LFC-24-049x

Procurement of Managed Security Information Event Management System

Report to:	**Date:**
Finance and Investment Board.....	25 April 2024
Commissioner's Board	14 May 2024
Deputy Mayor's Fire Board	3 July 2024
London Fire Commissioner	

Report by:
Chief Information Officer

Report classification:
For decision

For publication

I agree the recommended decision below.

Andy Roe
London Fire Commissioner

Date This decision was remotely signed on 9 September 2024

PART ONE

Non-confidential facts and advice to the decision-maker

Executive Summary

The report seeks authority for the LFC to enter into a contract to provide a managed "security information event management service" (SIEM). A SIEM is a solution that helps organisations detect, analyse, and respond to security threats before they have the opportunity to harm business operations. The system collects "event" log data from a range of sources and analyses a high volume of data in seconds to alert on activity that deviates from the norm with real-time analysis.

Recommended decision

For the London Fire Commissioner

The London Fire Commissioner delegates authority to the Assistant Director Procurement and Commercial to enter into contracts for the procurement of a managed SIEM, up to the value stated in part 2 of this report, for a period of up to five years.

1. Introduction and background

1.1 The security threat posed to organisations around the globe from cyber-attacks, including ransomware/malware, data extortion and associated threats, has increased exponentially in recent years. The on-going situation in Ukraine has resulted in an increased threat level to the UK, as a result of hostile cyber events emanating from a range of sources, including state actors.

1.2 The LFC regularly receives security information from a range of sources, central & local government, other fire and rescue services, as well as specialist security organisations. The view from Government at present is that whilst there is no specific threat emanating from hostile actors in relation to the LFB, there is a risk of organisations suffering collateral damage in the event of a sophisticated cyber-attack against the UK.

1.3 The threat from cyber criminals continues to increase with capability predicted to increase over the next two years, due to advancements in artificial intelligence [1](AI) and exploitation of this technology. In recognition of the ever-increasing threat posed to LFC systems and data by the

[1] AI - **Artificial intelligence**, or AI, is technology that enables computers and machines to simulate human intelligence and problem-solving capabilities

cyber threat, the LFC has installed a cyber-defence system "Darktrace". This system uses artificial intelligence and machine learning, to initially define a "normal" state and subsequently to detect "anomalies" and take autonomous action to neutralise threats.

1.4 However, in recognition of the current risk landscape, it is now considered essential for organisations to have multi-layered defences, offering "strength in depth", when it comes to the security of information and assets. Whilst the Darktrace system may be referred to as the ultimate line of defence to cyber threats, a SIEM is concerned with consuming and analysing large volumes of information from a wide range of sources rapidly, identifying anomalies and alerting on suspicious behaviour, before an actual security incident occurs.

1.5 The LFC currently uses a SIEM from Microsoft known as "Sentinel" which has been configured to interface with a small number of LFC systems. However it is clear that once the SIEM is fully deployed, the amount of information provided will be significant and consume scarce security team resource. It is therefore considered that the security needs of the LFC could better be met by contracting with an external organisation to provide the SIEM as a "service".

1.6 Taking the above into account, the proposal is to enter into a contract with an external organisation to manage the SIEM on behalf of the LFC. This provides an opportunity to ensure that security alerts are appropriately acted on and prioritised by dedicated analysts, to provide crucial insight and expertise on a 24x7 basis. In addition, the solution by design will be scalable, so that as the number and complexity of LFC systems increases and services continue to be migrated from on-premise to the cloud[2], the managed service will have the ability to "flex" to accommodate this with fast deployment and reduced setup costs.

2. Objectives and Expected Outcomes

2.1 The objective of this report is to secure authorisation to enter into a contract for the provision of a managed SIEM, with an external organisation.

2.2 The outcome of this procurement will be that once implemented, the LFC will be able to take additional assurance that information and systems (in support of both font line and back-office systems) are protected by a multi-layered security approach, reducing the likelihood of security events impacting on LFC operations.

3 Equality comments

3.1 The LFC and the Deputy Mayor for Planning, Regeneration and the Fire Service are required to have due regard to the Public Sector Equality Duty (section 149 of the Equality Act 2010) when taking decisions. This in broad terms involves understanding the potential impact of policy and decisions on different people, taking this into account and then evidencing how decisions were reached.

[2] The cloud is a metaphor **for a global network of remote servers that operates as a single ecosystem**, commonly associated with the Internet.

3.2 It is important to note that consideration of the Public Sector Equality Duty is not a one-off task. The duty must be fulfilled before taking a decision, at the time of taking a decision, and after the decision has been taken.

3.3 The protected characteristics are: age, disability, gender reassignment, pregnancy and maternity, marriage and civil partnership (but only in respect of the requirements to have due regard to the need to eliminate discrimination), race (ethnic or national origins, colour or nationality), religion or belief (including lack of belief), sex, and sexual orientation.

3.4 The Public Sector Equality Duty requires decision-takers in the exercise of all their functions, to have due regard to the need to:

- eliminate discrimination, harassment and victimisation and other prohibited conduct.
- advance equality of opportunity between people who share a relevant protected characteristic and persons who do not share it.
- foster good relations between people who share a relevant protected characteristic and persons who do not share it.

3.5 Having due regard to the need to advance equality of opportunity between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:

- remove or minimise disadvantages suffered by persons who share a relevant protected characteristic where those disadvantages are connected to that characteristic.
- take steps to meet the needs of persons who share a relevant protected characteristic that are different from the needs of persons who do not share it.
- encourage persons who share a relevant protected characteristic to participate in public life or in any other activity in which participation by such persons is disproportionately low.

3.6 The steps involved in meeting the needs of disabled persons that are different from the needs of persons who are not disabled include, in particular, steps to take account of disabled persons' disabilities.

3.7 Having due regard to the need to foster good relations between persons who share a relevant protected characteristic and persons who do not share it involves having due regard, in particular, to the need to:

- tackle prejudice
- promote understanding.

3.8 An equalities impact assessment has not been carried out for this procurement. The introduction of a managed SIEM should be entirely transparent to LFC staff.

4. Other Considerations

Workforce comments

4.1 There are no plans for workforce consultation.

Sustainability comments

4.2 This reports discusses a managed security information event management service which will help LFB detect, analyse, and respond to security threats before they have the opportunity to harm business operations.

4.3 This report does not introduce any significant sustainability impacts. Where new policies and/or corporate projects arise, they are subject to the Brigade's sustainable development impact assessment process.

Procurement comments

4.4 Procurement will identify a suitable route to market once the procurement starts. The GLA Collaborative Procurement Board have been formally approached regarding collaboration in respect of this procurement. However, the LFC has been advised that there are currently no collaborative opportunities available in respect of a managed SIEM.

4.5 The NFCC has been approached with the intention of identifying collaboration opportunities. The NFCC have no specific plans to develop a managed SIEM for the sector. However, plans are being developed to put in place to develop a "security operations centre" for the FRS sector. The pre-requisite for joining this service will be that each FRS has either implemented its own SIEM (or service). It is anticipated that it will be at least three years until an opportunity exists for the LFC to join in this sector initiative, which will provide a range of services in the security space.

4.6 If appropriate procurement will assess the market and/or conduct some early market engagement with suppliers to ensure there is an appetite for the requirements and to test routes to market such as the Crown Commercial Service framework, Cyber Security Services 3.

4.7 The proposed new contract is intended to be for five years and that is what the funding requested in Part 2 supports. The procurement team will work with ICT to agree an optimum contract duration (e.g. this could be an initial three-year contract with the ability to extend the contract length by up to a further two-years but this will be confirmed prior to issuing the opportunity to market).

Communications comments

4.8 This report is not expected to have any direct communications implications.

5. Financial comments

5.1 The report seeks authority for the LFC to enter into a contract to provide a managed "security information event management service" (SIEM).

5.2 Further comments are set out in Part 2 of the report.

6. Legal comments

6.1 Under section 9 of the Policing and Crime Act 2017, the London Fire Commissioner (the "LFC") is established as a corporation sole with the Mayor appointing the occupant of that office. Under section 327D of the GLA Act 1999, as amended by the Policing and Crime Act 2017, the

Mayor may issue to the Commissioner specific or general directions as to the manner in which the holder of that office is to exercise his or her functions.

6.2 By direction dated 1 April 2018, the Mayor set out those matters, for which the LFC would require the prior approval of either the Mayor or the Deputy Mayor for Planning, Regeneration and the Fire Service (the "Deputy Mayor").

6.3 Paragraph (b) of Part 2 of the said direction requires the LFC to seek the prior approval of the Deputy Mayor before "[a] commitment to expenditure (capital or revenue) of £150,000 or above as identified in accordance with normal accounting practices…". The value of the SIEM service is set out in part 2 to this report and exceeds this threshold. The Deputy Mayor's approval is therefore required.

6.4 The SIEM service proposal is consistent with the LFC's power under section 7 (2)(a) of the Fire and Rescue Services Act 2004, under which the LFC must secure the provision of personnel, services and equipment necessary to efficiently meet all normal requirements for firefighting and section 5A of the Fire and Rescue Services Act 2004 may do anything they consider appropriate for purposes incidental to their functional purposes. This includes the provision of ITC equipment and the necessary cybersecurity measures to ensure their continued functionality.

6.5 Any proposed procurement will be undertaken in compliance with the Public Contracts Regulations 2015 and the LFC's standing orders and policies.

List of Appendices

Appendix	Title	Open or confidential
1.	None	

Part two confidentiality

Only the facts or advice considered to be exempt from disclosure under the FOI Act should be in the separate Part Two form, together with the legal rationale for non-publication.

Is there a part 2 form – YES