This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/007512-2023

Planning

SIEM / SOAR / TIP Technologies (Global)

NATIONAL GRID UK LIMITED

F04: Periodic indicative notice – utilities
Periodic indicative notice only
Notice identifier: 2023/S 000-007512
Procurement identifier (OCID): ocds-h6vhtk-03b2ff
Published 15 March 2023, 11:46am

Section I: Contracting entity

I.1) Name and addresses

NATIONAL GRID UK LIMITED

Grand Buildings,1-3 Strand

LONDON

WC2N5EH

Contact

Cora Russell

Email

cora.russell@nationgrid.com

Country

United Kingdom

Region code

UK - United Kingdom

Companies House

04508773

Internet address(es)

Main address

www.nationalgrid.com

I.3) Communication

Additional information can be obtained from the above-mentioned address

I.6) Main activity

Electricity

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

SIEM / SOAR / TIP Technologies (Global)

II.1.2) Main CPV code

- 48730000 - Security software package

II.1.3) Type of contract

Supplies

II.1.4) Short description

National Grid's Security Team is seeking to select a strategic partner to provide one or all of the below capabilities:

• SIEM (Security Information and Event Management)

• SOAR (Security Orchestration, Automation, and Response)

• TIP (Threat Intelligence Platform)

National Grid welcomes interested parties who lead in the above-listed areas to register their interest regarding this tender opportunity.

Please note that this tender will consist of 3 lots. Suppliers may choose to bid for any number of lots.

II.1.5) Estimated total value

Value excluding VAT: £15,000,000

II.1.6) Information about lots

This contract is divided into lots: Yes

Maximum number of lots that may be awarded to one tenderer: 3

The contracting authority reserves the right to award contracts combining the following lots or groups of lots:

The full and final scope of each lot has yet to be fully approved but a high-level scope has been provided to help you determine if you have the capabilities

II.2) Description

II.2.1) Title

SIEM (Security Information and Event Management)Technology

Lot No

1

II.2.2) Additional CPV code(s)

- 48730000 - Security software package

II.2.3) Place of performance

NUTS codes

- UK - United Kingdom
- US - United States

II.2.4) Description of the procurement

National Grid security team operates a 24*7*365 Cyber Security Operation Centre (CSOC) that monitors our estate for malicious, suspicious, or anomalous behavior and responds appropriately to ensure the consistency of services National Grid provides. SIEM / SOAR / TIP technologies are the cornerstone of an effective Security Operations organization. The successful solution will demonstrate the below:

SIEM

• Comprehensive log collection - The SIEM solution should be able to collect logs from all relevant sources. This includes servers, databases, network devices, end user devices, and applications.

• Alerting and Reporting - The SIEM solution should provide a catalog of alerts and reports out of the box that can be modified and tuned to meet the needs of National Gird.

• Advanced Analytics - The SIEM solution should have advanced analytic capabilities such as behavioral analytics (UEBA) and machine learning to detect anomalous activity and potential threats.

• Real-time (or near real-time) monitoring - The SIEM solution should be able to provide real-time monitoring to ensure security events are detected quickly.

• Integration - The SIEM solution should integrate with other industry-standard security tools to provide a complete view of the internal security landscape.

• Scalability - The solution should be able to scale up and down as required by the organizational needs of National Grid.

• Support - National Grid should have access to a 24/7/365 vendor support team to assist with any service issues. Vendor-provided training and certification should be available to all applicable National Grid staff.

• Usability - The solution should be user-friendly and initiative to configure and manage. It should allow teams to easily drill down into specific data points for more detailed analysis.

II.2.14) Additional information

Technical & Delivery Considerations

Due to the strictly regulated industries National Grid operate in, we have a strong preference towards vendors who can provide a hybrid architecture whereby infrastructure is split between on-premise and cloud.

The required solution will integrate with internal IT infrastructure and external vendors of National Grid. Vendors will be expected to demonstrate how they can effectively integrate with other tooling in the environment.

In addition to the software and hosting service, we will be looking for a robust plan around the operations support models available.

II.2) Description

II.2.1) Title

SOAR (Security Orchestration, Automation and Response)Technology

Lot No

2

II.2.2) Additional CPV code(s)

- 48730000 - Security software package

II.2.3) Place of performance

NUTS codes

- UK - United Kingdom
- US - United States

II.2.4) Description of the procurement

National Grid security team operates a 24*7*365 Cyber Security Operation Centre (CSOC) that monitors our estate for malicious, suspicious, or anomalous behavior and responds appropriately to ensure the consistency of services National Grid provides. SIEM / SOAR / TIP technologies are the cornerstone of an effective Security Operations organization. The successful solution will demonstrate the below:

SOAR

• Comprehensive integration - The SOAR solution should integrate with the internal and external tooling for automated enrichment and response

• Automation - The SOAR solution should contain a repository of playbooks that can be used to accelerate the adoption of the platform

• Case Management - The SOAR Platform should provide a centralized incident management console that allows for end-to-end incident management.

• Analytics and reporting - The SOAR solution should provide advanced analytics and reporting allowing National Grid to track key metrics, identify trends and gain insights into security operations.

• Scalability - The solution should be able to scale up and down as required by the organizational needs of National Grid.

• Support - National Grid should have access to a 24/7/365 vendor support team to assist with any service issues. Vendor-provided training and certification should be available to all applicable National Grid staff.

• Usability - The solution should be user-friendly and initiative to configure and manage. It should allow teams to easily drill down into specific data points for more detailed analysis.

II.2.14) Additional information

Technical & Delivery Considerations

Due to the strictly regulated industries National Grid operate in, we have a strong preference towards vendors who can provide a hybrid architecture whereby infrastructure is split between on-premise and cloud.

The required solution will integrate with internal IT infrastructure and external vendors of National Grid. Vendors will be expected to demonstrate how they can effectively integrate with other tooling in the environment.

In addition to the software and hosting service, we will be looking for a robust plan around the operations support models available.

II.2) Description

II.2.1) Title

TIP (Threat Intelligence Platform)Technology

Lot No

3

II.2.2) Additional CPV code(s)

- 48730000 - Security software package

II.2.3) Place of performance

NUTS codes

- UK - United Kingdom
- US - United States

II.2.4) Description of the procurement

National Grid security team operates a 24*7*365 Cyber Security Operation Centre (CSOC) that monitors our estate for malicious, suspicious, or anomalous behavior and responds appropriately to ensure the consistency of services National Grid provides. SIEM / SOAR / TIP technologies are the cornerstone of an effective Security Operations organization. The successful solution will demonstrate the below

TIP

• Comprehensive source integrations - The TIP should be able to take threat feeds from a variety of sources including open source and paid threat feeds, internal security tooling, and manual submissions from internal teams.

• Advanced Analytics - The TIP solution should be able to analyse ingested threat data to identify patterns and trends, allowing National Grid to gain insights into the nature of threats targeting the organization.

• Usability - The TIP solution should be user-friendly and initiative to configure and manage.

• Reporting - The TIP solution should provide customizable dashboards and reports that allow users to drill down into specific data points.

• Scalability - The solution should be able to scale up and down as required by the organizational needs of National Grid.

• Support - National Grid should have access to a 24/7/365 vendor support team to assist with any service issues. Vendor-provided training and certification should be available to all applicable National Grid staff.

• Usability - The solution should be user-friendly and initiative to configure and manage. It should allow teams to easily drill down into specific data points for more detailed analysis.

II.2.14) Additional information

Due to the strictly regulated industries National Grid operate in, we have a strong preference towards vendors who can provide a hybrid architecture whereby infrastructure is split between on-premise and cloud.

The required solution will integrate with internal IT infrastructure and external vendors of National Grid. Vendors will be expected to demonstrate how they can effectively integrate with other tooling in the environment.

In addition to the software and hosting service, we will be looking for a robust plan around the operations support models available.

II.3) Estimated date of publication of contract notice

10 April 2023

Section IV. Procedure

IV.1) Description

IV.1.8) Information about the Government Procurement Agreement (GPA)

The procurement is covered by the Government Procurement Agreement: No

IV.2) Administrative information

IV.2.2) Time limit for receipt of expressions of interest

Date

7 April 2023

IV.2.4) Languages in which tenders or requests to participate may be submitted

English

Section VI. Complementary information

VI.3) Additional information

Indicative Tender Timelines

To support the resource and planning of interested parties National Grid has outlined an indicative timetable below.

Please note this is not binding and subject to change.

1. PIN Issued: Wednesday 15th March 2023

2. PIN Closed: Friday 7th April 2023

3. PQQ Issued: Monday 17th April 2023

4. PQQ Closed: Friday 5th May 2023

5. RFP Issued: Monday 15th May 2023

6. RFP Closed: Friday 9th June 2023

7. Contract Award: Friday 15th September 2023

Pre-request to be eligible to participate

In order to participate in this tender, you must be registered on the Achilles UVDB system. UVDB is used to pre-qualify our suppliers to ensure they meet the minimum legal and regulatory requirements in order to contract with National Grid .

UVDB is the utility industry pre-qualification system used by the utilities sector in the UK to manage risk within the supply chain and comply with EU regulations. Joining UVDB as a supplier provides your organisation with an opportunity to showcase your capabilities and access multiple contract opportunities by completing a single pre-qualification questionnaire (PQQ). UVDB is used by many utility buyer organisations.

If you are already registered with UVDB you only need to ensure that you are registered under UVDB code 1.5.8.17 Software - (Safety, Health, Environment, and Security)

If you are not currently registered this can be done by registering at:
https://www.achilles.com/community/uvdb/

You will then need to register under UVDB code 1.5.8.17 Software - (Safety, Health, Environment, and Security)

If you require any further information regarding this registration, please contact:

Samuel Lloyd-Jones (samuel.lloydjones@achilles.com) who can support any issues with completion of your registration process on Achilles ahead of the qualification event commencing in mid April 2023.

Further to the enclosed PIN, please indicate your expression of interest and confirmation of which Lot you would be interested in (please note this is just for information purposes and will not exclude you from any lots in the future) also confirm that you are or will be registering on Achilles UVDB against code 1.5.8.17 Software - (Safety, Health, Environment, and Security).

emailing: cora.russell@nationalgrid.com