350 Albert Street, Suite 700
Ottawa, Ontario K1A 0S6
Canada

350, rue Albert, Bureau 700
Ottawa, Ontario K1A 0S6
Canada

# ADDENDUM NO. 2

## QUESTIONS AND ANSWERS (Q&A) No. 2

## RFP No. 106205.138

## MANAGED SECURITY SERVICES (“MSS”)

**September 11, 2023**

| No. | Questions | Answers |
|---|---|---|
| 1 | Schedule 1 to Appendix A references 250 endpoints. Please provide details on these endpoints. Are these a combination of workstations, servers, or both? Please provide details. | Combination of workstations and servers. |
| 2 | Appendix A references on-premises and cloud-based assets. Please confirm the number of data centers and cloud providers. | Microsoft is the main cloud system. There are a handful of other critical cloud systems that we'd also consider. i.e. HRIS. |
| 3 | Does CCC require the services to be delivered by Canadian resources? If so, do these resources require any Canadian security clearance. | Yes. Security clearance would be preferred. |
| 4 | The CCC requires the solution to comply with the Government of Canada’s Direction for Electronic Data Residency. In order to do so, the proponent is asking for clarification on how the CCC classifies its data. How does the CCC classify and categorize (Protected B, C, other) the specific information in scope of the required services including the logs and data collected in the SIEM. | Our data needs to reside in a Canadian data centre. We are unclear how the data classification applies to log data in scope for this project. CCC follows the PSPC security classification levels but they are not systematically applied across the organization. |
| 5 | We understand that the CCC does not have specific requirements for the yearly Penetration Test. However, please confirm that the CCC does not expect pricing for this capability at this stage. | These Penetration Test services are not included in the evaluation criteria and will not be rated. But, these services as well as other best practices services will be required. |
| 6 | Can the Penetration Testing services be delivered remotely by a global team? | No. |

| | | |
|---|---|---|
| 7 | At a high level, please describe your current security incident response and management process. | It's currently being developed, however, we need third party expertise to partner with us to remediate and respond in the event of an incident, hence this RFP. |
| 8 | Please outline the frequency or schedule for performing Dark Web hunting. | Unknown, we want to work with the partner to right size and address for this organization. |
| 9 | Please confirm: It is our understanding from section 1.4.1 that upon selection, the proponent will be required to provide terms and conditions and service description for review. | Yes. |
| 10 | Section 1.4.2 does not specify the number of renewals. Can the CCC clarify a maximum number of yearly renewals under the resulting contract? | No. |
| 11 | Please confirm what EDR and Antivirus are currently deployed (or planned to be deployed) on CCC infrastructure. | Microsoft 365 Defender (MDE, MDO, MDI), Windows Defender AV, Symantec AV. |
| 12 | Are EDR agents and Antivirus deployed on all assets in the infrastructure (both on premises and cloud)? | Yes, some exceptions. |
| 13 | How many major or critical incidents have CCC suffered in the last 12 months? | Zero. |
| 14 | If you have a current SIEM Solution: | No. |
| 15 | · How many EPS or MPS (Event/Messages Per Second) do you have generated from your current solution? | N/A. |
| 16 | · If not available, how many Gb per day/month of log data do you collect? | Under 1GB/day on premises (based on firewall / AD audit logs); M365 logs are difficult to estimate. The org comprises approx 120 active users and we are using E5 logging capabilities. |
| 17 | · Roughly how many use-cases do you currently have or would you like us to develop? | Do not understand this question. |
| 18 | · Do you have any SOAR playbooks configured? If so, how many? | No. |
| 19 | What is the number of sites you have where servers (log sources) are deployed? | One on premise data centre, and a few cloud based systems. Full scope will need to be determined. CCC is a small organization. |
| 20 | Can the deadline be extended two weeks | No. |

| | | |
|---|---|---|
| 21 | Please confirm if application servers, SQL and DCs are part of the 40-50 virtual machines. | Yes. |
| 22 | For integration with CCC Team Dynamix central ticketing system, please confirm that email notifications will meet your requirements. | E-mail should suffice, but API integration would be ideal. |
| 23 | In order to provide you with a quality response, we respectfully request an extension until October 6, 2023 | An extension is not being granted. |
| 24 | There is an ask regarding integration with CCC team ticketing system. How is this ticketing system expected to be used? Please elaborate. | Whatever method is typically used with your other customers. |
| 25 | Section 4.2, Item regarding installation and configuration of SIEM. Expectation is 45 days from signature to completing the onboarding. Are ALL log sources and ALL use case rules expected to be implemented within these 45 days? | The requirement is for the SIEM to be cloud based. There is flexibility with all log files. |
| 26 | Section 4.2, There is reference to Security Monitoring SLAs but there aren't any details given (or are not clear). Can you please provide the "monitoring SLA" expectations? | Please provide what you provide majority of customers. |
| 27 | Is the online retention requirement for 3 months mandatory? | Yes. |
| 28 | Dynamix central ticketing system, could we clarify if it is the Microsoft Dynamics 365 ticketing system or Team Dynamix ITSM? | Team Dynamix ITSM. |
| 29 | Do you have an ELA ( Enterprise License Agreement) with Microsoft? | Yes. |
| 30 | For the incident response team requirements, please confirm the number of hours per year for the Incident Response Retainer. | Vendor expected to provide this estimate based on their experience. |
| 31 | What is the number of users? (User: a person with an email and company owned device) | 120 users. |
| 32 | What is the number of Office 365 users? | 120 users. |
| 33 | How many locations with more than 50 users, servers on site and direct internet access and a firewall do you have? (if you backhaul the internet through a main location with a technology like Zscaler, that counts as 1 location) | One location, majority of staff are working remotely with managed client devices. |

| | | |
|---|---|---|
| 34 | What cloud environments do you have?(AWS, Azure, GPS) and what level of licensing? | Microsoft 365 Tenant with E5 licensing; Azure AD (no VM's or other IaaS deployed in Azure yet); HRIS, Corporate website (Wordpress). |
| 35 | How many servers do you have across your environment(on prem,  in the cloud, physical and virtual)? | Approximately 50. |
| 36 | Do you have any devices with base Windows OS in French or running English OS with French language pack on top? | No. |
| 37 | Is it understood that the supplier includes the price of the SIEM system in the proposal? If so, would it be possible to provide the following information: Firewall daily log quantities? | Under 1GB/day on premises (based on firewall / AD audit logs); M365 logs are difficult to estimate. The org comprises approx 120 active users and we are using E5 logging capabilities. |
| 38 | Do you accept that the SIEM is hosted in your Azure/Microsoft environments with billing directly integrated into your Microsoft contract? | The requirement is for a cloud based SIEM managed by the vendor. |
| 39 | Do you agree to have a virtual machine (linux) acting as a log/log collector and filter? - This virtual machine being the responsibility of the CCC at maintenance level? | Yes. |
| 40 | Would it be possible to supply the manufacturer of the firewall cluster? | Watchguard. |
| 41 | Apart from the tools/equipment mentioned in Appendix A, are there any other sources of logs that can be integrated into the SIEM (e.g. Darktrace, in-house systems, applications, etc.)? | Yes. |
| 42 | What is the current size of your cybersecurity team and the number of staff dedicated to monitoring and responding to alerts? | 1 staff. |
| 43 | Please share the pain points and any critical requirement in security services that would require immediate attention? | N/A. |
| 44 | Is CCC currently part of any threat intelligence sharing community? If yes, are these feeds already integrated into the SIEM? | N/A. |
| 45 | Is CCC open to having a SIEM solution such as Microsoft Sentinel that will be deployed in CCC's environment? | The requirement is for a cloud based SIEM managed by the vendor. |

| | | |
|---|---|---|
| 46 | Can a breakdown of the number of users be provided? | 120 users. |
| 47 | How many live external IPs are to be tested as part of the yearly penetration test? | Approximately 5. |
| 48 | Are there any web applications and if so, how many? | 1 web app. |
| 49 | Is there an expected GB/Day or Events Per Second (EPS) for the SIEM? | Our total footprint is fairly small so we don't have an expected minimum number of EPS or GB/day. |
| 50 | Is there a network diagram available? | We can provide rudimentary network diagrams. |
| 51 | What cloud services outside of O365 are in use like Azure, AWS, Google? | WP Engine for our Wordpress sites which uses Google Cloud Platform. |
| 52 | Is Microsoft Defender the current AV/EDR solution or is there something else deployed? | For remote devices yes, on premises we are using Symantec SEP with an on premises SEPM management server. |
| 53 | Based on the fact that you have current E5 licensing in place, is there appetite to continue down the Microsoft path with Microsoft Sentinel (SIEM)? | Yes, we would be open to using Sentinel as it makes sense to consolidate under the Microsoft umbrella, but we are open to other potential solutions as well. |
| 54 | What is the current number of employees? | Approx 120 active. |
| 55 | Who is the current Cyber Security insurance provider? | Coalition. |
| 56 | Are you utilizing a tool for vulnerability scanning? | Nessus. |
| 57 | Is there a current IR plan in place? If so, has it been reviewed? | It's currently being developed, however, we need third party expertise to partner with us to remediate and respond in the event of an incident, hence this RFP. |
| 58 | We work with a subcontractor whose data pipeline goes through AWS in Ireland without being stored. Tenancy remains in Canada. Would this be accepted by CCC? | We would consider this solution. |
| 59 | Are there any security clearance required for the proponent and/or subcontractor working on this project? | It would be an asset but not required. |

**END TO Q&A NO. 2**