This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/012388-2023

Planning

Security Operation Centre

West Yorkshire Combined Authority

F01: Prior information notice
Prior information only
Notice identifier: 2023/S 000-012388
Procurement identifier (OCID): ocds-h6vhtk-03c554
Published 28 April 2023, 4:39pm

Section I: Contracting authority

I.1) Name and addresses

West Yorkshire Combined Authority

Wellington House, 40-50 Wellington Street

Leeds

LS1 2DE

Contact

James Firth

Email

james.firth@westyorks-ca.gov.uk

Country

United Kingdom

Region code

UKE - Yorkshire and the Humber

National registration number

8876556

Internet address(es)

Main address

https://www.westyorks-ca.gov.uk

Buyer's address

https://uk.eu-supply.com/ctm/Company/CompanyInformation/Index/103257

I.3) Communication

The procurement documents are available for unrestricted and full direct access, free of charge, at

https://uk.eu-supply.com/ctm/Supplier/Documents/Folder/66481

Additional information can be obtained from the above-mentioned address

I.4) Type of the contracting authority

Regional or local authority

I.5) Main activity

General public services

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Security Operation Centre

Reference number

62580

II.1.2) Main CPV code

- 72000000 - IT services: consulting, software development, Internet and support

II.1.3) Type of contract

Services

II.1.4) Short description

West Yorkshire Combined Authority would like to procure an external party to implement Microsoft's Sentinel System Incident Event Monitoring (SIEM) tool into its Azure environment. The Combined Authority require security events, that are captured and correlated by the SIEM solution, to be monitored 24/7 using an externally hosted Security Operations Centre (SOC).

The Combined Authority will leverage the security alerts provided by the SOC:

• To understand where the Combined Authority needs to focus its resources to maximise its cybersecurity posture.

• To detect and respond to threats, keeping the information held on systems and networks secure.

• To increase resilience by learning about the changing threat landscape (both malicious and non-malicious, internal and external)

• To identify and address negligent or criminal behaviours.

To derive business intelligence about user behaviours to shape and prioritise the development of technologies.

II.1.5) Estimated total value

Value excluding VAT: £250,000

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.3) Place of performance

NUTS codes

- UKE - Yorkshire and the Humber

Main site or place of performance

Leeds

II.2.4) Description of the procurement

In January 2022, the Combined Authority received several recommendations from the Department Levelling Up, Housing and Communities (DLUHC). A number of these recommendations centred round a central logging solution and the ability to monitor events and act on alerts. Specifically, the following recommendations were stated:

• Identify a suitable solution which is the best fit for the Combined Authority by carrying out an assessment of key log sources, required alerts and cost.

• Upon implementation of a centralised logging solution ensure that log retention is documented and agreed.

• Upon implementation of a centralised logging solution, automated log analysis and correlation functionality and a formal log incident triaging process should then be developed and documented.

The SIEM solution must be able to provide a centralised logging solution which receives logs from all the Combined Authority’s endpoints, network devices and applications. The SIEM will primarily be for security event capture and alerting, not necessarily capturing non security technical events.

The SOC must be able to monitor and respond to the SIEM alerts on a 24/7/365 basis. Alerts which are of sufficient interest must be reported to ICT Services as per the Combined Authority’s ICT incident response process and within agreed Service Level Agreement (SLA) time frames.

The Combined Authority's Target Operating Model has considered both threats and assets. Threat analysis has taken into account the higher level of public awareness the Combined Authority has gained since it has become a Mayoral Authority.

The Threat Actor Sophistication has been assessed using the Stix v2.1 framework. The Combined Authority's threat actor sophistication is expected to range from none to intermediate and potentially advanced, as per the framework.

The Combined Authority faces several threats, typical of many government organisations. These threats range from data loss of sensitive Combined Authority data, ransomware, fraud via social engineering using attack vectors like phishing and smishing, to specific threats to a person of interest, such as politically or criminally motivated hacking attacks against the mayor and / or the Police & Crime Commissioner.

II.3) Estimated date of publication of contract notice

22 May 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: Yes