iCyber-Security
SAFEGUARDING YOUR DIGITAL WORLD

# Case Study
## Government Institution

# F5 ASM Web Application Firewall Policy Tuning To Protect Government ePortal

## Company Summary

This government institution provides a range of online services to the general public via a secure government e-portal.

## Requirement

Our client had a requirement to protect an online portal against web-based Advanced Persistent Threats (APTs) and DDoS. F5 Networks was selected to deliver the Web Application Firewall (WAF) functionality. The main task was to tune the existing F5 ASM policies and ensure that the configuration was robust and optimized to protect the e-portal against web based attacks. Be-spoke training was also required by the application security team.

## Solution

iCyber-Security was selected for this project because of our combined expertise in network and application security having helped several clients deploy and optimize their F5 ASM policies to protect sensitive data against APTs. The ASM policy was tuned following OWASP recommended top 10 best practices and a strong combination of F5 ASM negative and positive security. By enabling features such as L7 DDoS and Data Guard protection, our client was able to protect the portal against sensitive data leakage.

## Business Benefits

- Increase application defence against L7 DDos and APTs
- Leveraging the F5 platform to strengthen apps security
- Increased e-portal availability by stopping DDoS attacks

## Key Challenges

- F5 ASM policy review
- F5 ASM policy tuning to optimize web application security and effectively defending against APTs
- Be-spoke training and knowledge transfer

## iCyber-Security Delivery

- Delivered F5 ASM policy review and tuning in line with OWASP Top 10 threats
- Delivered be-spoke training and knowledge transfer to the application security team
- Provided advise and recommendations on best practice for on-going F5 ASM policy management