**Request for Information (RFI) to identify   
Security Information and Event Management (SIEM) Vendors**

**Background**

The Information and Communications Technology Services (ICT) of the Organization for Security and Cooperation in Europe (OSCE) provides various ICT services on different infrastructure and systems products both at the Secretariat and field level (please refer to [www.osce.org/where-we-are](http://www.osce.org/where-we-are) to learn about the OSCE presence in various countries).

A “Security Information and Event Management” (SIEM) solution shall be implemented to centralize the log data storage and analysis in a Security Operations Centre (SOC).

1. **Purpose of RFI**

This RFI shall provide the OSCE with information to:

* Identify potential qualified Vendors for the subsequent competitive tender;
* Enhance the Terms of Reference (ToR) for the competitive tender;
* Identify the available capabilities and any obstacles/limitations;
* Structure the tender to lower operational cost.

1. **Scope of Solution**

The ICT is seeking qualified Vendors capable of implementing a SIEM solution with the following capabilities:

**Log Data Collection (Sensors):**

* Collect log data from various sources (detailed in Annex I) in multiple locations;
* Safe transport to centralized storage (buffering);
* Data processing options (filtering, aggregation, enrichment);
* Deployment options and management;
* Perform security scans or process security scan information (vulnerabilities).

**Log Data Storage (Logger):**

* Tamper-proof long term storage (digitally sign data, compression);
* Search (including full text/field based index capabilities and search options);
* Compliance certifications of data storage.

**Log Data Analyses (Server):**

* Centralized management of the SIEM solution;
* User Interface customizable for different tenants (support of multi-tenancy) ranging from public performance screen to Security Operations Centre (SOC);
* Classification/Taxonomy;
* Threat Intelligence;
* Correlation;
* Data enrichment;
* Asset Behaviour Analytics, Anomaly Detection;
* Performance Indicators processing.

**Sizing:**

* Estimated average log volume 40 GB/day;
* Estimated average event generation 1500 events/second (EPS).

The Vendor shall propose an architecture and deployment options for its selected SIEM solution including licensing model, product support, performance estimation, scalability and High Availability/Disaster Recovery (HA/DR) options.

*The above mentioned structure is just an example and the Vendor shall provide the best suited architecture/setup for its chosen product.*

***The OSCE’s preference will be given to the Vendor providing the most capable product and best suited implementation/services in terms of price/performance.***

***As outcome of the competitive tender process which might follow this RFI, the OSCE wants to award the Contract to a single Vendor.***

***Subcontractors may be appointed by the Vendor (Product Vendor Support).***

1. **List of Activities under the planned Contract**

The appointed Vendor will be requested to provide the following activities to fulfil the requirements listed under the Scope of Services:

* Design of the SIEM solution;
* Implementation of the SIEM product and log collection;
* Customization of data sources, analyses and SOC;
* Knowledge Transfer;
* SOC support options:   
  - Managed Security Services Provider (MSSP);  
  - Co-Managed SOC On-Site;  
  - Training and support of local SOC team.

1. **Place of Performance and Delivery Method**

Provide services on-site at the OSCE Secretariat premises in Vienna, Austria. An on-site delivery model is preferred, remote assistance is possible, if required for the service.

1. **Vendor Qualification**

Interested Vendors are required to have a suitable Partner status with their chosen Product Vendor at the stage of responding to this Procurement Notice as well as during the duration of the Contract.

**Certification**

It is expected that at least one member of the Vendor's Key Personnel assigned to perform for the OSCE shall hold a valid certificate of the Product Vendor at any time during their assignment to the OSCE and have a minimum of 3 years of professional experience in SIEM implementations. Additional certifications and experience in Information Security are highly appreciated for Key Personnel.

1. **Expected Contract Duration**

The OSCE intends to enter into a Contract with a qualified Vendor for the performance of the implementation. The support Contract will be for a period of 1 year and will be subject to annual renewals subject to the need of service, funds availability and Contractor’s performance (maximum Contract duration period at the OSCE is 5 years).

1. **Requested Information**

Interested Vendors are requested to provide the following information as part of their RFI response:

1. General company information (maximum 1 page), including a statement attesting that the Vendor has the capabilities, qualifications, and financial and human resources to cover the Scope of Service and perform services listed under the List of Activities;
2. Response to the Annex I – RFI Questionnaire;
3. Reference information which would prove that the Vendor has experience providing requested services to other clients.
4. **Communication**

The OSCE requires all communication, documentation, software, training, and support to be in the English language.

1. **Request for Information Procedure**

Please note that this is not an invitation for submission of a bid or proposal. This Request for Information (RFI) intends identifying interested and capable Vendors to provide services as stated above.

Interested Vendors should respond in writing to the points 1 – 3 listed under the Chapter 8 – Requested Information. Please address your response by email to Mr. Yury GOLOVKOV, Associate Procurement Officer at [yury.golovkov@osce.org](mailto:yury.golovkov@osce.org) by 12 October 2018 at 17:00HRS CET.

Please note that there is no specific format designed to provide your response to this RFI; however, please use Annex I – RFI Questioner as a template providing your clarifications.

Should you have any questions concerning this RFI, please address them in writing to the above mentioned email address.

**END.**

**Annex I – RFI Questionnaire**

*Question no. 1 – Please specify the selected SIEM solution and included products*

Answer no. 1 – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Question no. 2 – Which type of partnership does your company have with the SIEM solution Vendor?*

Answer no. 2 – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Question no. 3 – Please specify quantity, certificates and SIEM/Information Technology experience of available staff according to their role (implementer, support, analyst).*

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Role(s)** | **Certificates** | **Experience** |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

*Question no. 4 – Please describe the components of the SIEM Solution (sensor, logger, server) with deployment options (virtual or hardware appliances, software including supported operating systems, cloud or other) and capabilities (according to Scope of Solution).*

|  |  |  |  |
| --- | --- | --- | --- |
| **No.** | **Product Component** | **Deployment** | **Capabilities** |
| 1. |  |  |  |
| 2. |  |  |  |
| 3. |  |  |  |
| 4. |  |  |  |
| 5. |  |  |  |
| 6. |  |  |  |
| 7. |  |  |  |

*Question no. 5 – Please describe the license model (depending on component, if necessary)*

Answer no. 5 – \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

*Question no. 6 – Please confirm which technologies/products/collection methods from the below table are supported by the SIEM solution and comment on the alternative collection methods, normalization/rule support and customization options.*

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Product** | **Yes** | **No** | **Comments** |
| 1. | Forwarded pre-processed Events (Syslog) **Microsoft:** Windows Server 2008 R2 – 2016 Active Directory Network Policy Server ADFS Key Management Service Windows Firewall Identity Manager Group Policy Management SCCM SCOM Privileged Access Management Advanced Threat Analytics |  |  |  |
| 3 | Forwarded pre-processed Events (Syslog) **VMWare** vSphere vCenter Site Recovery Manager vRealize Operations Manager NSX AirWatch |  |  |  |
| 2. | Forwarded pre-processed Events (Syslog) **MicroFocus:** Access Manager Identity Manager |  |  |  |
| 4. | Check Point Firewall Management - Syslog collector - OPSEC LEA - SHA254 support for certificate |  |  |  |
| 5. | Databases - MS SQL Audit Logs - Oracle Audit Logs - Custom Application Logs |  |  |  |
| 6. | Windows Event Forwarded Logs from Windows 7-10 - RPC (Event Log Reader Permission) |  |  |  |
| 7. | Linux OS Syslog Messages - SuSe Linux Enterprise Server - RedHat Linux |  |  |  |
| 8. | IDS Events |  |  |  |
| 9. | Netflow Data |  |  |  |
| 10. | CISCO Network Device Logs |  |  |  |
| 11. | Mail Proxy: postfix |  |  |  |
| 12. | Web Proxy: squid |  |  |  |
| 13 | Vulnerability Scanner data |  |  |  |
| 14. | Baramundi Management Suite |  |  |  |
| 15. | Microsoft Exchange |  |  |  |
| 16. | Microsoft Sharepoint |  |  |  |
| 17. | Skype for Business |  |  |  |
| 18. | **McAfee:** ePolicy Orchestrator McAfee Agent McAfee Endpoint Protection Virus scan Enterprise McAfee protection for SharePoint |  |  |  |
| 19. | **Kaspersky:** Security for Exchange EndPoint SecuritySecurity Center |  |  |  |
| 20. | RSA ACE |  |  |  |
| 21. | **Cloud Services** Microsoft Azure Active Directory Microsoft Office 365 |  |  |  |

*Question no. 7 – Please describe the analysis features of the SIEM available for a SOC (according to Scope of Solution)*

|  |  |  |
| --- | --- | --- |
| **No.** | **Feature** | **Description** |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |
| 4. |  |  |
| 5. |  |  |
| 6. |  |  |
| 7. |  |  |
| 8. |  |  |
| 9. |  |  |
| 10. |  |  |

*Question no. 8 – Please describe available Services to support a SOC (*MSSP, Co-Managed, Training and support or other)

|  |  |  |
| --- | --- | --- |
| **No.** | **Service/Support Model** | **Description** |
| 1. |  |  |
| 2. |  |  |
| 3. |  |  |