June 26, 2024

A – Addendum #1

RFP – IT2024MDR – Managed Detect and Response Services

Q1: Is the RMOW looking to have the successful proponent to provide MDR service across the RMOW's entire attack surface including networks, firewalls, SaaS applications, authentication, and Cloud environments? If so, can you please provide background on these environments.

> A1: As per section 2.1 Solution Requirements, the scope of work includes proactive monitoring of RMOW 362 Desktop and Laptop Workstations and 91 Server Endpoints only.

Q2: Will there be an opportunity for short-listed proponents to present their solution as part of this RFP process?

> A2: See section 5.4 Interviews in the RFP document.

Q3: Is the RMOW looking for the proponent to provide on-going support and recommendations to strengthen their security posture on an on-going basis?

> A3: Yes, on-going support is required as it relates to the requirements in section 2.1 Solution Requirements. However, broader Cyber Security assessments and recommendations are not part of the scope of work.

Q4: Clarification questions regarding the Resort Municipality of Whistler's Request for Proposal #IT2024MDR for Managed Detect and Response Services:

1. How many Internet-facing firewalls do you have?
2. Where are servers located? (on-prem, private data center, Azure, AWS, etc.)
3. Are all servers Windows 2012 R2 or newer? Please specify if otherwise, including quantities.
4. How many IT users do you have?
5. Are all IT users considered "knowledge workers," or do you have e-mail only users as well? Please specify quantities of each.
6. Where is email hosted? (On-premise, Google, Microsoft, etc.)
7. What Antivirus/EDR is in place on workstations and servers?
8. Are all workstations Windows 10 or newer? Please specify if otherwise, including quantities.
9. Do you use Microsoft 365 services? And if so, can you specify licenses and quantities in use?
10. What (if any) email hygiene products are in use (Defender for Office, Proofpoint, Mimecast, etc.)
11. Are there any SIEM products in place, and is there a preference to keep or replace them?
12. Do you have a Security Aware solution in place? (KnowB4, Beauceron, SafeTitan, etc.)

13. Is Intune in place for management of mobile devices and workstations?
14. Do you operate, or subscribe to, a SOC service currently?

A4: Please see number points below, additionally product specifics that are not required to meet requirements in Section 2.1 Solution Requirements will not be published:

1. Not required as per Section 2.1 Solution Requirements
2. On Premise
3. Server OS version is Microsoft Windows Server 2016 or newer, 91 Windows Servers.
4. 430
5. 430, no email only users.
6. Microsoft Exchange Online
7. CrowdStrike Falcon
8. Workstations are Windows 10 or newer
9. The RMOW has 430 M365 licenses
10. Not in scope as per Section 2.1 Solution Requirements
11. Yes, a SIEM is in place
12. Yes
13. Yes, for Cell Phone, Tablet and Laptop devices
14. Yes

Q5: Given the nature of the RFP and the required time to develop a comprehensive response and consolidate questions to the client, we respectfully request a 2-week extension to the submission date from July 4th to July 18th.

A5: No extension will be granted.

Q6: What was the annual spending on this project last year? If this is a new contract, what is the annual budget?

A6: Approximately $50,000

Q7: How many vendors will be awarded?

A7: Please refer to section 4. Project Brief.

Q8: Is this bid refresh? If yes, Can you share details from where we can get old proposal details.

A8: This is a new bid opportunity.

Q9: Is RMOW able to provide an extension to the due date of July 4th, 2024?

A9: No extension will be granted.

End of Addendum