DDoS Mitigation Advisory

The Distributed Denial of Service (DDoS) Mitigation Advisory provides guidance to organisations on how to prepare for, identify, contain and mitigate DDoS attacks whilst minimising impact to business operations.

The Advisory is structured around the Govern, Identify, Protect, Detect, Respond and Recover (GIPDRR) functions from the National Institute of Standards and Technology's Cybersecurity Framework (CSF) 2.0.

Best Practices

Govern

- Establish organisational policies that outline the security goals
- Establish a DDoS Incident Response Plan to facilitate smoother execution of DDoS response

Identify

- Identify critical assets and services of the organisation that are exposed to public internet

Protect

- Design for resiliency and conduct DDoS sustainability tests
- Maintain good cyber hygiene and be familiar with the Response Plan
- Engage DDoS Protection Service Providers

Detect

- Monitor for early warnings for DDoS attacks for prompt response and minimal disruption
- Determine the nature and scope of the DDoS attack and communicate details to the right teams

Respond

- Execute DDoS Incident Response Plan and other mitigation measures to minimise the impact of the DDoS attack and reduce service disruption

Recover

- Perform restoration activities to resume normal operations
- Review and incorporate lessons learned into DDoS Response Plan

For more information, visit www.csa.gov.sg

Follow us on:

CSA SINGAPORE
Cyber Security Agency of Singapore