RED BUTTON
DDoS Experts

WHITEPAPER

DDoS Education

Training, Playbooks & Wargames

Introduction

It takes more than technology to mitigate a DDoS attack. It is therefore crucial that technical teams have the required skills, know how to quickly identify an attack, and take the correct mitigation measures.

To address the human factor and skills, and increase the ability of organizations to effectively respond to DDoS attacks, Red Button offers:

- Training courses
- DDoS playbook procedures
- DDoS wargames

DDoS Training Courses

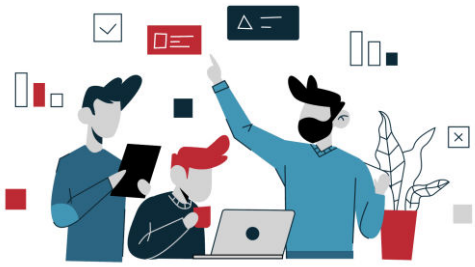
Our DDoS training courses help NOC, SOC and security teams build their skills in effectively preventing and mitigating DDoS attacks.

Courses combine both theory and hands-on labs, incorporate the most up-to-date insights on DDoS attack trends, and include the best prevention practices used by our own teams.

Available training courses include:

DDoS Basics 101 – an introductory, online course for information security personnel, network engineers, CISOs, NOC/SOC managers, and IT staff who handle DDoS attacks. The course introduces the DDoS attack landscape and exposes students to different types of attacks, mitigation techniques and architecture.

DDoS Advanced 102 – a second-level course for students who completed the Basics course. Typically, this course is delivered on site and customized for the customer's product-specific information and their specific network architecture.



DDoS Playbook Procedures

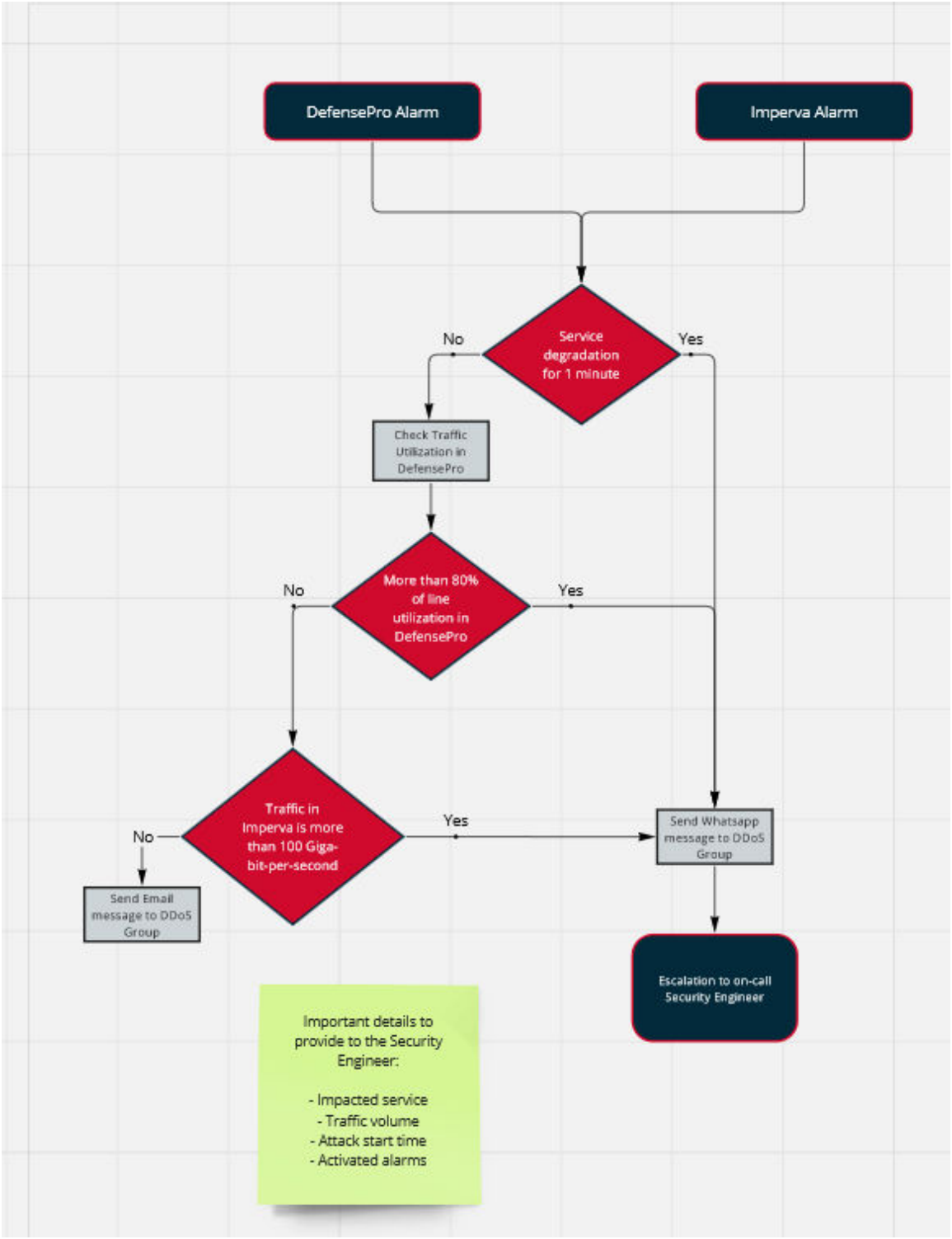
A DDoS playbook describes how your organization should respond to a DDoS attack. The reasoning behind preparing such a playbook is that it's much better to design your response before an attack, rather than during one.

The DDoS Playbook describes the entire process - from the early signals of a potential attack until its full mitigation. This includes, for example, the initial actions typically taken by the SOC/NOC teams to identify an attack, the alerts to relevant personnel, decision and escalation processes, the procedures for involving additional technical or IT personnel, as well as the roles of the CISO or CIO in case of a severe attack.

The diagram below illustrates an example of the first step of a DDoS procedure flow (part of the full Playbook) for a Red Button customer. It focuses on the initial steps taken by the NOC/SOC engineer.

- The procedure begins with an alarm that arrives from a Radware DefensePro or from Imperva.
- The NOC/SOC engineer checks whether there is any service degradation and, if so, sends a message to a pre-defined DDoS group.
- Next is an escalation to an on-call security engineer. (Note: The sample diagram below ends here, as it only includes the first step of the process.)
- If the SOC/NOC team member does not identify a service degradation, then they must check traffic utilization in DefensePro. If utilization is 80% or above, then escalation would follow since it would still be considered a DDoS attack.

  If utilization is less than 80%, then traffic is checked in Imperva. If traffic is more than 100 Gbps, then the same escalation procedure as above is followed.
- The playbook also defines the details that the SOC/NOC team member should include with the alert (impacted services, traffic volumes, attack start time, etc.).



Creating such a playbook, which is unique to each company, is a time-consuming process. It involves internal discussions with all stakeholders to decide on the most efficient actions to be taken during an attack, in order to prevent every minute of downtime.

The procedures are designed to be simple and clear enough so that action can be taken without any of the stakeholders present (such as on Friday night at 2:00 AM).

DDoS Wargames

Wargames are designed to help your teams practice DDoS mitigation procedures in a realistic setting. We offer two options:

- **Actual wargames**: After conducting several DDoS test simulations, we will execute a 'surprise' DDoS attack aimed at testing how the NOC/SOC teams identify the attack and perform the expected procedures. The wargame can be known to a control management team, but in some cases network and security engineers can be among those tested.
- **Tabletop exercise:** Aimed at management level personnel (IT, CISO, CIO, etc.), our theoretical drill exercise describes different events related to DDoS and provides multiple-choice questions to test how different emergency attack scenarios would be managed.