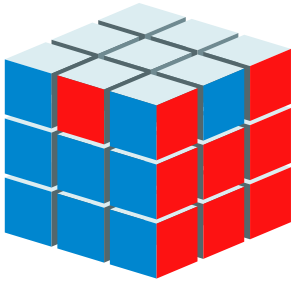


ImmuniWeb®

AI for Application Security

SOFTPROM

Gartner Cool Vendor

SC awards EUROPE highly recommended

IDC Innovator

BIG INNOVATION 2024

AI ARTIFICIAL INTELLIGENCE EXCELLENCE AWARD 2024

2024 FORTRESS CYBER SECURITY AWARD

2024 WINNER CYBER SECURITY EXCELLENCE AWARDS

TOP APPLICATION SECURITY STARTUPS OF THE YEAR ENTERPRISE LEAGUE

Cyber Security Awards

GLOBAL INFOSEC AWARDS WINNER CYBER DEFENSE MAGAZINE 2024

Software Suggest Momentum Leader WINTER 2024

TITAN AWARDS

TOP INFOSEC INNOVATOR WINNER CYBER DEFENSE MAGAZINE 2024

ImmuniWeb - Global Application Security Company

We Intelligently Automate, Simplify and Cut Costs of Application Security for over 1,000 Customers in 50+ Countries

SOFTPROM

Award-Winning Technology - Recognized Globally

Gartner

ImmuniWeb disrupts traditional application security testing by delivering web and mobile application testing augmented with proprietary machine-learning technology and human testing

IDC

ImmuniWeb has woven together machine learning with its own expert testers to confidently offer unique zero false-positive SLA

SOFTPROM

JVP Play CyberNYC

JVP VC and New York City Economic Development Corporation selected ImmuniWeb to join JVP Play CyberNYC, a leading cybersecurity growth program

ImmuniWeb is a Winner of 2024 Big Innovation and AI Excellence Awards, Cybersecurity Excellence Awards, Global Infosec Awards, Fortress Cybersecurity Award, SC Awards Europe 2023, and more

CSO FROM IDG

ImmuniWeb offers true automated penetration testing where its machine speed allows it to scale, while the human penetration testers ensure complete accuracy

The Hacker News

ImmuniWeb, an AI pioneer and award-winning application security company, stands out among emerging cybersecurity visionaries with its consolidated approach aimed to sharply reduce complexity and costs

ImmuniWeb Values

Creating Long-Term Value for Customers

We provide our customers with proven solutions that solve real problems in a cost-efficient and effective manner. We always place interests of our clients above ours: if our products cannot attain the customer's goals, we will disclose this and propose a better alternative.

Delivering Best Value for Money

We do not think that low-cost cybersecurity or cheap prices can create value for our clients. We rather strive to continually bring best value for money, pragmatically surpassing other offers available on the market by delivering the best possible quality for the best possible price to our clients.

Staying Curious to Innovate

We believe that by always staying hungry for new knowledge, our technical and scientific teams stay on the edge of emerging technologies, separating noise and hype from genuine innovation. This is why we invest at least half of our annual profit into research and development.

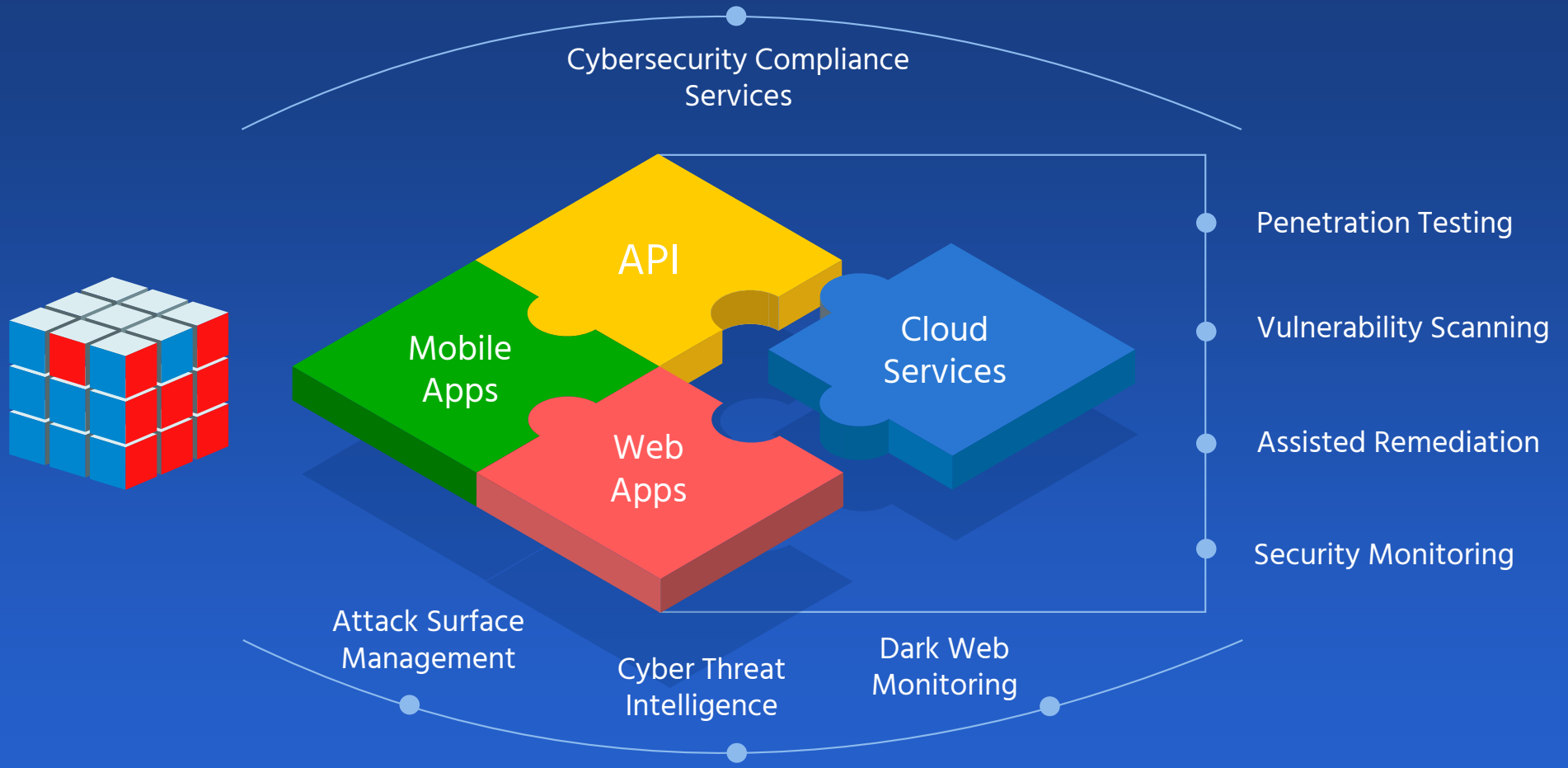
Building Bridges and Synergies

We team up with other vendors and even with our niche competitors to deliver more value by synergizing efforts instead of competing with each other. We believe that building bridges, partnerships and joint offerings creates substantially more value for our clients and builds a healthier market environment.

Perfecting Corporate Governance

We believe that a solid corporate governance is the foundation of business sustainability, being an ISO 9001 and ISO 27001 certified company. Our Board of Directors is comprised of independent and experienced industry practitioners who oversee corporate governance with help from our external financial auditors and Advisory Board.

One Platform. All Needs.



ImmuniWeb® AI Platform for Application Security

1 Platform

6 SaaS Products

20 Use Cases

SOFTPROM

ImmuniWeb®
AI Platform

- ImmuniWeb® Discovery
- ImmuniWeb® Neuron
- ImmuniWeb® Neuron Mobile
- ImmuniWeb® On-Demand
- ImmuniWeb® MobileSuite
- ImmuniWeb® Continuous

- API Penetration Testing
- API Security Scanning
- Attack Surface Management
- Cloud Penetration Testing
- Cloud Security Posture Management
- Continuous Automated Red Teaming
- Continuous Breach and Attack Simulation
- Continuous Penetration Testing
- Continuous Threat Exposure Management
- Cyber Threat Intelligence
- Dark Web Monitoring
- Mobile Penetration Testing
- Mobile Security Scanning
- Network Security Assessment
- Penetration Testing-as-a-Service
- Phishing Websites Takedown
- Third-Party Risk Management
- Threat-Led Penetration Testing
- Web Penetration Testing
- Web Security Scanning

DevSecOps &
CI/CD Integrations:

All Integrations

API Penetration Testing

Test your microservices and APIs for SANS Top 25 and OWASP API Security Top 10 vulnerabilities with ImmuniWeb® On-Demand API Penetration Testing

SOFTPROM

Just upload your API schema in a Postman, Swagger, GraphQL or another format, customize your API security testing requirements, schedule the penetration test date and get your pentest report. The API penetration testing is accessible around the clock 365 days a year.

We deliver every API penetration test with a contractual zero false positives SLA. If there is a false positive in your API penetration testing report, you get the money back. Detect all vectors of privilege escalation, authentication bypass, improper access control, and other sophisticated business logic vulnerabilities in your APIs, both in a cloud environment and on premise.

Our API penetration testing is provided with unlimited patch verification assessments, so your software developers can first fix the problems and then verify if the vulnerabilities have been properly remediated. Download your report in a PDF format or export the vulnerability data into your SIEM or WAF via our DevSecOps and CI/CD integrations. Enjoy 24/7 access to our security analysts may you have any questions or need assistance during the API penetration test.

API Security Scanning

Run unlimited scans of your APIs and microservices for OWASP API Top 10 vulnerabilities with ImmuniWeb® Neuron premium API Security Scanning

Customize your API security scanning requirements and authentication including SSO and MFA. Schedule recurrent API scans in a few clicks and configure email notifications about completed API scans.

Our API security scanning is provided with a contractual zero false positives SLA. If there is a false positive in your API security scanning testing report, you get the money back. Additionally, our award-winning Machine Learning technology provides better vulnerability detection and coverage rate compared to traditional software scanners that rely solely on heuristic vulnerability detection algorithms.

The API scanning reports are available via a multiuser dashboard with flexible RBAC access permissions. Our turnkey CI/CD integrations enable 100% automation of your web and API security testing within your CI/CD pipeline, both in a cloud environment and on premise. Our 24/7 technical support is at your service may your software developers have questions or need assistance during API security scanning.

SOFTPROM

Attack Surface Management

Illuminate your entire external attack surface with ImmuniWeb® Discovery
Attack Surface Management just by entering your company name

The non-intrusive and production-safe discovery process will rapidly detect, classify and score the risks of all your external IT assets located both on premise or in a multi-cloud environment. Find outdated or vulnerable software, expiring domains and SSL certificates, exposed or misconfigured systems, forgotten servers and shadow IT infrastructure including shadow cloud.

Detect leaked source code, container images or system snapshots available in third-party repositories. Visualize the geographical areas and countries where your data is physically stored for the compliance and data localization purposes. Moreover, all your IT assets are searched for mentions in the Dark Web to ensure risk-based and threat-aware attack surface management. Setup granular email alerts to your team for any newly discovered IT assets, misconfigurations, vulnerabilities or security incidents. Use groups and tags for asset management and triage.

Our attack surface management solution is provided at a fixed monthly price per company regardless of the number of your IT assets, security events or incidents. Leverage our API to synchronize the attack surface management data flow directly with your SIEM or other internal systems, or export selected findings into a PDF or XLS file.

SOFTPROM

Cloud Penetration Testing

Test your web applications, cloud-native apps or APIs hosted in AWS, Azure, GCP or other cloud service providers (CSP) with ImmuniWeb® On-Demand Cloud Penetration Testing

Customize your cloud penetration testing scope and requirements, schedule the penetration testing date and get your cloud penetration test report. The cloud penetration testing is accessible around the clock 365 days a year.

Our cloud penetration testing is provided with a contractual zero false positives SLA. If there is a false positive in your penetration testing report, you get the money back. Detect OWASP Top 10 and SANS Top 25 vulnerabilities, as well as OWASP API Top 10 weaknesses, CSP-specific security issues and misconfigurations. Uncover what can be done with cloud IMDS pivoting and privilege escalation attacks by exploiting excessive access permissions or default IAM policies in your cloud environment.

Every cloud penetration test is provided with unlimited patch verification assessments so your cloud engineers can fix the security flaws and then validate, at no additional cost, that everything has been properly remediated. Download your cloud penetration test report from the interactive and user-friendly dashboard into a PDF file or just export the data directly into your SIEM via our DevSecOps and CI/CD integrations. Enjoy 24/7 access to our security analysts may you need any assistance during the cloud penetration test.

SOFTPROM

Cloud Security Posture Management

Get a helicopter view on your multi-cloud attack surface with
ImmuniWeb® Discovery Cloud Security Posture Management

In contrast to other vendors, you don't need to provide us with your cloud IAM account: just enter your company name to start searching for your exposed cloud assets and endpoints of AWS, Azure, GCP and over 50 other public cloud service providers (CSP) around the globe. Detect shadow cloud resources or unwarranted cloud usage that may violate compliance requirements.

Our award-winning cloud security posture management rapidly detects your externally visible cloud assets including cloud computing instances, data storage, gateways, load balancers, databases, and various APIs or endpoints of cloud services. In addition to assessing your cloud attack surface for various misconfigurations, such as excessive access permissions or insecure IAM policies, we also visualize your geographical data storage for compliance and regulatory purposes.

Leverage our API to synchronize the cloud security posture management data flow with your SIEM or cloud-native monitoring systems, or simply export the findings into a PDF or XLS file. Enjoy a fixed monthly price per company regardless of the number of cloud assets, endpoints or security events. Customize instant alerts to relevant people in your DevOps of cybersecurity team once a misconfiguration is detected in your cloud.

SOFTPROM

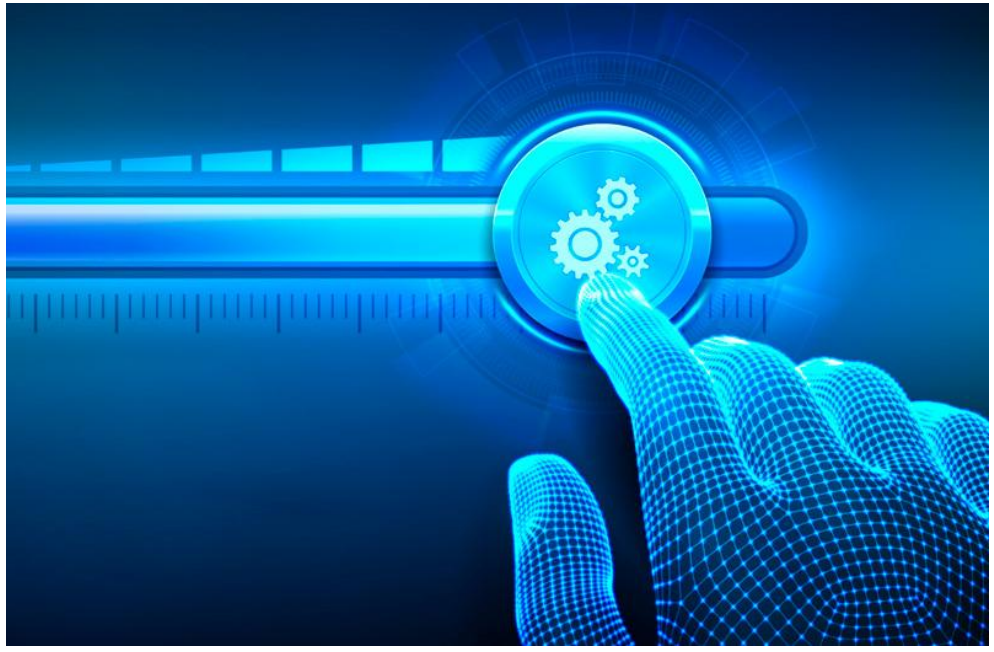
Continuous Automated Red Teaming

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

Outperform traditional one-time penetration tests with 24/7 continuous automated red teaming (CART) by ImmuniWeb® Continuous offering. 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.



SOFTPROM

Continuous Breach & Attack Simulation

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

Outperform traditional one-time penetration tests with 24/7 continuous breach and attack simulation (BAS) by ImmuniWeb® Continuous offering. 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.

SOFTPROM

Continuous Penetration Testing

Outperform traditional penetration testing with 24/7 Continuous Penetration Testing by ImmuniWeb® Continuous offering

We rapidly detect new code, functionalities or features in your web applications and APIs and then test the changes for security vulnerabilities, compliance or privacy issues in real time. Once a security issue is identified and confirmed, you will be immediately alerted by email, SMS or phone call in case of emergency.

For all customers of continuous penetration testing, we offer a contractual zero false positives SLA and money-back guarantee: if there is a single false positive on your continuous penetration testing dashboard, you get the money back. Our award-winning technology and experienced security experts reliably 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. 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 penetration testing data into your bug trackers or SIEM.

SOFTPROM

Continuous Threat Exposure Management

Detect and prioritize the most relevant cybersecurity and privacy risks, threats and vulnerabilities with ImmuniWeb® Discovery before malicious threats actors find or exploit them

In today's rapidly evolving threat landscape, organizations face a constant barrage of cyberattacks. To effectively protect themselves, they need a proactive and continuous approach to security. Continuous Threat Exposure Management (CTEM) is a comprehensive framework designed to provide organizations with real-time visibility into their security posture, enabling them to identify and mitigate threats before they can cause significant damage.

CTEM involves a continuous process of collecting, analyzing, and responding to threat intelligence. It leverages a combination of technologies, including threat intelligence feeds, vulnerability scanning, network monitoring, and security analytics, to provide organizations with a holistic view of their security landscape.

ImmuniWeb is a comprehensive cybersecurity platform that offers a range of services to help organizations manage their threat exposure.

SOFTPROM

Cyber Threat Intelligence

Monitor the surrounding cyber threat landscape and security incidents with ImmuniWeb® Discovery Cyber Threat Intelligence offering

Bundled with our award-winning attack surface management technology, the cyber threat intelligence will automatically search for security incidents implicating any of your systems, domain names, applications, servers, clouds, brands or users, including shadow IT assets and shadow cloud resources.

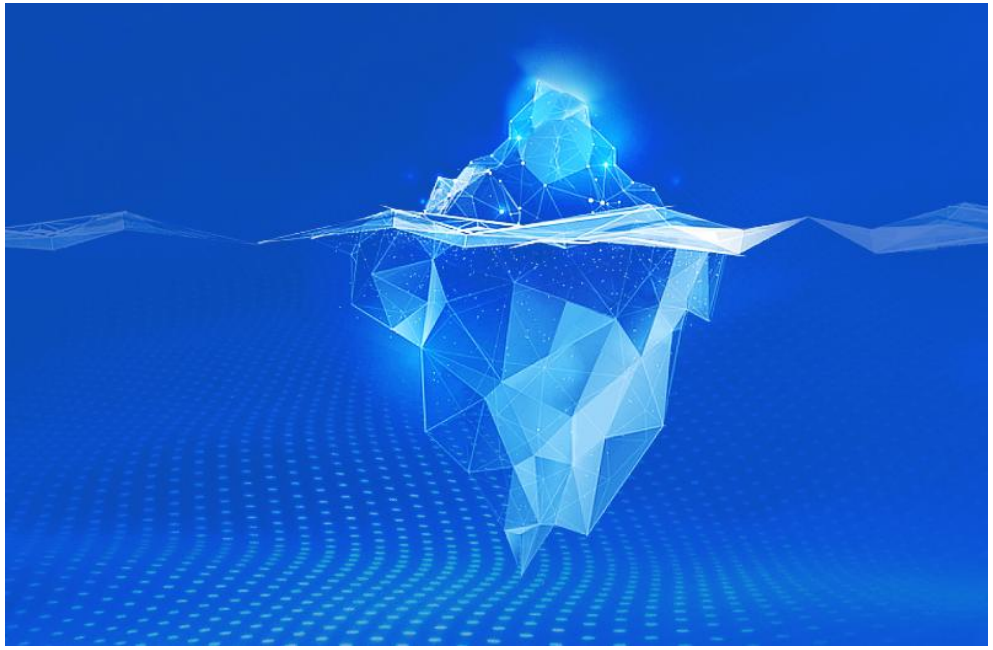
Just enter your company name to get all mentions of your company or its IT assets on the Dark Web, hacking forums, underground marketplaces or Telegram channels. Our award-winning Machine Learning technology removes duplicates and fakes, offering reliable cyber threat intelligence feeds. Get instant alerts about the ongoing phishing campaigns, squatted domain names, fake accounts on social networks or malicious mobile apps usurping your corporate identity. Detect indicators of compromise (IoC) of your on-premise or cloud-based systems, as well as any mentions of your systems in various blacklists for suspicious or hacking activities.

Dispatch instant alerts about new security incidents, data leaks and cyber threats to relevant people in your DFIR or legal team by using groups and automated incident classification on the interactive dashboard. Export the cyber threat intelligence findings into a PDF or XLS file, or just dispatch them directly into your SIEM by using our API. Enjoy a fixed price per company regardless of the number of security incidents and mentions on the Dark Web. Our security analysts are here to help may you need details or support.

SOFTPROM

Dark Web Monitoring

Discover your data leaks, stolen credentials, backdoored systems and stolen documents on the Dark Web with ImmuniWeb® Discovery Dark Web Monitoring



SOFTPROM

Just enter your company name to launch the Dark monitoring enhanced complemented by the continuous monitoring of phishing campaigns, domain squatting, fake social network accounts, malicious mobile apps usurping your corporate brand, and indicators of compromise (IoC) of your on-premise or cloud-based IT assets.

Monitoring of underground marketplaces and hacking forums is enhanced with 24/7 surveillance of paste websites, social networks, IRC and Telegram channels. In contrast to other vendors, our Dark Web monitoring is bundled with our attack surface management technology to automatically detect all mentions of any of your IT systems, domain names, servers, cloud instances, applications or users on the Dark Web without the need to enter them manually, as well as to discover compromised shadow IT assets and shadow cloud resources.

Browse risk-based security incidents on the user-friendly, interactive and customizable dashboard, export the findings into a PDF or XLS file, or use the API to automatically synchronize the data with your SIEM system. Enjoy a fixed monthly price per company regardless the number of security incidents, mentions or leaks in the Dark Web. Our security analysts are here to help may you need additional details or support.

Mobile Penetration Testing

Test your mobile application security, compliance and privacy with
ImmuniWeb® MobileSuite Mobile Penetration Testing

Just upload your iOS or Android mobile app, customize your penetration testing requirements, schedule the penetration test date and download your mobile penetration test report. Verify whether your mobile app's privacy and encryption mechanisms conform to the industry best practices, and detect dangerous misconfigurations affecting your mobile app's backend and APIs.

Our mobile penetration testing is equipped with a contractual zero false positives SLA and a money-back guarantee: if there is a single false positive in your penetration testing report, you get the money back. Detect OWASP Mobile Top 10 weaknesses in your mobile app and discover SANS Top 25 and OWASP API Top 10 vulnerabilities in the mobile app's backend including APIs and web services. Run a Black Box or authenticated security testing using SSO, MFA or OTP authentication mechanisms. The mobile penetration testing is accessible around the clock 365 days a year.

Leverage our unlimited patch verification assessments after the mobile penetration test, so your software developers can easily validate whether all the findings have been properly patched. Export vulnerability data from your interactive dashboard to a PDF or XLS file, or just get the mobile penetration testing data directly into your SIEM or bug tracking system for faster remediation via our DevSecOps integrations. Enjoy 24/7 access to our security analysts if you have questions or need assistance during the test.

SOFTPROM

Mobile Security Scanning

Detect OWASP Mobile Top 10 weaknesses in all your mobile apps with
ImmuniWeb® Neuron Mobile Security Scanning

SOFTPROM

The mobile security scanning offering provides a comprehensive and rapid detection of mobile app vulnerabilities and weaknesses, offering a contractual zero false positives SLA for each mobile security scan. In addition to mobile security audit, you will get an overview of your mobile privacy, compliance and encryption issues including a comprehensive inventory of the mobile app's backend endpoints and APIs.

Automated SAST, DAST and SCA mobile security scanning can be launched instantly after uploading your .ipa or .apk file to detect OWASP Mobile Top 10 vulnerabilities and weaknesses in a simple, fast and reliable manner. Scan results are usually available within minutes depending on the application size and complexity. On top of the mobile vulnerability scanning, we will also inspect excessive or dangerous mobile app permissions, missing or weak encryption, and suspicious external communications of the mobile app. Additionally, a broad spectrum of privacy, compliance and encryption checks will be conducted to ensure that your mobile ecosystem conforms to regulatory requirements such as GDPR.

Enhancing the value of our advanced mobile security scanning features, our security analysts and mobile security experts are available 24/7 to answer your questions about the findings or remediations. ImmuniWeb Neuron Mobile pricing model is simple and flexible, is based on the number of your mobile apps and the annual number of scans, making our pricing one of the most competitive one on the global market.

Network Security Assessment

Discover your externally accessible network devices and services with ImmuniWeb® Discovery Network Security Assessment offering

Just enter your company name to get a comprehensive visibility of your external servers, network and IoT devices, and other IT assets hosted both on premise and in a multi-cloud environment. The network security assessment offering is bundled with our award-winning attack surface management technology to ensure that all your network services are detected and assessed, including shadow IT and shadow cloud infrastructure that may lead to disastrous data breaches.

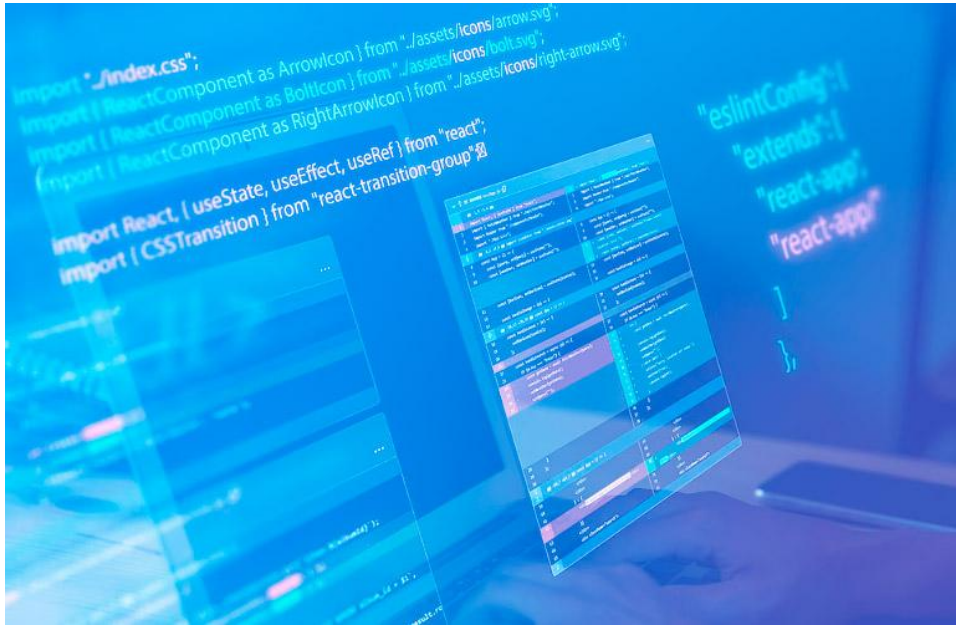
During the non-intrusive network security assessment, every open network port is carefully analyzed with our smart fingerprinting technology to detect the running network service and its version to provide you with a risk-based scoring for each of your network IP address. Unlike the traditional network vulnerability scanning solutions, our production-safe network scanning technology will not disrupt or slow down your network services, while getting all the information.

Detect shadow, abandoned or forgotten servers and network equipment with critical vulnerabilities. Reduce your network attack surface to accelerate and cut the costs of network penetration testing or PCI DSS scanning. Dispatch instant alerts to the relevant people in your team by using groups, tags and alerts on the interactive dashboard. Export vulnerability data via the API into your SIEM or simply get the findings in a PDF or XLS file. Enjoy a fixed monthly price per company regardless the number of network assets and services.

SOFTPROM

Penetration Testing-as-a-Service

Don’t leave a chance to cybercriminals by testing your applications and APIs with our ImmuniWeb® On-Demand Penetration Testing-as-a-Service solution



SOFTPROM

In today's rapidly evolving threat landscape, organizations face a constant barrage of cyberattacks. To effectively protect themselves, they need to conduct regular security assessments to identify and address vulnerabilities. Penetration testing is a crucial component of a comprehensive security strategy, but it can be resource-intensive and time-consuming for many organizations. Penetration Testing-as-a-Service (PTaaS) offers a scalable and cost-effective solution to meet the growing demand for security testing.

PTaaS is a cloud-based service that provides organizations with access to professional penetration testing services on demand. It allows organizations to outsource their security testing needs to experienced security experts, freeing up their internal resources to focus on other critical tasks.

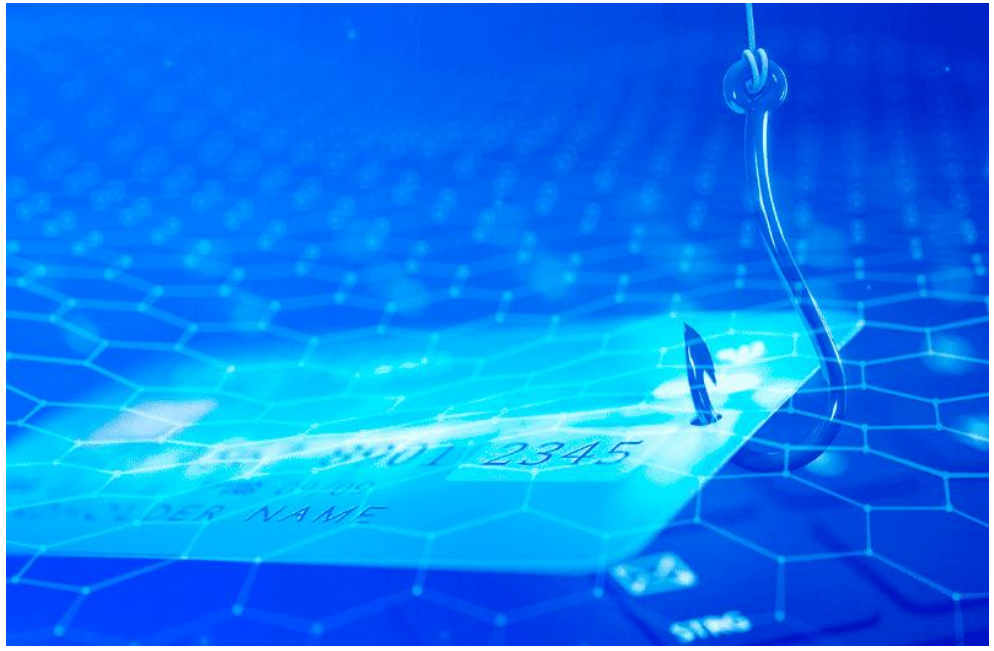
ImmuniWeb offers a comprehensive Penetration Testing-as-a-Service (PTaaS) solution that helps organizations identify and address security vulnerabilities in their applications, infrastructure, and networks.

ImmuniWeb's expertise and comprehensive approach make us a valuable partner for organizations seeking to strengthen their security posture through effective penetration testing.

Phishing Websites Takedown

Take down malicious phishing websites from any country or TLD in a few clicks with ImmuniWeb® Discovery Phishing Websites Takedown

Prevent your employees, customers and partners from falling victims to surging phishing attacks with ImmuniWeb® Discovery phishing websites takedown. Just enter your company name to launch the Dark Web monitoring enhanced with the continuous monitoring of phishing websites, squatted domain names, fake accounts in social networks, rogue mobile apps usurping your corporate brand or identity, fraudulent or malicious web pages, and indicators of compromise (IoC) of your IT assets located on premise or in a multicloud environment.



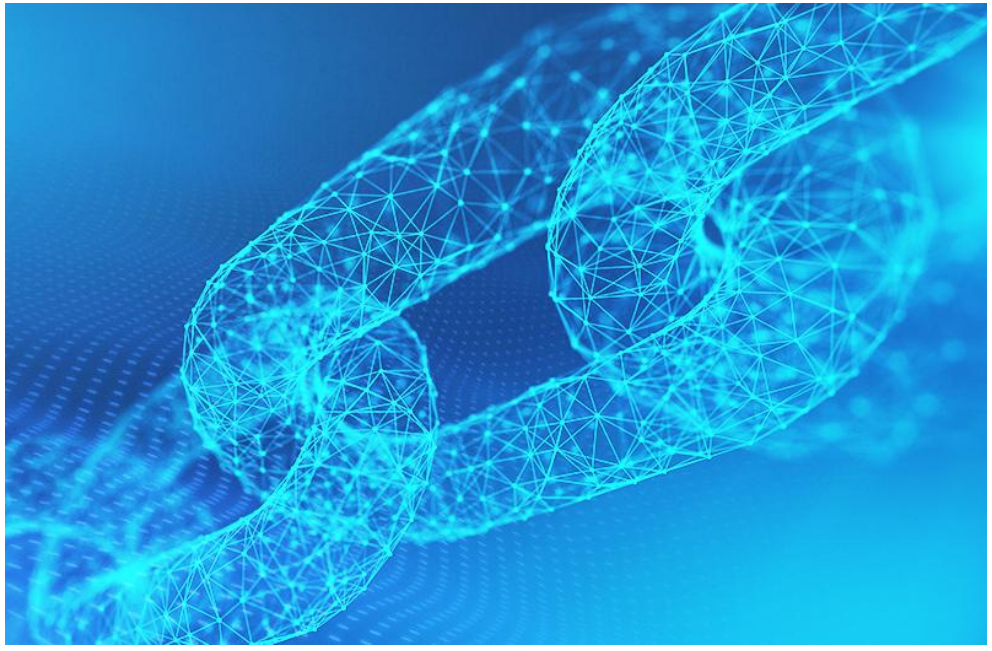
Once you receive an alert about a phishing website, just click on a button to request its takedown. ImmuniWeb's cybercrime investigators and legal experts will rapidly analyze the case and then undertake the necessary steps to lawfully take down the malicious website. Depending on the circumstances of the case, the takedown usually takes from one day to one week. May you have any questions, our security analysts are at your service 24/7.

All detected incidents, including phishing websites, are available on the user-friendly, interactive and customizable dashboard from where you can export the findings into a PDF or XLS file, or just use the API to automatically synchronize the data with your in-house SIEM system. Enjoy a fixed monthly price per company regardless the number of phishing websites takedowns or complexities of the case.

SOFTPROM

Third-Party Risk Management

Prevent supply chain attacks and mitigate third-party risks with
ImmuniWeb® Discovery Third-Party Risk Management



The third-party risk management offering is bundled with our award-winning attack surface management technology and is also enhanced with Dark Web monitoring to ensure inclusive visibility of cybersecurity risks and threats that external suppliers may pose for your business. The third-party risk management is available both as a one-time assessment and continuous security monitoring for business-critical vendors.

Just enter the name of your supplier or vendor to get a comprehensive snapshot of its external attack surface, misconfigured or vulnerable systems and applications, unprotected cloud storage, mentions on the Dark Web and data leaks, stolen credentials or compromised systems, ongoing phishing or domain squatting campaigns. The entire process is non-intrusive and production-safe, making it a perfect fit for your third-party risk management program. Our security analysts are available 24/7 may you have questions about the findings or need further assurance.

Get the risk-scored findings on the interactive dashboard where your vendors can also connect to see the details and rapidly remediate the problems. Prevent surging supply chain attacks by taking your vendor risk management program to the next level. Fulfill the compliance requirements to regularly audit third-party systems that process personal, financial or other regulated data of your company. Enjoy a fixed price per vendor regardless the number of IT assets, mentions on the Dark Web or number of security incidents.

SOFTPROM

Threat-Led Penetration Testing

Perform a threat-driven and context-specific penetration testing with ImmuniWeb® On-Demand to test your resilience to most relevant TTPs and threat actors

In today's rapidly evolving threat landscape, traditional penetration testing methods may not be sufficient to identify and address the most critical vulnerabilities. Threat-led penetration testing is a more targeted approach that focuses on simulating real-world attacks based on current threat intelligence. By aligning testing efforts with actual threats, organizations can prioritize their security efforts and improve their overall resilience.

ImmuniWeb's Threat-Led Penetration Testing approach focuses on simulating real-world attack scenarios based on current threat intelligence. This methodology provides a more targeted and effective assessment of your organization's security posture.

By simulating real-world attack scenarios, ImmuniWeb provides a more accurate assessment of your organization's security posture. Threat-led testing helps you focus on the most critical vulnerabilities and threats. By understanding your organization's vulnerabilities to specific threat actors, you can develop more targeted mitigation strategies. Threat-led testing can help you demonstrate compliance with industry regulations and standards.

ImmuniWeb's Threat-Led Penetration Testing approach provides a comprehensive and effective way to assess your organization's security posture against real-world threats.

SOFTPROM

Web Penetration Testing

Test your web applications and APIs for SANS Top 25 and OWASP Security Top 10 vulnerabilities with ImmuniWeb® On-Demand Web Penetration Testing

SOFTPROM

Customize your web penetration testing scope and requirements, schedule the penetration testing date and download your penetration testing report. The penetration testing is accessible around the clock 365 days a year.

Our web application penetration testing is equipped with a contractual zero false positives SLA and a money back guarantee: if there is a single false positive in your web penetration testing report, you get the money back. Detect all vectors of privilege escalation, authentication bypass, improper access control, and other sophisticated business logic vulnerabilities in your web applications and APIs, both in a cloud environment and on premise. Discover privacy and compliance misconfigurations in your web applications that may lead to penalties for non-compliance.

The web penetration testing is provided with unlimited patch verification assessments, so your software developers can first fix the problems and then verify if the vulnerabilities have been properly remediated. Download your penetration testing report in a PDF format or export the vulnerability data into your SIEM or WAF via our DevSecOps and CI/CD integrations. Enjoy 24/7 access to our security analysts may you have any questions or need assistance during the web penetration test.

Web Security Scanning

Run unlimited scans of your web applications and APIs for OWASP Top 10 vulnerabilities with ImmuniWeb® Neuron premium Web Security Scanning

Select your targets, customize your web security scanning settings and setup authentication scanning if necessary, including SSO and MFA authentication. Schedule recurrent web security scans in a few clicks and configure instant email notifications about completed scans, dispatching relevant scan reports to your team in a flexible and easily configurable manner.

Our web security scanning is provided with a contractual zero false positives SLA. If there is a false positive in your web security scanning testing report, you get the money back. Additionally, our award-winning Machine Learning technology provides better vulnerability detection and coverage rates compared to traditional software scanners that use only heuristic vulnerability detection algorithms.

Web security scanning reports are available via a multiuser dashboard with RBAC access permissions. Our turnkey CI/CD integrations enable 100% automation of your web and API security testing within your CI/CD pipeline, both in a multi-cloud environment and on premise. Our 24/7 technical support is at your service may your software developers have questions or need assistance during web security scanning.

SOFTPROM

Why Choosing ImmuniWeb® AI Platform

Because You Deserve the Very Best

Reduce Complexity

All-in-one platform for 20 synergized use cases

Learn More

Optimize Costs

All-in-one model & AI automation reduce costs by up to 90%

Learn More

Validate Compliance

Letter of conformity from law firm confirming your compliance

Learn More

> *At ImmuniWeb, we always carefully listen to all our customers to continuously make our award-winning Platform even better to stay ahead of the rapidly evolving cyber threats. This unique synergy helps us maintain the customer retention rate above 90%.*

Dr. Ilia Kolochenko
Chief Architect & CEO

Trusted by 1,000+ Global Customers

We used ImmuniWeb for some of our products and we have been highly satisfied from the provided service as valid vulnerabilities with no false positives were identified. The report ImmuniWeb delivered to us was quite clear in terms of the classifications and the description of the identified vulnerabilities, linking to the corresponding CVE and the fix recommendations. We recommend ImmuniWeb to other vendors to make their web products secure.

ebay

ImmuniWeb is the best and simplest way to secure your business online. It's really fantastic experience to get report with zero false positive with detailed actions how to resolve problems and remove vulnerabilities. I think ImmuniWeb is definitely the best alternative to pen testers. As well as a way to save on staff and other costs. I am glad that I can get it all without any hidden costs and without complicated licensing schemes.

BDO

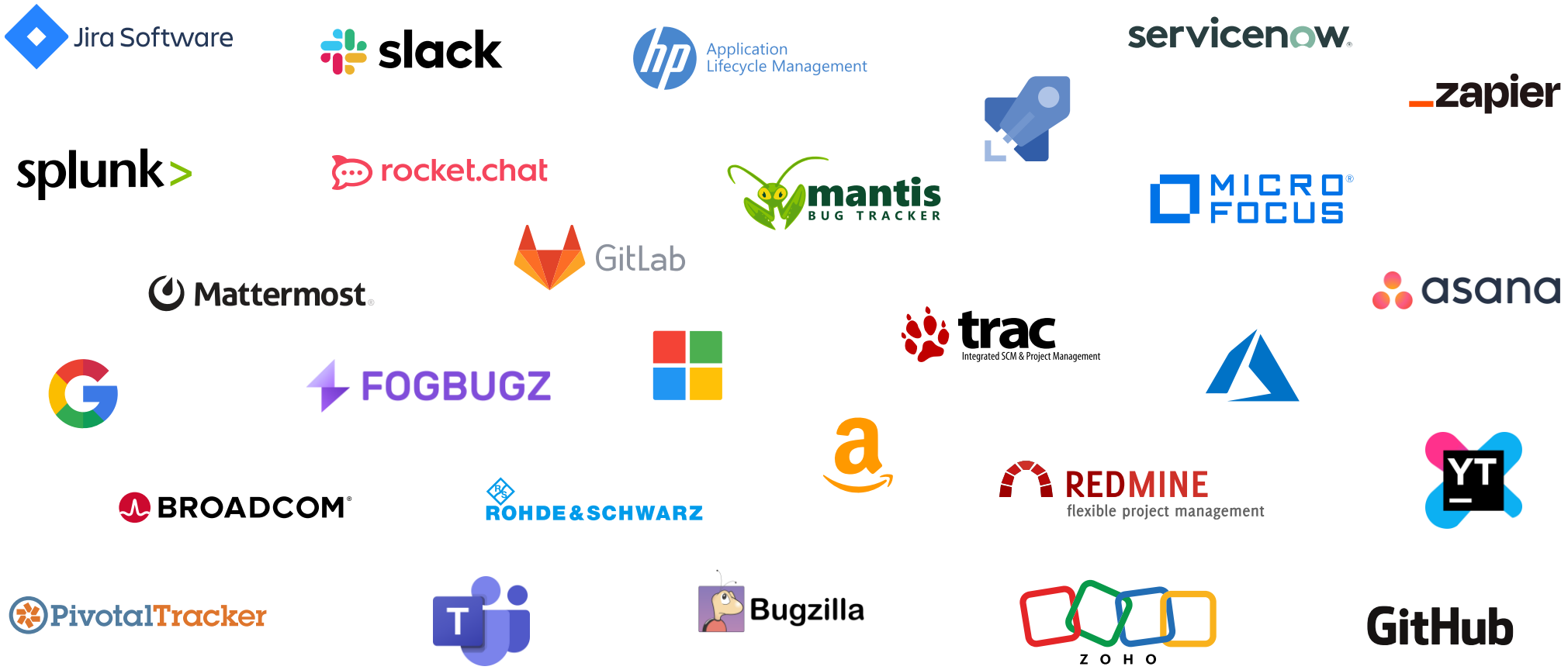
The security assessment was extremely useful and highlighted some minor but interesting vulnerabilities on our web site that are being addressed.

ITU

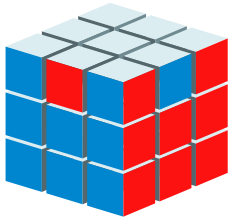
ImmuniWeb is an efficient and very easy-to-use solution that combines automatic and human tests. The results are complete, straightforward and easy to understand. It's an essential tool for the development of the new digital activities.

next bank
CRÉDIT AGRICOLE

DevSecOps and CI/CD Integrations



Partnerships with the Industry Leaders



ImmuniWeb®

AI for Application Security

SOFTPROM

CREST ACCREDITED

SYSTEM CERTIFICATION ISO 9001 SGS

SYSTEM CERTIFICATION ISO/IEC 27001 SGS

UKAS MANAGEMENT SYSTEMS 005

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

SC awards EUROPE Winner

One Platform. All Needs.