The Institute of Singapore Chartered Accountant (ISCA) would like to invite vendors to submit quotation for ISCA's Web Application Firewall (WAF).

1. WAF Requirements

- **Cloud base Web Application Firewall**
- **Website security**
  1. The underlying technology of the integrated WAF must be based upon and/or built upon proven WAF technology that is a Leader in the Magic Quadrant for WAFs.
  2. The technology of the WAF must not be based upon opensource WAF technology
  3. The integrated WAF solution must be PCI-DSS certified.
  4. The solution must provide real time visibility across all website security incidents detected.
  5. The solution must support the capability to provide complete incident reporting and also able to drill down to a detailed level on a per-incident basis.
  6. The solution must support SIEM integration and also come with pre-built dashboards.
  7. The solution must be able to provide protection against OWASP Top 10 vulnerabilities.
  8. The solution must support custom security rule creation via an user-friendly GUI rule builder for responding to zero day or other new vulnerabilities.
  9. The solution must be able to restrict/block access via whitelisting and blacklisting of the following parameters:
     - - Country
     - - URLS accessed
     - - IP addresses
  10. The WAF solution must have an "Application Awareness" capability which automatically detects the application stack of the website and applies pre-defined templates both to apply specific mitigation rules and to apply exceptions that will eliminate the need for fine tuning.
  11. The solution must provide real-time notifications via email when threats are detected on the protected web application.
  12. *Bot Protection*
      - The solution must be capable of protecting against bots performing (but not limited to) the following actions:
        - - Site Scraping
        - - Vulnerability scanning
        - - Comment spamming
      - The solution must be capable of performing bots whitelisting and blacklisting.
      - The solution must be able to issue CAPTCHA challenge without any change to the web application.
      - The solution must be capable of restricting even good bots from accessing the web site.

13. *Backdoor Protection*
    - The solution must be capable of detecting and blocking backdoor code that is installed on the web application.

- **DDOS protection**

1. The solution must have Points of Presence (POPs) datacenter globally. Preferably, each and every of the POPs must be able to perform ALL of the following functions:
   - DDoS scrubbing
   - WAF
   - CDN
   - Load balancing and failover capability

2. *Website DDoS Protection:*
   - The solution must provide an always-on Layer 7 protection against application layer DDoS attacks.
   - The solution must provide an always-on Layer 3 and Layer 4 protection against volumetric DDoS attacks.

3. *Network/Infrastructure DDoS Protection:*
   - The solution must be capable of protecting against direct-to-origin server DDoS attacks by providing the availability of Infrastructure/BGP protection for Class C IP ranges. I.e. protecting an entire Class C subnet
   - The solution must be capable of protecting against direct-to-origin server DDoS attacks by providing the availability of Infrastructure/BGP protection for a single IP address. I.e. protecting a single IP address.

- **Content Delivery Network (CDN)**

1. Caching
   - The solution must be able to cache static content according to web server response headers.
   - The solution must be able to perform automatic profiling of applications to determine cacheable content. This is to automatically determine which dynamic content can be cached.
   - The solution must provide the capability to instantly purge the cache for the entire page or discrete elements.
   - The solution must provide API access to CDN for purging and making policy changes.

2. Content Optimization
   - The solution must provide the capability to perform image compression
   - The solution must provide the capability to perform content minification
   - The solution must provide the capability for session reuse optimization, TCP optimization and TCP session pre-pooling

- **Load Balancing and Availability**
  1. The solution must support failover and global load balancing for the following setup:
     - Single origin server
     - Multiple origin servers in a single Datacenter
  2. The solution must support application layer load balancing based on HTTP request monitoring.
  3. The solution must support real time health monitoring, per URL, with expected response thresholds.
  4. The solution must support global server load balancing using advanced application layer algorithms such as:
     - Least Pending Requests
     - Least Open Connections
     - Source IP Hash
     - Random"

2. Scope of work

- **Purchase of ISCA WAF system**
  1. Cloud Web Application Firewall
  2. Licensed No: 5 websites

- **Professional services**
  1. Analysis of ISCA websites. (Hosted on Cloud / datacentre)
  2. Configuration of WAF to protect ISCA websites
  3. Testing/Monitoring WAF to work smoothly
  4. WAF administrator training

3. Quotation Breakdown

Please provide a breakdown of the cost for required license costs and professional services including but not limited to the following:

1. 1-year WAF Licensing for protect up to 5 websites.
2. Professional Services

4. Quotation Validity

Quotations submitted must be valid for 2 months from the date of opening of ITQ.

5. Disclaimers

ISCA shall be under no obligation to accept the quotation with the lowest quote or enter into correspondence with any vendor regarding the reason for non-acceptance of quotation.

ISCA reserves the right, unless the vendor expressly stipulates to the contrary in its quotation, to accept only such portion(s) of a quotation as ISCA may in its sole discretion decide and the quotation shall be adjusted accordingly.

6. Enquiries

For any enquiry or submission, please email to **ict.tenders@isca.org.sg** with the subject "*ICT-12-2020*" before the closing date.
Closing date: 25 September 2020, 5pm