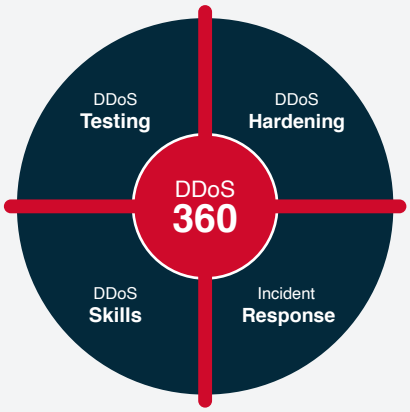
RED BUTTON
DDoS Experts

DDoS 360

DDoS 360 is the ultimate DDoS protection service for high-risk companies, maximizing the security posture and the ability to withstand any DDoS attack regardless of its intensity and persistence.

Unlike the common practice of a single DDoS test session, the DDoS 360 program contains multiple, year-round activities carried out by our top DDoS experts. This includes extensive pre-attack activities to strengthen your technological infrastructure and improve the skills of your teams, as well as a dedicated incident response expert team in the event of an attack. Combined, these activities form an all-inclusive DDoS strategy that increases your organization's ability to withstand any DDoS attack by over 90%.

Comprehensive, Year-Round DDoS Preparedness



Activities in the DDoS 360 program are tailored to each customer's needs, yet always include a combination of the following categories:

DDoS Testing

Periodic DDoS testing sessions (per quarter) to validate the security posture, evaluate protection improvements, and identify issues.

DDoS Hardening

A thorough audit of your network architecture and DDoS protection system configuration to assess your current protection status against all types of attacks. This is followed by detailed recommendations for hardening and optimization. When relevant, the hardening activities may include a POC for the selection of a DDoS vendor.

DDoS Skills

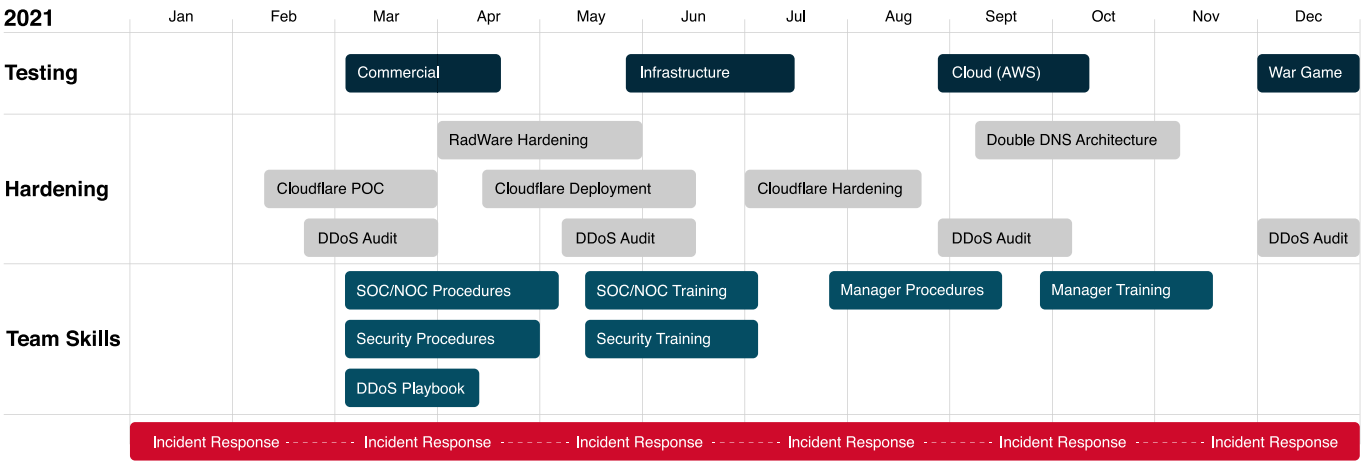
DDoS training of all stakeholder teams (NOC/SOC, Security, Network, and IT managers), a DDoS attack playbook with detailed procedures to follow during a DDoS attack, and war game simulations to validate teams' preparedness.

Incident Response (IR)

In case of an attack, our DDoS experts are immediately assigned to manage the attack until its full mitigation.

DDoS 360 activities are spread throughout the year based on the needs and constraints of your organization. An activity roadmap plan is put together and may be dynamically adjusted to respond to changes such as a new threat or a newly detected security gap.

DDoS 360 – Example of Yearly Activities

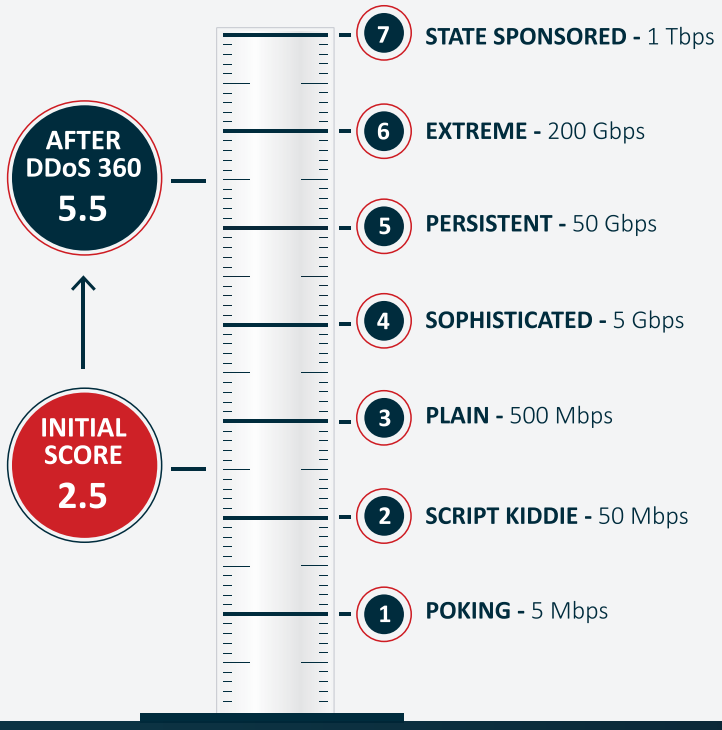


Quantifiable Improvement

The DDoS 360 program provides measurable improvements of the DDoS security posture and readiness for attacks.

Upon launching DDoS 360, we conduct a simulation and measure your DDoS Resiliency Score. This provides a baseline score, outlining a list of attack types that your organization can withstand prior to an outage.

Throughout the program, we run multiple testing sessions to measure your resiliency score and compare it to the baseline. Typically, the score improves by at least 90%.



Why Red Button?

We are DDoS experts. We have managed hundreds of attacks at commercial and federal banks in Europe, Asia, and South and Central America, online trading and payment services, Internet and ISP providers, and large international gaming companies.

Our experience has taught us that DDoS testing is only the first step in preparing for a DDoS attack, and extensive "know-how," combined with ongoing hardening, training, and simulation, is the only way to fully prepare for serious attacks, which are executed on companies in high-risk categories. Our 360 program combines our full range of DDoS expertise.

Rich DDoS experience. Since 2010, our team has mitigated hundreds of DDoS attacks, including some of the most massive, sophisticated ones. We regularly handle attacks of over 100 Gbps and have mitigated one of the largest volumetric attacks, at over 1.2 Tbps. This provides us with the most up-to-date insights on DDoS attack trends and knowledge of the most effective prevention practices.

Incident response (IR). Each year, our team handles ~30 global incident response incidents, helping mitigate intense volumetric attacks from 100 Gbps to 1.2 Tbps. Our IR practice enriches our knowledge of attack trends, failure points, and vendors, which is transferred to our customers.

Solution-agnostic. Our vendor-agnostic approach ensures that we provide objective consulting based on our hands-on experience with all the top DDoS software and hardware vendors.

Objective measurement. We initiated and established the DDoS Resiliency Score (DRS), an open DDoS benchmark standard, which allows for measuring and evaluating DDoS mitigation strategies in objective, quantitative terms.

Industry recognition. Red Button is an authorized AWS DDoS Test Partner—one of very few companies authorized to conduct DDoS testing for AWS customers.

www.red-button.net **info@redbutton.net**