RISK-DRIVEN APPLICATION SECURITY TESTING

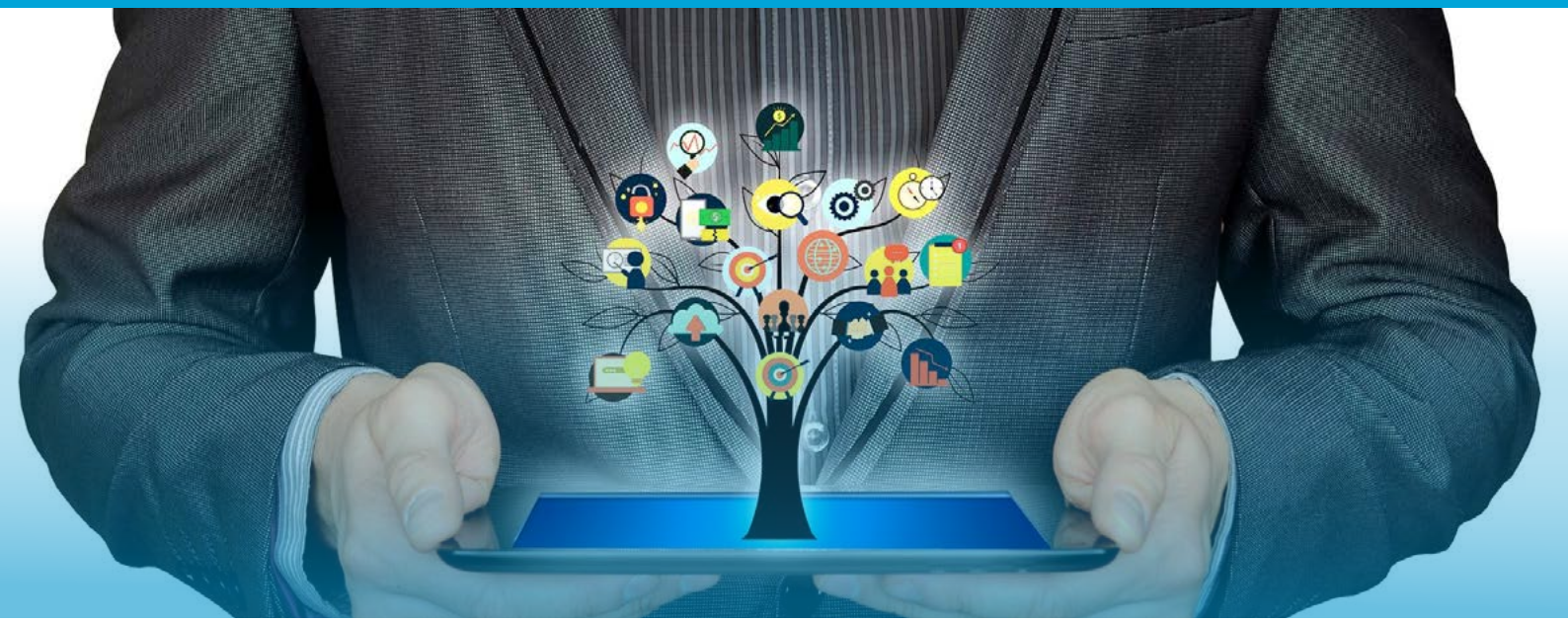
Secure Your Applications Before Launch

www.riskcrew.com/security-testing

OVER 80% OF ALL ATTACKS OCCUR ON THE APPLICATION LEVEL

According to SAP, around 84% of cyber-attacks happen on the application layer. The application layer is the easiest to attack and the hardest to defend as it is the most exposed and accessible. Simply put, applications are the primary attack vectors for threat actors. Attackers play the game on the application level – so should you.

Let the PROCESS be the PRODUCT



Our Risk-Driven Application Testing Service is a proven process for ensuring the security integrity of business-critical applications. **This innovative service is comprised of four steps.**

Design Review

1

Threat Assessment

2

Four Step Proven Process

4

Security Penetration Testing

3

Threat & Attack Modeling

THE PROCESS

Implementing this four-step testing process can significantly reduce the attack surface associated with your applications by addressing the vulnerabilities inherent in their design, development, and deployment life cycle. By identifying and shutting down the attack vectors associated with the application's design, development, and deployment – you can radically reduce the threat of a breach.

This holistic approach is not only extremely effective, but it also results in a bigger return for your security spend. But very few organisations understand this and invest their security budgets on products rather than process.

STEP 1

Security Design Review

STEP 2

Threat Assessment

STEP 3

Threat & Attack Modeling

STEP 4

Security Penetration Testing

The process begins by conducting a detailed analysis of the design, development, testing and hosting documentation associated with the application. The purpose is to identify all of the access points, existing access controls and any inherent security design flaws. The application's development and testing processes are examined for adherence to OWASP best practices. Additionally, hosting service level agreements are reviewed for security shortcomings. Upon completion, Risk Crew provides a comprehensive report detailing vulnerabilities in design, development and deployment documentation with recommended remedial measures.

The design review is then followed by a threat assessment. In this step, the information asset(s) processed, stored or transmitted by the application and its (their) sensitivity classification level(s) are then identified and confirmed with the business. An information threat and risk assessment is then conducted for the application based upon the information obtained in the design review. Upon completion, a detailed report is produced documenting the application vulnerabilities, threats which could exploit these vulnerabilities, and the associated likelihood and impact of those threats if executed.

The results of the threat assessment provide valuable data for the next step of defining and documenting the "attack surface" associated with the application given its design, development and deployment flaws. This step is critical and is done to identify the probable threat agents and their most likely attack vectors. This modeling is essential for scoping effective security penetration testing for the application that simulates real-life attack scenarios. Upon completion, the model is provided for reference and application life cycle documentation.

Finally, a security penetration test is conducted on the application. The testing scope, approach, tools and methodology are determined by the actual attack surfaces associated with the application. In this way, testing simulates real-world attack scenarios, from threat agents through existing attack vectors. This pragmatic approach significantly increasing the value of testing and results in remedial recommendations that if implemented will reduce the threat to your application.

THE BENEFITS

The benefits of this simple risk-driven approach should be obvious. The service results in a more robust and applicable security controls for the applications that process stores or transmits your business-critical information assets. It confirms that they are 'fit for purpose' and can withstand a real-world attack. **Specific service benefits include:**

Understanding the Vulnerabilities

Vulnerabilities are identified in the application design, build and hosting security

Receiving a Clear Picture of the Likelihood & Impact of Risk

The (likelihood & impact) of the application's security risks are both identified and quantified

Knowing the Threat Agents & Vectors

The threat agents and attack vectors associated with the application are identified and documented

Getting a Full View of the Application's Security Integrity

The overall security integrity of the application is confirmed by security penetration testing

Preventing a Breach

Specific recommendations are provided to enhance the security integrity of the application and reduce the risk of a breach

RISK CREW'S UNMATCHED DELIVERABLES

Our team provides a comprehensive service which includes a detailed report, courtesy workshop, retesting and on-call assistance – all backed by a 100% satisfaction guarantee.

"The exercise was perfectly designed and we got a real value from it. We didn't know what to expect and were very impressed"

"As always, the team at Risk Crew were outstanding"

"Service was top notch - both personal and professional"

Courtesy Workshop

The report is presented in a workshop with applicable business stakeholders to ensure their understanding of the findings and the risks associated with hosting the business information assets on the platform.

Detailed Report

We provide advice and assistance for 30 days following the report submittal and answer any questions that arise from implementing remedial actions and ensuring risk reduction.

On-call Advice Assistance

The report details specific vulnerabilities identified on the platform, how they were identified, the methods and tools used to identify them and visual evidence if applicable. The report will indicate a security vulnerability risk rating for risk reduction references.

Complimentary Retesting

We offer retesting to verify remedial actions were effective. Upon completion, we'll provide you with a summary report verifying remedial measures have been implemented.

Customer Promise

Risk Crew provides an unparalleled penetration testing solution covered by a 100% satisfaction guarantee.

ABOUT RISK CREW

We are an elite group of information security governance, risk & compliance experts and the forerunners in the design & delivery of innovative & effective solutions with a 100% satisfaction guarantee.

Contact us for more information

+44 (0) 20 3653 1234
riskcrew.com
info@riskcrew.com

5 Maltings Place
169 Tower Bridge Road
London, SE1 3JB
United Kingdom