

DMPC Decision – PCD 906

Title: Network Intrusion & Prevention (ExtraHop) Industrialisation

Executive Summary:

This paper seeks approval to proceed with the procurement and further implementation of a network intrusion and prevention solution based upon the ExtraHop Reveal(x) technology. A proof of value pilot based on the ExtraHop Reveal(x) technology has completed successfully and the MPS are now looking to turn this into an enterprise scale solution. This is in support of the MPS Cyber Security Strategy.

Recommendation:

The Deputy Mayor for Policing and Crime is recommended to:

1. Approve the contract award and procurement via CDW the current value added reseller contract at a value of £2,439,500 for a 3 year period.
2. Approve:
 - Capital expenditure of £577,700 (£370,900 in 2020/21 and £206,800 in 2021/22) to cover the industrialisation of ExtraHop. This includes the purchase of work of the SIAM, Network and Hosting Towers to implement ExtraHop and Kedron (3rd Party) to deploy the solution. This will be funded from the MOPAC approved Digital Policing Capital Budget.
 - Project Revenue expenditure of £36,600 (£35,000 in 2020/21 and £1,600 in 2021/22) to cover an IT Health Check and the decommissioning of the old infrastructure. This will be funded from the MOPAC approved Digital Policing Project Revenue Budget.
 - Ongoing Revenue expenditure of £4,201,100 (£198,300 in 2020/21 and £1,000,700 per annum thereafter) to cover Business As Usual costs of licencing and support. This will be funded from the MOPAC approved Digital Policing Revenue Budget.

Deputy Mayor for Policing and Crime

I confirm I have considered whether or not I have any personal or prejudicial interest in this matter and take the proposed decision in compliance with the Code of Conduct. Any such interests are recorded below.

The above request has my approval.

Signature



Date 16/12/2020

PART I - NON-CONFIDENTIAL FACTS AND ADVICE TO THE DMPC

1. Introduction and background

- 1.1. The MPS published the Cyber Security Strategy externally in late 2019, which focused on a number of key themes revolving around protecting data, reinforcing identities, inspecting network traffic and training preparedness. These are borne out from the need to protect the organisation from external threats and from those emanating from within. The Strategy focuses on providing approaches and outcomes in meeting the perceived and actuated threats.
- 1.2. Traditionally Policing operated from closed environments within its own boundary with only essential egress of services to other Police / Criminal Justice partners. The boundary controls robust as they are generally kept external threats at bay. Over time and more so today through mobility and accessing external services (e.g. Cloud, Collaboration etc.) these closed environments have opened up and data is now accessible on the move. While the landscape is changing the threat exposure is greater, organisations evolve and so do threats.
- 1.3. One of the core pillars of the strategy is Transparency of Traffic, where harmful content must be excluded where possible, detected where not and contained where it exists. Understanding and monitoring data movement throughout systems is critical.
- 1.4. The proposed solution from ExtraHop Reveal(x) uses the network and the transactions that flow across it as the most comprehensive source of data, which provides insight into what is happening in the environment. Reveal(x) is central to the Met's ability to provide visibility across these discrete areas. Reveal(x) can also aid in the identification of where sensitive data is accessed and moved unexpectedly and in the aftermath of a breach, can pinpoint exactly what data was accessed, from where and by whom to determine the breadth and severity of a breach and identify compromised records.

2. Issues for consideration

- 2.1. This information is contained in the restricted section of the report.

3. Financial Comments

- 3.1. £577.7k of Capital costs for the industrialisation of Network Detection and Response technology will be funded from the MOPAC approved Digital Policing Capital Budget.
- 3.2. £36.6k of Project Revenue costs will be funded from the MOPAC approved Digital Policing Project Revenue Budget.
- 3.3. £198.3k Year one Ongoing Revenue costs (Year 2 onwards: £1,000.7k) will be funded from the MOPAC approved Digital Policing Revenue Budget. As Network traffic analysis supports the MPS Cyber Security Strategy, investment of ongoing costs has been factored into the medium term financial plans for Digital Policing.

4. Legal Comments

- 4.1. The Mayor's Office for Policing and Crime ("MOPAC") is a contracting authority as defined in the Public Contracts Regulations 2015 ("the Regulations"). All awards of public contracts for goods and/or services valued at £189,330 or above shall be procured in compliance with the Regulations and MOPAC governance. This report confirms the value of the proposed contract exceeds the above threshold. Accordingly, the Regulations shall be engaged.
- 4.2. The route to market shall be the MOPAC's reseller contract with CDW. The report confirms the proposed contract falls within the technical and financial scope of the CDW contract and that the CDW contract was procured compliantly. The procurement of ExtraHop Reveal(x) via CDW is a compliant route to market.
- 4.3. Paragraph 4.8 of the MOPAC Scheme of Delegation and Consent provides that the Deputy Mayor for Policing and Crime (DMPC) has delegated authority to approve business cases for revenue or capital expenditure of £500,000 or above.
- 4.4. Under paragraph 4.13 of the MOPAC Scheme of Delegation and Consent the Deputy Mayor for Policing and Crime ("DMPC") has delegated authority to approve all requests to go out to tender for contracts of £500,000 or above. Further, the DMPC has delegated authority under the same paragraph to approve the procurement strategy for all revenue and capital contracts of a total value of £500,000 or above, such determination to include decisions on the criteria and methodology to be adopted in the tendering process, any exemptions from procurement requirements, and any necessary contract extensions.
- 4.5. Under paragraph 4.15 of the MOPAC Scheme of Delegation and Consent the DMPC has authority to award contracts with a total value of £500,000 or above.

5. Commercial Issues

- 5.1. This software will be procured for a contract period of 3 years at a value of £2,439.5k via the Value added reseller (VAR) contract with CDW, which was awarded via the Tech products Crown Commercial Services Framework Agreement. This is a compliant procurement route.
- 5.2. A review of the market was conducted to identify the market leaders in Network, Detection and Response technology, with particular emphasis on the ability to monitor "network traffic analysis".
- 5.3. Four vendors were considered. The Cyber security team completed a technical review of the options, which included both technical demonstrations and commercial presentations.
- 5.4. From this, two options were shortlisted. Both vendors provided the MPS with a device to test in a lab environment. This gave analysts an insight into the level of effort

required to integrate such technology into the MPS infrastructure using the current technology available.

5.5. Following evaluation of each solution ExtraHop Reveal(x) was deemed to be the most suitable solution for the MPS as it met the business requirements.

5.6. The remainder of this information is contained in the restricted section of the report.

6. GDPR and Data Privacy

6.1. There are no GDPR issues arising from this request.

6.2. The MPS is subject to the requirements and conditions placed on it as a 'State' body to comply with the European Convention of Human Rights and the Data Protection Act (DPA) 2018. Both legislative requirements place an obligation on the MPS to process personal data fairly and lawfully in order to safeguard the rights and freedoms of individuals.

6.3. Under Article 35 of the General Data Protection Regulation (GDPR) and Section 57 of the DPA 2018, Data Protection Impact Assessments (DPIA) become mandatory for organisations with technologies and processes that are likely to result in a high risk to the rights of the data subjects.

6.4. The Information Assurance and Information Rights units within MPS will be consulted at all stages to ensure the project meets its compliance requirements.

6.5. The project does not use personally identifiable data of members of the public, so there are no GDPR issues to be considered.

7. Equality Comments

7.1. There are no equality or diversity issues arising from this request.

8. Background/supporting papers

8.1. MPS Report.

Public access to information

Information in this form (Part 1) is subject to the Freedom of Information Act 2000 (FOIA) and will be made available on the MOPAC website following approval.

If immediate publication risks compromising the implementation of the decision it can be deferred until a specific date. Deferral periods should be kept to the shortest length strictly necessary.

Part 1 Deferral:

Is the publication of Part 1 of this approval to be deferred? NO

If yes, for what reason:

Until what date: n/a

Part 2 Confidentiality: Only the facts or advice considered as likely to be exempt from disclosure under the FOIA should be in the separate Part 2 form, together with the legal rationale for non-publication.

Is there a **Part 2** form – YES

ORIGINATING OFFICER DECLARATION

Tick to confirm statement (✓)

Financial Advice:

The Strategic Finance and Resource Management Team has been consulted on this proposal.

✓

Legal Advice:

The MPS legal team has been consulted on the proposal.

✓

Equalities Advice:

Equality and diversity issues are covered in the body of the report.

✓

Commercial Issues

The proposal is in keeping with the GLA Group Responsible Procurement Policy.

✓

GDPR/Data Privacy

- GDPR compliance issues are covered in the body of the report.
- A DPIA is not required.

✓

Director/Head of Service:

The Interim Chief Finance Officer has reviewed the request and is satisfied it is correct and consistent with the MOPAC's plans and priorities.

✓

Chief Executive Officer

I have been consulted about the proposal and confirm that financial, legal and equalities advice has been taken into account in the preparation of this report. I am satisfied that this is an appropriate request to be submitted to the Deputy Mayor for Policing and Crime.

Signature



Date 9/12/2020

MAYOR OF LONDON
OFFICE FOR POLICING AND CRIME

Network Intrusion & Prevention (ExtraHop) Industrialisation

MOPAC Investment Advisory & Monitoring meeting 17/11/2020

Report by Angus McCallum on behalf of the Chief of Corporate Services

Part 1 – This section of the report will be published by MOPAC. It is classified as OFFICIAL – PUBLIC**EXECUTIVE SUMMARY**

This paper seeks approval to proceed with the procurement and further implementation of a network intrusion and prevention solution based upon the ExtraHop Reveal(x) technology. A proof of value pilot based on the ExtraHop Reveal(x) technology has completed successfully and we are now looking to turn this into an enterprise scale solution. This is in support of the MPS Cyber Security Strategy.

Recommendations

The Deputy Mayor for Policing and Crime, via the Investment Advisory and Monitoring meeting (IAM), is asked to:

1. **Approve the contract award and procurement via CDW the current value added reseller contract at a value of £2,439.5k for a 3 year period.**
2. **2.1 Approve Capital expenditure of £577.7k (£370.9k in 2020/21 and £206.8k in 2021/22) to cover the industrialisation of ExtraHop. This includes the purchase of work of the SIAM, Network and Hosting Towers to implement ExtraHop and the 3rd Party supplier to deploy the solution. This will be funded from the MOPAC approved Digital Policing Capital Budget.**
2.2 Approve Project Revenue expenditure of £36.6k of Project Revenue (£35k in 2020/21 and £1.6k in 2021/22) to cover an IT Health Check and the decommissioning of the old infrastructure. This will be funded from the MOPAC approved Digital Policing Project Revenue Budget.
2.3 Approve ongoing Revenue expenditure of £4,201.1k (£198.3k in 2020/21 and £1,000.7k per annum thereafter) to cover Business As Usual costs of licencing and support. This will be funded from the MOPAC approved Digital Policing Revenue Budget.

Time sensitivity

A decision is required from the Deputy Mayor by (01/12/2020) to ensure that we secure commercial discount.

Non-confidential facts and advice to the Deputy Mayor for Policing and Crime

Introduction and background

- 1.1 The MPS published the Cyber Security Strategy externally in late 2019, which focused on a number of key themes revolving around protecting data, reinforcing identities, inspecting network traffic and training preparedness. These are borne out from the need to protect the organisation from external threats and from those emanating from within. The Strategy focuses on providing approaches and outcomes in meeting the perceived and actuated threats.
- 1.2 Traditionally Policing operated from closed environments within its own boundary with only essential egress of services to other Police / Criminal Justice partners. The boundary controls robust as they are generally kept external threats at bay. Over time and more so today through mobility and accessing external services (e.g. Cloud, Collaboration etc.) these closed environments have opened up and data is now accessible on the move. While the landscape is changing the threat exposure is greater, organisations evolve and so do threats.
- 1.3 One of the core pillars of the strategy is Transparency of Traffic, where harmful content must be excluded where possible, detected where not and contained where it exists. Understanding and monitoring data movement throughout systems is critical.
- 1.4 The proposed solution from ExtraHop Reveal(x) uses the network and the transactions that flow across it as the most comprehensive source of data, which provides insight into what is happening in the environment. Reveal(x) is central to the Met's ability to provide visibility across these discrete areas. Reveal(x) can also aid in the identification of where sensitive data is accessed and moved unexpectedly and in the aftermath of a breach, can pinpoint exactly what data was accessed, from where and by whom to determine the breadth and severity of a breach and identify compromised records.

Issues for consideration

This information is contained in the restricted section of the report.

Contributes to the MOPAC Police & Crime Plan 2017-2021¹

ExtraHop Reveal(X) provides a Network Detection and Response capability that will protect the digital infrastructure of the MPS by making best use of technology in

¹ [Police and crime plan: a safer city for all Londoners | London City Hall](#)

readiness for Cyber emergencies.

Financial, Commercial and Procurement Comments

£577.7k of Capital to fund the industrialisation of Network Detection and Response technology will be funded from the MOPAC approved Digital Policing Capital Budget.

£36.6k of Project Revenue costs will be funded from the MOPAC approved Digital Policing Project Revenue Budget.

£198.3k Year one Ongoing Revenue costs (Year 2 onwards: £1,000.7k) will be funded from the MOPAC approved Digital Policing Revenue Budget. As Network traffic analysis supports the MPS Cyber Security Strategy, investment of ongoing costs has been factored into the medium term financial plans for Digital Policing.

This will be procured for a contract period of 3 years at a value of £2,439.5k via the Value added reseller (VAR) contract with CDW, which was awarded via the Tech products Crown Commercial Services Framework Agreement.

Two potential Network Detection and response solutions were shortlisted. Following evaluation of each solution ExtraHop Reveal(x) was deemed to be the most suitable solution for the MPS as it met the business requirements.

The remainder of this information is contained in the restricted section of the report.

Legal Comments

The Mayor's Office for Policing and Crime ("MOPAC") is a contracting authority as defined in the Public Contracts Regulations 2015 ("the Regulations"). All awards of public contracts for goods and/or services valued at £189,330 or above shall be procured in compliance with the Regulations and MOPAC governance. This report confirms the value of the proposed contract exceeds the above threshold. Accordingly, the Regulations shall be engaged.

The route to market shall be the MOPAC's reseller contract with CDW. The report also confirms the proposed contract falls within the technical and financial scope of the CDW contract and that the CDW contract was procured compliantly. The procurement of ExtraHop Reveal(x) via CDW is a compliant route to market.

Paragraph 4.8 of the MOPAC Scheme of Delegation and Consent provides that the Deputy Mayor for Policing and Crime (DMPC) has delegated authority to approve business cases for revenue or capital expenditure of £500,000 or above.

Under paragraph 4.13 of the MOPAC Scheme of Delegation and Consent the Deputy Mayor for Policing and Crime ("DMPC") has delegated authority to approve all requests to go out to tender for contracts of £500,000 or above. Further, the DMPC has delegated authority under the same paragraph to approve the procurement strategy for all revenue and capital contracts of a total value of £500,000 or above, such determination to include decisions on the criteria and methodology to be adopted in the tendering process, any exemptions from procurement requirements, and any necessary contract extensions.

Under paragraph 4.15 of the MOPAC Scheme of Delegation and Consent the DMPC has authority to award contracts with a total value of £500,000 or above.

Equality Comments

There are no equality or diversity issues arising from this request.

Privacy Comments

There are no GDPR issues arising from this request.

The MPS is subject to the requirements and conditions placed on it as a 'State' body to comply with the European Convention of Human Rights and the Data Protection Act (DPA) 2018. Both legislative requirements place an obligation on the MPS to process personal data fairly and lawfully in order to safeguard the rights and freedoms of individuals.

Under Article 35 of the General Data Protection Regulation (GDPR) and Section 57 of the DPA 2018, Data Protection Impact Assessments (DPIA) become mandatory for organisations with technologies and processes that are likely to result in a high risk to the rights of the data subjects.

The Information Assurance and Information Rights units within MPS will be consulted at all stages to ensure the project meets its compliance requirements.

The project does not use personally identifiable data of members of the public, so there are no GDPR issues to be considered.

Real Estate Implications

There are no estate issues as a result of this request.

Environmental Implications

The suppliers will need to adhere to environmental legislation, the MPS Environmental policy and the waste duty of care code of practice in relation to any waste disposal as a result of decommissioning equipment.

Background/supporting papers

The MPS report.

Report author: (Natalie Gabriel, Business Analyst)

Part 2 – This section refers to the details of the Part 2 business case which is NOT SUITABLE for MOPAC Publication.

The Government Security Classification marking for Part 2 is:
OFFICIAL-SENSITIVE [COMMERCIAL]

Part 2 of the Industrialisation of My1Login Platform paper is exempt from publication for the following reasons:

- Exempt under Article 2(2)(a) of the Elected Local Policing Bodies (Specified Information) Order 2011 (Data Protection Section 43 – Commercial Interests).
- The relevant sections under the FOIA that would exempt this information from disclosure, for example:
 - Commercial Interest Section 43

The paper will cease to be exempt in accordance with the MPS Records Management Policy to retain information for a minimum of 6 years in line with MoPI guidelines.