Your SECURITY with
RALFKAIROS

Secure your IT assets and prevent from being compromised with RALFKAIROS. Assess your business vulnerability to attackers.

1. We help you secure and better reinforce your IT system and train your Team in Korea and Europe with a customized approach that fits you best.

2. We address your corporate requests and/or we assist you thanks to our understanding of business processes, risks and IT issues.

IT Security Inspection

- Incident Management
- Patch Management
- Data Management
- Monitoring Controls
- Physical Security
- Healthcheck report

Risks, organization, processes & infrastructure
Compare actual conditions with benchmarks
Conclusion report and Action Plan
High-level & interne proactive ITcheck

Survey, Docs inventory, Interviews, Infrastructure review

Penetration test

- Security exercise where our expert attempts to find and exploit vulnerabilities in a IT system
- Propose security upgrades to plug up any vulnerabilities discovered during the test
- Have a third party expert opinion and maintain trusts with your stakeholders

Cyber Bootcamp & Training

- Training program for entry level jobs in cybersecurity or reskill IT professionals
- In-demand skills development
- 20 Topics, +350 hours and remote coach. 2 to 4 months class
- Theoretical knowledge, real-world cases, hands-on exercises

IT Security Inspection

- Network
- System
- PenTest
- Application
- Crypto
- Security Tools
- Risks
- Audit

CISO Assistance

- Lead information security department
- Project Management

Implementation and deployment
Monthly incident report

CISO ON DEMAND | CISO ON CONTROL | CISO DELEGATION

Certifications

Contact us!

www.ralfkairos.com
team@ralfkairos.com

Copyright © 2022 RALFKAIROS All rights reserved
Penetration Testing with RALFKAIROS

Reduce your risk of a breach by identifying and exploiting business-critical vulnerabilities with ondemand penetration testing expertise.

RALFKAIROS ’s penetration testing services maximizes risk reduction, while minimizing any disruption to the business.

We evaluate systems by subjecting them to external Internet attacks and/or by considering insider threats.

- Help our clients ensure that their IT systems are protected to the different threats spread over internet.
- Demonstrate that a system or device is either susceptible or not susceptible to particular security weaknesses.
- Provide clear recommendations for vulnerability mitigation that are straightforward to implement and tailored to the required functionality of the system being tested.
- Can your company’s IT systems resist a hacker attack? Do you want to know it?

At RALFKAIROS , we have some of the best Ethical Hackers you will ever meet.

With the highest certification available, they know the hacker’s methods and tools - and use them only for your benefit.

The test consists of a pre-agreed attack on your application.

Afterwards you receive a wrap-up meeting and a report, so you get a clear view of your company’s or SaaS vulnerability.

Get in touch and learn more.

Using our penetration testing services regularly helps our clients stay one step ahead of potential attackers, enabling their IT systems to grow with their business, while keeping the enterprise secure. Our approach to penetration testing provides a thorough, quality service with the flexibility necessary to test a wide range of IT systems.

RALFKAIROS EXPERTISE

Our team holds qualifications from Offensive Security and CREST, for network and web application testing. We offer seven broad areas of testing, which are normally combined to provide the optimal balance of testing.

- **Internal testing** is carried out while connected directly or close to the network under test, on either ‘full knowledge’ or ‘zero knowledge’ engagements. The purpose is to demonstrate that an IT system has been configured in a manner that makes it as secure as possible.

- **Internet testing** takes a “black box” (zero-knowledge) approach and is often used to understand what target information attackers can discover from the Internet and other public domain resources.

- **Remote testing** is conducted from external networks to which the IT system is connected. There is generally some sort of perimeter security, for example, a firewall or filtering router that is designed to limit the access available from a given external network to the IT system under test.

- **Web application testing** ensures that an application has been configured securely so that attackers cannot gain unauthorized access to it or its data; users cannot access data for which they are not authorized; and there are no vulnerabilities that users can leverage to gain access to services outside of their restricted operating environment.

For more information about RALFKAIROS, visit ralfkairos.com, or email us at team@RALFKAIROS.com.