

# **Continuous Breach and Attack Simulation**

Test your web infrastructure and applications continuously with real-life attacks from MITRE's ATT&CK matrix with ImmuniWeb<sup>®</sup> Continuous Breach and Attack Simulation



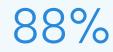




#### www.immuniweb.com

Copyright © 2024 ImmuniWeb SA

## Why Investing in Continuous Breach and Attack Simulation



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+

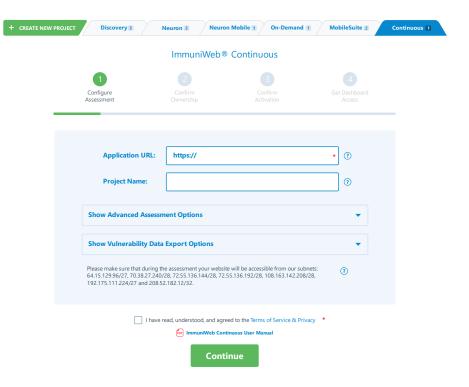
countries have laws imposing a personal liability on executives for a data breach

ImmuniWeb

Continuous Breach and Attack Simulation (BAS) offers a significant advantage over traditional security measures by mimicking real-world attacks, constantly testing an organization's defenses. Unlike point-intime assessments, BAS provides a proactive and ongoing evaluation, identifying vulnerabilities as they emerge, such as through new software installations or configuration changes. Furthermore, BAS helps prioritize remediation efforts by highlighting the most critical vulnerabilities and their potential impact. This enables security teams to focus their resources on addressing the most pressing threats, optimizing their effectiveness in protecting sensitive data and systems.

### Continuous Breach and Attack Simulation with ImmuniWeb<sup>®</sup> Continuous

+	CREATE NEW PROJECT Discovery 5	Neuron 2 Neu	ron Mobile 1 On-Demand	1 MobileSuite 2	Continuous 1
	no.example.com Ung scription Valid Untibuly 1, 2024	2 2 5 3	Patched Vulnerabilities	SCA 0 2 1	發 API & User Access ☞ User Manual
	Unpatched Vulnerabilities Archived Vulnerabili	ties SCA	Statistics Executive Vie	w Vulnerability Notification	s Configuration
- Čy-Below you can see recently detected vulnerabilities that are not patched yet					
A	I Targets	02/02/202	08/2024	Medium Low Warning	Export 👻
0 new vulnerability or warning since your last login Show only new or updated vulnerabilities since my last login					
	Vulnerability 🕈	CWE-ID \$	Detected *	Status 🗢 🛛 Risk 🗢	Actions 📃
	Blind SQL Injection in /e-shop/profile.php demo.example.com	SQL Injection CWE-89	25 Mar 2024	Unpatched CRITICAL	() 🛃 🖷
	Improper Authentication in /sendmail/ demo.example.com	Improper Authentication CWE-287	23 Mar 2024	Unpatched MEDIUM	1 🖌 🛃 🖷
	Path Traversal in /sendfile/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched MEDIUM	0 🖉 🛃 🖏
	Information Exposure in /systemstate.php demo.example.com	Information Exposure CWE-200	25 Mar 2024	Unpatched LOW	1 🛃 🖷
	Misconfigured Content Security Policy (CSP) demo.example.com	Security Warning	23 Mar 2024	Unpatched WARNING	0 🖉 🛃 🖏
	Path Traversal in /version/files/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched MEDIUM	1 🕗 🛃 🖷
	RCE via Server-Side Request Forgery (SSRF) in /items demo.example.com	Server-Side Request Forger CWE-918	ry 25 Mar 2024	Unpatched CRITICAL	() 🕹 🖷
	Misconfigured TLS Encryption demo.example.com	Security Warning	23 Mar 2024	Unpatched WARNING	1 🛛 🗠 🖷
	Path Traversal in /sendfile/ demo.example.com	Path Traversal CWE-22	12 Mar 2024	Unpatched MEDIUM	0 🕗 🕹 🖏



# Efficient. Simple. Cost-Effective.

We continuously monitor and test your web applications and APIs for security vulnerabilities, their exploitability and subsequent data exfiltration by using most relevant TTPs (tactics, techniques and procedures) from MITRE's ATT&CK matrix. Once a security flaw is confirmed, you will be immediately alerted by email, SMS or phone call.

For all customers of continuous breach and attack simulation, we offer a contractual zero false positives SLA and money-back guarantee: if there is a single false positive on your breach and attack simulation 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, 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





Paytweak

haymarket®







# Looking for Something Else?

Explore 20 use cases we have for you



**API** Penetration Testina



**API Security** Scanning



**Attack Surface** Management



**Cloud Penetration** Testing



**Cloud Security Posture** Management



20

</>>

Ģ



**Continuous Automated** 

**Mobile Penetration** 

**Mobile Security** 

**Network Security** 

Assessment

Red Teaming

Testing

Scanning



Continuous Penetration Testing

Cyber Threat 000 Intelligence

> Cybersecurity Compliance





**Digital Brand** Protection







**Third-Party Risk** Management

 $\square$ 



Web Penetration







# www.immuniweb.com



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



One Platform. All Needs.