BLAZE

INFORMATION SECURITY

Technical excellence and worldwide experience.

We are information security at its best.

Be secure. Be ahead. Be Blaze.

Helping customers overcome the challenges of keeping their confidential information secure and their business undisrupted from cyber security threats is the core of what we do.

Blaze Information Security advises organizations in improving their readiness for real life cyber threats and offers expertise in mitigating and responding to them.

Our team has decades of combined experience in cyber security and a proven track record of publishing security research.

Blaze provides cutting-edge cyber security services that include penetration testing of infrastructure, web and mobile applications, software security consultancy, vulnerability management, product security assessments and more.

We work closely with customers to understand their information security needs and apply our expertise and the ability to adapt to different requirements. Blaze has served customers from industries such as banking, fintech, retail, e-commerce, oil and energy, telecommunication and online casinos. Our team possess the indispensable know-how to deal with complex and critical projects.

The everchanging technological environment is a great challenge to information security. This is why **we are strong believers in technical excellence and being on top of the game at all times is what we strive for.**

About us

With offices in Brazil, Portugal and Poland, **we are ideally placed to work with clients worldwide, having delivered projects in over 13 countries and four continents.**

Experienced
professionals

Bespoke
services

International
presence

OFFICES

Our services

Source code review

The existence of software vulnerabilities often originate in the source code. Our experienced consultants are able to perform code review of software written in popular languages such as Java, Ruby, Python, C/C++, PHP, ASP.NET, C#.NET as well as less popular ones such as Solidity, for smart contracts and blockchain applications.

The review consists of code scanning using security-focused static analysis tools together with man-powered expertise to perform manual code review to identify vulnerabilities and design errors that can pose a serious risk to the application.

The final result is a description of all issues discovered along with information advising your development team how to fix the vulnerabilities identified and how to prevent similar design and implementation mistakes in the future.

Product security assessment

Blaze Information Security offers security assessments of products developed in-house or that are commercial off-the-shelf.

Product security assessments evaluate all security aspects that will be impacted by a new application or device that will be inserted in the corporate network.

A detailed analysis of the attack surface of the product under test is performed, taking into consideration its security expectations and objectives and threat model. In general, product security aims to verify the resilience of all components of the product under test – typically, this service is composed of architecture analysis, supporting infrastructure testing, application security, code review and reverse engineering, as well as the creation of bespoke tools such as fuzzers and custom network protocol analyzers.

Our offering benefits vendors that want their product to be evaluated from a security point of view before it is shipped to the market, and for organizations that want to make sure that bringing in another appliance or software to their network will not cause an adverse impact to client's security posture.

Mobile application security assessment

Business-critical mobile apps bring new risks for organizations that rely on mobile devices on a daily basis.

Another risk factor for mobile application is the current security maturity level for such platforms – many risks are still not well understood and the lack of well-established security practices and frameworks, as well as the overall lack of maturity of application developers make the mobile world more prone to vulnerabilities than others.

Penetration test of mobile apps involve simulating the actions of a skilled attacker to identify vulnerabilities both in the application's supporting infrastructure (backend APIs and databases), in the communication between the app and the server, and an analysis of the application per se, along with its interaction with the device.

Ultimately, the organization can improve the security of its business-critical mobile applications and reduce the risk to acceptable levels.

Vulnerability management

The constant discovery of new vulnerabilities brings new challenges to the security management of an organization.

Our vulnerability management service periodically monitors the security posture of your IT infrastructure, web and mobile applications to identify the level of risk they may bring to your organization.

The analysis takes place on a daily basis, where our consultants perform security tests against the systems under scope.

When a vulnerability is identified, the client's IT team is immediately notified via e-mail and through the dashboard of Lantern, our exclusive vulnerability management platform.

Our clients benefit from a 360 degrees vision of the risk their IT infrastructure and assets may be exposed to, and count with the assistance of Blaze's experts in the entire lifecycle of the vulnerability – supporting the client in all steps from risk identification to remediation.

Defense mechanisms resilience testing

It is common for organizations to take advantage of multiple layers of security controls that include web gateways, firewalls, anti-virus, intrusion detection systems and other mechanisms. Combining them together is part of a popular approach known as defense in depth.

Blaze's Defense Mechanisms Resilience Testing was designed to assess the effectiveness of the current defense mechanisms against several advanced scenarios to verify which layers of security controls can be pierced by an attacker with varying levels of sophistication.

This service is divided in three tiers, each of them with its own degree of effort.

The first tier of the test is designed to assess the resilience of the endpoint and network-based protection mechanisms currently in place.

The second step of the test comprises of sending the same artefacts wrapped in different types delivery methods and using simple artefacts compiled in other executable formats.

The third and last part of testing relies on a number of advanced techniques to attempt to get past the defenses in place.

The final result of this service provides the client with the opportunity to understand how to improve its defense mechanisms – from network to the endpoint, and prioritize efforts to plug gaps and reduce risks related to these technologies.

Security development lifecycle

Security Development Lifecycle or SDLC is a software development process that supports developers to build more secure software in compliance with modern security requirements.

Early in the project phase, **Blaze advises customers by building security in every element of the project** with activities such as: definition of the security requirements and objectives, design review, threat modeling, source code analysis, penetration test at each major release, fuzz testing, secure programming guidance, and more.

The different activities during SDLC projects aim to reduce the attack surface offered by the project and its systems, strengthening its confidentiality, integrity and availability. **This reduces the chances for fraud and future maintenance costs to correct defects originated from security flaws.**

Infrastructure penetration test

Infrastructure penetration test consists in the identification and exploitation of vulnerabilities and threats to businesses from the perspective of either an external adversary or an insider in the organization.

The main objective of this service is to be ahead of the game of a malicious insider, such as a disgruntled employee, that may have basic access to the network. This service can also be used to evaluate and validate the organization's defenses against a scenario of a motivated and persistent external attacker with no privileged access or knowledge about the network infrastructure.

Such assessment provides a valuable insight into the business's security policies, patch management and can be used for audit processes that require security testing such as PCI-DSS and ISO/IEC 27001.

Web application security testing

The aim of web application and API security testing is to identify vulnerabilities that can cause direct interference to the continuity and resilience of the business, as in many cases web applications and APIs often handle sensitive information and other resources considered vital to an organization.

The assessments are performed by our expert consultants in a manual fashion, aided by the development of tools and scripts specific to each application under test.

We go above and beyond common issues found in OWASP Top 10 and also cover many modern vulnerability classes affecting web-based technologies.

With the result of the assessment our clients can protect their assets and direct the efforts to mitigate the identified issues, enhancing the robustness and bolstering the resilience of the application or API against cyber-attacks.

Red team and adversary simulation

Unlike traditional penetration testing exercises, a red team assessment takes into account a wider scope – it goes above and beyond just individual applications and systems, identifying weaknesses in security controls and gaps in the detection and response capabilities of the entire organization.

This type of exercise emulates a persistent and technically capable adversary, with a combination of physical security tests, social engineering, network and application attacks.

Throughout the adversary simulation, Blaze's red team will use tools, tactics and procedures of real-world adversaries in an attempt to achieve the goals established for the engagement and gain access to business-sensitive data and systems.

The main objective of this assessment is to illustrate the risks that an organization may face from the viewpoint of a determined threat actor, and most importantly improve its detection and response capabilities.

Cyber security risks in M&A and investments

Mergers & Acquisitions (M&A) are a frequent occurrence in the modern business landscape, with companies using M&A's as a strategy to gain access to different markets, or a greater market share by merging with smaller players.

As part of the technical due-diligence of acquisitions and investments, **Blaze Information Security can aid your organization in assessing the cyber security risk of the company your business is planning to merge with or invest in**, in order to understand the impact to the security of your business and effort needed to reduce these risks to acceptable levels.

Our services help your business with actionable advice to make informed decisions about third-party cyber security risks in M&A's, guaranteeing peace of mind and a maximized return on investment.

PORTUGAL (EUROPE HQ)
Praça Bom Sucesso 131
Península, Office 206, Porto
+351 222 081 647

BRAZIL (SOUTH AMERICA HQ)
Rua Visconde de Jequitinhonha 279
Office 701, Recife
+55 81 3071 7148

POLAND (SATELLITE OFFICE)
ul. Józefa Sarego 5/4
31-047, Kraków
+48 792 436 755

sales@blazeinfosec.com
www.blazeinfosec.com