



emitec
datacom

Emitec AG
Birkenstrasse 47
6343 Rotkreuz

+41 41 748 60 10
info@emitec.ch
www.emitec-datacom.ch



Emitec Group
#1 in Test & Measurement, worldwide.



Are you truly prepared for a DDoS attack?

Discover your network's **strengths and vulnerabilities** with LoDDoS's specialized **DDoS testing and assessment services** — tailored to identify potential weaknesses before they can be exploited, ensuring your defenses are **tested, tried, and true**.

LoDDoS is Your Premier Partner in DDoS Preparedness and Testing. At LoDDoS, we specialize in providing state-of-the-art automated Distributed Denial of Service (DDoS) **testing and assessment services**. Our mission is to empower organizations by exposing and addressing vulnerabilities within their network defenses, ensuring they are equipped to withstand the most severe DDoS attacks.

Through our comprehensive **testing methodologies and advanced testing technologies**, we offer unparalleled insights into the resilience of your digital infrastructure. Our goal is to safeguard your connectivity and ensure business continuity by preparing you today for the cyber challenges of tomorrow.

Why Choose LoDDoS?



Hyper - Realistic Tests:

Our tailored replicate the sophistication and intensity of real-world DDoS attacks. We leverage a vast arsenal of attack vectors, from overwhelming volumetric floods to insidious application-layer assaults, to comprehensively evaluate your network's ability to withstand pressure.



Comprehensive Attack Tests:

LoDDoS's DDoS testing framework is designed to Test a wide range of attack scenarios, including sophisticated tactics employed by modern cyber adversaries. With the ability to launch attacks using up to 4,000 bots and reaching intensities of up to 240 Gbps, our tests offer a realistic assessment of how your network can withstand extreme conditions.



Automated or Operator-Guided Test Execution:

LoDDoS introduces Autopilot, a revolutionary advancement in DDoS testing technology, offering a fully automated solution that streamlines the process of testing DDoS attacks against your digital infrastructure. Designed to meet the evolving needs of businesses in safeguarding their online presence, LoDDoS also provides an Operator-Guided Testing option, allowing customers to benefit from the expertise of our cybersecurity professionals.



Insight-Driven Optimization:

Go beyond simple pass/fail assessments. Our experts meticulously analyze test results, providing detailed reports pinpointing the root causes of vulnerabilities. You'll receive actionable recommendations to plug security gaps and boost your defensive strategies.



Security Through Transparency:

We understand the sensitivity of network testing. LoDDoS tests are conducted within secure, controlled environments, adhering to industry best practices and ethical guidelines. Our transparent approach ensures you have full visibility and control throughout the process.



Beyond Testing: Strategic Planning and Cybersecurity Consulting

LoDDoS is more than just a testing tool. We offer consulting services to help you refine your incident response plans and improve staff readiness. By testing attack scenarios, we empower your team to respond confidently and decisively in a real-world crisis.



Self-Service and Operator-Supported Testing:

Our next-generation LoDDoS platform empowers organizations to test their own infrastructure for vulnerabilities. The intuitive interface allows users to launch attack tests independently on selected targets while also offering professional operator support for businesses that require

How We Conduct Tests:

- At LoDDoS, our methodology for executing DDoS tests is deeply rooted in ethical practices and a commitment to security, demanding explicit consent via a comprehensive written agreement from our valued clients before any test is initiated. This foundational step ensures mutual trust and clarity on the scope and limitations of the test exercises.

How We Conduct Tests:

- ✓ At LoDDoS, our methodology for executing DDoS tests is deeply rooted in ethical practices and a commitment to security, demanding explicit consent via a comprehensive written agreement from our valued clients before any test is initiated. This foundational step ensures mutual trust and clarity on the scope and limitations of the test exercises.
- ✓ Our tests are not just about testing; they are about understanding and strengthening. They are crafted through a meticulous collaborative planning process involving our expert team and our client's stakeholders. This process is vital for setting crystal-clear objectives, identifying potential vulnerabilities, and establishing a precise timetable for the tests. Such detailed planning ensures that every test is tailored to address the unique challenges and requirements of each client's infrastructure.
- ✓ The technical execution of our tests leverages dedicated servers and an extensive network of globally positioned agents. This strategic deployment is crucial for creating realistic traffic patterns and attack scenarios without the ethical and legal concerns associated with the use of compromised hosts. Our choice to use dedicated resources underscores our commitment to not only the efficacy but also the integrity of our tests.

The LoDDoS Testing Process: A Blueprint for Resilience

- ✓ **Strategic Planning:** Our specialists delve into your network's intricacies, threat landscape, and business priorities. Together, we create a customized DDoS Test Plan defining objectives, timelines, and simulation parameters.
- ✓ **Tailored DDoS Testing:** We execute multi-pronged attacks across network, transport, and application layers. Testing is calibrated to your specific risk profile, with intensities ranging from disruptive to potentially crippling.
- ✓ **Deep Analysis & Optimization:** You'll receive comprehensive analysis, including technical breakdowns of successful attack paths, pinpointing the precise sources of failure. Expert guidance offers practical steps to bolster network design, optimize mitigation tools, and streamline processes.

Flexible Testing Options

Organizations can execute tests using three different methods:

Self-Directed Testing:



Run tests independently with your internal security team.

Guided Testing with LoDDoS Experts:



Schedule tests in advance and let them execute automatically at the specified time. Test reports are available for review and download at your convenience.

Auto Run Feature:



Get step-by-step assistance from our professionals.

Multi - Attack & Multi Monitoring Capabilities

Multi-Attack: Execute up to three attack types simultaneously on the same target to simulate real-world multi-vector threats.

Multi-Monitoring: During each attack, track how your infrastructure responds across all OSI layers in real time, allowing for deep performance analysis.

Carpet Bombing Attack Tests:

In addition to ICMP, TCP, UDP, DNS, and HTTP-based attacks, we have introduced Carpet Bombing, a powerful technique that distributes attack traffic evenly across multiple targets within a designated IP range. This method allows organizations to bypass rate-limiting defenses and assess resilience against more sophisticated attack scenarios.

Global Bot Network and Enhanced Capacity:

LoDDoS now supports a distributed bot network spanning multiple continents (excluding Antarctica), leveraging infrastructure from major cloud providers including Google, Rackspace, Huawei, Akamai, and DigitalOcean. With 4,000 active bots and an expanded bandwidth capacity of 240 Gbps, LoDDoS delivers an unprecedented level of testing realism.

AI-Powered Optimization and Mitigation Recommendations:

LoDDoS integrates Artificial Intelligence (AI) to enhance test insights and generate customized mitigation recommendations based on attack results. AI-driven assistance ensures efficient attack execution and real-time guidance throughout the testing process.

ASM (Attack Surface Management) Tool:

Our ASM Tool identifies attack surface vulnerabilities and automatically suggests optimal attack vectors, ensuring maximum efficiency in every test scenario.

Flexible Licensing and Whitelabel Solutions:

Flexible Pricing Models

60-Minute Packages: Ideal for standard testing needs.

Credit-Based System: A flexible pay-as-you-go model allows you to manage your balance efficiently and scale testing as needed.

Whitelabel Solution for Security Partners:

Our Whitelabel Program enables cybersecurity service providers to rebrand the LoDDoS platform with their own logo and identity, allowing them to offer professional DDoS testing services under their own brand.

LoDDoS Key Features

Extensive Range of Simulated Attacks:



Volumetric Attacks: UDP Floods, ICMP Floods, DNS Amplification and many more.

Protocol Attacks: SYN Floods, fragmented packet attacks, reflection attacks and many more.

Application-Layer Attacks: Slow Loris, HTTP floods, targeted API attacks, and more.

Granular Test Customization:



Adjust attack intensity from targeted probes to high-volume saturation.

Fine-tune the mix of attack types to mirror real-world scenarios or your specific risk profile.

Define specific targets within your infrastructure (application servers, firewalls etc.)

Global Attack Infrastructure:



LoDDoS is engineered to work harmoniously with multiple cloud platforms, including the foremost providers in the industry.

This ensures that no matter the diversity of your cloud infrastructure, LoDDoS can deliver precise and thorough DDoS testing.

Real-Time Performance Monitoring:



Access a dynamic, user-friendly dashboard that provides live updates and comprehensive insights into the DDoS tests as they happen.

This interactive platform allows you to observe the test's progress, including attack vectors used, intensity, duration, and real-time impact on your network's performance.

Partner Portal:



The Partner Portal is a dedicated online platform that empowers our partners with extensive resources, tools, and support to enhance their service offerings.

Through the portal, partners can access detailed analytics, management console, marketing materials, and technical support.

Preparedness & Beyond:



We help you translate testing findings into improved readiness.

This includes updating incident response protocols, conducting staff training against test attacks, and continuous monitoring for emerging threats.

MSSP Offering:



Our Managed Security Service Provider (MSSP) Offering is tailored to enable service providers to deliver cutting-edge DDoS testing as a managed service.

This comprehensive package includes customizable security solutions, operational support, and detailed reporting capabilities, allowing MSSPs to offer their clients end-to-end DDoS testing services.

By leveraging our MSSP offering, partners can expand their portfolio, enhance customer satisfaction, and generate new revenue streams with minimal investment.

Flexible Pricing Options:



LoDDoS offers flexible pricing options tailored to accommodate a variety of budgetary requirements and testing frequencies.

Our models include both pay-per-use for occasional testing needs and subscription packages for regular, ongoing assessments.

This approach ensures that businesses of all sizes can access our advanced DDoS testing services, aligning with their financial and operational strategies for optimal cybersecurity investment.

Comprehensive Post-Test Reporting:



Receive detailed analysis of your defense responses, pinpoint bottlenecks, and receive optimization recommendations.

AI-enhanced reports provide detailed insights into detected threats, vulnerabilities, and remediation actions.

These reports are not only comprehensive but also actionable, offering clear guidance on how to strengthen security postures based on AI-driven analysis.

