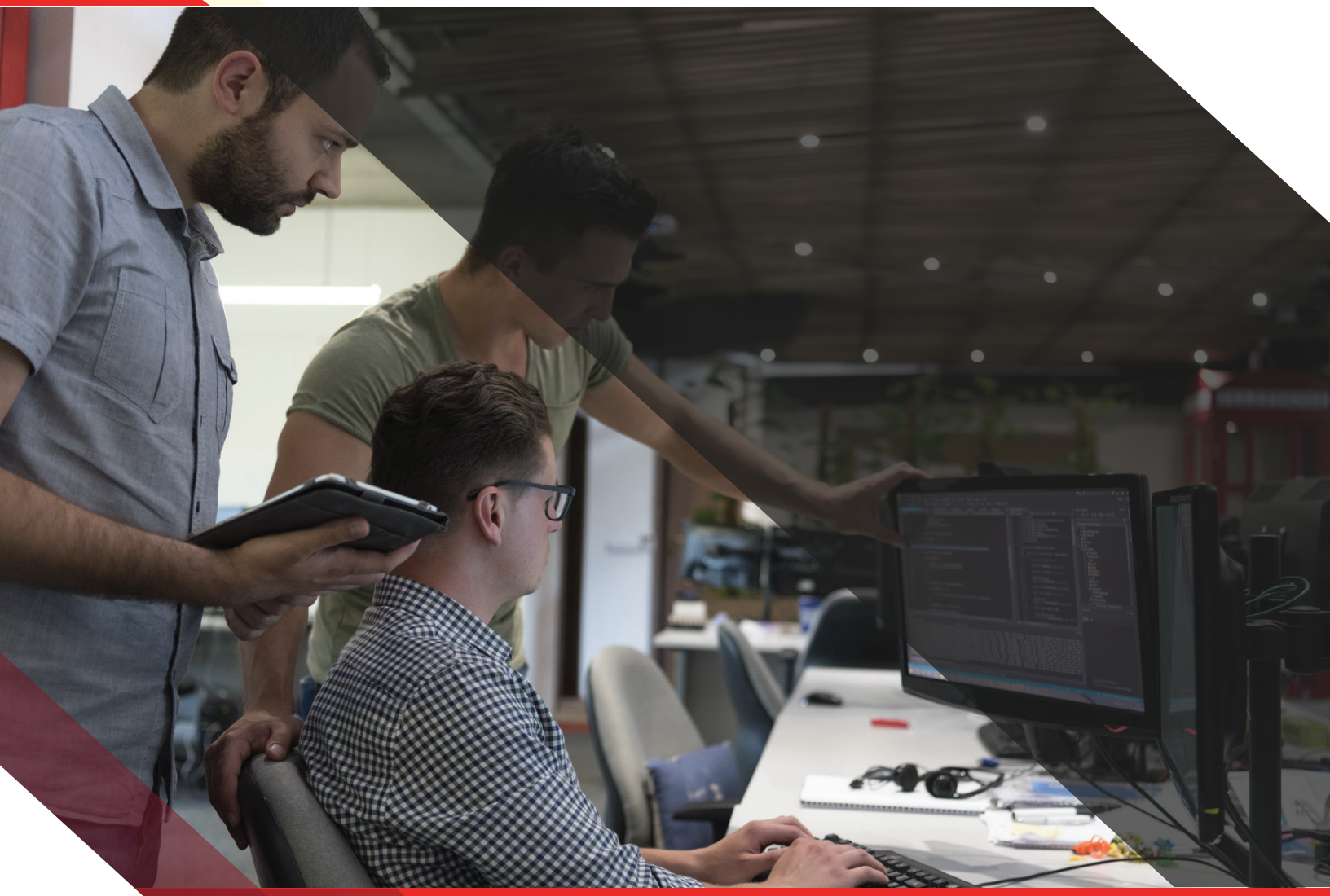
EC-Council

C|ASE .NET
Certified Application Security Engineer

C|ASE JAVA
Certified Application Security Engineer



Certified Application Security Engineer

www.eccouncil.org

EC-Council

Course Description

The Certified Application Security Engineer (CASE) credential was developed in partnership with 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 was developed to prepare software professionals with the capabilities that are expected by employers and academia globally. It is designed to be a hands-on, comprehensive application security training course to teach software professionals to create secure applications.

The training program encompasses security activities involved in all phases of the secure 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 the post development phases of application development.

This makes CASE one of the most comprehensive application security certifications for secure software development on the market today. It's desired by software application engineers, analysts, and testers from around the world and is respected by hiring authorities.

EC-Council

Application Security: the Current and NEXT BIG THING

For most organizations, software and applications determine their success. However, expedition, duplication, and penny-pinching often take center stage and security considerations take a backseat - or are not considered at all. An insecure or vulnerable application places these businesses at risk.

1.8 Billion Active Websites
Managed by 21 Million Developers Globally
One of the Largest Economies - $5.6 Trillion by 2021

3.5 Billion Active Users
Making the Largest Platform For Identity and Financial Theft

Average of 19 Vulnerabilities Found Per Day
Over 50% Termed Critical
64% of Top 1 Million Alexa Websites Are Vulnerable

Do you belong to the pack that follows unsafe coding and deployment practices? Are you one of the 21 million, putting the security of the software or web application at risk, resulting in a catastrophic loss?

Security Risk is Not Limited to Web Applications

Many globally-recognizable retail outlets have dealt with enormous data breaches recently because they ignored application security.

Billion-dollar companies with global footprints have faced massive data leakage, including their customers' and employees' personal and financial information, because their applications were faulty.

Retail giants like Forever 21, GameStop, Panera Bread, Sonic, KMart, and Hudson Bay (Saks Fifth Avenue) are a few on the list of retailers with thousands of outlets that used POS machines or payment gateways that allegedly resulted in information theft. There are many more modern, digital platforms like Uber, Yahoo, Dropbox, Adobe, LinkedIn, and Tumblr who also faced similar breaches, owing to the same reason: lack of application security.

Application Security

How Secure Are You?

75%

of All Cyber Attacks Target Web Applications

90%

of Java Applications Contain At Least One Vulnerability

69%

Web Application Attacks Rise in 2017

.NET

The Gap Between Patching Software and Security Is Vast!
The .NET framework has increased in popularity because of its open source nature, interoperability, language independence, library of codes, and ease of deployment. It's become the preferred choice for application developers. However, there are not many classes that teach developers how to ensure their code is secure as well as correct. Moreover, any gap in the application development and deployment process can be damaging. .NET developers often learn security on the job. This is primarily because the basic education of programming does not usually cover or emphasize security concerns.

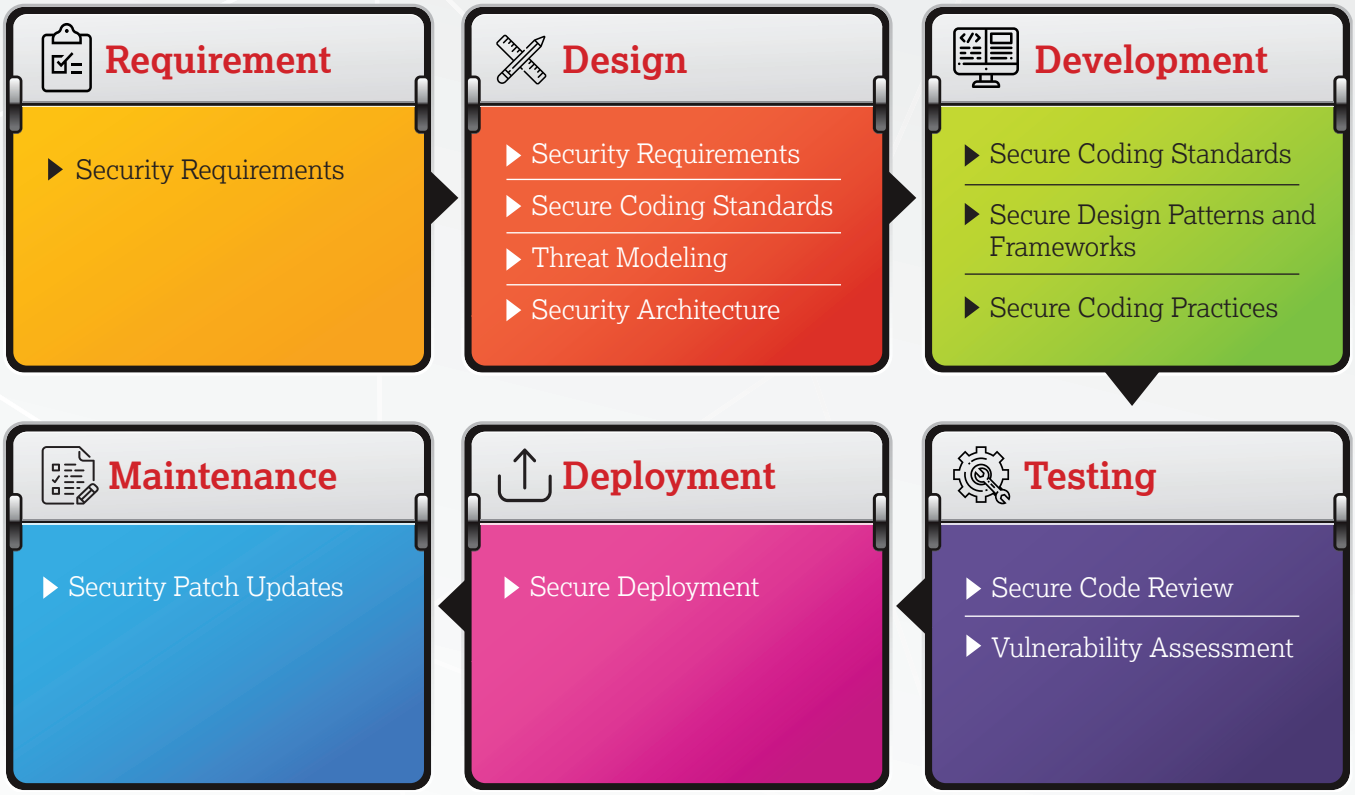
Java

Java Based Applications: The Most Popular and Yet the Most Vulnerable?
According to the 2017 State of Software Security Report, nearly 90% of Java applications contain one or more vulnerable components, making them ideal breach points for hostile attackers.

Although Java has come a long way from its development in 1995, cyber crime has also spread, reaching epidemic levels, increasing the need for secure Java developers, regardless of whether they're creating a new program or upgrading an old one.

Secure Software Development Process

The Certified Application Security Engineer (CASE) program provides a comprehensive application security approach which encompasses security activities involved in all of the phases of Software Development Lifecycle (SDLC).



EC-Council

What You Will Learn

- In-depth understanding of secure SDLC and secure SDLC models
- Knowledge of OWASP Top 10, threat modelling, SAST and DAST
- Capturing security requirements of an application in development
- Defining, maintaining, and enforcing application security best practices
- Performing manual and automated code review of application
- Conducting application security testing for web applications to assess the vulnerabilities
- Driving development of a holistic application security program
- Rating the severity of defects and publishing comprehensive reports, detailing associated risks and mitigations
- Working in teams to improve security posture
- Application security scanning technologies such as AppScan, Fortify, WebInspect, static application security testing (SAST), dynamic application security testing (DAST), single sign on, and encryption
- Following secure coding standards that are based on industry-accepted best practices such as
- OWASP Guide, or CERT Secure Coding to address common coding vulnerabilities.
- Creating a software source code review process that is a part of the development cycles (SDLC, Agile, CI/CD)

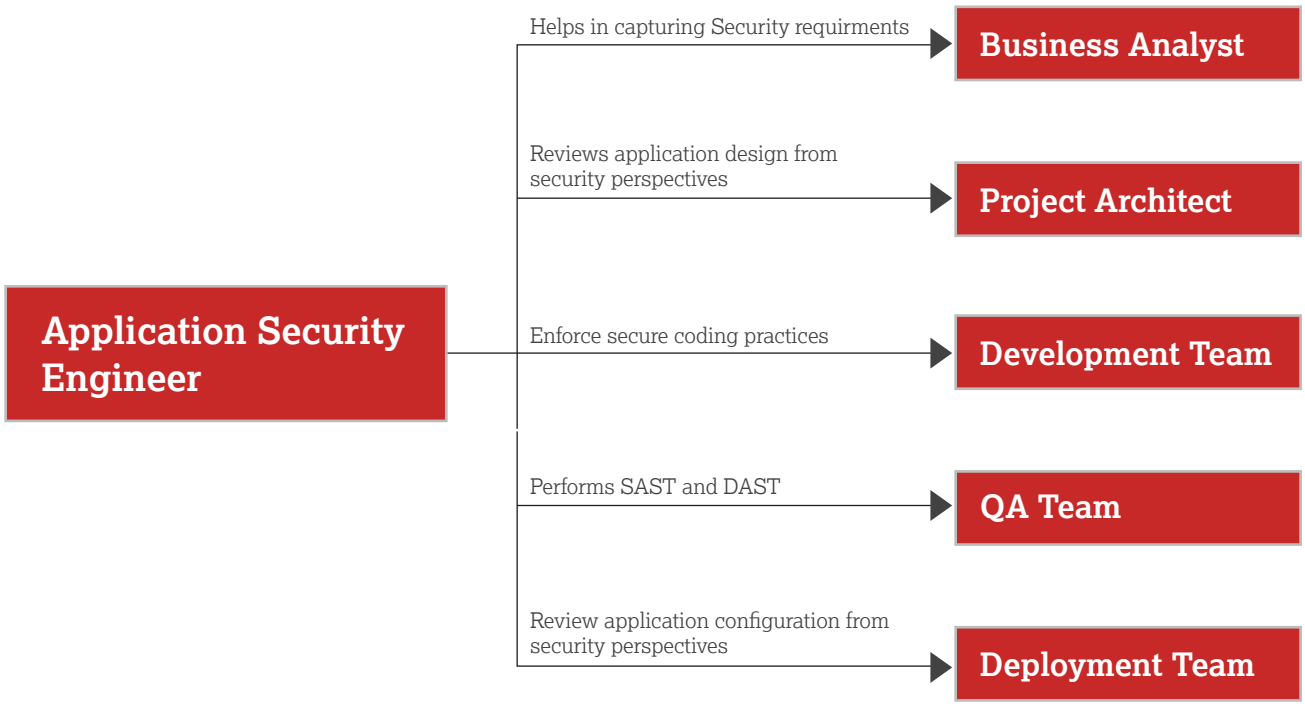
Top Components of CASE

CASE is today's industry compliant application security credential because it is a hands-on, comprehensive application security program.

1. **Security Beyond Secure Coding -** Challenging the traditional mindset where secure coding means a secure application.
2. **Testing and credentialing** secure app development across the SDLC.
3. **The most comprehensive training program** for application developers covering techniques such as input validation, defensive coding practices,authentication and authorization, cryptographic attacks, error handling techniques, session management techniques, among many others
4. **An exhaustive range of labs** to ensure real-world practice.
5. Available for both **.NET** and **Java**
6. Maps to the "Securely Provision category" in the **NICE 2.0 Framework**

Job Task Analysis

To further ensure that CASE is relevant across the right benchmarks, CASE was built to provide for the Job Task Analysis (JTA) of roles involved in application security as well as to many Specialty Areas under “Securely Provision category” in the NICE 2.0 Framework.



Course Outline of CASE

- Understanding Application Security, Threats, and Attacks
- Security Requirements Gathering
- Secure Application Design and Architecture
- Secure Coding Practices for Input Validation
- Secure Coding Practices for Authentication and Authorization
- Secure Coding Practices for Cryptography
- Secure Coding Practices for Session Management
- Secure Coding Practices for Error Handling
- Static and Dynamic Application Security Testing (SAST & DAST)
- Secure Deployment and Maintenance

> ***100% of Web Applications are Vulnerable to Hackers.***
>
> *- 2018 Global Security Report, Trustwave*

Who Is CASE For?

.NET and Java Developers with a minimum of 2 years of experience and individuals who want to become application security engineers, analysts, or testers.

Individuals involved in the role of developing, testing, managing, or protecting applications

Duration

Total Training - 24 hours or 3 full day sessions

Course Material

All attendees will receive a personal copy of the CASE courseware, an EC-Council CASE exam voucher, and access to iLabs (EC-Council's cloud driven labs environment).

Certification

The CASE exam can be challenged after attending official CASE training. Candidates that successfully pass the exam will receive their CASE certificate and membership privileges. Members are required to adhere to the policies of EC-Council's Continuing Education Policy.

Application Security Is No Longer An Afterthought But a Foremost One!

Attaining the Certified Application Security Engineer

CASE allows application developers and testers to demonstrate their mastery of the knowledge and skills required to handle common application software security vulnerabilities.

- **Exam Title: Certified Application Security Engineer**
- **Number of Questions: 50**
- **Test Duration: 2 Hours**
- **Test Format: Multiple Choice Questions**
- **Passing Score : 70%**
- **Availability: EC-Council Exam Portal**

EC-Council

Eligibility Criteria

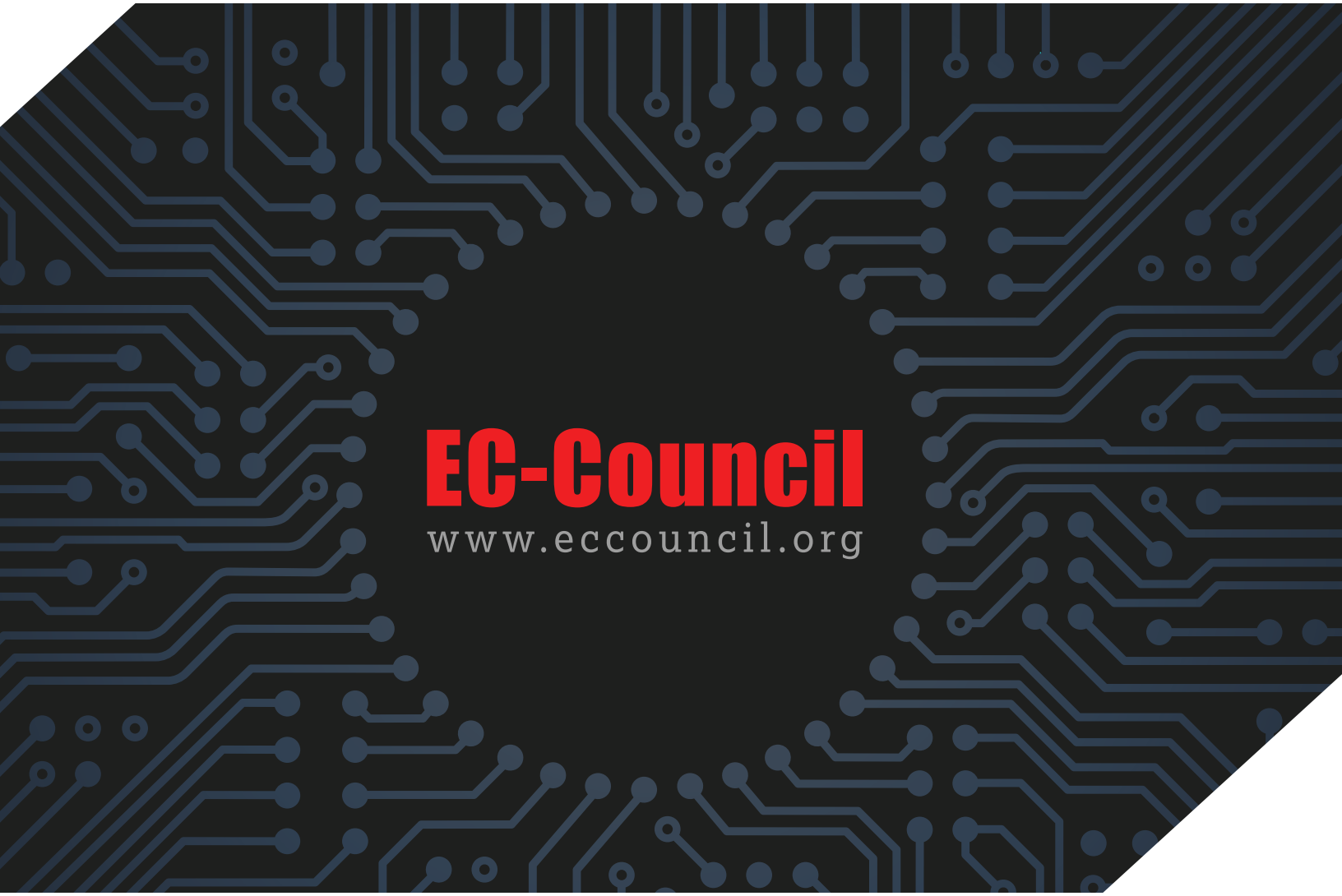
To be eligible to challenge the CASE Exam, candidate must either:

- Attend the official EC-Council CASE training through an accredited EC-Council Partner (Accredited Training Centre/ iWeek/ iLearn) (All candidates are required to pay the USD100 application fee unless your training fee already includes this) or

- Be an ECSP (.NET/ or Java) member in good standing (you need not pay a duplicate application fee, as this fee has already been paid) or

- Have a minimum of 2 years working experience in information security or software design(you will need to pay USD 100 as a non-refundable application fee) or

- Have any other industry equivalent certifications such as GSSP .NET/Java (you will need to pay USD 100 as a non-refundable application fee).


EC-Council
www.eccouncil.org