

This is a published notice on the Find a Tender service: <https://www.find-tender.service.gov.uk/Notice/009392-2023>

Planning

## **Managed Detection and Response**

Satellite Applications Catapult

F01: Prior information notice

Prior information only

Notice identifier: 2023/S 000-009392

Procurement identifier (OCID): ocids-h6vhtk-03b791

Published 31 March 2023, 8:47am

### **Section I: Contracting authority**

#### **I.1) Name and addresses**

Satellite Applications Catapult

Electron Building, Fermi Avenue, Harwell

Didcot

OX11 0QR

#### **Email**

[procurement@sa.catapult.org.uk](mailto:procurement@sa.catapult.org.uk)

#### **Telephone**

+44 1235567977

#### **Country**

United Kingdom

#### **NUTS code**

UK - United Kingdom

**Internet address(es)**

Main address

[www.sa.catapult.org.uk](http://www.sa.catapult.org.uk)

Buyer's address

[https://www.mytenders.co.uk/search/Search\\_AuthProfile.aspx?ID=AA42845](https://www.mytenders.co.uk/search/Search_AuthProfile.aspx?ID=AA42845)

**I.2) Information about joint procurement**

The contract is awarded by a central purchasing body

**I.3) Communication**

Additional information can be obtained from the above-mentioned address

**I.4) Type of the contracting authority**

Other type

RTO

**I.5) Main activity**

Other activity

Space Sector

---

## **Section II: Object**

### **II.1) Scope of the procurement**

#### **II.1.1) Title**

Managed Detection and Response

Reference number

SAC-PIN-24-004

#### **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**

The Satellite Applications Catapult is seeking a reliable and experienced Managed Detection and Response (MDR) service provider to help enhance its cybersecurity defences, by replacing its current provider. The provider will be responsible for monitoring the company's endpoints, detecting, and responding to security incidents, and providing actionable insights to improve the company's overall security posture. The provider must have a deep understanding of the latest cyber threats and the tools and techniques used to prevent and mitigate them.

The scope of work for the MDR service provider will include the following:

Threat Intelligence

Security Monitoring

Incident Response; and

Reporting and Analytics

See more about each of these headings in the description of the procurement section.

#### **II.1.6) Information about lots**

This contract is divided into lots: No

## **II.2) Description**

### **II.2.2) Additional CPV code(s)**

- 72246000 - Systems consultancy services
- 72222300 - Information technology services
- 72250000 - System and support services
- 72253200 - Systems support services
- 72510000 - Computer-related management services
- 72511000 - Network management software services
- 72610000 - Computer support services
- 72700000 - Computer network services
- 72910000 - Computer back-up services
- 72590000 - Computer-related professional services
- 72600000 - Computer support and consultancy services

### **II.2.3) Place of performance**

NUTS codes

- UKJ1 - Berkshire, Buckinghamshire and Oxfordshire

Main site or place of performance

Harwell

### **II.2.4) Description of the procurement**

Threat Intelligence: Responsible for collecting, analysing, and sharing threat intelligence with the company. This includes identifying and analysing threats in real-time, providing recommendations on how to mitigate them, and sharing insights into the latest threat trends and attack techniques.

Security Monitoring: Continuously monitor endpoints for signs of suspicious activity, using advanced tools and techniques to detect and respond to threats in real-time. This includes monitoring for malware, phishing attacks, data exfiltration, and other types of cyber threats.

**Incident Response:** In the event of a security incident, the provider will take immediate action to contain the threat and prevent further damage. This includes investigating the incident, containing the affected systems, and working with the company to develop a remediation plan.

**Reporting and Analytics:** Provide regular reports and analytics to the company, highlighting the current state of the company's security posture and identifying areas of improvement. These reports should be actionable and provide specific recommendations for enhancing the company's security defences.

#### **II.2.14) Additional information**

PLEASE NOTE: THIS PIN SUPERCEDES PIN ISSUED ON 28/03/2023 IN ERROR UNDER THRESHOLD. PLEASE RE-REGISTER YOUR INTEREST AGAINST THIS PIN.

#### **II.3) Estimated date of publication of contract notice**

1 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

---

### **Section VI. Complementary information**

#### **VI.3) Additional information**

PLEASE NOTE: THIS PIN SUPERCEDES PIN ISSUED ON 28/03/2023 IN ERROR UNDER THRESHOLD. PLEASE RE-REGISTER YOUR INTEREST AGAINST THIS PIN.

NOTE: To register your interest in this notice and obtain any additional information please visit the myTenders Web Site at

[https://www.mytenders.co.uk/Search/Search\\_Switch.aspx?ID=229073](https://www.mytenders.co.uk/Search/Search_Switch.aspx?ID=229073).

(MT Ref:229073)