June 26, 2024

# A – Addendum #2

RFP – IT2024MDR – Managed Detect and Response Services

Q1: Is RMOW able to provide an extension to the due date of July 4th, 2024?

A1: No extension will be granted.

Q2: MDR Data Center: What threat detection capabilities do you have for your network servers and endpoints in your data center?

A2: Crowdstrike Falcon

Q3: MDR Cloud: How do you handle threat detection for your cloud resources?

A3: Not required as per Section 2.1 Solution Requirements

Q4: MDR Users: What methods do you use for threat detection based on User Behavior Analytics (UBA)?

A4: Unknown

Q5: MDR Response: How do you quickly contain threats with auto response (Auto Containment)?

A5: Yes Auto Containment

Q6: What existing security products do you want to include for the 24x7 Managed Detection & Response service?

A6: Crowdstrike Falcon

Q7: How many network protection products (FW, NGFW, IPS/IDS, UTM) do you have installed?

A7: Not required as per Section 2.1 Solution Requirements

Q8: How many advanced network protection products (NAC, APT, NTA) do you have installed?

A8: Not required as per Section 2.1 Solution Requirements

Q9: How many endpoints are covered by your end point protection product (AV)?

A9: Please refer to Section 2.1 Solution Requirements.

Q10: How many endpoints are covered by your advanced end point protection product (EDR, ATP, EPP)?

A10: Please refer to Section 2.1 Solution Requirements.

Q11: How many employees are covered by your web protection products (Proxy with URL Filtering)?

A11: Not required as per Section 2.1 Solution Requirements

Q12: How many application protection products (WAF) do you have installed?

A12: Not required as per Section 2.1 Solution Requirements

Q13: How many devices are onboarded to your log monitoring product (SIEM)?

A13: Not required as per Section 2.1 Solution Requirements

Q14: MDR Data Center: How do you integrate your data center assets, including existing security products, critical servers, and network resources?

A14: Not required as per Section 2.1 Solution Requirements

Q15: What critical data center products, such as L3 switches & routers that need log monitoring, do you have?

A15: Not required as per Section 2.1 Solution Requirements

Q16: What is the approximate volume of NetFlow traffic in GB per day?

A16: Not required as per Section 2.1 Solution Requirements

Q17: Servers: What critical servers do you want to include for the 24x7 Managed Detection & Response service? We will deploy MDR agents on these servers to detect threats, vulnerabilities, configurations, and for investigation.

A17: As per section 2.1 Solution Requirements, the scope of work includes proactive monitoring of 91 Server Endpoints.

Q18: Workloads: What cloud workloads and their counts do you have?

A18: Not required as per Section 2.1 Solution Requirements

Q19: Security Resources: What cloud security resources and their counts do you have?

A19: Not required as per Section 2.1 Solution Requirements

Q20: MDR Cloud: How do you ensure unified security for your assets in Azure, AWS, GCP, and for all your SaaS applications?

A20: Not required as per Section 2.1 Solution Requirements

Q21: SaaS Applications: What SaaS solutions do you currently use and want to include for MDR service?

A21: Not required as per Section 2.1 Solution Requirements

Q22: If you have provided us with Proxy, O365, and/or SaaS users, you will get UBA by default. Do you want to add any of the following user sources? If so, please provide details:

A22: Not required as per Section 2.1 Solution Requirements

Q23: How many users are covered by your Active Directory?

A23: Not required as per Section 2.1 Solution Requirements

Q24: How many users are covered by your email gateway?

A24: Not required as per Section 2.1 Solution Requirements

Q25: How many users are covered by your VPN?

A25: Not required as per Section 2.1 Solution Requirements

Q26: How many users are covered by your PIM/PAM?

A26: Not required as per Section 2.1 Solution Requirements

Q27: EDR: If you want to add EDR to your existing user computing devices, how many desktops and laptops do you have?

A27: 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.

Q28: MDR Users & Endpoints: How do you integrate your user sources for user monitoring with User Behavior Analytics (UBA)?

A28: Unknown

Q29: Will it be okay if the services team is based outside Canada but accessing/processing data services? Is there requirement for onsite visit or can all these devices be managed fully remote?.

A29: Solution must comply with all legislation and privacy requirements that are applicable to Local BC Government organizations**.** No requirement for onsite visit

Q30: Could you please confirm if Whistler currently has an Endpoint Detection and Response (EDR) solution deployed? If yes, could you specify the brand and whether it is deployed across all IT assets?

A30: Yes. Crowdstrike Falcon, deployed to 453 workstations and servers

Q31: Does Whistler manage its MDR services in-house, or are they outsourced? If so, could you describe the current capabilities and any limitations of the existing MDR services?

A31: Managed by Crowdstrike

Q32: We would like to understand Whistler's IT environments -are they solely on-premises, hybrid, or cloud-native?  If cloud is used, which provider is currently in use?

A32: On-premise

Q33: Could you specify the regulatory or compliance standards that the MDR services must adhere to?

A33: Solution must comply with all legislation and privacy requirements that are applicable to Local BC Government organizations.

End of Addendum