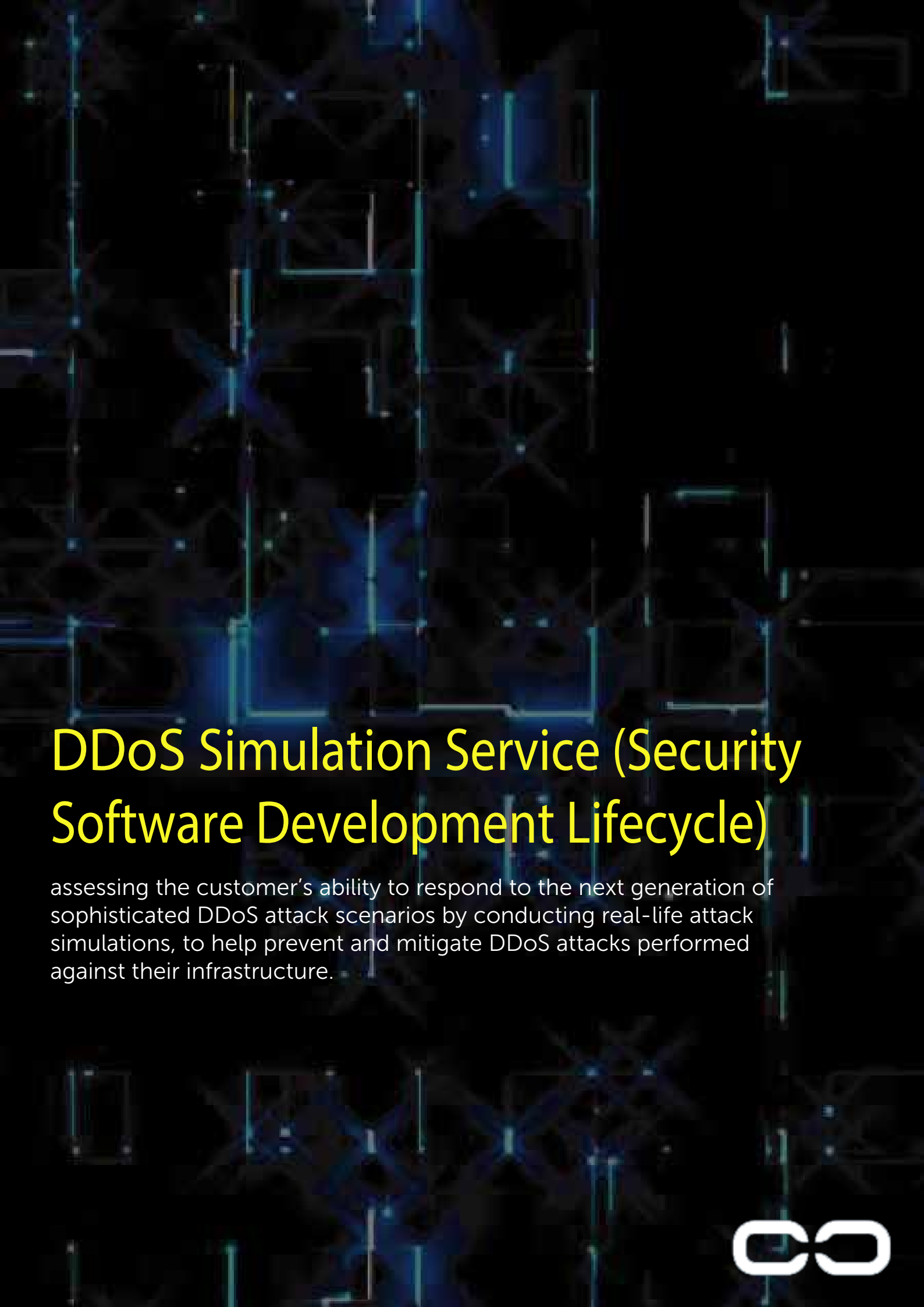

DDoS Simulation Service (Security Software Development Lifecycle)

assessing the customer's ability to respond to the next generation of sophisticated DDoS attack scenarios by conducting real-life attack simulations, to help prevent and mitigate DDoS attacks performed against their infrastructure.

DDoS
Simulation Service (Security Software Development Lifecycle)

What is DDos?

Nowadays, organizations are facing multiple kinds of attacks, as DDoS attack is aiming to disrupt the normal traffic sent to one or more of the organization's resources to make an impact on its availability. The most common security solutions are then deployed over the network to prevent those attacks but the organization doesn't know exactly what tomorrow brings. Therefore, some of the configurations may be partial, or wrong for the organization to use. In some cases the organization lacks of crucial protections against different DDoS attacks. And this is where we get into the picture.

Comsec's unique DDoS simulation service assess the customer's ability to respond to the next generation of sophisticated DDoS attack scenarios by conducting real-life attack simulations, to help prevent and mitigate DDoS attacks performed against their infrastructure.

Over the past seven years Comsec has performed hundreds of successful, fully controlled DDoS simulations adding "Real-Life" hands on experience to each attack scenario.

Prior to the simulation, the Comsec DDoS attack team conducts extensive research of the customer's websites and infrastructure in order to collect valuable intelligence information. Based on the information gathered, Comsec's attack team creates different attack scenarios aimed to simulate real-world DDoS attacks. A simulation is then comprised of several scenarios executed according to the customer's needs.

Attack Types

Each scenario can be divided into two different groups:
Network (Infrastructure) level attacks – attacks targeting the network's components such as firewalls, routers, and load balancers. The effects of these attacks effectively disable physical access to the targeted servers. The attacks can affect the component's CPU, memory and/or bandwidth usage by targeting all layers except for layer 7 in the OSI 7 layers model.
Application level attacks – attacks targeting the server's resources by abusing the application's functions that consume physical resources (such as CPU, memory, bandwidth usage and hard disk usage). These attacks target layer 7 in the OSI 7 layers model.

Attack Scenarios

Each of the described scenarios targets one or more of the following resources:
Bandwidth: The attacker floods the server with requests from numerous bots and thus, consumes network access to the target servers. The flood can either be generic (such as TCP flood) or an application level attack which is customized to the client's website. As a result of this attack, the network bandwidth is consumed (either upstream or downstream bandwidth) and legitimate users cannot access the attacked servers.
Memory (volatile): The attack depletes the available memory of the attacked servers by abusing sensitive memory consuming functions in the attacked application. An example of such an attack is slow HTTP post, which causes the server to allocate a significant amount of memory.

CPU: CPU exhaustion can be caused by flooding the system with high level computations and may affect network components, servers and the application itself. An example of such an attack is SSL exhaustion, which results in high CPU consumption. It should be noted that most of these attacks are client-specific and target a specific functionality of the client's website (such as, but not limited to, flooding calculating modules, search modules and login mechanisms).
Storage: Many applications use databases that contain customer records, business transactions, system information (such as logs) and even uploaded files. An attacker can generate requests that consume the available disk space (for example abusing the registration mechanism), thereby disabling the application.
Connection Table: Each network component contains a connection table which lists existing connections and their status. In this kind of attack, the attacker open numerous connections (either valid or invalid connections), thus flooding the connection table. Once the connection table is full, the server is unable to process new connections resulting in a denial of service attack.