REQUEST FOR EXPRESSION OF INTEREST (EOI)

**Subject: Security Intelligence Platform**

Date of this EOI: 04 July 2016

Closing date of this EOI: 18 July 2016

Reference Number: EOI 120948

Address EOI for the attention of: Mr. Kent Foster

Fax no.: +31 70 515 8336

E-mail address: [kent.foster@icc-cpi.int](mailto:kent.foster@icc-cpi.int)

It is anticipated that the International Criminal Court (ICC) located in The Hague, The Netherlands, will shortly be issuing a solicitation for the provision of a Security Intelligence Platform. In this connection, the ICC is requesting expression of interest from qualified firms.

**Description**

Security Intelligence Platform

Summary of needs:

The customer seeks to develop an in-house capability to rapidly detect and respond to emerging cyber-threats it faces. The capability sought includes facilitating the customer’s centralised collection, correlation, analysis and assessment of security information from network security devices, user-access endpoints and application and data hosts on an Internet connected network.

The customer’s aspiration is towards “more than just a SIEM”, with functionality to actively and rapidly identify potential threats and threat-like behaviour and establish a basis from which mitigation and incident response may be conducted.

The capability should permit the rapid and automated detection of potentially suspicious activity on the network and at its perimeter, and may also include the detection of potentially abnormal user and other entity activity on endpoints, devices, networks and interfaces.

The capability should facilitate the provision of alerts to a human operator of identified threats and behaviours that are “scored” in a manner to help prioritise important events and activities. Alerting should include a minimum of a dashboard, and may include alerts transmitted to other systems.

The capability should permit a human operator to easily gather information related to a potential incident (case-building), as well as permit a detailed (forensic) analysis to be quickly performed on related data. The capability should also include traditional compliance and analytical reporting features.

The capability may allow for semi—automated remediation actions to be initiated (such as instructing an account to be locked, an IP address to be blocked, an item of software to be blacklisted, etc.). This remediation feature may include an approval workflow.

The capability should allow for security data to be received or gathered (agentless /agent) from multiple sources across a local area network (multiple VLANs), and should be scalable to accommodate various ranges of events per second without major system change.

The capability should be based upon on-premises technologies as far as possible due to customer concerns about confidentiality, and should allow for on-premises storage (online, near-online and archive).

The capability should be supported by appropriate training for the customer’s staff.

The customer operates a single site in The Netherlands and utilises traditional networking and security equipment including Cisco, FortiGate, etc. The customer has around 400 virtualised servers and around 1500 Windows clients. The anticipated security traffic is estimated to be in the area of 400 mps.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Interested firms/organizations should forward their Expression of Interest by facsimile or e-mail to the attention of Kent Foster at fax no. +31 70 515 8336 or by e-mail [kent.foster@icc-cpi.int](mailto:kent.foster@icc-cpi.int) Please use the attached form.

Interested firms/organizations registered with the UN Global Marketplace, please indicate your vendor registration number. Please be advised that this Request for EOI does not constitute a solicitation. It should also be noted that the ICC reserves the right to change or cancel this requirement at any time.

**EXPRESSION OF INTEREST**

**ICC EOI 120948**

**Subject: Security Intelligence Platform**

1. Company information:
2. Company’s name: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Address & Website (address responding to this EOI): \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Telephone:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Fax: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. E-mail: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Company contact - as main point of contact for all further tender correspondence: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
4. UNGM Vendor Registration No.: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Note: It is not mandatory to register with the UNGM ([http://www.ungm.org](http://www.ungm.org/)). Contracts can be awarded to non-registered suppliers. The full RFP documents can be provided to you per e-mail, even without a UNGM vendor registration number. However, by registering on the UNGM your company details will be entered in the database the UN buyers use when searching for suppliers.