digital assets are and how any security policy might affect them.
Constant cybersecurity awareness training programs for employees and vendors will also help create a safer cyber environment and control insider threats to a large extent.

Security awareness training programs such as EC-Council's **Certified Secure Computer User (CSCU)** is specifically designed for today's computer users who rely on the internet extensively to work, study, and play. This course introduces students to security and teaches them how to secure operating systems, internet safety, social network safety, mobile safety, email safety, and data backup and disaster recovery.

Cybersecurity is not just the responsibility of the IT department nor is it the responsibility of the top management alone; it requires a collective effort from all levels of an organization in order to develop a cybersafe environment.

As a professional, it is imperative that you help create a secure cyberspace by attending and understanding Cyber Risks / Threats Awareness training programs.
You can also play a bigger role in the cybersecurity industry with the help of EC-Council – the world's leading information security certification **Certified Ethical Hacker (CEH)**, in order to spread awareness and encourage more professionals in cybersecurity.

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED SECURE COMPUTER USER (CSCU)

Course Description:

The purpose of the CSCU training program is to provide individuals with the necessary knowledge and skills to protect their information assets. This class will immerse students into an interactive environment where they will acquire a fundamental understanding of various computer and network security threats such as identity theft, credit card fraud, online banking phishing scams, virus and backdoors, emails hoaxes, sex offenders lurking online, loss of confidential information, hacking attacks and social engineering. More importantly, the skills learned from the class helps students take the necessary steps to mitigate their security exposure.

EC-Council's **Certified Secure Computer User (CSCU)** Foundation program is a simplified cyber- security awareness course created to teach students and other end-users how to protect themselves from cyber threats. This course was designed with a special focus on some of today's most vulnerable computer users: young people and non-technical end users.

TRAINING & EXAMS FEES:

- Self-Paced Study: $150
- On Premise Training: $200
- **Voucher valid for 1 year**

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED ETHICAL HACKER

COURSE OUTLINE:

A **Certified Ethical Hacker** is a skilled professional who understands and knows how to look for weaknesses and vulnerabilities in target systems and uses the same knowledge and tools as a malicious hacker, but in a lawful and legitimate manner to assess the security posture of a target system(s). The CEH credential certifies individuals in the specific network security discipline of Ethical Hacking from a vendor-neutral perspective.

The **Certified Ethical Hacker** program is the most desired information security training program any information security professional will ever want to be in. To master the hacking technologies, you will need to become one, but an ethical one! The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals alike to break into an organization. As we put it, **"To beat a hacker, you need to think like a hacker".**

This course will immerse you into the Hacker Mindset so that you will be able to defend against future attacks. The security mindset in any organization must not be limited to the silos of a certain vendor, technologies or pieces of equipment.
The ethical hacking course puts you in the driver's seat of a hands-on environment with a systematic process. Here, you will be exposed to an entirely different way of achieving optimal information security posture in their organization; by hacking it! You will scan, test, hack and secure your own systems. You will be taught the five phases of ethical hacking and the ways to approach your target and succeed at breaking in every time! The five phases include Reconnaissance, Gaining Access, Enumeration, Maintaining Access, and covering your tracks.

TRAINING & EXAMS FEES:

- Self-Paced Study: $400
- On Premise Training: $650
- **Voucher valid for 1 year**

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED ETHICAL HACKER - MASTER (CEH MASTER)

To be placed at the tip of your organization's cyber spear, you must be confident, proficient in your job, and be at the top of your game. You must be able to think on your feet, act quickly, appropriately, and proportionally. Make a mistake and bad things can happen.

CEH Master gives you the opportunity to prove to your employer, your peers, and most importantly to yourself that you can in fact take on and overcome challenges found in everyday life as an Ethical Hacker. To prove this, though, we don't give you exam simulations. We test your abilities with real-world challenges in a real-world environment, and with a time limit, just as you would find in your job.

Do you run towards danger? Do you take charge during unsettling and challenging times? Do you want to be the one your team can rely on to take the fight to the bad guys? If your answers are yes, prove yourself with CEH Master!

CEH Master, is the next evolution for the world-renowned **Certified Ethical Hacker** credential, and a logical 'next step' for those holding the prestigious certification. Earning the CEH Master designation is your way of saying, "I learned it, I understood it, and I proved it."

The purpose of the CEH credential is to:

Help you master an ethical hacking methodology that can be used in a penetration testing or ethical hacking situation. You walk out the door with ethical hacking skills that are highly in demand, as well as the internationally recognized **Certified Ethical Hacker** certification!

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED NETWORK DEFENDER CERTIFICATION (CND)

The **Certified Network Defender** (CND) certification program focuses on creating Network Administrators who are trained on protecting, detecting and responding to the threats on the network. Network administrators are usually familiar with network components, traffic, performance and utilization, network topology, location of each system, security policy, etc. A CND will get the fundamental understanding of the true construct of data transfer, network technologies, software technologies so that the they understand how networks operate, understand what software is automating and how to analyze the subject material. In addition, network defense fundamentals, the application of network security controls, protocols, perimeter appliances, secure IDS, VPN and firewall configuration, intricacies of network traffic signature, analysis and vulnerability scanning are also covered which will help the Network Administrator design greater network security policies and successful incident response plans.

CND is a skills-based, lab intensive program based on a job-task analysis and cybersecurity education framework presented by the National Initiative of Cybersecurity Education (NICE).
Network administrator can play a significant role in network defense and become first line of defense for any organizations.

The purpose of the CND credential is to:

Validate the skills that will help the Network Administrators foster resiliency and continuity of operations during attacks.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

Certified Threat Intelligence Analyst (CTIA)

Certified Threat Intelligence Analyst (CTIA) is designed and developed in collaboration with cybersecurity and threat intelligence experts across the globe to help organizations identify and mitigate business risks by converting unknown internal and external threats into known threats. It is a comprehensive, specialist-level program that teaches a structured approach for building effective threat intelligence.

In the ever-changing threat landscape, CTIA is an essential program for those who deal with cyber threats on a daily basis. Organizations today demand a professional-level cybersecurity threat intelligence analyst who can extract the intelligence from data by implementing various advanced strategies. Such professional-level programs can only be achieved when the core of the curricula maps with and is compliant to government and industry published threat intelligence frameworks.

CTIA is a method-driven program that uses a holistic approach, covering concepts from planning the threat intelligence project to building a report to disseminating threat intelligence. These concepts are highly essential while building effective threat intelligence and, when used properly, can secure organizations from future threats or attacks.

The purpose of the CTIA credential is to:

Address all the stages involved in the Threat Intelligence Life Cycle. This attention to a realistic and futuristic approach makes CTIA one of the most comprehensive threat intelligence certifications on the market today. This program provides the solid, professional knowledge that is required for a career in threat intelligence, and enhances your skills as a Threat Intelligence Analyst, increasing your employability. It is desired by most cybersecurity engineers, analysts, and professions from around the world and is respected by hiring authorities.

This program will benefit students who are looking to build effective threat intelligence for their organization in order to combat modern-day cyber-attacks and prevent future attacks.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED SECURITY ANALYST (ECSA): PENETRATION TESTING

You are an ethical hacker. In fact, you are a Certified Ethical Hacker. Your last name is Pwned. You dream about enumeration and you can scan networks in your sleep. You have sufficient knowledge and an arsenal of hacking tools and you are also proficient in writing custom hacking code.

Is that enough?

Can you become an industry accepted security professional? Will organizations hire you to help them protect their systems? Do you have any knowledge in applying a suitable methodology to conduct a penetration test for an enterprise client?

The ECSA pentest program takes the tools and techniques you learned in the Certified Ethical Hacker course (CEH) and enhances your ability into full exploitation by teaching you how to apply the skills learned in the CEH by utilizing EC-Council's published penetration testing methodology. It focuses on pentesting methodology with an emphasis on hands-on learning.

The ECSA program offers a seamless learning progress, continuing where the CEH program left off.

Unlike most other pen-testing programs that only follow a generic kill chain methodology; the ECSA presents a set of distinguishable comprehensive methodologies that are able to cover different pentesting requirements across different verticals.

The purpose of the ECSA credential is to:

Provide 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.

A Security Credential Like No Other!

ENROLL NOW

LICENSED PENETRATION TESTER (MASTER) CERTIFICATION (LPT Master)

There are good penetration testers and then there are great penetration testers. Unless you are bent on being nothing other than the best in penetration testing, don't bother registering for this program, as you are probably not cut out for it.

Being an LPT (Master) means that you can find chinks in the armor of defense-in-depth network security models with the help of network pivoting, making exploit codes work in your favor, or by writing Bash, Python, Perl, and Ruby scripts. The exam demands that you think on your feet, be creative in your approach, and not rely on the conventional techniques. Outsmarting and out maneuvering the adversary is what sets you apart from the crowd. This completely hands-on exam offers a challenge like no other by simulating a complex network of a multi-national organization in real time. This experience will test your perseverance and focus by forcing you to outdo yourself with each new challenge.

EC-Council brings to you a new range of real-world challenges that will not only test your Pen-testing skills but guarantees you an experience that is not built for the weak hearted. If you have been looking for a way to test your Pen-testing abilities, this is your chance to prove you have what it takes.

The purpose of the LPT Master credential is to:

This Exam has One purpose: to differentiate the experts from the novices in penetration testing!
Learn professional security and penetration testing skills. The course is designed to show advanced concepts like scanning against defenses, pivoting between networks, deploying proxy chains, and using web shells.

ENROLL NOW

COMPUTER HACKING FORENSIC INVESTIGATOR CERTIFICATION (CHFIC)

Computer hacking forensic investigation is the process of detecting hacking attacks and properly extracting evidence to report the crime and conduct audits to prevent future attacks. Computer crime in today's cyber world is on the rise. Computer Investigation techniques are being used by police, government and corporate entities globally and many of them turn to EC-Council for our **Computer Hacking Forensic Investigator** CHFI Certification Program.

Computer Security and Computer investigations are changing terms. More tools are invented daily for conducting Computer Investigations, be it computer crime, digital forensics, computer investigations, or even standard computer data recovery. The tools and techniques covered in EC-Council's CHFI program will prepare the student to conduct computer investigations using groundbreaking digital forensics technologies.

Computer forensics is simply the application of computer investigation and analysis techniques in the interests of determining potential legal evidence. Evidence might be sought in a wide range of computer crime or misuse, including but not limited to theft of trade secrets, theft of or destruction of intellectual property, and fraud. CHFI investigators can draw on an array of methods for discovering data that resides in a computer system, or recovering deleted, encrypted, or damaged file information known as computer data recovery.

The purpose of the CHFI credential is to:

Validate the candidate's skills to identify an intruder's footprints and to properly gather the necessary evidence to prosecute in the court of law.
The CHFI certification will fortify the application knowledge of law enforcement personnel, system administrators, security officers, defense and military personnel, legal professionals, bankers, security professionals, and anyone who is concerned about the integrity of the network infrastructure.

ENROLL NOW

CERIFIED NETWORK DEFENDER ARCHITECT (CINDA)

How to Become a CNDA?

STEP 1
Obtain CEH + Be Employed

STEP 2
Fax the CNDA Application

STEP 3
CNDA Achieved

CERTIFIED CHIEF INFORMATION SECURITY OFFICER (CCISO)

The CCISO Certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. The CCISO Body of Knowledge covers all five the CCISO Information Security Management Domains in depth and was written by seasoned CISOs for current and aspiring CISOs.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED ENCRYPTION SPECIALIST (CES)

This program introduces professionals and students to the field of cryptography. The participants will learn the foundations of modern symmetric and key cryptography including the details of algorithms such as Feistel Networks, DES, and AES.

The purpose of the CES credential is to:

This course is excellent for ethical hackers and penetration testing professionals as most penetration testing courses skip cryptanalysis completely. Many penetration testing professionals testing usually don't attempt to crack cryptography. A basic knowledge of cryptanalysis is very beneficial to any penetration testing.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

ADVANCED NETWORK DEFENSE (CAST 614)

Come experience a comprehensively structured and fast paced program that immerses you into world of an ethical hacker, providing insights of their mindset; a critical weapon for defending against some of the most malicious attacks around.

With this course you can be among the few who transcend the old idea of the hacker having all the fun, take pride being the defender, form an offensive mindset to skillfully orchestrate robust and solid defenses and reinvent popular belief by beating the hacker at his own game.
You will be evaluating advanced hacking methods of defense fortification bringing you closer to establishing perfect security best practices and methodologies you can apply to secure environments. This course provides segmentation and isolation to reduce the effectiveness of the advanced persistent threats.

The purpose of the CAST614 credential is to:

Cover fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and how to harden your enterprise architecture from the most advanced attacks. Once a strategy for a fortified perimeter is defined the course moves on to defending against the sophisticated malware that is on the rise today and the importance of live memory analysis and real time monitoring.

ENROLL NOW

CERTIFIED SOC ANALYST (CSA)

The **Certified SOC Analyst** (CSA) program is the first step to joining a security operations center (SOC). It is engineered for current and aspiring Tier I and Tier II SOC analysts to achieve proficiency in performing entry-level and intermediate-level operations.

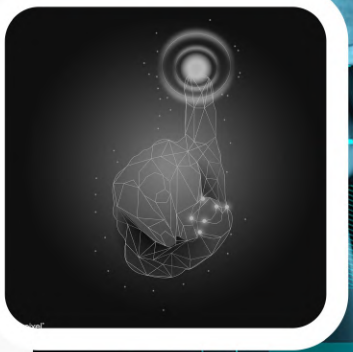
CSA is a training and credentialing program that helps the candidate acquire trending and in-demand technical skills through instruction by some of the most experienced trainers in the industry. The program focuses on creating new career opportunities through extensive, meticulous knowledge with enhanced level capabilities for dynamically contributing to a SOC team. Being an intense 3-day program, it thoroughly covers the fundamentals of SOC operations, before relaying the knowledge of log management and correlation, SIEM deployment, advanced incident detection, and incident response. Additionally, the candidate will learn to manage various SOC processes and collaborate with CSIRT at the time of need.

As the security landscape is expanding, a SOC team offers high quality IT-security services to actively detect potential cyber threats/attacks and quickly respond to security incidents. Organizations need skilled SOC Analysts who can serve as the front-line defenders, warning other professionals of emerging and present cyber threats.

The purpose of the CSA credential is to:

The lab-intensive CSA program emphasizes the holistic approach to deliver elementary as well as advanced knowledge of how to identify and validate intrusion attempts. Through this, the candidate will learn to use SIEM solutions and predictive capabilities using threat intelligence. The program also introduces the practical aspect of SIEM using advanced and the most frequently used tools. The candidate will learn to perform enhanced threat detection using the predictive capabilities of Threat Intelligence.

ENROLL NOW



CERTIFIED APPLICATION SECURITY ENGINEER (CASE)

JAVA and .NET

The **Certified Application Security Engineer** (CASE) credential is developed in partnership with large application and software development experts globally.
The CASE credential tests the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices in today's insecure operating environment.

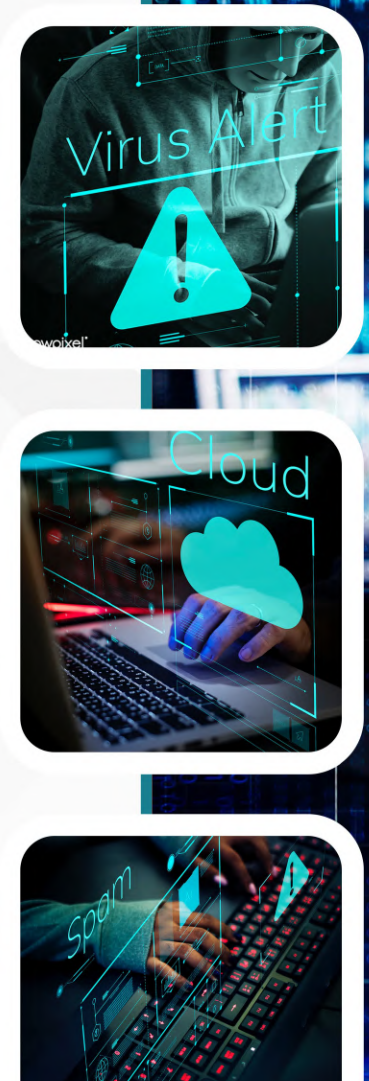
The CASE certified training program is developed concurrently to prepare software professionals with the necessary capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security course that will help software professionals create secure applications.

The purpose of the CASE credential is to:

The training program encompasses security activities involved in all phases of the Software Development Lifecycle (SDLC): planning, creating, testing, and deploying an application.
Unlike other application security trainings, CASE goes beyond just the guidelines on secure coding practices and includes secure requirement gathering, robust application design, and handling security issues in post development phases of application development.

This makes CASE one of the most comprehensive certifications on the market today. It is desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

ENROLL NOW



DISASTER RECOVERY PROFESSIONAL v3

EDRP provides the professionals with a strong understanding of business continuity and disaster recovery principles, including conducting business impact analysis, assessing of risks, developing policies and procedures, and implementing a plan. It also teaches professionals how to secure data by putting policies and procedures in place, and how to recover and restore their organization's critical data in the aftermath of a disaster.
The business community globally has been hit over and over again by one disaster after another in the past decade and a half. The scary part is that the frequency is increasing exponentially in the past few years, thanks to the growing number of cyber-attacks.

Even scarier is the study that shows that 2 out of 5 business still do not even have a BC/DR plan. And out of the ones that do, only about half of them even test it regularly to see if it is still relevant. Furthermore, industry experts have reiterated the fact in every forum possible, that the size of the business is irrelevant to having a BC/DR plan. Everyone needs to have one to stay relevant in current times.
This scenario can only be amended by trained BC/DR professionals who not only understand the gravity of the situation, but also are equipped to ensure that businesses are least impacted when disaster strikes.

The purpose of the CASE credential is:

aimed at educating and validating a candidate's ability and skills to plan, strategize, develop, implement, and maintain enterprise-wide business continuity and disaster recovery plans.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CERTIFIED SECURITY SPECIALIST (ECSS)

EC-Council Certified Security Specialist (ECSS) allows students to enhance their skills in three different areas namely information security, network security, and computer forensics. Information security plays a vital role in most organizations. Information security is where information, information processing, and communications are protected against the confidentiality, integrity, and availability of information and information processing. In communications, information security also covers trustworthy authentication of messages that covers identification of verifying and recording the approval and authorization of information, non-alteration of data, and the non-repudiation of communication or stored data.

ENROLL NOW

Promote CyberSafety, Increase CyberWellness, Enhance Business Efficiency!

CONCLUSION

At Zeta-Web Nigeria, we do not only offer your staff with updated Cybersecurity knowledge, but also empower them with the right skills needed to make your business stand-out in the corporate world.

To register for any of our EC Council Training Programs;

Please send an Email to info@zeta-web.com

Telephone: 01-270 1444

Address: 32 Providence Street, Lekki Phase 1. Lagos.

Website: www.zeta-web.com

Accredited Training Center

Cert ID
EATC32378