This is a published notice on the Find a Tender service: https://www.find-tender.service.gov.uk/Notice/023781-2023

Planning

Provision of Security Incident Event Management Tool

Crown Prosecution Service

F01: Prior information notice
Prior information only
Notice identifier: 2023/S 000-023781
Procurement identifier (OCID): ocds-h6vhtk-03efa9
Published 14 August 2023, 4:42pm

Section I: Contracting authority

I.1) Name and addresses

Crown Prosecution Service

102 Petty France

LONDON

SW1H 9EA

Contact

Patience Arinaitwe

Email

patience.arinaitwe@cps.gov.uk

Country

United Kingdom

Region code

UKI3 - Inner London – West

Justification for not providing organisation identifier

Not on any register

Internet address(es)

Main address

https://www.cps.gov.uk

I.3) Communication

Additional information can be obtained from the above-mentioned address

I.4) Type of the contracting authority

Ministry or any other national or federal authority

I.5) Main activity

Other activity

Provision of a Security Incident Event Management Tool

Section II: Object

II.1) Scope of the procurement

II.1.1) Title

Provision of Security Incident Event Management Tool

II.1.2) Main CPV code

- 72250000 - System and support services

II.1.3) Type of contract

Services

II.1.4) Short description

Provision of a Security Incident Event Management Tool:

The Crown Prosecution Service (CPS) is issuing a Prior Information Notice (PIN) to inform prospective suppliers of its intention to procure a Security Information and Event Management (SIEM) tool.

CPS will go to market for a new SIEM system as part of its overall cybersecurity strategy.

II.1.6) Information about lots

This contract is divided into lots: No

II.2) Description

II.2.2) Additional CPV code(s)

- 72250000 - System and support services
  - FB09 - For security system

II.2.3) Place of performance

NUTS codes

- UKI3 - Inner London – West

II.2.4) Description of the procurement

The Crown Prosecution Service (CPS) is issuing a Prior Information Notice (PIN) to inform prospective suppliers of its intention to procure a Security Information and Event Management (SIEM) tool.

CPS will go to market for a new SIEM system as part of its overall cybersecurity strategy.

As a minimum, the tool should provide the following functionality:

1. Log Collection and Aggregation: The SIEM should be capable of collecting and aggregating logs and data from various sources across the CPS, such as network devices, servers, applications, cloud infrastructure, and endpoints/end-user-devices.

2. Integration and Compatibility: The SIEM should integrate seamlessly with existing security tools and technologies, such as intrusion detection/prevention systems (IDS/IPS), firewalls, antivirus solutions, and threat intelligence feeds.

3. Real-time Monitoring: The SIEM should provide real-time monitoring capabilities to detect and alert on suspicious or malicious activities as they occur. This involves continuous analysis of incoming log data to identify anomalies and patterns indicative of security threats.

4. Event Correlation and Analysis: The system should be able to correlate and analyse events from multiple sources to identify complex attack patterns that may go unnoticed when analysing individual events in isolation.

5. Threat Detection and Alerts: The SIEM should have threat detection mechanisms that can identify known threats based on signatures and behaviours, as well as emerging threats using advanced analytics and machine learning techniques. It should generate timely and actionable alerts for security teams.

6. Incident Response: The SIEM should facilitate efficient incident response by providing workflow and case management capabilities. This allows security teams to track, investigate, and remediate security incidents effectively.

7. Automated Remediation: The SIEM should be capable of integrating with network services and infrastructure to automatically mitigate significant threats in real time.

8. Data Retention and Storage: A SIEM system must be capable of storing and managing large volumes of log data over extended periods to support historical analysis, compliance requirements, and forensic investigations. An indicative estimate is 50TB of data over a rolling year.

9. Scalability: The SIEM should be scalable to accommodate growing data volumes and an expanding IT infrastructure. It should be able to handle the increasing demands of log collection, analysis, and storage.

10. User and Entity Behaviour Analytics (UEBA): Advanced SIEM systems incorporate UEBA capabilities to establish baselines of normal behaviour for users and entities. Deviations from these baselines can trigger alerts for potential insider threats or compromised accounts.

11. Compliance and Reporting: The SIEM should assist organisations in meeting regulatory compliance requirements by offering predefined compliance reports and helping to demonstrate adherence to industry standards and regulations.

12. Advanced Analytics and Machine Learning: Employing machine learning and advanced analytics can enhance threat detection by identifying subtle patterns and anomalies that may indicate novel or sophisticated attacks.

At this stage, the CPS is seeking to engage with the supply market as part of an information-gathering exercise to understand how suppliers might approach the provision of the services outline above, particularly with regards to any developments in service delivery and innovation.

Suppliers who wish to express their interest in this potential opportunity should do so via the contact details contained within the notice and shall subsequently be invited to attend a virtual engagement session in which they may present their observations on how the requirements within this Prior Information Notice could be fulfilled.

This presentation may take any format and should cover the following areas:

• the latest developments / capabilities in SIEM technology

• a cost estimation - provide a comprehensive breakdown of potential cost associated with the service provision to the CPS. This should include: setup costs, ongoing service costs, any cost related to customisation, support, or upgrades as well as any other incidental costs that may be incurred during the service.

II.3) Estimated date of publication of contract notice

31 January 2024

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