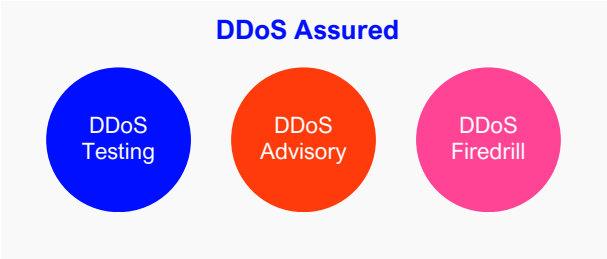
Distributed Denial of Service (DDoS) Assured

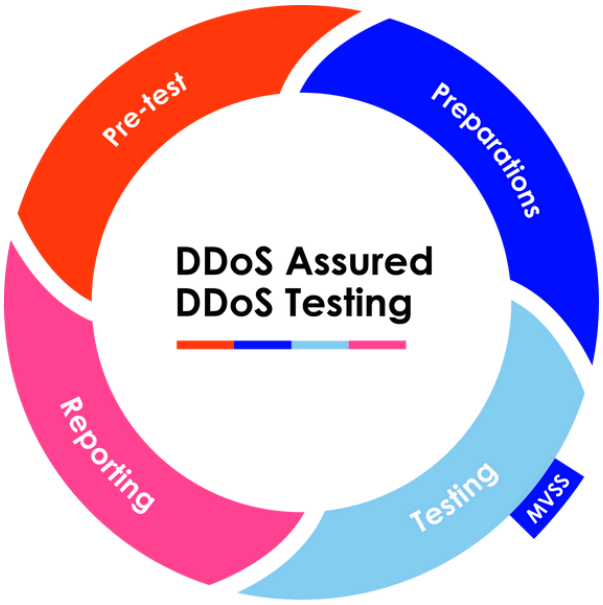
Many organisations have attempted to address the increased threat of a Distributed Denial of Service (DDoS) attack by putting mitigation services in place. However, will they work should the threat of a DDoS attack become a reality?

NCC Groups DDOS service is a fully managed ongoing service designed to monitor your external perimeter to identify changes, which may have occurred without your authorisation, potentially creating security flaws/vulnerabilities in your external infrastructure.



DDoS Testing

Our DDoS Testing service has the ability to emulate a real attack in a secure, controlled manner and test all aspects of an organisation's ability to detect and respond to an attack.



Features

- Consultant led, with a high degree of control means that the test can start 'slow and low' and build up to enormous request volumes.
- The service is operated from our central Managed Security Services facilities and is fully monitored during active use 24 hours a day.
- The service has been meticulously designed to fail safe and has several independent 'kill switches' to stop any simulation quickly should it become necessary.
- The service is highly flexible and extensible to suit a wide range of customer circumstances from reputationally sensitive brochureware sites to full e-business applications.
- As well as testing that bad traffic is filtered, our web performance tools run alongside the test to check that real user traffic remains unaffected during an attack. This is critical in measuring the effectiveness of any mitigation service or appliance.
- Simulation runs are followed up with a concise report detailing what types and volumes of sessions/traffic were generated and (where deployed) what stress levels were experienced throughout the test run.

Key facts and benefits

- DDoS attacks can bring all communication to and from their target(s) to a grinding halt.
- Being prepared for a DDoS attack is key.
- DDoS attacks continue to be a dominant threat.
- From our own testing we have found that 70% of tests fail due to ineffective mitigation.
- A study of IT managers found that it takes an average of ten hours before a company can even begin to resolve a DDoS attack.
- Our DDoS testing services are delivered in a controlled environment to provide you with the peace of mind you need.

DDoS Advisory

Our DDoS Advisory service will guide you through your DDoS defence strategy and provide a full readiness review to get you prepared.

Features

- Review of your DDoS response plan. Our consultants work with you to examine and critically assess the management and technical response procedures against a framework we have developed as we have seen these attacks grow over the years. This provides assurance that a DDoS attack would be rapidly identified, and the mitigation procedures are appropriate and can be aligned to other compliance requirements, if desired, such as ISO27001 to show a formal methodology.
- A readiness exercise to test your response plan. These can range from tabletop exercises conducted on premises through to simulated botnet attacks at a time of your choosing – developed by our in-house team with fail safe mechanisms that automatically cancel the exercise if necessary.
- Assessment of reputation management processes to contain and manage the spread of bad PR and social media exposure.
- Advice on your DDoS defence strategy with intelligence around emerging threat profiles, protocols, volumes of attacks and likelihood of coming under attack.

DDoS Fire Drill

While DDoS Testing emulates a real attack in a secure and controlled situation, DDoS Fire Drill gives you the assurance that your defence thresholds would withstand a DDoS attack as you have planned. DDoS Fire Drill gives you the ability to evaluate the resilience of your people, processes and procedures in this scenario.

Features

- We simulate the trigger levels and alerts of your mitigation in a controlled manner.
- The responses of your people and policies are monitored in terms of their effectiveness in dealing with the alerts.
- The test shows your teams capabilities in following the policies they must apply in the event of your mitigation alerts being triggered.
- It helps you understand and analyse the effects of any mitigation applied to incoming DDoS traffic.

The unpredictable nature of DDoS attacks means that simply implementing mitigation methods isn't enough. If in the event of an attack your staff don't do what they are meant to; the subsequent impact could be worse.

Don't wait till your attacked to fully understand how your people, processes and technologies will react

Questions to ask yourself:

- Does your mitigation provide you with the right coverage?
- Have you got the right people, polices and processes in place?
- Will your mitigation stand up in the face of a real DDoS attack?

Did you know?

- 70% of your controlled DDoS tests overcome their targets due to ineffective mitigation solutions.

About NCC Group

NCC Group is a full-spectrum cyber security specialist delivering the expertise and solutions to research and mitigate threats and vulnerabilities and secure citizen services from initial design right through to day-to-day operation.

In the UK, the nation's digital infrastructure and public services are now central to how citizens live, work, learn and play. They are also core to the UK's national security and international success. Which is why we've made it our mission to create a safer, more resilient United Kingdom.

NCC Group partners with public sector organisations to help develop resilient digital solutions where security is an enabler, not a barrier.

We'll help you turn your strategy into real-world services that balance high-trust, proven security measures with intuitive ease of use for citizens. We'll support you with world-class experts who will test and refine your security, systems and infrastructure against both existing and emerging threats.

Ultimately, we provide continuous assurance that the systems, services and infrastructure the country relies upon, are resilient in the face of today's sophisticated cyber security threats. Whether it's national security programmes, digital transformation initiatives or the delivery of local services, we help secure the UK's citizens in the digital world.

NCC Group's Unmatched Capabilities in Public Sector Protection

NCC Group has a number of distinct advantages in the public sector market.

We understand public sector objectives and the challenges in accomplishing them — so we can tailor our solutions to help customers make tangible real-world progress towards their most important outcomes.

We have both depth and breadth of technical capability — from managed detection and response to threat intelligence and cloud services, we NCC Group has a number of distinct advantages in the public sector market.

We understand public sector objectives and the challenges in accomplishing them — so we can tailor our solutions to help customers make tangible real-world progress towards their most important outcomes.

We have both depth and breadth of technical capability — from managed detection and response to threat intelligence and cloud services, we

For more information from NCC Group on our G-Cloud 15 service, please contact:

+44 (0)161 209 5200

bidteam@nccgroup.com