ImmuniWeb®
AI for Application Security

Continuous Automated Red Teaming

Test your web infrastructure and applications continuously using advanced hacking techniques and real-life attack scenarios with ImmuniWeb® Continuous Automated Red Teaming

Gartner Cool Vendor™

SC **2023 awards** EUROPE highly recommended

IDC Innovator

www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

Why Investing in Continuous Automated Red Teaming

88%

of companies now consider cybersecurity a critical business risk

Gartner

$4.45M

is the average cost of a data breach in 2024, a 15% surge in just three years

IBM

100+

countries have laws imposing a personal liability on executives for a data breach

ImmuniWeb

Continuous Automated Red Teaming (CART) offers a proactive approach to cybersecurity. Instead of occasional security snapshots, CART keeps your defenses constantly on their toes by automatically simulating real-world attacks. This identifies vulnerabilities faster, helps you fix them before they're exploited, and keeps your defenses sharp against evolving threats. CART also frees up your security team's time. By automating repetitive vulnerability testing, your experts can focus on strategic defense improvements and responding to the most complex threats.

Continuous Automated Red Teaming with ImmuniWeb® Continuous

Efficient. Simple. Cost-Effective.

We continuously monitor and test your web applications and APIs for resilience to advanced hacking techniques, real-life attack scenarios and techniques from MITRE's ATT&CK matrix that are relevant for your industry. Once a security flaw is confirmed, you will be immediately alerted by email, SMS or phone call.

For all customers of continuous automated red teaming, we offer a contractual zero false positives SLA and money-back guarantee: if there is a single false positive on your automated red teaming dashboard, you get the money back. Our award-winning technology and experienced security experts detect SANS Top 25 and OWASP Top 10 vulnerabilities, including the most sophisticated ones that may require chained, multi-step or otherwise untrivial exploitation.

Leverage our integrations with the leading WAF providers for instant virtual patching of the discovered vulnerabilities. Request to re-test any finding with one click. Ask our security analysts your questions about exploitation or remediation of the findings at no additional cost around the clock. Get a customizable live dashboard with the findings, download vulnerabilities in a PDF or XLS file, or use our DevSecOps integrations to export the continuous breach and attack simulation data into your bug tracker or SIEM.

Trusted by 1,000+ Global Customers

Looking for Something Else?

Explore 20 use cases we have for you

API Penetration Testing

API Security Scanning

Attack Surface Management

Cloud Penetration Testing

Cloud Security Posture Management

Continuous Automated Red Teaming

Mobile Penetration Testing

Mobile Security Scanning

Network Security Assessment

Continuous Breach and Attack Simulation

Continuous Penetration Testing

Cyber Threat Intelligence

Cybersecurity Compliance

Dark Web Monitoring

Digital Brand Protection

Phishing Websites Takedown

Red Teaming Exercise

Third-Party Risk Management

Web Penetration Testing

Web Security Scanning

www.immuniweb.com

ImmuniWeb outperformed IBM Watson for Cybersecurity and won in the "Best Usage of Machine Learning and AI" category

One Platform. All Needs.